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

Dengan permintaan yang semakin meningkat untuk sistem Pengenalpastian Frequensi Radio (RFID), terdapat keperluan untuk merekabentuk protokol pengesahan Pengenalpastian Frequensi Radio Ultra-ringan supaya ianya menjadi lebih serasi dengan sistem dan juga mampu bertahan terhadap kemungkinan serangan. Walaubagaimana pun, protokol pengesahan Pengenalpastian Frequensi Radio Ultra-ringan yang sedia ada amat terdedah kepada pelbagai serangan. Oleh itu, kajian ini adalah sebagai satu usaha untuk meningkatkan keselamatan protokol Kerahsiaan Teguh, Integriti, dan Pengesahan (RCIA) terutama yang berkaitan dengan isu-isu privasi. Dalam protokol RCIA, nilai *IDs* dihantar melalui pembaca dan *tag* sebagai nilai malar. Nilai malar ini membolehkan penyerang untuk mengesan lokasi *tag* yang akhirnya menceroboh privasi pengguna. Dalam usaha untuk meningkatkan keselamatan protokol RCIA, teknik Penjanaan Nombor Rawak (RNG) telah digunakan. Teknik ini bergantung kepada penjanaan nombor rawak di bahagian sebelah *tag*, menggunakan operasi *Bitwise*. Idea teknik ini adalah untuk menukar *IDs tag* pada setiap sesi pertanyaan supaya ia tidak akan kekal sebagai nilai malar. Pelaksanaan penambahbaikkan RCIA telah dilaksanakan dengan menggunakan teknik simulasi. Teknik simulasi ini menyediakan keupayaan untuk membandingkan operasi protokol RCIA sedia ada dengan inovasi RCIA yang baru. Hasilnya menunjukkan bahawa inovasi RCIA terbukti mampu mengatasi keupayaan sistem keselamatan yang sedia ada.

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 12
2.5.1. Traceability Attack 12
2.5.2. Impersonation Attack 12
2.5.3. Disclosure Attack 12
2.5.4. Desynchronization Attack 13

2.6. Ultra-Lightweight Authentication Protocols 13

2.7. Summary 27

CHAPTER THREE RESEARCH METHODOLOGY 28

3.1. Introduction 28

3.2. Phase 1 – Conceptual Design 29

3.3. Phase 2 – Implementation of RNG 30

3.5. Phase 3 – Evaluation 32

3.6. Summary 33

CHAPTER FOUR RESULT & ANALYSIS 34

4.1. Introduction 34

4.2. The Random Number Generator (RNG) Technique 34
4.2.1. XOR-Shift* Algorithm 36

4.3. Implementation of the RNG 37

4.4. Evaluation 42

1.5 Summary 47

CHAPTER FIVE DISCUSSION & CONCLUSION 47

5.1. Introduction 48

5.2. Discussion 48
5.3 Research Contribution 50

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 Authenticaion 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

LIST OF ABBREVIATIONS

AIDC	Automatic Identification and Data Capture
AVISPA	Automated Validation of Internet Security Protocols and Applications
CA	Certificate authority
CRC	Cyclic Redundancy Code
DoS	Denial-of-Service
EMAP	Efficient mutual authentication protocol
GA	Good approximations
IFF	Identify friend or foe
LMAP	Lightweight Mutual Authentication protocol
LSB	Least Significant Bit
MSB	Most Significant Bit
OCR	Optical Character Recognition
RAD	Rapid Application Development
RAPP	RFID authentication protocol with permutation
RCIA	Robust Confidentiality, Integrity, and Authentication
RFID	Radio Frequency Identification
RNG	Random Number Generator

Rn	Random Number
SASI	Strong Authentication and Strong Integrity
UHF	Ultra High Frequency
UMAP	Ultra-lightweight Mutual Authentication Protocol

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

[1] S. A. Weis, "Security and privacy in radio-frequency identification devices," Massachusetts Institute of Technology, 2003.

[2] F. Thornton and P. Sanghera, *How to Cheat at Deploying and Securing RFID*: Syngress, 2011.

[3] S. A. Weis, "RFID (Radio Frequency Identification): Principles and applications," *Retrived from www. eecs. harvard. edu/rfid-article. pd f on,* vol. 1, 2011.

[4] P. R. Agarwal and P. R. Agarwal, "RFID (Radio Frequency Identification) growth in daily life," *International Journal of Scientific Engineering and Technology,* vol. 1, pp. 71-78, 2012.

[5] A. Alqarni, M. Alabdulhafith, and S. Sampalli, "A Proposed RFID Authentication Protocol based on Two Stages of Authentication," *Procedia Computer Science,* vol. 37, pp. 503-510, 2014.

[6] United States Government Accountability Office, "Information Security: Radio Frequency Identification Technology in the Federal Government," Washington GAO-05-551, May 2005.

[7] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and A. Ribagorda, "Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol," in *Information security applications*, ed: Springer, 2009, pp. 56-68.

[8] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *Dependable and Secure Computing, IEEE Transactions on,* vol. 4, pp. 337-340, 2007.

[9] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," in *RFID privacy workshop*, 2003.

[10] M. David and N. R. Prasad, "Providing strong security and high privacy in low-cost RFID networks," in *Security and privacy in mobile information and communication systems*, ed: Springer, 2009, pp. 172-179.

[11] Y. Tian, G. Chen, and J. Li, "A new ultralightweight RFID authentication protocol with permutation," *Communications Letters, IEEE,* vol. 16, pp. 702-705, 2012.

[12] U. Mujahid, M. Najam-ul-Islam, and M. A. Shami, "RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash," *International Journal of Distributed Sensor Networks,* vol. 2015, 2015.

[13] A. Juels and S. A. Weis, "Authenticating pervasive devices with human protocols," in *Advances in Cryptology–CRYPTO 2005*, 2005, pp. 293-308.

[14] S. Kinoshita, M. Ohkubo, F. Hoshino, G. Morohashi, O. Shionoiri, and A. Kanai, "Privacy enhanced active RFID tag," *Cognitive Science Research Paper-University of Sussex CSRP*, vol. 577, p. 100, 2005.

[15] S. Kumar and C. Paar, "Are standards compliant elliptic curve cryptosystems feasible on RFID," in *Workshop on RFID Security-RFIDSec*, 2006.

[16] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," in *Security in Pervasive Computing*, ed: Springer, 2005, pp. 70-84.

[17] H.-Y. Chien, "Secure access control schemes for RFID systems with anonymity," in *null*, 2006, p. 96.

[18] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005, pp. 74-88.

[19] J. Bringer, H. Chabanne, and E. Dottax, "HB^+^+: a Lightweight Authentication Protocol Secure against Some Attacks," in *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on*, 2006, pp. 28-33.

[20] J. Munilla and A. Peinado, "HB-MP: A further step in the HB-family of lightweight authentication protocols," *Computer Networks*, vol. 51, pp. 2262-2267, 2007.

[21] H.-Y. Chien and C.-H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards," *Computer Standards & Interfaces*, vol. 29, pp. 254-259, 2007.

[22] M. Hutter and J.-M. Schmidt, *Radio Frequency Identification: Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers* vol. 8262: Springer, 2013.

[23] X. Zhuang, Z.-H. Wang, C.-C. Chang, and Y. Zhu, "Security analysis of a new ultra-lightweight RFID protocol and its improvement," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, pp. 166-177, 2013.

[24] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in *Workshop on RFID security*, 2006, pp. 12-14.

[25] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An efficient mutual-authentication protocol for low-cost

RFID tags," in *On the move to meaningful internet systems 2006: Otm 2006 Workshops*, 2006, pp. 352-361.

[26] T. Li, G. Wang, and R. H. Deng, "Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols," *JSW*, vol. 3, pp. 1-10, 2008.

[27] T. Cao, E. Bertino, and H. Lei, "Security analysis of the SASI protocol," *Dependable and Secure Computing, IEEE Transactions on*, vol. 6, pp. 73-77, 2009.

[28] G. Avoine, X. Carpent, and B. Martin, "Strong authentication and strong integrity (SASI) is not that strong," in *Radio Frequency Identification: Security and Privacy Issues*, ed: Springer, 2010, pp. 50-64.

[29] H.-M. Sun, W.-C. Ting, and K.-H. Wang, "On the security of Chien's ultralightweight RFID authentication protocol," *IEEE Transactions on Dependable and Secure Computing*, pp. 315-317, 2009.

[30] G. Avoine, X. Carpent, and B. Martin, "Privacy-friendly synchronized ultralightweight authentication protocols in the storm," *Journal of Network and Computer Applications*, vol. 35, pp. 826-843, 2012.

[31] E. Taqieddin and J. Sarangapani, "Vulnerability analysis of two ultra-lightweight RFID authentication protocols: RAPP and gossamer," in *Internet Technology And Secured Transactions, 2012 International Conference for*, 2012, pp. 80-86.

[32] K.-H. Yeh and N. Lo, "Improvement of two lightweight RFID authentication protocols," *Information Assurance and Security Letters*, vol. 1, pp. 6-11, 2010.

[33] Z. Bilal, A. Masood, and F. Kausar, "Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol," in *Network-Based Information Systems, 2009. NBIS'09. International Conference on*, 2009, pp. 260-267.

[34] M. Zubair, E. U. Mujahid, and J. Ahmed, "Cryptanalysis of RFID Ultra-lightweight Protocols and Comparison between its Solutions Approaches," *Bahria University Journal of Information & Communication Technologies*, vol. 5, pp. 58-63, 2012.

[35] J. C. Hernandez-Castro, P. Peris-Lopez, R. C.-W. Phan, and J. M. Tapiador, "Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol," in *Radio Frequency Identification: Security and Privacy Issues*, ed: Springer, 2010, pp. 22-34.

[36] D. F. Barrero, J. C. Hernández-Castro, P. Peris-Lopez, and D. Camacho, "A genetic tango attack against the David–Prasad RFID ultra-lightweight authentication protocol," *Expert Systems*, vol. 31, pp. 9-19, 2014.

[37] G. Avoine and X. Carpent, "Yet another ultralightweight authentication protocol that is broken," in *Radio Frequency Identification. Security and Privacy Issues*, ed: Springer, 2013, pp. 20-30.

[38] W. Shao-hui, H. Zhijie, L. Sujuan, and C. Dan-wei, "Security analysis of RAPP an RFID authentication protocol based on permutation," *College of computer, Nanjing University of Posts and Telecommunications, Nanjing*, vol. 210046, 2012.

[39] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Desynchronization attack on RAPP ultralightweight authentication protocol," *Information processing letters*, vol. 113, pp. 205-209, 2013.

[40] G. Marsaglia, "Xorshift rngs," *Journal of Statistical Software*, vol. 8, pp. 1-6, 2003.

[41] S. Vigna, "An experimental exploration of Marsaglia's xorshift generators, scrambled," *arXiv preprint arXiv:1402.6246*, 2014.

[42] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in pervasive computing*, ed: Springer, 2004, pp. 201-212.