# Vulnerability and Countermeasures of RFID System

Nidhi Chauhan

***Abstract*— In future Radio Frequency Identification (RFID) will become most widely used device. Radio Frequency identification is an emerging technology which brings gigantic productivity advantage in application where target have to be identified automatically in mobiles and ubiquitous estimate. A primary RFID security concern is the forbidden tracking of RFID tags which are world readable, artificial position a risk to both personal location privacy and corporate/ Military security such responsibility have been elevated with respect to the unites state department of defence .more generally privacy organization have show concern in the context of ongoing efforts to implant electronic product code (EPC) RFID tags in consumer product. To underrate security threats, security protocol play vital role. As with any protocol the security protocol comprises a prescribed sequence of communication between entities and is designed to achieve a certain solution. The non line of sight property of RFID increased convenience and efficiency but it also increased the system vulnerability. In this paper we review the existing security threats and security protocol.**

***Index Terms*—interrogator (reader), transponder (tags), security threats, security protocols.**

## I. Introduction

The basic concept of radio frequency identification (RFID) were developed during world war II, only recently has RFID become a ubiquitous technology in today's industry, market, and society. RFID is the wireless use of EM fields to transfer data for purpose of automatically identification and tracking tags attach to the object .RFID has ability to improve efficiency economy ,In every aspect like in access control ,supply chain , management ,public transportation ,open air events, airport baggage, express parcel , logistics many others . RFID do not have any protection mechanism for the stored information on the tag. In RFID finding the solution for security requirements has become major concern.

## II. Security Threats For RFID

### *A. Spoofing*

Spoofing is an activity whereby a counterfeit tag masquerades as a valid tag and thereby takes an illicit advantage. Tag cloning is a type of spoofing attack that take the data from a valid tag and then creates a copy of the captured data with a blank tag.

### *B. Mediator attack (man in the middle)*

A man in the middle attack is possible when the data is transfer between the two object. An attacker can impede the communication path and manipulate the information between the RFID components. The attack will change the information before it reaches to the intended device.

### *C. Snooping*

There exists a risk when the communication between transponder and reader takes place which is called snooping. Snooping takes place when a tag is being read by an authorized RFID reader an enemy block the data with any compliant reader for the correct tag family and frequency. Since the most RFID system use clear text communication due to tag memory capacity and cost. Snooping is a simple but efficient means for the attacks to obtain information which is stored in the transponder.

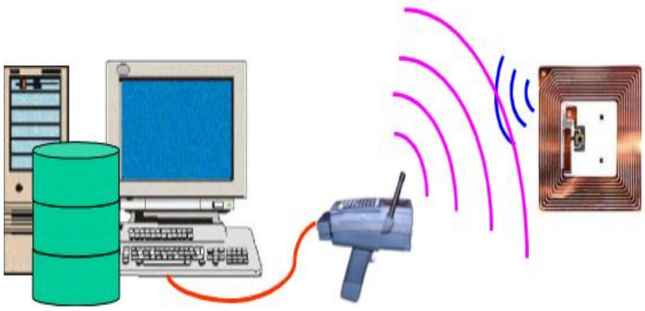


**Figure 1. A generic RFID system**

### *D. Repudiation of Services*

The purpose of ROS is not to abduct or modify the information but to debilitate the RFID system so that it cannot be used. Another type of ROS is to destroy or debilitate RFID tags by removing them from the items, washing out their stored information.

### *E. Replay*

In this type of attack an enemy stop the communication between transponder and interrogator and to capture a valid RFID signal. At after some time when the attacker receives a query from the interrogator this captured signal is re-entered into the system. Since the data appears valid it will accepted by the system.

### *F. Desynchronizing attack*

Antagonist can create a desynchronizing state between interrogator and transponder by intercepting certain transmitted data. This aberrant state can occur in a TID and secret key update of RFID .If any one of the secret key's values in the transponder is desynchronize the legal transponder cannot be authenticate.

### *G. Side channel analysis*

Side channel analysis is a form of power analysis in which the aim is, by analyzing the change of power consumption to crack the password. It is true that power consumption patterns

**Manuscript received September 20, 2014.**

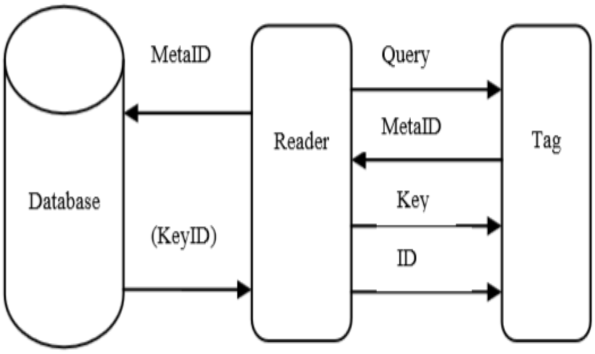
**Nidhi chauhan** : I did Btech from GBTU and currently pursuing MTECH from Jaypee University of Information and Technology.

are different when the tag receive incorrect and correct password bits.

## III. Security Protocol Review for RFID

### A. *Hash lock protocol*

Hash lock protocol includes the concept of locking and unlocking the transponder to allow access. In hash lock scheme it is require on the tag to implement the cryptographic hash function and managing keys at the backend. The tag does not declare its stored information until the interrogator sends the correct key corresponding to the meta-ID [4].



### B. *Enhanced Hash lock Protocol*

This enhanced protocol helps to prevent the disclosure of meta-ID during a tag is in the lock mode. The randomized hash lock protocol requires transponder to figure out a one way hash function and add an onboard, random number generator. During the questioning process prevents tracking of individuals depends upon metal id's.

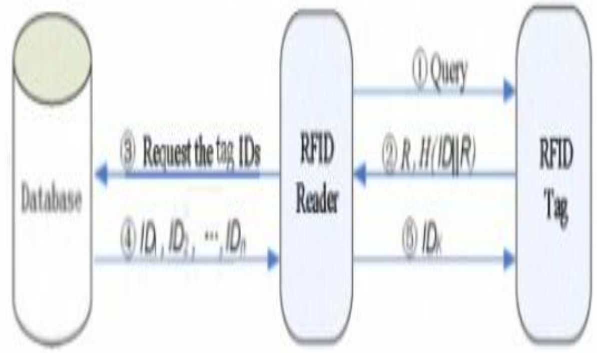


Fig. Execution process of Enhanced Hash lock

### C. *Li's Protocol*

Li's protocol is depend on XOR operation and shared pseudonym. In this protocol by using a shared SID between transponder and back end system database so that during each reading the transponder challenges the interrogator with two arbitrary numbers. Which mark a segment of SID become the partial ID.

### D. *Henrici and Muller's protocol*

For low cost RFID system Henrici and Muller proposed an adequate and easy authentication protocol. This protocol is depend on a hash function is inserted into a tag and a random number generator on a back-end database to secure the user privacy information, user location privacy and the replay attack [5]. However this protocol cannot stand against the man in middle attack.

### E. *Jules' Protocol*

Juels' enter into the concept of multiple pseudonyms as one time pads [7]. In this protocol the whole back end database must search by each reading to rule out impossible tags and then mark the corresponding pseudonym invalid. The cut down version focused that most tags only perform the first step of the protocol so that attacker cannot obtain useful information but only pseudonym. This also create a problem of running out of pseudonyms due to the fact they were statically planted into the tag before being sold.

### F. *Sasi Protocol*

This protocol is based on the same basic operation of m^2 AP [8] which is called ultra-light-weight it has 3 share secret key and two arbitrary number by taking XOR operation to implement the encryption. The share secret key and random number update each time for achieving forward security feature. But this easily suffers de-synchronization attack because the key's updating does not adopt strict limit, exploratory retroversion mechanism and lack the exception handling mechanism.

### G. *LPN Based Protocol*

In this protocol juels et [7] proposed HB+ which based on the learning parity with noise (LPN)

Problem and employs binary inner product. HB+ [7] [9] with a noise bit repeats a basic authentication protocol and accepts the tag of a very limited number of response are invalid. But this protocol suffers from tracking problem, MIM problem and violation of tag anonymity.

### H. *Universal Composability Protocol*

This protocol provides a mechanism to prevent de-synchronization of secret key attack as well as it also prevent privacy, forward security .O-FRAP uses pseudonym approach for privacy purpose [20].O-FRAP can also use the concept of key exchange [11] [15].

### I. *Multi Tag Scanning Protocol*

This is the first protocol which focus the multiple tag scanning problem. This protocol is also called yoking-proof [12] [13] in which the main idea is to let 2 tags sign each other in order to prove each other presence.

### J. *Distance Bounding Protocol*

The first protocol which focused mafia fraud attack [14] [16] against RFID. The key idea behind this protocol is to simply repeat the authentication step multiple times so that each step can be complete in very less time.

## REFERENCES

[1] Qinghan Xiao1, Senior Member, IEEE, Cam Boulet1, and Thomas Gibbons2"RFID Security Issues in Military Supply Chains" Defence Research and Development Canada Ottawa Qinghan.Xiao@drdc-rddc.gc.ca Boulet.Cam@drdc-rddc.gc.ca 2 Operational Support Transformation – CANOSCOM.

[2] Hoda Daou, Ayman Kayssi, Ali Chehab" RFID Security Protocols" Department of Electrical and Computer Engineering American University of Beirut, Lebanon.

[3] Dang Nguyen Duc, Hyunrok Lee, Divyan M. Konidala, Kwangjo Kim KAIST, Daejeon "Open Issues in RFID Security" , Republic of Korea.

[4] S.A.Weis, S.E.Sarma, R.L. Revest, D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems" accepted for publication to the First International Conference on Security in Pervasive Computing (SPC 2003),March 12-14,2003.

[5] D. Henrici and P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," Proc. 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOM W'04),p p. 149-153,2004.

[6] Ari Juels and Stephen Weis, "Authenticating Perva- sive Devices with Human Protocols", In the Proceed- ings of CRYPTO'05, Victor Shoup (Eds.), Springer- Verlag, LNCS 3261, pp. 293-308, 2005

[7] Jonathan Katz and Ji Sun Shin, "Parrallel and Concurrent Security of the HB and HB+ Proto- cols", Available at http://eprint.iacr.org/ 2005/461.pdf.

[8] H.Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," IEEE Trans. Dependable and Secure Computing,p p. 337-340,2007.

[9] J. Bringer, H. Chabanne, and E. Dottax, "HB++: A Lightweight Authentication Protocol Secure against Some Attacks", In the Proceedings of IEEE Intl Con- ference on Pervasive Services, Workshop Security, Privacy and Trust in Pervasive and Ubiquitous Com- puting, 2006.

[10] Tri Van Le, Mike Burnmester and Breno de Medeiros, "Universally Composable and Forward Secure RFID Authentication and Authenticated Key Exchange", In the Proceedings of the 2nd ACM Symposium on In- formation, Computer and Communications Security, pp. 242-252, March 2007.

[11] MikeBurnmester, TriVanLe, BreneDeMedeirosand Gene Tsudik, "Universally Composable RFID Identi- fication and Authentication Protocols", In the ACM Transactions on Information and Systems Security, Vol. 12, No. 4, Article 21, April 2009.

[12] Ari Juels, "Yoking-Proofs for RFID Tags", In the Pro- ceedings of First International Workshop on Pervasive ComputingandCommunication Security, IEEEPress, pp. 138-143, 2004.

[13] Selwyn Piramuthu, "On Existence Proofs for Multiple RFIDTags",IntheProceedingsofACS/IEEEInternational Conference on Pervasive Services, IEEE Com- puter Society, pp. 317-320, 2006.

[14] Chong Hee Kim and Gildas Avoine, "RFID dis- tanceboundingprotocolwithmixedchallengestopre- vent relay attacks", Available at http://eprint. iacr.org/2009/310.

[15] Khaled Ouafi and Raphael C.-W. Phan, "Traceable Privacy of Recent Provably-Secure RFID Protocols", In the Proceedings of ACNS 2008, Springer-Verlag LNCS 5037, pp. 479-489, 2008.

[16] G. Hancke and M. Kuhn, "An RFID distance bound- ing protocol", In the 1st International Conference on Security and Privacy for Emergin Areas in Communi- cations Networks (SECURECOMM05), IEEE Com- puter Society, pp. 67-73, 2005.

[17] "Research on RFID Security Protocol Based on Grouped Tags and Re-encryption Scheme" Chunhui Piao School of Economics and Management Shijiazhuang Tiedao University Shijiazhuang, China Zhenjiang Fan School of Computer and Information Engineering Shijiazhuang Tiedao University Shijiazhuang, China fanzj Chunyan Yang Office of Academic Affairs Shijiazhuang Tiedao University Shijiazhuang, China , Chunyan Yang Office of Academic Affairs Shijiazhuang Tiedao University Shijiazhuang, China .

[18] Lijun Gaol,2 ,Zhang LuI" Low-Cost RFID Security Protocols Survey " Department of Computer Science and Technology, Shenyang Aerospace University, gaolijun061O@163.com 2School of Computer Science and Technology, Tianjin University, Tianjin.

[19] Hyun-Seok Kim, Jin-Young Choi Dept. of Computer Science and Engineering Korea University Seoul, KOREA Dept. of Electronics Engineering and Information Science Korea Military Academy Seoul, KOREA .

**Nidhi chauhan** : I did Btech from GBTU and currently pursuing MTECH from Jaypee University of Information and Technology.