Research Survey of RFID Security and Privacy Based on Identification and Authentication Protocols

Yunus Usman Memon[#1],Sameen Ahmed Khan[*2]

[1] Research Scholar,JJTU, Jhunjunu, Rajasthan,India

[2] Salalah College of Technology, Salalah, Department of Engineering, OMAN
[1]E-Mail: iyunus2003@yahoo.com

Abstract—The objective of this paper is to present recent technical research proposed in the literature for addressing the security and privacy issues in Radio Frequency Identification . RFID technology is being used since world war II has been deployed in various applications. However when it comes to low cost, reliable and long lasting RFID there are number of challenges posed by the inter security and privacy of RFID system. Solving these privacy and security issues is a challenge for this technology. This paper investigates non cryptographic and cryptographic authentication protocol proposed by the researcher in recent years for security and privacy of RFID systems.

***Keywords*– RFID, security, privacy symmetric encryption, EPC**

I. INTRODUCTION

RFID is a enable technology by which the user communicate, collaborate, educate, sell, entertain and distribute products. It is a technology in which there exist contactless transfer of data, between the device which carries the data and its reader. It is one of the fast developing and a technique which has tremendous potential and has been implemented in many areas such as asset management, identify objects or people, supply chain, healthcare etc. The basic RFID system consists of tag which is attached to an object with unique identification. The tag has all the information of the object. The tag has three flavors active, passive and semi-active. Active tags have a read range of up to 300 feet (100 meters) and can be read reliably because they broadcast a signal to the reader (some systems can be affected by rain). They generally cost from $10 to $50, depending on the amount of memory, the battery life required [29].Passive tags have no built in power source. A semi-active tag is combination of passive and active tags. A RFID system has three important components namely the reader, tag and backend servers [6].

A. RFID SECURITY AND PRIVACY THREATS

RFID technology significantly increases the efficiency and effectiveness of company deploying RFID technology. In operation RFID technology requires complex computing and communication skills, the characteristics like the frequency, range, types of memory data and security affects RFID performance. There are two types of coupling used inductive coupling for low and high frequency passive systems, the read range is smaller, as tag needs energy for operation from reader, and propagation coupling uses ultra high frequency for long distance. A reader acquires data stored from the tag which is in the read range converts the signal into one or zero bits of stream which is then passed to a backend server which regains the detailed information of object attached by RFID tags. A reader has capability of reading multiple tags in the read range at the same time. Since the communication is contactless it exposes many security and privacy threats such as Passive/active eavesdropping, Cloning, Man-in-the-Middle, Denial of Service (DoS), Physical threat [10].The detail classification is depicted in figure 1.

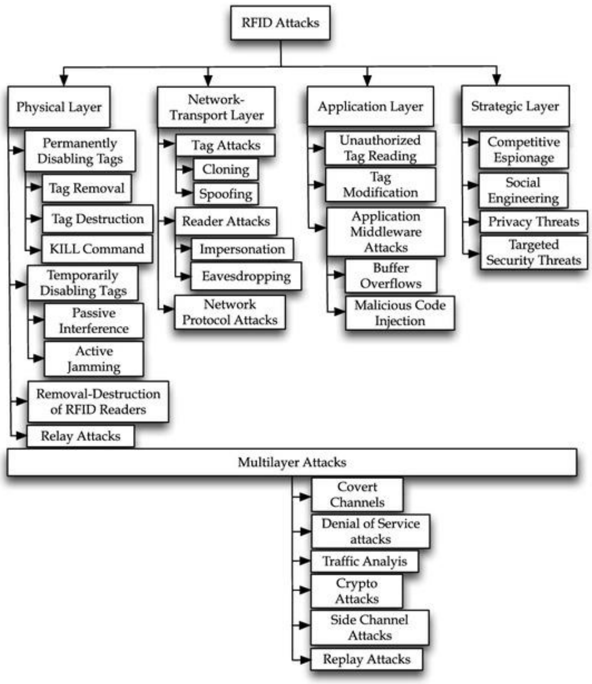

Figure. 1. Classification of RFID attacks [15]

The structure of rest of the paper is as follows. In the following section various basic approaches to the privacy based on non cryptographic such as Kill and sleep, Clipped tag approach is described. Then in section III we enumerate the survey based on cryptographic approaches followed by APF, hash based protocol and in the last section protocol based on lightweight and ultraweight.

II. APPROACHES WITHOUT CRYPTOGRAPHIC

Basically RFID tags offer few or no security features. Tags with basic security increases the cost of tags especially if encryption features are needed. Here in this section RFID tags with low cost security and privacy approaches are addressed.

1) *Kill and sleep approaches:*

In [18] Juels suggested the use of kill command which is one of the simplest privacy approaches. The EPC (Electronic Product Code) tag supports kill command. A 32 bit access password protected kill command is sent to the tag to permanently deactivate it. Once the command is executed the tag will no longer respond to a reader. The disadvantage of kill command is that the tag is permanently deactivated and cannot be used again. A case study of application of EPC tags by [20] suggested counter measure to protect the tags for reuse The sleep approach by [4] proposes to put the tag in sleep mode and activate it when needed.

2) *Blocker tag approach:*

It is one of the low cost implementable approach for RFID. In this selective blocking approach[9] the blocker tags enables the consumer to hide or reuse the tag for scanning, when carried by a consumer instead of kill or sleep command the blocker tag can block particular ID codes or those in a privacy zone.

3) *Clipped tag approach:*

In [11] Gunter and Paul proposed the clipped tag approach. In this approach a consumer can mechanically deactivate a tag at checkouts using perforated tear off by separating the chip from the antenna without physical destruction as it can damage the original item [23] .Reactivation of the tag can be done by electromechanical means. Sozo I. and Hiroto Y. [22] proposed a method in which each object has two ID, one permanent and other temporary this protect privacy of each user.

4) *RFID Guardian:*

Rieback [25] proposes a battery powered device which performs two way RFID communication and manages RFID keys, block the users RFID tag form unauthorized readers. It Provide access to in vicinity RFID readers and display all RFID tags it has scanned. It is portable and solely meant for personnel use. It integrates four security properties auditing, key management, authentication and access control.

III. CLASSIC CRYPTOGRAPHIC APPROACH

The basic idea in these approaches is to protect the data by storing in chipper text format instead of clear text format.

1) *Probabilistic public key encryption:*

In [21] suggested the implementation of encrypted ID inside the tag. This scheme generates different anonymous ID whenever there is a communication between tag and reader. The encryption results are totally different even if same ID is encrypted. This scheme prevents leaking of consumer data but tracking is still possible. In this regard [3] implemented re-encryption which refreshes anonymous ID stored in the tag frequently by external re-encryption device. The reader obtains the encrypted ID from the tag memory and replaces the encrypted ID with the new re-encryption ID.

2) *Public key re-encryption:*

Golle, et.al [27] propose to have a private and public key in communication of RFID tag and reader respectively the encrypted message prevents unauthorized reading and the additional feature of re-encryption the public key on a particular tag is changed to avoid tracking and protects the privacy of consumer.

3) *Shamir Tag:*

The Juels [1] approach fulfill the basic privacy requirement of providing unauthorized reading and tracking by the use throttling tag replies and simple ID rotation without the use of expensive crypto-circuitry respectively. In the extended research, [13] proposes a approach that combines Minimalist cryptography with crypto graphically light weight solution called Shamir tag. The need of cumbersome and costly password management and ID mapping is alleviated by using bit throttling and shared secret mechanism.

IV. AUTHENTICATION PROTOCOL FRAMEWORK APPROACH

Xiaoqing and Hui [2] has proposed a authentication protocol conforming EPC global standard for RFID security. The tag memory is divided into four logical memory bank each reserved for storing a tag kill password, EPC memory, tag information for transmission and public key. The tag reader communication is certified by CA server. This protocol provides a strong security between a tag and a reader. In each authentication process different key is shared to avoid tracking by message encryption and eavesdropping

Lan zhang [5] propose a approach based on symmetric encryption. The tags memory holds the reader ID as a secret key in advance. If a reader communicates with a tag the reader will sent a random number ‘k’ for encryption. The output of the tag is the encryption of tagID $\oplus$ k with readerID without mutual authentication, as the encryption process is very fast multiple tags can be read. The reader gets the tagID by decryption This scheme prevents spoofing and prevents attack by unauthorized reader or tags. The encryption and decryption increases the cost of the tag.

Shuai shao & Yanfei scheme [12] is based on Scalable RFID Pseudonym Protocol [7] which utilizes tags response based on hash functions. In this scheme multiple tags can be managed with high security and privacy in a constant time only if the reader was the last to communicate with the tag else the tag cannot be authorized by the reader. This protocol defends against replay attack eavesdropping, tampering and impersonation attack.

V. HASH FUNCTION BASED AUTHENTICATION PROTOCOLS

Authentication protocol based on hash function is an important category used in RFID system which is capable of computing one way cryptographic function and provides high security as compared to basic RFID tags, but the cost factors limits the use.

1) *Locking approach:*

In this protocol [14] the hash enabled tag operates in locked or unlocked state with the help of a temporary metalID which is a hash of random key .To lock a tag the metalID (the random hash key) is stored in the tag. To unlock the reader sends the query to a tag ,the tag respond to the query with metalID to backend which computes and provide a proper a key and ID, the tag hashes the key and compares it with metalID if the value matches the it unlocks itself ,This process is illustrated in figure 2.

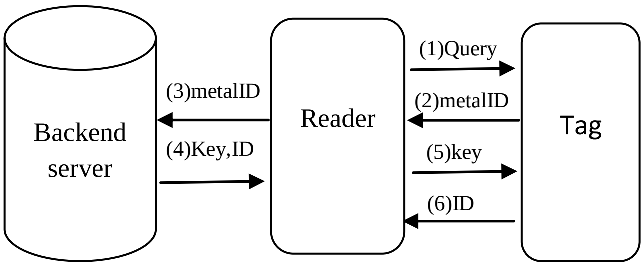

Figure 2. The work process of Hash Locking approach

2) *Randomized locking:*

This is a hash locking extended scheme with random number generation.[19]In unlocking operation the tag respond to the reader by generating a random number along with its ID and computes it with hash function. In each communication a different random number is generated. This scheme protects location privacy. This process is illustrated in figure 3

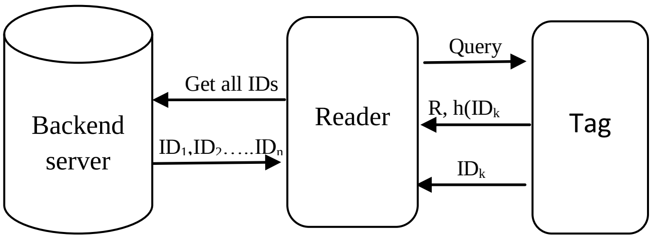

Figure 3. The work process of Randomized locking approach

3) *One-time pad scheme:*

In [8] scheme the tag is identified by the tag keys along with the list of one time pads of each tag. A low cost, effective XOR operation is used. This scheme uses fresh pseudonym for the data encryption and GNY logic [26] to guarantee data anonymity and data authenticity and data secrecy

VI. LIGHTWEIGHT AND ULTRALIGHTWEIGHT PROTOCOLS

Low cost tags are classified as Lightweight and ultralightweight. Both can perform simple XOR operation. In addition to this ultralightweight can process RNG and CRC also. The three protocol proposed by Lopez et.al in 2006 were ultralightweight protocols a first step towards low cost tags security.M^{2}AP (Mutual-Authentication Protocol) [30], EMAP (Efficient Mutual Authentication Protocol) [32] and LMAP (Lightweight Mutual Authentication Protocol) [33].

In [28] Juels extended the human to computer authentication protocol adopted by Hopper and Blum(HB) [30] which can also be considered as ultralightweight protocoland proposed a new HB$^+$ protocol suitable for EPC Gen-2 tag using lightweight symmetric keys. The security of [28] and [31] is based on learning parity with noise problem. This protocol provides security against active adversaries

Li et al [16] proposed a lightweight protocol for low-cost RFID which uses substring function. As this protocol uses only XOR operation along with substring function hence it is called as lightweight. In this protocol, the tag and backend server share a secure ID (SID) of *l*-bit length. Each time the tag and reader communicate, the reader must authenticate the two random numbers n_1 and n_2 by the tag thus a secure ID (SID) becomes a partial ID (PID).This process is illustrated in figure 4.

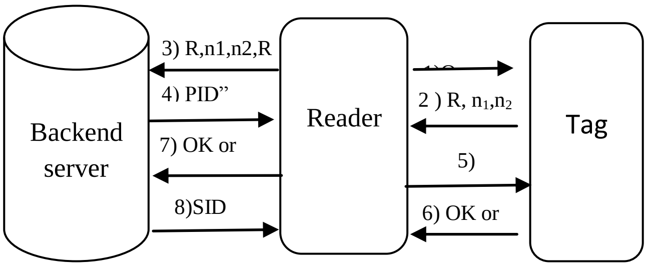

Figure 4. The work process of Li et al

Burmester and Medeiros [24] proposes four protocols with different levels of privacy for EPC gen 2 compliant RFID protocol using (Pseudo Random Function) based on PRNG. The tag encrypts the message using RNG along with a key of size 16 bits shared by the tag and reader. After completion of operation the backend server and tag updates their values. This scheme does not provide anonymity or ensure privacy.

In [17], Lee proposes two new ultralightweight authentication protocols, DIDRFID and SIDRFID. In this XOR and rotation operation is used. The computation cost is very low hence it is implemented in ultralightweight RFID tags. In process DIDRFID protocol each tag needs one static and two pairs of (DIDT and K) dynamic identity and secret information. In SIDRFID protocol each tag store the rag and reader identity.

VII. CONCLUSIONS

RFID is a fast growing technology which is being incorporated and used in many applications such as assets tracking, manufacturing, supply chain management, retailing applications such as shopping, passport, security and access control, smartphones. All these advantages are overshadowed by security and privacy issues especially for low cost RFID systems. In this paper we examined many of the basic and recent research made in the direction of security and privacy of RFID based basic approaches and authentication protocols but this solution fails to provide full security and privacy for low cost RFID resource constrained tags. So there is wide scope of research and development in low cost RFID system.

REFERENCES

[1] A. Juels, “Minimalist cryptography for RFID tags”, in Security of Communication Networks (SCN), C. Blundo, Ed., Amalfi, Italy, Sept. 2004.

[2] Gong, Xiaoqing, et al. "An Authentication Protocol Applied to RFID Security Systems" Information Assurance and Security, 2009. IAS'09. Fifth International Conference on. Vol. 2, IEEE, 2009.

[3] Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID Privacy Issues and Technical Challenges. Communications of the ACM, 48(9), 66-71.

[4] Pateriya, R.K., 2011. Sangeeta Sharma, “The evolution of RFID security and privacy”, International Conference on Communication Systems and Network Technologies.

[5] Lan Zhang, Huaibei Zhou, etc., "An Improved Approach to Security and Privacy of RFID Application System", Wireless Communications, Networking and Mobile Computing, Proceedings. 2005 International Conference on, Vol 2, pp.1195-1198.

[6] Imran Erguler , Emin Anarim, “Security flaws in a recent RFID delegation Protocol”, Personal and Ubiquitous Computing, v.16 n.3, p.337-349, March 2012.

[7] Song, C. J. Mitchell, "Scalable RFID Pseudonym Protocol", Proc. 3rd International Conference on Network and System Security, Gold Coast, Queensland, Australia, Oct. 2009, pp. 216-224.

[8] Jung-Hyun Oh, Hyun-Seok Kim and Jin-Young Choi, “A Secure Communication Protocol for Low-cost RFID System”, Computer and Information Technology, 2007. 7th IEEE International Conference on.

[9] L. Rivest, and M. Szydlo, “The blocker tag: Selective blocking of RFID tags for consumer privacy,” in Proc. 8th ACM Conf. Comput. Commun. Security, V. Atluri, Ed., 2003, pp. 103–111.

[10] D.C. Ranasinghe, P.H. Cole, “Confronting Security and Privacy Threats in Modern RFID Systems”, Fortieth Asilomar Conference on Signals, Systems and Computers (ACSSC '06), 2006, pp. 2058-2064.

[11] Gunter Karjoth and Paul A. Moskowitz. Disabling RFID tags with visible con_rmation: clipped tags are silenced. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES 2005), pages 27{30, Alexandria, VA, USA, 2005. ACM Press.

[12] Shuai Shao, Guoai Xu, and Yanfei Liu. “Efficient RFID authentication scheme with high security”, In Communication Software and Networks (ICCSN), 2011IEEE 3rd International Conference on, pages 238 –241, may 2011.

[13] Marc Langheinrich and Remo Marti. Practical minimalist cryptography for RFID privacy. IEEE Systems Journal, 1(2):115{128, December 2007. Available from World Wide Web: ww.vs.inf.ethz.ch/publ/papers/ shamirtags07.pdf.

[14] Xingxin Gao; Zhe Xiang; Hao Wang; Jun Shen; Jian Huang; Song Song;;An approach to security and privacy of RFID system for supply chain; IEEE International Conference on 13-15Sept.2004 Page(s):164-168.

[15] Mitrokotsa, M. Rieback, and A. Tanenbaum, "Classifying RFID attacks and defenses," Information Systems Frontiers, vol. 12,2010, pp. 491-505.

[16] Y.Z. Li et al., “Security and Privacy on Authentication Protocol for Low-Cost RFID,” Proc. Int’l Conf. Computational Intelligence and Security (CIS ’06), Nov. 2006

[17] Yung-Cheng Lee. Two ultralightweight authentication protocols for low-cost RFID tags. Applied Mathematics and Information Sciences, 6(2S):425{431, May 2012.

[18] Juels, “Rfid security and privacy: A research survey,” IEEE Journal on Selected Areas in Communication, vol. 24, no.2, pp.381– 394,February 2006

[19] S. A. Weis, S. E. Sarma, and R. L. Rivest et al, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, Inter. Conf. on Security in Pervasive Computing-SPC 2003, pp. 454-469, 2003.

[20] Koscher, K., Juels, A., Kohno, T., and Brajkovic, V. (2008) EPC RFID tags in security applications:passport cards, enhanced drivers licenses, and beyond. RSA Laboratories; Manuscript.

[21] Karl Christian, maria elisabet Oswald, side Channel Analysis of stream ciphers, Institute for Applied Information Processing communication (IAIK),Graz university of Technology,2004

[22] Sozo Inoue and Hiroto Yasuura, “RFID privacy using user-controllable uniqueness,” in Proc. RFID Privacy Workshop, Nov. 2003.

[23] D. Luckett. The supply chain. BT Technology Journal, 22(3):50–55, July 2004

[24] Mike Burmester and Breno De Medeiros. The security of epc gen2 compliant RFID protocols. In Proceedings of the 6th international conference on Applied cryptography and network security, ACNS’2008, pages 490–506, Berlin, Heidelberg. Springer-Verlag.

[25] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006.

[26] Gong, Needham and Yahalom, "Reasoning About Belief in Cryptographic Protocols”. 1990.

[27] Golle, P., Jakobsson, M., Juels, A., Syverson, P. (2004). Universal Re-encryption for Mixnets. In Okamoto, T. (Ed.), RSA Conference Cryptographers’ Track ‘04 (pp. 163-178). Springer-Verlag.

[28] Ari Juels and Stephen Weis. Authenticating pervasive devices with human protocols.In Victor Shoup, editor, Advances in Cryptology - CRYPTO 2005, volume3621 of Lecture Notes in Computer Science, pages 293–308. Springer Berlin /Heidelberg, 2005.

[29] http://www.rfidjournal.com/articles/view?1337/2

[30] Pedro Peris-Lopez, Julio César Hernández Castro, Juan M. Estévez-Tapiador,and Arturo Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In UIC, pages 912–923, 2006.

[31] Nicholas J. Hopper and Manuel Blum. A secure human-computer authentication scheme. Technical report, 2001

[32] Pedro Peris-lopez, Julio César Hernández Castro, Juan M. Estevez-tapiador, and Arturo Ribagorda. EMAP: An efficient mutual authentication protocol for lowcost RFID tags. In In: OTM Federated Conferences and Workshop: IS Workshop,pages 352–361. Springer-Verlag, 2006.

[33] Pedro Peris-lopez, Julio César Hernández Castro, Juan M. Estevez Tapiador, and Arturo Ribagorda. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In In: Proc. of 2nd Workshop on RFID Security, page 06. Ecrypt, 2006.