A RESEARCH SURVEY: RFID SECURITY & PRIVACY ISSUE

Monika Sharma[1] and Dr. P. C. Agrawal[2]

[1]Research Scholar Mewar University
Department of Computer Science & System Studies, Chittorgarh, Raj., INDIA
monika_05@rediffmail.com
[2]Guest Professor Mewar University &
Retired 'Scientist E' Ministry of communication &
Information Technology Govt. Of India, New Delhi.

ABSTRACT

"Information security and privacy" is one of the major challenges in the communication world of IT as each and every information we pass need to be secured enough to the extent that it doesn't hurt anyone's privacy. In trace and track world RFID play a pivotal role. We cannot track people as it causes a privacy risk. Migration of data to cloud also comes under threat as many things cannot be control over there. A trusted database is needed which can maintain and enforce the privacy policy. In order to cater all these requirements, a secure, cheap and complex computation encryption-decryption algorithm is required to meet this challenge.

This paper is based on the research survey of previous and current security and privacy techniques used for securing RFID tag and reader communication and their impact on real world.

KEYWORDS

RFID, Security, Privacy, PIR, Encryption, Decryption.

1. INTRODUCTION

RFID is a system that facilitates the tracking of objects as well as people via a technology comprised of a reader, a Transceiver with decoder and a transponder (RF tag). RFID Journal magazine defines an RFID tag as "a microchip attached to an antenna that is packaged in a way that it can be applied to an object. A tag is a type of device that can be attached to a person or a manufactured object for the purpose of unique identification and a reader is an electronic device that broadcasts a radio signal to a tag, which then transmits its information back to the reader [8].

There are following components which define the RFID Tracking System:-

- Determining location i.e. where the tag was read.
- Determining time i.e. what time the tag was read.
- The EPC (Electronic Product Code) is a unique identifier of the tagged object or person.

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA, UBIC - 2013
pp. 255–261, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3526

Streams of RFID data records are defined in the form of EPC (Electronics Product Code), location (loc) and time (t) where each record indicates that an RFID reader in location (loc) has detected an object having EPC at time t. The path of an object is defined by loci, ti, which is a sequence of pair that is obtained by first grouping the RFID records by EPC and then sorting the records in each group by timestamps. A timestamp is the entry time of an object in location assuming that the object is staying in the same location until its new location is detected by another reader [7]. RFID is a wireless system that works in conjunction with an organization's information technology infrastructure to improve business processes [1].

The RFID tag cannot determine the time and location independently [2]. The RFID tag cannot maintain an internal clock to determine time by itself, not capture IP address or GPS coordinates to determine its location independently.

RFID technology is used in many areas like medical, transportation, passport, library etc. for object identification. In today's scenario as of now, RFID tags are mostly used in proximity cards, automated toll-payment transponders and payment tokens. Previously as its readings are more accurate than (mostly manually operated) barcode systems, RFID tags can be integrated within the structure of packaging material or even within products.

2. SECURITY & PRIVACY RISK

Widespread RFID deployment creates privacy risks for everyone. In this case, a reader would periodically broadcast a query and all the reader in the vicinity will respond to that reader. The reader will then forward these responses to the database.

For instance, an unauthorized user can use the reader or buy another to communicate directly with the tag. So, RFID data can easily be attacked. There are various attacks like sniffing, tracking, spoofing, replay [20] and Denial of service cause security and privacy risk for RFID technology [21].

2.1 Data Security Issues of RFID Tag

At present, RFID is mainly facing the following three issues of security:

- Information of RFID tags are intercepted
- RFID tags can be cracked
- RFID tags can be copied

Louis Parks, president and CEO of SecureRF, had spoken on RFID security on 1st June-2011. He said that there's a great need for security in the case where we see data-enriched tags coming onto the market. That means we're going to push the critical data out to the very edge of a supply chain or a maintenance chain where the data will be on the tag and it will be critical that the data needs to be protected.

3. PRIVACY SOLUTIONS AND THEIR LIMITATIONS

3.1 Privacy Threats Phases & Preserving Techniques

There are two phases of data privacy threats in terms of physical RFID tags:-

- Data Collection
- Data Publishing

Many privacy preserving technology [8] like EPC re-encryption and killing tags[9] addresses the privacy threat in the data collection phase whereas anonymization algorithms works on the privacy threat in the data publishing phase [7]. The anonymization algorithm for the query engine transforms the raw object-specific RFID data into a version that is immunized against privacy attacks.

Many privacy models such as K-anonymity, L-diversity, T-closeness has been proposed to thwart privacy threats caused by the record linkage and attributes linkage attacks in the context of relational databases. All these models works assuming that a given set of attributes called quasi-identifier (QID) can identify an individual. However these models are effective for anonymization on relational databases but these models are not applicable to RFID data (due to high dimensionality nature of RFID data).

RFID is high dimensional because of the large combinations of location and timestamp. For example, if a subway is having 100 stations that operate 20 hrs per day, then RFID table would have 100 X 20=2000 dimensions. Applying traditional privacy model, such as K-anonymity, would include all dimensions into a single QID and require every path to be shared by at least K records. However, in real-life privacy attacks, it is unlikely that an adversary could know all locations and timestamps that the target victim has visited because it requires non-trivial effort to gather each piece of prior knowledge from so many possible locations at different time. Thus, it is reasonable to assume that the adversary's prior knowledge is bounded by at most L pairs of locations and timestamps that the target victim is visited. Based on this LKC, privacy model is defined for anonymizing high-dimensional RFID data [7] but the limitation of this model is that the data holder must have advance knowledge of all the adversaries, which is impossible in reality.

Most of the previous work on privacy preserving RFID technology focused on the threats caused by the physical RFID tags and proposed techniques like sleeping tags, and EPC re-encryption. Basically the privacy and security issue was at communication layer among tags and readers not on the database layer where a large amount of RFID data actually resides. The important part here is to preserve the data truthfulness, if data will be examined by human users for the purpose of auditing and data interpretation. [7].

3.2 Private Information Retrieval (PIR) Approach

There are various fundamental approaches based on PIR (private information retrieval) like:

- Range queries - to Process range queries
- k-nearest neighbour queries - to Process k-nearest neighbour queries

These above approaches provide secure and cheap location base user privacy services as compare to anonymity and cloaking based approaches, which require a trusted intermediate anonymizer to protect a user's location information during query processing [6] and one more important thing is that the high dimensionality of RFID results applying traditional anonymity causes data of RFID suffers from the curse of high dimensionality, hence results in the poor data usefulness [7].

3.3 Strawman1 'Query Encryption'

According to Strawman1, encryption of the data protects user's privacy but may cause slow query performance and according to Strawman2 the protocol must ensure that user's query does not reveal useful information that an adversary can use to violate user's privacy.
Strawman Solution is used for encryption of query to improve privacy but Solution-1 is only suitable for small size table and Solution-2 prevents likability so long as the adversary never observes a user querying a database [2].

Privacy protection is an important part in ubiquitous computing environments [3]. For example in June 2005, names and credit card numbers of more than 40 million MasterCard cardholders were exposed and In May 2006, disks containing the names, social security numbers and dates of birth of more than 26 million United States veterans were stolen from the home of an employee of the department of Veterans Affairs [4]. Retrieval of sensitive data from databases invokes concerns on user privacy. Thus a PIR (Private Information Retrieval) scheme allows a user to retrieve a data from a database without revealing other information. Earlier "Query Privacy" was also proposed [5].

In a current scenario various fundamental approaches like anonymity and clocking-based approach can't give surety of information privacy as well as cheap computation and communication overhead.

3.4 Other Techniques

There are some techniques like EPCglobal tags come with a password protected kill function that permanently deactivates tag. Digital signatures are an important tool for data and device authentication. Techniques like RFID tags pseudonyms consist of names that are periodically refreshed, either by trusted RFID readers or an on-tag pseudorandom number generator. A mix net of RFID readers can also periodically re-encrypt tag data which protect RFID devices from attacks. *Detection and evasion* is a technique where consumers can detect unauthorized RFID activity and devices like Guardian (www.rfidguardian.org), will interpret RFID scans and log their meaning [21].

4. RFID DATA SECURITY AT COMMUNICATION LAYER

4.1 Data security Solutions

A. Symmetric key cryptography-it requires same key for encryption and decryption.
B. Public key cryptography-it require different cryptographic key for encryption and decryption.

In case of symmetric key cryptography techniques, secure authentication relies on a symmetric key shared between a tag and reader. For privacy, a tag cannot identify itself to a reader before an authentication interaction, thus the reader does not know which key to use in the interaction. Thus the results reader had to try every key which was quite costly too. To reduce the cost of key, public key cryptography can be used.

In case of public key cryptography, the response generation is performed using a secret key that is also called private key, but the response verification on the reader side can be performed without any secret key only with a public key, which is not required to protect against misuse.

As we know RFID tag respond to radio interrogation automatically, even if the information emitted by a tag is encrypted, the information may be used to track the tag, thus causing privacy issues. Thus RFID protocols must provide privacy and authenticity.

RFID tag is one kind of chip of integrated circuits yet the electronic process is not complicated, which uses 40 bit cipher code in usual conditions, it can be cracked in one hour. Even RFID with more robust encryption can also be cracked through a special hardware device, which called brute force cracking. Firstly, use special liquid to dissolve the protective layer of the RFID tags. Secondly, connect the special hardware device with the integrated circuit. In this case, the attacker can not only access the data in the label, but also analyze the structural design of labels. Overall, whether how micro the RFID tags is, it was still possibly cracked.

4.2 Data Encryption Techniques and Their Limitations

There are the various Data encryption techniques were used for ensuring the data transmission security between server and RFID tag. For example, Y P. Zhang et al. proposed a stream cipher algorithm with respect to the traditional block-based cipher approaches [19]. M. E. Smid and D. K. Branstad analyzed the past and future of DES algorithm [18].T. Jamil proposed an enhanced algorithm for the typical DES algorithm, called AES (Advanced Encryption Standard) [13]. J. Jiang proposed a parallel processing algorithm for the RSA [14]. S. Lian et al. proposed a fast video encryption scheme based on chaos [15]. M. McLoone and J. V. McCanny designed a hardware circuit for DES based on the FPGA technique [16]. M.Shaar et al. proposed a new data encryption algorithm, called HHEA [17]. But these techniques not completely secure to protect data between tag and reader.

Now let’s take the scenario where the encryption is strong enough so that it cannot be cracked, but RFID tags are still faced the danger of being copied. In other words, smart card equipment can easily copy the information from RFID tags and the work will be rapidly finished. Clearly, RFID encryption protection is not absolute security, but in any case, this is still the most important and effective application of preserving RFID products. Public Key Encryption based on IBE technology to RFID system, which can effectively solve the issues of data privacy, integrity and non-repudiation as well and also it can conquer the disadvantages such as storage and management difficulties, system complexity, high cost and low efficiency shortcomings when PKI technology applies to RFID system. IBE Security Solutions is on Encrypt Tag Data and Label Reading and Writing Process [10].

To protect privacy violation against various attacks like eavesdropping, location tracking, spoofing, message losses or replay attack etc. various encryption schemes were proposed by researchers such as blocker-tag [22], hash lock scheme [23], randomized hash lock [23], hash chain(Ohkubo et al., 2003), variable ID, re-encryption etc.. All of these schemes are not perfect against all types of attack like Hash lock scheme is week against all attacks, Randomized hash chain scheme is comparatively strong against location tracking and message loss but week against eavesdropping and replay attack, Hash chain scheme is strong against location tracking, replay attack and message loss but week against replay attack [24].

In current scenario lots of research going on communication security of RFID through light weight cryptography like elliptic curve cryptography [24] to ensure RFID system security and privacy friendly.

5. CONCLUSIONS

RFID data security consumers want to ensure that their personal information isn’t misused, and that RFID tags are used responsibly.

As we know RFID tag respond to radio interrogation automatically, even if the information emitted by a tag is encrypted, the information may be used to track the tag, thus causing privacy issues. To protect RFID against various attacks public key approach is used as it provide secure communication in comparison of symmetric key approach. But on the other hand public key approach is comparatively complex, requires higher implementation effort in chip size, lower performance and high power consumption.

Thus a low cost RFID tag authentication protocols must be developed in such a way that provides better privacy and authenticity also. In current scenario lots of research solutions are proposed on low cost lightweight cryptography but still they are costly as well as vulnerable to security. So strong encryption-decryption technique is needed which should be cheap, complex and efficient. In other words low cost RFID tag is required with high computation speed.

Performing operation on encrypted query is also more challenging. So a secure encryption-decryption algorithm is required for PIR scheme. These are the useful tools for protecting the confidentiality of sensitive data.

REFERENCES

[1] Monika Sharma and Manind Goyal “Improving Security by embedded RFID” National Confer-ence on Advance Computing & Communication Technology (2010).

[2] Chiu C. Tan,Qun Li,and Lei Xie “Privacy Protection for RFID-based Tracking System” IEEE RFID (2010).

[3] D. Anthony, T. Henderson, and D. Kotz, “Privacy in location aware computing environments” IEEE Pervasive computing, (2007).

[4] Zhiqiang Yang, Sheng Zhong and Rebecca N. Wright, “Privacy-Preserving Queries on Encrypted Data”. http://www.cs.rutgers.edu/~rwright1/Publications/esorics06.pdf

[5] Shuhong Wang, Xuhua Ding, Robert H. Deng and Feng Bao,”Private information Retrieval Using Trusted Hardware”.http://www.mysmu.edu/faculty/xhding/publications/pir.pdf

[6] Ali Khoshgozaran and Cyrus Shahabi, “Private Information Retrieval Techniques for Enabling Location Privacy in Location Based Services”. http://infolab.usc.edu/DocsDemos/Khoshgozaran-shahabi-PIR-Chapter.pdf

[7] Benjamin C. M. Fung, Khalil Al-Hussaeni and Ming Cao, “Preserving RFID Data Privacy” IEEE International Conference on RFID (2009).

[8] S. E. Sarma, S. A. Weis, and D. W. Engels, RFID systems and security and privacy implications. In Proc, of the 4th International Workshop of Cryptographic Hardware and Embedded System (CHES), pages 1-19, San Diego (2003).

[9] Ari Juels, RFID Security and Privacy :A Research Survey, IEEE Journal on Selected Areas in Communications (2005).

[10] Xian Zhang, Danning Li IBE Technology Applying to the Information Security of RFID Tags IEEE Xplore (2010).

[11] R.K Pateriya, sangeeta sharma, The Evolution of RFID Security and Privacy: A Research Survey, IEEE Conference on Communication System and Network Technologies (2012).

[12] M. Aikawa, K. Takaragi, S. Furuya, and M. Sasamoto, "A Lightweight Encryption Method Suit-able for Copyright Protection," IEEE Trans. on Consumer Electronics, Vol. 44, No.3, pp. 902-910 (1998).

[13] T. Jamil, "The Rijndael Algorithm," IEEE Potentials, Vol. 23, Issue 2, pp. 36-38 (2004).

[14] J. Jiang, "Pipeline Algorithms of RSA Data Encryption and Data Compression," Proc. of IEEE Int'l Conf: on Comm. Technology (ICCT'96), Vol. 2, 5-7 May 1996, pp. 1088-1091 (1996).

[15] S. Lian, J. Sun, Z. Wang, and Y. Dai, "A Fast Video Encryption Scheme Based-on Chaos," Proc. of the 8th IEEE Int'l Conf: on Control, Automation, Robotics, and Vision (ICARCV 2004), Vol. 1, 6-9 Dec. 2004, pp. 126-131 (2004).

[16] M. McLoone and J. V. McCanny, "A High Performance FPGA Implementation of DES," Proc. Of IEEE Workshop on Signal Processing Systems (SiPS 2000), 11-13 Oct. 2000, pp. 374-383 (2000).

[17] M. Shaar, M. Saeb, M. Elmessiery, and U. Badwi, "A Hybrid Hiding Encryption Algorithm (HHEA) for Data Communication Security," Proc. of the 46th IEEE Int'l Midwest Symposium on Circuits and Systems (MWSCAS'03), Vol. 1, 27-30 Dec. 2003, pp.476-478 (2003).

[18] M. E. Smid and D. K. Branstad, "Data Encryption Standard: Past and Future," Proc. IEEE, Vol. 76, No. 5, May 1988, pp. 550-559 (1988).

[19] Y P. Zhang, J. Sun, and X. Zhang, "A Stream Cipher Algorithm Based on Conventional Encryption Techniques," Proc. of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2004) Vol. 2, 2-5 May 2004, pp. 649-652 (2004).

[20] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. In Workshop on RFID Security, RFIDSec'10, Istanbul, Turkey, Jun. 2010 (2010).

[21] Saroj Kumar Panigrahy, Sanjay Kumar Jena, and Ashok Kumar Turuk "Security in Bluetooth, RFID and Wireless Sensor Networks" Proceedings of the 2011 International Conference on Communication, Computing & Security Pages 628-633 (2011).

[22] Jules, A, Rivest, R. L. & Szydlo M. , "The blocker tag : selective blocking of RFID tag for consumer privacy", Proceeding of ACM conference on Computer and Communication Security (2003).

[23] S.A. Weis, S.E. Sarma, R.L. Rivest & D.W. Engels, "Security and Privacy aspects of low cost Radio frequency identification system", First International Conference on Security in Pervasive Computing, pp. 201-202, Lecture Notes in Computer Science 2802, Springer-Verlag (2003).

[24] Ji-Yeon Kim, Jong-Jin-Jung and Geun-Sik Jo, "Shared Tag RFID System for Multiple Application Objects", Development and Implementation of RFID Technology Online Book Chapter-25 (2009).