RFID Security Issues in Military Supply Chains

Qinghan Xiao[1], Senior Member, IEEE, Cam Boulet[1], and Thomas Gibbons[2]
[1] *Defence Research and Development Canada Ottawa*
Qinghan.Xiao@drdc-rddc.gc.ca
Boulet.Cam@drdc-rddc.gc.ca
[2] *Operational Support Transformation - CANOSCOM*
Gibbons.TA@forces.gc.ca

Abstract

Radio frequency identification (RFID) technologies have been used by the military to gain in-transit visibility and improve inventory management. The advantages of using RFID to track assets over using barcode have been broadly recognized. However, recent research has proven that RFID is vulnerable to attacks. This brings a challenge at a time when RFID systems are being employed in various applications, including military supply chain systems. In this paper, underlying vulnerabilities of RFID system are analyzed, different attacks that can be made against RFID system are illustrated, and countermeasures against the attacks are recommended. The objective of this article is to secure military logistics by identifying the common threats to RFID systems.

1. Introduction

Radio frequency identification (RFID) is a term applied to a number of technologies that utilize radio waves to automatically identify an object. The object is labeled with an RFID tag that comprises a chip and an antenna that can transmit stored data, usually identification information, to a reader. The first application of RFID was developed by Britain to identify friend and foe aircraft in World War II. In recent years, RFID technology has been used to replace bar code and successfully exploited by commercial supply systems to enable inventory tracking, warehouse management, and asset location. Compared with the bar code that must be optically scanned in a direct line of sight, RFID provides transparency across the product handling lifecycle and offers increased efficiencies in supply chain management. The most widely known RFID applications are supply chain RFID systems deployed by Wal-Mart and the US Department of Defense (DOD).

However, a military supply chain differs from a civilian supply chain in a number of respects, such as readiness for war at any time, great flexibility during times of war, large diversity of items, and long span with unstable demand. The major goal of the civilian supply chain is for profit, while the major goal of the military supply chain is for troop readiness. The US DOD began using RFID technologies as a response to lessons learned from Operations Desert Shield in the early 1990s. It has been reported: "In the Gulf War, the United States wasted $2 billion. They shipped five containers if someone needed one in hopes of finding something."[1] Since "logistics accounts for more than 50 percent of the war costs [2]", DOD officials came up with a plan directing the use of RFID technology as a standard business process across the department to address massive supply chain inefficiencies. RFID is seen by the US DOD as a key technology that "allows military logisticians to synthesize and integrate end-to-end information about assets". In 2004, the Acting Undersecretary of Defense for Acquisition, Technology and Logistics issued a policy that required the implementation of RFID technology across DOD.

> The desired end state for the DOD supply chain is a fully integrated, adaptive entity that uses state-of-the art enabling technologies and advanced management information systems to automate routine functions and achieve accurate and timely in-transit, in storage and in repair asset visibility with the least amount of human intervention.

Not only has the RFID solution developed by the US Army provided instant access to information about equipment and supplies, but also it ensures warfighter readiness and safety. According to its implementation plan, the DOD expects all of its 43,000 suppliers to be RFID-enabled so that the military could take the

Second International Conference on Availability, Reliability and Security (ARES'07)
0-7695-2775-2/07 $20.00 © 2007 IEEE

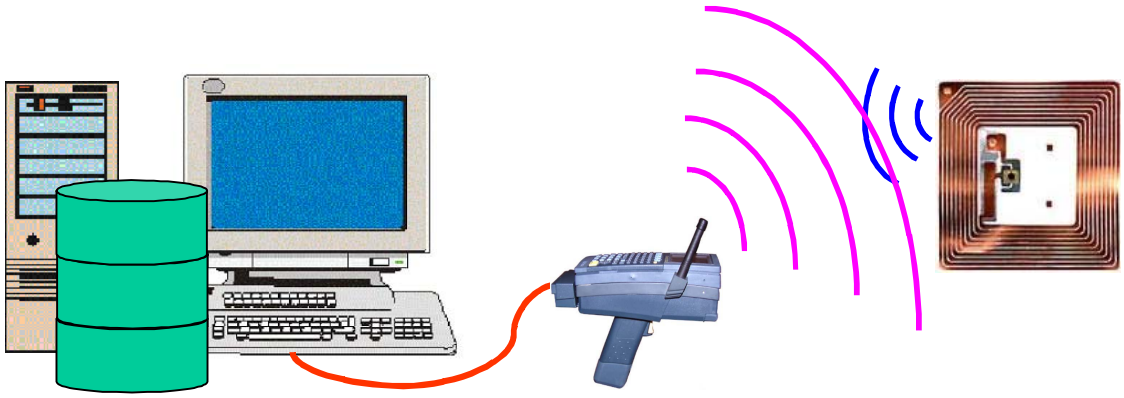

Figure 1. A generic RFID system

advantage of cost savings and effective operations by 2007 [3]. The recent Canadian Forces experience in Afghanistan indicates that a similar vision for the use of RFID technology is also required to provide effective and efficient operational support [4].

> In August 2006, Canadian Department of National Defense (DND) representatives met with PM J-AIT to request programmatic and technical assistance in fielding the US Radio Frequency In-Transit Visibility (RF-ITV) solution to multiple nodes in Canada, Turkey, and Afghanistan in support of Operation Enduring Freedom (OEF). This request was initiated by Canada to track over 500 Canadian assets using active RFID tags, write stations, fixed and handheld readers, and Early Entry Deployment Support Kits.

As with the Internet or mobile telephony, RFID is a wireless networking technology. System and data security are critical issues for RFID applications in military logistics. The non-contact and non-line-of-sight property of RFID increased convenience and efficiency. On the other hand it also increased the system vulnerability. Although RFID is just becoming popular for the mainstream (still an emerging technology), the security of some RFID systems has already been broken. Like other wireless communication and automation technologies, RFID technology is vulnerable to attack and security breaches can occur at the RFID tag, in the network, or in the backend systems. This paper will reveal possible attacks to RFID systems. The purpose of this paper is to provide information and defenses against these attacks. The rest of the paper is organized in the following manner. Section 2 presents a brief overview of RFID technology. Section 3 illustrates different attacks and countermeasures. Section 4 concludes the paper with the field where future research is needed.

2. RFID system

RFID is an emerging technology that uses radio waves as means to identify items or objects. Figure 1 shows a typical RFID system that contains one or more RFID tags, a reader, and a back-end sever.

2.1. System components

RFID tags, also known as transponders, are the identification devices attached to objects. Each tag typically consists of an antenna that is constructed of a small coil of wires, a microchip to store information electronically about the object, for example a military vehicle or a container being shipped overseas, and an encapsulating material. In addition, next generation tags are also linked to sensors that can track and report the shipment's environmental parameters, including temperature, shock and humidity. Like there are various types of barcode, RFID tags are available with different memory sizes and encoding options. However, different from the bar code, the information on the chip could include a unique serial number and product information, which benefits for retailers, manufactures and supply chain operators. Although their capabilities are impressive, RFID tags need to work with the readers.

An RFID reader, sometimes called an interrogator or scanner, is a device to communicate with the RFID tag. It emits RF signals to, and receives radio waves from, the tag via antennas. The reader then converts the radio waves into digital information that is usually passed to the back-end server. Readers can either be

handheld terminals or stationary devices, which consist of transmitter, receiver, antenna, microprocessor, memory, controller, and power.

The real power of RFID in supply chain management comes in integrating RF technology with a back-end server. The back-end sever can filter the digital information received from the reader and route it to the correct application. A back-end database stores records of product information, tracking logs or key management information associated with an RFID tag.

2.2. RFID tag categories

RFID tag is at the heart of an RFID system, and can be categorized as passive, semi-passive and active in relation to power, as well as read/write and read only in terms of its memory [5], [6].

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 powers 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 sends the information back to the reader. Because of the lack of a battery, passive tags have a reading range of several meters.

Semi-passive tags have a power source that keeps the chip on the tag constantly powered. Semi-passive tags use the power to monitor environmental conditions, but communicate by drawing power from the RFID reader in a manner similar to that of passive tags. Due to the use of batteries, semi-passive tags have faster response times and greater memory capacity compared to passive tags.

Active tags contain their own battery that supplies energy for both to power the chip on the tag and boost the return signal. This makes the tags able to continuously monitor high-value goods or record container seal status. Compared to passive and semi-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 up to 5 years.

Depending on the memory type, the tags can further classified as read-only, write once read many (WORM) or read/write.

Read-only tags are typically passive and most like bar codes because only a serial number is carried. Although the 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 allows users to encode tags one time during production or distribution. After that the code 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 and other assets in logistic applications. When the contents of the container are changed, new information can be updated on the tag.

Within this paper, RFID is used as generic term to describe any automated tagging and reading technology. It can include passive, semi-passive and active RFID technologies and various formats and applications.

2.3. Frequency bands

RFID systems are also distinguished by their wavelength frequency. Four primary frequency bands are low frequency (LF), high frequency (HF), ultra-high frequency (UHF), and microwave frequency (MW) [7]. Current RFID technology uses frequency ranges between 30 kHz to 5.8GHz. The choice of frequency is dependent on 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.

Frequencies from 30 KHz to 300 KHz are considered low, and RFID systems commonly operate between 125 KHz and 134 KHz. LF systems are generally use passive tags with short read ranges (up to 20 inches) and lower system costs, which are most commonly used in security access control, animal identification and asset tracking.

HF ranges from 3 MHz to 30 MHz, while HF RFID tags typically operate at 13.56 MHz. Like LF tags, a typical HF RFID system uses passive tags that have a maximum read range of up to 3 feet with faster data rates than LF tags. Not only have HF systems been widely used in library, mass transit and product authentication applications, but also adopted to make smart ID such as e-Passport.

The next frequency range is UHF that lies from 300 MHz to 3 GHz. Typically, passive UHF RFID systems operate at 915 MHz in the United States and at 868 MHz in Europe, while active UHF RFID systems operate at 315 MHz and 433 MHz, respectively. UHF systems can send information faster than LF and HF tags and offer the longest read range of all tags, from 3-6 meters for passive tags and more than 30 meters for active tags.

Table 1. RFID frequency bands and standards

	LF	HF	UHF	MW
Frequency	30 – 300 KHz	3 – 30 MHz	300 MHz – 3 GHz	2 – 30 GHz
Typical RFID Frequencies	125-134 KHz	13.56 MHz	433 MHz (Active) 865 – 956 MHz 2.45 GHz	2.45 GHz 5.8 GHz
Read Range	up to 1m with long-range fixed reader	up to 1.5m	433 MHz → up to100m 865-956 MHz → 0.5m to ≈5m	Passive ≈ 3 m Active up to 15m
Data Transfer Rate	Less than 1 kilobit per second (kbit/s)	≈ 25 kbit/s	433-956 →30 kbit/s 2.45 GHz →100 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 because a longer more expensive copper antenna is required.	Antennas can be printed on substrate or labels. HF signal penetrates water but not metal. HF tags are less expensive and offer higher read rate than LF.	Active RFID has a very long read range with high price of tags. Since using a battery, tags have a finite lifespan (typically 5 years). UHF tags have the highest read range for passive tags and capable of reading multiple tags quickly. However, they 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

A typical microwave RFID system operates either at 2.45 GHz or 5.8 GHz. The former is traditionally used in long-range access control applications, which has a read range of up to 1 meter as a passive tag or longer range as an active tag. In Europe, the 5.8 GHz frequency band has been allocated for road traffic and road-tolling systems.

Table 1 highlights the different types of RFID frequency bands with their characteristics, such as read ranges, data transfer rates, application areas and corresponding ISO standards. Among the ISO standards, the ISO 18000 serious covers the air interface protocol – the way RFID tags and readers communicate – for major frequencies used in RFID systems.

3. Attacks and countermeasures

Like other information systems, RFID systems are vulnerable to attack and can be compromised at various stages. Generally the attacks against a RFID system can be categorized 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 spoof and power attacks. This section illustrates different kinds of attacks and provides countermeasure against these attacks.

3.1. Eavesdropping

Since an RFID tag is a wireless device that emits a unique identifier upon interrogation 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 any compliant reader 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 – used later in other attacks against the RFID system. Countermeasures against eavesdropping include establishing a secure channel and/or encrypting the communication between the tag and reader. Another approach is to only write the tag with sufficient information to identify the shipment to another automated database that then provides the relevant information about the shipment, thus requiring the attacker to have access to both the tag and the database.

3.2. Man-in-the-middle (MIM) attack

Depending on the system configuration, a man-in-the-middle 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. This is a real-time threat. The attack will reveal the information before the intended device receives it and can change the information en route [8]. Even if it received some invalid data, the system being attacked might assume the problem was caused by network errors, but would not recognize that an attack occurred. An RFID system is particularly vulnerable to MIM attacks because the tags are small in size and low in price. Several technologies can be implemented to reduce the MIM threats, such as encrypting the communication, sending the information through a secure channel, and providing an authentication protocol.

3.3. Denial of service (DoS)

DoS attacks can take different forms to attack the RFID tag, the network, or the back-end to defeat the system. 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 on physical layer attacks, such as jamming and interference. Jamming with noise signals can reduce the throughput of the network and ruin network connectivity to result in overall supply chain failure. A device that actively broadcasts radio signals can block and disrupt the operation of any nearby RFID readers. Interference with other radio transmitters is another possibility to prevent a reader from discovering and polling tags. Fortunately, the risk of physical layer attacks to threaten a military supply chain's RFID system is low because the power of a signal drops 6dB when doubling the distance between sender and receiver [9]. In general, an attacker cannot get very close to the target or use an extremely strong transmitter within an effective distance. 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. Fortunately, this kind of DoS attack has a low risk to threaten military supply chains for the same reason mentioned above. However, the threats must be re-evaluated when outsourcing military logistics to private companies.

3.4. Spoofing

In the context of RFID technology, spoofing is an activity whereby a forged tag masquerades as a valid tag and thereby gains an illegitimate advantage. Tag cloning is a kind of spoofing attack that captures the data from a valid tag, and then creates a copy of the captured sample with a blank tag. Another example is that an attacker can read a tag's data from a cheap item and then upload the data onto another tag to replace the serial number for 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!"[10] A common way to defeat a spoofing attack is to implement RFID authentication protocol and data encryption, which will increase the cost and technology complexity.

3.5. Replay

In replay attack, an attacker intercepts communication between a reader and a tag to capture a valid RFID signal. At a later time, this recorded signal is re-entered into the system when the attacker receives a query from the reader. Since the data appears valid, it will be accepted by the system. The most popular solution is using a challenge and response mechanism

to prevent replay attacks. The time-based or counter-based scheme can also be used as countermeasures against replay attacks.

3.6. Virus

Since most of the passive RFID tags only have a small storage capacity of 128 bits, virus is probably not a big threat to RFID systems. However, the situation has been changed when three computer researchers released a paper in March 2006, which reported 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 [11]. A well-developed middleware can be used to avoid virus attack by blocking strange bits from the tag.

3.7. Power analysis

Power analysis is a form of side-channel attack, which intends to crack passwords through analyzing the changes of power consumption of a device. It has been proven that the power consumption patterns are different when the tag received correct and incorrect password bits. Professor Adi Shamir demonstrated the ability to use a password to kill a tag during the RSA Conference 2006. He also predicted that a power analysis attack on an RFID tag could be performed using a very common device such as a cell phone [12]. Either masking the spikes in power consumption or improving the hash algorithm will protect the tags being attacked by power analysis.

3.8. Tracking

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

4. Conclusion

Integrating RFID technology into military supply chains makes it possible to reduce the time of finding materiel pallets and reduce the risk of losing supplies in transit to an operational mission area. A major difference between a military supply chain and a civilian supply chain is the potential security threat posed by adversaries or their sympathizers who may wish to disrupt the distribution of materiel. Even though RFID tags are small, there are many potential exploitation points in RFID systems. In this paper, we analyzed the vulnerabilities of RFID technology, illustrated the threats of possible attacks, and provided countermeasure techniques. Although most of the attacking methods discussed in this paper have existed for several years, there is a chance that they are being applied to a new area – attacking RFID technology. With the increasing use of RFID in passports, personal IDs and consumer products, the attacks on RFID may pose security and privacy risks to both system infrastructures and individuals. Further work is needed in the following areas, such as the conduct of risk assessments, definition of security policy and development of more sophisticated approaches to defeat the attacks.

5. Acknowledgement

The authors would like to thank Colonel Frederick Michael Boomer for his support and valuable comments in the preparation of this article.

6. References

[1] R. B. Ferguson, "RFID: Locked and Loaded for NATO", *eWeek*, February 20, 2006, [Online]. http://www.eweek.com/article2/0,1895,1926586,00.asp

[2] F. Tiboni, "GAO Finds Iraq Logistics Problems", *Federal Computer Week*, December 18, 2003, [Online]. http://www.rfidnews.org/weblog/2003/12/30/gao-finds-12-billion-supply-discrepancy-in-iraq/

[3] C. Gardner, "DoD: Radio Frequency Identification", *AIAG's third annual RFID Summit*, November 2, 2006, [Online]. https://mows.aiag.org/scriptcontent/event_presentations/files/E6RFID01SP/DOD_final.pdf

[4] S. Philip, “Canadian Tracking Solutions”, *jWave Journal*, November 2006, [Online]. http://www.eis.army.mil/ait/Resources/jWave_Journal/jWave_journal_Nov06.pdf

[5] M. Ward, “RFID: Frequency, Standards, Adoption and Innovation”, *JISC Technology and Standards Watch*, March 2006, [Online]. http://www.rfidconsultation.eu/docs/ficheiros/TSW0602.pdf

[6] “RFID Primer”, *RFID Gazette*, November 21, 2005, [Online]. http://www.rfidgazette.org/2005/11/rfid_primer.html

[7] D. P. Mullen, “AIM Global Response to DHS Data Privacy and Integrity Advisory Committee”, *AIM Global*, June 13, 2006, [Online]. http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=1342&zoneid=26

[8] D. Welch and S. Lathrop, "Wireless security threat taxonomy," *Proc. of the 2003 Workshop on Information Assurance*, IEEE Systems, Man and Cybernetics Society 18-20 June 2003 pp. 76 – 83.

[9] P. Egli, “Susceptibility of wireless devices to denial of service attacks”, White Paper Embedded World 2006, [Online].http://www.netmodule.com/store/publications/susceptibility_of_wireless_devices_to_DoS.pdf

[10] A. Newitz, “The RFID Hacking Underground”, *Indymedia News Alerts*, May 14, 2006, [Online]. http://sf.indymedia.org/news/2006/05/1727888.php

[11] M. Rieback, B. Crispo, and A. S. Tanenbaum, “Is Your Cat Infected with a Computer Virus?” *Proc. of 4th Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM’06)*, March 2006, [Online]. http://vx.netlux.org/lib/aat02.html

[12] R. Merritt, “Cellphone could crack RFID tags, says cryptographer”, *EE Times*, February 14, 2006, [Online]. http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=180201688