Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Efficient Authentication in RFID Devices Using Et Al's Algorithm

By Vinita Sharma, Jitendra Kumar Gupta & K. K. Mishra

SR Group of Institution, CSE Campus Jhansi, India

Abstract - Security plays a vital role during the transmission of private data from one sender to the other. Although there are many security algorithms implemented but here we are providing the security algorithms on the RFID devices. The authentication techniques implemented in RFID is based on the new algorithm based on smart cards. The data send through the tags can be made secure using the proposed algorithm so that the un-authorised users can't access the data without any further unique numbers.

Keywords : *RFID, tags, reader, authentication, counterfeiting, privacy, security.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

© 2012. Vinita Sharma, Jitendra Kumar Gupta & K. K. Mishra. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Efficient Authentication in RFID Devices Using Et Al's Algorithm

Vinita Sharma[α], Jitendra Kumar Gupta[σ] & K. K. Mishra[σ]

Abstract - Security plays a vital role during the transmission of private data from one sender to the other. Although there are many security algorithms implemented but here we are providing the security algorithms on the RFID devices. The authentication techniques implemented in RFID is based on the new algorithm based on smart cards. The data send through the tags can be made secure using the proposed algorithm so that the un-authorised users can't access the data without any further unique numbers.

Keywords : RFID, tags, reader, authentication, counterfeiting, privacy, security.

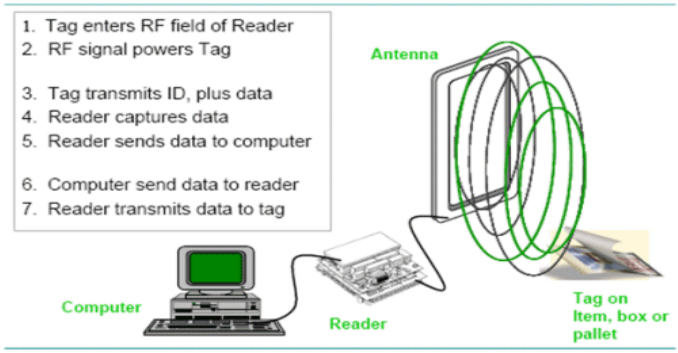
I. Introduction

Radio Frequency Identification (RFID) system is the latest technology that plays an important role for object identification as ubiquitous infrastructure. RFID has many applications in access control, manufacturing automation, maintenance, supply chain management, parking garage management, automatic payment, tracking, and inventory control.

RFID tag: is a tiny radio chip that comprises a simple silicon microchip attached to a small flat aerial and mounted on a substrate. The whole device can then be encapsulated in different materials (such as plastic) dependent upon its intended usage. The tag can be attached to an object, typically an item, box, or pallet, and read remotely to ascertain its identity, position, or state. For an active tag there will also be a battery. Reader or Interrogator: sends and receives RF data to and from the tag via antennas. A reader may have multiple antennas that are responsible for sending and receiving radio waves.

RFID offer several advantages over barcodes: data are read automatically, line of sight not required, and through non conducting materials at high rate and far distance. The reader can read the contents of the tags by broadcasting RF signals via antennas. The tags data acquired by the readers is then passed to a host computer, which may run middleware (API). Middleware offers processing modules or services to reduce load and network traffic within the back-end systems. RFID basic operations can be summarized as in Figure.

RFID systems are vulnerable to a broad range of malicious attacks ranging from passive eavesdropping to active interference. Unlike in wired networks, where computing systems typically have both centralized and host-based defenses (e.g. firewalls), attacks against RFID networks can target decentralized parts of the system infrastructure, since RFID readers and RFID tags operate in an inherently unstable and potentially noisy environment. Additionally, RFID technology is evolving quickly – the tags are multiplying and shrinking - and so the threats they are susceptible to, are similarly evolving.



Basic Operations of RFID

RFID tags may pose a considerable security and privacy risk to organizations and individuals using them. Since a typical tag answers its ID to any reader and the replied ID is always the same, an attacker can easily hack the system by reading out the data of a tag and duplicating it to bogus tags. Unprotected tags may have vulnerabilities to eavesdropping, location privacy, spoofing, or denial of service (DoS). Unauthorized readers may compromise privacy by accessing tags without adequate access control. Even when the content of the tags is protected, individuals may be tracked through predictable tag responses.

a) Security Issues

1. Security of the tag and the reader as well as the server: As the data from tag moves to the reader, security has to be maintained during the flow of data. Hence the security is maintained at the tag and the reader for the better efficiency of the data.
2. The original data stored at the receiver side: The original data from the tag is readed by the reader and is stored at the server, if the server can be accessed in an unauthorized manner and if the server damages the data will be lost, hence chances of fault tolerance.

Author α : M,Tech Scholar, Department of Computer Science & Engineering, SR Group of Institution, CSE Campus Jhansi, India.
Author σ : Assistant Professor, Department of Computer Science & Engineering, SR Group of Institution, CSE Campus Jhansi, India.

© 2012 Global Journals Inc. (US)

3. Low computational and storage cost: During the manufacturing of tag and the reader devices various functions have been designed for the better authorization of the data, hence when this function are been implemented the tag and the reader should not increase the computational and the storage cost.
4. Various security features implemented in various protocols: The table shown below is the various security features that are implemented in various protocols used in RFID devices. Hence the protocol that doesn't contain these security features is not very efficient and can be attacked by the external or internal user.
5. Chances of eavesdropping: The protocols that are implemented for the security of the data from tag to reader should be authenticated so that the chance of eavesdropping has been reduced.
6. Synchronization between tag and the reader: Synchronization between the tag and the reader is the flow of control from tag to the reader. The data moved from tag to the reader should be synchronized such that the data can't be lost and the chance of congestion has been reduced.

b) 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. Related Works

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. 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).

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 [22].

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 [15] 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

© 2012 Global Journals Inc. (US)

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, M2AP and EMAP[17]*, 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].

The weakness of this authentication protocol comes from the fact that each round the advesary gets some information from the same key. So a quick way to counter our attack is to include a key-updating mechanism similar to OSK[18] at the end of the protocol using a one-way function. In this case, adversaries do not get more than P equations for each key so that the security proof and reduction to the SAT problem become sound. The resulting protocol is even forward-private providing that adversaries do not get side-channel information from the reader [28].

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[7],

Hash-based Access Control (HAC), as defined by Weis et al. [16]*, is a scheme which involves locking a tag using a vone-way hash function. A locked tag uses the hash of a random key as its metaID. When locked, a tag responds to all queries with its metaID. However, the scheme allows a tag to be tracked because the same metaID is used repeatedly [5].

In[13] Ohkubo, Suzki, and Kinoshita (OSK) propose an RFID privacy protection scheme providing indistinguishability (i.e. a tag output is indistinguishable from a truly random value and unlinkable to the ID of the tag) and backward untraceability. This scheme uses a low-cost hash chain mechanism to update tag secret information to provide these two security properties.

III. Problem Statement

The attack on SASI is a passive one. Passive attacks are achievable in practice since they only necessitate only eavesdropping, which is a typical hazard or threat in RFID setting where the physical wireless communication station or channel is open to parties within communication and transmission. The security provided by the SASI might be more but for the passive attacks only and the chances of eavesdropping is more.

IV. Proposed Solution

Registration Phase - In the registration phase, Tag Ti wants to register himself/herself in remote server S. Firstly Tag chooses his/her ID and PW. Before register on Server, registration authority computes h (ID) and h (ID||PW) and sends to Reader R over a secure channel. Upon receiving the registration request from Tag Ti. Reader R computes same parameters related to the Tag Ti.

R computes Ai= h (ID) xor h (X || h (ID))
Bi = Ai xor h (ID || PW)
Ci = h (Ai)
Di = h (ID || PW) xor h(X)

And stored some of them in the memory and issues this to Tag Ti.

Login Phase- This phase provides the facility of a secure login to the Tag .Tag wants to access same services on remote server S. first it gain the access right on the remote server S. Tag keys in ID* and PW*. The Tag device memory computes –

$$Ai^* = Bi \text{ xor } h(ID^* || PW^*)$$

And Ci* = h (Ai*) and checks whether Ci (stored in the Tag memory) and Ci* are equal or not. If not, terminate to again login process. Otherwise yes, Tag Ti is legitimate bearer of the device. Then the Tag device generates a random nonce Ri and computes –

Ei = Ai* xor Ri
Cid = h (ID || PW) xor Ri
Fi = h (Ai || Di || Ri || Tu)

Where Tu is current time when login request proceed. And send the login request massage {Fi, Ei, Cid, Tu, h (ID)} to remote Reader R.

Verification Phase- Upon receiving the login request massage {Fi, Ei, Cid, Tu, h (ID)}. Reader verifies the validity of time delay between Tu‟ and Tu. Where Tu' is the travel time of the massage. Tu'-Tu ≤ ΔT where ΔT denotes expects valid time interval for transmission delay. Then Reader accepts the login request and go to next process, otherwise the Reader reject login request.

Reader computes –

Ai* = h (ID) xor h (X || h (ID))
Ri* = Ai* xor Ci
G = h (ID || PW)* =Cid xor Ri
Di* = h (ID || PW)* xor h(X)

And computes F* = h (Ai* || Di* || Ri* || Tu) And checks whether F and F* are equal or not. If they are not then reject the login request. If equal, then Reader R

Computes–

$$Fs = h(h(ID) || Di || Ri || Ts)$$

Where, Ts is remote Reader current time. And send acknowledge massage {Fs, G, Ts} to Tag Ti.

© 2012 Global Journals Inc. (US)

Upon receiving acknowledge massage Tag device compute G* = h (ID || PW) Fs* = h (h (ID) || Di || Ri || Ts) And checks where G =G*and Fs = Fs* are same or not. It is mutual authentication process. In which both Reader and Tag verify to each other. If they are same then Tag device makes session key (Sk) and both Reader and Tag share it. Sk = h (h (ID) || Ts || Tu || Ai) Otherwise terminate to again login process.

Password change Phase- This phase is involved whenever Tag T want to change the password PW with a new Password PWnew. Tag T keys in ID* and PW* and request to change password. The Tag device checks whether C = C* are equal or not. If it is satisfy User U is a legitimate bearer of the device. Then the Tag device asks the Tag Ti to input new password PWnew. After entering the new password the Tag calculate-

Bnew = Ai xor h (ID || PWnew) and

Dnew = h (ID || PWnew) xor h (ID || PW) xor Di

And change B with Bnew and D with Dnew in Tag device memory.

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. Result Analysis

Storages /Scheme	Our Scheme	Yoon Yoo al et. [3]	Liou al et. [7]	R.Song al et.[10]
Tag	480 bits	480 bits	480 bits	320 bits
Server	160 bits	320 bits	320 bits	480 bits

Table 1 : Storage Capacity Comparison

Table 1 shows, the storage comparison of the proposed scheme with the relevant user authentication based on smart card, Which shows our proposed scheme is reduced burden on the server, because the Server has store only server secret key (X).

Communication/Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Authentication (bits)	5*160	5*160	6*160	5*160

Table 2 : Communication Cost

The proposed scheme requires little more computation cost and equal to related user authentication scheme, Because our proposed scheme has strong secure mutual authentication scheme is resistance to insider attack, resistance to masquerade attacks, parallel session attack, replay attack, password attack, secure password change, protecting server spoofing attack, session key generation and agreement and other possible attack, that why some cost of execution are little more. Table 2 shows, the communication cost of the proposed scheme with the relevant user authentication based on Tag memory, which shows communication cost weightage between Tag and Reader in term of authentication.

Resistance to / Scheme	Our Scheme	Yoon Yoo et al. [3]	Liou et al. [7]	R.Song et al.[10]
Insider attack	Yes	No	Yes	No
Masquerade attack	Yes	No	Yes	Yes
Parallel session attack	Yes	No	Yes	No
Replay attack	Yes	Yes	Yes	No
Offline password attack	Yes	No	Yes	No
Secure password change process	Yes	Yes	Yes	Yes
Denial of service	Yes	No	Yes	No
Session key generation and agreement	Yes	No	No	Yes

Table 3 : The Efficiency Comparison

The efficiency of the proposed algorithm is very high because it is not involved in any time consuming modular exponential computing as shown in the Table 3.

© 2012 Global Journals Inc. (US)

VI. Conclusion

In this paper we show that the other authentication techniques involved in RFID are not so much secure and have high communication cost. We showed that our scheme is vulnerable to Denial-of-Service attack, Insider attack, Offline password attack Forward secrecy attacks. We present an efficient and secure ID- base remote user authentication scheme. The proposed scheme is proved to be able to withstand the various possible attacks. 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 Références Referencias

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.
15. Weis, sarma, rivest and Engels: a brief survey on rfid privacy and security. Crises reserch groupunesco chair in data privacy, 2003.
16. Boyeon song, chris j mitchell "rfid authentication protocol for low-cost tags" wisec'08, alexandria, virginia, usa.copyright 2008 acm 978-1-59593-814-5/08/03. march 31–april 2, 2008
17. Tieyan li, guilin wang, robert h. deng," security analysis on a family ofultra-lightweight rfid authentication protocols" journal of software, vol. 3, no. 3, march 2008
18. Md. endadul hoque," protecting privacy and ensuring security of rfid systems using private authentication protocols" marquette university, 2010.
19. E. Yoon and Yoo, 2005 "More efficient and secure remote user authentication scheme using smart card", in proceeding of 11th international conference on Parallel and Distributed System, pp.73-77.
20. Y.P. Liou, J. Lin and S.S. Wang, 2006 "A New Dynamic ID Based Remote User Authentication

© 2012 Global Journals Inc. (US)

Scheme using Smart Cards," Proc. 16th Information Security Conference, Taiwan, pp. 198-205, July.
21. R. Song. 2010 "Advanced smart card based password authentication Protocol". Computer Standards & Interfaces, Volume 32, Issue 4, June, Pages 321-325.
22. 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.

© 2012 Global Journals Inc. (US)