FACTA UNIVERSITATIS
Series: **Mechanical Engineering** Vol. 7, N° 1, 2009, pp. 93 - 100

RFID INFRASTRUCTURES AND SECURITY ISSUES

UDC 65.011 : 65.011.56

Mehmet Kis

Ege University, Dept. of Computer Eng., 35100 Bornova Izmir, Turkey
E-mail: mehmet.kis@gmail.com

Abstract. *This paper emphasizes efficiency, productivity and privacy of the integration of Radio Frequency Identification (RFID) technologies to mobile information systems. It also mentions the project that has been developed with the idea of creating a common RFID infrastructure that can be used with wireless/mobile information systems and of securing this infrastructure for reliability.*

Key Words: *RFID, Infrastructure, LMS, SCORM, Security, Privacy*

1. INTRODUCTION

The rapid and accelerating move of the mobile technologies provides us with the ability of working independently at any location and on the move. Using portable computers, pocket PCs and smart phones, we can be fully independent of the environment; furthermore, the implementation of a wireless system and of various types of services is also available. For a better service in this wireless system, for context awareness and adaptability, we need to integrate tracking technologies, such as RFID, to the mobile information system.

By the integration of RFID tags and readers to the portable computers and pocket PCs, the properties such as context - awareness and adaptive services will be added to the information gathering progress. RFID technology will obtain the individual context determination and adaptation regarding the position tracking ability; therefore the quality and effectiveness of the service will also increase.

In addition to great productivity gains, RFID systems may create new threats to the security and privacy of individuals or organizations. RFID tags may pose security and privacy risks to both organizations and individuals.

This paper will explain the "RFID Infrastructure for Wireless Mobile Systems (RIWIS)" project, which is developed as an infrastructure that can be used for enabling context awareness and adaptivity in mobile information environments. The security and privacy problems of this infrastructure will also be dealt with in the paper.

Received March 6, 2009

2. Basic Ideas And System Overview

The improvements in the technologies give us the chance of creating an infrastructure for other projects that will be developed as a standardized, context aware, wireless/mobile information systems.

Our first goal is to create a generic RFID interface tool which is compatible with wireless information systems. The second one is to enhance this tool and make it inter operable with learning systems which comply with the standards. This system will be called as "RFID Infrastructure for Wireless Mobile Systems (RIWIS)" project and will also support dynamic integration of new components to systems.

This project has been developed with the idea of creating an RFID infrastructure that can be used with wireless/mobile information systems and standardized learning management systems. RIWIS project aims to add the context awareness property to the learning environment. With the integration of RFID technology to a traditional learning management system, we intend to create a context aware, mobile and standardized information system that can be used in a variety of types of application areas such as projects of Wireless RFID networks for real-time customer relationship management[1] and a ubiquitous and interactive zoo guide system[2].

Using RFID technology, RIWIS project aims to add the context awareness property to the learning environment. Context awareness is one of the key points in ubiquitous learning. The challenge here is that, most of the systems that have the context awareness property are dedicated to context-awareness sub-systems for specific application areas, and this leads to unavailability of reusing the components of the systems in other projects. RIWIS tries to create an infrastructure to meet the necessity of more generic programming frameworks that can be used in different application domains with a few changes.

RIWIS project uses ADL's sample Learning Management System (LMS), which supports SCORM 2004 (Shareable Content Object Reference Model) standard, in its LMS sub-unit. This minimizes the standardization problems and brings the benefits such as reusability and interoperability of the learning content and context aware structures.

The "context" word in "context awareness" denotes the physical and social conditions of the computational devices. The aim of the context awareness is to collect the environment data of the device, analyze the given data, evaluate and serve them, accordingly. With the integration of RFID technology to a traditional learning management system, RIWIS creates a context aware, mobile and standardized learning system that can be used in various types of application areas.

3. The RIWIS Project

RFID Infrastructure for Wireless Mobile Systems (RIWIS) project has been developed with the idea of creating a common RFID infrastructure that can be used with wireless/-/mobile information systems and of making this infrastructure interoperable with standardized learning management systems.

RIWIS is being developed for research and teaching purposes. It is developed using the Java and C# programming languages, following the basic concepts of object oriented programming in implementation.

At the development process of RIWIS project, some of the other projects which are also using context awareness in their structure, learning management systems, mobile learning

techniques and standards are taken in to consideration. The aim here is to create a learning management system which supports standards of content distribution, enable the mobile access to learning content and also to create the context awareness property. RIWIS creates an adaptive, ubiquitous learning environment with a standardized way.

The RIWIS project makes it easier, cheaper and faster of reusing, developing, sharing and distributing the learning content by using a SCORM compatible learning management system as a part of its architecture.

The integration of the RFID unit which consists of RFID readers, RFID tags and software, makes the system context aware and adds to it the ability of tracking the behaviors of the users, and of serving them accordingly. With the help of the RFID tags, the system can guide, inform the users and make them focus just on the related content.

System Architecture

The parts which aggregate RIWIS can be grouped under five sections: a SCORM compatible learning management system, basic components of an RFID system, the software interface between LMS, the RFID enabled user, and the database which keeps the position specific data.

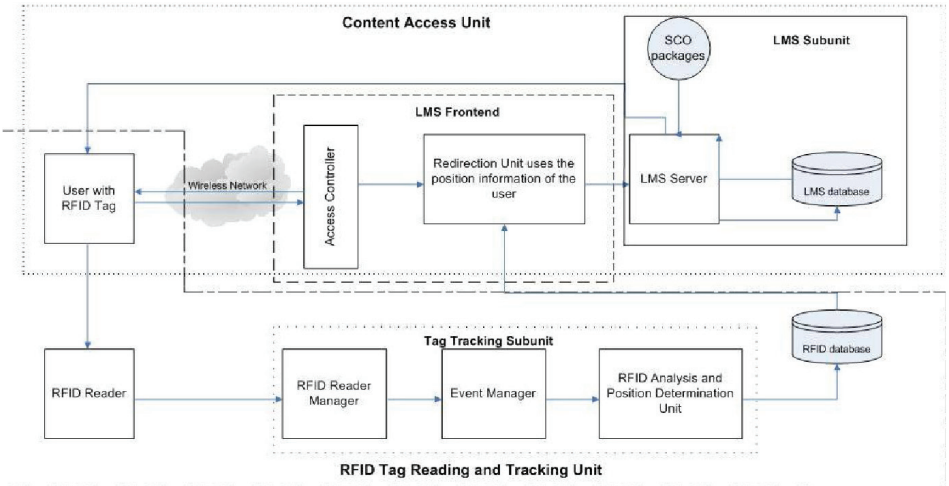

Fig. 1 Architecture of RIWIS Project

An RFID enabled user is a part of the system which has an assigned RFID tag with him and makes the requests to learning management system using a web browser. When a user enters the read range of an RFID reader, the system stores the data which the reader reads from the tag that belongs to the user. The RFID readers are controlled by the RFID Reader Manager of RIWIS which works under the control of Event Manager. When an event occurs, Event Manager informs the RFID Analysis and Position Determination Unit which is responsible to communicate with database to track the positions and to store the data of the users. RFID Analysis and Position Determination Unit processes the data that is sent by the readers and updates the details of the user in database using this data

RIWIS is using ADL's sample Learning Management System (LMS), which supports SCORM 2004 standard, as the part which is used to manage, distribute and share the learning content. When an authorized RFID enabled user requests information from RIWIS, Redirection Unit of the system queries the database for the client user's id, retrieves the position information of the user and informs the LMS to be able give the related learning content to user. This information also contains the position information of the user. When LMS gets a request from Redirection Unit, related content is being prepared to serve according to the position of the user.

The system tracks the users' behaviors using the RFID readers that are controlled by Tag Tracking Unit and responds to request with the help of the wireless information network. The communication between the user and the LMS, is controlled by the Access controller and supported with the Redirection Unit.

4. Security and Privacy Issues

While yielding great productivity gains, RFID systems may create new threats to the security and privacy of individuals or organizations. Unprotected tags may have vulnerabilities to eavesdropping, traffic analysis, spoofing or denial of service. Unauthorized readers may compromise privacy by accessing tags without adequate access control. Even if tag contents are protected, a problem closely related to privacy is tracking, or violations of "location privacy".

This is possible because the answers provided by tags are usually predictable: in fact, most of the times, tags provide always the same identifier, which will allow a third party to easily establish an association between a given tag and its holder or owner. RIWIS users will also be under the threat of RFID exploits. Some well known attacks are[4]:

- Physical Attacks: Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others.
- Denial of Service (DoS): A common example of this type of attack in RFID systems is the signal jamming of RF channels.
- Counterfeiting: There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.
- Spoofing: When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.
- Eavesdropping: In this type of attacks, unintended recipients are able to intercept and read messages.
- Traffic analysis: Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and can not be decrypted.

RFID attacks are commonly conceived as properly formatted but fake RFID data. However, no one currently expects an RFID tag to send a SQL injection attack or a buffer overflow. The life of a buffer overflow begins when an attacker inputs data either directly (i.e. via user input) or indirectly (i.e. via environment variables). This input data is deliberately longer then the allocated end of a buffer in memory, so it overwrites whatever else happens to be there. RFID tags can exploit buffer overflows to compromise back-end RFID

middleware systems. This is counterintuitive, since most RFID tags are limited to 1024 bits or less. However, commands like 'write multiple blocks' from ISO-15693 can allow a resource poor RFID tag to repeatedly send the same data block, with the net result of filling up an application-level buffer [5].

One of the other methods is "Code Insertion". An attacker can inject a malicious code into an application by using any number of scripting languages. These attacks performed using of the following special characters in input data:

< > . ' % ;) (& + -

RFID tags with data written in a scripting language can perform code insertion attacks on some back-end RFID middleware systems. If the RFID applications use web protocols to query back-end databases (as EPCglobal does), there is a chance that RFID middleware clients can interpret the scripting languages (perhaps because the software is implemented using a web client). If this is the case, then RFID middleware will be susceptible to the same code insertion problems as your typical web browsers [5].

SQL injection is also a type of code insertion attack which tricks a database into running SQL code that was not intended. Attackers have several objectives with SQL injection. First, they might want to .enumerate. (map out) the database structure. Then, the attackers might want to retrieve unauthorized data, or make equally unauthorized modifications or deletions. For example, the injected command [5]:

;shutdown--

will shut down a SQL server instance, using only 12 characters of input. Another nasty command is:

drop table <tablename>

which will delete the specified database table. Just as with standard SQL injection attacks, if the DB is running as root, RFID tags can execute system commands which could compromise an entire computer, or even the entire network! One notable spoofing attack can be performed with clonning an RFID transponder, using a sniffed (and decrypted) identifier, and this can be used to unlock an RFID-based system[5].

RFID automates information collection about individuals' locations and actions, and this data could be abused by hackers, retailers, and even the government. There are a number of well-established RFID security and privacy threats. While the idea of RFID viruses has surely crossed people's minds, the desire to see RFID technology succeed has suppressed any serious consideration of the concept. Furthermore, RFID exploits have not yet appeared in the wild. So people conveniently figure that the power constraints faced by RFID tags make RFID installations invulnerable to such attacks.

Proposed Solutions

There are a number of solutions proposed so far to solve the security problems and threats associated with the use of RFID systems. Some of these can also be applied for RIWIS. The fundamental principles and a critical review of every proposal can be summarized as follows. Precise details can be found in the paper of Lopez[4].

- Kill Command: This solution was proposed by the Auto- ID Center and EPCglobal. In this scheme, each tag has a unique password, for example of 24 bits, which is programmed at the time of manufacture. Upon receiving the correct password, the tag will deactivate forever.

▪ The Faraday Cage Approach: Another way of protecting the privacy of objects labeled with RFID tags is by isolating them from any kind of electromagnetic waves. This can be made using what is known as a Faraday Cage (FC), a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). There are currently a number of companies that sell this type of solution.

▪ The Active Jamming Approach: Another way of obtaining isolation from electromagnetic waves, and an alternative to the FC approach, is by disturbing the radio channel, a method which is known as active jamming of RF signals. This disturbance may be done with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers.

▪ Blocker Tag: If more than one tag answers a query sent by a reader, it detects a collision. The most important singulation protocols are ALOHA (13.56 MHz) and the treewalking protocol (915 MHz). Juels [6] used this feature to propose a passive jamming approach based on the tree-walking singulation protocol, called blocker tag. A blocker tag simulates the full spectrum of possible serial numbers for tags[4].

▪ Bill of Rights: Garfinkel proposed a so-called RFID Bill of Rights3 that should be upheld when using RFID systems. He does not try to turn these rights into Law, but to offer it as a framework that companies voluntarily and publicly should adopt[4].

▪ Classic Cryptography:
  – Rewritable Memory: In 2003, Kinoshita proposed an anonymous-ID scheme. The fundamental idea of his proposal is to store an anonymous ID, E(ID), of each tag, so that an adversary can not know the real ID of the tag. E may represent a public or a symmetric key encryption algorithm, or a random value linked to the tag ID. In order to solve the tracking problem, the anonymous ID stored in the tag must be renewed by re-encryption as frequently as possible.
  – Symmetric Key Encryption: Feldhofer proposed an authentication mechanism based on a simple two- way challenge-response algorithm. The problem with this approach is that it requires to have AES implemented in an RFID tag.
  – Public Key Encryption: There are solutions that use public-key encryption, based on the cryptographic principle of re-encryption.

▪ Schemes Based on Hash Functions: One of the more widely used proposals to solve the security problems that arise from RFID technology (privacy, tracking, etc.) is the use of hash functions.
  – Hash Lock Scheme
  – Randomized Hash Lock Scheme
  – Hash-Chain Scheme

▪ A Basic PRF Private Authentication Scheme: This protocol uses a shared secret s and a Pseudo-Random Function (PRF) to protect the messages exchanged between the tag and the reader.

▪ Authentication Methods: The transponders should be validated before the system accept its data as a true value and starts to process it. A cloned transponder can be recognized by creating a "challenge-response (C-R) authentication system". This system will send a query to the transponder and according to response message, transponder will be authenticated and it's data will be processed [7,8]. Using passwords or tag identifiers allow to authorize tags and easily track unauthorized tags [9].

▪ Validation of SQL Queries: Against to the SQL injection attacks; a validator module can be included into the system. This module can be developed as a software which contains artificial intelligence characteristics. SQL attacks can be blocked by the control of this intelligent validator.

▪ Ban Mechanisms: To prevent a transponder to be used as a service blocker, frequent usage of transponder must be eliminated. This prevention can be made both using hardware and software systems.

▪ Unclonable RFID chips: The world's first unclonable silicon chip – the Vera X512H RFID chip - is based on recently announced breakthrough technology called Physical Unclonable Functions (PUF). PUF technology is a type of electronic DNA or fingerprinting technology for silicon chips that makes each chip unclonable. Basic passive RFID chips can be easily cloned by copying the data residing on one chip to another. Verayo's PUF-based RFID chips cannot be cloned, and provide a very strong and robust authentication mechanism. No other chip or device can be disguised as the original chip, even if the data is copied from one Verayo RFID chip to another. [3]

5. CONCLUSION

In this paper, we tried to explain the benefits of RFID infrastructures and the importance of using standards. An RFID integrated mobile learning environment (RIWIS) is described; possible security and privacy problems related to the system have been discussed. For these possible problems, the proposed solutions from some previous works have been introduced.

As we have seen, most of the solutions offer cryptographic techniques. Additional techniques like intelligent application behavior could be developed to bring more security to RFID systems. For the optimization of the security options of RFID systems, each attack type must be taken into consideration as a different scenario. All security characteristics should be analyzed according to these scenarios and different security methods should be put in operation for defense.

Besides the system security, RFID systems also threaten personal privacy. As animals are under control with RFID tags, in the future, the same will refer to human beings. The security and privacy of people will be one of our major problems that should be solved taking care of ethics and issues of privacy.

REFERENCES

1. P. Schloter and H. K. Aghajan, "Wireless rfid networks for real-time customer relationship management." in EUC Workshops, 2005, pp. 1069– 1077.
2. H. Hlavacs, F. Gelies, D. Blossey, and B. Klein, "A ubiquitous and interactive zoo guide system." in INTETAIN, 2005, pp. 235–239.
3. World's first unclonable RFID chip**,** www.net-security.org, Web: http://www.net-security.org/secworld.php?id=6480, September 2008.
4. P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in 11th IFIP International Conference on Personal Wireless Communications – PWC06, ser. Lecture Notes in Computer Science, vol. 4217. Springer-Verlag, September 2006, pp. 159–170.

5. M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "Is your cat infected with a computer virus?" in PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06). Washington, DC, USA: IEEE Computer Society, 2006, pp. 169–179.
6. A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of rfid tags for consumer privacy," in CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, 2003, pp. 103–111.
7. K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," in International Conference on Security in Pervasive Computing – SPC 2005, ser. Lecture Notes in Computer Science, D. Hutter and M. Ullmann, Eds., vol. 3450. Boppard, Germany: Springer-Verlag, April 2005, pp. 70–84.
8. S. Stankovski, G. Ostojić, V. Jovanović, B. Stevanov, B., Using RFID Technology in Collaborative Design, Facta Universitatis: Series Mechanical Engineering, Vol. 4, No. 1, pp 75- 82, 2006
9. S. L. 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.

RFID INFRASTRUKTURE I PITANJA SIGURNOSTI

Mehmet Kis

Ovaj rad ističe efikasnost, produktivnost i privatnost integracije tehnologije identifikacije putem radio frekvencije (ili RFID) u odnosu na mobilne informacione sisteme. Takođe pominje projekat koji je razvijen sa idejom da se stvori zajednička RFID infrastruktura koja se može koristiti sa bežičnim ili mobilnim informacionim sistemima a i da se osigura pouzdanost te infrastrukture.

Ključne reči: *RFID, Infrastruktura, LMS, SCORM, Sigurnost, Privatnost*