An RFID-based Track-and-trace Anti-counterfeiting System

S.H. Choi and C.H. Poon

***Abstract*—RFID facilitates processing of product information, making it a promising technology for anti-counterfeiting. A number of RFID anti-counterfeiting mechanisms have recently been proposed. This paper first compares the strengths and weaknesses of these mechanisms, and evaluates possible impacts of threats to RFID. Subsequently, a track-and-trace anti-counterfeiting system using RFID is proposed. The proposed system is aimed at relatively high-end consumer products, and it helps protect genuine products by maintaining the product pedigree and the supply chain integrity. As such, consumers can safeguard their stake by authenticating a product with RFID readers before making payment. The mechanism is relatively simple and easy to implement.**

***Index Terms*—RFID, anti-counterfeiting, track and trace, security analysis**

I. Introduction

Counterfeiting is generally considered one of the greatest threats to the world economy. In 2006, it was estimated that counterfeit goods account for 5% of the world trade, totalling US$250 each year, and that over the past ten years counterfeiting has destroyed 120,000 jobs each year in the United States, and 100,000 in Europe [1].

The Radio Frequency Identification (RFID) technology is a method of unique items identification using radio waves, typically a reader communicates with tags that hold digital information in microchips [2]. RFID has emerged as a promising tool to combat counterfeiting because it complements the common anti-counterfeiting measures, such as holograms, colour shifting inks, taggants, fingerprints, and chemical markers [3], which do not avail automatic verification of product authenticity.

Several RFID anti-counterfeiting solutions have been proposed in recent years, which would be discussed in details in section III. While these solutions have not yet been implemented in practice, the United States Food and Drug Administration (FDA) has passed the Prescription Drug Marketing Act (PDMA) in 1999, which requires pharmaceutical wholesalers to track and trace the drugs they distribute. Drug wholesalers are required to supply a "pedigree" in either paper or electronic form which records every entity that has handled the drug since its manufacturing. FDA recommended RFID [4] [5] for such purposes.

However, there are doubts about the security level that RFID can provide in such applications [6]. Thompson et al. proposed a STRIDE model that categorizes different RFID threats [7], while Rieback et al. presented a self-replicating RFID virus that infects back-end RFID systems [8].

This paper reviews these threats and analyses how they may affect the security of RFID applications in anti-counterfeiting. Subsequently, a track-and-trace system using RFID technologies is proposed for anti-counterfeiting.

II. Threats to RFID

A. *Spoofing*

Spoofing is cloning of RFID tags by copying the information of one tag to another. This threatens RFID systems by creating a copy of the supposed-to-be unique, authentic RFID tags. With RFID now being deployed in various areas, such as access control to homes, offices and vehicles, or electronic payment, victims could include any users of such services [6]. Researchers at Johns Hopkins University and RSA Security demonstrated how the security of the car immobilizers of 2005 model Fords could be tampered with, and that the electronic payment systems of Exxon-Mobil SpeedPass^{TM} could be compromised by cloning the Digital Signature Transponders (DST) manufactured by Texas Instruments [9].

B. *Tampering with data*

It refers to a situation when an adversary modifies, adds, deletes, or reorders data in RFID tags. Tampered tags may disrupt the normal operations of the backend system.

C. *Replay attacks*

Although the holder of an RFID tag may expect that any readers out of the normal operation range (typically 10cm for Gen 2 tags) cannot retrieve any information from the tag, Kfir et. al. demonstrated that by placing a "ghost" between a reader and a tag, the communication range can be much farther away [10]. This leads to a false perception of safety. A challenge-response type authentication could be a solution to the problem. However, stronger public key cryptography means more expensive tags [11].

D. *Repudiation*

Repudiation may result when there is not evidence to prove that a user has actually performed a certain action [7]. Tracking the actions of individual players throughout the supply chain is vital for maintaining the visibility and integrity of the supply chain, which is in turn important in reducing counterfeit gray market distribution [12].

S.H. Choi is with the Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong (email: shchoi@hku.hk)
C.H. Poon is with the Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong (email: ekmanson@hku.hk)

E. *Information disclosure (sniffing)*

Sniffing occurs when RFID tags are read without the knowledge of the tag bearer, therefore leaking information to unauthorized users [7] [8]. This does not only destroy the integrity of the supply chain, but also infringe consumers' privacy.

F. *Denial of service*

Denial of Service (DoS) occurs when an RFID system cannot function properly to provide normal services to valid users; it is a common threat to internet server systems. Service of an RFID system may be denied by "signal jamming", where the communication between a tag and a reader is clouded or is shielded by a Faraday Cage, which can prevent tags from being read properly. An adversary may also jam the system by generating a return signal stronger than the authentic one to make it unavailable to valid users.

G. *Elevation of privilege*

This occurs when an adversary gains higher privileges in an RFID system than the authorized level. Although the adversary may not disrupt the system operations directly, he may implement some malicious software in the system thus spread virus through RFID tags.

H. *RFID Virus*

Rieback et al. designed an RFID virus that self-replicates, which requires only one virus tag as the initiator. The affected systems run SQL injection codes unintentionally. The codes do not only affect the back-end system, but also spread the virus upon further communications [8]. Although it does not possess propagation capabilities of common computer virus, it poses a substantial threat to the "trusted entities" within a corporate RFID system.

III. RFID IN ANTI-COUNTERFEITING

RFID has gained popularity of being an anti-counterfeiting technology in recent years. It has an obvious advantage over other existing anti-counterfeiting technologies that it enables efficient and automated product verification. In such a way, massive checks can be performed at pallet or even item level for product originality verification. Based on this distinct advantage, the following several schemes have been proposed for deploying RFID in anti-counterfeiting.

A. *Numeric Tokens*

Johnston proposed a "Call-in the Numeric Token" (CNT) technique [13]. This technique is relatively low-tech and low-cost, but requires customer participation in authenticating the products they purchase via the phone or the internet. A random, unique and unpredictable identity number, which is a virtual tag or token, is assigned to each product at item level. The anti-counterfeiting mechanism relies on the difficulties in guessing the valid identify numbers. By setting an appropriate threshold, any items with a high-enough instance of query for validation would be deemed counterfeit.

Although the identity numbers can be printed on the packaging materials of the product item, it would enable the supply chain partners to automate the call-in validation process if these numbers are recorded in RFID tags.

1) *Security Analysis*

Theoretically spoofing is not a threat under this solution, since the CNT technique relies on difficult-to-guess random tokens to make cloning of tags difficult. However, it might give false negative results. Therefore, by carefully controlling the number of counterfeit tags cloned from each genuine tag, an adversary might avoid triggering the call-in system.

Assume that tags without authentication mechanisms are used in the CNT system, both tampering and spoofing would become easy. However, because of random tokens, tag tampering would easily make the tags invalid. This could still be a security hole to the supply chain partners who use automated systems to validate tags because the tampered tags may disrupt their normal operations.

As the CNT system does not rely on the movement history of products, repudiation does not pose a threat. However, this may leave genuine tags unprotected, because if a genuine tag token was sniffed and queried for many times, the real tag would become an counterfeit and there would be no way to prove its authenticity, causing loses to genuine product owners.

The CNT technique poses least requirements on the back-end server operations. Therefore, it is less susceptible to the DoS and elevation of privilege attacks, as well as the RFID virus. Virus writers may turn to infect local systems of those using automated systems to scan the tokens for batch call-in verification. However, this would become less beneficial since individual local systems tend to be different from each other, rendering them ineffective channels to spread RFID virus.

B. *Strengthened EPC Tags for secure authentication*

The Electronic Product Code (EPC) is a global unique identification service for physical objects [14]. In 2005, EPCglobal, a non-profit making organization that aims to increase visibility and efficiency throughout supply chains, developed the global standards of the EPC Network. It ratified the EPC Class-1 Generation 2 UHF standard, which is expected to be used by most companies in the near future. Commonly known as "Gen 2", this standard defines the physical and logical requirements for a RFID system operating in the 860 MHz - 960 MHz frequency range [15] [16].

As the Gen 2 standard was developed with little considerations on security and privacy issues [17], Juels proposed a model to strengthen the EPC tags against cloning attacks [18]. The primary assumption is that Gen 2 tags can reliably authenticate product items if they are unique. In the Gen 2 standard, a 32-bit kill PIN is used to make a tag permanently inoperable; Juels proposed another 32-bit access PIN, which is optional in the Gen 2 standard, for permitting a certain tag commands. Authentication is done by a fix-value mutual-authentication protocol, where the access PIN serves to authenticate the reader, while the kill PIN authenticates the tag. Under this scheme, readers are assumed trustworthy.

However, Duc et al. thought that Juel's solution does not take into account sniffing threat and privacy issues. They proposed another solution that includes security features of authentication, traffic encryption, and privacy protection [17]. Their scheme employs Gen 2 compliant cryptographic features like Pseudo-random Number Generator (PRNG) and Cyclic Redundancy Code (CRC). The scheme makes use of the PRNG to generate a new session key to encrypt each session of tag-to-reader communication, rendering sniffing impossible, while tag authentication is done by the PIN features described in the Gen 2 standard. Since a tag emits a different bit string in each and every session (because of the new session key), even a compatible reader would not be able to track the tag holders' activities for a time longer than the session period.

1) *Security Analysis*

The primary motivation for developing cryptography for RFID tags is cloning resistance [19]. When there is such an authentication protocol to prevent cloning, it can also protect tags from tampering, sniffing, virus and replay attacks.

"Secure" tags are obviously beneficial to product stakeholders, as well as to the society as a whole. However, product stakeholders never know when adversaries would actually succeed in cracking the system, nor to what extent they would crack it. Therefore, it would be risky to rely solely on the uniqueness of a tag to perform anti-counterfeiting functions, especially in areas of life-threatening consumer products (e.g. pharmaceutical products).

When an RFID tag, and thus the product it attaches to, is assumed unique and secure, efforts can be saved in tracking the product's movements through the supply chain. However, repudiation may become more likely since the product's status is not monitored by the central anti-counterfeiting system throughout its lifespan in the supply chain.

All the secure tag solutions mentioned above rely on a central server for the authentication process. For efficiency purposes, a distributed server infrastructure can be used to reduce reliance on a single server. However, it opens up more penetration points for DoS or privilege elevation attacks.

C. *The Track-and-Trace Approach*

Koh et al. proposed a scheme to track and trace products through a supply chain, utilizing the EPC infrastructure [20]. Under this scheme, pallets or cartons are each embedded with an RFID tag that contains an EPC number. The EPC number serves as a pointer to specific product information which may be queried through an Object Name Server (ONS) accessible through the Internet. As the product moves through the supply chain, each node in the supply chain updates the product pedigree information to the central repository. Therefore, the central repository database would contain complete information on the trail of exchange of a product, which includes origin, destination, timestamp, company names, etc. In such a way, a product can be tracked and traced with a complete product pedigree as it moves from the manufacturer to retailers.

However, Staake et al. thought that Koh's solution is adequate only for some products [21]. They argued that RFID tags, which store the EPC numbers in plaintext can be easily cloned, and the products cannot be sufficiently authenticated. When a counterfeiter does not update the central repository, nor the customer registers the deal, the counterfeit product may still give an incomplete but plausible history. There may also be other reasons that the central repository may not be updated correctly. Therefore, they suggested extending the EPC Network by adding an EPC Product Authentication Service (EPC-PAS) to allow a secure product authentication in a database-reader-tag environment. A cryptographic unit (CU) is placed behind an RFID reader, therefore it does not raise new requirements on reader devices. However, RFID tags that support this kind of cryptography are not only more expensive than normal tags [11], such secure functionalities do not comply with the EPC Gen 2 standard.

Therefore, Kim et al. proposed another model that authenticates products in mobile RFID environment, utilizing watermarking technologies. It aims at addressing the Gen 2 compatibility problem of Staake's model, as well as the problem of readers' trust level of Juel's model [22] [23]. With digital camera cell phones embedded with RFID devices to come in the near future [2], it may be feasible to require a consumer to scan the product EPC and capture the watermark-embedded image on the product, and then send them over the GSM or CDMA network to the EPC-PAS for authentication. Then it returns a digital certificate with digital signature that states the authentication results.

1) *Security Analysis*

The primary benefit of the track-and-trace approach is that it does not rely on clone resistance of RFID tags. Assuming that the readers and the partners along the supply chain are all trustworthy, consumers are protected without any involvement in the anti-counterfeiting mechanism, merely by relying on the credit of the retailers (and of their hardware) for checking the product authenticity. To the manufacturers, this approach best protects their interests, as genuine products will not be deemed counterfeits because of the existence of other counterfeit items.

However, a lack of authentication mechanism between the tags and the reader or the back-end server tends to render tampering or RFID virus attacks more likely. With the standardized EPC structure, it would become easier for a virus to spread around.

Replay and sniffing attacks would be the primary source of problems that lead to intense debates over privacy issues of RFID, which is the primary concern of a lot of consumers' rights groups. Tags without a secure authentication mechanism can practically communicate with any readers, regardless of their trustworthiness. Unencrypted communication between tags and readers may also be sniffed by an adversary. Although leakage of sensitive information could possibly be used to produce counterfeit tags or readers, this is considered impractical in the protected supply chain environment because the adversary devices have to be close enough to the genuine readers and tags [19]. Therefore, this is more of a privacy concern to the end consumers.

The track-and-trace approach is resistant towards repudiation attacks because all movements of products and actions of supply chain partners are tracked by the central sever. A customer may simply refuse to purchase products without a pedigree, or those with a suspicious pedigree. This approach relies on the ONS to retrieve pedigree information. The common weaknesses of Doman Name Servers (DNS) of the internet directly transfer to ONS, because of their similarity in functionalities [24]. As a highly exposed service, the ONS becomes the primary targets of DoS or privilege attacks.

IV. The Proposed System

A. Overview

A number of anti-counterfeiting systems adopting various algorithms and mechanisms have been proposed. These systems perform universal functions for virtually all kinds of products. They are generally large in scale with complex functionalities. However, they are not without shortcomings: 1. The larger the scale they are, the more the points of penetration vulnerable to attacks; 2. The complex functionalities force host companies to adapt to redundant functionalities that do not suit the company needs; 3. The universal system mandates the disclosure of product information to third parties.

To address these problems, this paper proposes an anti-counterfeiting system aimed to provide a product pedigree which supply chain partners and end consumers can both access. The anti-counterfeiting mechanism is based on the track-and-trace approach, as mentioned in section III(C), with an extra feature that enables end consumers to verify the products through their own mobile phones.

The system requires various partners along the supply chain to record product transactions using RFID technologies. As such, the integrity of the supply chain is maintained by forming a chain of custody from the product transaction records stored in a central database. All the supply chain partners are expected to verify the incoming products and reject those with a suspicious pedigree, while consumers can verify a product before they make payment with a handheld RFID device, which is expected to be embedded into the mobile cell phones in the foreseeable future; if there is not any valid pedigree or the pedigree is deemed suspicious, the payment should be halted.

The system primarily targets at high-end consumer products, such as apparels, handbags, purses, etc. The RFID hardware costs are relatively low compared to the value of these products, and hence the system implementation cost will be justifiable. More importantly, the high values of these products provide enough incentives for end consumers to verify them before making payment.

B. System Design

1) The anti-counterfeiting mechanism

The proposed system performs anti-counterfeiting by maintaining supply chain integrity, the significance of which is twofold. Firstly, the path of transaction of a product is clear and its source can be traced accordingly; secondly, product authenticity can be validated.

The pedigree of a product is generated by its transaction records along the supply chain, which may be retrieved from the host company server through RFID readers and the internet. With the growing popularity of internet connection through phone networks and RFID enabled cell phones coming into market place, the system allows consumers to check the pedigrees of the products they are purchasing.

This mechanism hinders counterfeiters from cloning the products or the tags because of three reasons: 1. companies have to pre-register before they can access the host company server to record product transactions, and thus excluding counterfeiters from attempting to do so; 2. suspicious transactions would be screened out accordingly; 3. consumers will refuse to purchase products without a plausible history.

To customers, making sure that the products are genuine protects their own safety and guarantees value for money. There are indeed sufficient incentives for them to verify product authenticity, given a convenient-enough way to do so. Similarly, since products without a plausible history may not be saleable to end-users or the next carrier, the current carriers have a stake in recording transactions. In anticipation of the enhanced customer confidence, it would be justifiable for the product producer to host the system. The product producer, who is also the hosting company, is also responsible for tracking suspicious transactions, and tracing through the sources of security breaches in the various supply chains as the product items move along.

2) System architecture

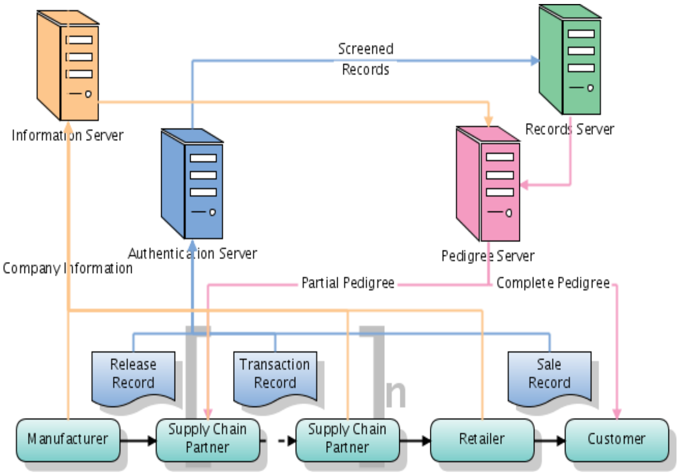

Fig.1 System Architecture

There are four different servers in the system, as shown in Fig.1. They perform different functions in the anti-counterfeiting system. Three of them are front-end servers that contact with the external parties while the remaining one is a back-end server that is accessible from the other three servers only, and it is responsible for storing the transaction records. The functions of each server are described as follow.

The Information Server is responsible for collecting company information from the supply chain partners. The information is crucial for the product pedigrees because they form the geographical picture of the product history, and it also forms the basis for tracing problems when suspected counterfeits emerge. The information should be pre-registered by the supply chain partners and verified by the host company before the first transaction record was sent to the Authentication Server.

As the products move along the supply chain, each supply chain partner should record each transaction accordingly. The products are identified by the embedded RFID tags, which contain a unique tag ID, and they can be read by the RFID readers installed at the partners' site. They are supposed to be connected to the internet through a PC. The tag ID forms the basis of a transaction record, which is sent to the Authentication Server. The Authentication Server verifies the transaction records and screens out suspicious activities. The screened records are then sent to the Record Server for storage purposes.

The supply chain partners can verify the partial product pedigree from the point of manufacturing to the previous owner by making requests to the Pedigree Server, which in turn retrieves transaction records from the Records Server as well as company information from the Information Server to generate the required pedigree. They should reject any products with a suspicious partial pedigree.

The Pedigree Server is also responsible for generating complete product pedigrees to end consumers for verification, which are sent through the internet and the mobile phone network. When a customer is satisfied that a product is genuine and pays for it, the retailer should generate a sale record, which is subsequently sent to the Authentication Server. Any further transactions of the same product after the sale record shall be deemed suspicious.

The server architecture is divided according to the various system functions. The Records Server, which stores the transaction records, is classified as a back-end server; it should be protected from public connection for enhanced security, because the records it stores form the backbone of the product pedigrees. Such division of work allows a smaller workload and hence quicker responsiveness of each server. More importantly, in case of exceptional events, the failure of the Authentication Server would only affect the transaction operations along the supply chain, but not the product sales at the retailing shops.

C. System Operation

1) The product flow

As the products move along the supply chain, the system operations are detailed as follow.

a) Manufacturers

For both in-house and third-party manufacturers, they are required to generate a Release Record to the Authentication Server before their products can be transferred to the next owner. The Release Record contains the tag ID, the product type, the timestamp of release, as well as the "Chain Level", which is set to 1 in the Release Record. Its use will be explained in the next section.

The manufacturers also pre-register its company information to the Information Server. The pre-registered information includes the company title, its location, and the product types that they are manufacturing.

This is the first record of the product pedigree. The Release Record serves the purpose of certifying the root source of the product item, which assures the following owners in the supply chain that they are receiving genuine products from the right manufacturer.

b) Supply Chain Partners

Upon receiving the product, the supply chain partners should request the partial product pedigree which records the transactions of the item since it was released from the manufacturers. They should only receive products with a plausible history. For suspicious products, they should reject or return to the previous owner, and report to the host company.

The product pedigree must satisfy the following conditions so that a product is considered genuine.

1. *There exists a record of release for the product*
2. *There exists no record of sales for that product*
3. *The recorded previous owner is the party that is selling the product*

After verifying and accepting the product items, the company continues to process the items for value-adding activities. Before the items leave the company, they will have to go through the RFID reader again. There are two jobs for the reader. Firstly, it reads the Chain of Level information (k) from the tag, do an increment (k+1) and then rewrites it back. Secondly, the reader reads the Product ID (Tag ID) for each product, and together with the Partner ID, the timestamp, and the new Chain Level (k+1), to form a pedigree entry for each item which is sent to the Authentication Server. The pedigree entries from the supply chain partners accumulate to form the complete product pedigree.

c) Retailer

Upon receiving the products, the retailer should verify the product pedigrees in the same way described above. The retailer holds a stake on so doing because when the end consumers find what they have purchased is a counterfeit, its goodwill and reputation would be damaged.

When the end consumer pays for a product, the retailer should update the chain level information in the tag by 1 (from n-1 to n), and mark it "sold". The Product ID (Tag ID), the Retailer ID, the timestamp of sale and together with the updated chain level (n), they form the sale record which is sent to the Authentication Server. Any further sale attempts or transactions of supposed-to-be-sold products are deemed suspicious.

d) End Consumer

In order to protect their own stake, the customers should verify the pedigrees of the products they want to purchase before making the payment. This can be done by reading the Product ID (Tag ID) through a handheld RFID device. With RFID-enabled mobile phones are coming to the market [2], and improved internet connectivity for the mobile networks, this method has the potential to be popular in the foreseeable future.

The verification criteria are similar to the above. This allows the customers to verify the product pedigrees by themselves, instead of relying on the retailers.

2) The Authentication Server

The Release Record, all the Transaction Records as well as the Sales Record must go through the Authentication Server. Therefore, by interacting with the Information Server and the Records Server, the Authentication Server performs an important function in spotting suspicious transactions. It verifies the Transaction Records going through it by spotting for the following items:

1. *Duplicate sales record / transactions after sale*
2. *Duplicate transaction records at the same chain level*
3. *Unreasonable transfer of ownership*

It is not necessary for the Authentication Server to carry out a certain set of activities or to give immediate response on all suspicious activities. Rather, different thresholds can be set for different products for different companies. Based on this information, the host company can set a certain course of actions to different situations according to their own needs.

V. Conclusion

RFID brings huge potential in enhancing the supply chain efficiency. When mass authentication at item levels becomes possible, the cost of maintaining the integrity of supply chains would be significantly reduced. Although RFID is subject to a number of threats and it cannot provide perfect security, it is now technically feasible and financially justifiable to integrate RFID with the internet for anti-counterfeiting, particularly with customer participation in the automatic product authenticity verification process.

The proposed RFID-based anti-counterfeiting system utilizes the track-and-trace approach. It requires the supply chain partners to record all the transactions of a product along the supply chain, which forms a pedigree for the product. Consumers can verify the product authenticity at sale points. This proposed system is characterized by customer participation in the product authenticity verification. Indeed, consumer power provides the ultimate source of incentives for the supply chain partners to maintain the supply chain integrity.

The proposed system is also simple in architecture. It does not require much sophisticated technologies, making it relatively easy to implement. Such a simple structure and hardware requirement makes it cost-effective for companies to host the system. The system can be tailored to suit specific needs of individual companies, saving money on unnecessary functions. In particular, the product pedigrees stored in the system facilitates real-time tracking of problems and further investigations into suspicious activities. As such, a company can afford to host an anti-counterfeiting system without the need to disclosure sensitive information to any third parties.

References

[1] International Chamber of Commerce Commercial Crime Services, International Guide to IP Rights Enforcement First Edition 2006. 2006, International Chamber of Commerce Counterfeiting Intelligence Bureau.

[2] RFID Journal. Nokia Unveils RFID Phone Reader. 2004 [cited 2006; Available from: http://www.rfidjournal.com/article/articleview/834/1/13/.

[3] United States Food and Drug Administration, COMBATING COUNTERFEIT DRUGS - A Report of the Food and Drug Administration. 2004, U.S. Food and Drug Administration: Rockville, Maryland 20857.

[4] Editors, FDA Will Begin Enforcing Anti-Counterfeiting Law In December, in Medical News Today. 2006.

[5] United States Food and Drug Administration, COMPLIANCE POLICY GUIDE 160.900 Prescription Drug Marketing Act – Pedigree Requirements under 21 CFR Part 203. 2006.

[6] Sparkes, M., Gambling on chips, in IET Manufacturing Engineer. 2006. p. 10-11.

[7] Thompson, D.R., N. Chaudhry, and C.W. Thompson, RFID security threat model, in Conference on Applied Research in Information Technology. 2006: Conway, Arkansas.

[8] Rieback, M.R., B. Crispo, and A.S. Tanenbaum. Is Your Cat Infected with a Computer Virus? in Fourth IEEE International Conference on Pervasive Computing and Communications 2006.

[9] Bono, S.C., et al. Security Analysis of a Cryptographically-Enabled RFID Device. in 14th USENIX Security Symposium. 2005. Baltimore, Maryland, USA: USENIX Association.

[10] Kfir, Z. and A. Wool. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems. in 1st International Conference on Security and Privacy for Emerging Aeas in Communication Networks. 2005.

[11] Sarma, S.E., S.A. Weis, and D.W. Engels. RFId Systems and Security and Privacy Implications. in Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS 2523. 2003. Springer-Verlag Berlin.

[12] TransportGistics, I. SUPPLY CHAIN INTEGRITY, A Basis to Upset Gray Market Distribution. 2004 [cited 2006/02/10]; Available from: http://www.insourceaudit.com/WhitePapers/supply_chain_integrity.asp.

[13] Johnston, R.G., Ph.D., CPP, An Anti-Counterfeiting Strategy Using Numeric Tokens. International Journal of Pharmaceutical Medicine 2005. 19(3): p. 163-171.

[14] Brock, D.L., White Paper: The Electronic Product Code (EPC). A Naming Scheme for Physical Objects 2001, Auto-ID Labs, Massachusetts Institute of Technology.

[15] EPCglobal Inc., Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9: "Gen 2". 2005.

[16] EPCglobal Inc. EPCglobal Homepage. 2006 [cited 2006/12/17]; Available from: http://www.epcglobalinc.org/home.

[17] Duc, D.N., et al. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. in The 2006 Symposium on Cryptography and Information Security. 2006. Hiroshima, Japan.

[18] Juels, A. Strengthening EPC Tags Against Cloning. in ACM Workshop on Wireless Security (WiSe). 2005.

[19] Lehtonen, M., et al., From Identification to Authentication – A Review of RFID Product Authentication Techniques, in Workshop on RFID Security 2006. 2006, Institute for Applied Information Processing and Communications, Graz University of Technology: Graz.

[20] Koh, R., et al., White Paper: Securing the Pharmaceutical Supply Chain. 2003, AUTO-ID CENTER, Massachusetts Institute of Technology.

[21] Staake, T., F. Thiesse, and E. Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. in ACM Symposium on Applied Computing. 2005. Santa Fe, New Mexico.

[22] Kim, J. and H. Kim. Anti-Counterfeiting Solution Employing Mobile RFID Environment. in TRANSACTIONS ON ENGINEERING, COMPUTING AND TECHNOLOGY. 2005. Budapest, Hungary.

[23] Kim, J. and H. Kim. A Wireless Service for Product Authentication in mobile RFId environment. in 1st International Symposium on Wireless Pervasive Computing, 2006. 2006.

[24] Fabian, B., O. Günther, and S. Spiekermann., Security Analysis of the Object Name Service for RFID. Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2005.