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.	**Dr.Mazdak Zamani** **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.

ABSTRACT

Radio Frequency Identification (RFID) is a new in technology field. This emerging technology has been use 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

Radio Frequency Identification (RFID) adalah satu perkara yang baru dalam bidang teknologi. Teknologi baru ini telah digunakan dalam aplikasi yang berbeza. Sistem RFID mempunyai cabaran-cabaran keselamatan mereka sendiri dan kajian ini akan meneroka serangan integriti dalam sistem RFID. Walaupun kerja-kerja yang berkaitan sebelum ini mempunyai kekuatan sendiri dan kelemahan mereka.Kedua-dua faktor kaedah berasaskan pengesahan adalah dicadangkan untuk mencegah serangan Ulangan. Dalam kaedah ini, proses yang perlu disebut, tag dan pembaca dua faktor pengesahan dengan menggunakan tanda keselamatan dan integriti akan dijamin. Ia boleh mencegah serangan ulangan dalam sistem RFID melalui menggunakan TOTP. Dalam kes ini, langkah keselamatan tambahan tag sah dan palsu akan diiktiraf. Integriti maklumat tag akan tercapai. Di samping itu, serangan Ulangan dihalang dengan melaksanakan token kata laluan satu-satu masa. Serangan penting seperti serangan Ulangan, serangan Penjejakan, serangan MITM, serangan Menipu, Penyamaran, Pengklonan, Mengganggu, serangan Pemalsuan boleh dicapai apabila penyerang tidak boleh menjana kata laluan satu masa. Ini berasaskan kaedah RFID integriti boleh digunakan untuk mencegah dan menghalang akses capaian yang tidak dibenarkan.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

C1G2	-	Class 1 Generation 2
DCAP	-	Dual Cryptography Authentication Protocol
DDOS	-	Distributed Denial-Of-Service
DoS	-	Denial of Service
EPC	-	Electronic Product Code
FAR	-	False Acceptance Rate
FPGA	-	Field-Programmable Gate Array
FRR	-	False Rejection Rate
HMAC		Keyed-Hashing for Message Authentication
HTTP	-	Hypertext Transfer Protocol
KAAP	-	Key Array Authentication Protocol
OTP	-	One Time Password
PAM	-	Pluggable Authentication Modules
PRNG	-	Pseudorandom Number Generators
PUF	-	Physical Unclonable Function
RFID	-	Radio Frequency Identification
RNG	-	Pseudorandom Number Generators
ROC	-	Receiver Operating Characteristic
ROI	-	Return On Investment
SAPCC1G2	-	Secure Authentication Protocol Conforming To EPC C1G2

SSL	-	Transport Layer Security
TOPT	-	Time-based One-time Password
ZKAP	-	Zero-Knowledge Authentication Protocol

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.

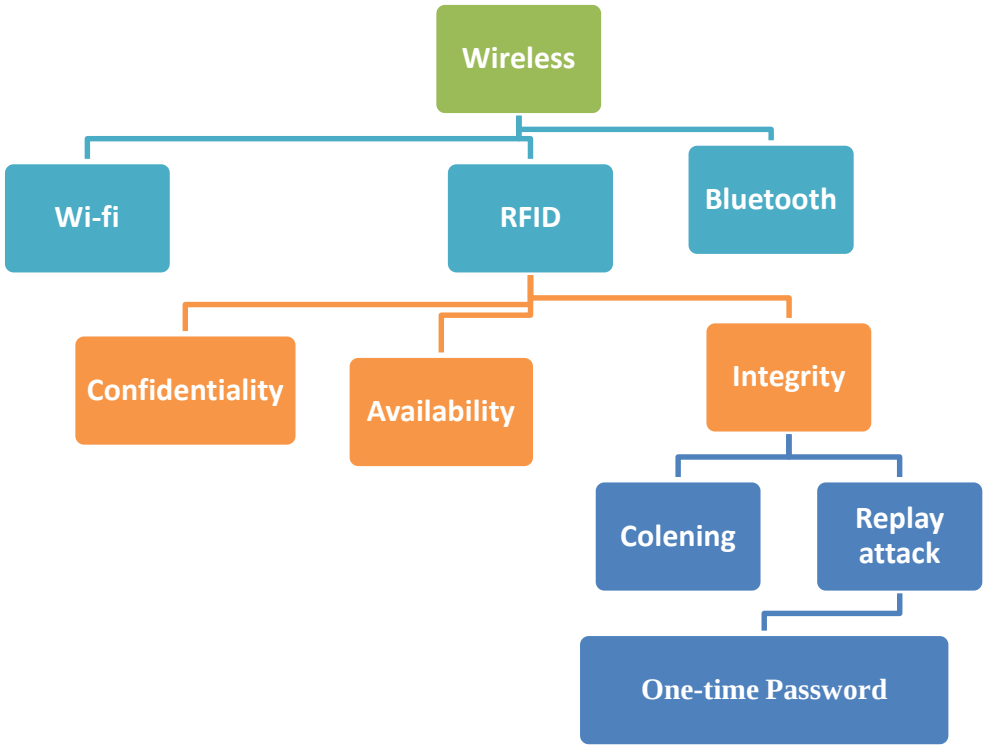

Figure 1.1 : Research scenario overview

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.

REFERENCES

Ahson, S. A. and Ilyas, M. (2008). RFID handbook: applications, technology, security, and privacy: CRC.

Attaran, M. (2007). RFID: an enabler of supply chain operations. *Supply Chain Management: An International Journal*, 12(4), 249-257 .

Burmester, M., De Medeiros, B., Munilla, J. and Peinado, A. (2009). Secure EPC Gen2 compliant radio frequency identification. Proceedings of the 2009 *8th International Conference on Ad-Hoc, Mobile and Wireless Networks, ADHOC-NOW 2009, September 22, 2009 - September 25, 20* 09Murcia, Spain, 227-240.

Chen, X., Su, Y., Xiong, H., Yao, Y., Liu, G. and Yue, M. (2010). An improved authentication approach to enhance security and privacy in RFID system. Proceedings of the 2010 *2010 2nd International Conference on Intelligent Human-Machine Systems and Cybernetics, IHMSC 2010, August 26, 2010 - August 28, 2010* Nanjing, China, 217-220.

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

Di Pietro, R. and Molva, R. (2011). An optimal probabilistic solution for information confinement, privacy, and security in RFID systems. *Journal of Network and Computer Applications*, 34(3), 853-863. doi: 10.1016/j.jnca.2010.04.015

Doss, R., Sundaresan, S. and Zhou, W. (2013). A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. *Ad Hoc Networks*, 11(1), 383-396. doi: 10.1016/j.adhoc.2012.06.015

Doss, R. and Zhou, W. (2012). A secure tag ownership transfer scheme in a closed loop RFID system. Proceedings of the 20 2012 12*IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2012, April 1, 2012 - April 1, 2012* Paris, France, 164-169.

Doss, R., Zhou, W., Sundaresan, S., Yu, S. and Gao, L. (2012). A minimum disclosure approach to authentication and privacy in RFID systems. *Computer Networks*, 56(15), 3401-3416. doi: 10.1016/j.comnet.2012.06.018

Doss, R., Zhou, W., Yu, S. and Gao, L. (2011). A novel mutual authentication scheme with minimum disclosure for RFID systems. Proceedings of the 2011 *2011 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2011, December 6, 2011 - December 9, 2011* Adelaide, SA, Australia, 544-549.

Gao, H. D., Guo, Y. J., Cui, J. Q., Hao, H. G. and Shi, H. (2012). A communication protocol of RFID systems in internet of things. *International Journal of Security and its Applications*, 6(2), 91-102 .

Gong, J., Chen, G., Li, L. and Li, J. (2011). A secure authentication protocol for RFID based on Trivium. Proceedings of the 2011 *2 011International Conference on Computer Science and Service System, CSSS 2011, June 27, 2011 - June 29, 2011* Nanjing, China, 107-109.

Hua, L. and Hong, X. (2012). Application of apparel network customization based on the Internet of Things. Proceedings of the 2012 *Computer Science & Education (ICCSE), 2012 7th International Conference on*, 888-892.

Huey, K. J., Ismail, W. and Rahman, M. G. (2011). Fingerprint-based mutual authentication RFID protocol. Proceedings of the 2011 *2011 IEEE International Conference on Signal Processing, Communications and Computing, ICSPCC 2011, September 14, 2011 - September 16, 2011* Xi'an, China, IEEE Xi'an Section; IEEE Hong Kong Section; Northwestern Polytechnical University; Xidian University; Xi'an Jiaotong University.

Jialiang, H., Dantong, O. and Haiyan, W. (2012). A RFID authentication protocol with index inner table used in reader. *International Journal of Digital Content Technology and its Applications*, 6(2), 119-127. doi: 10.4156/jdcta.vol6.issue2.15

Jin, Y., Xin, W ,.Sun, H. and Chen, Z. (2012). PUF-based RFID authentication protocol against secret key leakage. Proceedings of the 2012 *14th Asia Pacific Web Technology Conference, APWeb 2012, April 11, 2012 - April 13, 2012* Kunming, China, 318-329.

Jones, E. C. and Chung, C. A. (2007). RFID *in logistics: a practical introduction*: CRC.

Khor, J. H., Ismail, W. and Rahman, M. G. (2012). Prevention and detection methods for enhancing security in an RFID system. *International Journal of Distributed Sensor Networks*, 2012 .doi: 10.1155/2012/891584

Kim, C.-J., Yun, S.-Y. and Park, S.-C. (2010). A lightweight ECC algorithm for mobile RFID service. Proceedings of the 2010 *5th International Conference on Ubiquitous Information Technologies and Applications, CUTE 2010, December* - 2010 ,16 *December 18, 2010* Sanya, China ,

Lai, Y.-C. and Lin, C.-C. (2011). Secure coexistence proofs for RFID tags. *ICIC Express Letters*, 5(4 B), 1441-1448 .

Lee, K. (2010). A two-step mutual authentication protocol based on randomized hash-lock for small RFID networks. Proceedings of the 2010 *4th International Conference on Network and System Security, NSS 2010, September 1, 2010 - September 3, 2010* Melbourne, VIC, Australia, 527-533.

Li, J.-S. and Liu, K.-H. (2011). A hidden mutual authentication protocol for low-cost RFID tags. *International Journal of Communication Systems*, 24(9), 1196-1211. doi: 10.1002/dac.1222

Lien, Y.-H., Leng, X., Mayes, K. E. and Chiu, J.-H. (2011). Select-response grouping proof and its verification protocol for RFID tags. *International Journal of Intelligent Information and Database Systems*, 5(2), 101-118. doi: 10.1504/ijiids.2011.038967

Liu, H. and Ning, H. (2011). Zero-knowledge authentication protocol based on alternative mode in RFID systems. *IEEE Sensors Journal*, 11(12 .3245-3235 ,(doi: 10.1109/jsen.2011.2160052

Luo, J. N. and Yang, M. H. (2012). Mobile RFID mutual authentication and ownership transfer. *International Journal of Advancements in Computing Technology*, 4(7), 28-40. doi: 10.4156/ijact.vol4.issue7.4

M'Raihi ,D., Bellare, M., Hoornaert, F., Naccache, D. and Ranen, O. (2005). Hotp: An hmac-based one-time password algorithm. *The Internet Society, Network Working Group. RFC4226* .

Macari, J. (2012). *Wireless Internet/Technology*, 2012, from http://www.uri.edu/personal/jmac7019/FinalWebpage.htm

Mitrokotsa, A., Rieback, M. R. and Tanenbaum, A. S. (2010). Classification of RFID attacks. *Gen*, 15693, 14443 .

Moessner, M. and Khan, G. N. (2012). Secure authentication scheme for passive C1G2 RFID tags. *Computer Networks* .286-273 ,(1)56 ,doi: 10.1016/j.comnet.2011.09.008

Morshed, M. M., Atkins, A. and Yu, H.-N. (2012). An efficient and secure authentication protocol for RFID systems. *International Journal of Automation and Computing*, 9(3), 257-265. doi: 10.1007/s11633-0124-0642-

Najafi, V., Jenabi, M., Mohammadi, S., Fotowat-Ahmady, A. and Marvasti, M. B. (2008). A dual mode EPC Gen 2 UHF RFID transponder in 0.18 μm CMOS. Proceedings of the 2008 *Electronics, Circuits and Systems, 2008. ICECS 2008. 15th IEEE International Conference on*, 1135-1138.

Ning, H., Liu, H., Mao, J. and Zhang, Y. (2011). Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems. *IET Communications*, 5(12), 1755-1768. doi: 10.1049/iet-com.2010.0625

Ning, H., Liu, H. and Yang, C. (2011). Ultralightweight RFID authentication protocol based on Random partitions of pseudorandom identifier and pre-shared secret value. *Chinese Journal of Electronics*, 20(4), 701-707 .

Ning, H., Liu, H., Yang, L. T. and Zhang, Y. (2012). Dual cryptography authentication protocol and its security analysis for radio frequency identification systems. *Concurrency Computation Practice and Experience*, 24(17), 2040-2054. doi: 10.1002/cpe.1827

Quan, Q., Xiang, G. and Rui, Z. (2.(011 RFID protocol based on random number and encryption hash. Proceedings of the 2011 *IET International Communication Conference on Wireless Mobile and Computing, CCWMC 2011, November 14, 2011 - November 16, 2011* Shanghai, China, 169-174.

Rong, J. and Huang, S. (2011). SAPCC1G2: A mutual authentication protocol promote the security of RFID and WSN integration system. *International Journal of Communication Networks and Distributed Systems*, 7(3-4), 249-261. doi: 10.1504/ijcnds.2011.042378

Shang-Ping, W ,.Qiao-Mei, M., Ya-Ling, Z. and You-Sheng, L. (2011). An Authentication Protocol for RFID Tag and its Simulation. *Journal of Networks*, 6(3), 446-453. doi: 10.4304/jnw.6.3.446-453

Shao, S., Xu, G. and Liu, Y. (2011). Efficient RFID authentication scheme with high security. Proceedings of the 2011 *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011, May 27, 2011 - May 29, 2011* Xi'an, China, 238-241.

Shelly, G. B., Gunter, G. A. and Gunter, R. E. (2011). *Teachers discovering computers*: Course Technology Ptr.

van Deursen, T. and Radomirović, S. (2009). Algebraic attacks on RFID protocols. *Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks*, 38-51 .

Wang, S.-P., Ma, Q.-M., Zhang, Y.-L. and Li, Y.-S. (2010). A HMAC-based RFID authentication protocol. Proceedings of the 2010 *2nd International Symposium on Information Engineering and Electronic Commerce, IEEC2010, July 23, 2010 - July 25, 2010* Ternopil, Ukraine, 66-69.

Wiberg, M .(2009) .*Exploring an open-loop RFID implementation in the automotive industry*: Division of Packaging Logistics, Lund University.

Wu, N. C., Nystrom, M., Lin, T. R. and Yu, H. C. (2006). Challenges to global RFID adoption. *Technovation*, 26(12), 1317-1323 .

Yang, M. H. (2010). Controlled delegation protocol in mobile RFID networks. *Eurasip Journal on Wireless Communications and Networking*, 2010. doi: 10.1155/2010/170150

Yao, Q., Qi, Y., Chen, Y. and Zhong, X. (2010). A desynchronization tolerant RFID private authentication protocol. Proceedings of the 2010 *5th International Conference on Wireless Algorithms, Systems, and Applications, WASA 2010, August 15, 2010 - August 17, 2010* Beijing, China, 120-124.