A Novel Security Method For RFID Tags

IMRAN ALI JOKHIO*, SANA HOOR JOKHIO**, AND JAVED ALI BALOCH**

RECEIVED ON 10.12.2011 ACCEPTED ON 21.06.2012

ABSTRACT

RFID (Radio Frequency Identification) tags use lightweighted security methods because of cost constraints. In this paper a lightweight security method is investigated and proved that it significantly lacks in protecting RFID tags against simple cloning attack. In order to protect RFID tag from cloning attacks a novel security method is proposed in this paper. The proposed security method provides high level computational difficulty against the three basic attacking techniques, i.e. eavesdropping, replay and man in the middle. In order to clone a tag, attacker eavesdrops the tag responses and creates a replica of the tag. The novel security method presented in this paper increases the hardness to avoid guessing tag secrets resulting in a conditional none clone able tags. The proposed security method is also evaluated using propositional logic proofs to demonstrate the level of security it can provide.

Key Words: **RFID Security, RFID Attacks, Cloning Attack, Lightweight Security Method.**

1. INTRODUCTION

In RFID system, tags have ability to digitize information and make it available, as these are very distributed and pervasive sources of information. The information RF (Radio Frequency) tag provides is the location and time of a physical object to a database system. EPC (Electronic Product Code) network that makes the most of the RFID technology has defined and specified the services for global implementation of RFID based SCM (Supply Chain Management) system. The middleware for RFID based distributed systems is based on the EPC Network [1]. An RF tag is a powerless source of information in the EPC network. It gets power from an RF signal sent by a reader. The communication channel between an RF tag and a reader is wireless [2]. An RF tag as a source of information must be checked if it is a reliable and authentic source, as any intruder can also send fake information. The tag has very little processing power and memory, which cannot be significantly increased because of the tag's manufacturing cost. The tags are attached to the physical objects that could also lead to personal privacy invasion for one who owns the physical object. Therefore, for successful and scalable deployments of RFID technology in SCM, inventory control etc. it needs to be assured that a tag may not be a source of information for an unauthorized entity.

In order to avoid above described issues, there is a need of a mechanism/method between the tag and the reader, which not only mutually authenticates the reader and the tag, but also prevents any leakage of information and avoids tracking of a tag [3-4].

* Assistant Professor, Department of Software Engineering, Mehran University of Engineering & Technology, Jamshoro.
** Assistant Professor, Department of Computer Systems Engineering, Mehran University of Engineering & Technology, Jamshoro.

Though a number of security and privacy methods are proposed, but there is no single method that protects the tag information against all known attacks. The methods available in the literature are aimed to protect certain attacks but not all. This work is focused at cloning attacks.In order to protect tags against cloning attack a method [5] is proposed. In this paper we prove that this work [5] is vulnerable to cloning attack. It is also proved that the security method is not scalable by analysing a number of scenarios. Beside, depicting a successful attack, we also propose an improved version of the security method that is more secure than [5].

2. RELATED WORK

In order to address the security and privacy requirements of RFID system, a number of security methods have been proposed. But in the context of this paper we only discuss the [5] as the shortcomings of this methods are highlighted and an improved version is proposed. For a thorough analysis and review of these proposed methods, [6-9] can be referred.

A very simple and straightforward algorithm is proposed to provide scalability [5]. In this work authors refer scalability, as:

"higher level security is possible with more computational facilities".

The algorithm suggests a secret C shared between tag and reader, a tag just needs a multiplication operation. The tag replies to the reader $E=R*C+I$, where * is a multiplication and + is an addition operator whilst R is a random number, I is a tag identifier. The reader identifies and authenticates a tag by calculating $I=E\%C$.

In order to clone a tag using this method, an adversary can easily launch an eavesdropping attack to get E and clone the tag at time t_o. Later at some other time t_1, cloned tag can easily get an illicit identification and authentication by just sending the eavesdropped response E of the genuine tag.

However, this cloning or spoofing attack is not possible against the method when R is also sent along with the E. Though it is not clear in the proposed work whether the tag or reader generates R. In order to discuss the method, all the scenarios are analyzed i.e. tag generates R and sends both R and E to the reader or the reader generate R and sends it to the tag. In fact it is not important where R is generated, but its more important that whether its transmitted over the wireless channel or not. Hence, if reader generates R then it must be transmitted. There can be two more scenarios if tag generates R, either it is transmitted over the wireless channel or not. An adversary capable of eavesdropping can get the secret C from a tag in a scenario when a tag generates R and transmits it, by just recording two sessions. Adversary can record the responses to get two equations of type $E=R*C+I$, where I and C are constants and adversary knows the E and R for the two equations. This enables an adversary to simply solve the two equations simultaneously to get the secre C and identifier I. This proof holds for a scenario when a reader generates R and sends it to a tag, as adversary can still get the similar two equations of type $E=R*C+I$ and solve them simultaneously. Therefore, this proof reveals that the proposed work is not secure at all. If R is not transmitted by either of the parties in an authentication and identification session, the authentication and identification overhead will be very high compared to that of an adversary's that tries to guess the secrets.

3. PROPOSED SECURITY METHOD

Security and privacy methods of RFID systems may have different requirements depending on applications and system entity requirements. The hash tree methods [10] are aimed toward a deterministic authentication server behavior while tags have some memory to store keys and encryption or one-way keyed hashing capability. Although

there are a number of applications where a tag may be restricted to very limited capabilities i.e. it may have some memory and it can only perform very few arithmetic and logical operations such as +,*,⊕ etc. The authentication server may need to use brute force or exhaustive searching whilst identifying and authenticating a tag.

A simple RFID security and privacy method [5], which requires minimal tag capabilities (i.e. basic arithmetic and logical operations) proposes that a tag and authentication server share secrets *C* and tag ID *I*. In an authentication and identification session the tag replies to a reader's hello message as:

$E = R^* C + I$

Where *R* is a random number generated by a tag.

The authentication server finds a tags from its database by calculating *I* as:

$I = E\%C$

The flaws in this method are discussed in previous section.

In order to overcome the deficiencies of this method, a very lightweight method is proposed that does not require a significant increase in tag capabilities. However, the proposed method uses only one more logical operation as compared to the method in [5]. Therefore this method is termed as ALGCAL (ALGebraic-LogiCAL).

In this method, a tag and authentication server share two secrets *C* and *D* instead of just one secret *C*. The tag ID *I* is same as in [5]. As a part of enhancing of the method there are certain issues regarding the shared secrets that should be taken into account while initializing tags. The length *l* of the shared secrets *C* and *D* has to be large enough that an adversary may not able to compute the shared secret *C D*, and tag ID I from a transmitted message over an unsecured wireless channel. The length of ID such as an EPC may be not increased because its length and data structure is a well-defined standard [11], so the difficulty to compute it also depends on the size of the secrets. The security method operations are shown in Fig. 1 and explain in following section.

3.1 Protocol Operation

A reader initiates an authentication and identification session with a hello message. A tag in reply generates a random number *R*, and to send a reply to the reader device, a tag computes *E* as:

$E = (R^*C+I) \oplus (R^*D+I)$

A tag's response is delivered to the authentication server as *(E,R)*. As the authentication server shares *C* and *D* with a tag, so it computes and performs a check find a match for a tag with ID *I* as:

$E_1 = R^*C + 1$ and $E_2 = R^*D + l$ (1)

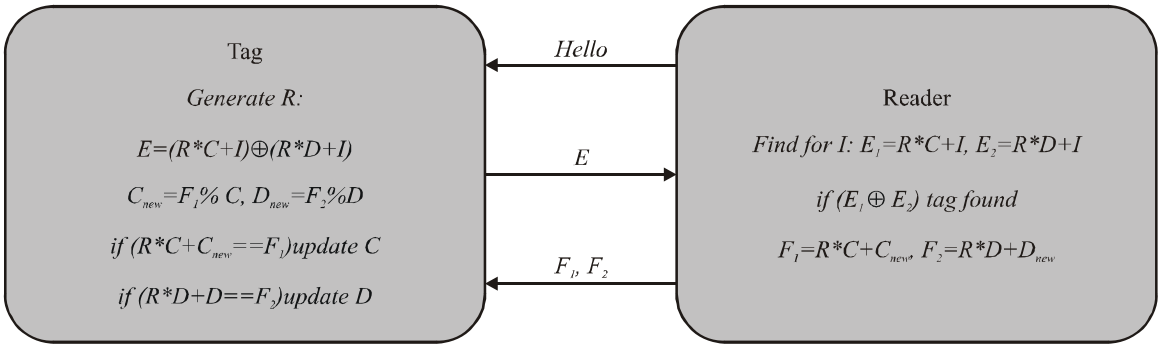

FIG. 1. ALGCAL SECURITY METHOD

if $(E_1 \oplus E_2)$ tag is found with an ID I. When the server authenticates a tag, the shared secrets for the tag are updated with F_1, F_2.

$F_1 = R*C+C_{new}$ and $F_2 = R*D+D_{new}$

On receiving F_1,F_2 the tag updates the secrets recovering C_{new}, D_{new} as:

$C_{new} = F_1 \% C$ and $D_{new} = F_2 \% D$

if $(R*C + C_{new} = = F_1)$ *updated C*

if $(R*D + D_{new} = = F_2)$ *update D*

The tag sends an acknowledgment to the server that it has updated the secrets. The ALGCAL method proposed in this paper provides the same or even increased level of security and privacy against active attacks as in [5].

This method provides enhanced security against passive eavesdropping and soft cloning or spoofing attacks. However it requires slightly more memory to store an extra secret and a $\oplus$ operator is also used in the tags. The authentication server uses the same searching technique: brute force search. Overall, this method does not require a significant increase in tag capabilities and provides an enhanced security and privacy for an RFID.

Following is the proof of correctness to show that this proposed method provides a secure identification and authentication scheme for RFID tags.

3.2 Proof of Correctness

For an RFID tag, authentication means a unique validity and verification of an encrypted string while maintaining the integrity (i.e. an encryption scheme needs to be collision resilient). In the proposed authentication method the encryption is done as given in Equation (1). A false detection of two tags is possible:

Suppose the secrets C_1, C_2 for two tags are related as:

$$C_1 > C_2 \tag{2}$$

then C_1 can be expressed as with some m,n relation bit strings or integers:

$$C_1 = n*C_2 + m \tag{3}$$

From equation (1):

$$G_1 = R_1 + C_1 + l_1 \tag{4}$$

Solving the above equations for an R_1 we can have:

$$G_1 = n*R_1*C_1 + I_2 \tag{5}$$

This will decrypt G_1 as a tag I_2. Similarly, this kind of decryption may occur for two D_1,D_2. In order to avoid the impact of this collision in the $E=E_1 \oplus E_2$ one of the randomly generated secrets C or D can be assigned monotonically arranged I's such that:

$$\textit{if } (I_2 > I_1) \textit{ then } C_2 > C_1 \tag{6}$$

Therefore with this condition applied in the server results in a collision resilient encryption method.

4. ANALYSIS OF MEMORY OVERHEAD

The overhead of a security method is calculated in terms of permanent memory requirement.

The proposed security method ALGCAL, improves the [5], hence comparison be- tween the two methods are compared for the analysis. The permanent memory required for [5] is 2l-bits, while the proposed ALGCAL security method requires 3l-bits. The additional l-bit are need to store an extra secret. However, this additional requirement of the memory is justifiable as the proposed security method ALGCAL provides additional security against the algebraic attack that can be launched against [5].

5. SECURITY ANALYSIS

Exposing RFID tags to an open environment, leads to a common threat model where a number of attacks may be launched using attacking techniques i.e. eavesdropping, replay attack and man-in-the-middle. Therefore strength of the proposed security method is evaluated against these basic attacking techniques.

In the proposed ALGCAL method, a tag can be identified and authenticated using the shared secrets *C,D* and tag ID *I.*

The proposed method is considered secureif the following proposition holds.

Proposition-1

The proposed security method is secure if it protects the shared secrets *C,D* and *I* against eavesdropping, replay and man-in-the-middle attacks.

Proof-1

Aneavesdroppingattackispossibleifanadversarycanget *C,D,Dnew,Dnew* or *I* from the messages *E*, F_1, F_2 and *ack.* In order to find *C,D* from $E=E_1 \oplus E_2$, the computational difficulty is $2^l x 2^l = 2^{2l}$, and finding the *C* and *D* simultaneously the computational difficulty is $2^{2l} x 2^{2l} = 2^{4l}$. Similarly,thecomputationaldifficultytofind C_{new}, D_{new} from *F1*, *F2*, is 2^l x 2^l = 2^{2l}. Therefore, it is proved that Proposition 1 holds for an eavesdropping attack.

End of Proof-1

Proof-2

A replay attack on server is not possible, if secrets of a security method are updated securely in each authentication session. In the proposed method secrets *C,D* are updated in each session and by Proof 1 an adversary cannot feasibly extract the secrets. Hence a replay attack is resisted on a server. An adversary may launch a replay attack on tag by resending F_1,F_2 captured from a previous successful authentication session *i* of the tag. This attack cannot be successful because the tag has already update ditssecret sintheauthentication session *i* as $C \leftarrow C_{new}$, $D \leftarrow D_{new}$. Whereas, the replayed F_1,F_2 have un-updated *C,D*, hence the tag resists this attack and does not update its secrets. Therefore, it is proved that Proposition 1 holds for replay attacks.

End of Proof-2

Proof -3

In a man-in-the-middle attack on server an adversary modifies or creates *E* by choosing correct secrets *C,D* and *I* for a tag. From proof 1, the computational difficulty of choosing correct secret is 2^l. Choosing each secret correctly are three independent events. This increases the computational difficulty of an integrity check to pass in server to 2^{3l}. Hence, a man-in-the-middle attack is not feasible on server. Similarly, finding the correct secrets to modify and construct F_1,F_2 is not feasible. Therefore it is proved that Proposition 1 holds for man-in-the-middle attacks.

End of Proof-3

In order to protect the shared secrets and tag ID, the proposed security method provides the computational difficulty in the order of 2^l that is normally considered as an acceptable security method. The appropriate length of the *l*, i.e. length of the secrets can be adapted to provide required level of security in a tag and server.

6. CONCLUSION

In this paper, a light weighted security method is investigated to evaluate its security strength. A formal proof to show that an attacker can easily launch attacks

against the existing security method. This is followed by the design of a novel security method that improves the security and privacy of RFID tags. The proposed security method is more secure, however it requires slightly more memory while implementing on RFID tags. This is justifiable with the improved security. A formal security evaluation is also done using propositional logic prove and depict the level of security provided by the proposed security method.

ACKNOWLEDGEMENTS

Authors are thankful to Mehran University of Engineering & Technology Jamshoro, HEC, Pakistan, and University of Leeds, UK, for providing funding to carry out this research work. This work would not have been possible without Prof. Jie's, guidance and suggestions. Authors are also thankful to colleagues and research team members for their support both at University of Leeds, and Mehran University.

REFERENCES

[1] EPCglobal, "The EPCglobal Network", 2004. http://www.epcglobalinc.org/. (Last Accessed January 2012).

[2] EPCglobal, "EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz", Standard, January, 2005.

[3] Juels, A., and Stephen, A., "Weis. Defining Strong Privacy for RFID", ACM Transactons on Information Systems Securiry, Volume 13, No. 1, pp. 1-23, 2009.

[4] Ronald, L., and Rivest, S.A., Weis, S.E.S., and Daniel, W.E., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing, Volume 2802, 2004 of Lecture Notes in Computer Science, pp. 50-59. Springer Berlin/Heidelberg, January, 2004.

[5] Mala, M., "Privacy for RFID Systems to Prevent Tracking and Cloning", International Journal of Computer Science and Network Security, Volume 8, No. 1, pp. 1-5, January, 2008.

[6] Domingo-Ferrer, J., Posegga, J., FrancescSebe, and Vicenc, T., "Advances in Smart Cards", Computer Network, Volume 51, No. 9, pp. 2219-2222, 2007.

[7] Gilbert, H., Matthew, J.R., and YannickSeurin, "Good Variants of HB+ Are Hard to Find, Financial Cryptography and Data Security", 12th International Conference, Cozumel, Mexico, January 28-31, 2008. Revised Selected Papers, pp. 156-170, Berlin, Heidelberg, Springer-Verlag, 2008.

[8] Krishan, S.K., and Jingde, C., "A Comparative Study of RFID Solutions for Security and Privacy: POP vs. Previous Solutions", Proceedings of International Conference on Information Security and Assurance, pp. 342-349, Washington, DC, USA, 2008.

[9] Ouafi, K., Overbeck, R., and Vaudenay, S., "On the Security of HB against a Man-in-the-Middle Attack", Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, pp. 108-124, Berlin, Heidelberg, Springer-Verlag, 2008.

[10] Dimitriou, T., "A Secure and Efficient RFID Protocol that Could Make big Brother (Partially) Obsolete", Pervasive Computing and Communications, Fourth Annual IEEE International Conference, pp. 275, March, 2006.

[11] EPCglobal, "EPC Generation 1 Tag Data Standards", Standard Specifications, EPCglobal, May, 2005.