A REVIEW on EFFICIENT MUTUAL AUTHENTICATION RFID SYSTEM SECURITY ANALYSIS

S.Vijay Anand[#1], B.Santhi[*2]
[#] School of Computing, SASTRA University,
Tirumalaisamudram-613401, Thanjavur, India.
[*] School of Computing, SASTRA University,
Tirumalaisamudram-613401, Thanjavur, India.
[1] vijayanand1987@gmail.com
[2] shanthi@cse.sastra.edu

***Abstract* - This article describes the technical fundamentals of RFID systems and the associated standards. Specifically, it addresses the security and privacy aspects of this relatively new and heterogeneous Radio Technology. It relates the security requirements, threats and the implemented mechanisms. Then the current security and privacy proposals and their enhancements are presented. This paper would be a useful reference article for beginners as well as experts.**

Keywords: Radio Frequency Identification (RFID), Near Field Communication (NFC).

I. Introduction

A. Practical Relevance

Radio frequency identification, a non-contact data storage and access technology which reads or writes information in RFID tags by receiving radio frequency signals through RFID readers. RFID tags can signal their existence, uniqueness, locality and other user-preferred information through Wireless information transfer via radio waves. Reads are performed in milliseconds, automatically which is designed to replace the Barcode. No line of sight required and no physical contact such as Optical Reader.

B. Review Methodology

The purpose of this study is to understand the state of RFID research by examining the published literature to provide insights for RFID practitioners and researchers on the major historical trends in, and to compile a systematic reference. It is obvious to determine the principal concerns of current RFID research, whether technological, application, or security related. The framework includes a content-oriented classification of security proposals. Section II describes, RFID Technology. Section III discusses System Characteristics. Section IV discusses detailed description of Security Proposals. Section V compares various Security Parameters. Finally Section VI concludes the study.

II. RFID Technology :

RFID is a System of Tags (Transponder), Readers (Transceiver), and Backend Server (Electronic Databases). Reader, query tag for identification information, while all information about tags (Id, Assigned keys, etc.) are maintained on servers. It consists of an RF transmitter and receiver, a control unit, and a memory unit. These instruments work together to transfer and receive information stored on radio waves between it and an antenna attached to an RFID tag.

Servers can be assigned multiple readers, only engages in communication with constituent readers. Communication between server & readers is assumed to be over private and authenticate channels. RFID varies based on the following Constraints, Power, Processing, Memory, and Bandwidth.

III. System Characteristics :

A. Classification based on Frequency of Operation:

Low Frequency (LF), data transfer rate is low and frequency ranges between 125 kHz - 134 kHz. Typical applications involve Access control and Animal tracking. High Frequency (HF), have medium data transfer rate and frequency range is, 13.56 MHz. Mostly applied in Contact-Less Smart Cards, Libraries, Access Cards and Item Level tracking.

Ultra High Frequency (UHF), since data transfer rate is high, less sensitive to environmental detuning. Frequency ranges between 860 MHz - 960 MHz. Applications mostly involve tracking of Supply Chain. Microwave, have very high transfer rate, frequency ranges between 2.45 GHz - 5.8 GHz, but line of sight is required for long distance communication.

B. Classification based on Powering Techniques :

Passive tag do not include a battery or other power resource. Therefore, they have to wait for a signal from a reader. The tag contain a resonant circuit skilled of fascinating power from the reader's antenna. Obtaining power from the reader machine is done by means of an electromagnetic property (Near Field). **Semi-passive** tags include a battery to power the memory circuitry, but rely on the Near Field to power the radio circuits for the period of the receiving and sending data.

Active tags have their individual power source, usually an internal battery. They can dynamically transmit and receive on their own and so they are not restricted to operational within the Near Field. Active tags capable to transmit and obtain over longer distances. Our research mainly focus on security implementation on low cost RFID Tags, i.e., Passive RFID Tags.

In order to implement low-power, low-complexity and highly secured RFID authentication system, since only passive tag get closer to reader and get enough inductive coupled energy from antenna. Because of its passive feature, tags in the market doesn't have enough security, the high security system may take larger area and power. In order to overcome the weakness of security, system should have strong encryption algorithms and authentication mechanisms that can withstand a variety of attacks.

IV. Security Proposals

RFID security proposals either based on Cipher-based protocols and Hash-based protocols. Lack of computational resources is denoted as temporary state of affairs, but cost factor is still a problem since it is used in vast numbers. And if RFID replaces barcodes on individual items, they will substantially contribute cost of those items. This paper address security and privacy concerns of mutual authentication mechanism, during transmit from reader to tag and vice-versa. The System should be highly secured with authentication protocol which does anti-intrusion and encryption algorithm, that encrypts important data which cannot be decipher by attacker. The following figure 1.1 depicts security protocol types. The taxonomy of RFID security is shown in figure 1.2.

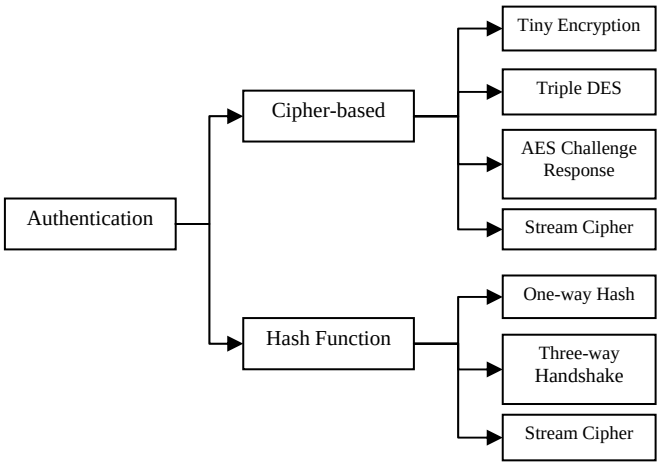

Fig 1.1 Classification of Security Protocols

A. Cipher-based Authentication

1) Tiny Encryption Algorithm :

Abdelhalim et al [11], proposed a Modified Tiny Encryption Algorithm (MTEA) , using Linear Feedback Shift Register (LFSR) which overcomes the security weakness of TEA against equivalent key attacks. This system implements a Pseudo random Number Generator to improve the security strength of TEA, such as LFSR, where key is frequently changed in each round instead of a single symmetric key for all rounds like in standard TEA. Key of final round is used as key of first round in the decryption. By implementing different decryption keys, key secrecy is highly preserved in MTEA.

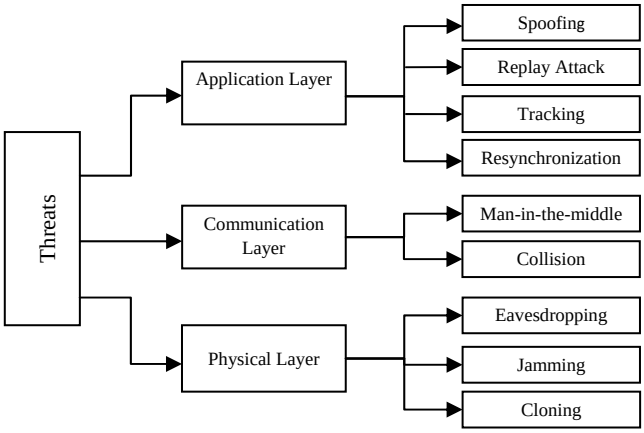

Fig 1.2 Taxonomy of RFID Security

2) Triple DES Algorithm :

Jianguo Hu et al [10], proposed a strong authentication for RFID system by implementing triple DES encryption algorithm on low cost passive RFID tag. To authenticate the legitimacy of both reader and tag, authors proposed unpredictable random key to replace authentication key, protect tag's key from being attacked. The key is generated using random number generator and predicted with a strong encryption algorithm. Random key can be generated at any time, so the system just transmit random number when need to authenticate. Can support 56-bit, 112-bit or 168-bit key length, thus provides enough security for the chip. Even the attacker acquires the authentication key, he gets nothing but some unpredictable number.

3) Advanced Encryption Standard, Challenge-Response Protocol

Tuan Anh Pham et al [12], proposed a mutual authentication based on symmetric block cipher AES-128, which overcomes the existing AES cryptographic proposals, where synchronization between the reader and the tag is lost if responsible from tag is blocked. A value seed 's' of each tag is stored on the server and on the rewritable memory of tag, which get automatically updated after each successful authentication. Since $E_k(s)$ changes every authentication cycle, attackers can't utilize the former data, to delude the authorized reader or tag during authentication process. Thus overcome Replay Attack and Man-in-the-middle Attacks.

4) Stream Cipher Based OTP, Challenge-Response Protocol

Young Sil Lee et al [12], proposed a low-resource hardware implementation appropriate for efficient mutual authentication in RFID systems. The System is composed of a stream cipher based One-Time Password (OTP) by challenge-response pair of a Physically Unclonable Function (PUF) which overcomes the security weakness of key disclosure problem. This system implements NLM-128, Non-Linear Stream Cipher to generate the OTP value. This OTP can only be used once and user has to authenticated with a new password key each time. Thus overcomes eavesdropping and even attempting reply attack can't be succeed.

B. Hash-based Authentication

1) One-Way Hash based Authentication Protocol :

He Lei et al [10], proposed a hash based authentication using forward security. This mechanism overcomes de-synchronization attacks. In this system both tag and backend database update variables, key 'k', secret value shared with all tags and 'id' using hash operation. Even if an adversary interferes the communication after tag authenticates backend database successfully and updates its 'k' and 'id' stored, backend database can use previous 'k' and 'id' to authenticate tag and resynchronize those variables. This proposed system is suitable for low-cost RFID system on storage, communication and computation cost of tags.

2)Reader-Dependent Key Management, Three-Way Handshake Protocol :

Roberto Di Pietro and Refik Molva [11], devised a technique to make RFID identification server dependent, a different unique secret key shared by a tag and a server. A probabilistic tag identification scheme, requires the server to perform just bitwise operations, thus speeding up the identification process. The tag identification protocol assures privacy, security and resilience to DoS attacks. The identification protocol requires the reader to access the local database(DB) of tags' keys O(n) times. The RFID tag to store a single secret key for all servers yet assuring the confinement property in case of server compromise.

3) Hash Chain based Tag Identification and Mutual Authentication :

Tsudik [06] *and Rhee et al.* [05], employed hash chains to allow tag identification and mutual authentication. The hash chain length corresponds to the lifetime of the tag stated in advance, leading to a waste

of memory on the server side. System implies cryptographic hash function, which uses single key or password to produce several one-time keys, on order of h(x) to a string.

Molnar and Wagner [04], proposal requires just $\log_\delta n$ interactions between the server and a tag for the server to identify the tag is proposed. This approach requires $\log_\delta$ keys to be stored on each tag. This technique weakens the privacy when an adversary is able to tamper at least one tag. This system suffers from an expensive time complexity on server side, because only symmetric cryptographic functions can be used, server needs to explore its entire database in order to retrieve the identity of the tag it is interacting with.

V. Security Analysis

In this section the comparisons of various security proposals have been listed. A comparison of security and privacy between the different schemes is shown in Table 1.1.

Table 1.1 shows Comparison in terms of Security and Privacy

Attacks/Methods	TEA	Triple-DES	AES	Stream Cipher Based OTP	One-way Hash	Three-way Handshake	Hash Chain
Information Leakage	No	Partial	Yes	No	Partial	Partial	Partial
Tag Tracing	Yes	Yes	Yes	Partial	Yes	Yes	No
Clone Resilience	Yes	Yes	Yes	Partial	Yes	Yes	No
Man-in-the-middle Attack	Partial	Yes	Partial	No	Partial	Partial	No
DOS	Partial	Yes	Yes	Yes	Partial	Yes	Partial
Replay Attacks	No	Yes	Yes	Yes	Yes	Yes	No
Resynchronisation	Yes	Yes	Yes	Yes	Yes	Yes	Partial

VI. CONCLUSION

It is generally agreed that the security and privacy of the tag play an important role in determining the cost and performance of the system as a whole. Among the RFID policy and security issues, these are the only two that relate to the standardization of RFID. However, to build a global internet of things, it is essential to ensure compatibility across the entire network and that need to be shared and processed are uniformly defined.

Lots of low complexity solution have been proposed for RFID but still they are expensive as well as vulnerable to the security system. There is a need for best solution. In [6], author uses simple bit-wise operations using random numbers. The computational requirements on the tag can be kept minimal by resorting to just a single hash function invocation, resulting in a lightweight protocol that achieves only the authentication of the tag by the reader. Still, the solutions provided in literature do not fully resolve the security issues, so there is a good research scope in the field of designing an efficient and effective light weight cryptographic protocol for Low-cost RFID.

REFERENCES

[1] M. B.Abdelhalim, M. El-Mahallawy, M. Ayyad, A. Elhennawy, "Implementation of a Modified Lightweight Cryptographic TEA Algorithm in RFID System", 6th International Conference on Internet Technology and Secured Transactions, 2011.

[2] Jianguo Hu, Deming Wang, Yanyu Ding, Jun Zhang and Hongzhou Tan, "Design and Implementation of Intelligent RFID Security Authentication System", IEEE International Conference on RFID-Technology and Applications, 2010.

[3] Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu, "A RFID mutual authentication protocol based on AES algorithm", UKACC International Conference on Control 2012, Cardiff, UK, 3-5 September 2012

[4] Young Sil Lee, Tae Yong Kim, Hoon Jae Lee, "Mutual Authentication Protocol for Enhanced RFID Security and Anti-Counterfeiting ", 26th International Conference on Advanced Information Networking and Applications Workshops, 2012.

[5] He Lei, Lu Xin-mei, Jin Song-he, Cai Zeng-yu, "A One-way Hash based Low-cost Authentication Protocol with Forward Security in RFID System", 2nd International Asia Conference on Informatics in Control, Automation and Robotics, 2010.

[6] Roberto DiPietro, RefikMolva, "An optimal probabilistic solution for information confinement, privacy, and security in RFID systems", Journal of Network and Computer Applications 34 (2011) 853–863.
[7] Tsudik G,"Ya-trap: yet another trivial RFID authentication protocol " In: PERCOMW '06: Proceedings of the 4th annual IEEE international conference on pervasive computing and communications workshops, Washington, DC, USA. IEEE Computer Society, 2006.
[8] Rhee K, Kwak J,Kim S,Won D, "Challenge-response based RFID authentication protocol for distributed database environment" In: Hutter D, Ullmann M, editors. International conference on security in pervasive computing - SPC 2005. Lecture notes in computer science, vol.3450, Boppard, Germany. Springer-Verlag: 2005. pp.70–84.
[9] Molnar D, Wagner D, "Privacy and security in library RFID: issues, practices, and architectures", In: CCS '04: proceedings of the 11th ACM conference on computer and communications security, New York, NY, USA. ACM Press; 2004. pp. 210–9.
[10] Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita campbell, "RFID Security : Protect the Supply Chain", Syngress Publishing, Inc. Rockland, MA 02370, 2006.