A Survey on Attacks in RFID Networks

Mojtaba Alizadeh[a,*], Mazdak Zamani[b], Ali Rafiei Shahemabadi[c],JafarShayan[b], Ahmad Azarnik[b]

[a]*Faculty of Computer and Information Systems, Universiti Teknologi Malaysia,81310 UTM Skudai, Malaysia*
[b]*Advanced Informatics School, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia*
[c]*Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor Darul Ehsan, Malaysia*

Abstract

Today, RFID applications are going to be ubiquitous and an importance of security and privacy of these applications are increasing day by day. By considering security and privacy issues in RFID systems, it is necessary to identify different attacks on RFID and propose appropriate countermeasures to reduce the effect of these attacks. At the first part of this research, RFID architecture is introduced. Next, different existing attacks which threat security and privacy of RFID applications are described. Finally, existing countermeasures that are proposed by different researchers are discussed.

Keywords: Radio-Frequency Identification, Attacks on RFID, Security Challenges in RFID.

1. Introduction

RFID is a useful technology that is becoming prevalent in current times in many different fields; it is especially prominent in business as it fine-tunes a lot of the business processes. The RFID system has been used to simplify many processes in inventory management which include tracking consumer goods or keeping track of books in a library. Unfortunately, given the pervasive nature of the RFID system, it is prone to risks such as privacy matters and security [1].

The RFID technology which encompasses the tag and reader system utilizes the wireless communication technology. Since this is based on radio frequency, it is pervasive and accessible to everyone, which makes it severely lacking in security [2]. The devices used by the RFID have some major resource constraints such as memory power, power supply, and computational aptitude. These constraints cause the design of a secured tag rather complex; if security is to be improved, then unbreakable encryption algorithms are needed which is not possible given the limited capacity of the RFID tags [3].

In the world we live in today, privacy and security are crucial components in people's lives. Considering that RFID is a system that can be utilized in various parts of people's lives, a secured system is of the utmost importance. In addition, the information contained within the RFID tag can include information regarding products and individuals, people's location in real time, and even biomedical health data. Wang Shang-ping (2011) claimed that the RFID technology is a critical technology founded in the 20th century and can easily be one of the top ten most important technologies. Given the popularity of the RFID system for future use and concerns regarding its privacy and security issues which concerns most people, it was felt that an in depth study into this matter would be of importance [4].

* Corresponding author. Tel.: +60-172389794;
E-mail address: amojtaba2@live.utm.my.

2. RFID Architecture

The electromagnetic spectrum contains many important components; the most critical component is the radio which includes all radiation formats. Some of the other components in this spectrum include visible light, x-rays, cosmic-ray photons, and gamma rays. The various Radio Frequency (RF) bands range from 30 MHz to 300 MHz. In the RFID system, there are mainly 3 bands in general. The Low Frequency (LF) or the first band ranges from 125 kHz to 134 kHz; the High Frequency (HF) or the subsequent band is at 13.56 MHz, and finally the Ultra HF which is the third band ranges from 860 to 930 MHz. There are different types of RFID that can be utilized for various reasons. The RFID manufacturers need to take into consideration various factors in order to select the right frequency band which includes the needed power for transmission purposes and the antennas' physical size [4].

The RFID technology does not require physical contact to detect objects that have the tags in various surroundings. A normal RFID system contains three important components namely the reader, tag and backend servers[5].

The transponder in the RFID systems is known as a chip or tag. A tag is attached to bigger equipments while a chip is attached to smaller items. In every tag, there are communications control, memory, antenna, encoding/decoding circuitry, and power supply [5].

Tags come in three types namely passive, semi passive and active. Most of the transponders in RFID are of the passive type. The reader contains a power supply that generated the RF field as a passive tag. This voltage supply for the passive tag is produced when rectifying the voltage generated by the reader's RF signal. The active tag contains its own power supply which is incorporated inside. Even though the function of the active tag is the same as the passive one, the processor's speed in this type of tag is much faster. The reader signals by trigging the most active tag[6]. A semi passive tag also comes with its own power source however it peruses the radio signal from the reader to enable powered communication[7].

The second part of the RFID system is known as the reader or the interrogator. The Reader or Transceiver is tasked to provide the necessary energy for the tag to use, besides trigging the signals for communication purposes in order for the tag to perform the required action[6].

The reader comes with an integrated or separated antenna. A reader has a system interface which includes power supply or battery, cryptographic encoding/decoding circuitry, control circuits for communications, and an Ethernet jack or RS-232 serial port. The readers have various sizes of antennas; there are large ones with unique panels and small pocket sized ones. The antenna's size is dependent on the type of tag that is utilized in the RFID system[8].

The backend server is the third part of the RFID. This backend server is a PC device that hosts many business related applications. Special business logics are implemented which include support for security enabled tasks and customized applications are engaged in order to interface with the middleware or the database. Several standard databases available commercially are utilized for this backend purpose such as My SQL, SQL, Postgres, Oracle, and others. The backend databases are run on an individual PC or multiple mainframes that have been networked based on the application that is utilized[9].

The antenna from the reader transmits or transfers a radio signal which is captured by the tag in order to communicate between the reader and the tag. The tag responds with a corresponding radio signal upon receipt of the signal from the reader; Fig. 1 illustrates this transmission. The receiver from the reader is able to read the signal that is sent by the tag. Some tags can conduct certain encryption processes if it has the computing capability. The RFID systems use various forms of tags; some come with read and write functions while others only have read functions[10].

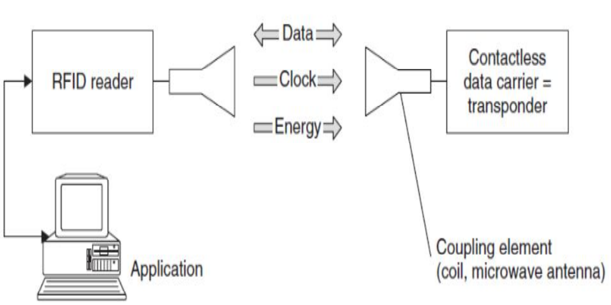
Data
Clock
Energy
RFID reader
Contactless data carrier = transponder
Application
Coupling element (coil, microwave antenna)

Fig. 1.Communication between Readers and Tag [11]

In the RFID systems, required energy for communication between tag and reader is provided by a reader which is produced via the field of radio frequency. Reader acts as a master and sends commands to instruct the tag to be executed.The RF signals which are received and decoded by the tag should be executed and replied. There are some basic functional modules, which are embedded in tag's IC as shown in Fig. 2 [7]:

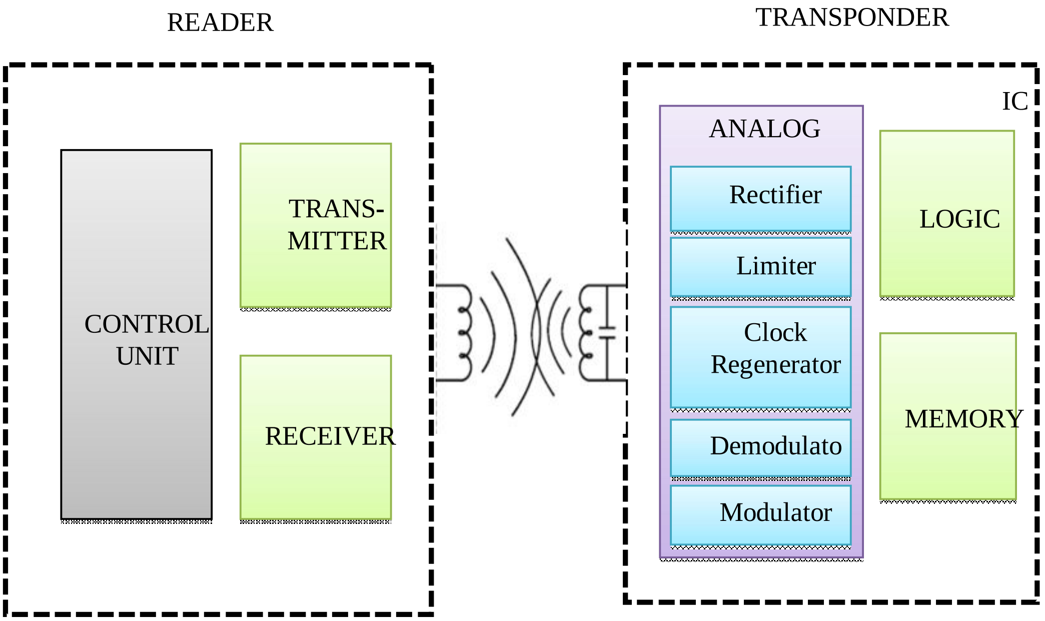

Fig. 2. RFID Functional Blocks [6]

The different functional blocks in fig. 2 are described as follows [6]:

- *Rectifier* purifies the induced voltage to supply the IC.
- To avoid over voltage, the *Limiter* limits the RF voltage at the input'spins.
- The frequency signal which is produced by RF is extracted by the *Clock Regenerator*and used as an internal clock.
- The incoming data signal should be decoded, and this can be done by the *Demodulator*.

- The decoded response is modulated by the *Modulator.*
- The digital circuitry of the tag is presented by the *Logic*.
- The tag data are stored in the *Memory* unit.

3. Attacks on RFID systems and Current Countermeasures against them

RFID systems face the potential risk of being spied out or manipulated similar to any other telecommunication and information technology system. Different types of attacks should be analyzed in order to have a better evaluate potential risks in RFID systems. Then, appropriate cryptographic procedures should be implemented to protect systems from common attacks [11].

There are a lot of malicious attacks that can be categorized from passive eavesdropping to active interference in RFID systems. Decentralized part of RFID networks can be attacked by an attacker unlike wired networks, where computing systems typically have both host-based defenses and centralized, because RFID tags and readers operate in potentially noisy and unstable environment. Additionally, as RFID technology is improving day by day, the threats are changing too. Hence, having a global view of the problem is so difficult [12].

3.1. Attacks on Different Layers of RFID Network

The attacks against RFID networks are classified as follows: the network-transport layer, the physical layer, the application layer,and the strategic layer[12]. The RFID networks' security problems can be listed as: tracking, spoofing attack, desynchronization, replay attack, eavesdropping, session hijacking, electromagnetic interference, etc. Each security problem belongs to one layer of different layers of RFID networks [13].

In this part of research, various threats that cause the security problems for RFID networks are discussed:

3.1.1. Physical Attack: The vulnerabilities in the implementation of higher level or transmission protocols, which are defined in the manufacturing process of RFID can be exploited in physical-layer attacks. One of the most important attacks which is categorized in physical-attacks is traceability attack, which abuses the variations in the manufacturing process of tags. This attack is discussed Danev et al [14].Due to cost of RFID tag, in many cases there is no physical security provision in RFID tags, and it makes a physical attack easier. According to this research, no physical attack has been reported in RFID networks yet.

*3.1.2. Spoofing Attack:*In this case, false information which the system accepts is produced by an attacker. Some important information that can be modified in RFID networks such as MAC Address, IP, and domain name are used by an attacker. As an example, an attacker broadcasts an incorrect EPC™ number over the air when a valid number was expected[4]. This attack can take place if no encryption algorithm is used in RFID tags for transmitting data.

3.1.3. Eavesdropping and Skimming Attack: One of the most famous threats in each wireless network is eavesdropping because of the nature of radio frequency, which can go everywhere. An unauthorized user uses an antenna to record the communication between the tag and reader in eavesdropping. An attacker can eavesdrop on both directions reader-to-tag and tag-to-reader. To get the radio signal, the location of an eavesdropper and also distance forthe reader and tag are important[12]. Different areas which are vulnerable to this attack are identified by the author, including credit cards, traveling ticketing, Epassports, and access control. In these cases, tag’s information should be secured because an attacker can get some advantages from these data.

3.1.4. *Tag Cloning Attack:*This attack can be happened when the RFID tag is not protected by any security policies. The tag’s ID and also the data that are stored inside the tag can be copied by an attacker [12] and in such situations, all characteristic features of RFID system is vulnerable to attacks. It is impossible to ask RFID manufacturer to produce a copy of RFID tag in theory[16];however, in practice cloning RFID tag is not difficult and does not need a lot of money to create it. The importance of this attack is raised because there is no special mechanism for distinguishing between fake and read tags in RFID networks.

*3.1.5. Denial Of Service (DOS) Attack:*This attack makes tags unusable by enabling an [15]. Computational resources of RFID systems can be abused if an attacker launched a large number of tags or even readers, and in this case disruption of service can be happened[16]. This attack includes buffer overflow, Active jamming, malicious code injection, etc.[17]. As explained in the introduction section, there are no longer enough resources in RFID tags and this issue shows that this attack can be more dangerous than other attacks.

*3.1.6. Clandestine Tracking:*The tag can emit a constant bit sequence and the vehicle or person carrying this tag, permitting clandestine physical tracking by broadcasting this value to readers[18]. Some information about the items that tag is attached to them can be broadcasting by the tag and allowing a clandestine reader and collecting intended information about a person or a company [19-22]. The importance of protection tags against this attack is increased when an attacker uses several readers to reveal the data of location of tag.

3.1.7. *Relay Attack:*This attack can be counted as man-in-the-middle attack where a fake tag tries to interact with genuine reader and fooling the reader into thinking it is realcard, and the communication is correct.In this case, the protection electronic system is breached, and genuine parties, remain unaware[23]. This attack is more hazardous when cryptographic algorithms are not implemented on RFID tags.

3.2. Current Countermeasures for Secure RFID

To counter the above threats, the following security properties are required: mutual authentication between tag and reader/back-end server, anonymous/privacy-preserving transaction, forward security, secure key exchange, and secure tag location. In the field of RFID networks, a lot of studies have been done to address the security and privacy problems with these systems. Most of the previous RFID protocols tried to solve both security and privacy issues, but the final solution has always been a security solution and not privacy. It is established that around 70 to 80 percent of related RFID security research works focused on security, 10-15 percent on privacy and only a few works on trust and trusted computing. It means that security, and privacy has always been the main focus for every RFID system and protocols [1]. We summarize some of the countermeasures proposed for secure RFID:

3.2.1. Kill Command: In the past few years, many researches have conducted, which focused on the KILL command operation and different attacks related to this field[24-27]. The tag is disabled when it has been killed according to the EPC Global standard [28]. According to recent studies, if the tag’s memory iserased, and the authenticated readers are able to bring the tag to life by reprogramming it [26]. The only issue related to this countermeasure is that it can be misused.

*3.2.2. RFID Guardian:*This platform suggests centralized RFID privacy and security management for each tag. The main idea of RFID guardian is that the tag holder carries a battery –powered mobile device which it can observe the RFID usage and also regulate it. The range of operation of the RFID must be increased from the head to toe of the user because it manages the RFID tags within physical proximity of tag or person, the radius of reader's signal should be one to two meters.To coverage full-body of a person, the RFID Guardian should be portable, for example, PDA-sized or integrated to cell phone.To install the RFID Guardian, some vacant places are available such as handbag, belt loop, and shirt pocket, etc. and as a result, it can remain close to the person[29]. The important security problem in RFID guardian is that if an attacker can have control over the tags when the battery-powered mobile is lost.

*3.2.3. RFID Blocker Tag:*To make founding the serial number of the tag more arduous, a blocker tag can simulate and produce a full spectrum of various serial numbers. The full space of tag's serial numbers which is extremely large should be swept by the blocker to make this process more difficult. It may be more difficult for a reader to simulate tags when a blocker tag producesthe physical region of protected tags [24]. By developing the technology, attackers launch more sophisticated attacks and in this case, they can find new method to find a serial number of the tags.

3.2.4. RFID Clipped Tag: This method allows consumers to disable a tag by physically changing the tag by providing RFID tags with especial structure. In this case, the consumer can check the activation status of the tag visually.The deactivation could not be undertaken without the user's permission because the user can check the tag physically to be sure that the antenna of the tag is connected[30]. However, the tags would be damaged by a physical destruction [33]; this method can separate the antenna from the chip physically. This method is proper for disposable items, and it is not recommended for expensive or fixed tags.

3.2.5. Authentication Protocols: one of the most important methods which is proposed by different researchers to protect security and privacy of tag is Authentication Protocol[31]. Some of these protocols are based on the mechanism of static IS such as the randomized Hash-Lock [32], Hash-Lock [33], the distributed RFID challenge-response authentication protocol [34], etc.

3.2.6. Faraday Cage: The Faraday Cage is one of the economic methods to protect tag from attackers which is effective at MMW frequency and embedded in the tags[35, 36]. High-aspect ratio and through-wafer vias are used by Faraday's cage [37]. Faraday's cages improved an isolation of have shown an 41 dB at 1 GHz, 30 dB at 10 GHz, and 16 dB at 50 GHz for a separation distance of 100 pm when compared to a reference structure [35]. This method can be helpful, especially in a situation that RFID tags are used occasionally not permanently because in many cases, the tags should be installed on the item, for example, in the supply-chain management.

3.2.7. Physical-Layer Identification Technique: The main purpose of this method is identifying device based on fingerprints that obtained by analyzing the device's communication at the physical layer [38]. Similar methods are proposed for different wireless platforms [14, 39-45] and few investigations addressed HF [14, 46] and UHF [47] RFID tags. This technique can be used to delete cloned tags by checking the fingerprints.

3.2.8. Controllable Tag: The control mechanisms can be integrated into RFID tag, and Controllable Tag designs these mechanisms. In this case, the antenna of the tag is separated from the chip physically, and this can help the user to control the connection between tag and reader. It is possible to limit the transmission activity of the tag information [48]. This method increases the cost of tag production, and in a case that cheap RFID tags are used, this technique is not reasonable.

3.2.9. Anti-Counterfeiting Technology: One of the famous Anti-counterfeiting technologies is PhysicalUnclonable Function (PUF). Using a digital cryptographic algorithm in Existing Radio-Frequency Identification (RFID) increases a cost of hardware [49]. Bolotnyy in 2006 proposed a low-cost hardware-based approach to improve the security of RFID based on PUF, which requires just hundreds of gates [50]. To prevent leakage of the PUF measurement, the chip and the PUF should be connected permanently [51].

3.2.10. Fingerprint Biometric Authentication On Smart Card: Fingerprint is the most reliable method among all the biometrics [51]. Fingerprint is required to improve the security of applications for identifying and matching individuals[51]. This method has the least security problems among all techniques that are discussed in this paper because it is so difficult to copy fingerprint.

4. Conclusion

This paper presents different existing attacks on RFID system which threat security and privacy of RFID tags. To protect RFID devices against these attacks, some countermeasures which are proposed by different researchers are provided in this study. In some cases, for a specific attack, there are some solutions that provided to protect RFID tag. The advantages and disadvantages of each proposed method, which is proposed to improve the security and privacy of RFID tag, are discussed by the authors.

5. FUTURE TRENDS

Many security problems are still unsolved; however, many researchers have tried to reduce security threats in RFID Applications. These problems include Functional Lightweight Cryptographic Primitives, Possibility of Certain Cryptographic Tasks, Effective Methods against Location-based Attacks, and Protection against Side Channel Analysis.

It should be mentioned that this paper may not be the complete list of open issues. It is a well-known fact that research on RFID security and privacy, and its attacking methods is fast evolving; therefore, we would certainly encounter new challenges and having a good understanding of the problems would lead to new innovative ideas and solutions.

ACKNOWLEDGMENT

This work is a part of a research that has been done under support from Universiti Teknologi Malaysia.

REFERENCES:

[1] Mubarak, M. F., J. L. A. Manan, and S. Yahya, "A critical review on RFID system towards security, trust, and privacy (STP)," in 2011 IEEE 7th International Colloquium on Signal Processing and Its Applications, CSPA 2011, March 4, 2011 - March 6, 2011, Penang, Malaysia, 2011, pp. 39-44.

[2] Poschmann, A., M. Robshaw, F. Vater, and C. Paar, "Lightweight Cryptography and RFID: Tackling the Hidden Overheads Information, Security and Cryptology – ICISC 2009." vol. 5984, D. Lee and S. Hong, Eds., ed: Springer Berlin / Heidelberg, 2010, pp. 129-145.

[3] Engels, D., X. Fan, G. Gong, H. Hu, and E. M. Smith, "Hummingbird: ultra-lightweight cryptography for resource-constrained devices," presented at the Proceedings of the 14th international conference on Financial cryptograpy and data security, Tenerife, Canary Islands, Spain, 2010.

[4] Thornton, F., B. Haines, A. M. Das, H. Bhargava, A. Campbell, and J. Kleinschmidt, RFID Security: Syngress, 2005.

[5] Erguler, I. and E. Anarim, "Security flaws in a recent RFID delegation protocol," pp. 1-13, 2011.

[6] Kitsos, P. and Y. Zhang, RFID security: techniques, protocols and system-on-chip design: Springer, 2008.

[7] Glover, B. and H. Bhatt, RFID essentials: O'Reilly, 2006.

[8] Yoon, W.-J., S.-H. Chung, and S.-J. Lee, "Implementation and performance evaluation of an active RFID system for fast tag collection," Computer Communications, vol. 31, pp. 4107-4116, 2008.

[9] Ahson, S. and M. Ilyas, RFID handbook: applications, technology, security, and privacy: CRC Press, 2008.

[10] Cole, P. H., Networked RFID systems and lightweight cryptography : raising barriers to product counterfeiting. Berlin [u.a.: Springer, 2008.

[11] Finkenzeller, K., D. M?ller, and D. Müller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication: John Wiley & Sons, 2010.

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

[13] Jiezhong, G., C. Gongliang, L. Linsen, and L. Jianhua, "A secure authentication protocol for RFID based on Trivium," in Computer Science and Service System (CSSS), 2011 International Conference on, 2011, pp. 107-109.

[14] Danev, B., T. S. Heydt-Benjamin, and S. apkun, "Physical-layer identification of RFID devices," presented at the Proceedings of the 18th conference on USENIX security symposium, Montreal, Canada, 2009.

[15] D'Arco, P., A. Scafuro, and I. Visconti, "Revisiting DoS Attacks and Privacy in RFID-Enabled Networks Algorithmic Aspects of Wireless Sensor Networks." vol. 5804, S. Dolev, Ed., ed: Springer Berlin / Heidelberg, 2009, pp. 76-87.

[16] Dang Nguyen, D., L. Hyunrok, D. M. Konidala, and K. Kwangjo, "Open issues in RFID security," in Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for, 2009, pp. 1-5.

[17] Yongqing, F., Z. Chun, and W. Jingchao, "A research on Denial of Service attack in passive RFID system," in Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference on, 2010, pp. 24-28.

[18] Fouladgar, S. and H. Afifi, "Scalable privacy protecting scheme through distributed RFID tag identification," presented at the Proceedings of the workshop on Applications of private and anonymous communications, Istanbul, Turkey, 2008.

[19] Juels, A., "RFID security and privacy: a research survey," Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 381-394, 2006.

[20] Juels, A. and S. A. Weis, "Defining strong privacy for RFID," ACM Trans. Inf. Syst. Secur., vol. 13, pp. 1-23, 2009.

[21] Weis, S. A., "Security parallels between people and pervasive devices," in Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on, 2005, pp. 105-109.

[22] Ranasinghe, D. C., D. W. Engels, and P. H. Cole, "Security and privacy solutions for low-cost RFID systems," in Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004. Proceedings of the 2004, 2004, pp. 337-342.

[23] Munilla, J. and A. Peinado, "Enhanced low-cost RFID protocol to detect relay attacks," Wireless Communications and Mobile Computing, vol. 10, pp. 361-371, 2010.

[24] Juels, A., R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," presented at the Proceedings of the 10th ACM conference on Computer and communications security, Washington D.C., USA, 2003.

[25] Juels, A., "Strengthening EPC tags against cloning," presented at the Proceedings of the 4th ACM workshop on Wireless security, Cologne, Germany, 2005.

[26] Bolan, C., "The Lazarus Effect : Resurrecting Killed RFID Tags," Security Management, 2006.

[27] Belcher, B., M. El-Said, and G. Nezlek, "Lightweight RFID authentication protocol: An experimental study," in Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on, 2008, pp. 583-588.

[28] El-Said, M. M. and I. Woodring, "An empirical study for protecting passive RFID systems against cloning," in 6th International Conference on Information Technology: New Generations, ITNG 2009, April 27, 2009 - April 29, 2009, Las Vegas, NV, United states, 2009, pp. 558-563.

[29] Rieback, M. R., B. Crispo, and A. S. Tanenbaum, "RFID guardian: A battery-powered mobile device for RFID privacy management," in 10th Australasian Conference on Information Security and Privacy, ACISP 2005, July 4, 2005 - July 6, 2005, Brisbane, Australia, 2005, pp. 184-194.

[30] Karjoth, G. and P. A. Moskowitz, "Disabling RFID tags with visible confirmation: Clipped tags are silenced," in WPES'05: 2005 ACM Workshop on Privacy in the Electronic Society, November 7, 2005 - November 7, 2005, Alexandria, VA, United states, 2005, pp. 27-30.

[31] Gharooni, M., M. Zamani, M. Mansourizadeh, and S. Abdullah, "A confidential RFID model to prevent unauthorized access," in Application of Information and Communication Technologies (AICT), 2011 5th International Conference on, 2011, pp. 1-5.

[32] Weis, S. A., S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," System, 2003.

[33] Sarma, S. E., S. A. Weis, and D. W. Engels, "RFID Systems and Security and Privacy Implications," presented at the Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, 2003.

[34] Rhee, K., J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," in Second International Conference on Security in Pervasive Computing, SPC 2005, April 6, 2005 - April 8, 2005, Boppard, Germany, 2005, pp. 70-84.

[35] Wu, J. H., J. Scholvin, J. A. del Alamo, and K. A. Jenkins, "A Faraday cage isolation structure for substrate crosstalk suppression," Microwave and Wireless Components Letters, IEEE, vol. 11, pp. 410-412, 2001.

[36] Wu, J. H. and J. A. del Alamo, "An equivalent circuit model for a Faraday cage substrate crosstalk isolation structure," in Radio Frequency Integrated Circuits (RFIC) Symposium, 2004. Digest of Papers. 2004 IEEE, 2004, pp. 635-638.

[37] Wu, J. H., J. Scholvin, and J. A. Del Alamo, "An insulator-lined silicon substrate-via technology with high aspect ratio," Electron Devices, IEEE Transactions on, vol. 48, pp. 2181-2183, 2001.

[38] Zanetti, D., B. Danev, and S. apkun, "Physical-layer identification of UHF RFID tags," presented at the Proceedings of the sixteenth annual international conference on Mobile computing and networking, Chicago, Illinois, USA, 2010.

[39] Brik, V., S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," presented at the Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, California, USA, 2008.

[40] Hall, J., "Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting," 2004.

[41] Jana, S. and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," presented at the Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, California, USA, 2008.

[42] Bonne Rasmussen, K. and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on, 2007, pp. 331-340.

[43] Tippenhauer, N. O., K. B. Rasmussen, C. P, and S. apkun, "Attacks on public WLAN-based positioning systems," presented at the Proceedings of the 7th international conference on Mobile systems, applications, and services, Krak&#243;w, Poland, 2009.

[44] Ureten, O. and N. Serinken, "Wireless security through RF fingerprinting," Electrical and Computer Engineering, Canadian Journal of, vol. 32, pp. 27-33, 2007.

[45] Wang, B., S. Omatu, and T. Abe, "Identification of the defective transmission devices using the wavelet transform," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 27, pp. 919-928, 2005.

[46] Romero, H. P., K. A. Remley, D. F. Williams, and W. Chih-Ming, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," Microwave Theory and Techniques, IEEE Transactions on, vol. 57, pp. 1383-1387, 2009.

[47] Chinnappa, S., G. Periaswamy, D. R. Thompson, and J. Di, "Ownership Transfer of RFID Tags based on Electronic Fingerprint," Work, 2008.

[48] Marquardt, N., A. S. Taylor, N. Villar, and S. Greenberg, "Visible and controllable RFID tags," presented at the Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems, Atlanta, Georgia, USA, 2010.

[49] Feldhofer, M. and C. Rechberger, "A case against currently used hash functions in RFID protocols," in OTM 2006 Workshops - OTM Confederated International Workshops, October 29, 2006 - November 3, 2006, Montpellier, France, 2006, pp. 372-381.

[50] Bolotnyy, L. and G. Robins, "Physically unclonable function -based security and privacy in RFID systems," in 5th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2007, March 19, 2007 - March 23, 2007, White Plains, NY, United states, 2006, pp. 211-218.

[51] Tuyls, P. and L. Batina, "RFID-Tags for Anti-counterfeiting," in Topics in Cryptology (CT-RSA). vol. 3860, D. Pointcheval, Ed., ed: Springer Berlin / Heidelberg, 2006, pp. 115-131.