Token Based RFID authentication using Identity Based Encryption

Pushplata Sahu, Prof. Sadhna Mishra, Prof. Vineet Richhariya

1M.Tech Computer Science Department
LNCT BHOPAL (M.P), INDIA
Email: psahu13@gmail.com, sadhnamanit@yahoo.com, vineet_rich@yahoo.com

ABSTRACT

Radio Frequency Identification (RFID) is a device used for the detection of objects such that the data can be monitored at each stage. A RFID device consists of a Tag, a Reader and a Server. The Data read by the Tag device need to be send wirelessly to the reader. During the transmission of Data from Tag to Reader the chances of eavesdropping and various attacks is possible. So here proposed a new technique of providing authentication between Tag and the Reader to prevent from various attacks and the data is send securely.

Keywords: RFID, Tags, Reader, authentication, counterfeiting, privacy, security.

1 INTRODUCTION

A RFID system consists of three main components that enable it to operate and function properly, and those are: a reader, a set of tags, and a backend database or a server. The reader is a device that wirelessly queries the tags to identify them. RFID tags are simple and cheap devices that consist of small integrated circuits equipped with a radio antenna. These tags are given each a unique ID number and are mounted on all the objects that are intended to be identified.[1]

Due to the benefits of the technology of RFID it is currently employed in various commercial sectors to provide automated assistance for mundane tasks. There are hospitals which have employed tagged bracelets to make sure that the maximum care is given to surgical patients. At various airports around the world, RFID is being utilized to track passengers’ bags to make sure that the position of the bags will be known at all times. Many of the pets contained RFID chips implanted to make sure of that, when it is getting lost, the authorities can find their owners’ information by simple searching the tag that are attached to the objects. In so many cities and countries the RFID-enabled toll system designed for cars at RFID enabled toll booths which allow drivers to continue on their journey and avoid the necessity of stopping to pay. Despite the advantages gained from RFID technology integration, various drawbacks prevent the wide-scale adoption into the majority of the commercial sector. There are three main issues concerning the integration of the architecture. The first issue is security when using the technology as tags are prone to various physical and virtual attacks upon the system. The second concern stems from the need of privacy surrounding the data collected as the observations recorded can be used for breaches in privacy. The third issue is that the data collected in various systems, generally in particular where passive tags are utilized, produces data characteristics that make the systems harder to use.[2]

RFID issues

Before RFID can be utilized to its maximum potential, as opposed to the fraction in which it is presently in work definite issues need to be understood by the users, and corrected if possible. The three core obstacles include the concerns of security, the problems surrounding the privacy of the data captured and the characteristics associated with the nature of RFID. Additionally, we will further examine the specific problems associated with anomalies present within the captured observational records which are regarded as characteristics of RFID. When all of these issues are rectified to provide maximum security, privacy and integrity, RFID will be able to realize its full potential in massive wide-scale adoptions.

RFID security

The issues associated with RFID Security, also known as Intrusion Detection, refer to the discovery of foreign attacks upon the system usually utilizing the tags that hinder the overall veracity of the data. There are various regarding the RFID, some of the most dominant with regard to RFID security (et al., 2010; Thamilarasu & Sridhar, 2008):

• Eavesdropping: The data send from tag to the reader can’t be access from the external user.
• Unauthorized Tag Cloning: Copying tag data onto an additional tag to gain the same privileges.
• Man-in-the-Middle (MIM) Attack: When an external object pretends to be either a tag or reader between actual tags and readers.
• Unauthorized Tag Disabling: When an external reader disables a tag not allowing it to be utilized again.
• Unauthorized Tag Manipulation: Manipulating the tag data using an external reader.
RFID privacy

Privacy within the context of an RFID-enabled facility refers to either unknowingly releasing critical information (deriving specific knowledge or tracking meaningless data) (Langheinrich, 2009), and compile a list of all items currently found on a person (Juels, 2006). There have been several methodologies proposed in the past to ensure maximum privacy of an individual, including the general approaches of Encrypting/Rewriting and Hiding/Blocking Tags (Langheinrich, in 2009). According to the general solutions possible, there have been more specific and advanced approaches suggested such as killing/sleeping the Tags, carrying around a privacy-enforcing RFID device, releasing certain information based solely on distance from the reader and introducing Government Legislations (Juels, 2006).

2 RELATED WORKS

The protocols implemented for the authentication of the tag and the reader provides security of the data send from the tag to the reader. Although there are many security protocols implemented for the RFID authentication. A brief survey is given in the papers.

Weis, Sarma, Rivest and Engels proposed in 2003 the use of hash-locks in RFID devices. A first approach, called Deterministic hash locks, was presented in. A tag is usually in a \"locked\" state until it is queried by a reader with a specific temporary meta-identifier Id. This is the result of hashing a random value (nonce) selected by the reader and stored into the tag. The reader stores the Id and the nonce in order to be able to interact with the tag. The reader can unlock a tag by sending the nonce value. When a tag receives it, the value is checked [7].

Most of the security protocols implemented in RFID are based on cryptographic and hash functions. But these security protocols are not much secure. The OSK protocol was proposed by Ohkubo, Suzuki and Kinoshita (OSK) in 2004 [8]. Its aim is to assure the valid answer of the tag even under an active attack. In this scheme each tag is initialized with a secret value xi and two unidirectional functions h1 and h2. When a tag receives a request from a reader, it updates the value xi with the new value obtained from the computation of h1(xi) [7].

YA-TRAP (Yet-Another Trivial RFID Authentication Protocol) was proposed by Tsudik in 2006 [9]. This protocol describes a technique for the inexpensive untraceable identification of RFID tags. YA-TRAP involves minimal interaction between devices and a low computational load on the back-end server. With these features, this scheme is attractive for applications where the information is processed in data groups [7].

Weis, Sarma, Rivest and Engels proposed in 2003 [10] the use of hash-locks in RFID devices. A first approach, called Deterministic hash locks, was presented in. A tag is usually in a \"locked\" state until it is queried by a reader with a specific temporary meta-identifier Id. This is the result of hashing a random value (nonce) selected by the reader and stored into the tag. The reader stores the Id and the nonce in order to be able to interact with the tag. The reader can unlock a tag by sending the nonce value. When a tag receives it, the value is checked [7].

In 2012, Dr.S.Suja proposed an RFID Authentication protocol for security and privacy which is based on Cyclic Redundancy Check (CRC) and Hamming Distance Calculation in order to achieve reader-to-tag authentication and the memory read command is used to achieve tag-to reader authentication. It will resist against tracing and cloning attacks in the most efficient way [5].

In 2011, Liangmin Wang, Xiaoluo Yi, implies improved protocol merely uses CRC and PRNG operations supported by Gen-2 that require very low communication and computation loads. They also develop two methods based on BAN logic and AVISTA to prove the security of RFID protocol. BAN logic is used to give the proof of protocol correctness, and AVISTA is used to affirm the authentication and secrecy properties [4].

In 2008, Tieyan Li analyzes the security vulnerabilities of a family of ultra-lightweight RFID mutual authentication protocols: LMAP, M2AP and EMAP [12]*, which are proposed by Peris-Lopez et al. Here they identify two successful attacks, such as de-synchronization attack and full discovery attack, against their protocols. The former permanently disables the authentication capability of a RFID tag by destroying synchronization between the tag and the RFID reader [3].

The weakness of this authentication protocol comes from the fact that each round the adversary gets some information from the same key. So a quick way to counter our attack is to include a key-updating mechanism similar to OSK [13] at the end of the protocol using a one-way function. In this case, adversaries do not get more than P equations for each key so that the security proof and reduction to the SAT problem become sound. The resulting protocol is even forward-private providing that adversaries do not get side-channel information from the reader.


Hash-based Access Control (HAC), as defined by Weis et al. [11]*, is a scheme which involves locking a tag using a one-way hash function. A locked tag uses the hash of a random key as its metaID. When locked, a tag responds to all queries with its metaID. However, the scheme allows a tag to be tracked because the same metaID is used repeatedly [5].

In [8] Ohkubo, Suzuki, and Kinoshita (OSK) propose an RFID privacy protection scheme providing indistinguishability and backward untraceability. This scheme uses a low-cost hash chain mechanism to update tag secret information to provide these two security properties.
RFID Authentication with SASI Protocol

In August 2011 [1] a new RFID verification procedure, calculated for providing Strong Authentication and Strong Integrity. These protocols, suitable for passive Tags with limited computational control and storage space, involve simple bitwise operations such as or operation, exclusive or, modular totaling, and recurring shift operations. SASI was explicitly proposed in [1] as an improvement of the UMAP protocols, in order to provide authenticity and integrity and withstand all the possible attacks the UMAP protocols are subject to.

3 PROBLEM STATEMENT

The SASI protocol is based on Strong Authentication and Strong Integrity of the data from the tag to the reader. Although this protocol and also many protocols are implemented for the authentication between the tag and the reader such as desynchronization attacks, identity disclosure attacks and many other attacks but in most of the protocols only certain types of attacks have been removed and if any party can attack the server.

4 PROPOSED SOLUTION

The protocol implemented here is based on two password authentication between the tag and the reader.

![Diagram](image)

As shown in the above figure is the generation of the token from the reader and send to the tag and server on the basis of the identity of the tag. As the tag logins it send the request first to the reader then the reader on the basis of the

Algorithm used

Step-1: New Tag account is created.
Step-2: Existing Tag is logged in by providing the identification of the Tag and entering the pin number.
Step-3: The token number is generated.
Step-4: The SHA256 algorithm is used for generating the Hash message.
Step-5: This Hash message is taken and XOR operation is made.
Step-6: Then the XOR-ed message was encoded using Base64 algorithm.
Step-7: From the encoded message a random six digit output is taken as token number.
Step-8: The generated token number is sent to the Tag and the server.
Step-9: With the help of the token number the Tag performs various operations like sending the data to the Reader over a secure channel.

5 RESULT ANALYSIS

As shown in the Table 1. is the generation of time complexity on the basis of number of keys. As the number of keys gets increases generation time also increases. Here multiple tags are used for the generation of data and hence each tag generates a separate token.

<table>
<thead>
<tr>
<th>Number of Keys</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>3.45</td>
<td>6.9</td>
<td>10.35</td>
<td>13.8</td>
<td>17.25</td>
<td>20.7</td>
</tr>
</tbody>
</table>

Table 1. Comparison of Time Vs No. of Keys

As shown in the Figure 1. Is the graph analysis of generation of keys and time takes to generate these keys which will acts as a token.
6. CONCLUSION & FUTURE SCOPE

During the transmission of data from Tag to Reader authenticity of the valid Tag and Reader is necessary. Here in this paper a concept of Token based authentication is proposed and the result analysis shows that the proposed technique is secure and takes less storage and computation cost. Also the proposed technique of authentication is more secure and provides prevention from various types of attacks.

Although the present technique of authentication provides prevention from various attacks and also the storage and time is less but we can implement the concept of authentication in tag and reader using the concept of one time private key (OTPK) so that two factor is not needed.

REFERENCES

[5] an rfid authentication protocol for security and privacy , dr. s. suja, m.e., ph.d., associate professor, electrical and electronics engineering, coimbatore institute of technology, coimbatore. a. arivarasi, m.e, embedded and real time systems, coimbatore institute of technology, coimbatore.
[6] d. n. duc, j. park, h. lee, and k. kim. enhancing security of epcglobal gen-2 rfid tag against traceability and cloning. in symposium on cryptography and information security — scis 2006, hiroshima, japan, january 2006. the institute of electronics, information and communication engineers.
[7] a brief survey on rfid privacy and security j. aragones vilella , a. martinez-ballest e and a. solanas crises research group unescor chair in data privacy dept. of computer engineering and mathematics, rovira i virgili university.
[9] g. tsudik. ya-trap: yet another trivial rfid authentication protocol. in fourth annual ieee international conference on pervasive computing and communications workshops (percomw’06), pages 640(643, 2006).

Table 2. Storage Cost needed with Keys Generation

As shown in the figure 2 is the graph analysis of storage cost needed in the authentication of token from the tag to the reader.

<table>
<thead>
<tr>
<th>Storage (bytes)</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>2500</td>
<td>50</td>
</tr>
<tr>
<td>5000</td>
<td>100</td>
</tr>
<tr>
<td>10000</td>
<td>200</td>
</tr>
<tr>
<td>25000</td>
<td>500</td>
</tr>
<tr>
<td>50000</td>
<td>1000</td>
</tr>
</tbody>
</table>

Figure 1. Graph Analysis of Time Vs Keys

As shown in the Table 2. is the storage cost needed to generate n tokens. Here the storage cost of the tags and the reader depends on the data and the number of keys needed.

Figure 2. Storage Cost Vs No. of Keys
