International Journal of Science Engineering and Advance Technology

Wireless Protocols for Anti Cloning and Security

Saurabh Gupta[1], Dr. R. K. Singh[2] & Dr. K. B. Singh[3]

Research Scholar - Department of Information Technology, MIT Muzaffarpur, India

Head – Department of Physics, G. P. Darbhanga, India

Head- Department of Information Technology, MIT, Muzaffarpur, India

saurabhg.mit@gmail.com , kbsphysics@yahoo.co.in

***Abstract* - RFID system (Radio-Frequency Identification) is a technology for automated identification of objects and people. Human beings are smart enough to identify an object under a variety of challenge circumstances. RFID systems are emerging as one of the most pervasive computing technologies. But there are still a large number of problems that are to be addressed. One of the fundamental issues still to be addressed is privacy, which concludes association threat, location threat, preference threat, constellation threat, transaction threat, action threat and breadcrumb threat (Kim, J., Yang, C, Jeon, J,2007). Misbehaviours of both readers and tags will lead to attacks to the system. The common attacks on the readers, tags and the air interface between them comprise: Tracking or Tracing, Tamper, Clandestine Scanning, Counterfeit Tags, Cloning Tags, Eavesdropping, Replay, man-in-the-middle attack, Spoofing, Differential power analysis, Timing Attacks, Denial of Service, Physical Attacking and so on (P. Cuenca and L. Orozco-Barbosa, 2006.),(Kim, J., Yang, C, Jeon, J, 2007). Due to scarceness of resources most of the proposed protocols were designed using symmetric key cryptographic algorithms. However, it has been shown that it is inevitable to use public-key cryptographic algorithms to satisfy these requirements.**

A number of mechanisms have been devised to overcome the problems related to security and privacy issue of RFID systems. In this paper we propose three anonymous RFID authentication protocols and prove that they are secure in the traditional cryptographic framework. Our model allows most of the threats that apply to RFIDs systems including, denial of service, impersonation, malicious traceability, information leakage through power analysis and active man-in-the middle attacks. Our protocols are efficient and scalable.

***Keywords* - RFID, Authentication, Privacy, Scalability, Counterfeiting, Cloning.**

I. INTRODUCTION

RFID (Radio-Frequency IDentification) is a technology for automated identification of objects and people. Human beings are skillful at identifying objects under a variety of challenge circumstances. RFID may be viewed as a means of explicitly labelling objects to facilitate their "perception" by computing devices. An RFID device – frequently just called an RFID tag – is a small microchip designed for wireless data transmission. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. The microchip itself can be as small as a grain of sand, some 0.4mm2 [1]. An RFID tag transmits data over the air in response to interrogation by an RFID reader. Today, large organizations, such as Wal-Mart, Procter and Gamble, and the United States Department of Defense are deploying RFID as a tool for automated oversight of their supply chains. Thanks to a combination of dropping tag costs and vigorous RFID standardization, we are on the brink of an explosion in RFID use.

RFID is supposed to be the successor of the optical barcode printed on consumer products, with two individual advantages:

i. Unique identification: A barcode indicates the type of object on which it is printed, e.g., "This is a 50 grams bar of XYZ brand 70% chocolate." An RFID tag goes a step ahead. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that "This is 50 grams bar of XYZ brand 70% chocolate, serial no. 887891873." The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items.

ii. Automation: Barcodes, being optically scanned, require line-of-sight contact with readers, and thus watchful physical positioning of scanned objects. Except in the most rigorously controlled environments, barcode scanning requires human intervention. In contrast, RFID tags are readable without line-of-sight contact and without precise positioning. RFID readers can scan tags at rates of hundreds per second. For example, an RFID reader by a warehouse dock door can today scan stacks of passing crates with high accuracy. In the future, point-of-sale terminals may be able to scan all of the items in passing shopping carts [2].

The main form of barcode-type RFID device is known as an EPC (Electronic Product Code) tag. An organization known as EPCglobal Inc. [3] oversees the development of

the standards for these tags. Not surprisingly, EPCglobal is a joint venture of the UCC and EAN, the bodies that regulate barcode use in the United States and the rest of the world respectively. EPC tags cost and RFID readers cost are dropping drastically [4].

In general, small and inexpensive RFID tags are *passive*. They have no on-board power source; they derive their transmission power from the signal of an interrogating reader. Passive tags can operate in any of a number of different frequency bands. LF (Low-Frequency) tags, which operate in the 124 kHz – 135 kHz range, have nominal read ranges of up to half a meter. HF (High-Frequency) tags, operating at 13.56 MHz, have ranges up to a meter or more (but typically on the order of tens of centimetres). UHF tags (Ultra High-Frequency), which operate at frequencies of 860 MHz – 960 MHz (and sometimes 2.45GHz), have the longest range – up to tens of meters. UHF tags, though, are subject to more ambient interference than lower-frequency types. In this paper, we enumerate the major standards for passive RFID devices. Some RFID tags contain batteries. There are two such types: *semi-passive* tags, whose batteries power their circuitry when they are interrogated, and *active* tags, whose batteries power their transmissions. Active tags can initiate communication, and have read ranges of 100m or more. Naturally, they are bit expensive.

II. RFID TODAY AND TOMORROW

Many of us already use RFID tags routinely. Examples include:

- Proximity cards, that is, the contactless cards used for building access.
- Automated toll-payment transponders – the small plaques mounted in automobile windshields. (These are usually semi-passive).
- The ignition keys of many millions of automobiles, which include RFID tags as a theft-deterrent.
- Payment tokens: In the United States, the SpeedPass™ token for petrol station payments is an example. Contact-less credit-cards, like American Express ExpressPay™ and the Mastercard PayPass™ use RFID.

Millions of house pets around the world have RFID tags implanted in their bodies, to facilitate return to their owners should they become lost.

In the world of the future – amazing things would be possible. Here are a few possibilities that the reader might dream up:

- **Smart appliances:** By exploiting RFID tags in garments and packages of food, home appliances could operate more cleverly. Washing machines might select wash cycles automatically, for instance, to avoid damage to delicate fabrics. Your refrigerator might warn you when the milk has expired or you have only one remaining carton of yogurt – and could even transmit a shopping list automatically to a home delivery service [5].
- **Shopping:** In retail shops, consumers could check out by rolling shopping carts past point-of-sale terminals. These terminals would automatically tally the items, compute the total cost, and perhaps even charge the consumers' RFID-enabled payment devices and transmit receipts to their mobile phones. Consumers could return items without receipts. RFID tags would act as indices into database payment records, and help retailers track the pedigrees of defective or contaminated items.
- **Interactive objects:** Consumers could interact with RFID-tagged objects through their mobile phones. (Some mobile phones already have RFID readers.) A consumer could scan a movie poster to display show times on her phone. She could obtain manufacturer information on a piece of furniture she likes by waving her phone over it.
- **Medication compliance:** Research at Intel and the University of Washington [6] exploits RFID to facilitate medication compliance and home navigation for the elderly and cognitively impaired. As researchers have demonstrated, for example, an RFID-enabled medicine cabinet could help verify that medications are taken in a timely fashion. More generally, RFID promises to bring tremendous benefits to hospitals [7].

But what, really, is "RFID"?

We have discussed the basics of RFID and laid out some evocative scenarios. Yet we have not formally defined the term "RFID." A wholly satisfying definition is elusive. ut it is not a mere pedantic exercise: The definition of RFID can have an important impact on technical and policy discussion [8]. In this paper, we use "RFID" to denote any RF device whose main function is identification of an object or person. At the rudimentary end of the functional spectrum, this definition excludes simple devices like retail inventory tags, which merely indicate their presence and on/off status. It also excludes portable devices like mobile phones, which do more than merely identify themselves or their bearers. A broad definition for "RFID" is appropriate because the technical capabilities and distinctions among RF devices will drift over time, and the privacy and authentication concerns that we highlight in this paper apply broadly to RF identification devices great and small. Most importantly, though, the names of standards like 'ISO 14443" or "EPC Class-1 Gen-2" do not trip off the tongue or inhere well in the mind.

III. CONCEPTUAL MODELS

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 field: 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 authorised keys (issued by S). Figure 1 illustrates the flow of exchanged data between a tag T and the trusted server S via the reader R, during the authentication of T.

$$\mathbf{T} \leftrightarrow \mathbf{R} \Leftrightarrow \mathbf{S}$$

Figure 1: The authentication flow in an RFID system

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 $R = R^S$, 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 $K \in \mathcal{K}$, that adhere to the protocol, the readers R that adhere to the protocol, and the trusted server.

IV. ATTACKS ON RFID

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:

A. 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 $K \in \mathcal{K}$. 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.

B. Types of Attacks

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 such attacks:

C. Side Channel Attacks (Power Analysis Attacks)

These are attacks in which the private key of a device is extracted by exploiting either its power consumption when inaccurate/accurate received bits are processed or the variations in the timing of its energy output. This is the idea of simple and differential power analysis was first introduced by Kocher [9]. This is a serious threat. Thus implementers need algorithms that are not only efficient but also SCA registrant.

D. Online Man-in-the-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.

E. Online Man-in-the-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).

V. SECURITY IN RFID

The security of an RFID protocol can be described in terms of three games, an authentication game G_{auth}, an anonymity game G_{anon}, G_{anon}, a tracing game G_{trace} and an

availability game G_{avail}, 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: G_{auth}, G_{trace}, G_{anon} and G_{avail}.

A. 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 [10], 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. [10] 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 [11]. This scheme used a cryptanalytic method. However, this method also causes some other problems. Since this protocol uses time-memory trade-off method [11], 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 [12] [13] 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 [14] uses a symmetric key encryption algorithm which is unsuitable in low-cost RFID systems.

In the second step of G_{auth}, 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 G_{auth} is the probability that A succeeds in authenticating itself to R. An RFID protocol is a secure authentication protocol if adv A G_{auth} 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 R‘ 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 G_{trace}, 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. This is the advantage adv A G_{trace} of the adversary in this game.

B. Untraceability

Untraceability is a weak notion of anonymity. In the second step of the tracing game G_{trace}, 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 G_{auth} of the adversary in this game is $|\text{Prob}[\text{A correct}] - ½|$,

where $\text{Prob}[\text{A correct}] = \text{Prob}[\text{A} = \text{yes}|\text{T} = \text{T‘}] + \text{Prob}[\text{A} = \text{no}|\text{T} \neq \text{T‘}]$ and we require that $\text{Prob}[\text{T} = \text{T‘}] = ½$.

We have untraceability if advA G_{trace} is negligible.

C. Unlinkability

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 G_{anon} of the adversary in the second step of G_{anon} in linking two different interactions to the same tag is negligible. The setting for G_{anon} is the same as in G_{trace}, except that in G_{trace} the adversary already knows T through other interactions in the first step. In G_{anon} 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 $K \in \kappa$ or not.

D. Availability

In G_{avail} 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 G_{anon} 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 G_{avail}.

VI. RFID MODELS TO DEAL WITH COUNTERFEITING AND ATTACKS

In order to protect a product against cloning (counterfeiting) a detection mark is embedded into the product or its packaging. This detection mark consists of a physical and a digital part. The mark is put there by a legitimate authority. The attacker (counterfeiter) has access to all components of this detection mark; i.e. she can read it, remove it from the product and investigate it. Based on the information that she obtained from investigating the legal detection mark, she produces a fake detection mark. The goal of the attacker is to produce a fake detection mark that can only with small probability be distinguished from an authentic one.

A. Components of Anti-Counterfeiting Technology

In order to protect a product against counterfeiting, technological means are needed to verify whether the product is authentic or not. In order to make an item unclonable, the following two components are needed.

Physical protection. This is obtained by using unclonable physical structures embedded in the package (removal of the structure leads to its destruction). One or more unique fingerprints derived from the physical structure will be printed on the product for the verification of the authenticity of the product.

Cryptographic protection is serving two goals. Firstly, cryptography provides techniques (digital signatures) to detect and prevent tampering with data (fingerprints) derived from a physical object. Secondly, it provides secure identification protocols to identify a product. Those protocols do not leak any necessary identification information to an eavesdropper attacking (actively or passively) the communication channel.

Good candidates for uncolnable physical structures that can be used for physical protection purposes, are so-called Physical Unclonable Functions (PUFs) [15].

B. General Anti-Counterfeiting Protocol

We give intuition for protocols that can be used to check the authenticity of a product based on embedding a PUF in the product in combination with the use of cryptographic techniques.

First there is an enrollment phase, which is performed by some trusted authority. During this phase the following steps are performed.

i. Several fingerprints are derived from the PUF by challenging it with multiple challenges and recording the responses. These responses are then turned into binary fingerprints (and some auxiliary data are derived for use during the verification phase).

ii. These challenges, fingerprints and auxiliary data are then signed with the secret key *sk* of the issuer of the product (the issuer is assumed to be trustworthy).

iii. The signatures, the challenges (corresponding to the fingerprints) and may be some auxiliary data (needed to perform processing during the authentication phase) are also printed on the product (and/or stored in a database).

During the verification phase, the authenticity is checked by running the following protocol.

i. The verification device reads the challenges and auxiliary data.

ii. The verification device challenges the physical structure with one of the challenges printed on the product. After having measured the responses, it derives the fingerprint from the response based on the auxiliary data.

iii. Then, using the fingerprint derived in step 2, the verification device checks the signature to verify that the fingerprint, challenges and auxiliary data were printed on the product by a legitimate authority. If the signature is not correct, the product is not authentic.

We briefly analyze the security of this protocol. An attacker who wants to counterfeit the product has to embed a fake physical structure on the product that produces correct fingerprints to the challenges (with correct signatures). Under the assumption that the physical structure is unclonable, she cannot produce a clone of the originally embedded physical structure. More precisely, we assume that given some challenges c_1 …., c_n and corresponding fingerprints s_1….,s_n she cannot produce a

(fake) physical structure that produces the same fingerprints s_1…., s_n given the original challenges c_1…., c_n. On the other hand she can produce another structure and create challenges, auxiliary data and fingerprints s'_1…., s'_n according to the procedures used during enrollment. However, since she does not know the secret key *sk* and the responses of her fake structure will be different with very high probability, she will not be able to put the correct signatures on these data. The verification device will detect that the signatures are not correct and reject this as a fake product. We note that the number of fingerprints that can be verified during a verification session is very limited by time and space constraints. Furthermore, the attacker can easily capture the required fingerprints (by measuring the responses according to the challenges printed on the product). Therefore the production of a clone only requires the fabrication of a physical structure (PUF) producing the same fingerprints for a limited number of challenges.

The PUF based solution for preventing counterfeiting of goods that was presented above can be improved with active components, that are inseparably linked with a PUF. An example consists of an RFID-tag equipped with a microchip that is inseparably bound to a PUF. Because of the presence of a microchip a secure identification protocol can be run without revealing any information on the fingerprint of the PUF. Additionally, by inseparably linking the chip and the PUF, it becomes possible to prevent leakage of the PUF measurement to the outside world.

Typical RFID systems consist of the following two components: the *RFID-tag* and a *reader*. The reader will perform the verification to detect whether a tag is authentic or not. The RFID-tag consists of an antenna connected to a microchip that can store and read data and has possibly some dedicated hardware to perform a small amount of computations. Typically, the power for performing operations is obtained from the RF-field (by inductive coupling). A reader can read and write data from/on a tag. The reader is often linked with some system that can perform computations on the data that it receives from tags.

In order to use RFID-tags for anti-counterfeiting purposes, we proceed as follows. An RFID-tag containing reference information is embedded in a product. The (identification) data stored in the memory of the tag is signed with the secret key *sk* of the legitimate issuer. The tag communicates with a reader for verification purposes over a public channel. The ROM memory of the tag is accessible to the attacker. The reader has a certified public key *pk* corresponding the issuer's secret key for verification of the digital signatures.

C. Power Analysis Attacks

Our RFID authentication protocols in the next section are designed to deal with power analysis attacks and offline man-in-the middle active attacks. For the online man-in-the middle attacks an \out-of-system" solution should be sought.

In this section we propose three RFID authentication protocols, a 2-pass authentication protocol and two 1-pass authentication protocols. The last protocol is optimistic, in the sense that its cost is low when the adversary is passive. We shall prove that these are secure using our security model, and that the tags are untraceable. These protocols address most of the drawbacks of the authentication protocols in [16, 17, 19, 18, 20], and will also thwart power analysis attacks. Our first protocol is an extension of YA-TRAP proposed by G. Tsudik [19] which we briefly describe below.

i. YA-TRAP [Yet Another Trivial Authentication Protocol]

For this protocol, the timeline is divided into small periods, during which each tag is allowed to be authenticated at most once. The readers and the server maintain a (loosely) synchronized timestamp t_{sys}. The tags do not have clocks. Each tag T is equipped with a pseudo-random number generator (which may be resolved as an iterated keyed hash function), and is initialized with a private key K and timestamps t_0 and t_{max}, κ is the set of all keys that have been issued to tags.

When a reader R activates tag T, it broadcasts the current timestamp t_{sys}. If $t_{sys} <= t_{tag}$, where t_{tag} was the last timestamp that T received, or if $t_{sys} > t_{max}$, then T broadcasts a pseudorandom string; otherwise T broadcasts $h = H_K(t_{sys})$, and sets $t_{tag} = t_{sys}$. Here $H_K(t_{sys})$ is the hash of t_{sys} with key K, and t_{tag} is initialized with the value t_0.

The server S finds the value of the key that T has used in h from a hash look-up table - see Figure 2. In this table, whenever a timestamp t_s is updated, the server computes the keyd hash values $H_K(t_s)$ for all keys $K \in \kappa$, and get the next row of the table. This table, $\{h_{i;j} = H_{Ki}(j)\}$, makes it possible for the server S to find out whether the tag T that issued the hash h is authentic, $h = h_{tsys;j}$ for some $j \in [1, n]$, without having to search exhaustively for the key each time a new tag is challenged during time period t_s (typically one or a few minutes).

	K_1	K_2	⋯	K_n
$t_s = 1$	$h_{1,1}$	$h_{1,2}$	⋯	$h_{1,n}$
$t_s = 2$	$h_{2,1}$	$h_{2,2}$	⋯	$h_{2,n}$
⋮	⋮	⋮	⋯	⋮
$t_s = i$	$h_{i,1}$	$h_{i,2}$	⋯	$h_{i,n}$

Figure 2: The hash look-up table.

Tsudik points out [19] that there is a drawback in YA-TRAP: the adversary can send a wildly inaccurate timestamp t'_{sys} (say the maximum timestamp allowed) and incapacitate the tag. This is a DoS attack which will kill the tag. It quite is difficult to address this attack since the tag T needs to update its time t_{tag} regardless of the value of the time t'_{sys} sent by adversary, otherwise its identity will be traced by sending the same t'_{sys} every time. To avoid tracing, it is not sufficient to randomize the tag's response since that would eliminate the savings that the server gets from using the look-up table.

There is also a "future-time" attack in which the adversary queries the tag offline with several valid time periods $t_{sys;\,i}$, i = 1, 2 , , , . .. The adversary then captures the tag's responses and can use that for online authentication when these time periods. Therefore, by using a predictable time value as a challenge for the tag will not work. In the following section we show who to deal with these attacks while keeping the server scalable by adapting the protocol YA-TRAP.

ii. *A 2-Pass Optimistic Anonymous RFID Authentication Protocol*

YA-TRAP is (essentially) a 1-pass protocol, in the sense that the timestamp is broadcast (not unicast) by R to all tags in range. We now show that how to extend YA-TRAP to deal with the DoS attack in which the adversary disables the tag T by sending an inaccurate timestamp.

The protocol we propose is essentially a 1-pass authentication protocol with an optional pass. In the first step the tag is authenticated, whereas in the second step the server authenticates the timestamp. The protocol is given in Figure 3.

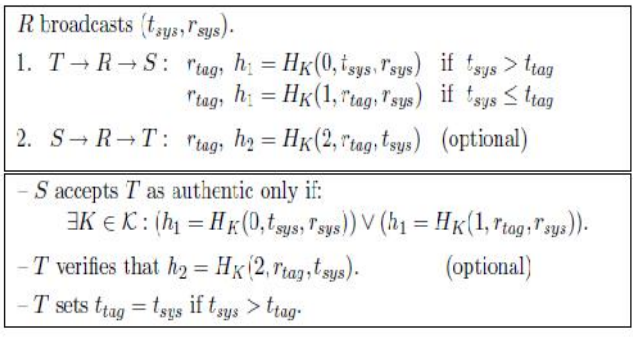

Figure 3: A 2-Pass optimistic anonymous RFID authentication protocol

In our protocol the tag T, instead of sending a pseudo-random string when the timestamp it gets is out of its bounds, it sends a keyd hash of the string (1, T_{tag} , t_{sys}). This will save the tag T, but now the server S must work harder. More specifically, if the hash value h is not in the look-up table (see Figure 2), then the server must search exhaustively for the key K. Of course, this only happens with tags that the adversary has tried to kill (or incapacitate).

Our approach is to shift the adversary's attack from the low complexity tags to the server. This approach is optimistic, in the sense that when the adversary is passive than the server need only use the look-up table. Note that pass 2 is optional. This pass is only used by the server during time periods when a number of attacks occur beyond a certain threshold and the server would like to resynchronize the time t_{sys} to all the tags so that their stored time t_{tag} is valid.

This is applied to all tags during such time periods so that no identity information are revealed. When this period passes, the server could return to normal operation and will bypass pass 2. This makes the scheme resistant to DoS while being almost as efficient as [19].

iii. *A 1-Pass Optimistic Anonymous RFID Authentication* protocol

keys	K_1	K_2	...	K_n
strings	r_{K_1}	r_{K_2}	...	r_{K_n}

Figure 4: A look-up string table.

This protocol uses a key lookup table in which the keys K are linked to session number T_K, see Figure 4. The optimistic protocol is described in Figure 5 and is only one pass.

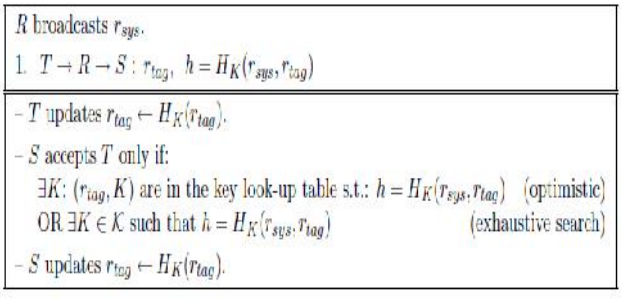

Figure 5: A 1-Pass anonymous RFID authentication protocol

The protocol described in Figure 5 always uses only one pass. When a tag has been attacked, its pseudo random value T_{tag} will be out-of-sync with its counterpart s_K stored in the server. At this time, the server will have to search for all keys to find the correct one and then resynchronize s_K. Even

when this happens, the scheme has the advantage that the server only needs to do extra computation for tags that are authenticated, not for all the tags. When no fault occurs, the server simply has to do one lookup and hashing for each authenticating tag. So computation is saved on tags that do not communicate.

In the non-optimistic version of this protocol, the tag and server uses true random T_{tag} and therefore the server needs to search and udpate its value for any tag that requires authentication. This scheme is suitable for cases where the number of active tags is smaller than the number of tags.

VII. CONCLUSION

It is astonishing how a modest device like an RFID tag, essentially just a wireless license plate, can give rise to the complex melange 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.

An important aspect of RFID security is 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.

Both the physical cloning attack as well as the cloning attack based on (actively or passively) attacking the protocol between the tag and the reader can be prevented. It has been shown that the required protocols are feasible on an RFID-tag in the offline situation.

REFERENCES

[1] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra Small individual recognition security chip. *IEEE Micro*, 21(6):43–49, 2001.

[2] D. White. NCR: RFID in retail. In S. Garfinkel and B. Rosenberg, editors, RFID: Applications, Security, and Privacy, pages 381–395. Addison-Wesley, 2005.

[3] EPCglobal Web site, 2005. Referenced 2005 at http://www.EPCglobalinc.org.

[4] S. E. Sarma, S. A. Weis, and D.W. Engels. RFID systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[5] Merloni unveils RFID appliances. RFID Journal, 4 April 2003. Referenced 2005 at http://www.rfidjournal.com/article/articleview/369/1/1/.

[6] K. P. Fishkin, M. Wang, and G. Borriello. A ubiquitous system for medication monitoring. In Pervasive 2004, 2004. Available as 'A Flexible, Low-Overhead Ubiquitous System for Medication Monitoring, Intel Research Seattle Technical Memo IRS-TR-03-011,25 October 2003.

[7] K. Fishkin and J. Lundell. RFID in healthcare. In S. Garfinkel and B. Rosenberg, editors, RFID: Applications, Security, and Privacy, pages 211–228. Addison-Wesley, 2005.

[8] M. Baard. RFID invades the capital. Wired News, 7 March 2005. Referenced 2005 at http://www.wired.com/news/privacy/0,1848,66801,00.html.

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

[10] 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.

[11] 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.

[12] 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.

[13] Xingxin Grace Gao, Zhe Xiang, HaoWang, 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.

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

[15] P. Tuyls, B. Skoric, S. Stallinga, A.H.M. Akkermans, and W. Ophey. Information theoretical security analysis of physical unclonable functions. In A.S. Patrick and M. Yung, editors, Proceedings of 9th Financial Cryptography and Data Security Conference, volume 3570 of Lecture Notes in Computer Science, pages 141{155. Springer-Verlag, 2005.

[16] D. Johnson and A. Menezes. The elliptic curve digital signature algorithm (ECDSA). Technical Report CORR 99-34, Department of Combinatorics & Optimization, University of Waterloo, Canada, February 24 2000. http://www.cacr.math.uwaterloo.ca.

[17] M. Joye and S.-M. Yen. The montgomery powering ladder. In B. S. Kaliski Jr., CK. Kove, and C. Paar, editors, Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), number 2523 in Lecture Notes in Computer Science, pages 291{302. Springer-Verlag, 2002.

[18] A. Juels. Strengthening EPC Tags against Cloning. March 2005. manuscript.

[19] A. Menezes, P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[20] P. Montgomery. Speeding the pollard and elliptic curve methods of factorization. Mathematics of Computation, Vol. 48:243{264, 1987.