Security Challenges for User-Oriented RFID Applications within the 'Internet of Things'

G.P. HANCKE, K. MARKANTONAKIS and K.E. MAYES
ISG Smart Card Centre
Royal Holloway, University of London
UNITED KINGDOM
{gerhard.hancke, k.markantonakis, keith.mayes}@rhul.ac.uk

Abstract

In this article, we examine the role played by RFID in enabling user-oriented networked applications. We explain why RFID is seen to be an important building block of the 'Internet of Things' and examine how RFID, assisted by the deployment of NFC devices, is increasingly facilitating user-oriented, Internet-based application architectures. Finally, we look at the high-level security challenges that these user-oriented application architectures will need to address.

Keywords: RFID, NFC, security, 'Internet of Things', user-oriented architecture

1 Introduction

Radio Frequency Identification (RFID) is a technology that is being increasingly integrated into aspects of everyday life. RFID is often associated only with item 'tags' but is actually a collective term given to a number of technologies. A collection of mature standards and proprietary system specifications govern system operation and the variety of systems available allows RFID to be tailored to many applications. Electronic Product Code (EPC) tokens, contactless credit cards, e-passports and access control are just a few examples of systems that use variants of this technology.

The 'Internet of Things' is a vision of a ubiquitous Internet where everyday physical objects are integrated into information networks. The 'Internet of Things' requires objects to have a unique identity, which would make them addressable within the network when processing information. Such objects must also have the capability to communicate, even in environments where fixed network access infrastructure is weak or non-existent. RFID technology is therefore seen as a candidate building block for the 'Internet of Things', being able to assign a unique identifier to an object and operate in an ad-hoc environment.

In general, RFID has been deployed in controlled, 'closed', systems for very specific purposes and where only selected entities have access to the system information. If this continues to be the case, RFID tagging potentially offers little benefit once the item passes into the hands of the end user. There is an opinion that if users could exert more control over RFIDs and the associated data, they would use this purely to increase their personal privacy and thereby reduce functionality. However, users may become more comfortable with the technology and actively contribute to the 'Internet of Things' by labelling objects and linking these objects to data entries or applications. There are already cases where this approach is employed [14][15] and user-oriented applications are also expected to experience growth on the back of increased deployment of Near Field Communication (NFC) devices. NFC facilitates ad-hoc communication between a user's personal device such as a mobile phone or PDA and the RFID tagged objects.

Successful deployment of intelligent RFID-enabled Internet applications depends on strong technical or operational security and privacy solutions being in place. We discuss briefly the high-level system security aspects, which are in our opinion the main challenges that would need to be addressed for user-oriented RFID applications to be deployed: Privacy, ownership, data integrity, application integrity and standardisation.

2 RFID Technology

Even though recent times have seen a rapid increase in the deployment and research of RFID applications it is not a new technology. The concept of RFID has been around since the early 1940s when IFF (Identification Friend or Foe) transponders actively modulated the radiated ground radar signals to identify airplanes. The first patents that resembled modern RFID devices were filed in the 1970s and the basic communication principles first

demonstrated during this time is still used by RFID tokens today. In the late 1980s, RFID gained widespread acceptance in automated toll collection and access control systems, which was followed by implementation in public transport payment systems and the first serious attempts at standardisation in the 1990s. In 1999 it was first proposed that low-cost RFID `tags' could be used to track individual items in supply chains. Currently the use of Electronic Product Code (EPC) tokens for tracking at the pallet, case and item level is probably one of the most prominent RFID applications. RFID technology is, however, also used on a large scale in other applications such as machine readable travel documents (e.g. e-passports), ticketing, access control and payment [1,2,3].

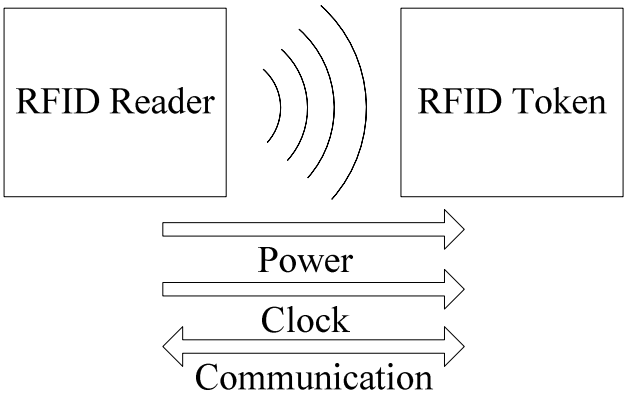

Figure1: Basic Passive RFID system

It should be clear by now that RFID is a collective term that covers a number of different systems. These systems can differ in a number of ways with regards to operating parameters, such as the range between the reader device and the tag (10 cm – 10 m), data rates (1.65 kbit/s – 424 kbit/s) and radio frequency (Low Frequency (LF), High Frequency (HF) or Ultra-high frequency UHF). Some RFID tokens can also be active, in other words they contain their own power source, but in most systems the tokens are passive and need to be powered by an external source. The basic operation of a passive RFID system is shown in Figure 1. The RFID reader transmits an RF carrier from which the passive token derives its power and system clock. The bi-directional communication between the token and reader is also modulated onto this RF carrier transmitted by the reader. Even thought the token is not actively transmitting it can influence the amplitude of the transmitted reader carrier by means of 'load modulation' or 'modulated backscatter', thereby effectively modulating the carrier with its response.

As RFID technology encompasses a range of systems from multiple vendors, several standards have been defined to encourage interoperability. The standards define, amongst other things, the RF interface, the initialisation sequence and the data format. In the HF radio band there are three main standards by ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) that deal with RFID technology operating at 13.56 MHz i.e. ISO 14443 [5], ISO 15693 [6] and ISO 18092 [8]. ISO 14443 is commonly used in systems requiring logic and µ-controller tokens at distances up to 10 cm. This means that the standard is a common choice for 'contactless smart cards' used for e-passports, credit cards and access control systems. ISO 15693 is most often implemented in systems requiring simple logic or memory only tokens for tracking or identification at a range up to 1 m. Due to the extended operating range the tokens are subject to power restrictions and therefore cannot offer the same functionality as contactless smart cards. ISO 18092, which is commonly referred to as the NFCIP-1 (Near-Field Communication Interface and Protocol) standard, specifies a near-field RF interface and a transmission protocol for communication between devices. This standard allows for a device, such as a mobile phone or PDA, to interact with RFID applications by acting as a reader, or a passive RFID token, and it can also be used for short range peer-to-peer communication. Devices adhering to ISO 18092 are compatible with ISO 14443 and Sony FeliCa RFID systems, and the NFCIP-2 specification (ISO 21481 [9]) also allows for compatibility with ISO 15693.

In the UHF radio band the EPC Class-1 Generation-2 standard [4] is widely used for tagging objects in supply chain and logistic applications. EPC tokens are simple memory devices containing a Unique Identifier (UID) that was designed specifically as a low-cost method for tagging and identifying individual items. Although the functionality of UHF tokens is constrained when compared to HF tokens, these tokens' main advantage is the extended operating range of up to 10 m. Another standard that should be mentioned is ISO/IEC 18000 [7], which defines alternative RFID communication interfaces for several operating frequencies, with specific emphasis on tokens used for Automatic Identification and Data Capture (AIDC) within supply chain applications. ISO 18000 defines a generic structure for use in item management applications (Part 1), along with air interfaces for operation at less than 135 kHz (Part 2), 13.56 MHz

(Part 3), 2.45 GHz (Part 4), 5.8 GHz (Part 5), 860-930 MHz (Part 6) and 433 MHz (Part 7). The operation of Electronic Product Code (EPC) tokens is incorporated into ISO 18000 Part 6, and Part 3 corresponds closely to ISO 15693.

3 RFID and the 'Internet of Things'

The 'Internet of Things' is a vision of a ubiquitous Internet where everyday physical objects are integrated into information networks. This aims to provide an interconnected infrastructure supporting new and innovative services based on widespread access to contextual information about objects in the physical world [12].

One of the main requirements for the 'Internet of Things' is that objects must have a unique identity, which would make them practically addressable when exchanging information. RFID tokens, such as EPC tokens, have sufficiently long identifiers to allow for unique identities to be assigned to individual items, rather than to groups of items as is currently done with barcodes. RFID tokens are also easy to integrate into many objects as they do not need to be visible or adhere to a specific form factor. RFID technology is therefore seen as a candidate building block for the 'Internet of Things' as it could be used to assign a unique identifier, or label, to any item [10]

The 'Internet of Things' also requires that tagged objects have the capability to function, potentially within an ad-hoc network infrastructure. Passive RFID is a useful technology for enabling ad-hoc interactions, although the fact that it operates as a slave to reader devices, i.e. not capable of standalone peer to peer communications, departs a little from the truly ubiquitous "vision". Initiating communication to RFID tokens is normally quick and may not require human intervention. If a user wishes to initiate communication the process is intuitive, i.e. bring the object in close proximity to a reader (or vice versa). Wireless operation ensures that the object does not need to be oriented perfectly and it also reduces the need for external mechanical parts, which makes the system durable. Passive RFID tokens are also powered by the reader when required to communicate. This is an advantage over short range wireless nodes, which require a constant power source, but as mentioned before this does mean that tags cannot communicate with each other or initiate an action in environments with no additional infrastructure.

RFIDs also rely further on networked systems to provide added functionality. Attempting to store all information about an object in an RFID token may not be practical due to storage and cost limitations. It may also be inadvisable from a data back-up and security standpoint, taking into account that a broken token will result in the record being lost altogether and that current tokens provide only limited security mechanisms for facilitating access control and data integrity. Instead, each token in a networked system could contain partial information, or in the simplest case only an identifier, with links to associated information stored in a network repository [11].

3.1 The User-Oriented Approach

Typically, RFID has been deployed in 'closed' systems. In other words, the entity issuing the tokens was also the entity responsible for interacting with them. For example, in some electronic ticket systems a user purchases the token from the transport operator and in all subsequent transactions, like loading credit or gaining access to transport, the token interacts with the operator's infrastructure. RFID systems in which the entity issuing the token can differ from the entity owning the infrastructure are seen as 'open'. Contactless credit cards are often classified as components of an open system because payment can be made regardless of whether the bank issuing the card is the same as the bank subscribed to by the merchant. In fairness the system is not truly 'open' as the two banks have a prior relationship, enforced further by the network of the credit card operator, e.g. Mastercard or Visa, and the use and creation of tokens are tightly controlled. A similar argument can be made for tracking systems where interconnected manufacturers and suppliers can track shipments and monitor inventory, although the token information is not useful to other parties who cannot access the associated tracking data repositories.

If RFID tagging remains "closed" it potentially offers little benefit once an item passes out of the supply chain and into the hands of the end user. However, if RFID systems evolved towards a more open architecture, then new value added services and functionality could be provided to the end-user. Such services might allow users to exert more control over tokens and the associated data, whether for privacy or functional reasons. Users might also actively contribute to the 'Internet of Things' by labelling objects and linking them to data entries or applications. Such a user-oriented approach could

promote an even more open architecture allowing for multiple entities, including the user, to truly interact with tokens in an ad-hoc and meaningful way.

There are already cases where this user-oriented approach is employed to encourage people to build their own 'Internet of Things'. Services such as *touchatag* [14] and *Violet* [15] allow user to attach actions and meta-data to objects using RFID tokens. Scanning these tokens could trigger a pre-configured event like launching a webpage or initiating a VOIP call. Both services provide client-side software, which controls the RFID reader that serves as the interface for linking tokens to the chosen events. *Touchatag* also allows for the development of custom applications using its software APIs. This allows businesses to quickly develop RFID services, such as loyalty schemes, with a simplified token personalisation process and at a relatively low expense. For example, a *touchatag* 'starters kit' with a reader and ten tokens can be purchased for as little as $39.99, with additional tokens selling for approximately $1 [14].

User-oriented RFID applications are also expected to experience growth on the back of increased deployment of NFC. One of the main goals of NFC is to facilitate ad-hoc communication between the user and tagged objects and the NFC Forum has therefore specified several standards that can enable user-oriented services [16]. The main specification that could enable such services is the NFC Data Exchange Format (NDEF), which defines a common data format for NFC-forum compliant devices and the four types of NFC Forum-compliant RFID tokens. The NFC Record Type Definition (RTD) specifies the format and rules for building standard record types based on the NDEF data format. The RTD specification provides a way to efficiently define record formats for new applications and gives users the opportunity to create their own applications adhering to NFC Forum specifications. Standard RTDs are currently specified for storing text strings in multiple languages, storing Uniform Resource Identifiers (URI) and triggering a specific action (such as starting an application). As an example of how to apply NDEF and RTDs the NFC Forum provides a Smart Poster specification, which defines how to put URLs, SMSs or phone numbers on an NFC token. The Smart Poster RTD builds on the RTD mechanism and NDEF format and uses the URI RTD and Text RTD as building blocks.

NFC will effectively provide anyone with a suitably enabled mobile phone or PDA with a portable RFID reader, which could interact with RFID tokens and also link to networked services. This would eliminate the need for users to obtain special static reader hardware to interact with RFIDs. NFC enabled devices are therefore attractive platforms for third party services, e.g. touchatag already provides a software client for Nokia's 6212 NFC phone that can trigger events on the mobile platform [14].

4 Security Challenges

Public acceptance of a RFID-based 'Internet of Things' depends on strong technical and operational, security and privacy solutions being in place [12]. The security issues surrounding RFID and the challenges of providing security services, to meet the cost and interoperability requirements of the business process, with a resource limited device have been written about extensively in academic, government and industry publications. In this section we discuss only briefly the high-level system security aspects, which include some of the main challenges for the deployment of user-oriented RFID applications. The reader is referred to the following papers for a detailed overview of specific attack scenarios and countermeasures [17][18][19] [20][21].

It is a misconception that the security of a RFID system is only dependent on the security of the token, or the transaction between the token and the reader. In other words, if the token can authenticate entities, regulate access to stored data, encrypt communication and generate cryptographic data integrity checks then it would be simple to construct a secure system. We are not disputing that such a token would greatly contribute to system security but there are other critical system security challenges, which cannot be resolved by the RFID alone.

To illustrate this point we consider a simple use case: *A customer purchases a new refrigerator, labelled with an RFID token, from his local store. The token contains the following data records: A URI to the installation and setup instructions, a URI to an online user-manual, a URI to a service record database and a URI to a local accredited maintenance contractor. The delivery men identify and load the correct package using the token identifier and the shipping manifest is automatically updated when delivered. At the customer's residence*

they install the refrigerator using the instructions pointed to by the RFID label. Upon delivery and installation the user scans the token and is directed to the user manual, and is also prompted to register for his manufacturer's warranty as the service record contains no information about his refrigerator. A year later the refrigerator needs to be serviced so the user reads the token and is put in contact with the maintenance contractor. The maintenance contractor has used the provided identifier to look at the service record and model of refrigerator so he knows what sort of service to perform. Once at the user's residence the contractor finds a malfunctioning part, which he replaces. He updates the online service record accordingly. The customer moves to a new residence and decides to sell the refrigerator to his neighbour.

The use of RFID in this example scenario might not even be justified, as it requires infrequent use and stores no dynamic data, and the interaction with networked applications is limited. However, even in what appears to be an elementary tagging example several important security considerations come to the fore.

4.1 Privacy

In our use case scenario it can be seen that there are a number of people with access to the product tag information. This raises the question of what data is associated with the RFID token and stored by the local store, the manufacturer or even the maintenance and delivery companies; and else who has access to this data? RFID's potential for tracking consumers and the personal information that these tokens might reveal about their owners have often overshadowed the technical advantages [29]. Privacy with regards to location and personal data of the user is obviously a concern that needs to be adequately addressed. Technical improvement can mitigate some privacy concerns, e.g. encryption prevents the eavesdropping of transactions [22], but privacy also requires complementary operational regulation or legislation to be enforced [27]. Policy can take the form of governmental recommendation [13] on privacy and data protection or be short set of operating principles protecting end users, such as Garfinkel's 'RFID Bill of Rights' [30]. One drawback of regulation and legislation promoting best practices could be that while it is effective in discouraging larger entities from illegitimately keeping track of tags owned by customers, business partners or competitors, it does not provide a strong deterrent in a user-oriented domain where one person could read a token to obtain information about another. For example, if a user scanned his neighbour's medicine container and got redirected to a prescription history.

4.2 Ownership

Ownership should define which entity has the authority to control the access rights to the RFID - normally the owner or temporary guardian of the tagged object. This authority is complicated, by the fact that a tagged object may change owners during its lifetime and there might be multiple logical data 'owners' who are entitled to access information stored about a token even if they do not own the physical object. In the short time line of our use case the tagged refrigerator has changed owners/guardians several times. The first owner was the manufacturer, the shop, the delivery company, then the original customer and finally the neighbour. Furthermore the maintenance contractor might be entitled to read the tag and update the service record. The notion of ownership links to other security mechanisms, such as authentication, key management and information access control, which in turn allow services like privacy and data integrity to be implemented. Defining token ownership and the transfer of ownership is therefore an important aspect of user-oriented RFID applications [23][24]. Tag ownership schemes should allow for privileges to be added and removed, e.g. a new owner can access the associated information while the previous owner's access is revoked, and specify which entity has the right or the responsibility to modify privileges. It should also take into account that the information might have multiple owners, even if the physical object only has one, and that these can also change during the lifetime of the token.

4.3 Data Integrity

RFID applications rely on the integrity of data stored on the token and in many cases on networked repositories. Sufficient measures must therefore be in places to ensure that this data is correct and authentic. The customer purchasing the refrigerator would like an assurance that the product is genuine, i.e. that it is not a counterfeit product referencing to the legitimate manufacturer's documentation, while the maintenance contractor might wish to verify that the refrigerator he is servicing is the one associated with the services record, i.e. the user did not modify a token on an old product to get a free service under another person's warranty. The risk associated with

storing data on RFID tokens is that adversaries, (this includes the object's owner), have the opportunity to tamper with or analyze tokens with the purpose of creating clones or modifying the stored data [28]. This risk could be mitigated by controlling who can modify data and then making it possible for entities to verify that the data was modified by an authorised party. The same security principles apply to networked data repositories where traditional network security risks also need to be addressed [17]. Data integrity is not only a security concept but, also encompasses additional operational processes that ensure that records are simply correct. [30].

4.4 Application Integrity

User-oriented applications require an application client to be run locally by the end user to access the RFID token and trigger associated events. Requests for services and related information will often be directed to a networked application server, interacting with the online data repositories. If security vulnerabilities are identified within the application software and these are exploited it will obviously impact negatively on the operation of the system. If the refrigerator owner's client is compromised, an adversary might be able to modify triggered events or reroute URI requests for fraudulent means e.g. redirect to a spoof service record server for stealing private information or connecting the call to a rogue maintenance contractor. Rieback *et al.* [25] have proposed the idea of RFID-based malware, which would be able to exploit software vulnerabilities by using token responses to execute buffer overflow, malicious code insertion and SQL injection attacks. Mulliner [26] also demonstrated a proof-of-concept worm affecting NFC-enabled mobile phones that is capable of redirecting URI requests and self propagation by writing itself to accessible RFID tokens. These examples serve to emphasise the importance of securing the user's hardware platform in addition to the client and back-end application software.

4.5 RFID Security Standards

As previously mentioned, there are a number of standards defining technical aspects of RFID systems but security aspects are unfortunately not addressed in the same way and often excluded or only discussed briefly. Security policies and 'standards' take the weaker form of recommendations or guidelines, such as [21], which are seldom strictly enforced [27] so it is left to the developer to design and implement security on an application by application basis. Allowing developers to implement RFID security based on their own proprietary standards is a risk and often leads to 'security through obscurity' approaches, which result in systems that are potentially easier to compromise [31]. Apart from the weakened security that might result from proprietary solutions the lack of a consistent industry standard also affects interoperability. In our earlier use case the owner, the shop, the manufacturer, the maintenance contractor and delivery men needed to access the token and the associated data repositories. Each one of these entities does not necessarily operate the same application client or server so for this system to function all systems need to be interoperable with regards to technology, data formats and security. It could therefore be advantageous if the technical and policy aspects of RFID security could be defined in open and peer reviewed industry standards that would promote user confidence and ensure interoperability.

5 Conclusion

Currently, RFID object tagging systems offer limited benefit after objects have been passed on to the end user. To encourage more user-oriented, networked applications a more open approach to RFID is needed, which allows for multiple entities outside the supply chain to interact with tokens in an ad-hoc and meaningful way. Such an approach would allow users themselves to exert more control over tokens and the associated data, whether for privacy or functional reasons. Furthermore, if users felt they are in control and their privacy and security is not at risk they might begin to actively contribute to the ‘Internet of Things’ themselves by labelling objects and/or linking objects to data entries or applications. However, widespread public acceptance of RFID-based tagging systems is some way off and will depend on strong security solutions being in place within a user-oriented, open architecture. Achieving public acceptance would therefore require that major challenges with regards to privacy, ownership, data integrity, application integrity and security standards are verifiably addressed.

References

[1] M.R. Rieback, B. Crispo and A.S. Tanenbaum. The Evolution of RFID Security. *IEEE Pervasive Computing*, Vol. 5, Issue 1, pp 62-69, January 2006.

[2] The History of RFID Technology. *RFID Journal*, December 2006.

[3] J. Landt and B. Catlin. Shrouds of Time: The history of RFID. *AIM White Paper*, October 2001.

[4] EPC Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2.

[5] ISO/IEC 14443: Identification cards - Contactless integrated circuit cards - Proximity cards.

[6] ISO/IEC 15693: Identification cards - Contactless integrated circuit cards - Vicinity cards.

[7] ISO/IEC 18000: Information technology - AIDC techniques - RFID for item management - Air interface.

[8] ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1).

[9] ISO/IEC 21481 Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-2).

[10] RFID and the 'Internet of Things'. *Digital ID World*, pp 66-69, November 2003.

[11] G. Roussos, S.S. Duri, C.W. Thompson. RFID Meets the Internet. *IEEE Internet Computing*, Vol. 13, Issue. 1, pp 11-13, January 2009.

[12] 'Internet of Things' in 2020. *EPoSS – European Technology Platform on Smart Systems Integration Report*. August 2008.

[13] Commission Recommendation on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification. *Commission of the European Communities Recommendation {SEC(2009) 585, SEC(2009) 586}*, May 2009.

[14] touchatag. *www.touchatag.com*

[15] violet. *www.violet.net*

[16] NFC Forum Technical Specifications. *www.nfc-forum.org/specs/spec_list/*

[17] A. Mitrokotsa, M.R. Rieback and A.S. Tanenbaum. Classifying RFID Attacks and Defences. Information Systems Frontiers, Springer, July 2009.

[18] A. Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp 381-394, February 2006.

[19] P. Rotter. A Framework for Assessing RFID System Security and Privacy Risks. *IEEE Pervasive Computing Magazine*, Vol. 7, Issue 2, pp 70-77, April 2008.

[20] Bundesamt für Sicherheit in der Informationstechnik. Security Aspects and Prospective Applications of RFID Systems, October 2004.

[21] Guidance for Securing Radio Frequency Identification (RFID) Systems}, *NIST: Special Publication 800-98*, April 2007.

[22] G.P. Hancke. Eavesdropping Attacks on High-Frequency RFID Tokens. *4th Workshop on RFID Security - RFIDSec08*, July 2008.

[23] B. Song. RFID Tag Ownership Transfer. *4th Workshop on RFID Security - RFIDSec08*, July 2008.

[24] K. Osaka, T. Takagi, K.Yamazaki and I. Takahashi. An Efficient and Secure RFID Security Method with Ownership Transfer. *Conference on Computational Intelligence and Security*, pp 1090-1095, November 2006.

[25] M.R. Rieback, B. Crispo and A. Tanenbaum. Is Your Cat Infected with a Computer Virus? *4th IEEE Conference on Pervasive Computing and Communications*, pp 169-179 , 2006.

[26] C. Mulliner. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. *1st Workshop on Sensor Security*, March 2009.

[27] J. Ayoade. Privacy and RFID systems, Roadmap for Solving Security and Privacy Concerns in RFID Systems. *Computer Law and Security Report*, Vol 23, pp 555-561, 2007.

[28] A. Karygiannis, T. Phillips and A. Tsibertzopoulos. RFID Security: A Taxonomy of Risk. *1st International Conference on Communications and Networking in China*, pp 1-7, October 2006.

[29] S. Garfinkel, A. Juels and R.Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, Vol. 3, No. 3, pp 34-43 2005.

[30] S. Garfinkel. An RFID Bill of Rights. *Technology Review*, October 2002.

[31] T. Phillips, T. Karygiannis and R. Kuhn. Security Standards for the RFID Market. *IEEE Security and Privacy*, Vol. 3, No. 6, pp 89, November 2005.