ENHANCING THE SECURITY OF RCIA ULTRA-LIGHTWEIGHT AUTHENTICATION PROTOCOL BY USING RANDOM NUMBER GENERATOR (RNG) TECHNIQUE

SHAYMAH AKRAM YASEAR

MASTER IN INFORMATION TECHNOLOGY (IT)
UNIVERSITI UTARA MALAYSIA
2015
Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Abstrak


Kata kunci: RFID, ultra-ringan, protocol, nombor rawak, kemungkinan serangan
Abstract

With the growing demand for low-cost Radio Frequency Identification (RFID) system, there is a necessity to design RFID ultra-lightweight authentication protocols to be compatible with the system and also resistant against possible attacks. However, the existing ultra-lightweight authentication protocols are susceptible to wide range of attacks. This study is an attempt to enhance the security of Robust Confidentiality, Integrity, and Authentication (RCIA) ultra-lightweight authentication protocols especially with regard to privacy issue. In the RCIA protocol, IDs value is sent between reader and tag as a constant value. The constant value will enable attacker to trace the location of the tag which violates the privacy users. In order to enhance the security of RCIA protocol, Random Number Generator (RNG) technique has been used. This technique relies on generating random numbers in the tag side, based on Bitwise operations. The idea of this technique is to change the IDs of a tag on every query session so that it will not stay as a constant value. The implementation of Enhanced RCIA has been conducted by using a simulation. The simulation provided the ability to show that the operations of RCIA protocol as to compare with the enhanced RCIA. The outcome shows that the enhanced RCIA outperforms existing one in terms of privacy.

**Keywords**: RFID, ultra-lightweight, protocol, random number, traceability attack.
Acknowledgement

I would like to express my sincere thanks and appreciation to my supervisor Dr. Nur Haryani Zakaria for her guidance, support and the many helpful discussions throughout the course of this study.

I take this opportunity to express my gratitude to Dr. Mohd Nizam for his help in the preparation of this work.

I wish to thank my parents for their persistence encouragement and patience throughout. Special thank is also extended for my lovely sister Zainab for her encouragement, motivation and precious advices.

Shayma Akram
Table of Contents

PERMISSION TO USE .......................................................................................................................... II
ABSTRACT ........................................................................................................................................ IV
ACKNOWLEDGEMENT ..................................................................................................................... V
TABLE OF CONTENTS ..................................................................................................................... VI
LIST OF TABLES ............................................................................................................................. IX
LIST OF FIGURES ........................................................................................................................... X
LIST OF ABBREVIATIONS ............................................................................................................... XI

CHAPTER ONE INTRODUCTION ............................................................................................... 1
  1.1. Introduction ............................................................................................................................. 1
  1.2 Background of RFID Technology .......................................................................................... 1
  1.3. Problem Statement ............................................................................................................... 4
  1.4. Research Questions .............................................................................................................. 5
  1.5. Research Objectives ............................................................................................................ 5
  1.6. Scope of the Study ............................................................................................................... 6
  1.7. Significance of the Study .................................................................................................... 6
  1.8. Summary ............................................................................................................................... 7

CHAPTER TWO LITERATURE REVIEW ...................................................................................... 8
  2.1. Introduction ............................................................................................................................ 8
  2.2. Radio Frequency Identification (RFID) System ................................................................... 8
  2.3. Classification of RFID Authentication Protocols ............................................................... 11
2.5. Attacks on Ultra-Lightweight Authentication Protocols

2.5.1. Traceability Attack

2.5.2. Impersonation Attack

2.5.3. Disclosure Attack

2.5.4. Desynchronization Attack

2.6. Ultra-Lightweight Authentication Protocols

2.7. Summary

CHAPTER THREE RESEARCH METHODOLOGY

3.1. Introduction

3.2. Phase 1 – Conceptual Design

3.3. Phase 2 – Implementation of RNG

3.5. Phase 3 – Evaluation

3.6. Summary

CHAPTER FOUR RESULT & ANALYSIS

4.1. Introduction

4.2. The Random Number Generator (RNG) Technique

4.2.1. XOR-Shift* Algorithm

4.3. Implementation of the RNG

4.4. Evaluation

1.5 Summary

CHAPTER FIVE DISCUSSION & CONCLUSION

5.1. Introduction

5.2. Discussion

5.3 Research Contribution
5.5. Future Work .......................................................................................................... 51

5.6. Conclusion ............................................................................................................ 52

5.7. Summary ............................................................................................................... 52

APPENDICE SOURCE CODE ................................................................................ 57
List of Tables

Table 2.1 Type of RFID Tag ................................................................. 10
Table 2.2 Characteristics of Ultra-Lightweight Authentication Protocols .......... 11
Table 2.3 The Main Notation in the Ultra-lightweight Authentication Protocols ......................................................... 14
Table 2.5 Attacks Resistance Comparison between ultra-lightweight authentication Protocols ............................................................................................................. 26
Table 4.1 Bitwise Operations................................................................................. 35
Table 4.2 Evaluation scenario.................................................................................. 42
Table 4.3 The Query Results of the Tag Using RCIA and enhanced RCIA .......... 45
List of Figures

Figure 2.1. RFID System Components ................................................................. 9
Figure 2.2. RFID tag components ....................................................................... 9
Figure 2.3. Classifications of RFID Authentication Protocols [8] ...................... 11
Figure 2.4. Ultra-Lightweight Authentication Protocols .................................... 14
Figure 2.5. LMAP protocol ................................................................................. 15
Figure 2.6. EMAP Protocol ................................................................................ 16
Figure 2.7. SASI protocol .................................................................................... 18
Figure 2.8. Gossamer protocol .......................................................................... 19
Figure 2.9. David-Prasad Protocol ................................................................... 20
Figure 2.10. Permutation function ...................................................................... 21
Figure 2.11. RAPP Protocol .............................................................................. 22
Figure 2.12. Recursive hash function Rh() ......................................................... 23
Figure 2.13. RCIA Protocol ................................................................................ 25
Figure 2.14. Operations of RCIA Protocol ........................................................... 26
Figure 3.3. Phases of The Study ......................................................................... 29
Figure 3.1. Summary of Enhanced RCIA ............................................................... 30
Figure 3.2. The Structure of The Simulation Tool .................................................. 32
Figure 4.1. Random Number Generator (RNG) .................................................... 35
Figure 4.2. XOR-Shift* Algorithm ...................................................................... 36
Figure 4.3. The Role of RNG in Enhanced RCIA ............................................... 37
Figure 4.4. The processes of Enhanced RCIA ....................................................... 39
Figure 4.5. The Main Interface of the Prototype .................................................... 40
Figure 4.6. The Interface of RCIA ...................................................................... 40
Figure 4.7. The interface of The Enhanced RCIA .................................................. 41
Figure 4.8(a). First Query Session of Simulated RCIA ....................................... 44
Figure 4.8(b). Second Query Session of Simulated RCIA ................................... 44
Figure 4.9(a). First Query Session of Simulated Enhanced RCIA ...................... 45
Figure 4.9(b). Second Query Session of Simulated Enhanced RCIA ............... 45
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIDC</td>
<td>Automatic Identification and Data Capture</td>
</tr>
<tr>
<td>AVISPA</td>
<td>Automated Validation of Internet Security Protocols and Applications</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate authority</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Code</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial-of-Service</td>
</tr>
<tr>
<td>EMAP</td>
<td>Efficient mutual authentication protocol</td>
</tr>
<tr>
<td>GA</td>
<td>Good approximations</td>
</tr>
<tr>
<td>IFF</td>
<td>Identify friend or foe</td>
</tr>
<tr>
<td>LMAP</td>
<td>Lightweight Mutual Authentication protocol</td>
</tr>
<tr>
<td>LSB</td>
<td>Least Significant Bit</td>
</tr>
<tr>
<td>MSB</td>
<td>Most Significant Bit</td>
</tr>
<tr>
<td>OCR</td>
<td>Optical Character Recognition</td>
</tr>
<tr>
<td>RAD</td>
<td>Rapid Application Development</td>
</tr>
<tr>
<td>RAPP</td>
<td>RFID authentication protocol with permutation</td>
</tr>
<tr>
<td>RCIA</td>
<td>Robust Confidentiality, Integrity, and Authentication</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>RNG</td>
<td>Random Number Generator</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Rn</td>
<td>Random Number</td>
</tr>
<tr>
<td>SASI</td>
<td>Strong Authentication and Strong Integrity</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>UMAP</td>
<td>Ultra-lightweight Mutual Authentication Protocol</td>
</tr>
</tbody>
</table>
CHAPTER ONE
INTRODUCTION

1.1. Introduction
This chapter will involve studying the background of Radio Frequency Identification (RFID) technology, additionally, the topics that will be covered are statement of the problem, research questions, research objectives, significance of research, and scope of the study.

1.2 Background of RFID Technology
The evolution of technology has contributed in reducing the gap between the physical and digital worlds [1]. One manifestation of this convergence is emerging a new technology that helps to identify objects automatically without the need for human intervention. This technology, called Automatic Identification and Data Capture (AIDC) or also known as "Auto-ID." This technology includes RFID, bar codes, magnetic stripes, Optical Character Recognition (OCR), voice recognition, biometrics, and smart cards. One of the most important relatively recent additions to Auto-ID technologies is RFID Technology. RFID is a communications technology that depends on radio waves to collect data automatically without the need for contact [2].

The origins of RFID technology dating back to the 19th century, which was during the Second World War when British Royal Air Force deployed "identify friend or foe" (IFF) system. This system was the first usage of RFID technology, which helped in distinguishing between the enemy and friendly aircraft [3]. In 1973, Mario Cardullo
The contents of the thesis is for internal user only
5.6. Conclusion

This study aimed to enhance the security of RCIA ultra-lightweight authentication protocol. This objective has achieved by adopting random number generator (RNG) technique. The RNG produced based on XOR-Shift* algorithm and used to provide a variable values for IDs. The RNG technique helped in preventing a traceability attack and as a result, solves a privacy issue.

The implementation of RNG technique has been conducted by using simulation technique. In order to provide a comparison between RCIA and enhanced RCIA, the simulation included simulating the operations of both protocols. Furthermore, the simulation used to evaluate the enhanced RCIA. The result of simulated enhanced RCIA showed that the RNG technique has successfully prevented the traceability attack.

5.7. Summary

This chapter has presented the overall discussion of the study. Along the discussion was done, the objectives of the study was also addressed to indicate that all were successfully carried out. Also included in this chapter was the contribution of this study. This chapter end with a highlight on future work as well some a brief conclusion to end the chapter.

REFERENCES


