An Ultra Lightweight RFID Protocol Based on Random Partitions of Pseudorandom Identifier and Pre-shared Secret Value

Er.Vinita Sharma
Computer Science and Engineering
College of Science and Engineering
Jhansi, India

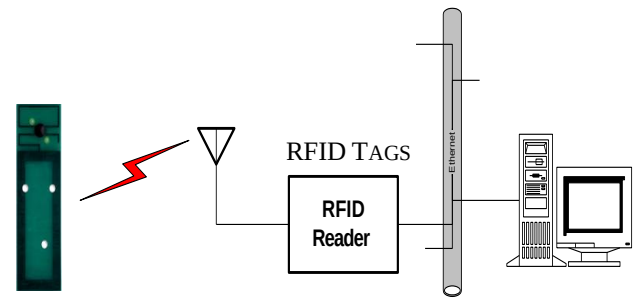
Er.Jitendra Gupta
Computer Science and Engineering
College of Science and Engineering
Jhansi, India

ABSTRACT: Security is the degree of protection against danger, damage, loss, and crime. Securities as a form of protection are structures and processes that provide or improve security as a condition. Here in this paper we are trying to implement the security in RFID applications. RFID is the radio frequency identification that uses tags and readers. RFID is a device which is attached to any object and at the time of manufacturing these tags are provided a unique identification number. These devices also contain a reader which is directly attached to the server for the authentication. Although the security at the receiver side don't need to take care of, but threats at the tag side is necessary that can be accesses by the unauthorised users, so the idea is to generate a more secure and authenticated protocol used for the authenticity of the data from the tag to the reader. We are implementing a new technique to secure the data read by the tags.

Keywords -RFID,Tags,Reader,LMAP,M2AP,EMAP)

I. INTRODUCTION

Radio-frequency identification (RFID) is a technology, whose origins are found in the WWII era that incorporates electromagnetic or electrostatic coupling in the RF portion of the EM spectrum to uniquely identify an object, animal or person. It is also gaining increasing use in industry as an alternative to the bar code. It requires a transceiver, antenna, and transponder and can operate in Passive or Active Modes.
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. Some tags require no battery and are powered by the electromagnetic fields used to read them. Others use a local power source and emit radio waves (electromagnetic radiation at radio frequencies). The tag contains electronically stored information which can be read from up to several meters (yards) away. 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 objects.



Tags can be attached to almost anything:

- Items, cases or pallets of products, high value goods
- vehicles, assets, livestock or personnel

Passive Tags

- Do not require power – Draws from Interrogator Field
- Lower storage capacities (few bits to 1 KB)
- Shorter read ranges (4 inches to 15 feet)
- Usually Write-Once-Read-Many/Read-Only tags
- Cost around 25 cents to few dollars

Active Tags

- Battery powered
- Higher storage capacities (512 KB)
- Longer read range (300 feet)
- Typically can be re-written by RF Interrogators
- Cost around 50 to 250 dollars.

1.1 Security

We classify security threats to RFID protocols into weak and strong attacks.

1.1.1 Weak attacks

These are attacks which are feasible just by observing and manipulating communications between readers and tags.

• *Tag Impersonation***:** An eavesdropper could impersonate a target tag without knowing the tag's internal secrets. It could communicate with readers instead of the tag and be authenticated as the tag.

• *Replay attack***:** In such an attack, an attacker reuses communications from previous sessions to perform a successful authentication between a tag and a server.

• *Denial of Service attack***:** An adversary disturbs the interactions between readers and tags by intercepting or blocking messages transmitted. Such an attack could cause a server and a tag to lose synchronization. For example, the server might update the shared data, while the tag does not; in such a case they would no longer be able to authenticate each other.

1.1.2 Strong attacks

These are threats possible for an attacker which has compromised a target tag. The memory of a low-cost tag is not tamper-resistant, and hence the tag's internal data are liable to be exposed by physical attacks. Thus addressing such attacks is essential for the security of RFID schemes.

• *Backward Traceability:* This occurs if, given all the internal state of a target tag at time t, the attacker is able to identify target tag interactions that occurred at a time t0 < t [12]. That is, knowledge of a tag's current internal state could help identify the tag's past interactions, and the past transcripts of a tag may allow tracking of the tag owner's past behavior [12]. In some previous papers, backward untraceability is referred to as forward security [5, 7, 9, 18]. Here we use the terms backward traceability and forward traceability defined as in [12] to clearly distinguish between threats to past and future anonymity.

• *Forward Traceability***:** This can similarly be defined as where knowledge of a tag's internal state at time t can help to identify tag interactions that occur at a time t0 > t [12]. The only way of maintaining future security once the current tag secrets have been revealed is to detect key compromise as soon as possible, and to replace the exposed key to protect future transactions [12]. This issue is related to tag ownership transfer. This is because, if an RFID scheme does not provide forward untraceability, when the ownership of a tag is transferred, the previous owners might be able to read communications between the new owner and the tag.

• *Server Impersonation***:** This means that an adversary with knowledge of the internal state of a tag is able to impersonate the valid server to the tag. This attack does not appear to have been discussed previously, despite its potential importance. One reason that this is a genuine threat is because of the following attack. If it is possible to impersonate a server to a tag, an adversary could request a target tag to update its shared secrets. The tag and the real server would then be desynchronized, and incapable of successful communications.

1.2 Performance

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce.

• *Capacity minimization:* The volume of data stored in a tag should be minimized because of the limited size of tag memory.

• *Computation minimization***:** Tag-side computations should be minimized because of the very limited power available to a tag.

• *Communication compression***:** The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags [4, 18].

• *Scalability:* The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel [11]. Performing an exhaustive search to identify individual tags could be difficult when the tag population is large [6].

II. BACKGROUND

The work that we are presenting here involves a new security protocol implemented over RFID. A RFID consists of a Tag and a Reader. Tags are generally used with any objects that are used to read the data from the source and readers are used for the authentication of these tags. Although each of these tags consists of a unique identification number allotted at the time of manufacturing. The new protocol implemented here performs better performance as compared to the existing protocol implemented over RFID. The idea is to use pseudorandom identifiers and initially allotted a shared secrete key for the better authentication between the Tags and the Reader.

III. RELATED WORK

Most of the security protocols implemented in RFID are based on cryptographic and hash functions. But these security protocols are not much secure. The OSK protocol was proposed by Ohkubo, Suzuki and Kinoshita (OSK) in 2004 [13]. Its aim is to assure the valid answer of the tag even under an active attack. In this scheme each tag is initialized with a secret value xi and two unidirectional functions h1 and h2. When a tag receives a request from a reader, it updates the value xi with the new value obtained from the computation of ht 1(xi) [8].

YA-TRAP (Yet-Another Trivial RFID Authentication Protocol) was proposed by Tsudik in 2006 [14]. This protocol describes a technique for the inexpensive untraceable identification of RFID tags. YA-TRAP involves minimal interaction between devices and a low computational load on the back-end server. With these features, this scheme is attractive for applications where the information is processed in data groups [8].

Weis, Sarma, Rivest and Engels proposed in 2003 the use of hash-locks in RFID devices. A first approach, called Deterministic hash locks, was presented in. A tag is usually in a \locked" state until it is queried by a reader with a specific temporary meta-identifier Id. This is the result of hashing a random value (nonce) selected by the reader and stored into the tag. The reader stores the Id and the nonce in order to be able to interact with the tag. The reader can unlock a tag by sending the nonce value. When a tag receives it, the value is checked [8].

In 2012, Dr.S.Suja proposed an RFID Authentication protocol for security and privacy which is based on Cyclic Redundancy Check (CRC) and Hamming Distance Calculation in order to achieve reader-to-tag authentication and the memory read command is used to achieve tag-to reader authentication. It will resist against tracing and cloning attacks in the most efficient way [1].

In 2011, Liangmin WANG, Xiaoluo YI, implies improved protocol merely uses CRC and PRNG operations supported by

Gen-2 that require very low communication and computation loads. They also develop two methods based on BAN logic and AVISTA to prove the security of RFID protocol. BAN logic is used to give the proof of protocol correctness, and AVISTA is used to affirm the authentication and secrecy properties [2].

In 2008, Tieyan Li analyze the security vulnerabilities of a family of ultra-lightweight RFID mutual authentication protocols: LMAP [10], M2AP [11] and EMAP [12], which are proposed by Peris-Lopez et al. Here they identify two effective attacks, namely de-synchronization attack and full disclosure attack, against their protocols. The former permanently disables the authentication capability of a RFID tag by destroying synchronization between the tag and the RFID reader [3].

IV. PROPOSED SCHEME

The proposed algorithm that we are implemented here is based on symmetric key cryptosystems and modular exponentiations. The scheme consist of five phases: Initial phase, registration phase, login phase, verification phase and password change phase.

1. *Initial Phase*- Server Si selects two large prime numbers p and q such that p = 2q +1 and chooses a secret key "x". Server keeps both p and x secret. Then S selects a symmetric key cryptography algorithm with encryption Ek (.) and decryption Dk (.) a secure one way hash function.
2. *Registration Phase*- Tag Ti submits his/her Identity IDi and Password PWi to the remote Reader through a secure channel for registration. Upon receiving the registration request, it computes A = h (IDX mod p*)* h (PWi). Then Ri issues a package to Ti containing (IDi, Ai, h (.), E (.)} over a secure channel and also sends it over to the server.
3. *Login Phase*-Tag Ti log on the remote Reader Ri; he/she must insert the package into reader and type his Identity ID and password PWi. The reader first generates a random number R. and gets the current timestamp Tu. Then it computes K =A xor h (PWi), W =EK(R xor Tu), and Cu =h (Tu || R|| W || ID). Where EK is the symmetric key encryption operation with the key K, Finally the package sends the login request message {IDi, Cu, W, Tu} to Reader Ri.
4. *Authentication Phase*- Upon receiving the login request from Tag Ti at time T‟ the Reader Ri first checks validity of the identity IDi and (T‟- Tu) ≤ ΔT, where ΔT is a predefined transmission delay. If it is fail, the request is rejected else it consider for next step. The Reader Ri computes K= h (IDX mod p) and R‟ = DK (W) Tu and checks whether Cu = h (Tu || R‟ || W || ID). If they are equal, the Tag Ti is authenticated, then Reader computes Cs= h (ID ||R‟ ||Ts) and sends the reply massage {ID, Cs, Ts) to Tag Ti. Where, Ts is the current timestamp. Upon receiving the relay massage from Ri, the reader checks the validate ID and freshness of Ts. Then compute h (IDi || R ||Ts) and checks Cs = h (IDi || R || Ts). If they are equal, the Reader is authenticated. After both user and Reader authenticated each other, they compute a common shared secret session key SK=h (IDi || Ts || Tu || R).
5. *Password Change Phase*- Tag Ti is allowed to change his/her password from PW into PW‟. He/she insert package into reader and type IDi and PWi. Then, a mutual authentication between the Reader Ri and the package is performed first. Then authentication is complete. The card asks Ti to enter a new password PW‟. Then, it computes A‟ = A xor h (PW) xor h(PW‟) and replaces A with A‟.

Tag Ti	Reader Ri
Initial Phase	
	Select p,q,x Keep p,x secretly
Registration Phase	
Select IDi and PWi	A=h(ID^x mod p) xor h(pWi) Store (ID,A,h(.),E(.) into package <---------- card
Login and Authentication Phase	
Input IDi and PWi Select R K=A xor h(PWi) W=EK(R xor Tu) Cu=h(Tu||R||W||IDi) --------→	verify IDi and Tu K=h(ID^x mod p) R'=DK(W) xor Tu Cu'=h(Tu||R||W||IDi) Verify cu'=cu Cs=h(IDi||R'||Ts)
Verify ID and Ts Cs=h(IDi||R||Ts) Verify Cs'==Cs	<----------
Compute Common Secrete Key	
Sk=h(IDi||Ts||Tu||R) ←-------→	Sk=h(IDi||Ts||Tu||R')

V. RFID BASED PROTOCOL ANALYSIS

Protocol	**Hash[16]**	**Advanced Hash[18]**	**Chien et al's Protocol[5]**	**Yoking Proof[11]**	**ULAP [6]**	**Proposed protocol**
Low-cost	N.S	N.S	S	N.S	P.S	S
Mutual-Authentication	N.S	N.S	S	N.S	S	S
Mutual-Authentication for Multi-	N.S	N.S	N.S	P.S	N.S	S

Tags						
Forward Security	S	S	S	S	S	S
Tag Anonymity	S	S	P.S	P.S	S	S
Replay Attacks	N.S	N.S	N.S	S	P.S	S
Privacy	S	S	P.S	N.S	S	S
Eavesdropping	S	S	S	S	S	S

S-satisfied P.S-partially satisfied N.S-not satisfied

Protocol	**Storage Req.(bits)**	**Communication Cost (bits)**
Gossamer	**960**	**520**
LMAP	**1056**	**520**
SASI	**864**	**520**
Work in [9]	**864**	**424**
Work in [10]	**960**	**712**

VI. CONCLUSION

The security protocol implemented here provides a more efficient technique for the authentication of the tags as well as low communication cost and less memory storage. Although the existing protocols provides the best hashing technique for the authentication between the tags and the reader. The proposed algorithm provides here provides a more authenticated protocol using the concept of pre shared secrete key for the authenticity between the tags and the reader using the technique of card generation.

REFERENCES

1] An RFID Authentication protocol for security and privacy,Dr.S.Suja, M.E.,PhD., Associate Professor, Electrical and Electronics Engineering, Coimbatore Institute of Technology, Coimbatore. A. Arivarasi, M.E, Embedded and Real Time Systems, Coimbatore Institute of Technology, Coimbatore.

[2] Security Improvement in Authentication Protocol for Gen-2 Based RFID System, Liangmin WANG, Xiaoluo YI, Chao LV, Yuanbo GUO ,School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China School of Communication Engineering, Xidian University, Xi'an, 710071, China School of Electronic Technology, Information Engineering University of PLA, Zhengzhou, 450004, China doi:10.4156/jcit.vol6. issue1.18.

[3] Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols Tieyan Li, Institute for Infocomm Research (I2R), 21 Heng Mui Keng Terrace, Singapore 119613.

[4] G. Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Protocols. PhD thesis, Ecole Polytechnique Federale de Lausanne (EPFL), Lausanne, Switzerland, December 2005.

[5] H. Chien and C. Chen. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Computer Standards & Interfaces, 29(2):254–259, February 2007.

[6] H. Lee, J. Yang, and K. Kim. Enhanced mutual authentication protocol for low-cost RFID. White Paper WP-HARDWARE-031, Auto-ID Labs, 2006.

[7] D. N. Duc, J. Park, H. Lee, and K. Kim. Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning. In Symposium on Cryptography and Information Security — SCIS 2006, Hiroshima, Japan, January 2006. The Institute of Electronics, Information and Communication Engineers.

[8] A Brief Survey on RFID Privacy and Security J. Aragones-Vilella_, A. Martinez-Ballest_e and A. Solanas CRISES Reserch Group UNESCO Chair in Data Privacy Dept. of Computer Engineering and Mathematics, Rovira I Virgili University.

[9] T. Le, M. Burmester, and B. Medeiros. Forward secure RFID authentication and key exchange. Cryptology ePrint Archive Report 2007/051, IACR, 2007. [18] M. Ohkubo, K. Suzki, and S. Kinoshita. Cryptographic approach to "privacy-friendly" tags. In RFID Privacy Workshop, MIT, MA, USA, November 2003. http://www.rfidprivacy.us/2003/agenda.php.

[10] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez- Tapiador, and A. Ribagorda. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. In: Proc. of 2nd Workshop on RFID Security, July 2006.

[11] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez- Tapiador, and A. Ribagorda. M2AP: A Minimalist Mutual- Authentication Protocol for Low-cost RFID Tags. In: Proc. of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923. Springer-Verlag, 2006.

[12] 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: OTM Federated Conferences and Workshop: IS Workshop, November 2006.

[13] M. Ohkubo, K. Suzuki, and S. Kinoshita. Efficient hash chain based RFID privacy protection scheme. In International Con- ference on Ubiquitous Computing - Ubicomp, Workshop Privacy: Current Status and Future Directions, 2004.

[14] G. Tsudik. YA-TRAP: Yet another trivial RFID authentication protocol. In Fourth Annual IEEE International Conference on Pervasive Computing and Communications Work- shops (PERCOMW'06), pages 640{643, 2006.

AUTHORS PROFILE

Er.Vineeta Sharma

MTech-Computer Science (persuing)

College of Science and Engineering JHANSI

Er.Jitendra Gupta

Asst.Prof.(CSE)

Computer Science and Engineering JHANSI