SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

Mobile RFID Security Issues

Divyan M. Konidala * Kwangjo Kim †

Abstract— Radio Frequency Identification (RFID) is currently being used for auto-identification of objects, assets, pets, and people. Its initial success in offering strategic advantages for businesses, by efficient tracking of inventory in the supply chain, has left this technology wide open to many applications that are only limited by people's imagination. This technology will have a tremendous impact on our society, once it starts to assist people in their daily life. A right step in this direction would be Mobile RFID, where a RFID reader chip is integrated into a portable mobile device like mobile phone, and PDA. Mobile RFID would help consumers in shopping, and allows quick and easy access to information, just by bringing their mobile devices near to an object that has a RFID tag. This paper pioneers in describing Mobile RFID's new applications and security challenges. It focuses on different Mobile RFID application zones, and their related security threats, and security requirements. Finally it proposes a simple security architecture for Mobile RFID applications in Location-based Services zone.

Keywords: Mobile RFID, Mobile RFID Security, RFID Security

1 Introduction

1.1 RFID Technology

Radio Frequency Identification (RFID) is a means to efficiently, easily, and quickly auto-identify objects, assets, pets, and people. So far, RFID technology is used by some big companies like Wal-Mart, Proctor & Gamble Co., Hewlett-Packard, Prada, Gillette, GAP, Target Corp., and the Albertsons Inc., to track their inventory in the supply chain. With the current barcode technology, each product's barcode label (Uniform Product Code - UPC) must be brought before the reader or laser and labels must be scanned one by one. This leads to laborious, painstaking, human-error prone, and time consuming inventory check, and also makes customers in a store to wait in long queues at the cashier counter.

That line-of-sight between label and reader is often difficult, impractical, or even impossible to achieve in industrial environments, therefore RIFD technology allows accurate and very quick scanning of products in large bulks thus speeding up the supply chain management. Other advantages of RFID technology include: RFID tags can stand a harsh environment, long read ranges, portable database, multiple tag read/ write, tracking people, items, and equipment in realtime, *etc.* [4] gives a detailed description about RFID technology and its advantages for supply chain management.

Passive RFID tags are attached to objects/products and these tags contain tiny, but durable computer chips with very small antennas. Passive tags are powered-up from the interrogation Radio-Frequency (RF) signal of a reader. The tiny computer chips contain an Electronic Product Code (EPC) that uniquely identifies the object to which it is attached to, and the antennas automatically transmit this EPC number without requiring line-of-sight (*i.e.,* visual) scanning, to RFID readers within a certain RF range.

1.2 Building Blocks of RFID Infrastructure

This sub-section introduces the four main building blocks of RFID Technology. This infrastructure is currently being developed by EPCglobal Inc. [2]. This organization is entrusted by industry to establish and support a global standard for real-time, automatic identification of information in the supply chain of any company, anywhere in the world.

1.2.1 RFID Tags

As mentioned above, every RFID tag contains its unique EPC number. EPC is a globally unique serial number that identifies an item in the supply chain. EPC data/number contains: EPC Manager number (identifies the company), Object class (similar to a stock-keeping unit, also called product number), Serial number (specific instance of the object class being tagged, objects own unique identifier). EPCglobal allocates manufacturers specific blocks of EPC numbers, and manufacturers then add their own product codes and serial numbers to their assigned manufacturer numbers to create unique identifiers - EPCs.

Further information about the product is stored on a network of servers and databases called EPC Network. Therefore, unique EPC number acts like a pointer directing the RFID reader to the right entity on the EPC Network from where the reader can download additional related data about the product it scanned.

* International Research Center for Information Security (IRIS), Information and Communications University (ICU), 103-6, MunjiDong, YusungGu, Daejeon 305-714, Republic of Korea. (divyan@icu.ac.kr)

† IRIS, ICU, (kkj@icu.ac.kr). This work was partly done while the author was visiting, Department of Computer Science & Engineering, University of California at San Diego (UCSD).

1.2.2 RFID Readers

RFID readers are used to scan RFID tagged items. RFID readers send scanned EPC data for processing to EPC Middleware.

1.2.3 EPC Middleware

In order to handle the billions of reads that happen in a typical warehouse we need is to have a middleware (filtering software) for the readers. The data created by an RFID reader needs to be filtered and smoothed before it is useful for any application. Hence EPC Middleware manages real-time read events and information, provides alerts, and manages the basic read information for communication to EPC-IS as well as company's other existing information systems. It enables efficient useful data exchange between RFID readers and EPC Network.

1.2.4 EPC Network

Just like the global look-up system such as the Domain Name Service (DNS), VeriSign [4], after obtaining the contract from EPCglobal, has invested heavily in building and marketing an EPC Network specifically to look up EPC data. It becomes very necessary to look up each EPC number on a central data repository like we do with a Web page or other system using DNS. Keeping EPC data as an unique reference or primary ID, further information about the respective product is stored on databases and servers of EPC Network. This network assists local company staff and geographically distributed supply chain partners to easily and efficiently access information on any product they are handling from any location. The EPC Network [4] consists of three main components: Object Naming Service (ONS), the EPC-Information Services (EPC-IS), and the EPC-Discovery Services (EPC-DS).

- The ONS like DNS, is an authoritative global directory of EPC-IS. EPC data is registered within the ONS. A retailer may need to get information about the product it has just received. He scans the EPC number of the product's RFID tag and sends it to the ONS. ONS returns the location of the manufacturer's EPC-IS. This query process is transparent to the retailer takes only milliseconds to execute.

- EPC-IS are individual companies' publicly accessible databases that contain the details related to a product. EPC-IS would contain the EPC data, product description, size, weight, packaging, shipments, product arrival and departure details, and various other data that are appropriate to share with supply chain partners.

- The EPC-DS interacts with Information Services throughout the life of the product and maintains a history of each status change for the EPC tag. As products make their way across multiple points throughout the supply chain, this process of products being scanned, and the knowledge of their data within EPC-IS being passed on, repeats itself. The registration of this product knowledge by each EPC-IS into the EPC-DS enables full supply-chain visibility. By enquiring EPC data from ECP-DS any member of the supply chain can obtain real-time, complete visibility of the supply chain.

1.3 Mobile RFID Technology

As mentioned above, most applications of RFID for tagging and tracking items have been for operations within a single big company and its supply chain partners. The reason being, RFID tag costs are still relatively high, but they are declining quickly and approaching a level at which it becomes practical to tag products at the item level. This will open the door for large-scale use of RFID tags on consumer goods. Very soon we can realize, one of the visions of automatic identification and ubiquitous computing, which is the creation of an "Internet of Objects".

In such a highly connected network; devices, objects, items of any kind dispersed through an enterprise or in our society can talk to each other, providing real-time information about the objects, location, contents, destination, and ambient conditions. This communication allows much-sought-after, efficient and easy machine-to-machine identification, communication, and decision-making. Thus RFID technology will have a tremendous impact on our society, once it starts to assist people in their daily life. A right step in this direction would be Mobile RFID, where a RFID reader chip is integrated into portable mobile devices like mobile phones, and Personal Digital Assistants (PDA).

In near future, Mobile RFID would equip people to carry along with them a portable RFID reader in their mobile phones. This extends mobility, allowing people to scan RFID tagged items as and when they want and provides an easier, user-friendly approach to quickly and efficiently access information from RFID tags. [3] Nokia is now offering portable RFID readers that even interoperate with mobile phones. Thus every individual is capable of carrying a RFID reader embedded in his mobile phone/portable device, making RIFD readers ubiquitous. With the presence of billions of geographically distributed RFID tagged items all around, providing us with instant real-time information, it becomes necessary to look up each EPC number of a tagged item on a publicly accessible central data repository. Therefore, minor modifications to the RFID infrastructure described in section 1.2, would best suit this future Mobile RFID technology.

1.3.1 Applications of Mobile RFID

Once the RFID tags become cheap, we can literally attach them to as many items as possible. As a result, just by bringing mobile devices near to a RFID tagged object, we can quickly and easily download information held by that object and view it via mobile phone's display screen. For example:

- We can download information about a particular location by scanning RFID tagged sign posts, and

landmarks

- We can download bus routes by scanning RFID tagged Buses
- We can download prices of RFID tagged merchandise sold at stores, published in catalogs for Compare Shopping
- We can download movies, music, trailers, show timings, and theater locations by scanning RFID tagged movie posters, music CDs, *etc.*
- We can download current menu being served at a particular restaurant by scanning its RFID tag, published in a restaurants catalog
- We can make a quick call or send an instant message by scanning RFID tagged photographs, business cards, address books, *etc.*

1.4 Related Work

We strongly believe that Mobile RFID technology has a great future and it's a very challenging research area. It is poised to be one of the future killer applications and services of mobile communications. Since Mobile RFID technology is still in its infancy stage, to the best of our knowledge we did not find any literature that discusses about security for Mobile RFID technology. This paper could be the first of its kind to discuss about the vision and security challenges of Mobile RFID technology.

2 Mobile RFID Application Zones

Applications of Mobile RFID can be broadly categorized into three zones namely: Location-based Services (LBS) Zone, Enterprise Zone, and Private Zone. Security threats and security requirements for Mobile RFID differ with respect to these zones. Figure 1 is self-explanatory about the various security threats and security requirements for these three zones. [1] provides a detailed description of various security and privacy threats for RFID technology and also discusses certain proposed security models.

2.1 Location-based Services (LBS) Zone

In a location-based services zone, service providers can provide us with services "related to" and "available at" that location. The coverage of this zone is very large which includes all public places. In this zone, service providers and vendors want to provide services that are available at customer's current location. To accomplish this, service providers deploy RFID tagged items/devices all around, which provide us with instant real-time information about services available at that location. However the communications between the mobile RFID and EPC network must be secured.

Mobile RFID thus identifies and interacts with such smart devices/items and obtains services like information about a particular location by scanning RFID tagged sign posts, and landmarks, download bus routes by scanning RFID tagged Buses, download prices of RFID tagged merchandize sold at stores, for Compare Shopping, download movies information, trailers, show timings, and nearest theater locations by scanning RFID tagged movie posters *etc.*

Security framework for this zone is very much open. In this zone all RFID tagged items respond to every mobile RFID, otherwise the main purpose of these items to provide instant information would be defeated. Therefore in this zone there would be no security requirements for authentication and securing the communications between RFID tag and mobile RFID. But there is one problem, these publicly available tags can be fake or must have been illegally modified and hence no longer truly represent the services of the tagged item.

In such an unprotected zone, establishing a appropriate security architecture is very difficult. Mobile RFID must contact many EPC-IS which might be either genuine or malicious. It should also be able to identify and securely communicate with only genuine EPC-IS. But these tasks could create a huge burden on the low-computing and resource-poor mobile device.

Our proposed security architecture (explained in the following section) for Mobile RFID - LBS zone describes a convincing trust model and secure job delegation to mobile operator. Therefore the mobile operator can help in reducing the communication and computational burden on the mobile RFID. The architecture also provides users privacy protection.

2.2 Enterprise Zone

In this zone Mobile RFID assists company's mobile staff/employees like inventory checkers, field engineers, maintenance and repair staff, and security guards. It helps them in real-time inventory management, work attendance log, instructions on how to operate tagged items, 'identification of' and 'access control to' tagged equipment and secure enclosures, and proof of staff presence at certain locations in a building that needs to be monitored periodically, *etc.*

The security framework for enterprise zone Mobile RFID applications could be proprietary and confined to the boundaries of a particular organization. In such a confined and well-monitored zone it's not very difficult to establish and enforce an efficient security architecture, trust model, and security & privacy policies. With the availability of up-to-date list of registered employees and items/products in a company; designing and implementing key/ password distribution, data integrity & confidentiality, identification, authentication, and access control protocols among staff, RFID readers, RFID tagged items, and EPC Network is moderately easy and mostly risk free when compared to LBS zone.

Since this zone needs precise authentication and security auditing in order to access RFID tagged items, issues like user identity privacy and tag information privacy will not arise.

2.3 Private Zone

In this zone, Mobile RFID assists users in their private space like home, garden, garage, car, and workshop. It helps them to make an instant call or send an instant message by scanning RFID tagged photographs, business cards, and address books. By scanning RFID tagged household items with a mobile phone, we can quickly obtain information like; when would the milk stored in the refrigerator expire, details of the books in the bookshelf, when was the last time a RFID tagged plant has been watered, and when to change the engine oil, *etc.*

This zone is small when compared to the other two zones and therefore it requires a simple security model that can be easily deployed and maintained by the user at his home. Users in this zone can buy off-the-shelf Mobile RFID Kits. These kits can contain RFID tags, Mobile RFID, related hardware, and software with user-friendly GUI. The software can assist the users to easily encode EPC numbers of their choice into the RFID tags, create a portable database in their PC with details about the tagged household items, create passwords to access these tags and the database, and finally secure the wireless/WiFi network in the home environment.

Other option could be, the user can obtain storage space (for free or fee) on the EPC Network (EPC-Information Servers) and via a password protected user-friendly website, he can upload his personal EPC numbers and details of the tagged household items. Whenever he scans his private RFID tag in his home, the Mobile RFID contacts his personal page on the EPC-Information Server and downloads the details about the item in question. This approach alleviates user's burden of configuring his own security system. The EPC-Information Server must provide user privacy protection, and secure communication.

3 Building Blocks: Mobile RFID - LBS Zone

The building blocks of Mobile RFID infrastructure in LBS zone is similar to above mentioned RFID infrastructure. Expect that we introduced mobile operator and eliminated the need of EPC Middleware. Since mobile RFID would mostly scan one tagged item at a time, there is no need for filtering software to make the mobile RFID data clear.

- Mobile RFID (M-RFID): Mobile Phone with RFID Reader Chip, is used to scan tagged items available everywhere.
- RFID Tags
- Mobile Operator (MO): In the current mobile communications paradigm we have already put in a great deal of trust in MO, as it handles all our voice and data communications. It maintains a record of each subscriber's call details, contact information, and credit card details, *etc.* It even has the capability to easily determine our current location and tap into our communications. But what protects us from MO turning hostile is that it has to very strictly adhere to and follow legal, security and privacy policies imposed by the law. Our architecture extends this trust in MO to secure and provide privacy protection for Mobile RFID transactions. This approach is very practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. MO takes responsibility on behalf of M-RFID to select, identify, and authenticate genuine ECP-IS. MO behaving like a "Trusted Proxy" processes the request on behalf of the M-RFID, greatly reducing the communication and computational burden on the user's mobile phone and also provides users privacy protection.
- EPC Network

Threat	Security Req.	LBS Zone		Enterprise Zone		Private Zone	
		T* & MR*	MR & N*	T & MR	MR & N	T & MR	MR & N
Overall Security	Security Architecture	Large		Medium		Small	
Tag Info. Privacy	Tag Killing / Pwd Protection		x			x	x
User Identity Privacy	Anonymous Transaction		x				x
Key/Pwd Compromize	Trust Model		x	x	x		x
	Key/Pwd Mgt. & Distribution		x	x	x	x	x
Illegal Tag Info. Access / Cloning / Denial of Service Attack	Authentication		x	x	x	x	x
	Authorization		x	x	x	x	x
	Access Control		x	x	x	x	x
Illegal Tag Info. Alteration	Tag Data Integrity & Confidentiality	x		x		x	
Network Eavesdropping	Encryption (symmetric / Assymmetric)		x	x	x	x	x
	Wireless Network Security		x		x		x
Transaction between: *T: Tag, *MR: Mobile RFID Reader, *N: EPC Network							

Figure 1: Comparison of Security Threats and Security Requirements of 3 zones

4 Security Requirements: Mobile RFID - LBS Zone

We identified the following security requirements associated with the deployment of Mobile RFID:

- Secure Job Delegation
- Trust Model
- Unauthorized Tag Information Access
- User Privacy Protection
- Tag Access-Control Management
- Tag Access Authorization
- Data Integrity & Confidentiality

4.1 Secure Job Delegation

The Mobile RFID on behalf of its owner may need to communicate with ONS, EPC-IS to retrieve the information of a particular tagged item. It should identify and authenticate genuine EPC network and be able to secure the entire transaction and also protect the owner's privacy. But these tasks could create a huge burden on the low-computing and resource-poor mobile device and is certainly not user friendly. Therefore it would be lot easier for the mobile device to securely delegate its work to a nearby trusted high-computing and resource-rich entity, the mobile operator. This approach helps in reducing the communication and computational burden on the mobile device.

4.2 Trust Model

Establishing an efficient and convincing trust model is very much required to ensure secure transactions, key distribution, and job delegation. With existence of a trust model, it would be lot easier for the mobile device to delegate its work to the mobile operator.

4.3 Authorized Tag Information Access

Scenario: Alice goes to a shopping mall. She uses her Mobile RFID reader to know the price, and manufacturer details of a particular commodity. The commodity's RFID tag must not reveal other sensitive details like the number of pieces sold so far, its profit margin, and stock availability, *etc.* in order to prevent corporate espionage. This information is strictly for the shopping malls inventory checking staff

4.4 User Privacy Protection

Scenario: Charlie stalks Alice into the elevator. Charlie has a RFID reader embedded in his mobile phone. Charlie can easily scan and read sensitive information off any RFID tagged item that Alice is carrying in her bag/purse. After scanning a particular RFID tag for information, the identity and location of Alice must not be revealed to the vendor or the service provider. This personal information could allow service providers and vendors to generate detailed profiles of the user, his buying interests, and transactions information.

4.5 Tag Access-Control Management

Sometimes information from the tags needs to be available to authorized parties only. But for mobile RFID scenario, the set of authorized parties is constantly changing, making access management a priority for businesses. Therefore providing tag information based on the privileges of the user in question is very essential.

4.6 Tag Access Authorization

Certain RFID tags needs to respond to mobile RFID readers whose owners are

- Above 18 years old
- Gold card Members or certain privileged members of certain organizations
- Staff of a particular organization
- Security guards
- Construction workers

4.7 Data Integrity & Confidentiality

We must keep the data that resides in a tag secure and also provide Secure Electronic Data Interchange (EDI) transactions between the Mobile RFID, Mobile Operator, and EPC Network.

5 Security Architecture: Mobile RFID - LBS Zone

This section describes our proposed security architecture of the Mobile RFID as depicted in Figure 1.

- Step 1: M-RFID scans a RFID tag
- Step 2: RFID tag responds with EPC number
- Step 3: M-RFID authenticates itself to MO via login ID/pwd and sends the EPC number to MO
- Step 4: MO sends EPC number to the ONS
- Step 5: ONS responds with URL of the EPC-IS related to the EPC number in question
- Step 6: MO fetches the anonymous M-RFID certificate from its database and sends it along with EPC number to the URL of EPC-IS. The certificate does not contain the identity of M-RFID but contains some related information like age, proof of privileged membership, *etc.*
- Step 7: EPC-IS verifies the certificate and checks the access-control list in its database.
- Step 8: Depending on the access rights of that certificate, EPC-IS responds to MO with related data about the EPC number in question.
- Step 9: MO sends the EPC information to the M-RFID. This communications can be encrypted using an established session-key
- Step 10: MO stores details of this transaction in the database of this M-RFID. Later, M-RFID can query some information about the tags it accessed previously on a particular date, time, location (for compare shopping) and also items it purchased.
- Step 11: M-RFID can purchase tagged items. MO can pay the vendor on behalf of M-RFID and later get the money from M-RFID via monthly telephone bills. When a tagged item is purchased MO makes sure that the details of that particular EPC number is removed from EPC-IS. This prevents adversary to scan and know the details of the purchased items in the handbag of M-RFID's owner.

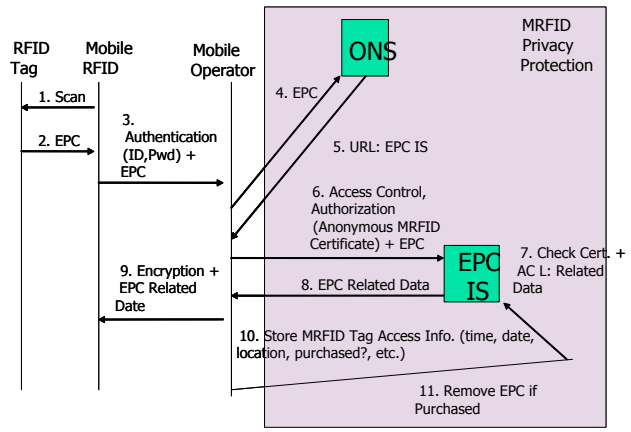

Figure 2: Mobile RFID - LBS Zone Security Architecture

5.1 Security Solutions

5.1.1 Mutual Authentication mechanism between M-RFID and MO

A simple ID/Password authentication for M-RFID and MO's PKI certificate verification by M-RIFD is necessary for mutual authentication between M-RFID and MO. This provides secure job delegation, trust model, data integrity and confidentiality between M-RFID and MO.

5.1.2 Mutual Authentication mechanism between MO and EPC-IS

Since MO and EPC-IS are resource rich entities, they both can authenticate each other via PKI-based certificates. Thus providing data integrity and confidentiality.

5.1.3 Anonymous Certificates for Identity management, authentication, and authorization

M-RFID can request anonymous certificate from MO. This certificate does not contain the true identity of M-RFID but contains other details like age, whether the user is a gold card member or not, staff or visitor, *etc.* This protects the privacy of the owner of M-RFID and also assists EPC-IS to provide corresponding information about the EPC number in question.

5.1.4 M-RFID privacy

Our approach protects both location and information privacy of M-RFID. With the use of anonymous certificate the vendor or the service providor of the tagged item can never know the true identity of the M-RFID's owner. And once the tagged item is purchased by M-RFID, MO makes sure that its reference is deleted from the EPC-IS. This way even though, an adversary can scan the handbag of Alice, he can no longer obtain information about the tagged items purchased by Alice as their references are deleted from EPC-IS.

6 Conclusions

This paper provides future vision and security challenges of Mobile RFID. We mentioned the various security threats and security requirements at different zones of Mobile RFID applications namely LBS, enterprise, and private zones. And proposed a simple security architecture for the LBS zone, that fits the RFID EPC Network. The advantages of this architecture are as follows: simple, involves less user interactions, secure job delegation between Mobile RFID and Mobile Operator. Also the Mobile Operator conceals the identity of users, as a result service providers and vendors of tagged items cannot maintain users detailed profiles and location information, this protects users privacy. It could be a good revenue generator for the mobile operator and service providers through commissions for every transaction. Our approach is practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable. And vendors can still use the the popular RFID EPC network. As our future work we would propose more concrete security architectures for the other two zones of Mobile RFID applications and also propose a simple, secure and privacy preserving payment phase for Mobile RFID applications.

References

[1] Ari Juels, "RFID Security and Privacy: A Research Survey", RSA Laboratories, 2005,

[2] EPCglobal Web site, 2005, `http://www.EPCglobalinc.org`

[3] Nokia, "RFID Phones - Nokia Mobile RFID Kit", `http://europe.nokia.com/nokia/0,,55739,00.html`

[4] VeriSign, "The EPCglobal Network: Enhancing the Supply Chain", White Paper 2005, `http://www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf`