RFID Infrastructures and AI Approaches For Security

T. E. KALAYCI

Ege University

September 05th, 2007

1 Introduction

2 The RIWIS Project
- System Architecture

3 Security and Privacy Issues
- Threats
- Proposed Solutions

4 Conclusion

Introduction

- RIWIS (RFID Infrastructure for Wireless Mobile Systems)
- The security problems and proposed solutions

RFID

- RFID(Radio Frequency Identification) is a method of auto identification that is suitable for identifying both products and assets within the supply chain environment.
- Adapting the RFID to mobile environments is both cheaper and easier to use than the technologies like GPS.
- By the help of the position tracking ability, RFID technology will obtain the individual context determination and adaptation, therefore the quality and effectiveness of the learning progress will also increase.

Basic Ideas and System Overview

- Creating an infrastructure for other projects that will be developed as a standardized, context aware, wireless/mobile learning system.
- First goal : Create a generic RFID interface tool that can work compatible with wireless information systems.
- Second goal : Enhance this tool and make it interoperable with learning systems which conform the standards.
- This system will be called RFID Infrastructure for Wireless Mobile Systems (RIWIS) and will also support dynamic integration of new components to systems.

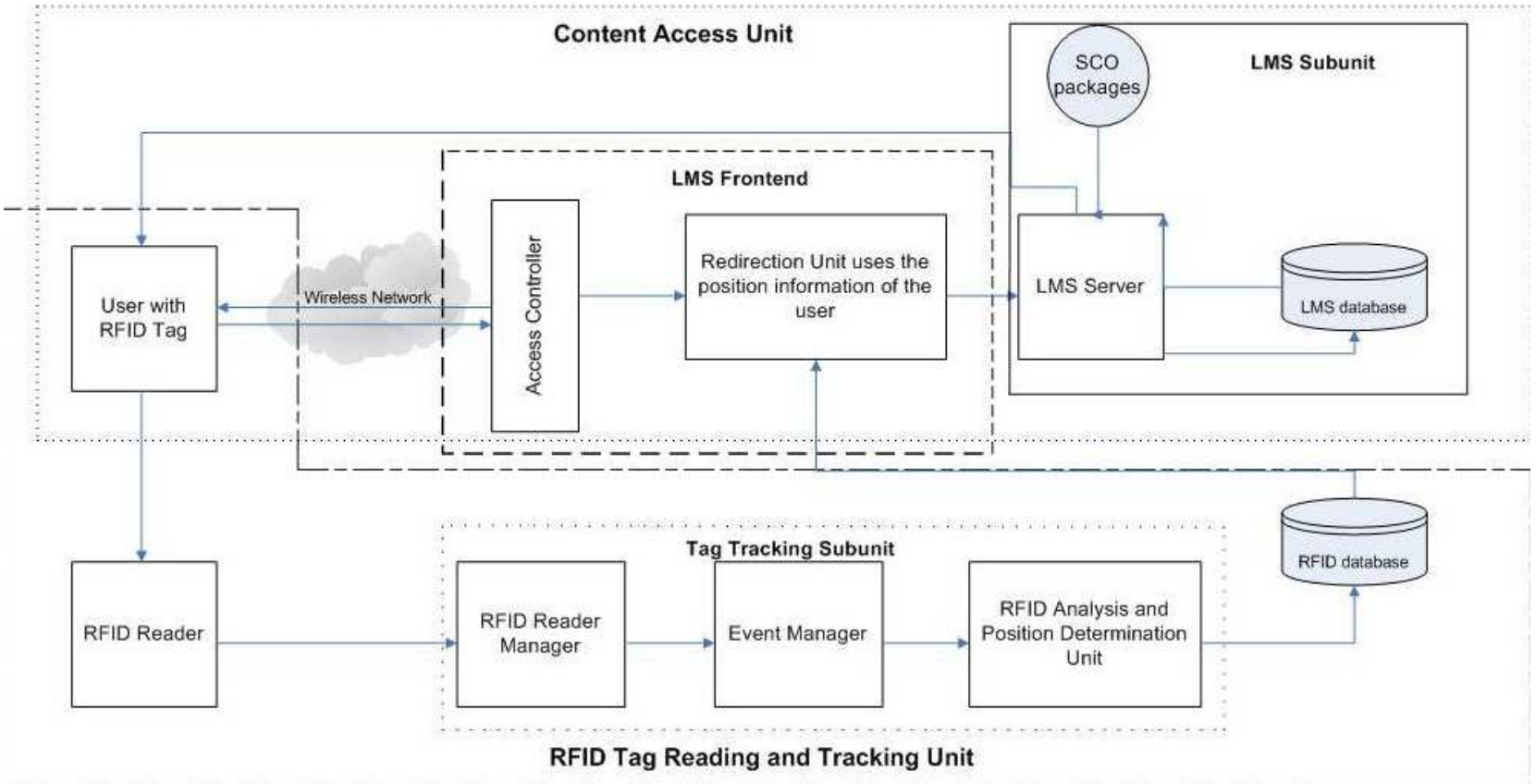
What is RIWIS

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

Aims of Developing RIWIS Project

- Add the context awareness property to the learning environment. Context awareness is one of the key points in ubiquitous learning.
  - The challenge: Most of the systems that have the context awareness property are dedicated context-awareness sub-systems for specific application areas, and this leads to unavailability of reusing the components of the systems in other projects.
- 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 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.

System Architecture



Security And Privacy Issues

- Threats
- Proposed Solutions

Threats

- Physical attacks (probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, etc.)
- Denial of service (signal jamming of RF channels)
- Counterfeiting (modifying the identity of an item - tag manipulation)
- Spoofing (impersonating a legitimate tag)
- Eavesdropping (unintended recipients are able to intercept and read messages)
- Traffic analysis (intercepting and examining messages in order to extract information)
- SQL Injection (running SQL code that was not intended)
- Buffer overflow (input data is deliberately longer then the allocated end of a buffer in memory)
- Code Insertion (Malicious code can be injected into an application using scripting languages and special characters)

Malwares

- RFID installations have a number of characteristics that make them outstanding candidates for exploitation by malware
  - Lots of source code (backend RFID middleware systems may contain hundreds of thousands of lines of source code with lots of exploitable holes)
  - Generic protocols and facilities
  - Back-End databases (Databases are a critical part of most RFID systems and they are also susceptable to security breaches)
  - High-Value data
  - False sense of security (nobody expects RFID malware (yet))

Proposed Solutions

- Kill Command
- The Faraday Cage Approach
- The Active Jamming Approach
- Blocker Tag
- Bill of Rights
- Classic Cryptography
  - Rewritable Memory
  - Symmetric Key Encryption
  - Public Key Encryption

Proposed Solutions

- Schemes Based on Hash Functions
  - Hash Lock Scheme
  - Randomized Hash Lock Scheme
  - Hash-Chain Scheme
- A Basic PRF Private Authentication Scheme
- Authentication Methods
- Validation of SQL Queries
- Ban Mechanisms
- RFID Guardian

Conclusion

- We tried to describe an RFID integrated mobile learning environment and possible security and privacy problems that could have effect on such systems.
- For these possible problems proposed solutions from previous works has been introduced.
- For the optimization of the security options of RFID systems, each attack type must be taken into consideration as a different scenario.
- Beside the system security, RFID systems also threats personal privacy.
- The security and privacy of people will be one of our major problems that should be solved with the care of ethics and privacy issues.

Thanks for Listening!
Questions?