AN INTEGRITY BASED RADIO FREQUENCY IDENTIFICATION (RFID) METHOD AGAINST REPLAY ATTACK

SEYED MOSTAFA MIR HOSSEINI

UNIVERSITI TEKNOLOGI MALAYSIA
UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS PAPER AND COPYRIGHT

Author’s full name: Seyed Mostafa Mirhosseini
Date of birth: 14 Aug 1987
Title: An Integrity Based Radio Frequency Identification (RFID) Method Against Replay Attack

Academic Session: 2012 / 2013

I declare that this thesis is classified as:

☐ CONFIDENTIAL (Contains confidential information under the Official Secret Act 1972)*
☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*
☑ OPEN ACCESS I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange

Certified by:

__________________________     ______________________________
SIGNATURE                             SIGNATURE OF SUPERVISOR

__________________________     ______________________________
PASSPORT NO.                             NAME OF SUPERVISOR

Date:                      Date:
"I hereby declare that I have read this project, in my opinion this project report is sufficient in terms of scope and quality for the award of the degree of Master of Computer Science (Information Security)."

Signature : ........................................
Name of Supervisor : DR. Mazdak Zamani
Date : May 2013
AN INTEGRITY BASED RADIO FREQUENCY IDENTIFICATION (RFID) METHOD AGAINST REPLAY ATTACK

SEYED MOSTAFA MIR HOSSEINI

A thesis submitted in partial fulfillment of the requirements for the award of the degree of Master of Computer Science (Information Security)

Advanced Informatics School
Universiti Teknologi Malaysia

MAY 2013
I declare that this project report entitled “An Integrity Based Radio Frequency Identification (RFID) Method Against Replay Attack” is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

Signature : ........................................
Name : Seyed Mostafa Mirhosseini
Date : May 2013
Dedicated to my beloved mother, father, brothers and sisters
ACKNOWLEDGEMENT

First, thank you Allah for giving me strength to take up this challenge and with your blessing to complete this study. Second and foremost, i am deeply indebted to my supervisor, Dr. Mazdak Zamani for his patience in assisting, advising and guiding me throughout this project. Special thanks to my examiners, Associate Professor Dr. Mohd Shahidan Abdullah and PM Dr Salwani Daud for their comments and critics that make this study more comprehensive and precious. To the admin staff of UTM AIS, thank you for your continuous help and kind assistance during my presence in UTM AIS.

To my family, a million thanks for your understanding and ardent support extended to me throughout my journey to accomplish this study. Last but not least i want to thank all of my friends especially all my dear classmate who helped and understood me during this project.
Radio Frequency Identification (RFID) is a new technology field. This emerging technology has been used in different applications. RFID systems have their own security challenges and this research is going to explore integrity attacks in RFID systems. Even though the previous related works have their own strength and weaknesses. The two-factor authentication-based method is proposed to prevent Replay attacks. In this method, necessary processes are mentioned, tag and the reader two-factor authentication by using a security token and integrity would be guaranteed. It can prevent replay attack in RFID systems through using TOTP. In this additional security step legitimate and fake tag will be recognized. Integrity of tag information will be achieved. In addition, Replay attack is prevented by implementing one-time password token. The significant attack such as Replay attack, Tracking attack, MITM attack, Spoofing attack, Impersonation, Cloning, Tampering, Forgery attacks can be achieved when attacker cannot generate a one-time password. This integrity-based RFID method can be used in access control to prevent unauthorized access.
ABSTRAK

# TABLE OF CONTENT

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td></td>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>ACKNOWLEDGEMENTS</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>LIST OF ABBREVIATIONS</td>
<td>xiii</td>
</tr>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Background of the Problem</td>
<td>2</td>
</tr>
<tr>
<td>1.3</td>
<td>Problem Statement</td>
<td>2</td>
</tr>
<tr>
<td>1.4</td>
<td>Research Questions</td>
<td>3</td>
</tr>
<tr>
<td>1.5</td>
<td>Project Objectives</td>
<td>3</td>
</tr>
<tr>
<td>1.6</td>
<td>Project Aim</td>
<td>4</td>
</tr>
<tr>
<td>1.7</td>
<td>Project Scope</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>LITERATURE REVIEW</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>Wireless Technology</td>
<td>6</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Wi-Fi</td>
<td>7</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Bluetooth</td>
<td>8</td>
</tr>
<tr>
<td>2.1.3</td>
<td>RFID</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>RFID Component</td>
<td>9</td>
</tr>
</tbody>
</table>
2.2.1 Active Tag 12
2.2.2 Passive Tag 13
2.2.3 Semi-Active Tag 15
2.2.4 Scanners And Readers 16
2.2.5 Antennas 17
2.2.6 Host 18
2.2.7 RFID Adoption Phases 20
2.2.8 Challenges To RFID Adoption 21

2.3 Classification OF RFID Attack 25
2.3.1 Physical Layer 26
2.3.2 Network Transport Layer 28
2.3.3 Application Layer 29
2.3.4 Strategic Layer 30
2.3.5 Multi-Layer Attacks 32

2.4 Related Works 35
2.4.1 Hash Lock and Randomized Hash Lock 35
2.4.2 PRNG Operation 39
2.4.3 XOR Operation 42
2.4.4 Encryption Technique 43
2.4.5 Zero Knowledge Formulation 47

2.5 One Time Password 54
2.5.1 Mathematical Algorithms Method 55
2.5.2 Time-Synchronized Method 56
2.5.3 Time Based One-Time-Password 56

3 RESEARCH METHODOLOGY 57
3.1 Introduction 57
3.2 Investigation of Current Methods 58
3.3 To Propose a Method 58
3.4 To Evaluate The Proposed Method 59
3.5 Summary of Deliverables 60

4 DESIGN AND IMPLEMENTATION 61
4.1 Introduction 61
4.1.1 TOTP Algorithm Design Description
4.2 Method Design Overview
  4.2.1 Tag And Reader Connection
  4.2.2 Back-End Server
  4.2.3 User Side
  4.2.4 Attacker Side
4.3 Implementation

5 RESULT AND DISCUSSION
  5.1 Introduction
  5.2 Suggested RFID Method
  5.3 Result Evaluation
    5.3.1 Simulation RFID Attack 1
    5.3.2 Simulation RFID Attack 2
  5.4 Analytical Comparison
    5.4.1 Doss et al. Solution Analysis
    5.4.2 Moessner and Khan Solution Analysis
    5.4.3 Doss and Zhou Solution Analysis
    5.4.4 Ning et al. Solution Analysis
    5.4.5 Di Pietro and Molva Solution Analysis
    5.4.6 Doss et al. Solution Analysis
    5.4.7 Ning et al. Solution Analysis
    5.4.8 Yang et al. Solution Analysis
    5.4.9 Liu and Ning Solution Analysis
  5.5 Summary

6 CONCLUSION AND FUTURE WORKS
  6.1 Introduction
  6.2 Project Summary and Conclusion
  6.3 Contribution and Related Achievements
  6.4 Future Works

REFERENCES

Appendices A-B
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Technical Differences Between Barcode and RFID (Wiberg, 2009)</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>Frequency band. (Wu <em>et al.</em>, 2006)</td>
<td>11</td>
</tr>
<tr>
<td>2.3</td>
<td>The RFID Implementation Process (Cheung <em>et al.</em>, 2010)</td>
<td>21</td>
</tr>
<tr>
<td>2.4</td>
<td>Preview of RFID attacks in Literature Review</td>
<td>48</td>
</tr>
<tr>
<td>3.1</td>
<td>Summary Of Deliverables</td>
<td>60</td>
</tr>
<tr>
<td>5.1</td>
<td>Telnet Command</td>
<td>87</td>
</tr>
<tr>
<td>5.2</td>
<td>Method Result</td>
<td>92</td>
</tr>
<tr>
<td>5.3</td>
<td>Method Result</td>
<td>105</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Research scenario overview</td>
<td>4</td>
</tr>
<tr>
<td>2.1</td>
<td>Components of a RFID tag (Wiberg, 2009)</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Components Of An Active Tag (Wiberg, 2009)</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>Components Of A Passive Tag (Wiberg, 2009)</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>Tag’s Price Prediction (Wiberg, 2009)</td>
<td>15</td>
</tr>
<tr>
<td>2.5</td>
<td>Components Of A Semi-Active Tag (Wiberg, 2009)</td>
<td>15</td>
</tr>
<tr>
<td>2.6</td>
<td>Logical components of RFID (Wiberg, 2009).</td>
<td>18</td>
</tr>
<tr>
<td>2.7</td>
<td>Layers of RFID Communication</td>
<td>25</td>
</tr>
<tr>
<td>2.8</td>
<td>Classification of RFID attacks (Mitrokotsa, Rieback, &amp; Tanenbaum, 2010)</td>
<td>26</td>
</tr>
<tr>
<td>2.9</td>
<td>Multi-Layer Attacks</td>
<td>32</td>
</tr>
<tr>
<td>2.10</td>
<td>Doss et al. (2012) Scheme</td>
<td>38</td>
</tr>
<tr>
<td>3.1</td>
<td>Operational Framework</td>
<td>57</td>
</tr>
<tr>
<td>3.2</td>
<td>Investigation Phase</td>
<td>58</td>
</tr>
<tr>
<td>3.3</td>
<td>Proposed Method Phase</td>
<td>59</td>
</tr>
<tr>
<td>3.4</td>
<td>Proposed Method Phase</td>
<td>59</td>
</tr>
<tr>
<td>4.1</td>
<td>Steps for RFID method</td>
<td>63</td>
</tr>
<tr>
<td>4.2</td>
<td>TOTP Algorithm Design Description</td>
<td>64</td>
</tr>
<tr>
<td>4.3</td>
<td>Tag And Reader Connection</td>
<td>66</td>
</tr>
<tr>
<td>4.4</td>
<td>Back-End Server Side</td>
<td>67</td>
</tr>
<tr>
<td>4.5</td>
<td>TOTP Sent</td>
<td>68</td>
</tr>
<tr>
<td>4.6</td>
<td>TOTP Back To Server</td>
<td>68</td>
</tr>
<tr>
<td>4.7</td>
<td>Attacker Side</td>
<td>69</td>
</tr>
<tr>
<td>4.8</td>
<td>Prevent Replay Attack</td>
<td>70</td>
</tr>
<tr>
<td>4.9</td>
<td>Method Overview</td>
<td>70</td>
</tr>
</tbody>
</table>
4.10 TOTP Method Implementation Overview 71
4.11 TOTP Method Implementation Description 71
4.12 Unix Time 72
4.13 Timestamp 73
4.14 Check The Value 73
4.15 Result Message 74
4.16 Numeric keypad 75
4.17 Log File 76
4.18 Result Part 77
4.19 Attack Sample 78
5.1 RFID integrity based method 80
5.2 Rifidi 82
5.3 Starting a Virtual Reader 83
5.4 Select the reader 84
5.5 Supply the reader’s IP and port 85
5.6 Start on the reader to begin 85
5.7 Tag creation wizard 86
5.8 Tags on an Antenna 87
5.9 RawCap Dump File 88
5.10 RawCap screen 89
5.11 Wireshark 90
5.12 Simulation Method 91
5.13 RFDump Live 93
5.14 Rifidi Emulator 94
5.15 virtual serial ports 95
5.16 VMware Workstation 96
5.17 Rfdump Attack 96
5.18 Attack Diagram 97
5.19 Legitimate User and Attacker Condition 104
6.1 Schematic Method 108
# LIST OF ABBREVIATION

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1G2</td>
<td>Class 1 Generation 2</td>
</tr>
<tr>
<td>DCAP</td>
<td>Dual Cryptography Authentication Protocol</td>
</tr>
<tr>
<td>DDOS</td>
<td>Distributed Denial-Of-Service</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EPC</td>
<td>Electronic Product Code</td>
</tr>
<tr>
<td>FAR</td>
<td>False Acceptance Rate</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field-Programmable Gate Array</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
</tr>
<tr>
<td>HMAC</td>
<td>Keyed-Hashing for Message Authentication</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>KAAP</td>
<td>Key Array Authentication Protocol</td>
</tr>
<tr>
<td>OTP</td>
<td>One Time Password</td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable Authentication Modules</td>
</tr>
<tr>
<td>PRNG</td>
<td>Pseudorandom Number Generators</td>
</tr>
<tr>
<td>PUF</td>
<td>Physical Unclonable Function</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>RNG</td>
<td>Pseudorandom Number Generators</td>
</tr>
<tr>
<td>ROC</td>
<td>Receiver Operating Characteristic</td>
</tr>
<tr>
<td>ROI</td>
<td>Return On Investment</td>
</tr>
<tr>
<td>SAPCC1G2</td>
<td>Secure Authentication Protocol Conforming To EPC C1G2</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>SSL</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TOPT</td>
<td>Time-based One-time Password</td>
</tr>
<tr>
<td>ZKAP</td>
<td>Zero-Knowledge Authentication Protocol</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Overview

Wireless telecommunications is the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters of the television remote control, or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants, and wireless networking (Shelly et al., 2011).

Radio Frequency Identification (RFID) is one type of wireless network that classify in short range wireless. RFID networks exist in a broad range of environments and their rapid proliferation has been underway for quite some time. RFID systems consist of tiny integrated circuits equipped with antennas (RFID tags), that communicate with their reading devices (RFID readers) using electromagnetic fields at one of several standard radio frequencies. Additionally, there is usually a back-end database that collects information related to the physically tagged objects (Song & Mitchell, 2008).
1.2 Background of the Problem

Radio Frequency Identification (RFID) is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object (Hua and Hong, 2012).

RFID tags are used in many industries. Since RFID tags can be attached to clothing, possessions, or even implanted within people, the possibility of reading personally-linked information without consent has raised security concerns (Hua and Hong, 2012).

Not only vital information privacy, protection solutions, detection the risks and threats are the popular issues in RFID technique but also authentication through the insecure wireless channel and data integrity are the sensitive challenges.

Tag and reader are two critical items of RFID because they are vulnerable to the threat of data counterfeiting. On the other hand read and write and alter the data will be occurred without any permit that is a big threat for the user. People’s important belongings should be protected against modification.

Although the above problems do not cover all concerns about this technology, but from the security point of view, data integrity and modification are the important problems that should be considered.

1.3 Problem Statement

A common defense approach to attacks is the use of a previous response protocol. RFID tags and readers usually share a secret and use a challenge response protocol to authenticate their identities. Nevertheless, very often this approach is
subject to Replay attacks. In a Replay attack, an adversary broadcasts a tag’s response recorded from a past transaction in order to impersonate the tag to a reader. Typical example of this attack is the unauthorized access to restricted areas by broadcasting an exact Replay of the radio signal sent from a legitimate tag to the reader that grants access (van Deursen and Radomirović, 2009).

There are some attacks on RFID like Replay attack and cloning attack that focus on integrity of RFID. In replay attack an adversary can repeated previous transaction to impersonate the tag to the reader (Replay attack) that compromise integrity which is a big problem in information security. This research will focus on Replay attack and will try to provide a solution against it.

1.4 Research Questions

Research questions related to this project is listed as below:

- What are the available current RFID attack and techniques had been used?

- Why RFID is affected by Replay attack?

- How we can improve security?

1.5 Project Objectives

During this project to achieve the aim the following step is intended:

- To identify current attacks on RFID and investigate existing technique against these attacks
- To propose a new method to prevent Replay attack on RFID
- To test and evaluate proposed method by creating simulation attacks

### 1.6 Project Aim

The main contribution of my study is developing a method against replay attack. In following paper, there is implementation a method for increase security on RFID base on one time password as shown in Figure 1.1.

![Research scenario overview](image)

**Figure 1.1** : Research scenario overview

### 1.7 Project Scope

The scope of this study focuses on the integrity of data transmission between tags and readers in RFID technology. In RFID three concepts should be considered:
Confidentiality, Integrity, and Availability (CIA). Therefore attacks can be divided by the CIA.

Eavesdropping, unauthorized tag reading, and privacy threats are several attacks that influence confidentiality in authentication and communication sector. Traceability and collection of personal information are the privacy threat’s capabilities. DDOS attack and Dos attack are threats that can influence Availability. Replay attack and cloning attack are threats that influence integrity. The scope explains the identification of significant security threats and their solutions to prevent information modification and integrity issues.

In following this research focus on one time password and use TOTP to prevent common attacks and finally proposed method will be evaluated in simulation environment.


Cheung, W., Chu, S.-C. and Du, T. C. (2010). Three Phases RFID Adoption: A Road Map to Success.


