A Study on Comparing the Performance of Low Cost RFID Authentication Protocols

Ms. C. Divya
Assistant Professor in School of Information Technology and Science,
Dr G R Damodaran College of Science, Coimbatore -641014, Tamilnadu, India
Email: mercy_twin@yahoo.com

Abstract **---- Radio frequency identification (RFID) is a new technology that is used everywhere as RFID tags will be applied to every-day items in order to yield great productivity gains or "smart" applications for users. The use of RFID tags opens up the possibility for various attacks violating user privacy. This paper describes a complete analysis of various authentication protocols in three perspectives, namely data protection, tracking protection, and forward security.**

Keywords: *RFID Tag, Authentication Protocols, Security***.**

I. INTRODUCTION

RFID stands for radio frequency identification. Radio frequency waves are the invisible signals that travel through the air and the walls of our homes to bring us music and news. Radio waves can be sent at different frequencies, like the different stations on the radio.

Because of their low production costs [1] and small size, RFID tags are expected to replace traditional identification methods such as bar codes. Currently, RFID tags are deployed, for instance, in passports [2], access control cards for public transportation [3], and location tracking systems [4, 5].

There are two basic types of RFID tags: Active tags and passive tags. RFID tags operate as transponders, while RFID readers act as transceivers [6].

Request
DATABASE <--> RFID Tag **……>** RFID Tags
Reader **<……..**
Response

Basic RFID communication protocol

Contributions: This study is aimed at comparing some low cost RFID authentication protocols in terms of three perspectives, data protection, tracking protection, forward security.

Organizations: The remainder of the paper is organized as follows. In Section 2, we review RFID protocols addressing the scalability issue and Section 3 concludes the paper.

II. ANALYSIS ON PROTOCOLS

A. One-Time Pad based on XOR

[7].It requires a very simple XOR operation; therefore low computational cost for RFID is satisfied. A reader has the common list of randomly generated key for each tag. The reader and the tag find that both of them have the same key of the key list with several message exchanges between them. Then the tag transmits its ID to the reader. This method needs several exchanges for authentication between the tag and the reader. Besides the common key list must be refreshed to guarantee the security.

B. External Re-Encryption Scheme

C.

This method [8] uses public key cryptosystem. Tag data is re-encrypted when a user requires using the data transferred from an external unit. As public key encryption needs high computation cost, a tag cannot process for itself.

This method has difficulty to frequently refresh each tag's data since the encrypted ID stored on tag is constant so that user location privacy is compromised.

ISBN: 97881 8371 362 7

D. Hash Chain based Scheme

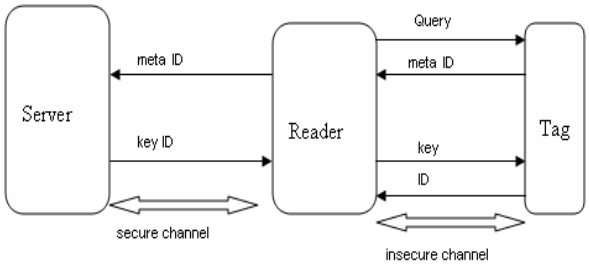
This operation is mainly applied as a simple mechanism to provide better protection of user privacy with the basic concept of refreshing the identifier of the tag each time it is queried by a reader. The protocol changes RFID identities on each read based on hash chains. This protocol is flawed to certain replay attacks which makes it difficult to guarantee forward security.

E. Blocker Tag

It is designed [9] to protect privacy that makes the tag unable to be used for theft, denials of service, and other malicious uses. It uses an individual tag, namely blocker tag for each tag and according to its purpose. To protect a tag's data, the blocker tag makes responses for attacker's request to get the tag's data. The responses from the blocker tag are not for the tag but all tags.

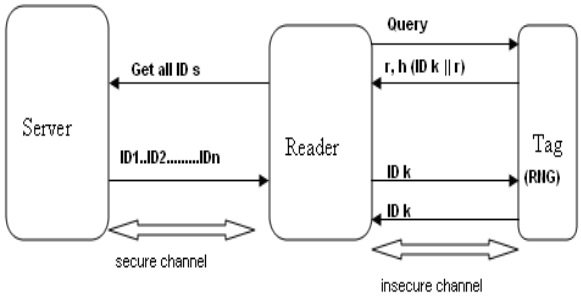
E. Extended Hash lock Scheme

Hash lock and extended hash lock are appropriate for low-cost RFID. It uses a backend server (to store keys k in its database), a reader and a tag. Each tag unique key with metaID = h (k) as its key, where h is a hash function. The tag transmits metaID as a response to a reader's query to the tag. Unfortunately this protocol fails to overcome eavesdrop attacks since metalID is always constant which opens tracing problem.



HASH-LOCK SCHEME

In extended hash lock protocol provides a mechanism to overcome the tracing problem. In this scheme a tag is introduced a tag with random number generator to randomize metaID value.
The tag picks pseudo random number r uniformly and calculates c=hash (IDjjr) as the tag's unique identification for every session. The tag transmits its c and r to a back-end server by way of the reader. The server sends the unique identifier of the tag comparing c with r and all IDs that is stored in database of the server. But it is not fully satisfy data protection and forward security.



EXTENDED HASH LOCK SCHEME

F. Hash-based Varying Identifier

This adopts a hash function and a random number generator, but a pseudo random number is generated by a back-and server and transmitted to the tag for every interrogation to make the tag's queried identifier random and to preserve location privacy. A tag has only a unique identifier and remaining original data used for applications stored and controlled in a back-end database.

This protocol focus on securing location privacy problems by making a tag's ID randomized in every interrogation. The attacker is able to perform reply attack since forward security is not well provided.

G. Improved Hash-based Varying Identifier

In this protocol the reader utilizes what is called a random number generator (RNG) to prevent the man-in-middle attack. In every query, the reader sends a pseudo-random number, S, to the tag. Then the tag replies h (ID) for finding the record of a back-end server and half of a new identifier, half(R). The scheme protects the location privacy as a tag's unique identifier is changed in every read attempts. This scheme is still vulnerable to the man-in-the middle attack particularly if there is no guarantee that the reader is a trusted party.

H. Mutual Authentication

The RFID reader and the tag carryout the authentication based on their synchronized secret information. It is monitored by a component of the database server. This protocol is claimed to have satisfied the low-cost requirement of RFID tags, it is highly dependable on back-end database which was confirmed as serious limitation. Fully relying on a central database will create a single point of failure, opening up the entire RFID system to denial of service attacks.

I. Ultra Lightweight

It is proposed to deal with maintain security and privacy of RFID by using simple operations.

- Lightweight Mutual Authentication Protocol
- Minimalist Mutual Authentication Protocol.
- Efficient Mutual Authentication Protocol.

LAMP Protocol uses only 300 gates to provide security; the 96 bit key is divided into 4 which provides 4 messages, by which the reader sends A, B, C messages to the tag. However there are some risks regarding data. forgery and data fabrication during transfer.

M2AP employs 300 gates. The difference here is, addition of E value to add more Security in database authentication compared to LMAP [10].
EMAP is most efficient protocol among the above two. It uses only 150 gates provide Security of RFID It produce the XOR algorithm sigma value by which provide a more accurate way of authentication. It provides security within close ranges. All these protocols come with new weakness.

The protocol is not robust since no assurance that the tag really recognized no matter whether the replying messages are indeed received and verified by a legitimate reader or not. As a result ultra lightweight protocols also do not provide full protection for forward security and location tracking.

Table 1: Comparative Study Result

Protocol	Tracking Protection	Data Privacy	Forward Security
One time Based on XOR	Satisfied	Partially Satisfied	Not Satisfied
External Re-Encryption Scheme	Partially Satisfied	Satisfied	Not Satisfied
Hash Chain Based Scheme	Satisfied	Satisfied	Not Available
Blocker Tag	Satisfied	Partially Satisfied	Satisfied
Extended Hash Lock Scheme	Satisfied	Partially Satisfied	Partially Satisfied
Hash Based Varying Identifier	Partially Satisfied	Satisfied	Not Satisfied
Improved Hash Based Varying Identifier	Satisfied	Satisfied	Not Satisfied
Mutual Authentication	Satisfied	Satisfied	Partially Satisfied
Ultra Weight	Partially Satisfied	Satisfied	Partially Satisfied

III. CONCLUSION

The low cost character is a very important reason for RFID mass implementation. Therefore, security and privacy are still inherent problems in RFID communications. These nine protocols address different security and privacy requirements through simple mathematical operations under low cost RFID.

This study focus on the analysis of determining how strong the protocols are in dealing with tracking protection, data privacy and forward security.

- Tracking Protection (A, C, D, E, G, H) show ability to satisfy.
- Data Privacy Requirements (B, C, F, G, Hand I) is fulfilled here.
- Forward Security (D) is satisfied here.

Finally, since there has been no single low cost RFID protocol capable to securing RFID from any attacks, economic consideration might also be
applied in the future development of RFID protocol to define equilibrium of both security and low cost requirements.

ACKNOWLEDGMENT

The author wish to sincerely thank the management of Dr. G R Damodaran College of Science, Coimbatore for their constant encouragement and financial support rendered during the course of this research work.

REFERENCES

[1]. Sarma, S. E., D. Brock and D. W. Engels, "Radio frequency identification and the electronic product code", IEEE Micro 21 ,2001.

[2] Hoepman, J.-H., E. Hubbers, B. Jacobs, M. Oostdijk and R. Wichers Schreur, Crossing borders:"Security and privacy issues of the european e-passport" in: H. Yoshiura, K. Sakurai, K. Rannenberg,Y. Murayama and S.-i. Kawamura, editors, Advances in Information and Computer Security, First International.

[3] Transport for London, Oyster card, http://www.oystercard.co.uk

[4] Kulyukin, V., A. Kutiyanawala, E. LoPresti, J. Matthews and R. Simpson, iWalker: "Toward a rollator-mounted wayfinding system for the elderly" in: Proceedings of the 2008 IEEE International Conference on RFID, 2008,

[5]. P.P.Lopez, J.C.H .Castro , J.M.E Tapiador and A.Ribagorda, " RFID Systems: A Survey on Security Threats and Proposed Solutions", IFIP 2006 , PWC 2006.

[6] Li, Z., C.-H. Chu and W. Yao, SIP-RLTS: "An RFID location tracking system based on SIP", in Proceedings of the 2008 IEEE International Conference on RFID, 2008.

[7] A.Juels "Minimalist Cryptography for Low cost RFID Tags", SCN, 2004.

[8] A.Juels and R.Pappu ,"Squealing euros: Privacy Protection in RFID Enabled Banknotes", In Proceeding of Financial Cryptography ,Springer Verlag, 2003.

[9] A.Juels and R.L .Rivest and M.Szydlo,"The blocker tag: Selective blocking of RFID tags for consumer Privacy" ,ACM Press,2003.

[10] C.C Tan, B.Sheng and Q,Li, " Serverless "Search and Authentication protocols for RFID", in Proceedings of Pervasive Computing Conference ,2006.

AUTHOR PROFILE

Ms. C.Divya has passed MCA degree in 2006 from Bharathiar University. She has completed her M.Phil in Computer Science in 2008.She is working as an Assistant Professor in School of Information Technology and Science, Dr G R Damodaran College of Science, Coimbatore, Tamilnadu since June 2006.Her research areas include Network Security and Cryptography, Data Mining and Database Management System. She has presented three research papers in UGC sponsored National Conferences.