

Evaluating and improving the security of RFID tags in eSeals at the L.A. and L.B. Ports

Burkhard Englert, Dolgorsuren Byambajav and Aniketh Parmar *
California State University Long Beach
Department of Computer Engineering and Computer Science
1250 Bellflower Boulevard
Long Beach, CA 90840
Tel: (562) 985-7987
Email: benglert@csulb.edu

Abstract

Over the last few years there has been a steady increase of international trade and of shipments arriving at US ports from countries where security practices are considered less reliable. This led to a parallel rise of the vulnerability of the supply chains and the ports in particular. As a possible way to reduce these vulnerabilities, the use of Radio-Frequency IDentification (RFID) tags in shipping containers has been suggested. RFID tags ideally can be used to identify and monitor individual containers without physically having to inspect them. However these tags themselves can possible become security risks. In this paper we study the potential vulnerabilities of such tags as they likely will be used in the near future in RFID systems at the Long Beach and Los Angeles ports. Based on the results of this investigation we make some recommendations on how to best protect the supply chains and the ports of Long Beach and Los Angeles themselves.

1 Introduction

Recently there has been considerable media attention concerning the vulnerability of US ports in general, and the Los Angeles and Long Beach ports in particular. This is largely due to a shift in cargo security emphasis from prevention of theft and contraband to terrorism. Since this new threat is very difficult to evaluate and quantify, however, resistance among many companies to spend on cargo security has been growing continuously over the last few years. At the same time, as a result of a 10 percent annual increase in global trade and an increased proportion of shipments from countries where security practices are less reliable, the vulnerability of U.S. companies supply chains has been steadily increasing.

To deal with this problem in an efficient manner, the World Customs Organization recently proposed a "Framework of Standards to Secure and Facilitate Global Trade" (World Customs Organization 2005). It calls for national programs that distinguish authorized economic operators(AEO's), shipping companies that volunteer to comply with the respective countries security guidelines. Such companies would then be considered "trusted" and their cargo would be marked to receive expedited handling at the country's borders. In

*Research supported by the US Dept. of Transportation under METRANS 06-01.

the U.S., the Department of Homeland Security through its Bureau of Border and Customs Patrol introduced and supports two main new programs designed to ensure the safety of shipments arriving at U.S. ports: the Container Security Initiative (CSI) (US Customs) and the Smart & Secure Trade Lanes (SST) program (Smart and Secure Tradelanes 2003). The Container Security Initiative is designed to extend the U.S.'s security perimeter outwards, making US borders the nation's last line of defense rather than its first. The program, which was announced in January 2002, attempts to identify high-risk maritime cargo containers and search them for weapons of mass destruction at foreign ports before they are shipped to the United States.

The SST program, on the other hand, is an initiative of the Strategic Council on Security Technology. It is a phased, industry-driven initiative using an open technology platform in coordination with U.S. Customs, the Transportation Security Administration, Operation Safe Commerce, C-TPAT (Customs Trade Partnership Against Terrorism) (US C-TPAT) and the Container Security Administration to improve the security and productivity of cargo shipments.

What are the incentives for companies to participate in the voluntary C-TPAT program? The Bureau of Customs and Border Patrol describes at least four possibilities: (1) fewer inspections of inbound cargo, (2) "green lanes" to speed up handling of compliant cargo, (3) "restart priority" in the event of port closure due to disaster and (4) paperless information exchange. Until now only reduced cargo inspections (1) have been implemented. As a result only about 4,000 out of about 50,000 U.S. importers have applied to join C-TPAT. If, however, in the near future it can be shown that an investment in cargo security is contributing to supply chain efficiency, this number is bound to grow dramatically. To support such growth it will be important to carefully analyze the security implications of the proposed technologies. The SST application, the focus of this paper, uses Radio-Frequency Identification (RFID) systems.

Paper Outline In Section 2 we will review the basic characteristics of RFID Systems. In Section 3 we will discuss the risks and threats associated with RFID technology and present some of the techniques used to control these risks. In Section 4 we will investigate the use of eSeals at the L.A. and L.B. ports and discuss the new eSeal ISO 18185 standard and the Savi tags on which it is based. Based on this current state of affairs we conclude with some recommendations for the local ports in Section 5.

2 RFID Systems

What are RFID Systems? In the following section we will describe some basic characteristics of RFID Systems.

2.1 Technical Characteristics of RFID systems

RFID systems are comprised of three main components (Peris-Lopez et al.):

- RFID tag or transponder - the data carrier in the RFID system.
- RFID reader or transceiver - able to read data from tags and possibly write data to them.
- Data Processing subsystem or back-end database - processes the data received from the transceiver in some useful manner.

1. **RFID tag or transponder.** A typical tag consists of a microchip that stores data and a coupling element like a coiled antenna that communicates using radio frequency communication. RFID tags can be classified according to three main criteria:

- The type of memory they provide: read-only, write-once read-many, or fully rewritable.
- Their source of power: active, semi-passive or passive. The most inexpensive and smallest tags are *passive*, they receive all their transmission power from the reading device. These tags are also the most physically robust RFID tags. *Active* tags on the other hand contain batteries. As a result they are able to broadcast much longer distances than passive tags but they also suffer more from outside interference. ESeals are usually based on active tags. Recently *semi-active* (sometimes also called *semi-passive*) tags have found a lot of interest. Semi-active tags make use of battery power to run local circuitry, but use reader power to communicate. Most tags, both active and passive, communicate only when they are queried by a reader.
- The frequency tags use to communicate.

While lower frequencies have shorter associated ranges, they also offer better penetration of materials; higher frequencies on the other hand offer greater range, but are subject to greater physical interference. The two most important RFID-frequency categories are as follows:

- Ultra-High Frequency (UHF): UHF tags operate in the 868-956 MHz frequency band. Passive UHF tags have a range, in many environments, of over ten feet (and sometimes as much as tens of feet). Additionally, RFID readers can scan hundreds of UHF tags simultaneously. A major drawback of UHF tags is that they cannot be easily read in the presence of high concentrations of liquids, as found in such things as beverage containers and humans.
- High-Frequency (HF): Passive HF tags have the drawback of low transmission range of just over a foot. They are usually also larger than UHF tags; flat HF tags are typically about 50mm by 100mm in size. HF tags, however, are readable in the presence of water. HF tags operate at 13.56 MHz, a frequency known as the Industrial-Scientific-Medical (ISM) band.

RFID tags also come in a low-frequency (LF) variety operating at 120-140 KHz or operate at higher UHF frequencies, most notably at 2.45 GHz. More details about the specifics of the communication between RFID tag and reader can for example be found in (Sarma et al. 2002).

The least expensive RFID tags, such as basic Electronic Product Code (EPC) tags, are read-only. Such a tag is capable of transmitting a unique serial number a distance of several meters or more in response to a query from a reading device. Writable tags are more expensive, while rewritable tags (containing EEPROM) are still more expensive.

The tags that are most inexpensive are passive and lack the computing power to perform even basic cryptographic operations. (They will have about 500-5000 gates, many devoted to the basic tag functions. By contrast, the Advanced Encryption

Standard (AES) requires some 20,000-30,000 gates.) Such tags are at best capable of employing static keys, i.e., PINs and passwords as security mechanisms.

More expensive RFID tags (usually active tags with battery power) are capable of advanced functionality, and often include the ability to perform basic cryptographic algorithms, such as symmetric-key encryption and challenge-response identification protocols. (Public-key cryptographic is expensive, and used on few RFID tags.) Implementing and using such cryptographic algorithms, however will put a large strain on the battery of an active tag. Once the battery of an active tag becomes depleted the tag itself usually must be replaced. This increases the cost of any cryptography enabled active tag based RFID system.

2. **RFID Reader or Transceiver.** RFID readers consist of a radio frequency module, a control unit and a coupling element used to query tags via radio frequency communication. Many also have an interface that allows them to forward data received to a data processing subsystem.

To identify many tags in its read range, an RFID reader must communicate with the tags in an anti-collision or singulation protocol. Otherwise the signals of multiple tags would interfere with one another, making reading impossible. Singulation protocols enable tags to take turns in transmitting to a reader.

In UHF tags, singulation uses a variant of a protocol known as tree-walking. Briefly speaking, a reader traverses the k-bit "tree" of tag ids, asking subsets of tags to broadcast a single bit at a time. Consequently in the basic tree-walking protocol the RFID reader must broadcast tag serial numbers over very large distances, which can introduce vulnerability to eavesdropping.

HF tags on the other hand generally use a variant of the classic ALOHA protocol. Briefly stated, tags in the ALOHA protocol transmit their identifiers to the reader at randomly determined times so as to avoid transmission collisions. ALOHA-based RFID reading leaks less information than most UHF tree-walking protocols. But most HF readers are capable of scanning only several dozen tags simultaneously.

3. **Back-end databases.** The information that is provided by a tag usually represents a simple index in a back-end database. As a result it suffices to store only very few bits on the tag itself (in many cases as little as 96 bits. Communication between readers and back-end databases is usually secured with strong encryption using SSL or other suitable protocols.

3 RFID Security

We will now discuss some of the main possible security problems associated with RFID Systems.

3.1 RFID Risks and Threats

1. **Privacy Attacks.** One of the most fundamental problems associated with RFID tags that still needs to be addressed is privacy, that is items that are tagged indiscriminately reveal sensitive information when queried by a reader. This may also lead to tracking, a violation of location privacy. Since most tags when queried always provide the same

identifier it is possible to establish an association between a tag and its owner. Even in cases where tags do not reveal any valuable information that could be used to identify them it might still be possible using an assembly of tags to perform this kind of tracking.

2. Physical attacks. In this case tags are manipulated physically, e.g. radiation imprinting, circuit disruption, clock glitching. Tags usually are not resilient against such attacks.
3. Counterfeiting. In this case tags are directly manipulated to modify the identity of an item.
4. Spoofing. In a spoofing attack an attacker successfully impersonates a legitimate tag. The attacker can, for example, record the signal transmissions between tag and reader (if the attacker is close enough to both tag and reader) and replay them when desired to impersonate the recorded tag.
5. Eavesdropping. In this case attackers are able to intercept and read RFID communications.
6. Skimming Attacks. Most RFID devices today broadcast a static identifier without any explicit authentication procedure. As a result an attacker in a so called *skimming* attack can simply scan identifying data. Such skimmed data can then be used to produce cloned tags, exposing several lines of attack. In the case of shipping containers for example, an attacker could feasibly break into a container and then replace the now silent tag with a cloned tag that simply rebroadcasts the id skimmed from the original tag. Such a container would then most likely escape inspection. Another possibility would be that in a *swapping* attack the attacker simply swaps the original container and its RFID tag with an alternate container and its cloned tag.
7. Denial of Service, e.g. signal jamming of RF channels. Clones can also create denial-of-service issues. If several, valid-looking clones appear simultaneously at a port, should they be honored as legitimate? Or must they all be inspected and rejected as fraud? In this way cloned tags could be intentionally designed to corrupt supply chain databases.

Recently researchers were able to demonstrate practical cloning attacks against real world RFID devices. Mandel, Roach and Winstein (Mandel et al. 2004) showed how to read access control proximity card data from a range of several feet and produce low cost clones. This was possible even though the cards they tested themselves had a legitimate read range of only several inches. Researchers from Johns Hopkins University and RSA Laboratories (Bono et al. 2005) recently studied and performed attacks against cryptographically enabled RFID tags as they are used in payment and automobile immobilization systems. In their attack they were able to extract secret keys using reverse engineering and to simulate target transponders. They showed an existing risk of auto theft from the compromise of RFID systems.

8. Traffic analysis. In this case an attacker attempts to extract information from a pattern of communication. Such an attack is possible even if the messages transmitted are encrypted.

3.2 Possible Solutions

Securing RFID tags is challenging because of their limited resources and small physical form. Limited power, storage and circuitry make it difficult to implement traditional authentication protocols.

We will now briefly describe some proposed techniques to secure RFID tags.

1. **The Kill command.** Proposed by the Auto-ID Center (Auto-ID Center 2003) and EPCglobal. Tags have unique passwords that are programmed at the time of manufacture. Once a tag receives the correct password it deactivates forever.
2. **Tag shielding and isolation.** To ensure privacy tags are isolated from all electromagnetic waves. Shielding can occur in what is called a Faraday cage. Several companies sell this solution (mCloak 2005). Shielding potentially prevents tag cloning and skimming attacks.
3. **Active Jamming.** In this case to isolate a tag from electromagnetic waves the radio channel on which communication is supposed to occur is disturbed. A device simply broadcasts radio signals on the same frequency that reader and tag would use and as a result prevents the normal operation of a potential attackers reader.
4. **Blocker Tag.** If a reader sends a query to a tag and more than one tag responds a collision is detected. To nevertheless enable communication with individual tags a singulation protocol is used. Based on such protocols Juels (Juels et al. 2003b) introduced a passive jamming approach called a *Blocker Tag*. In a paper with Rivest and Szydlo (Juels et al. 2003b), Juels describes a Blocker RFID tag that acts as a "spamming" device, disabling any reader that attempts to scan tags without the right authorization.
5. **Silent Tree Walking.** Another technique suggested by Weis, Sarma, Rivest and Engels to prevent this type of attack is called *silent tree walking* (Weis et al. 2004). This technique is a refinement of the tree walking singulation protocol and effective against long range adversaries that are able to listen to reader transmissions but not to tag responses.
6. **Traditional Cryptography.**
 - (a) Kinoshita (Kinoshita et al. 2005) proposed an anonymous-ID scheme specifically designed for active tags. Instead of storing the "real ID" of a tag, an anonymous ID $E(ID)$ is stored, where E is a symmetric or asymmetric cryptographic function or a random value linked to the tag ID. In implementation tests, however, it became clear that changing the id of the tag can potentially reduce the battery life of an active tag. Ids should be changed at most once per hour.
 - (b) Feldhofer (Feldhofer et al. 2004) suggested an authentication scheme based on a simple two-way challenge response algorithm. This algorithm, however, requires AES to be installed on the tag. AES is a very powerful but also expensive (in terms of computing power required) and hence impractical cryptographic algorithm. Recently some AES implementations for RFID were presented (Jung et al. 2005).

- (c) **Public Key Encryption.** These solutions use the cryptographic principle of re-encryption (Juels et al. 2003a). Golle, Jacobsson, Juels and Syverson (Golle et al. 2004) propose the concept of universal re-encryption. In the case of RFID's, "public" readers could simply re-encrypt a ciphertext for tags in their vicinity, freeing tags from the power consuming encryption task and preserving the tags privacy at the same time. The scheme fails, however, if a malicious agent re-encrypts a ciphertext after adding malicious messages to it.

7. Hash functions.

- (a) **Hash Lock Scheme.** Weis (Weis et al. 2004) proposed an elegant security scheme that is based on one-way hash functions. Every tag stores in its memory a temporary metaID and is either locked or unlocked. The metaID stored is the hash value of a given key k that was hashed by the reader. If a tag is locked it simply responds with the stored metaID and provides no other functions. To unlock a tag a reader queries the back-end database with the metaID, receives the appropriate key k and sends k to the tag. The tag rehashes k and compares it with metaID. If the two match, the tag is unlocked.
- (b) **Randomized Hash Lock Scheme.** This is an extension (Weis et al. 2004) of the previous scheme (requiring the availability of a pseudo random generator) where the metaID is changed repeatedly in an unpredictable way.
- (c) **Hash-Chain Scheme.** Ohkubo (Ohkubo et al. 2004) proposed a hash chain scheme where two distinct hash functions are embedded in a tag. The scheme hopes to guarantee complete user privacy, does not require external rewrites of tag information, minimizes tag cost, reduces power needs of tags and provides forward security.

8. Pseudo Random Function Authentication Schemes (Molnar et al. 2004).

This scheme allows tags and readers to mutually authenticate each other while at the same time guaranteeing privacy for the tag. It requires a secret s that is shared between tag and reader and a Pseudo Random Function, that is a function whose output is "almost" indistinguishable from truly random output.

- 9. **Tree-based Private Authentication (Molnar et al. 2004).** This scheme reduces the load of the server to $O(\log n)$ (where n is the number of tags) on the server but requires the use of a Trust Center (TC). To reduce the load on the TC an offline delegation was suggested (Molnar et al. 2005). Avoine and Oechslin (Avoine et al. 2005) on the other hand proposed a time-space trade-off to deal with this problem.
- 10. **Defense against Spoofing for Active Tags (Yamada et al. 2005).** Yamada et al. proposed that readers encrypt (with a shared secret) the system time, allowing tags to recognize spoofing attacks.
- 11. **Human Protocols.** Juels and Weis (Juels et al. 2005) proposed to adapt human computer authentication protocols as described by Hoppner and Blum to low-cost RFID. Recently Juels and Weis (Juels et al. 2005) extended this idea by proposing a lightweight symmetric-key authentication protocol called HB^+ .

At the present time most cryptographic schemes are not yet feasible for RFID tags or have not yet been tested enough to justify confidence in their security. This to a large extent determines any attempt to secure such tags. The following Security study illustrates these problems.

3.3 RFID Security Studies

The National Institute of Standards and Technology (NIST) recently (May 2007) issued a report, Guidelines for RFID Security (NIST RFID Security 2007) that contains a list of recommended practices for RFID security and two case studies. To ensure the security and privacy of RFID systems the report recommends:

- Firewalls that separate RFID databases from an organization's other databases and Information technology Systems.
- Encryption of radio signals when *feasible*.
- Shielding of RFID tags or tag reading areas with metal screens or films to prevent unauthorized access.
- Security measures for audit and recycling procedures and tag disposal.

One of the two case studies specifically addresses the supply chain management of hazardous materials using RFID systems: The Radionuclide Transportation Agency (RTA) supervises the movement of radioactive research materials between relevant locations. The agency wants to know who is in possession of what quantity of materials at any given time. Moreover RTA would like to be able to locate materials at a site quickly without having to search the complete site. Simple bar codes do not have these capabilities. In addition RTA would like to measure environmental conditions and record readings on the tag. Finally the handling of radioactive materials is a homeland and national security issue, access should be restricted to authorized personnel.

The case study (NIST RFID Security 2007) provides concrete examples for the obstacles to RFID security in the supply chain. The authors identified the following risks:

- Based on an RFID tag read, an adversary could *identify and target* a vehicle containing RTA-regulated material.
- An adversary could eavesdrop on tag transactions to learn the characteristics of material to determine its value.
- An adversary could damage or disable a tag, and as a result be able to steal material without detection.
- An adversary could alter data stored on the tag to undermine the business process for which the material is used.
- Radiation from readers could accidentally cause combustion of collocated volatile materials when several readers are operating concurrently close to each other.

To reflect these risks the agency required that tagged items only be identifiable during embarkation, debarkation and storage and not during transport. Moreover active tags had

to be used and tag-reader communication should be authenticated whenever technically feasible. All personnel involved in the handling of the tagged materials was required to be provided with RFID security and privacy awareness training.

The design team determined that the risk of eavesdropping and rogue RFID transactions could be within acceptable levels if adversaries were located at least 100 meters from the storage area. To prevent readings during transport, the design team specified mechanisms for shielding containers and vehicles. The team realized that even though some users might benefit from being able to read a tag from outside a vehicle that the risk this introduced outweighed the benefits.

The tags themselves were password protected using a proprietary technology. Because the materials with the tags moved through the supply chain a central password database was established. This database could remotely be accessed by the RFID middleware of each stake holder. The database was also placed into a Virtual Private Network that was isolated from public networks.

To address the risk of spontaneous combustion it was decided to use HF and not UHF or microwave technology.

4 Active Tags at the Ports - ESeals

The main focus of this paper is the study of the security of RFID chips in shipping containers. One main application of RFID technology in the context of shipping containers is their use as "eSeals". Such - usually active - tags are, for example, used to provide efficient, instant notification of container security breaches. Traditional container seals only provide evidence of unauthorized entry when they are physically inspected. RFID container seals, however, provide automatic notification of tampering by going "silent." To be truly effective, this approach requires systems that can constantly log and monitor all container seals in a given geographical area so that any that suddenly stop responding can be flagged for action. Smart tags can also be equipped with sensors to monitor environmental conditions within the container. It is not possible to counterfeit tags, so there is no possibility that one tag will be removed and another used to replace it. Eavesdropping on RFID readers, however, is a major threat for such systems. RFID readers can broadcast RFID tag data over long distances, often up to hundreds of meters away. It is difficult to shield the radio emissions of readers effectively without disrupting their functionality. Thus, an eavesdropper with an antenna and some basic receiving equipment can gather the same RFID tag information that is compiled by the reader at the port. An eavesdropper may also be able to physically tamper with a container seal and hide this intrusion by creating a signal that impersonates that of the original RFID tag. These possibilities illustrate the need for strong authentication and data transmission protection.

The new ISO 18185 for electronic seals standardizes under 18185-4 the data protection requirements of such eSeals (ISO 18185-4). More precisely, the standard addresses data protection, device authentication and conformance. Originally the publication of this standard had been delayed because of concerns about RFID security. As it appears now however, ISO was finally able to ratify the standard by simply ignoring these concerns and postponing any meaningful approaches to a later date. With respect to data protection the standard states that "under the terms of this first generation part of ISO 18185, the current communication with the electronic seal is performed in **clear text** and does not include any confidential information. Consequently there are no requirements regarding confidential information at

this time” (ISO 18185-4). In terms of eSeal authentication, only physical identification is required at this time. ”The seal manufacturer shall be able to identify and authenticate the seal as a valid seal based on proprietary information, its unique manufacturing characteristics, and the fixed data” (firmware) (ISO 18185-4). No electronic authentication is required at this time. Finally with respect to conformance ”electronic seals claiming compliance with this part of ISO 18185 shall have the high security mechanical seal physical properties defined in ISO/PAS 17712. They shall further comply with the electronic seal manufacturers’ security related practices identified in Annex A” (ISO 18185-4).

This annex specifies the security responsibilities of the seal manufacturers. It mainly states that manufacturers have total responsibility for the e-Seal design and manufacturing process and are responsible to maintain data on production, sales and ID numbers of e-Seals, readers and related equipment. In all other phases of the e-Seal life cycle the main responsibility falls on the users and manufacturers are simply asked to help educate such users.

By providing a common standard ISO 18185 at least removes one of the major obstacles for the widespread use of eSeals. Other major obstacles that remain are of a more practical nature. ESeals will have to work in harsh environments under often severe conditions. Moreover the tags themselves will be placed within a metal container causing interference and possibly impeding the radio signal emitted.

4.1 SaviTM Tags

The RFID tags produced by Savi Technology (Savi website) have become a market leader in the area of eSeals. Early adopters of the Savi system include the US military. Founded in 1989, Savi is a wholly owned subsidiary of Lockheed Martin.

Savi’s active tags are based on their patented EchoPointTM technology. EchoPoint uses a multi-frequency design and a three-element system architecture to achieve relatively reliable long-range communication and short-range locating capability. In addition to the customary tag plus reader architecture, EchoPoint adds a third element, the signpost. Signposts communicate with tags over a short-range inductive (123 Khz) link and the tags communicate with readers over a long range 433 MHz UHF frequency. Signposts themselves can be either fixed, mobile or hand held and notify tags of their location whenever they are in range of such a ”post”. Tags then notify readers of their location (together with a unique identification code). As a result, even though readers communicate with tags over relatively large distances (100 yards) they are able to obtain precise location information.

In 2006 Savi introduced Savi Tag ST-656 specifically designed to withstand severe conditions. This tag comes in a U-shaped form and clamps tightly onto the left container door. As a result the RFID electronics are protected within the container while a low-profile plate outside the container holds an antenna that is used for communications. This plate also contains a beeper for audio alerts of the tag’s location and status. This combination of low-external profile and the protected RFID components is supposed to reduce the risk of damage under harsh operating conditions. The tag includes an onboard processor, memory and radio transmit and receive capability. It is possible to write to the tag while it is in transit and to capture data about the shipment from mobile readers.

These tags alone, however, come with a significant price tag of at least \$100 for each tag, not including readers, signposts and operating software. These cost factors, together with a lack of interoperability, standards and a perceived lack of security led many companies to question any potential return on investment into this new technology. As a result only

agents such as the US military that have a large amount of control over their supply chains - that can enforce interoperability by simply changing all their systems - were early adopters.

Hence to convince other international shippers of the usefulness and the benefits of this technology several large scale demonstrations were recently executed. For example, Savi and Oracle teamed up in early 2007 to provide a critical information link to track in real time the location of containers shipped from Honk Kong to Japan. The project was initiated by GS1 EPCglobal, the nonprofit organization driving adoption of the Electronic Product Code (EPC) to improve supply chain performance. In this project for the first time, real-time information generated by active (battery powered) RFID tags on sea containers was exchanged with EPC Information Services (EPCIS), a draft GS1 EPCglobal standard enabling trading partners to communicate in a common language about objects moving through the supply chain. The communication interface was enabled through the integration of the Oracle Sensor Edge Server, Savi Site Manager operating software and active RFID tag and data collection systems. A similar project linking the port of Shanghai China and the Savannah port in Georgia is currently under preparation.

Earlier this year it was also announced that Savi's SaviTrak real-time information service would be extended to include the Port of Busan in South Korea.

4.2 Savi Tags and ISO 18185

The new ISO 18185 standard for eSeals (April 2007) is based on Savi's active RFID technology. All eSeals based on ISO 18185 require the use of Savi in electrode property (ISO 18185-4).

Since Savi intellectual property (IP) is incorporated into ISO 18185, Savi released RFID Patent licensing for e-Seals in May 2007. After obtaining a license companies gain access to Savi's intellectual property that is incorporated into the ISO standard 18185. In particular users need to obtain a license for the use of Savi's IP that implements the tag-to-reader communication requirement in ISO 18185.

4.3 ESeals at the Ports of L.A. and L.B.

There is currently no widespread use of eSeals at the ports of LA and LB. Based on experiments in other supply chain applications and the ratification of ISO 18185 it is to be expected that this will change in the very near future. This implies a need to find ways to secure ISO 18185 based eSeal systems. We will address this in the next section.

5 Recommendations

So far RFID Systems are only used in a very limited fashion at the ports of L.A. and L.B. (e.g. Pierpass).

In the case of eSeals not much progress has yet been made at the ports of Los Angeles and Long Beach. While other ports and supply chains are currently in the process of testing such applications (Hong Kong to Japan, Shanghai to Savannah, the Port of Busan South Korea etc.), progress has been relatively slow at the L.A. and L.B. ports. There are several possible reasons for this delay.

1. Besides all the promises made by RFID System manufacturers the technology has not yet matured sufficiently. There are still many unresolved issues with respect to

reliability. The failure rate of many RFID systems is still too high causing many companies to hesitate with an investment.

2. Many interoperability problems have not yet been addressed. It still appears to be very cumbersome to integrate an RFID system with existing enterprise software. Many companies simply do not want to invest into new technology that they cannot seamlessly integrate into their existing systems.
3. Until recently there was a complete lack of eSeal communication standards.
4. There is still widespread concern about the security of eSeals.
5. These issues combined lead to the general perception of a non existent or very low return on investment in an eSeal RFID system, re-enforcing many affected companies in their "wait and see" attitude.

5.1 ESeal Security

The new ISO standard 18185-4 does not demand any encryption of data transmissions between an eSeal and an RFID reader. This is most likely due to the fact that satisfactory encryption techniques have not yet matured enough to be useable for eSeals. While there is a relatively large amount of research results on RFID security, most of these results are not yet ready for real implementations. The reasons are mainly of a more technical nature. In the cases of eSeals (active RFID tags) the battery power severely limits the capabilities of these tags. Once a tag's battery is discharged the tag must be replaced. At a price of usually at least \$100 per tag this adds a significant amount of additional costs. Using powerful cryptographic functions would deplete a tag battery even faster. But not only expensive cryptographic functions can deplete a tag battery very fast, even simply periodically changing a tags id number depletes the battery faster and therefore lowers the return on investment.

On the other hand, even if we had unlimited battery power available it would still be difficult to settle on a final cryptographic implementation. In contrast to code embedded on a hardware device such as an RFID tag, strictly software based programs essentially can be updated and 'repaired' whenever need be, that is when based on a successful hacking attack a security flaw has been discovered. On an RFID tag, however, the cryptographic programs will essentially have to be hardwired onto each tag. This means that they are practically not changeable after the tag has been manufactured. Hence, if ever weaknesses or flaws in the cryptographic implementations on an already produced RFID tag are discovered, tags cannot be "repaired". To be safe all such tags would have to be removed, new tags (without the flaw) would have to be bought and installed.

This fact further fuels the current hesitation with respect to strong (cryptography based) security features on RFID tags. It is probably the main unresolved challenge for RFID system manufacturers to manufacture tags that have a sufficiently long battery life and that have been tested so thoroughly that with very high certainty their security implementation will withstand all known attacks and is software bug free. This by itself is a very difficult and challenging problem whose complexity to a certain extent justifies the hesitation to install strong cryptographic functions on RFID tags: Any premature, error prone release could have devastating consequences for the future of RFID based technology and would likely wipe out or at least greatly decimate the whole RFID manufacturing industry. In

this sense this industry has a very careful approach to any plans to require strong security primitives for RFID communication, explaining a general hesitation and lack of progress in this area. It also helps to explain the lack of any encryption requirements in the new ISO 18185 standard.

As a result, any real progress with respect to RFID security may have to be motivated and initiated by the non private sector. Governments and governmental organizations will have to lead the push for strong RFID security by investing into the technology through research grants and by installing and using it for government related enterprise. This practical proof may be the only way to convince the private sector of the benefits of RFID and to provide a tangible and convincing example of its safety and strong business and security benefits.

5.2 Future Developments and Recommendations

Nevertheless as a result of ISO 18185 and a constant stream of eSeal experiments it seems more and more likely that in the very near future - if not already - eSeals will start to be used at the Ports of Los Angeles and Long Beach. So the question of their security must be addressed and should not be ignored. Based on the lack of any data protection and encryption standards it will be essential to rely on a more broad approach to security for eSeals. It will take the interplay of several different approaches to provide the desired security. In other words, instead of - through the use of strong cryptography - simply relying on the security of the data transmissions between tags and readers we should at the present time focus on protecting and shielding these transmissions directly themselves. This requires a comprehensive approach that addresses and includes all aspects of Port Security:

- Tag transmissions should be shielded whenever tags are not currently read by a reader. This will help prevent skimming attacks and will make it more difficult for an attacker to impersonate a tag by simply replaying the tag Id. Tags could be covered by a faraday cage comparable device before loading overseas, while on the ship and when on a truck / rail car. This cage will shield the tag while in transit. This will make it much more difficult for an attacker to simply record a tags signal and then after breaching a container to simply replay it to impersonate the tag.
- In addition, tag signals should be continuously jammed while the tag and the container that contains it are in transit to a US port.
- The autoID scheme should be used to provide an additional amount of security. The autoId scheme allows tags to periodically change their id's. As long as this does not happen too often it is manageable by the currently available tag batteries (without reducing their life-span significantly). It will likely suffice for tags to change their ids every time when they enter a US Port.
- Readers should be installed only in the interior of the port (and terminal) areas so that - if possible - a radius of 100 to 150 meters around each reader will still fall within the Port or terminals area. This area should then be closely supervised by port police and other agencies to prevent attackers from accessing RFID signals.
- Until tag-reader transmissions can be sufficiently encrypted a large amount of 'traditional security' is required. Tag shielding devices should be tamper proof. All

personnel with access to the ports should be subject to thorough security checks so that only trusted personnel has access to the read range of the used active tags.

With this steps it will be possible to use eSeals at a time when they cannot yet provide for their own data transmission protection.

References

- [Auto-ID Center 2003] Auto-ID Center. 900 MHz class 0 radio frequency (RF) identification tag specification. Draft, March 2003.
- [Avoine et al. 2005] G. Avoine and P. Oechslin. A scalable and provably secure hash-based RFID protocol. In *PERSEC'05*, pp. 110-114. IEEE Press, 2005.
- [Balanis 1997] C.A. Balanis. Antenna Theory: analysis and design. *John Wiley and Sons*, 1997.
- [Bono et al. 2005] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin and M. Szydlo. Security Analysis of a Cryptographically-Enabled RFID device. In *USENIX Security 2005*. To appear. Available at <http://rfdanalysis.org>
- [Feldhofer et al. 2004] M. Feldhofer, S. Dominikus and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *Proc. of CHES'04*, LNCS 3156, pp. 357-370, 2004.
- [Food and Drug Administration 2004] Food and Drug Administration. Combating counterfeit drugs. *Tech. Rep. US Department of Health and Human Services*, Rockville, MD, February 2004.
- [Golle et al. 2004] P. Golle, M. Jakobsson, A. Juels and P. Syverson. Universal Re-encryption for Mixnets, RSA-CT 04, pp. 163-178, 2004.
- [Henrici et al. 2004] D. Henrici and P. Müller. Hash-based enhancement of Location Privacy for radio-Frequency Identification Devices using Varying Identifiers. In *Pervasive Computing and Communications (PerCom) 2004*, IEEE Computer Society, pp. 149-153.
- [ISO 18185-4] ISO 18185-4, available at <http://www.iso.org>, 2007.
- [ITU 2005] ITU page on definition of ISM bands. <http://www.itu.int/ITU-R/terrestrial/faq/index.html>, 2005.
- [Juels et al. 2004c] A. Juels and J. Brainard. Soft Blocking: Flexible blocker tags on the cheap. In *WPES'04*, pp. 1-7. ACM Press 2004.
- [Juels et al. 2003a] A. Juels and R. Pappu. Squealing Euros: Privacy Protection in RFID-enabled banknotes. In *Financial Cryptography (2003)*, vol. 2742 Lecture Notes in Computer Science, pp. 103-121.
- [Juels et al. 2003b] A. Juels, R. Rivest and M. Szydlo. The Blocker Tag: Selective blocking of RFID tags for consumer privacy. In *Computer and Communication Security (2003)*, ACM Press, pp. 103-111.

- [Juels et al. 2005] A. Juels and S. Weis. Authenticating Pervasive devices with human Protocols. In *CRYPTO 2005*, pp. 293-308.
- [Jung et al. 2005] M. Jung, H. Fiedler and R. Lerch. 8-bit microcontroller systems with area efficient AES coprocessor for transponder applications. In *Ecrypt workshop on RFID and Lightweight Crypto*, 2005
- [Kinoshita et al. 2005] S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri and A. Kanai. Privacy Enhanced Active RFID Tag. *1st International Workshop on exploiting context histories in smart environments*, 2005.
- [Mandel et al. 2004] J. Mandel, A. Roach and K. Winstein. MIT Proximity Card Vulnerabilities. *Tech. Rep. Massachusetts Institute of Technology*, March 2004.
- [mCloak 2005] mCloak for RFID tags. Available at <http://www.mobile-cloak.com/rfidtag/rfid.tag.html>, 2005.
- [Molnar et al. 2005] D. Molnar, A. Soppera and D. Wagner. A scalable, delegatable, pseudonym protocol enabling ownership transfer of RFID tags. In *Ecrypt Workshop on RFID and Lightweight Crypto*, 2005.
- [Molnar et al. 2004] D. Molnar and D. Wagner. Privacy and Security in Library RFID: Issues, Practices and Architectures. In *Computer and Communications Security (2004)*, B. Pfizmann and P. McDaniel Eds. ACM, pp. 210-219.
- [NIST RFID Security 2007] NIST Guidelines for RFID security. Available at http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf, 2007.
- [Ohkubo et al. 2004] M. Ohkubo, K. Suzuki and S. Kinoshita. Efficient Hash-Chain based RFID Privacy Protection Scheme. In *Ubiquitous Computing (UBICOMP)* September 2004.
- [Peris-Lopez et al.] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador and A. Ribagorda. RFID Systems: A survey on security threats and proposed solutions. Available at <http://lasecwww.epfl.ch/gavoine/rfid/>.
- [Sarma et al. 2002] S. Sarma, S. Weis and D. Engels. RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems (2002)*, vol. 2523, Lecture Notes in Computer Science, pp. 454-470.
- [Savi website] Information available at <http://www.savi.com>.
- [Smart and Secure Tradelanes 2003] Smart and Secure Tradelanes. White paper. Available at: http://www.savi.com/products/casestudies/wp.sst_initiative.pdf, May 2003.
- [Sybase website] Available at: <http://www.ianywhere.com>
- [US Customs] US Customs and Border Protection. Container Security Initiative. Available at: http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml.
- [US C-TPAT] US Customs and Border Protection. Customs-Trade Partnership Against Terrorism (C-TPAT). Information available at: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/.

- [Verichip 2005] VERICHIP. Website. <http://www.4verichip.com>, 2005.
- [Weis et al. 2004] S. Weis, S. Sarma, R. Rivest and D. Engels. Security and Privacy Aspects of low-cost Radio Frequency Identification Systems, In *Security in Pervasive Computing* (2004), vol. 2802 Lecture Notes in Computer Science, pp. 201-212.
- [World Customs Organization 2005] World Customs Organization. Framework of Standards to Secure and Facilitate Global Trade. Available at [http://www.wcoomd.org/ie/En/Press/Cadre de Normes GB_Version Juin 2005.pdf](http://www.wcoomd.org/ie/En/Press/Cadre%20de%20Normes%20GB_Version%20Juin%202005.pdf), June 2005.
- [Yamada et al. 2005] I. Yamada, S. Shiotsu, A. Itasaki, S. Inano, K. Yasaki and M. Take-naka. Secure Active RFID Tag System. *Proc. of Ubicomp 2005 Workshop*.