Volume 2, No. 12, December 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

OPERATIONAL AND SECURITY REQUIREMENTS FOR RFID SYSTEM

Daniyal M. Alghazzawi
Faculty of Computing & Information Technology
Department of Information Systems, King Abdul-Aziz University, Kingdom of Saudi Arabia
Dghazzawi@kau.edu.sa

***Abstract.*:** In many fields such as wireless communication, circuit and electromagnetic areas, RFID (Radio Frequency Identification) is one of the most challenging devices in recent year because of it's potential and ongoing applications of such as supply chains, livestock/inventory tracking, toll management, airline baggage management, access control and so on. This paper descibes briefly the various Operational and security requirements for RFID systems. It focus especially system scalability, anonymity and anti-cloning.

Keywords: RFID, counterfeiting, authentication, Adversary, small area implementations.

INTRODUCTION

RFID is expected to completely replace the bar code systems in near future. For commercial markets, RFID systems should overcome not only the restriction of cheap RFID tags but also operational and security problems such as scalability, the tracking problem and the cloning problem. In many cases, the security part is simplified in order to minimize a tags price. For example, Class-1 EPCglobal Gen2 [1] has a very simple authentication scheme where a password is transmitted in a plain text, which can cause many security problems.

Fortunately, the CMOS technologies steadily advance and the fabrication costs decrease, which allows stronger security solutions on tags. Moreover, some applications such as expensive goods and access control systems that should be highly secured can afford more expensive tags which may include more resources such as an extra power source, gate area and memory.

BACKGROUND

In this section we have described about the technology of RFID system, frequencies in RFID and about RFID Tag

The Technology behind RFID:

With RFID, the electromagnetic or electrostatic coupling in the RF (radio frequency) portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which read the radio frequency and transfers the information to a processing device (reader) and a transponder, or RF tag, which contains the RF circuitry and information to be transmitted. The antenna provides the means for the integrated circuit to transmit its information to the reader that converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can analyze the data. In RFID systems, the tags that hold the data are broken down into two different types. Passive tags use the radio frequency from the reader to transmit their signal.

Passive tags will generally have their data permanently burned into the tag when it is made, although some can be written. Active tags are much more sophisticated and have on-board battery for power to transmit their data signal over a greater distance and power random access memory (RAM) giving them the ability to store up to 32,000 bytes of data.

RFID Frequencies:

Much like tuning in to your favorite radio station, RFID tags and readers must be tuned into the same frequency to enable communications. RFID systems can use a variety of frequencies to communicate, but because radio waves work and act differently at different frequencies, a frequency for a specific RFID system is often dependant on its application. High frequency

RFID systems (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) offer transmission ranges of more than 90 feet, although wavelengths in the 2.4 GHz range are absorbed by water, which includes the human body, and therefore has limitations.

RFID Tags:

RFID-Tags are small devices used for identification purposes in many applications nowadays. It is expected that they will enable many new applications and link the physical and the virtual world in the near future. Since the processing power of these devices is low, they are often in the line of are when their security and privacy is concerned. It is widely believed that devices with such constrained resources cannot carry out sufficient cryptographic operations to guarantee security in new applications. RFID tags consist of an antenna connected to a microchip.

Because of the presence of this microchip, they can be considered as the next generation bar codes. One of their main advantages over bar codes is that they can be read out without line of sight. It is expected that in the near future trillions of these devices will be deployed. They will be used to identify goods and provide a link between the physical and the virtual world. It is predicted that this connection will lead to the next revolution after the Internet: The Internet of Things. Currently the main applications for RFID tags include: goods tracking in supply chain management, automated inventory management, automated quality control, access control, payment systems, etc. In the future, however, tagged items will also communicate with

intelligent devices in the home (intelligent fridges, washing machines, etc.) and provide additional benefits to consumers. For example, a fridge will automatically detect whether the food is still OK and warn the consumer when necessary, the washing machine will detect the color of clothes in the washing and switch on the appropriate program, and, in general, home appliances will be intelligent and be able to communicate with other devices.

The fact that tags can be read without the need for line of sight, introduces a privacy threat. While walking home with tagged items in their bags, consumers can be scanned by unauthorized readers without their consent or permission. This potentially reveals privacy sensitive information about their preferences, things they buy, etc. New applications for RFID-Tags will introduce additional security risks. For instance, an emerging application that is being considered is the use of RFID-Tags for anti-counterfeiting purposes [2].

By locating an RFID-tag with specific product and reference information on a product, one can verify the authenticity of the product. This is done by running a secure protocol between a tag and a reader. If the required information is on the tag and verified to be authentic, the product is declared to be genuine and otherwise not. In a cloning attack, the attacker captures the necessary authentication information (obtained e.g. by eavesdropping on the channel between the tag and the reader), and stores it in a new chip. In this way the attacker has effectively cloned the original tag. This clone cannot be distinguished from an original tag by a reader. In order to make the cloning of tags infeasible, it should not be possible to derive the tag secrets by active or passive attacks. Recently a lightweight version of such an authentication protocol was developed in [2]. The security of the protocol is based on the Learning Parity in the presence of Noise (LPN) problem. The protocol in [2] is proven secure against passive and against active adversaries in a detection-based model.

The fact that tags have very constrained resources (memory, power, speed, area) but need security measures poses very interesting challenges to the security community. First, it is natural to investigate whether existing cryptographic algorithms can be implemented on a tag. Second, it encourages research for new protocols and algorithms targeted at resource constrained devices. Efficient implementations of AES for RFIDs have been investigated in [5], where it was shown that AES can be implemented in under 5000 gates. New lightweight protocols for RFID-Tags were developed in [2]. To the authors' knowledge no implementations of ECC on RFID tags in less than 18,000 gates have been shown to be feasible.

Moreover, the research community lacks consensus as to the feasibility of implementing public-key crypto-algorithms on (high-end) RFID tags. For example, [3] claim that public key cryptography on a tag is possible and states: Unfortunately asymmetric cryptography is too heavy to be implemented on a tag".

Common use of RFID system:

RFID systems can be used just about anywhere, from clothing tags to missiles to pet tags to food - anywhere that a unique identification system is needed. The tag can carry information as simple as a pet owners name and address or the cleaning instruction on a sweater to as complex as instructions on how to assemble a car. Here are a few examples of how RFID technology is being used in everyday places: RFID systems are being used in some hospitals to track a patient's location, and to provide real-time tracking of the location of doctors and nurses in the hospital. In addition, the system can be used to track the whereabouts of expensive and critical equipment, and even to control access to drugs, pediatrics, and other areas of the hospital that are considered"restricted access" areas. RFID chips for animals are extremely small devices injected via syringe under skin. Under a government initiative to control rabies, all Portuguese dogs must be RFID tagged by 2007.

When scanned the tag can provide information relevant to the dog's history and its owner's information. RFID in retail stores offer real-time inventory tracking that allows companies to monitor and control inventory supply at all times.The Orlando/Orange County Expressway Authority (OOCEA) is using an RFID based traffic-monitoring system, which uses roadside RFID readers to collect signals from transponders that are installed in about 1 million E-Pass and Sun Pass customer vehicles.

The feature of RFID:

RFID is said by many in the industry to be the frontrunner technology for automatic identification and data collection. The biggest, as of yet unproven, benefit would ultimately be in the consumer goods supply chain where an RFID tag attached to a consumer product could be tracked from manufacturing to the retail store right to the consumer's home. Many see RFID as a technology in its infancy with an untapped potential. While we may talk of its existence and the amazing ways in which this technology can be put to use, until there are more standards set within the industry and the cost of RFID technology comes down we won't see RFID systems reaching near their full potential anytime soon.

MODEL OF AN RFID SYSTEM

A Model for an RFID authentication system An RFID authentication system has three components: tags *T*, readers *R*, and a trusted server *S*. Tags are wireless transponders: they typical have no power of their own and respond only when they are in an electromagnetic field. Readers are transceivers and generate such fields: they challenge by broadcast any responding tag. There are two types of broadcast challenges: multicast and unicast. Multicast challenges are addressed to all tags in the range of the reader, whereas unicast challenges are addressed to specific tags. In our protocols below we have both types of challenges. However, our multicast challenges are just random strings, and all tags in the range of a reader *R* are challenged with the same random string. This kind of action is not usually counted as a communication pass. We shall assume that all honest tags *T* adhere to the system specifications and the requirements of the authentication protocol.

The same applies for the readers *R* and of course the trusted server *S* they are all honest. Tags are issued with private keys *K* which they share (only) with the trusted server *S*.

These keys are used by the tags for identification. We denote by *K* the set of all authorized keys (issued by *S*). The following fig illustrates the flow of exchanged data, between a tag *T* and the trusted server *S* via the reader *R*, during the authentication of *T*.

$T \longleftrightarrow R \Leftrightarrow S$

We shall refer to the interaction between *T* and *R* as a conversation and the data as an authentication transcript. In our RFID authentication protocols we shall assume that *R* and *S* are linked by a secure communication channel (reliable and authenticated). Therefore,our protocols are essentially two party protocols, one party being a tag *T* and the other a reader *R = RS*, with secure access to a server *S*. These parties are abstracted as probabilistic Turing machines. T-machines with severely restrained resources, and R-machines with adequate resources. For optimistic authentication protocols, the resource must be minimized for both machines.

This model describes the setting for the honest parties: the tags that are authenticated with private keys $K \in K$, that adhere to the protocol, the readers *R* that adhere to the protocol, and the trusted server.

SECURITY PROPERTIES AND ADVERSARY

The Adversary:

The adversary *A* can control a certain number of tags and readers. The tags of the adversary, denoted by *T′*, are unauthorised, in the sense they do not have a private key $K \in K$. Similarly, the readers of the adversary, denoted by *R′*, are unauthorized, in the sense that they do not have authenticated access to the trusted server *S*.An active adversary *A* can modify the conversations between any pair *T*, *R* arbitrarily (e.g. adaptively and concurrently), and indeed initiate and terminate a session, at its choice. As an extension of a passive (eavesdropping) adversary, *A* is also allowed to learn the output of the session, i.e. the reader's decision to accept or not, at the end of every sessions. Since the channel between a reader *R* and the server *S* is assumed secure (authenticated), we do not need allow *A* to interact with the server *S* directly, but only through (honest) readers. When designing secure RFID authentication protocols one should also take into account attacks that are excluded from the security model used (the system). Sometimes these attacks may be prevented by using out-of-system protection mechanisms. Of course, it is preferable to deal with such attacks within the model. Below we list two such attacks:

Attack on RFID System When designing secure RFID authentication protocols one should also take into account attacks that are excluded from the security model used (the system). Sometimes these attacks may be prevented by using out-of-system protection mechanisms. Of course, it is preferable to deal with such attacks within the model. Below we list two such attacks:

Side Channel Attack Side Channel Attack (SCA) is an important issues on RFID tags and also some cheap protection i.e by means of balanced implementation is desirable. Side Channel Attack allowed adversaries to obtain the secret key in the cryptographic device, or partial information on it by observing information such as computing time and power consumption. This is the idea of simple and differential power analysis was first introduce by Kocher [4]. This is a serious threat. Thus implementers need algorithm that are not only efficient but also SCA registrant. Simple power analysis is a technique that involves directly interpreting power consumption measurement collected during cryptographic operations.SPA can yield information about device's operation as well as key material.

Differential power analysis is the technique that involve in large scale power variation due to the instruction sequence. There are effect correlated to data values being manipulated. These variations tend to be smaller and are some times overshadowed by measurement errors and other noise. In such cases,it is still often possible to breaks the system using statistical functions tailored to the target algorithm.

Online man-in-middle relay attacks These are attacks in which an unauthorised reader *R′* and tag *T′* interpose between an authentic tag *T* and reader *R* so that, the authentication flow in (*T;R; S*) is diverted to a flow (*T;R′; T′;R; TS*) that authenticates the imposter *T′* using the authentication data of *T*.

Offline man-in-middle active attacks These are attacks in which an unauthorized reader *R′* and tag *T′* interpose between an authentic tag *T* and reader *R* so that, when *R′* challenges *T* appropriately in (*T;R′*), the data obtained will leak private information of *T* when input to (*T′;R; S*).

Security Definitions:

The security of an RFID protocol can be described in terms of three games, an authentication game *Gauth*, an anonymity game *Ganon*, a tracing game *Gtrace* and an availability game *Gavail*, with players: the adversary *A* against the honest tags *T* and the honest readers *R*. In these games there are two steps. The first step is a preparing step for the adversary *A*:

A is allowed to interact arbitrarily with the tags and the readers. In the second step, A's knowledge is tested. The score of *A* in game *G* is his advantage adv *A* G . *A* wins if his advantage is non-negligible. We now describe in more detail the second steps of the four games: *Gauth*, *Gtrace*, *Ganon* and *Gavail*.

Authentication:

The authentications are done in two ways. By authenticating a reader to a tag, a tag is to be ready to open its information to a reader, and by authenticating a tag to a reader, the system prohibits the usage of fake tags. We can divide published authentication protocols into two types. The first type is the fixed access control in which a tag replies a reader with a fixed message. The second type is the randomized access control in which a tag replies to a reader with a pseudo-random message which varies each time of the responses. The fixed access control is the simplest type so that tags can be implemented in a cheap price. However, this kind of protocols is under the tracking problem [6]. Proposed a fixed access control using a hash based access control, where tags reply with MetaIDs, which are the hash outputs of their real IDs. Even though attackers cannot

figure out the real ID, the constant responses of tags cause the tracking problem.A solution to prevent the tracking problem is the randomized access control. In order to randomize messages, a reader and a tag need to share some secret information which is unknown to attackers so that only the entities which have the secret information can interpret the randomized messages. Again, the randomized access control can be divided into two types depending on whether all the readers and the tags share the same secret information. Without sharing the common secret information among all the readers and the tags, making the response pseudo-random causes some drawbacks. [6] described protocols which resolve tracking problems, but the systems are not scalable since the server needs to perform hashes for all the tags ID every time of authentication protocols. One approach to resolve the un-scalability of randomized access control is proposed in [7].

This scheme used a cryptanalytic method. However, this method also causes some other problems. Since this protocol uses time-memory trade-off method [7], in order to reduce the searching time they have to increase the amount of memory in the server. Another problem is that the searching algorithm is probabilistic, i.e. there is some probability to fail in searching for a tags ID. Even though they are saying the failure probability is small, it can cause a crucial problem in certain applications. Protocols proposed in [8] [9] resolve the tracking problem by sharing the common secret information among all the readers and the tags. Even though these schemes are scalable and resolve the tracking problem, they have a crucial problem. By capturing and compromising only one tag, attackers can reveal the secret information. Once the secret information is revealed, the tags which share the secret information will be under attack and attackers may clone some other tags. Moreover, the protocol in [9] uses a symmetric key encryption algorithm which is unsuitable in low-cost RFID systems.

In the second step of *Gauth;A* must impersonate some tag *T* to some reader *R*. During this impersonation step, *A* is allowed to interact arbitrarily with all other tags and readers, except the one tag *T* that *A* is trying to impersonate. The advantage of the adversary adv *A Gauth* is the probability that *A* succeeds in authenticating itself to *R*. An RFID protocol is a secure authentication protocol if adv *A Gauth* is negligible. We have excluded *A* from interacting with the tag *T* from the second step because this seems to correspond to reality: if *A* were allowed to interact with *T* as a reader *R* during this step, and then simply relay faithfully the conversation between T and R0 to an authorised reader *R* in order to get authenticated as *T* (without mounting any attack). This is the online man-in-the middle attack described above in Untraceability is a weak notion of anonymity. In the second step of the tracing game *Gtrace; A* must trace some tag *T*: *A* is given access to (i.e. ability to interact with) a challenge tag $T*$ and must tell whether $T*$, is *T* or not, better than guessing. In this tracing step, *A* is also allowed to interact with all tags and readers, in particular, interacting with *T*. The advantage adv *A Gtrace* of the adversary in this game is

Untraceability:

Is a weak notion of anonymity. In the second step of the tracing game *Gtrace*, *A* must trace some tag *T*: *A* is given access to (i.e. ability to interact with) a challenge tag $T*$ and must tell whether $T*$, is *T* or not, better than guessing. In this tracing step, *A* is also allowed to interact with all tags and readers, in particular, interacting with *T*. The advantage *advA Gauth* of the adversary in this game is |*Prob*[*A correct*]− 1 2

|, where *Prob*[*A correct*] = *Prob*[*A* = *yes*|*T* = *T′*] + *Prob*[*A* = *no*|*T* □= *T′*] and we require that *Prob*[*T* = *T′*] = 1

2. We have
untraceability if *advA*
Gtrace
is negligible.

Unlinkability:

Is a strong notion of anonymity, which is the one we use in this paper. For anonymity we require that the advantage adv A *Ganon* of the adversary in the second step of *Ganon* in linking two different interactions to the same tag is negligible. The setting for *Ganon* is the same as in *Gtrace*, except that in *Gtrace* the adversary already knows *T* through other interactions in the first step. In *Ganon* both *T* and *T* are challenge tags. Through interacting with *T* and $T*$,as well as all other normal tags and readers, *A* must tell whether it is interacting with identical tags or not, i.e. whether *T* and $T*$ have the same key $K \in K$ or not..

Availability:

In *Gavail* the adversary *A* must prevent a tag *T* from being authenticated by a reader *R* in a challenge session *ses*, without interacting with this session *ses*. In this attack, *A* is allowed to interact with all tags and all readers, except of course for the session *ses*. The advantage*adv A Ganon* of *A* in this game is the probability that *R* rejects *T* in the challenge session *ses*. For completeness of an authentication protocol *P*, we explicitly require that: for all authorized tags *T* and readers *R*, *P* accepts with overwhelming probability. We note that this is implied implicitly in the availability game *Gavail*.

OPERATIONAL AND CRYPTOGRAPHIC PROPERTIES OF RFID SYSTEM

In this section, we summarize some essential operational and cryptographic properties for general RFID systems.

Scalability*:*

If the computational workload of an authentication protocol increases linearly as the number of the tags, the system is not scalable. Noting that most RFID applications should accommodate a large number of tags, e.g. a large library may have millions of books and each book should have a tag, the scalability is a critical property in RFID systems.

Anti-cloning*:*

Since a large number of tags will be spread out in the RFID applications, an attacker may be able to capture a tag, investigate it by microscope probing [11], learn all the information in the tag, and make a counterfeit. However, an attacker should not be able to forge other tags except the cracked one. If a group of tags share secret information and a reader authenticates tags by the shared secret, it will be

possible to clone some other tags with the learned secret. This will also cause the tracking problem since an attacker can decrypt the exchanged messages. Therefore, the secret information on a tag should be pertinent to the tag so that the other tags except the cracked one are still secure. One possible way to protect the secret stored in a tag is to use a secure memory [10]. However, it is not practical to store a long-term secret (a group key, shared secret among a group of tags and readers) in tags and to use it for authentication since only single cracked tag may endanger all the tags and readers having the shared secret. In this paper, assuming that an attacker is able to crack and reveal the secret in a tag, we define an RFID system secured against the cloning attack as long as the secret of a tag is pertinent to the tag and secured from passive or active skimming attacks.

Anonymity*:*

RFID tags are supposed to respond with some message whenever they receive a query message from a reader. If the responses are fixed or predictable by an attacker, it results in a privacy problem. An attacker is possibly able to track a tag, and hence its owner too, and collect data for malicious purpose. Therefore, the responses of tags should be randomized so that it is infeasible to extract any information in communications between a tag and a reader. Some of the proposed authentication protocols use hash algorithms and/or symmetric key algorithms due to their simplicity compared to public-key algorithms. However, they fail to satisfy the mentioned basic requirements of RFID systems.
This is consequential noting the proof in, where it is shown that a public-key cryptographic algorithm is necessary to satisfy the required properties. Some other propose to adopt well-known public-key based authentication protocols such as the Schnorr protocol and the Okamoto protocol , which are suitable for general authentication systems that do not concern anonymity but not for RFID systems.

CONCLUSION

In this research we have discussed about various important security problems and the cryptographic properties of RFID System.It is astonishing how a modest device like an RFID tag,essentially just a wireless license plate, can give rise to the complex mélange of security and privacy problems that we explore here. RFID privacy and security are stimulating research areas that involve rich interplay among many disciplines, like signal processing, hardware design, supply-chain logistics, privacy rights, and cryptography. The majority of the articles treated in this survey explore security and privacy as a matter between RFID tags and readers. Of course, tags and readers lie at the fringes of a full-blown RFID system. At the heart will reside a massive infrastructure of servers and software. Many of the attendant data-security problems like that of authenticating readers to servers involve already familiar data-security protocols. But the very massive scale of RFID-related data flows and cross-organizational information sharing will introduce new data-security problems. We have mentioned key-management and PIN distribution for tags as one such potential problem. Other challenges will arise from the fluidity of changes in tag ownership. Sensors are small hardware devices similar in flavor to RFID tags. While RFID tags emit identifiers, sensors emit information about their environments, like ambient temperature or humidity. Sensors typically contain batteries, and are thus larger and more expensive than passive RFID tags.

Between active RFID tags and sensors, however, there is little difference but nomenclature. For example, some commercially available active RFID devices are designed to secure port containers.They emit identifiers, but also sense whether or not a container has been opened. Given such examples, there is surprisingly little overlap between the literature on sensor security and that on RFID security. The boundaries between wireless-device types will inevitably blur, as evidenced by the dual role of reader and tag played by NFC devices. Another important aspect of RFID security that of user perception of security and privacy in RFID systems. As users cannot see RF emissions, they form their impressions based on physical cues and industry explanations. RFID will come to secure ever more varied forms of physical access and logical access. To engineer usable RFID systems and permit informed policy decisions, it is important to understand how RFID and people mix.

REFERENCES

[1]. ”Specification of RFID Air Interface”, http://www.epcglobaline.org.

[2]. A Juels and S A Weis Authenticating pervasive devices with human protocols. In V. Shoup, editor, Advances in Cryptology: Proceedings of CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pages 293 308. Springer-Verlag, 2005.

[3]. P. Tuyls and L. Batina RFID-tags for Anti-Counterfeiting. In D. Pointcheval, editor, Topics in Cryptology - CT-RSA 2006, Lecture Notes in Computer Science, San Jose, USA, February 13-17 2006. Springer Verlag.

[4]. C. Kocher, J. Jaffe and B. June. Differential Power Analysis, CRYPTO99

[5]. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, Cryptographic Hardware and Embedded Systems, CHES 2004, volume LNCS 3156, pages 357-370. Springer, 2004.

[6]. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels” Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, in the First International Conference on Security in Pervasive Computing SPC 2003, March 2003.

[7]. Gildas Avoine and Philippe Oechslin” A Scalable and Provably Secure Hash-Based RFID Protocol”, the 2nd IEEE International Workshop on Pervasive Computing and Communication Security Persec 2005, March 2005.

[8]. Xingxin Grace Gao, Zhe Xiang, Hao Wang, Jun Shen, Jian Huang and Song Song” An Approach to Security and Privacy of RFID System for Supply Chain”, Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East04), 2004.

[9]. Martin Feldhofer Martin Feldhofer, An Authentication Protocol in a Security Layer for RFID Smart Tags, IEEE MELECON 2004, May 2004.

[10]. M. Neve, E. Peeters, D. Samyde and J. Quisquater. Memories” A Survey of their Secure Uses in Smart Cards.

The 2nd International IEEE Security In Storage Workshop (IEEE SISW03), pages 62-72, Washington DC, USA, 2003.

[11]. R. Anderson and M. Kuhn. ”Low Cost Attacks on Tamper Resistant Devices”, Proceedings of the 5th International Workshop on Security Protocols, volume 1361 of LNCS, pages 125-136. Springer Verlag, 1997.

