ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 3, No.15 , May 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

A Strengthened Version of a Hash-based RFID Server-less Security Scheme

Shahab Abdolmaleky[1], Shahla Atapoor[2] , Mohammad Hajighasemlou [3] and Hamid Sharini[4]

[1] Department of Computer Engineering, Science and Research Branch, IAU University
Tehran, Iran
s.abdolmaleky.ir@ieee.org

[2] Iran Telecommunication Research Centre (ITRC)
Tehran, Iran
sh.atapoor@itrc.ac.ir

[3] Faculty of Electrical and Computer Engineering, Tabriz University
Tabriz, Iran
m.hajighasemlou@tabrizu.ac.ir

[4] Tehran University of Medical Science (TUMS)
Tehran, Iran
hamid.sharini@razi.tums.ac.ir

Abstract

Radio Frequency IDentification (RFID) is a user-friendly and easy to use technology which has been deployed in different applications to identify and authentication objects and people. Due to employing RFID systems in some sensitive applications, the security of end-users has become more prominent and has got more attention by researchers. Recently, in order to provide security and privacy requirements of end-users, lots of RFID authentication have been proposed. In 2014, *Deng* et al. cryptanalyzed a server-less RFID authentication protocol and presented an improved protocol. They analyzed the security and privacy of the improved protocol and claimed that their protocol is safe against various attacks. However, in this paper we show that *Deng* et al.'s protocol is not safe yet and it suffers from secret parameters reveal, tag impersonation and reader impersonation attacks. In addition, we propose some modifications in *Deng* et al.'s protocol which overcomes all the reported weaknesses. Finally, the improved protocol compared with some similar protocols in the terms of security and privacy.

Keywords: *RFID Authentication Protocol, Hash functions, Server-less Protocol, Security and Privacy Attacks, Healthcare systems.*

1. Introduction

Radio Frequency Identification (RFID) technology is a progressive wireless kind of communication system which is developed in different aspects of authentication such as consumer electronics, defense, homeland security, transportation, healthcare organization and etc [1], [2], [3]. For example in healthcare, by using resources more effectively, not only hospital staff can spend less time running around trying to find medical supplies and more time with patients, but also reduce the counterfeiting of pharmaceuticals and other high-end products and monitor medical supplies in hospitals [4], as well as in payment systems [5], or we can mention the RFID's application in transportation which the destination [3], origin, owner, type and amount of products in a container which is carried with a trailer are clarified just by passing the trailer around the RFID reader, or we can detect the stolen cars by using RFID for vehicle registration.

An RFID system consist of three main parts, Tags, Readers, and a Back-end server [6] (Shown in Fig. 1). The tags and the readers are connected in a wireless manner via electromagnetic signal, while the connection between the readers and the back end server are consisted of two types, wired or wireless [7]. The tag and the reader introduce themselves by transcribing data and they operate according to the protocol after authentication [8].

So the major problem in using the RFID technology is establishing the security. Due to restriction of low-cost RFID tags caused by storage and computation, designing an RFID authentication protocols based on simplified cryptography mechanism is the goal of recent researchers [8], [9], [10]. As the simplicity of the design makes the protocol suitable to low-cost RFID tags, different types of encryption have been introduced in protocol which can be categorized in four classes: The first class discusses protocols which apply conventional cryptographic functions [11]. The second class are protocols that apply random number generator and one-way hash function [12]. The third class refers to protocols that apply random number generator and Cyclic Redundancy Code checksum [13]. The last one refers to those protocols which are using simple bitwise operations such as XOR, AND, OR, etc

which are called ultra-lightweight protocols [14]. Among these classification hash-based encryption provide a high level of security among RFID security methods [15].
The presence of the back-end server will accompany security and privacy protection by checking the validity of the tag and the reader from database, but being a

Fig. 1. An architecture of RFID systems [6].

connection between the server and the reader is the greatest weakness of server-based RFID system, because the leakage of information in this pass will destroy the situation. Moreover, it is in contrary with great application of RFID systems that are mobile and unable to connect with the back-end server in every position, although having a back-end server generates a single point of failure, which may result in the DoS attack [11], [16]. So by providing a secure server-less system not only we can reduce the price of this technology, but also the domain of its applications will be developed [17].
Some protocols by providing a mutual authentication between the reader and the tag, without the presence of the back-end server have been presented. In [18], *Hoque* et al. proposed a server-less authentication protocol which provide security and privacy protection as the central database without any connection with the back-end server. They claimed that their protocol will guarantee the authentication of both the tag and the reader during the communication and they believed that their method is forward secured and protected against tracking, cloning, eavesdropping, physical tampering, and Denial of Service (DoS) attacks. However, in 2014, *Deng* et al. [17] showed that [18] authentication protocol was vulnerable to data desynchronization attack which destroy the availability of the protocol. So they [17] modified *Hoque* et al.'s protocol by keeping both the current and the previous records of seeds and believed their improved protocol (referred as SLRAP) is forward security, and satisfies the security requirements, such as privacy protection, tracking attack resistance, cloning and physical attack resistance.
In 2015, *Pourpouneh* et al. analyzed the security of the SLRAP protocol and presented a DoS attack against that protocol [19]. In this study, we cryptanalyze the SLRAP protocol and we show that the security of the protocol has some another drawbacks which make the protocol vulnerable to *Secret parameters reveal*, *Tag impersonation* and *Reader impersonation* attacks. The cost of *Secret parameter reveal* attack is maximum 2^{16} computations. Then, in order to overcome the aforementioned weakness, we propose a strengthened version of the SLRAP protocol which prevents all the presented attacks in this study and [19]. Moreover, we investigate the security and the privacy of the strengthened protocol against various security and privacy attacks. Finally, we compare the performance of the proposed protocol and some similar RFID authentication protocols which are in the same family.
The structure of paper is organized as follows: the SLRAP protocol is introduced in section 2. In section 3, we investigate vulnerabilities of the SLRAP protocol. In section 4, an improved version of the SLRAP protocol presented. The security of the proposed protocol is analyzed in section 5, also in this section analysis of the proposed protocol is compared with some similar protocols which proposed recently. Finally, we conclude the paper in section 6.

2. The SLRAP Protocol

The SLRAP protocol is a RFID mutual authentication protocol based on Pseudo Random Number Generator (PRNG) that proposed by *Deng et al.* in [17]. This protocol belongs to the second class of authentication protocols family which apply PRNG and one-way hash function to protect exchanged messages over a wireless channel which claimed to provide security and privacy of RFID users. The structure of the SLRAP protocol and authentication procedure are shown in Fig. 2 with more details. Each run of the SLRAP protocol consists of three phases which can be seen in Fig. 1 with details. Table 1 shows the notations which are used in the SLRAP protocol and in order to avoid confusing, we also use the same notations in our analysis. In the SLRAP protocol, communication channel between the tags and the reader is insecure and can be eavesdropped by an attacker.

Table 1. The Notations of SLRAP protocol

Not.	Description
$\boldsymbol{rand_i}$	Random number generated by the reader R_i
$\boldsymbol{rand_j}$	Random number generated by the tag T_j
$\boldsymbol{n_i}$	Message generated by the reader R_i for authentication.
$\boldsymbol{n_j}$	Message generated by the tag T_j for authentication
$\boldsymbol{Seed_T}$	The secret value shared between the reader R_i and the tag T_j.
$\boldsymbol{Seed_{PT}}$	The previous secret value stored in the reader R_i.
$\boldsymbol{M}(.)$	One way hash function
$\boldsymbol{P}(.)$	Pseudo random number generator
$\|$	Concatenation operation
$\boldsymbol{A} \oplus \boldsymbol{B}$	Message A is XORed with message B
$\boldsymbol{A} \stackrel{?}{=} \boldsymbol{B}$	Compare whether A is equal to B or not

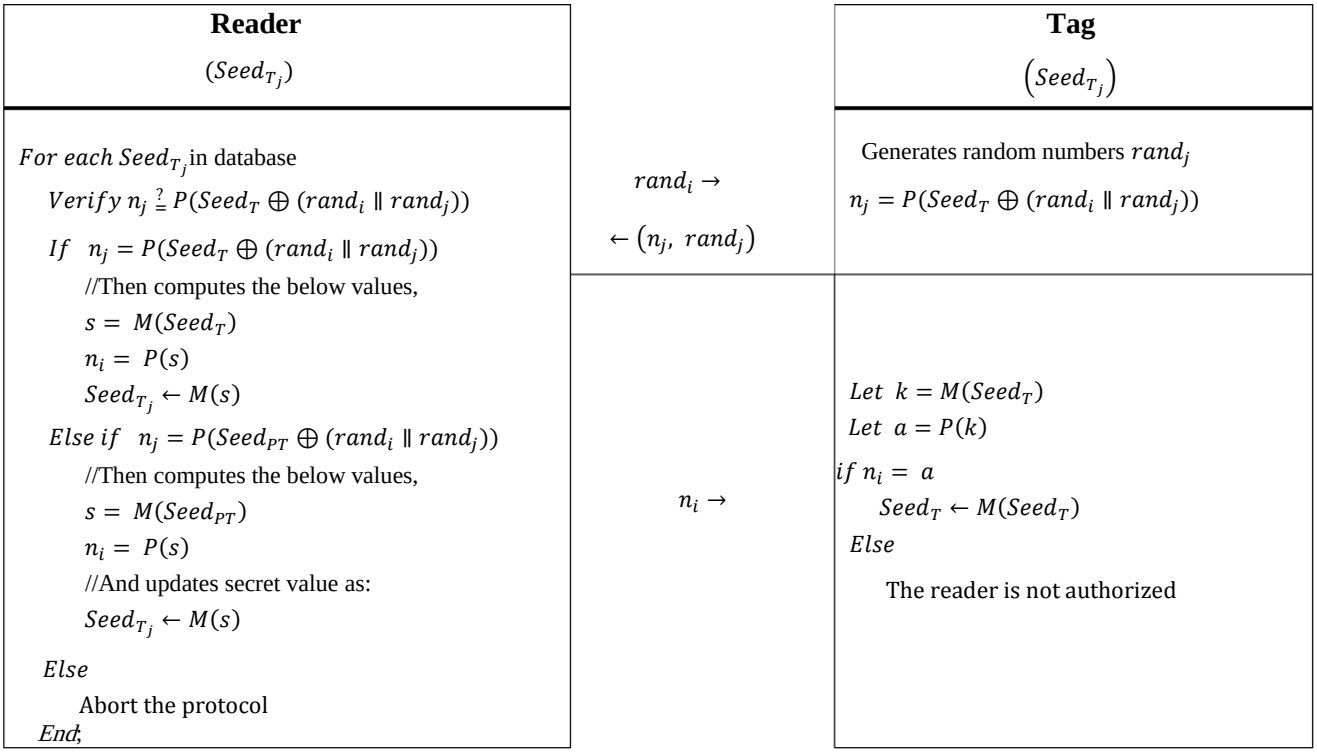

Fig. 2. The SLRAP protocol [17]

3. Vulnerabilities of the SLRAP Protocol

This section aims to cryptanalyze the SLRAP protocol. With a slightly different view it is clear that the SLRAP protocol has not an efficient design and it has some weaknesses which make it vulnerable to some attacks such as *Secret parameter reveal*, *Tag impersonation* and *Reader Impersonation* attacks.

3.1 Secret parameter reveal

In the RFID authentication protocols, it is so important and necessary which the secret parameters stay secure in communication and an attacker does not eavesdrop and obtain them. In this subsection, we show how an attacker can reveal the secret parameter $Seed_T$ and abuse it. This attack can be expressed in two phases as follows,

Learning phase: In this phase, the attacker is as an eavesdropper. After one successful run, he/she saves the exchanged data between the tag and the reader including $n_j, rand_j$ and $rand_i$ that the reader sent to the tag.

Attack phase: Then, the attacker uses $n_j = P\left(Seed_T \oplus \left(rand_i \parallel rand_j\right)\right)$, which is the obtained data in the learning phase. Now, since the length of $Seed_T$ is L-bit, thus $Seed_T \epsilon Z$, where $Z = \{z_1, z_2, \dots, z_{2^l}\}$. The attacker calculates $Seed_T$ as follows,

$For\ 1 \le q \le 2^l$
$Choose\ z_q \in Z$
$if\ n_j^{T_0} = P(z_q \oplus (rand_i \parallel rand_j))\ then$
return $z_q\ as\ Seed_T$
End

Note that, via $Seed_T$, the attacker can calculate the secret value of the target tag T_0 in every run such as run n, by n times applying P function and M function on the secret value $Seed_T$.

It is shown that, in order to perform secret parameter attack, the attacker needs to eavesdrop the transmitted data in one session of the SLRAP protocol, and needs 2^l *P(.)* computations.

3.2 Tag Impersonation Attack

In this attack, the attacker tries to impersonate a tag to receive response from the reader [20]. In the rest of subsection, tag impersonation attack is done on the *SLRAP* protocol. This attack can be summarized as follows,

Learning phase: In this phase, the attacker is as an eavesdropper. After one successful run, he/she saved the exchanged data between the reader and the target tag including $(n_j, rand_j, rand_i)$. Then by using Algorithm

presented in Section 3.1, the attacker calculates the secret value $Seed_T$.

Attack phase: The attacker plays role of the legitimate tag and starts a new session with the reader. When the reader sends $rand_{i+1}$to the target tag, the attacker, first generates a random number $rand_{j,adv}$, then he/she uses the obtained parameters in the *learning phase* and computes $n_{j,adv}$ as follows,

$$n_{j,adv} = P\left(Seed_T \oplus \left(rand_{j,adv} \parallel rand_{i+1}\right)\right)$$

After that, the attacker sends messages $n_{j,adv}$ and $rand_{j,adv}$ to the reader.

Finally, since $n_{j,adv}$ and $Seed_T$ calculated correctly, the reader admits the attacker as a legal tag and authenticates him/her.

3.3 Reader Impersonation attack

In this subsection, we will show that the SLRAP protocol is also vulnerable to reader impersonation attack. In this attack, the attacker tries to forge a legitimate reader. This attack can be perform as follows,

1) The attacker eavesdrops exchanged data between the target tag and the reader, and calculates $Seed_T$ the same as previous sections.
2) The attacker starts a new session with the target tag and sends $rand_{i,adv}$ to it. Then, he/she receives n_j and $rand_j$ from the target tag.
3) Using $Seed_T$, n_j and $rand_j$, the attacker computes $n_{i,adv}$ and s_{adv} as follows and forwards $n_{i,adv}$ to the target tag.

$$s_{adv} = M(Seed_T)$$

$$n_{i,adv} = P(s_{adv})$$

Since s_{adv} and $n_{i,adv}$ calculated correctly, the target tag admits the attacker and authenticates him/her and updates its secret value. As a result, the attacker can perform reader impersonation attack with successfully probability "1".

4. Improved Version of *SLR*AP Protocol

In section 3, it is shown that the SLRAP protocol has some weaknesses and it suffers from *Secret parameters reveal*, *Tag impersonation* and *Reader impersonation attacks*, so in this section we aim to propose a strengthened version of the SLRAP protocol which omits all existing weaknesses. In the proposed protocol, we apply some changes on the updating, authentication and exchanged messages that increase the security and privacy of the proposed protocol and make it secure against different attacks. The new changes can be expressed as follows,

- In the SLRAP protocol the value of n_j is equal to $n_j = P(Seed_T \oplus (rand_i \parallel rand_j))$ that in the proposed protocol we change it to $n_j = M(Seed_T \oplus (rand_i \parallel rand_j))$.
- The next change is in the reader responses. In the SLRAP protocol, the reader responses to the tag with $n_i = P(s)$. In the proposed protocol, we change it to

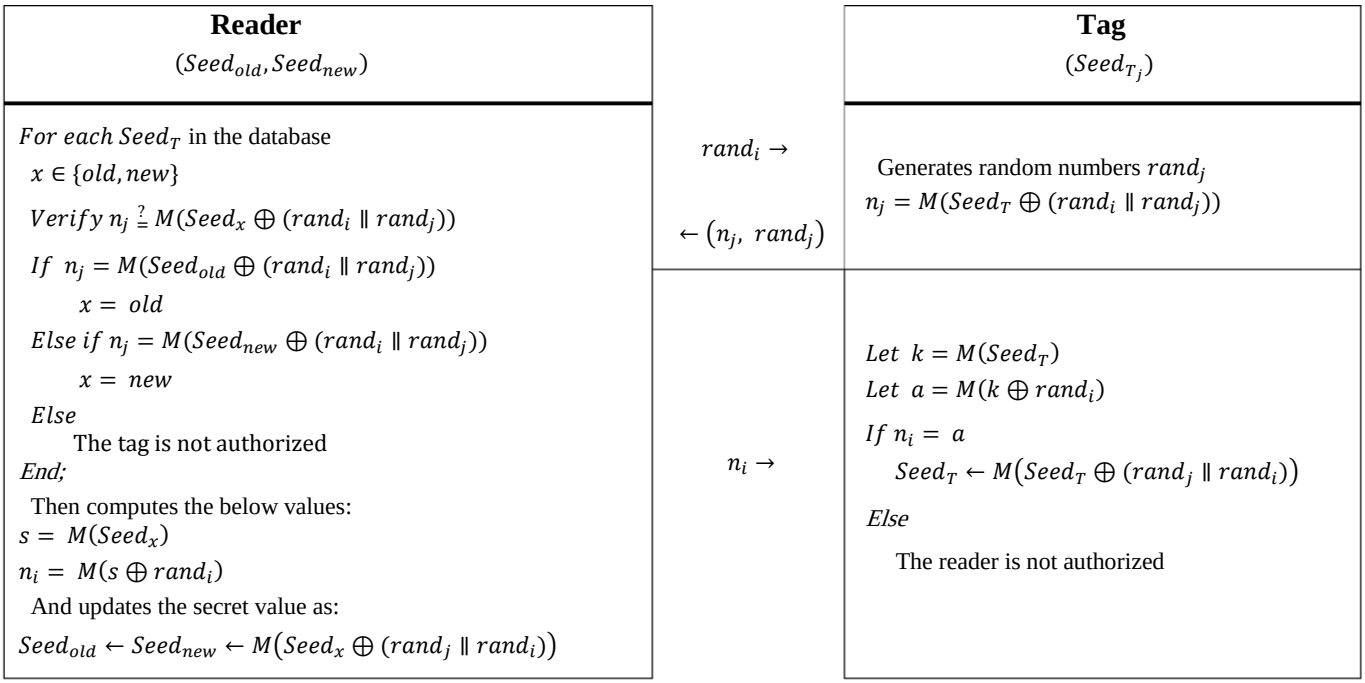

Fig. 3. The improved version of the SLRAP protocol.

$n_i = M(s \oplus rand_i)$.

- In the SLRAP protocol, the reader stores just secret value $Seed_T$ in its database which uses in current session. This fact make the protocol vulnerable to DoS attack. In the proposed protocol, we define two secret values $Seed_{old}, Seed_{new}$ which stored in the reader to prevent DoS attack.
- Moreover, we modify updating of SLRAP as follows,

$$Seed_T \leftarrow M\big(Seed_T \oplus (rand_j \parallel rand_i)\big).$$

After applying all the proposed modifications, the final structure of the strengthened version of the SLRAP protocol is shown in Fig. 3. The improved protocol is done in four steps which can be express as follows.

Reader → Tag: The reader generates a random number $rand_i$, and sends it to the tag.

Tag → Reader: The tag generates a random number $\boldsymbol{rand_j}$, and computes $\boldsymbol{n_j = M(Seed_T \oplus (rand_i \parallel rand_j))}$ and then forward them to the reader.

Reader→Tag: After receiving messages from the tag, the reader performs the following steps,

a) Using the stored $\boldsymbol{Seed_{old}}$ and $\boldsymbol{Seed_{new}}$ in its database, the reader calculates $\boldsymbol{M(Seed_x \oplus (rand_i \parallel rand_j))}$, where $\boldsymbol{x \in \{old, new\}}$ and verifies $\boldsymbol{n_j \stackrel{?}{=} M(Seed_x \oplus (rand_i \parallel rand_j))}$. If $\boldsymbol{n_j = M(Seed_{old} \oplus (rand_i \parallel rand_j))}$, the reader uses $\boldsymbol{Seed_{old}}$ to authenticate the tag else if $\boldsymbol{n_j = M(Seed_{new} \oplus (rand_i \parallel rand_j))}$ it uses secret parameter $\boldsymbol{Seed_{new}}$ and authenticates the tag. Otherwise the reader does not authenticate the tag and aborts the rest of protocol.

b) After authenticating the tag by the reader, the reader computes $\boldsymbol{s = M(Seed_x)}$ and $\boldsymbol{n_i = M(s \oplus rand_i)}$. Then the reader sends $\boldsymbol{n_i}$ to the tag and update its secret value as follows,

$\boldsymbol{Seed_{old} \leftarrow Seed_{new} \leftarrow M\big(Seed_x \oplus (rand_j \parallel rand_i)\big)}$ Which means first of all $\boldsymbol{Seed_{old} \leftarrow Seed_{new}}$ to keep one last updated secret value, then fills $\boldsymbol{Seed_{new}}$ with the new one ($\boldsymbol{M\big(Seed_x \oplus (rand_j \parallel rand_i)\big)}$).

Tag: After receiving the message $\boldsymbol{n_i}$ from the reader, the tag computes $\boldsymbol{k = M(Seed_T)}$ and $\boldsymbol{a = M(k \oplus rand_i)}$ and checks if $\boldsymbol{n_j = a}$ or not. If they were equal, the tag authenticates the reader successfully and updates its secret value as follows,

$$\boldsymbol{Seed_T \leftarrow M\big(Seed_T \oplus (rand_j \parallel rand_i)\big)}$$

Otherwise, the tag stops the session and the protocol aborts.

5. Analysis of the Proposed Protocol

In this section, in order to evaluate the security and the privacy of the proposed protocol, some security and privacy analysis are provided. Indeed, we will show that how the proposed modifications overcome to all of the reported weaknesses and also make the protocol resistant against various security and privacy attacks.

5.1 Secret Parameters Reveal

In section 3.1, we showed that how an attacker can use n_j to obtain the secret parameter$Seed_T$, but in the proposed protocol this weaknesses removed by changing $n_j = P(Seed_T \oplus (rand_i \parallel rand_j))$ to $n_j = M(Seed_T \oplus (rand_i \parallel rand_j))$. It is obvious that with the new n_j the attacker cannot obtain $Seed_T$, because of one-way hash function. As a result, the proposed protocol is safe against secret parameters reveal attack.

5.2 Replay Attack

In the proposed protocol, due to applied some changes in the transmitted data between the tag and the reader including n_j and$rand_j$, the security of the exchanged messages have increased which prevent any modifications and replay attack.

5.3 Impersonation Attack

In section 3.2, it is shown which the structure of the SLRAP protocol has some problems that make it vulnerable to impersonation attacks. In the proposed protocol, in order to perform impersonation attacks, the attacker needs $Seed_T$ to calculate exchanged messages between the tag and the reader including n_j andn_i, where $n_j = M(Seed_T \oplus (rand_i \parallel rand_j))$ and $n_i = M(s \oplus rand_i)$. In other side, since all mentioned secret parameters are protected by hash function, thus the attacker cannot impersonate the tag or the reader. As a result the proposed protocol is secure against impersonation attacks.

5.4 Privacy

In the proposed protocol, in order to enhance the privacy of the SLRAP protocol, we apply some changes in the updating procedures as $Seed_T \leftarrow M\big(Seed_T \oplus (rand_j \parallel rand_i)\big)$. With this modification, the stored keys in database will be protected and an attacker cannot use the secret parameters for his/her inauspicious goals. As a result, the proposed protocol can provide user privacy and it is safe against different traceability attacks.

Finally, Table 2 shows a comparison of the security and privacy analysis for the proposed protocol and some similar protocols that have been proposed recently. As it can be seen, the security and the privacy of the proposed

protocol are complete and it can provide secure communication for RFID users.

Table 2. Comparison of security analysis

Protocols / Attacks	Hoque et al. [18]	SLRAP [17]	Improved SLRAP
Secret Values Reveal	✓	×	✓
Replay	✓	✓	✓
Tag Impersonation	×	×	✓
Reader Impersonation	×	×	✓
DoS	✓	×	✓

✓: Secure ×: Insecure

6. Conclusions

In this study, we analyzed a mutual authentication protocol (SLRAP) for RFID systems that proposed by *Deng et al.* in 2014. They were claimed that their protocol is secure against various attacks. However we showed that their protocol has some weaknesses that makes it vulnerable against secret parameters reveal, tag impersonation, reader impersonation attacks. Moreover, we proposed an improved version of the SLRAP protocol that eliminates all existing weaknesses. Security analysis illustrated that the proposed protocol is secure against different attacks.

References

[1] G. D. Vecchia and M. Esposito, "A Knowledge-Based Approach for Detecting Misuses in RFID Systems, Designing and Deploying RFID Applications, DOI: 10.5772/17535.," 15 June 2011. Available: http://www.intechopen.com/books/ designing-and-deploying-rfid-applications/a-knowledge-based-approach-for-detecting-misuses-in-rfid-systems.

[2] D. Heyden , "RFID Applications," Fibre2Fashion, Available: http://www.fibre2fashion.com/industry-article/ 11/1023/rfid-applications1.asp. [Accessed 11 February 2014].

[3] "Transport for London, Oyster,". Available: http://www.tfl.gov.uk/tickets/27298.aspx. [Accessed 01 02 2014].

[4] P. Picazo-Sanchez, N. Bagheri, P. Peris-Lopez, and J. E. Tapiador, "Two RFID Standard-based Security protocols for healthcare environments," *Journal of Medical Systems*, vol. 37, no. 5, pp. 1-12, 2013.

[5] T. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Jules and T. Ohare , "Vulnerabilities in first-generation RFID-enabled credit cards," in *Financial Cryptography and Data Security*, 2007.

[6] S. M. Alavi, B. Abdolmaleki, and K. Baghery, "Vulnerabilities and improvements on HRAP+, a hash-based RFID authentication protocol," *Advances in Computer Science: an International Journal*, vol. 3, no. 6, pp. 51-56, 2014.

[7] J. Banks, M. Pachano. L. Thompson, and D. Hanny, RFID applied, John Wiley & Sons, Inc., 2007.

[8] M. Mohammadi, M. Hosseinzadeh and M. Esmaeildoust, "Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard," *Journal of Advances in Computer Science (ACSIJ)* , vol. 3, no. 2, pp. 10-16, 2014.

[9] M. R. Alagheband, and M. R. Aref , "Simulation-based traceability analysis of RFID authentication protocols," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1020-1038, 2014.

[10] S.M. Alavi, K. Baghery, B. Abdolmaleki, and M. R. Aref, "Traceability analysis of recent RFID authentication protocols," *Wireless Personal Communications, DOI 10.1007/s11277-015-2469-0*, March 2015.

[11] B. Abdolmaleki, K. Baghery, B. Akhbari, and M. R. Aref, "Attacks and improvements on two new-found RFID authentication protocols," in *7th International Symposium on Telecommunications (IST)*, Tehran, 2014.

[12] Sh. Wang, S. Liu, and D. Chen, "Security analysis and improvement on two RFID authentication protocols," *Wireless Personal Communications*, pp. 1-13, 2014.

[13] Z. Sohrabi-Bonab, M. R. Alagheband, and M. R. Aref, "Formal cryptanalysis of a CRC-based RFID authentication protocol," in *The 22nd Iranian Conference on Electrical Engineering (ICEE 2014)*, Tehran, 2014.

[14] G. Avoine, "Privacy-friendly synchronized ultralightweight authentication protocols in the storm," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 826-843, 2012.

[15] D. Z. Sun, and J. D. Zhong, "A hash-based RFID security protocol for strong privacy protection," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1246-1252, 2012.

[16] H. Kim, "Desynchronization Attack on Hash-based RFID Mutual Authentication Protocol," *Journal of Security Engineering*, vol. 9, no. 4, pp. 357-366, 2012.

[17] M. Deng, W. Yang, and W. Zhu, "Weakness in a server-less authentication protocol for radio frequency identification," in *Mechatronics and Automatic Control Systems*, pp. 1055-1061, 2014.

[18] M. E. Hoque, F. Rahman, S. Ahmed, and J. H. Park, "Enhancing privacy and security of RFID system with serverless authentication and search protocols in pervasive environments," *Wireless personal communications*, vol. 55, no. 1, pp. 65-79, 2010.

[19] M. Pourpouneh, R. Ramezanian, and F. Salahi, "An improvement over a server-less RFID authentication protocol," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 7, no. 1, pp. 31-37, 2015.

[20] G. Avoine, Cryptography in Radio Frequency Identification and Fair Exchange Protocols, PHD Thesis, Lausanne, University of EPFL, 2005.