19

RFID Technology, Security Vulnerabilities, and Countermeasures

Qinghan Xiao[1], Thomas Gibbons[2] and Hervé Lebrun[2]
[1]*Defence Research and Development Canada – Ottawa*
[2]*Canadian Operational Support Command*
Canada

1. Introduction

Radio frequency identification (RFID) is a means of automatic identification that uses radio waves to detect, track, identify, and thus manage a variety of objects. The purpose of an RFID system is transmitting data from a portable device, called a tag, to an RFID reader to execute a particular application based on the tag provided identification or location information (Graafstra, 2006; O' Brien, 2006).

RFID technology has been around for about 60 years and was originally developed for improving warfare technologies. The first application was developed by Britain as the Identify Friend or Foe (IFF) system, which was used to distinguish friendly aircraft from enemy aircraft during World War II (Landt, 2001). The second era of RFID technology began with the commercial activities in the 1960s. An early application was the development of electronic article surveillance (EAS) equipment to counter theft in retail stores. EAS as an early forerunner to RFID uses a '1-bit' signal to represent the presence or absence of a tag (Landt, 2005). The third era of RFID technology started in 1999, when the Auto-ID Centre was established at MIT to investigate new ways for improving bar code technology and implementing RFID technology in various commercial applications. The 1990's were a significant decade for RFID because of increased commercialization of RFID systems and the standardization activities on RFID technologies. Electronic toll collection systems were widely deployed in the United States; RFID tags were affixed to over 3 million rail cars in North America; and the International Organization for Standardization (ISO) developed several standards in the RFID field, including, for example, the ISO 18000 series of standards that define the air interfaces, collision detection mechanisms, and communication protocols for different frequency bands (Knospe & Pohl, 2004). In the 21st century, with the development of RFID standards, decreasing prices, and mandates from large organizations such as Wal-Mart and the U.S. Department of Defense (DoD), RFID has become "the first important technology of the twenty-first century" (Garfinkel & Rosenberg, 2005).

An RFID system has three key components: the tag, the reader, and the backend system. RFID tags, also known as transponders, are identification devices that are attached to objects. Each tag typically consists of an antenna constructed from a small coil of wires; a microchip used to store information electronically about the object (e.g. a vehicle or a container); and encapsulating material to enclose the chip and the coil. Like there are various types of barcode, RFID tags are available with different memory sizes and encoding

Source: Supply Chain, The Way to Flat Organisation, Book edited by: Yanfang Huo and Fu Jia,
ISBN 978-953-7619-35-0, pp. 404, December 2008, I-Tech, Vienna, Austria

options. However, an RFID tag offers the capability to store a unique serial number and product information for each item, not just the class of the items. The tag can also incorporate sensors to record temperature, shock, or humidity, for example, providing the ability to track and report on an object's environmental characteristics dynamically.

An RFID reader, also called an interrogator or scanner, is the device used to communicate with the RFID tag. It emits RF signals to, and receives radio waves from, the tag via an antenna or antennas. The reader converts the received radio waves into digital information that is usually passed to a backend system. Readers, either as stationary or handheld devices, consist of a transmitter, receiver, antenna, microprocessor, controller, memory and power source.

A backend system, sometimes referred to as an online database, is needed to collect, filter, process, and manage the RFID data. The backend stores complete records of product information, tracking logs, and key management information associated with the RFID tags. It is critical for an RFID application to perform data collection, data management, and data analysis accurately and efficiently.

There are various areas in which RFID technology has been implemented, including the following significant applications.

- RFID electronic toll collection systems identify vehicles mounted with RFID transponders and automatically deduct toll fees electronically without impeding traffic flow.
- Animal RFID implant tags have been used to identify and track animals and obtain information about their owners. Combined with GPS, it is possible to perform around-the-clock surveillance of individual animals and fish in the wild.
- RFID book tracking is a hot topic in the library community for use in managing extensive collections of books, manuscripts, and rare items, as well as offering self checkout and protection against theft.
- Healthcare providers are considering the use of RFID technology to improve the ability to accurately identify and track patients, hospital staff, medical equipment, and blood products. A number of case studies have demonstrated that not only does RFID technology make treatment safer and more efficient, but it also has the side benefits of preventing identity theft and reducing paper work, both of which cut costs. However, a newly published research study revealed that RFID systems in hospitals might cause critical care medical equipment to malfunction (van der Togt et al., 2008).
- The pharmaceutical industry deploys RFID technology to track drugs, reduce inventory cost, and prevent counterfeiting and theft. The administrator for the U.S. Centers for Medicare and Medicaid Services, Mark McClellan, called RFID "the most promising technology" for dealing with drug-counterfeiting problems (Whiting 2004).
- Access control has been among the most common applications of RFID technology because RFID badges provide many advantages over traditional access control badges, including fast access, durability without mechanical wear, and a superior ability to protect data on the card. In addition to traditional applications such as building access, RFID access cards have been used in less traditional applications such as ski passes, metro passes, and toll gates.
- The e-passport is the next generation of passport, which is equipped with an embedded RFID chip to store digital information and biometric data of the passport holder. The objective is to provide a trusted document to reduce fraud, make immigration control faster, and enhance the level of security.

- Supply chains are the biggest beneficiary of the RFID technology. The use of RFID in supply chains makes it possible to provide instant inventory management, increase asset visibility, track shipments, trace recalled products, and prevent theft.

Although RFID technology has been around for more than half a century, only recently have RFID security and privacy issues begun to attract attention from both academic and corporate research communities. In a research survey (Juels, 2005a), Juels provides an excellent overview of various RFID security and privacy concerns. In particular, when dealing with passive RFID tags, the author suggests that there is a need to divide the read range of a tag into four different ranges as follows:

- Nominal read range − the standard operating range of a tag under normal intended use
- Rogue scanning range − the read range of a tag when using a sensitive reader equipped with a powerful antenna or an antenna array and/or a higher signal transmission power
- Tag-to-reader eavesdropping range − the range that another reader can eavesdrop tag emissions without powering the tag itself, which can even be larger than the rogue scanning range
- Reader-to-tag eavesdropping range − the range that another reader can capture the signal sent by the reader to the tag, which is larger than any of the above ranges

It is necessary to point out that in addition to the above ranges there exists another range ─ detection range. This is the range from which the presence of a tag or a reader can be detected without the need to be able to send or capture information. We are carrying out a proof-of-concept study to examine whether an RFID system can be attacked by detecting the presence of the tag and reader communication.

From an information security point of view, Knospe and Pohl considered the RFID communication model to be similar in nature to the TCP/IP networking model used for computer networks. Their model consists of an application layer, a data link layer, and a physical layer for both the RFID reader and tag. They define RFID security from information security principles of confidentiality, integrity, availability, authenticity, and anonymity perspectives (Knospe & Pohl, 2004). In addition, RFID systems have their own vulnerabilities and security threats that are separate from the network model (Xiao et al., 2007). The security and privacy issues of RFID systems have been reviewed and evaluated in several studies (Ranasinghe & Cole, 2006; Rieback et al., 2006a; Aragones-Vilella et al., 2007; Rotter, 2008). The threats can be categorized based on their point of attack: the tag, the reader, or the air interface between the tag and the reader (Lieshout et al., 2007).

In recognizing the potential risks when deploying RFID technology, government agencies have played important roles in closely collaborating with industry groups and academia. In Germany, for example, the Federal Office for Information Security conducted a study about RFID security aspects to help German companies to understand security and privacy threats, such as eavesdropping, unauthorized reading of data, cloning, and tracking of people, along with possible protection strategies (Oertel et al., 2005). To meet requirements of the Federal Information and Security Management Act of 2002, the US National Institute of Standards and Technology (NIST) has published guidelines and a set of best practices for the use of radio frequency technology by federal agencies and private organizations. The guidelines focus specifically on the use of RFID technologies for asset management, tracking, matching, and process and supply chain control. NIST recommends the use of firewalls between RFID databases and an organization's IT systems. It also advises the use of

encryption of RFID signals, authentication to identify approved users, and shielding of RFID tags to prevent unauthorized skimming of information (Karygiannis et al., 2007). The U.S. Department of Defense has initiated the DoD RFID security taxonomy through the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration. Three areas of concern are being addressed: network-based risks, mission assurance risks, and order of battle risks. Since risks generally increase with system complexity, eleven high-level RFID security vulnerabilities have been identified, which include common threats, such as unauthorized reading of tag data and leaking tags' electronic information, and special threats specific to military applications, such as using RFID tags as trigger devices for explosives and using RFID readers as platforms for attack (Norton, 2006).

There are numerous publications focusing on RFID privacy issues. One of the major applications of RFID technology is for tracking and tracing of objects. However, the technology becomes a major privacy threat if it is used to track people (Thornton et al., 2006). Consumers are most afraid of being tracked without their consent or knowledge by RFID tags that are ubiquitously hidden in clothing and other consumer items (Ayoade, 2007). The privacy threats in RFID systems can be categorized into two classes: data privacy and location privacy (Oertel et al., 2005; Kim et al., 2006). The threats to data privacy involve discovering personal information stored on the tag and/or in the associated database, while the threats to location privacy comprise the information about a person's current location and past movement through a tag ID associated with that person (Langheinrich, 2007a). Both of these types of threats need to be addressed because the information could be used to profile the victims' preferences, movement, and/or social network. A survey has been conducted to review up-to-date RFID privacy approaches and their attributes (Langheinrich, 2007b). Governments have paid attention to RFID privacy challenges and may regulate RFID use to address privacy concerns. For example, the Ontario Commissioner for Information and Privacy released a set of guidelines to address privacy issues regarding use of item-level RFID technology in the retail/commercial sector. The guidelines were aimed at promoting RFID technology by addressing concerns about the potential threat to privacy (Cavoukian, 2006).

The Canadian Forces (CF) needs a lot of materiel from consumable logistics items to tanks in military operations. To deal with challenges of the visibility, tracking and traceability of its logistics assets, the Canadian Operational Support Command (CANOSCOM) has implemented RFID technology to provide effective and efficient support to CF operations at home and abroad. Defence R&D Canada – Ottawa (DRDC Ottawa), sponsored and funded by CANOSCOM, has been working on RFID security issues, such as the analysis of security threats and the identification of appropriate countermeasures. This chapter is based primarily on the results of our research, previous publications, and the currently available literature. We first present an overview of RFID technology with detailed exposition of the basic components and the essentials of RFID systems. Next, we analyze underlying vulnerabilities and security threats that exist in the RFID system. Then, we propose possible countermeasures to defeat the discussed attacks. Some case studies are presented to illustrate the real attacks. Finally, we conclude the chapter with a discussion of possible future research directions. Through identifying the common vulnerabilities and threats to RFID systems and providing possible countermeasures to resolve the security issues, the objective of this chapter is to provide information and defence techniques against the potential attacks.

2. Brief introduction to RFID technology

RFID is an emerging technology that uses radio waves as the means to identify items or objects. In order to analyze security and privacy issues, it is necessary to give a brief introduction to the basic components of RFID systems. As shown in Figure 1, a typical RFID system contains one or more RFID tags, a reader, and a backend system.

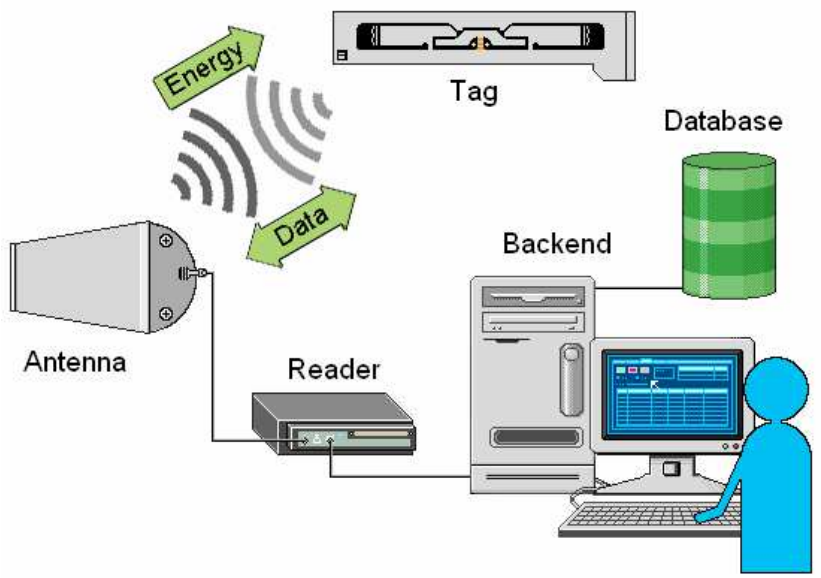

Fig. 1. A generic RFID system

2.1 System components

RFID tags consist of a microchip with an antenna. They come in a wide variety of sizes, from pencil lead thin tags used for animal tracking and credit-card sized ones for access control to heavy duty transponders used for tracking shipping containers, vehicles, and railroad cars. RFID tags can be categorized as either 'active', 'passive', or battery-assisted (semi-active/semi-passive), depending on how they are powered. Active tags are powered by a long-life internal battery and usually have both read and write capabilities. Passive tags are powered by the electromagnetic field generated from the reader and are usually read-only with shorter read ranges. Battery-assisted tags contain a battery that enables them to monitor, process, store, and transmit data over extended ranges. Based on the memory type, RFID tags can be further classified as read-only, write once read many (WORM), or read/write.

An RFID reader is a powered device that wirelessly communicates with the RFID tags and facilitates data transfer between the tag and the backend system. A typical reader consists of a radio frequency module, a control unit, and a coupling element to interrogate electronic tags via radio frequency (RF) communications. The basic functions of the reader include activating tags by sending querying signals, supplying power to passive tags, encoding the data signals going to the tag, and decoding the data received from the tag. RFID readers

differ considerably in complexity, depending on the type of tags being supported and the functions being performed, such as sophisticated signal conditioning, parity error checking, and correction. They can either be portable handheld units or fixed devices.
RFID systems also rely on software. The software can be divided into three groups: front-end tag reading algorithms, middleware, and backend system interface. The front-end algorithms carry out the signal processing tasks. RFID middleware connects readers to the backend server and database. It also filters the data acquired from the reader and handles various user interfaces. The real power of RFID comes in integrating RF technology with a backend system to perform functions such as matching digital information received from the reader against the backend database and routing the retrieved information to the correct application.

2.2 RFID tag categories

RFID tags are at the heart of an RFID system, and can be categorized as active, semi-active/semi-passive and passive in relation to power, as well as read/write and read only in terms of their memory (Thornton et al., 2006; Wyld, 2006).
Passive tags do not have an internal power source and need to draw power from an RFID interrogator. The interrogator emits electromagnetic waves that induce a current in the tag's antenna and power the chip on the tag. When the power to the tag's chip passes the minimum voltage threshold, the circuit turns on and the tag transmits its information to the reader. Because of the absence of a battery, passive tags have a relatively short reading range of only a few meters.
Active tags contain their own battery that is used for both powering the chip and boosting the return signal. The battery gives the tags the ability to continuously monitor high-value goods or a container's seal status. Compared to passive tags, active tags have wider read ranges (tens of meters and even hundreds of meters), larger memory capacities, and faster processing times. However, battery life limits the life of the tag.
There are three terms that are used to describe passive tags that contain batteries: semi-active, semi-passive, and battery-assisted. Some think the terms are interchangeable, while others think that "a semi-active tag is an active tag that remains dormant until it receives a signal from the reader to wake up. The tag can then use its battery to communicate with the reader" … "semi-passive tags are similar to active tags in that they have their own power source, but the battery only powers the microchip and does not broadcast a signal. The RF energy is reflected back to the reader like a passive tag" (Karygiannis et al., 2007). A problem in the above definitions is that some active tags can be put into sleep mode and later reactivated upon receiving a wake up signal from a reader. Therefore, it is more accurate to use the term "battery-assisted tag". Battery-assisted tags have a power source that can keep the chip on the tag constantly powered. However, they can be programmed to preserve battery power by only signaling if an alert condition is detected, or only at predetermined time intervals. In addition, battery-assisted tags may incorporate one or more sensors, enabling them to monitor environmental conditions, such as temperature, humidity, shock, or vibration.
Depending on the memory type, the tags can be further classified as read-only, write once read many (WORM), or read/write. Read-only tags are typically passive and are similar to bar codes because they only carry a serial number. Data stored on the tag cannot be

modified or appended unless the microchip is reprogrammed electronically. Read-only tags are available in many versions, varying in range, data bits, and operating temperature.
WORM memory allows users to encode tags one time during production or distribution. After the initial encoding, the tag's data becomes locked and cannot be changed.
Read/write tags function like computer disks because the data stored can be edited, added to, or completely rewritten an unlimited number of times. These tags are often implemented on reusable containers or other assets in logistic applications. When the contents of the container are changed, new information can be updated on the tag.
In this chapter, we will use RFID as a generic term to describe any automated tagging and reading technology, including active, passive, and battery-assisted RFID technologies, and various formats and applications.

2.3 Frequency bands

In addition to the types of tags used, RFID systems can also be distinguished by their radio frequency. The four primary radio frequency bands, ranging from 30 KHz to 5.8 GHz, are low frequency (LF), high frequency (HF), ultra-high frequency (UHF), and microwave frequency (MW) (Wyld, 2006). The choice of frequency is dependent on the application, the size of the tag, and the read range required. In general, the higher the frequency, the faster the data transfer or throughput rates, but the more expensive the system.
LF ranges from 30 KHz to 300 KHz. In this band, RFID systems commonly operate in a long waveband of 125 to 135 KHz. LF RFID systems generally use passive tags with short read ranges (up to 20 inches) and have lower system costs. The LF tags perform very well in most manufacturing environments. They work well around metal and are resistant to rain. The application areas include security access control, animal identification, and asset tracking.
HF ranges from 3 MHz to 30 MHz, but most HF RFID systems operate at 13.56 MHz. A typical HF RFID system uses passive tags that have a maximum read range of up to 3 feet and a faster data transfer rate than LF tags. This wavelength is robust against water, dust, and other environmental factors. Not only have HF systems been widely used in libraries, pharmaceutical manufacturing sites, and logistics, they have also been adopted for smart identification such as the e-passport.
The next frequency range is UHF that ranges from 300 MHz to 1000 MHz. The passive UHF tags operate around 865-868 MHz in Europe and 902-928 MHz in the United States, while active UHF RFID systems operate at 315 MHz and 433 MHz. Since UHF tags can be read at longer distances with a faster communication speed than LF and HF tags (from 3-6 meters for passive tags and more than 30 meters for active tags), this frequency band is emerging as the preferred band for supply-chain applications.
A typical MW RFID system operates either at 2.45 GHz or 5.8 GHz. The former frequency is traditionally used in long-range access control applications and has a read range of up to 1 meter as a passive tag or longer as an active tag. In Europe, the 5.8 GHz frequency band has been allocated for road traffic and road-tolling systems.
An overview of the characteristics of each RFID frequency band is presented in Table 1, which includes read ranges, data transfer rates, application areas, and corresponding ISO standards. From a standards perspective, the ISO 18000 standard covers the air interface protocol—the way RFID tags and readers communicate—for major frequencies used in RFID systems.

	LF	HF	UHF	MW
Frequency	30 – 300 KHz	3 – 30 MHz	300 – 1000 MHz	2 – 30 GHz
Typical Frequencies	125-134 KHz	13.56 MHz	433 MHz (Active) 865 – 956 MHz	2.45 GHz 5.8 GHz
Read Range	Up to 1m with long-range fixed reader	Up to 1.5m	433 MHz: Up to 100m 865-956 MHz: 0.5 – 5m	Passive ≈ 3 m Active ≈ 15m
Data Transfer Rate	Less than 1 kilobit per second (kbit/s)	≈ 25 kbit/s	≈ 30 kbit/s	Up to 100 kbit/s
Common Applications	Access control, Animal identification, Inventory control, Vehicle immobilizers	Smart cards, Contact-less access and security, Item level tracking, Library books, Airline baggage	Logistics case/pallet tracking, Baggage handling	Railroad car monitoring, Automated toll collection
Pros and Cons	LF signal penetrates water. It is the only technology that can work around metal. LF tags have a short read range and low data transfer rate, and are more expensive than HF and UHF tags because of their longer copper antennas.	HF system is able to read tags that are placed in a very close proximity to each other. HF signal penetrates water but not metal. HF tags are less expensive and offer higher read rate than LF tags.	Active RFID has a very long read range with high price tags. Since using a battery, tags have a finite lifespan (typically 5 years). UHF system is capable of reading multiple tags quickly. However, UHF tags are highly affected by water or metals.	Microwave transmission is highly directional, and enables precise targeting. MW tags provide the fastest data transfer rate. However, they cannot penetrate water or metal.
ISO Standards	11784/85, 14223	14443, 15693, 18000	15693, 18000	18000

Table 1. RFID frequency bands and standards

3. Security aspects

Like other information systems, RFID systems are vulnerable to attack and can be compromised at various stages of their use. Attacks against an RFID system can be categorized generally into four major groups: attacks on authenticity, attacks on integrity,

attacks on confidentiality, and attacks on availability. Besides being vulnerable to common attacks such as eavesdropping, man-in-the-middle, and denial of service, RFID technology is, in particular, susceptible to spoofing and power attacks (Figure 2). This section illustrates different kinds of attacks and provides countermeasures against these attacks.

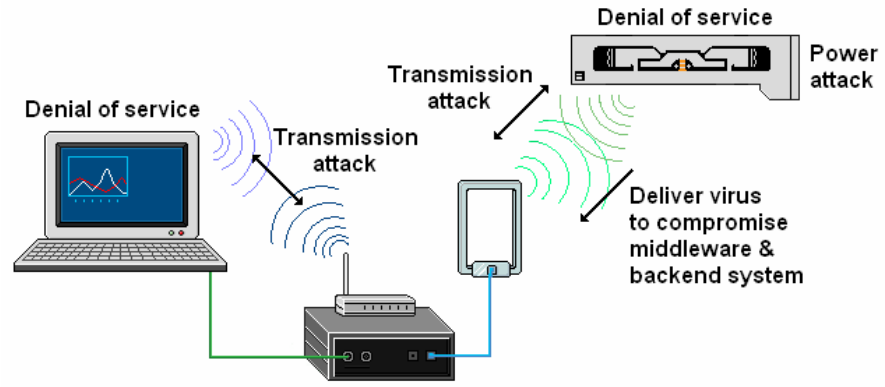

Fig. 2. Attack points

3.1 Reverse engineering

Reverse engineering is the process of taking something apart to discover how it works. Figure 3 shows an example of RFID physical elements (MacGillivray & Sheehan, 2006). Considering privacy issues related to the biometric e-passport, it may be possible for an attacker to gain access to the chip and read its memory contents optically to retrieve the PIN, biometric data, personal information, etc. The technical ability and equipment needed to reverse engineer an integrated circuit can be rated at three different levels from a knowledgeable individual using low cost and easily available tools to a highly skilled team, using equipment not commonly available in the commercial market (Actel, 2002). Unfortunately, the methods of attacking ASIC technology are not a secret and can be easily accessed (Blythe et al., 1993).

Countermeasures

A FIPS standard refers to chip coatings as an anti-reverse engineering method to prevent attacks. Various tamper proof techniques have been developed to defend against reverse engineering attacks. For instance, by adding a tamper-release layer to RFID tags, operations personnel can be alerted if a tag has been tampered with.

3.2 Power analysis

Power analysis is a form of side-channel attack that is intended to retrieve information by analyzing changes in the power consumption of a device. It has been proven that the power emission patterns are different when the card received correct and incorrect password bits or cryptographic keys. It is possible to breach smart card security by monitoring power consumption signals. Professor Adi Shamir demonstrated the ability to use a password to kill an RFID tag during the RSA Conference 2006. He also predicted that a power analysis attack on a RFID tag could be performed using a very common device such as a cell phone

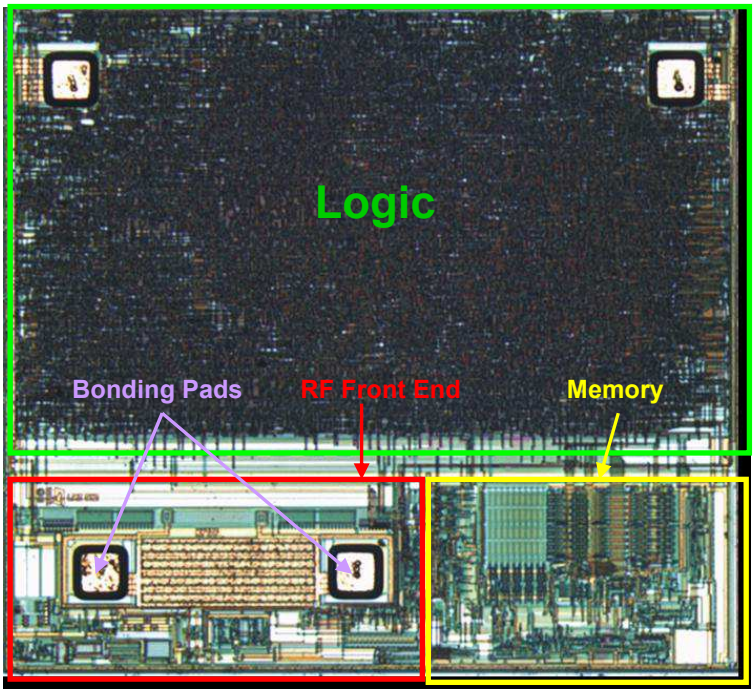

Fig. 3. Reverse engineering

(Merritt, 2006). Two methods—either masking the spikes in power consumption or improving the hash algorithm—can be used to protect the password for being cracked with power analysis attack. Figure 4 shows an example of using Hamming weight data to break the Data Encryption Standard (DES) through analyzing the power consumption (Messerges et al., 2002).

Countermeasures

The common methods used to defeat power analysis attacks are filtering or adding an element of randomness. Filtering power signals or delaying the computation randomly can increase the difficulty for the attacker to identify the power consumption patterns. Another method implemented in some smart card designs is adding an element that simply consumes a random amount of power. Unfortunately, this approach may cause a problem for RFID systems where minimizing power consumption is a priority.

3.3 Eavesdropping

Since an RFID tag is a wireless device that emits data, usually a unique identifier, when interrogated by an RFID reader, there exists a risk that the communication between tag and reader can be eavesdropped. Eavesdropping occurs when an attacker intercepts data with a compliant reader—one for the correct tag family and frequency—while a tag is being read by an authorized RFID reader. Since most RFID systems use clear text communication, due to tag memory capacity or cost, eavesdropping is a simple but efficient means for the attacker to obtain information on the collected tag data. The information picked up during the attack can have serious implications—it can be used in subsequent attacks against the RFID system. It is necessary to point out that in passive RFID systems readers have

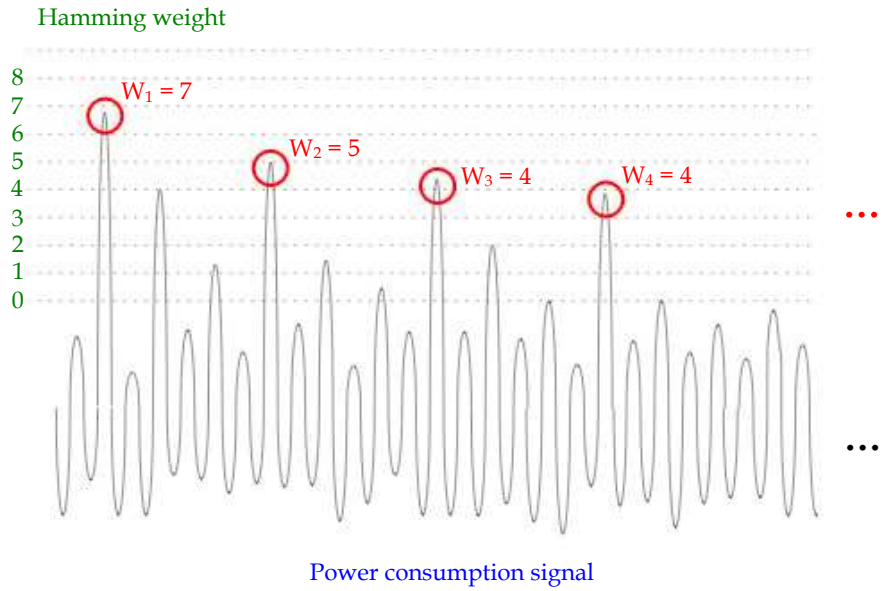

Fig. 4. An example of power analysis

significantly longer transmission ranges than tags. When passive tags modulate and backscatter the signal from the reader to communicate, they have only a fraction of the transmission power of the reader. Therefore, passive tags have a more limited transmission range and are less susceptible to eavesdropping (Karygiannis et al., 2007). However, it is necessary to keep in mind that even if the eavesdropper is out of the range of the tag signal, he or she may still be able to listen to the commands sent out from the reader (Figure 5).

Countermeasures

Countermeasures against eavesdropping include establishing a secure channel and/or encrypting the communication between tag and reader. Another approach is to only write the tag with enough information to identify the object. The identity is used to look up relevant information about the object in a back end database, thus requiring the attacker to have access to both the tag and the database to succeed in the attack.

3.4 Man-in-the-middle attack

Depending on the system configuration, a man-in-the-middle (MITM) attack is possible while the data is in transit from one component to another. An attacker can interrupt the communication path and manipulate the information back and forth between RFID components (Figure 6). This is a real-time threat. The attack reveals the information before the intended device receives it and can change the information en route (Welch & Lathrop, 2003). Even if it received some invalid data, the system being attacked might assume the problem was caused by network errors and would not recognize that an attack occurred. An RFID system is particularly vulnerable to MITM attacks because the tags are small in size and low in price, all of which means that there is generally a lack of sophisticated protection circuitry.

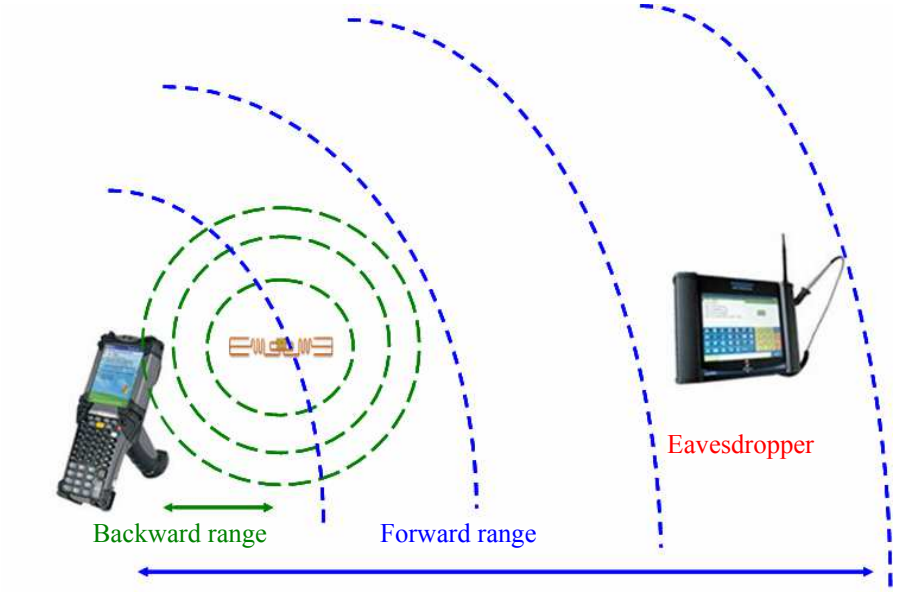

Fig. 5. Eavesdropping on reader-tag communication

Fig. 6. Man-in-the-middle attack

Countermeasures

Several technologies can be implemented to reduce MITM threats, such as encrypting communications, sending information through a secure channel, and providing an authentication protocol.

3.5 Denial of Service (DoS)

DoS attacks can take different forms by attacking the RFID tag, the network, or the backend. The purpose is not to steal or modify information, but to disable the RFID system so that it cannot be used. When talking about DoS attacks on wireless networks, the first concern is physical layer attacks, such as jamming and interference. Jamming using noise in the RFID system's frequency range can reduce the throughput of the network and ruin network connectivity resulting in overall supply chain failure (Egli, 2006). Jamming happens when a device that actively broadcasts radio signals can block and disrupt the operation of any and all nearby RFID readers. Interference with other radio transmitters can also launch a DoS attack to obscure the communications between the tags and reader. Another form of DoS is to destroy or disable RFID tags by removing them from the items, washing out their contents completely, or wrapping them with metal foil.

Countermeasures

In general, it is easier to detect DoS attacks than prevent them from happening. However, once detected, the attacks can generally be stopped before they do too much harm. For example, countermeasures against jamming can use passive listening to detect the tags whose transmission exceeds a predefined volume, and then use block functions to thwart them. Countermeasures against detaching the tags from the targeted items could be either through enhancing the mechanical connection between the tags and items, or adding an alarm function to active tags.

3.6 Spoofing

In relation to RFID technology, spoofing occurs when a forged tag masquerades as a valid tag and thereby gains an illegitimate advantage. Tag cloning is a spoofing attack where the attacker captures the data from a valid tag and creates a copy of the captured sample on a blank tag. Another example is an attacker reading a tag's data from a cheap item in a store and then uploading the data onto another tag attached to a similar but more expensive item. Mr. Lukas Grunwald, a German security expert, said "I was at a hotel that used smartcards, so I copied one and put the data into my computer, … Then I used RF Dump to upload the room key card data to the price chip on a box of cream cheese from the Future Store. And I opened my hotel room with the cream cheese!" (Newitz, 2006)

Countermeasures

A common way to defeat a spoofing attack is to implement an RFID authentication protocol and data encryption, which increases the cost and technology complexity needed for a successful attack.

3.7 Cloning

Tag cloning is a process that first captures the data from a legitimate tag and then creates an unauthorized copy of the captured sample on a new chip. Researchers from Johns Hopkins University and RSA Labs published experimental results of cloning a cryptographically protected Texas Instruments digital signature transponder (DST) that was used to buy gasoline and activate a car's ignition (Rieback et al., 2006a).

Countermeasures

In order to defeat physical cloning attacks, Tuyls and Batina proposed to use Physical Unclonable Functions (PUFs) as secure memory for the storing of the secret key on an RFID tag (Tuyls & Batina, 2006). The authors claimed that "both the physical cloning attack as

well as the cloning attack based on (actively or passively) attacking the protocol between the tag and the reader can be prevented."

3.8 Replay

In a replay attack, an attacker intercepts communication between a reader and a tag to capture a valid RFID signal. At a later time, the recorded signal is re-played into the system when the attacker receives a query from the reader. Since the data appears valid, it will be accepted by the system.

Countermeasures

The most popular solution is the use of a challenge and response mechanism to prevent replay attacks. Time-based and counter-based schemes can also be used as countermeasures against replay attacks.

3.9 Viruses

Since most of the passive RFID tags currently only have a small storage capacity of 128 bits, viruses are probably not a credible threat to RFID systems. However, the situation may be changing since three computer researchers released a paper in March 2006, which reported that RFID tags could be used as a medium to transmit a computer virus. It also explained how the RFID virus works in a supply chain. If a container arrived in a distribution center and the container's RFID tag had been infected with a computer virus, this particular RFID virus could use SQL injection to attack the backend servers and eventually bring an entire RFID system down (Rieback et al., 2006b).

Countermeasures

The virus attacks which have been demonstrated on RFID-based systems are the common attacks against information systems, such as buffer overflow attacks, code or SQL injection attacks, etc. Well-developed middleware can be used to avoid virus attacks by blocking anomalous bits from the tag.

3.10 Tracking

Unlike the previously discussed RFID attacks, tracking is a threat directed against an individual. Within the next few years, manufacturers may put item-level RFID tags into many more household products. There is a privacy concern because instead of tracking books and consumer products such as clothing, RFID systems can be used to track people's movements and even create a precise profile of their purchases.

Countermeasures

An easy method to disable tracking is to deactivate the RFID tags, which is known as "killing" the tag that will be introduced in the following section.

3.11 "Killing tag" approach

Typically killing an RFID tag is done to prevent it from communicating thus making it impossible to be read anymore. For example, a kill command is defined in standard Electronic Product Code (EPC) format, which is used to permanently disable the tags for purposes of privacy. Since it is necessary to make sure that RFID tags are not killed by an unauthorized party, the kill command is secured by a password called the kill password. However, the kill command also brings some drawbacks:

- Although the kill command was introduced to protect consumer privacy, consumers cannot easily detect whether a tag has been deactivated. Furthermore consumers cannot kill the tag by themselves. Because in order to do this, not only would they need an interrogator, but also a valid kill password.
- The kill feature also brings up a new threat to an RFID system. If an enemy deactivates RFID tags in a supply chain, the supported application will not function properly because the item identification numbers cannot be read anymore. Furthermore, once killed, a tag can never be re-activated for any further application, such as item recalls, product returns, etc.
- If the kill password is weak (for example, EPC Class-1 Generation-1's 8-bit kill password has only 256 possibilities, while EPC Class-1 Generation-2 has improved significantly with a 32-bit password—more than 4,000,000,000 possibilities), unauthorized parties can kill the tag very easily.
- Although the killed tags cannot emit radio frequency anymore, data are still stored in the tags' memory.

Countermeasures

In many applications, it is important to protect the tag from a kill command that permanently disables the tag's functionality. In order to do so, tag memory and reading can be password protected, and a command of permanent lock can make password and/or the tag data permanently unchangeable.

3.12 Block tag

Another method to protect against unwanted scanning of RFID tags attached to items that people are carrying or wearing is to block the tags. Blocking the tags can be accomplished with different approaches, such as Faraday Cage, active jamming, or "blocker tags". A Faraday cage is a metal or foil-lined container, which is impenetrable to radio-frequency waves. Petty thieves are already known to use foil-lined bags in retail shops to defeat shoplifting detection mechanisms. Since active jamming violates the regulations of most governments, a device called a "blocker" tag has been proposed to protect against inappropriate scanning (Juels et al., 2003). The blocker tag obstructs the RFID scanning process by simulating that all the possible IDs are present. Let us take the tree-walking protocol, which is often used to avoid collisions while reading, as an example. Because in tree-walking protocol the space of k-bit identifiers is viewed as the leaves in a tree of depth k, a reader traversing the tree needs to figure out whether the next bit is a "0" or "1". When a blocker tag is queried, it always responds with both "0"and "1" and causes a reader to stall. A blocker can be made from a cheap passive RFID tag. Therefore it is possible to embed a blocker into a portable device to actively prevent inappropriate scanning (Juels, 2005b).

3.13 Summary of security aspects

As mentioned above, there are many ways to attack various parts of RFID systems. Many efforts have been taken to study the countermeasures needed to defend against these threats. As a summary of this section, a threat-countermeasure map is provided for visualizing the relationships between security threats and countermeasures. In Figure 7, each attack is mapped onto as many countermeasures as possible to show that one threat can be defeated with a specific countermeasure or several countermeasures. In this way,

decision makers can easily determine the most efficient strategy to protect their RFID system.

From the threat-countermeasure map, it is clear that authentication and encryption are the most important security techniques for the protection of RFID systems. We can use them to address a wide variety of security threats. The purpose of authentication is to confirm that an entity is what it claims to be. In an RFID system, authentication is performed by tags to verify an authorized reader, making sure that an RFID reader cannot communicate with the tag unless being successfully authenticated. With different designs, the authentication can be either one way or two ways. Encryption is another major countermeasure, which is a process of scrambling data to make it difficult to unscramble or decipher. To heighten the security in an RFID application, both the data stored on a tag and the data communicated between a reader and the tags need to be encrypted. In real-life applications, encryption and authentication protocols are often used in a combination to enhance the security of an RFID system. However, such a solution will certainly increase the cost of the implementation.

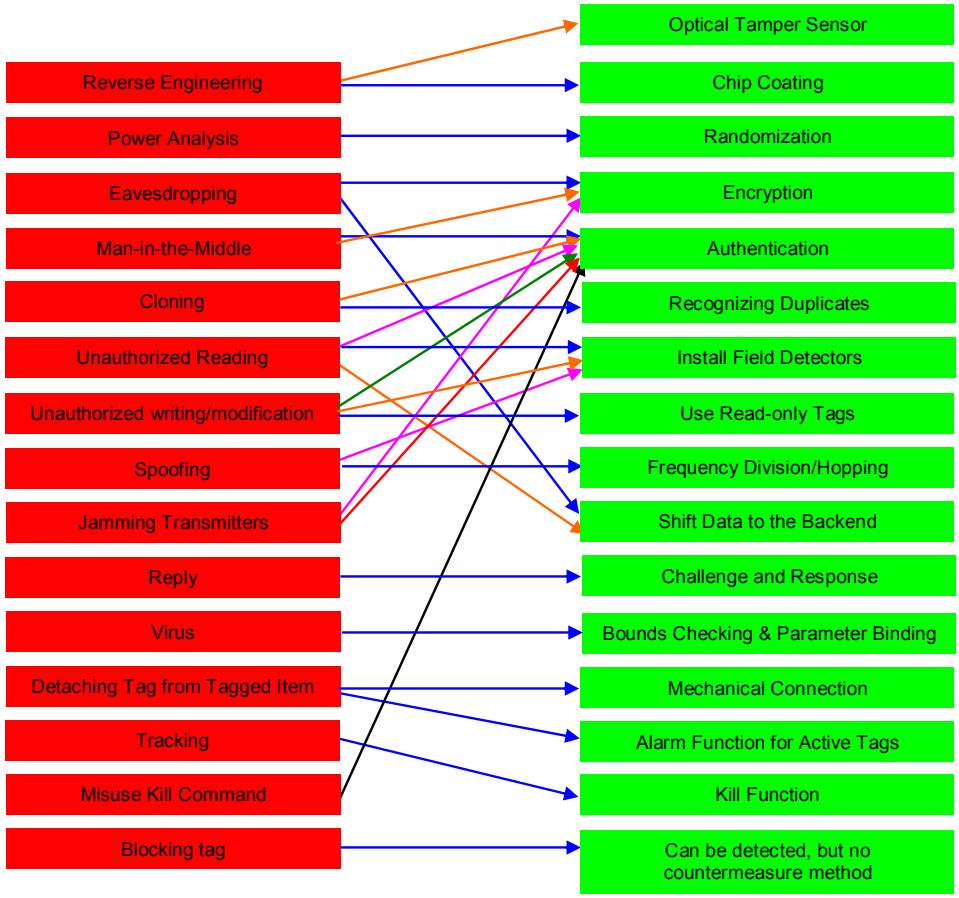

Fig. 7. Threat-countermeasure map

4. Authentication

From the above threat-countermeasure map, we can see that authentication is a primary method for ensuring RFID security. Authentication is a process of confirming the identity claimed by an entity. In the context of a tamper-resistant authentication protocol for an RFID system, the tag and reader establish a trusted relationship and agree on a common, secret, session key to secure the communication between them. It is not difficult to develop a trusted authentication protocol to make high-cost RFID tags directly authenticate RFID readers. However, the majority of RFID applications use low-cost and high-volume passive tags. Under this circumstance, developing a secure authentication protocol is a challenge because tags, compared with readers and back-end servers, are highly resource limited and cannot perform strong encryption. In order to solve this problem, various lightweight authentication algorithms and protocols have been proposed, debated, and tested.

4.1 Pseudonym

The pseudonym technique has been proposed to deal with this problem in low-cost RFID systems: each tag stores a list of pseudonyms that can only be understood by authorized verifiers (Juels, 2003). When the tag is queried, it emits the next pseudonym from the list. Since the protocol uses only the XOR operation and does not require the tag to perform any cryptographic operations, it fits with the restrictions of the low-cost RFID tags very well. A problem is that the tag can only store a small list of pseudonyms because of its small data capacity. One method used to solve this problem is renewing the list each time when the tag is queried. However, to allow the list to be renewed, a mutual authentication protocol is required between the tag and the reader to prevent an attacker from updating the list.

4.2 YA-TRAP, O-TRAP and YA-TRAP+

Yet Another Trivial RFID Authentication Protocol (YA-TRAP) presents a novel idea for RFID authentication. It uses monotonically increasing timestamps and a keyed hash to distinguish anonymous (adversary) tags from legitimate tags (Tsudik, 2006). In the beginning, a reader sends the current system time to a tag. The tag decides if the time is valid by checking if it is in the interval between the stored timestamp and a maximum system allowable timestamp. If the received time is valid, the tag will use it to update the stored timestamp and send the key-hashed timestamp to the reader. Otherwise, the tag will send a pseudo-random number to the reader. The information is forwarded to the backend system that maintains a hash lookup table and is able to quickly compare the values to validate the tag. However, YA-TRAP is susceptible to a trivial DoS attack when the adversary sends a wildly inaccurate timestamp to the tag.

In order to overcome the weakness of YA-TRAP, modified authentication protocols, such as O-TRAP and YA-TRAP+, have been proposed (Burmester et al., 2006). The protocol O-TRAP stands for "Optimistic" Trivial RFID Authentication Protocol, i.e., the security overhead is minimal when the parties are honest. O-TRAP is a revision of YA-TRAP with added one-pass anonymity for authenticated transponders and solves some vulnerabilities of YA-TRAP. YA-TRAP+ was proposed to deal with large scale DoS attacks by introducing an extra optional pass in which a server authenticates the timestamp. A major drawback for both O-TRAP and YA-TRAP+ is that the server workload is increased so that more computational resources are required on a per-tag basis for authentication.

4.3 HB, HB+ and HB++

Hopper and Blum proposed a human-to-computer authentication protocol, named the HB protocol (Hopper & Blum, 2001). Its extremely low computational cost makes the protocol well suited for resource-constrained devices like RFID tags. Unlike other classical symmetric key cryptography solutions, the security of the HB protocol is based on the hardness of the Learning Parity with Noise (LPN) problem. A random k-bit binary vector is generated by the reader and transmitted to the tag for challenge. The tag computes the inner dot product of the k-bit vector and a shared key, and XORs the value with a noise bit (=1 with probability $\eta \in [0, 1/2]$). The calculated value is sent back to the reader for checking to result in a pass or fail. This is one round of HB authentication with the same process being repeated several times. However, the HB protocol is only secure against passive attacks and not against active attacks. For example, an adversary can transmit a fixed k-bit vector to the tag several times and potentially deduce the key.

Addressing this problem, HB+ was proposed to secure against both passive and active attacks with some additions (Juels & Weis 2005). The first is an additional shared key so that the tag and reader share two independent keys (instead of using one shared key in the HB protocol). The other is a random "blinding vector" that is generated by the tag at the beginning of the process and is used in calculations later on. In HB+, a basic authentication step consists of three rounds. First, the tag sends a random "blinding factor" to the reader. Then the reader replies with a random challenge in the same way as HB protocol. Finally, the tag calculates a return value that is the inner dot product of the newly introduced key and blinding vector XORs with the HB return signal as before, and replies with it to the reader. However, it has been shown that HB+ is vulnerable to a simple man-in-the-middle attack that was not considered in HB protocol (Gilbert et al., 2005). As an improvement, a further modified HB protocol, HB++, was proposed to overcome the weakness of HB+ protocol (Bringer et al., 2005). However, it has been discovered that the HB++ is not immune to attacks from an adversary that pretends to be an authentic reader (Piramuthu 2006).

5. Case studies

In the previous sections, we analyzed the security threats and provided the corresponding countermeasures. "Unfortunately, businesses and governments are not the only ones interested in RFID. Civil liberties groups, hackers and criminals are also keenly interested in this new development, albeit for very different reasons" (Rieback et al., 2006c). Following are four case studies that illustrate how the security of some RFID systems could be compromised. The purpose is not to teach people how to attack an RFID system, but to help people become aware of the kinds of threats that need to be taken into account when designing a secure RFID application.

5.1 Cracking crypto-enabled RFID products

The Texas Instruments Registration and Identification System (TIRIS) is an RFID system that uses a 3.6x29mm cylindrical tag with a reading range of up to 40 inches. The TIRIS DST tags have been adopted by different companies to make millions of SpeedPass payment transponders and automobile ignition keys. In 2005, researchers from Johns Hopkins University and RSA Laboratories demonstrated a way to crack the encryption of Exxon Mobil's SpeedPass. The RFID tag they compromised was a DST-40 tag that consists of a small microchip and an antenna coil that uses a secret 40-bit cryptographic key.

The Mifare Classic RFID smartcard is a wireless card protected by an encryption algorithm, which has been used by transit operators in London, Boston and the Netherlands, as well as public and private organizations to control access to restricted areas. In 2008, two research groups managed to crack the encryption and reported the security flaw that allowed them to do so. They revealed that the method to retrieve cryptographic keys is relatively easy and does not rely on expensive equipment (Nohl et al., 2008 & Schreur et al., 2008).
The procedures to crack a crypto-enabled RFID tag, including collecting data, revealing encryption key, and creating a clone tag, are as follows:

1. Reverse engineering: The encryption algorithm can be reverse engineered through flawed authentication attempts. The method involves sending RFID devices carefully chosen electronic queries and recording the responses of the devices. The response information gives clues as to what is happening inside the microchip, and therefore makes it possible to reconstruct the encryption algorithm.
2. Key cracking: Once the algorithm is known, the keys can be figured out by brute force attack, i.e. simply trying all possible keys. Since the DST-40 tag uses a proprietary 40-bit and Mifare Classic uses a 48-bit encryption algorithm, it will take 9 to 10 hours to try all possible keys for both devices on advanced equipment.
3. Simulation: After obtaining the key (and serial number), it is possible to create a clone tag.

Lessons to learn
The impact of compromising tag encryption on supply chain RFID systems has not been determined. However, one lesson that can be learned from the details of these cases is that the cryptographic algorithm needs to be built into the RFID system correctly.

- It is better to use a longer key length, such as industry-standard 128-bit Triple DES encryption or AES encryption.
- It is necessary to use standard cryptographic algorithms that have been through peer reviews, instead of a proprietary cryptographic algorithm.
- It is better to use public key (asymmetric) encryption rather than secret key (symmetric) encryption.

5.2 RFID-Zapper

There are several ways to deactivate passive RFID tags. The RFID-Zapper is an easy-to-build electronic device that can permanently deactivate passive RFID-Tags. The device was developed by two German students in 2006. Their motivation was a privacy concern over the potential use of RFID tags on individual items purchased by consumers (Juels, 2005b). The technique is so simple that everyone can build his/her own RFID-Zapper. The concept of RFID Zapper was presented at the 22nd annual Chaos Communication Congress (22C3) as follows (MiniMe & Mahajivana, 2005).

> *Basically it copies the microwave-oven-method, but in a much smaller scale. It generates a strong electromagnetic field with a coil, which should be placed as near to the target-RFID-Tag as possible. The RFID-Tag then will receive a strong shock of energy comparable with an EMP and some part of it will blow, thus deactivating the chip forever.*

A prototype was built by modifying the circuit board of a single-use camera with a flash. The voltage of flash capacitor needs at least 100 V to supply enough electrical current. The flash bulb is replaced with a coil of 5 windings of 1 mm diameter copper wire. Disconnected

from the flash, the capacitor is re-connected to the coil with an added switch to turn the device on or off. The flash indicator light is re-connected so that it glows when the capacitor is fully charged and can be clearly observed. Since a large amount of energy can be emitted into the environment in a very short time, the magnetic field of the Zapper is sufficient to destroy an RFID forever at close range.

The prototype device was tested on the passive 13.56 MHz RFID tags successfully. Currently, the RFID-Zapper has been tested only on 13.56 MHz tags; however, the inventors hope to be able to try their device on other tags running at different frequencies soon. Another threat is that a German privacy advocacy group FoeBuD plans to manufacture and sell such a device that consumer could use it to disable RFID tags permanently (Collins, 2006).

Lessons to learn

The demonstration was performed with the capacitor loaded about 100 V. The RFID-Zapper was able to destroy the RFID tags placed right next to it.

- It is necessary to test the working range of the RFID-Zapper with a capacitor that can supply more power.
- Even though RFID technology offers several advantages over optical bar codes, it is a good practice to use both technologies in some critical applications because RFID tags could be deactivated or killed.

5.3 Trigger a bomb

The increasing threat of identity fraud has produced worldwide efforts on strengthening security features in identity documents. The International Civil Aviation Organization (ICAO) has been working on the new e-passports fitted with RFID tags for wireless processing when people pass through Customs. However, at Black Hat 2006, a group of security experts from Flexilis demonstrated that the proposed American RFID passports might be used by terrorists as potential bomb triggers (Coverson, 2006). Kevin Mahaffey, Director of Software Development at Flexilis, and his colleagues used a mockup e-passport, equipped with an RFID chip, and set up a small explosive charge nearby. With the passport opened about 1/2 inch, Mahaffey demonstrated how the explosive could be set off when a passport was detected by a nearby inquiring RFID reader.

In a report "RFID Passport Shield Failure Demonstration", they explained the mechanism behind their proof of concept experiment (Flexilis, 2006):

> *When present in a reading field, a passport RFID tag will wirelessly draw power from the reader in order to operate. The change in antenna current is detectable by the RFID-reading hardware; therefore, even if a tag is not directly sending data, it intrinsically discloses its proximity to the reader by its presence in the reading field.*

A potentially dangerous security breach is that the terrorists could potentially use the RFID tag to trigger a bomb.

Lessons to learn

At the moment, Flexilis's proof of concept experiment only demonstrated the ability to read passive RFID. However, the demonstration alerts us to a real world security threat.

- It is necessary to study whether it is possible to use active RFID tags as bomb trigger.
- It is necessary to research authentication methods for passive RFID tags so that they cannot be activated with an unauthorized reader.

5.4 Snooping attack

One of the advantages of RFID technology over barcodes is that RFID does not require a line of sight between tag and reader. However, it brings a new security threat to supply chains if RFID-tagged items can be read even if they are inside a truck. Sniffing the truck's payload was selected as "one of the five coolest hacks of 2007" (Higgins, 2007a). Researchers from PacketFocus Security Solutions and Atlas RFID Solutions have demonstrated reading EPC codes from tagged products on 18-whheeler tractor-trailers with standard tag readers and antennas (Higgins, 2007b). The test explored a vulnerability of RFID tags used in supply chain applications — business competitors or enemy forces could use the sniffed information for intelligence purposes. The detailed logistics information is vital to business and military success.

To evaluate the risk of such an attack, we carried out an experiment with four different passive RFID tags: Alien 9554, Avery AD222, Symbol Four T, and StongTech. First, we measured their readability in an indoor open area that is about 11 meters long and 6 meters wide. The test result in Figure 8 shows that all the tested tags can be reliably read within 4.5 meters when the tag and reader are parallel to each other.

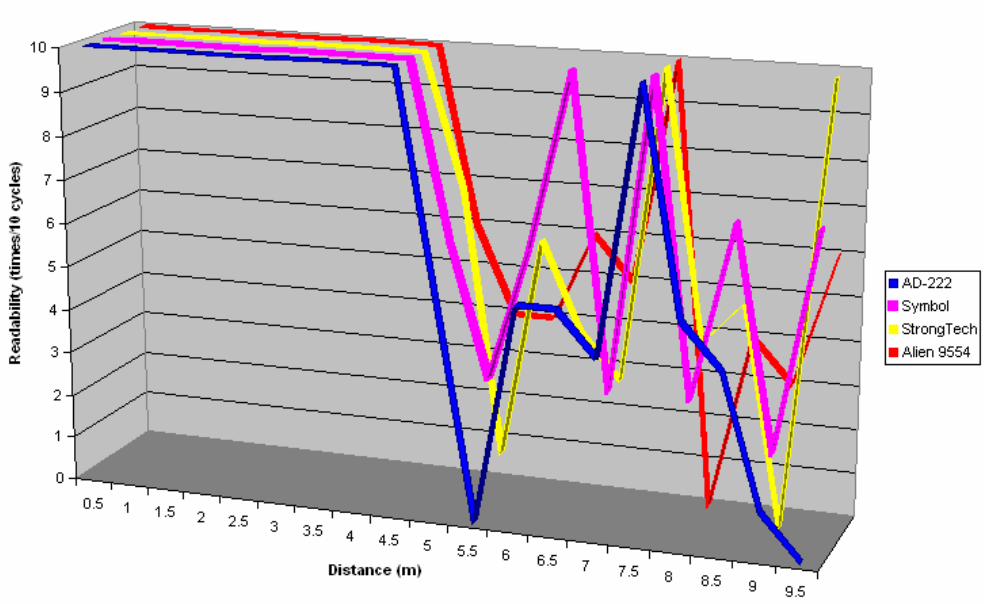

Fig. 8. Free space tag performance test

Then, we attached the tags to paper boxes and put them into a mini van (Figure 9 (a)). The reader, antenna and router were set up on the top of a wood frame on the side of the road. The router communicated with the backend computer wirelessly. We performed the tests in two situations: 1) when the vehicle was stopped; 2) when the vehicle was being driven at slow speeds, 5km/h to 30 km/h (Figure 9 (b)). The experimental results showed that the tag could only be read at an angle, through the door's edge, but not through metal, when the vehicle was stationary and the reader was within a short distance (less than 30 cm).

Lessons to learn
With an off-the-shelf reader and antenna, it is possible to scan and hack EPC labels on products being loaded on a car or truck. Several methods could be useful in protecting against sniffing information from the RFID tags:

- Limit the amount of sensitive information on the tag
- Use a masking technique that masks the structured tag information with a row of zeros
- Encrypt the EPC tag data

(a) Tagged boxes (b) Reading test

Fig. 9. Sniffing test

6. Conclusion

In this chapter, we focused on the issues and potential solutions for a range of security vulnerabilities of RFID systems. Recent advances in the uses of RFID technology have generated significant interest in society, not only because they have brought change to the industry and business sectors, but also because they will begin to influence our daily life more and more. As mentioned above, the use of RFID has grown exponentially across a variety of core industries, such as logistics, manufacturing, retail and healthcare. Although each application has its own special requirements, security vulnerabilities will be always a major concern when deploying RFID applications. Like the Internet or mobile telephony, RFID is a wireless networking technology. While the non-contact and non-line-of-sight properties of RFID systems increase the convenience and efficiency of their applications, these properties also increase the system's vulnerability. In this chapter, we have analyzed the underlying vulnerabilities that exist in RFID systems, illustrated the threats of possible attacks, and provided corresponding countermeasures. Case studies have been presented and discussed to examine four specific security threats. The objective of the chapter is to try to make life for an attacker very difficult, if not impossible.
The directions for further study are suggested in there major areas: technology standards, authentication protocols, and operational policies/guidelines. Security has not historically been the focus of technology standards for RFID systems and their components. With the increasing usages of RFID, such as passports, personal ID cards and consumer products, potential security threats and compliance risks in the future are enormous. It is necessary to pay attention to standardization of RFID systems. There are many different RFID standards

at the moment. The technology standards typically describe the physical and the link layers, covering aspects such as air interface, anti-collision mechanisms, communication protocols, host interface, data syntax, etc. However, there are some standards that are more important than others — ISO and EPC Global are main contributors in defining RFID standards. EPC tags were originally designed for supply chain and logistical applications. The people who established the EPC standards aimed on low-cost tags with high potential reading rates. Therefore, security was not a high priority issue resulting in the first generation EPC tags lacking the computational resources for cryptographic authentication.

It is important to put more effort into developing authentication protocols for passive RFID. The reasons, as mentioned above, are that 1) current proposed lightweight authentication protocols can still be compromised by attacks; 2) it is difficult or impossible to use computationally intensive cryptographic algorithms for low-cost RFID tags.

A well-designed RFID policy can reduce the risk of attacks. When dealing with security and risk management, policy decisions also play an important role in the security of an RFID system. An RFID security policy is a document that states how an organization plans to protect its physical RFID devices and information data assets. Since, sooner or later, new threats will appear, an RFID security policy should be considered a "living" document that needs to be continuously updated as the RFID technology and implementation requirements change. The policy also needs to take into account how the users will be trained in the proper use of RFID, and explain how security measures will be carried out and enforced.

7. References

Actel Corporation (2002). Design security in nonvolatile flash and antifuse FPGAs security backgrounder, Sunnyvale, California, 2002, from http://www.actel.com/documents/DesignSecurity_WP.pdf

Aragones-Vilella, J.; Martínez-Ballesté, A. & Solanas, A. (2007). A brief survey on RFID privacy and security, *Proc. of the World Congress on Engineering 2007*, pp. 1488-1493, ISBN 978-988-98671-5-7, July 2-4, 2007, London, UK.

Ayoade, J. (2007). Roadmap to solving security and privacy concerns in RFID systems, *Computer Law & Security Report*, Vol. 23, No. 6, pp. 555-561, ISSN: 0267-3649.

Blythe, S.; Fraboni, B.; Lall, S.; Ahmed, H; & de Riu, U. (1993). Layout reconstruction of complex silicon chips, *IEEE Journal of Solid-State Circuits*, Vol. 28 No. 2, pp. 138-145, ISSN: 0018-9200.

Bringer, J.; Chabanne, H. & Dottax, E. (2005). HB++: A lightweight authentication protocol secure against some attacks, *Proc. of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing* (SecPerU'06), pp. 28-33, ISBN: 0-7695-2549-0, 29 June 2006, Lyon, France.

Burmester, M.; van Le, T. & de Medeiros, B. (2006). Provably secure ubiquitous systems: Universally composable RFID authentication protocols, *Proc. of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks* (SECURECOMM 2006), pp. 1-9, IEEE Press, ISBN: 1-4244-0423-1, 28 Aug.–1 Sep. 2006, MD, USA.

Cavoukian, A. (2006). *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*, Information and Privacy Commissioner/Ontario, Toronto, ON, June 2006, from http://www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf

Collins, J. (2006). RFID-Zapper shoots to kill, *RFID Journal*, Hauppauge, NY, 23 January 23 2006, from http://www.rfidjournal.com/article/articleview/2098/1/1/

Coverson, L. (2006). Could the new passport trigger a bomb? *ABC News*, New York, NY, 16 August 2006, from abcnews.go.com/Technology/story?id=2319734&page=1

Flexilis (2006). RFID passport shield failure demonstration, *FLX[2006-0605]*, from www.flexilis.com/download/RFIDPassportShieldFailureDemonstration.pdf

Garfinkel, S. & Rosenberg, B. (2005). *RFID: Applications, Security, and Privacy*, Addison-Wesley Professional, ISBN: 0321290968, Boston, MA.

Gilbert, H.; Robshaw M. & Sibert, H. (2005). An active attack against HB+ — A provably secure lightweight authentication protocol, *Cryptology ePrint Archive*: Report 2005/237, from http://eprint.iacr.org/2005/237.pdf

Graafstra, A. (2006). *RFID Toys: 11 Cool Projects for Home, Office and Entertainment*, John Wiley & Sons, ISBN: 0471771961, New York.

Higgins, K. J. (2007a). The five coolest hacks of 2007, *Dark Reading*, Manhasset, NY, 31 December 2007, from http://www.darkreading.com/document.asp?doc_id=142127&page_number=4

Higgins, K. J. (2007b). Hacking truckers, *Forbes.com*, New York, NY, 25 June 2007, from http://www.forbes.com/2007/06/25/cx_0625darkreading.html?partner=alerts

Hopper, N. J. & Blum M. (2001). Secure human identification protocols, In C. Boyd (ed.) *Advances in Cryptology - ASIACRYPT 2001*, Vol. 2248 of LNCS, pp. 52-66, Springer-Verlag, ISBN 3-540-42987-5, Gold Coast, Australia.

Juels, A. (2003). Privacy and authentication in low-cost RFID tags, *RSA Laboratories*, from http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/

Juels, A. (2005a). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, Vol. 24, No. 2, pp. 381-394, ISSN: 0733-8716.

Juels, A. (2005b). RFID privacy: A technical primer for the non-technical reader, In K. Strandburg & D. S. Raicu (Eds.), *Privacy And Technologies of Identity: A Cross-disciplinary Conversation*, pp 57-74, Springer-Verlag, ISBN: 0387260501, New York, NJ, USA.

Juels, A.; Rivest, R. L. & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. *Proc. of the 10th ACM Conference on Computer and Communications Security*, pp. 103-111, ACM Press, ISBN: 1-58113-738-9, 27-30 October 2003, Washington D.C., USA.

Juels, A. & Weis, S. A. (2005). Authenticating pervasive devices with human protocols, In V. Shoup (Ed.): *Advances in Cryptology – Crypto 2005*, Vol. 3621 of LNCS, pp. 293–308, Springer-Verlag, ISBN: 3-540-28114-2, Santa Barbara, California, USA.

Karygiannis, T.; Eydt, B.; Barber, G.; Bunn, L. & Phillips, T. (2007). *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, Special Publication 800-98, National Institute of Standards and Technology (NIST), April 2007, Gaithersburg, MD.

Kim, H. W.; Lim, S.Y. & Lee, H. J. (2006). Symmetric encryption in RFID authentication protocol for strong location privacy and forward-security, *Proc. of the 2006 International Conference on Hybrid Information Technology*, pp. 718-723, ISBN 0-7695-2674-8, Nov. 9-11, 2006, Cheju Island, South Korea.

Knospe, H. & Pohl, H. (2004). RFID security, *Information Security Technical Report*, Vol. 9, No. 4, pp. 39-50. ISSN: 1363-4127.

Landt, J. (2001). Shrouds of time: The history of RFID, *An AIM Publication*, Pittsburg, PA, Oct. 2001, from www.rfidconsultation.eu/docs/ficheiros/shrouds_of_time.pdf

Landt, J. (2005). The history of RFID, *IEEE Potentials*, Vol. 24, Issue 4, Oct.-Nov., pp. 8-11, ISSN: 0278-6648.

Langheinrich, M. (2007a) RFID and privacy, In M. Petkovic & W. Jonker (Eds.): *Security, Privacy, and Trust in Modern Data Management*, Springer, ISBN 978-3-540-69860-9, pp. 433-450, Berlin Heidelberg New York, July 2007.

Langheinrich, M. (2007b). A survey of RFID privacy approaches, *The Fifth Workshop on Ubicomp Privacy - Technologies, Users, Policy*, September 16, 2007, Innsbruck, Austria.

Lieshout, M. van; Grossi, L.; Spinelli, G.; Helmus, S.; Kool, L.; Pennings, L.; Stap, R.; Veugen, T.; Waaij, B. van der & Borean, C. (2007). RFID technologies: Emerging issues, challenges and policy options, *Technical Report EN 22770*, European Commission Joint Research Centre Institute for Prospective Technological Studies, ISBN 978-92-79-05695-6, Printed in Spain.

MacGillivray, G. & Sheehan, C. (2006). RFID security, *Semiconductor Insights*, RFID Security Issues Briefing to CANOSCOM, July 27, 2006.

Merritt, R. (2006). Cellphone could crack RFID tags, says cryptographer, *EE Times Online*, Manhasset, NY, February 24, 2006, from http://www.eetimes.com/news /semi/showArticle.jhtml?articleID=180201688

Messerges, T. S.; Dabbish, E. A. & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks, *IEEE Trans. on Computers*, Vol. 51, Issue 5, pp. 541–552, ISSN: 0018-9340.

MiniMe & Mahajivana (2005). RFID-Zapper (EN), *the 22nd annual Chaos Communication Congress (22C3)*, Berlin, Germany, 27-30 December 2005, from http://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)

Newitz, A. (2006). The RFID hacking underground, *Wired*, May 14, 2006, from http://www.etdot.com/2006/05/09/the-rfid-hacking-underground/

Ngai, E. W. T.; Moon, K. K. L.; Riggins, F. J. & Yi, C. Y. (2008). RFID research: An academic literature review (1995-2005) and future research directions, *International Journal of Production Economics*, Vol. 112, No. 2, pp. 510-520, ISSN: 0925-5273.

Nohl, K.; Evans, D.; Starbug & Plotz, H. (2008). Reverse-engineering a cryptographic RFID tag. *USENIX Security Symposium*, San Jose, CA, 31 July 2008, from http://www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf

Norton, M. (2006). RFID security issues, *Presentation at the Wireless and RFID 2006 Conference*, Feb. 27-Mar. 1, 2006, Ronald Reagan Building, Washington, DC.

O' Brien, D. (2006). RFID - Introduction and security considerations, *Presentation at the ISS World*, Washington, DC., Dec. 4-6, 2006.

Oertel, B.; Wolk, M; Hilty, L.; Kohler, A.; Kelter, H.; Ullmann, M. & Wittmann, S. (2005). Security aspects and prospective applications of RFID systems, *Federal Office for Information Security*, Bonn, January 2005, from http://www.bsi.bund.de /fachthem/rfid/RIKCHA_englisch.pdf

Piramuthu, S. (2006). HB and related lightweight authentication protocols for secure RFID tag/reader authentication, *Proc. of CollECTeR Europe*, Basel, Switzerland 9-10 June 2006, from http://www.collecter.org/archives/2006_June/23.pdf

Ranasinghe, D. C. & Cole, P. H. (2006). Confronting security and privacy threats in modern RFID systems, *Proc. of the Fortieth Asilomar Conference on Signals, Systems and*

Computers, pp. 2058-2064, ISBN: 1-4244-0785-0, Oct. 29 –Nov.1, 2006, Pacific Grove, California.

Rieback, M. R.; Crispo, B. & Tanenbaum, A. S. (2006a). The evolution of RFID security, *IEEE Pervasive Computing*, Vol. 5, No. 1, pp. 62-69, ISSN: 1536-1268.

Rieback, M. R.; Crispo, B. & Tanenbaum, A. S. (2006b). Is your cat infected with a computer virus? *Proc. of the 4th Annual IEEE International Conference on Pervasive Computing and Communication*, pp. 169-179, ISBN: 0-7695-2518-0, 13-17 March 2006, Pisa, Italy.

Rieback, M. R.; Simpson, P. N. D.; Crispo, B. & Tanenbaum, A. S. (2006c). RFID viruses and worms, *Vrije Universiteit Amsterdam*, 02 March 2006, from http://www.rfidvirus.org/

Rotter, P. (2008). A framework for assessing RFID system security and privacy risks, *IEEE Pervasive Computing*, Vol. 7, Issue. 2, pp. 70-77, ISSN: 1536-1268.

Schreur, R. W.; van Rossum, P.; Garcia, F.; Teepe, W.; Hoepman, J. H.; Jacobs, B.; de Koning Gans, G.; Verdult, R.; Muijrers, R.; Kali, R.; Kali, V. (2008). Security flaw in Mifare Classic, *Press release, Digital Security Group*, Radboud University Nijmegen, 12 March 2008, from http://www.sos.cs.ru.nl/applications/rfid/pressrelease.en.html

Thornton, F.; Haines, B.; Das, A. M.; Bhargava, H. & Campbell, A. (2006). *RFID Security*. Syngress Publishing, Inc., ISBN: 1597490474, Rockland, MA, USA.

Tsudik, G. (2006). YA-TRAP: Yet another trivial RFID authentication protocol, *Proc. of the 4th IEEE International Conference on Pervasive Computing and Communication Workshops*, pp. 640-643, IEEE Computer Society Press, ISBN: 0-7695-2520-2, 13-17 March 2006, Pisa, Italy.

Tuyls, P. & Batina, L. (2006). RFID-tags for anti-counterfeiting, In D. Pointcheval (Ed.), *Topics in Cryptology – CT-RSA 2006*, Vol. 3860 of LNCS, pp.115-131, Springer-Verlag, ISSN: 0302-9743, San Jose, CA, USA.

van der Togt, R.; van Lieshout E. J.; Hensbroek R.; Beinat E.; Binnekade, J. M. & Bakker, P. J. M. (2008). Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment, *Journal of the American Medical Association (JAMA)*, Vol. 299, No. 24, pp. 2884-2890, ISSN: 0098-7484.

Welch, D. & Lathrop, S. (2003). Wireless security threat taxonomy, *Proc. of the 2003 Workshop on Information Assurance*, pp. 76 – 83, ISBN: 0-7803-7808-3, 18-20 June 2003, West Point, NY.

Whiting, R. (2004). Focusing on E-payments at Medicare, Medicaid, *InformationWeek*, April 5, 2004, from
http://www.informationweek.com/ story/showArticle.jhtml?articleID=18900188

Wyld, D. C. (2006). RFID 101: The next big thing for management, *Management Research News*, Vol. 29, No. 4, pp. 154-173, ISSN: 0140-9174.

Xiao, Q.; Boulet, C. & Gibbons, T. (2007). RFID security issues in military supply chains, *Proc. of the Second International Conference on Availability, Reliability and Security*, pp. 599-605, ISBN: 0-7695-2775-2, 10-13 April 2007, Vienna, Austria

Supply Chain the Way to Flat Organisation

Edited by Julio Ponce and Adem Karahoca

ISBN 978-953-7619-35-0
Hard cover, 436 pages
Publisher InTech
Published online 01, January, 2009
Published in print edition January, 2009

With the ever-increasing levels of volatility in demand and more and more turbulent market conditions, there is a growing acceptance that individual businesses can no longer compete as stand-alone entities but rather as supply chains. Supply chain management (SCM) has been both an emergent field of practice and an academic domain to help firms satisfy customer needs more responsively with improved quality, reduction cost and higher flexibility. This book discusses some of the latest development and findings addressing a number of key areas of aspect of supply chain management, including the application and development ICT and the RFID technique in SCM, SCM modeling and control, and number of emerging trends and issues.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Qinghan Xiao, Thomas Gibbons and Hervé Lebrun (2009). RFID Technology, Security Vulnerabilities, and Countermeasures, Supply Chain the Way to Flat Organisation, Julio Ponce and Adem Karahoca (Ed.), ISBN: 978-953-7619-35-0, InTech, Available from: http://www.intechopen.com/books/supply_chain_the_way_to_flat_organisation/rfid_technology__security_vulnerabilities__and_countermeasures

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821