Cataloging RFID Privacy and Security

Marcel Queisser, Florian Dautermann, Pablo Guerrero, Mariano Cilia, Alejandro Buchmann*
Databases and Distributed Systems Group
{queisser, dauterma}@rbg.informatik.tu-darmstadt.de, {guerrero, cilia, buchmann}@dvs1.informatik.tu-darmstadt.de
* GK Enabling Technologies for Electronic Commerce
Dept. of Computer Science, TU Darmstadt, Hochschulstr. 10, 64289, Germany

Abstract

Due to recommendations from government agencies such as the U.S. Department of Defense or the Food and Drug Administration, mandates from private sector companies such as WalMart, Metro or Tesco, and even visions such as that of the *Internet of Things*, Radio Frequency Identification (RFID) technologies have gained great thrust. The widespread realization of existing and envisioned applications, however, requires researchers, developers and adopters to carefully consider the way these technologies will be applied.
In this paper we inspect the current research on two quality attributes that greatly impact all actors of the RFID ecosystem: *privacy* and *security*. In order to ensure an appropriate quality of service, these aspects are tackled throughout the protocol stack linking tags and readers. We explore different mechanisms and catalog them in each of these layers, discerning the attacks faced and providing technical insight on the proposed alternatives.

1 Introduction

Radio Frequency Identification (RFID) technologies are proving they are a better way to do things in many areas. On one hand, for instance, its usage in supply chain management benefits many industries by increasing the visibility and accuracy of the shipment data [3]. In industrial automation, it helps to reduce overhead and errors associated with moving items through the manufacturing steps [2]. In human activity detection, it is used to infer people's current behavior and their actions as an implicit input for computer systems. On the other hand, however, all these applications made privacy and security concerns emerge. Final users and consumer rights groups argue against possible tracking and profiling of individuals. From a company's perspective, fear is whether others could steal sensible operational information.
In this paper we bring different research proposals on privacy and security together by exploring the communication *link* between the two characteristic RFID elements: *tags* and *readers*. Tags contain an antenna, a silicon chip with a receiver, a modulator, control logic and memory, whilst readers are devices able to recognize the presence of RFID tags and read the information stored on them. A tag that communicates with every reader is called *promiscuous*, while one that needs some kind of authentication, e.g. via password, is called *secure*.
The communication in this link can be divided into three layers[1] as depicted in Figure 1. First, the *Application Layer* deals with user-defined information, e.g. information about the tagged object or an (unique) identifier. Second, the *Communication Layer* specifies how reader and tag communicate, e.g., which mechanisms are used to isolate a specific tag and to avoid collisions, etc. Finally, the *Physical Layer* defines the rules for the communication such as frequency (which varies according to its use and region), data encoding, modulation etc.

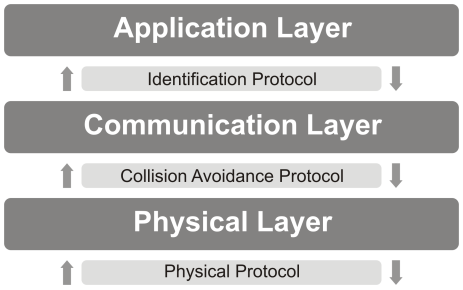

Figure 1 Layers of an RFID System

2 Privacy and Security Techniques

In order to gain the user's acceptance, RFID systems have to be trustworthy. There are two major problems which have to be considered:

- *Information Leakage.* Occurs if an unauthorized person or reader is able to obtain any information about the tagged item by reading the tag. A system in which Information Leakage is impossible will be called *secure*.
- *Traceability.* Occurs if an unauthorized person or reader is able to link two sightings of the same tag. A system which grants Non-Traceability will be called *privacy protecting*.

In this paper we use a bottom-up approach to outline some techniques (grouped by the layers in which they are applied) and to analyze their benefits and drawbacks.

2.1 Physical Layer

Privacy and Security techniques addressing the physical layer have to address the tags and readers. It is either possible to change the layout of the devices or to protect the contained data from retrieval.

2.1.1 Erasing the RFID Tag Contents

Tag owners can be traced by comparing scanned RFID tag data [10]. This can be avoided by simply 'killing' the tag, which means destroying the tag by disconnecting the antenna and/or destroying the rectification circuit. Although this resolves all privacy and security concerns, it prevents many benefits for the customer [6]. Reducing the contained RFID data to the product information is not an option since it is still possible to violate the privacy by examining the types of products someone carries.

2.1.2 Privacy-Protecting Tag

A simple way to protect the privacy of tag owners is to reduce the size of the antenna, thus reducing the read range of a tag, while granting full functionality in close proximity. IBM proposed such an architecture of tags with an alterable antenna size [7]. This altering could be done by scratching off printed conduit that links two parts of the antenna or by stripping off a part of the antenna at a built-in perforation line. With this method, the read range can be reduced from a few meters down to 2.5 to 5 centimeters. Even with highly amplified readers, the read range would not exceed about 15 centimeters according to estimations. This is a significant improvement to consumer privacy and information security because the tag owner can control access to the tag by not letting anyone near the tags. It also results in increased production costs and inconvenience for customers because they need to scratch off the antenna from every product carrying a tag.

2.2 Communication Layer

Communication between RFID devices is always wireless. Therefore it is vulnerable to eavesdropping and tracing. In order to protect wireless communication it has to be encrypted. However, the session keys have to be predefined, which usually requires devices with some amount of memory or the key exchange has to be done using an open channel. In the following we will present some techniques which can provide secure communication without the need of predefined communication keys and methods to prevent tracing devices using open communication sessions.

2.2.1 Singulation Protection

Singulation is needed to guarantee the undisturbed communication between a reader and many tags in its proximity. The reader and the tags agree on dividing the radio band by means of time division (TDMA). Singulation methods can be either deterministic or probabilistic.

- *Deterministic approach:* when the reader questions the tags they respond with a generated, random ID. They keep this ID during the whole singulation session. The reader starts by questioning all tags with a certain prefix in their ID. If only one tag responds, a slot is assigned, if two or more tags respond, the prefix is increased. With this method the singulation is finished after a deterministic time.
- *Probabilistic approach:* again, the tags choose a random ID. The reader questions all tags at once and assigns timeslots in which to send. Each tag then randomly sends in a timeslot. The reader can detect collisions and after the slots are finished, it sends a list with the IDs which had no collision and the free timeslots. Then, the tags which do not have a slot yet send again in a randomly selected slot. This process is repeated until there is no collision. The algorithm used here is called *Slotted Aloha*.

Due to the algorithms, the identifiers cannot be changed during one singulation session. This gives an attacker the opportunity to trace one specific tag by simulating an open singulation session, i.e. faking a collision every time the tag sends. Therefore both methods pose a threat to privacy. But they can easily be improved by adding a suitable timeout. Tracing is then only possible for the length of this timeout and if the singulation session was not successful after the timeout, a new session can be started.

2.2.2 Noisy Tag

Often, a common secret (session) key is required for secure communication. An approach to exchange those keys proposed in [4] is the Noisy Tag Protocol (NTP). This protocol requires a special tag within the vicinity of the reader, called noisy tag. The reader and this tag share a predefined secret key and a pseudorandom (hash)function h. At the beginning of the key exchange the reader broadcasts some random nonce N which is used by the noisy tag to compute a pseudorandom bitstring h(K,N). There exist three different proposals for the exchange itself, two bit-based protocols and one code-based. We will focus on the code-based protocol, because it eliminates some weaknesses of the bit-based protocols such as the *same-bit problem*. During the exchange-phase of the protocol, the noisy tag sends the pseudorandom bitstring and the tag sends a completely random code. The order in which the noisy tag and the tag send their replies has to be random, which can be achieved by implementing the Carrier Sense Multiple Access (CSMA) protocol. The reader however can filter the bitstring received from the noisy tag and retrieve the code sent by the tag. Now it is possible to generate a secret key by using these secrets. The probability of an attacker to select the code actually sent by the tag is $\frac{1}{2}$. Assuming a number of n rounds, the probability to generate the correct secret is $\frac{1}{2}^n$. The number of rounds necessary to gain a desired level of security can be decreased by increasing the number of noisy tags. The authorization process however is not part of NTP and has to be done by other means.

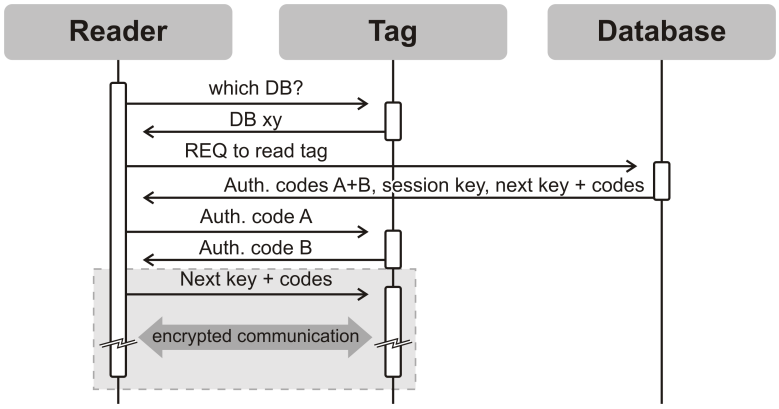

Figure 2 Achieving privacy and security through the usage of multiple shared secrets

2.3 Application Layer

Information Leakage can only be prevented if access to the tag's data is restricted to properly authenticated readers. Usage of tags for access control requires unique IDs of tags and their secure identification in order to prevent spoofing. In the following we will present several approaches to mutual authentication and creation of unique IDs.

2.3.1 MAC Implementation

Message Authentication Codes (MACs) are a very simple approach for secure identification of RFID tags [10]. Each of the so called μ-chips (MAC-equipped RFID chips) has a 128 bit id which is permanently stored on the chip at manufacturing time. This id consists of an encrypted MAC and the chip data. The MAC is created by taking a part (or all) of the chip data, applying a hash function and an encryption with a secret key. This secret key is known to the manufacturer and the clients. The main benefit of this method is a heightened difficulty for the creation of fake tags and eavesdropping. For large deployments, however, there is a high chance that the key gets compromised due to many devices, people and/or institutions knowing it. Moreover, privacy is not provided due to the fact that the μ-chips always send the same id. Another benefit of this approach is the suitability for all kinds of tags, so very cheap, non-reprogrammable chips without much processing power can be used.

2.3.2 PUF Circuits

During the fabrication of integrated circuits (ICs) minor variations occur, which lead to individual characteristics of each IC [10]. ICs which differ from the standard can be used as so-called Physical Unclonable Functions (PUF) circuits. Different PUF circuits do not react in the same way to given challenges. Some hundred of these PUF circuits seem to be enough to distinguish 10^9 chips with a probability $p \approx 1$ to 5×10^{10} by using 800 challenge response pairs. This can be used for RFID chip authentication. A reader queries the tag with a set of some hundred challenges and the tag evaluates these challenges with its PUF circuits. With this method, a unique response is generated and the reader can query the database to identify the tag. A big problem for this is a replay attack, where the attacker records the challenge answers and builds chips, which behave like the PUF circuit equipped chips to this specific challenge set. To counteract that, a list of possible challenges or encrypted communication can be used to deliver the challenges and the responses. PUF circuits function as a hardware decoded secret key for the RFID tag. As long as an attacker cannot replicate a PUF circuit or is able to model the behavior of the PUF circuit, this system is safe. Due to these tasks being difficult ones, the PUF circuit based security is a promising field of research.

2.3.3 Many Shared Secrets

This approach enhances security and privacy especially for chips with small memory and/or poor processing power [10]. Several random numbers, which play the role of authentication keys, are stored in the tag. When a tag is read, the address of a database to contact is obtained. After a successful authentication, the database tells the reader the next authentication code, which is then transmitted to the tag. The tag compares the obtained value with the next value in its memory. It then responds with a corresponding authentication code which is only known to the database and the reader verifies this code. Both the database and the tag now increment a counter to define the next authentication code. Besides the requirement of being online, this technique grants security and privacy protection at the cost of a limited number of readings per tag. A variant to this technique could be realized with reprogrammable tags. Therefore, the database generates a new authentication pair on questioning and transmits it to the reader. After the reader obtains the correct authentication code from the tag it transmits the new codes to the tag. This transmission has to be encrypted. As a result of this, the tag has to be equipped with processing power and a reprogrammable memory but has no reading number restrictions.

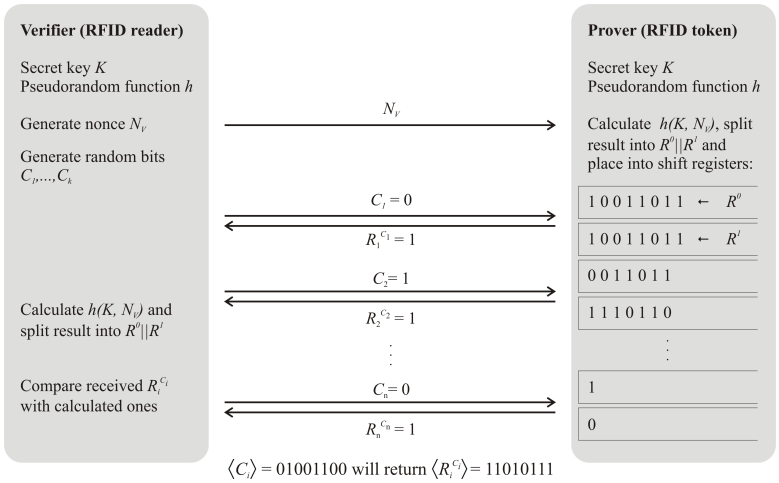

Figure 3 Challenge-response scheme used in the distance-bounding protocol [5]

2.3.4 Distance Bounding

To ensure the proximity of a device the distance bounding protocol can be used [5]. This protocol uses a challenge and response technique for authentication and calculates the distance between the reader and the tag by measuring the round-trip delay. It requires a secret key and a pseudo-random function known to both the reader and the tag. At the start of the protocol the reader generates an unique and unpredictable bitstring, used as a seed for the hash function. Both devices then calculate two bitstrings R^0 and R^1 of length n. After a predefined number of clock cycles the challenge-response exchanges begin. The reader sends one bit challenges C_i to which the tag replies with either R^0 or R^1 depending on the value of C_i. If all the responses are correct and received within a predefined time frame the tag is within proper bounds and access can be granted. Given the scenario of a relay attack, the attacker could accelerate the clock signal for the prover in order to gain the responses in advance by using a guessed challenge. If the guess is correct the response can be delivered to the verifier, otherwise the response has to be guessed. This results in a probability of $\frac{3}{4}$ of replying correctly to a single challenge and a probability of $\frac{3}{4}^n$ of proving all challenges. However this protocol requires a communication channel with high bandwidth which is not provided by existing RFID systems. Another problem is the corruption of challenges or responses due to background noise. Therefore a threshold must be introduced defining the number of false responses which can be received without rejecting authentication.

2.3.5 Trusted Computing

Towards the vision where RFID readers will be ubiquitously deployed even in physically insecure locations, Molnar, Soppera and Wagner have introduced techniques from *Trusted Computing* to improve the security of RFID systems [9]. This requires the reader design to be changed. A trusted reader consists of a *Trusted Platform Module (TPM)*, the *Reader Core*, the *Policy Engine* and the *Consumer Agent*. This design ensures security and privacy of communication even if the reader itself gets compromised. The reader's design consists of three main components as depicted if Figure 3. The *Reader Core* provides the basic reader functionality: it interfaces to the TPM without compromising it, and it can't be modified by applications run on top of it. The *Policy Engine* contains a uses a policy file to grant the reader permission to scan tags and determine the possibilities of the use of the data. It also provides the secrets needed to decrypt information obtained by reading a tag. Finally, the *Consumer Agent* (CA) performs auditing duties, i.e., logs every reading operation (e.g., whether they have been performed or denied). Its log and the policy details can then be transmitted to a controlling organization at regular intervals or on demand. The CA also reports if the configuration of the system gets compromised. This is a flexible design, although no implementations exist that can be used out-of-the-box.

2.3.6 Re-encryption of Tags

RFID tags usually answer to readers by sending their data without verifying the authorization of the reader. To eliminate this security and privacy threat, access to the tag must be controlled. An alternative to this approach is to allow the label to answer with a non-identifying response. One possibility for this is re-encryption [10], meant for rewritable tags. A retailer concatenates the RFID tag data with a random number, encrypts the result and stores it on the tag. The key to this encryption is only known to the retailer. When queried, the tag sends the encrypted data. An authorized RFID reader can decrypt the message and receive the original data and the random number. Later, it can rewrite the RFID data on the tag, again padded with a random number and encrypted with a key. This technique grants all the benefits of having unique IDs on all tagged items without the security issues raised by promiscuous tags, however, the key must be shared with the partners

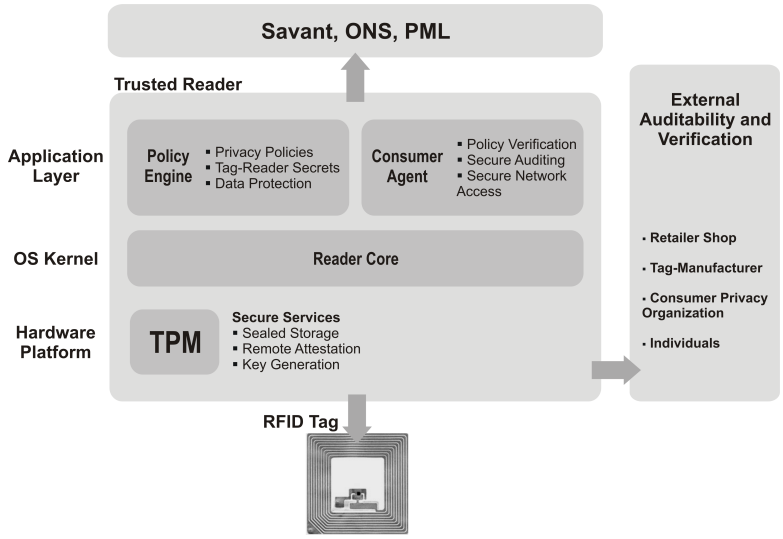

Figure 4 Block Diagram for a Trusted RFID Reader [9]

and be deployed at the readers. This method does not provide privacy protection because it is still possible to trace a tag.

2.3.7 Pseudonym Protocol

The two main problems concerning privacy are the linking of two sightings of a tag and ownership transfer, where only the new owner should be able to read the tag. These problems could be solved by a protocol proposed by Molnar, Soppera and Wagner in [8], which we will describe in this section.
What is new in this protocol is the delegation. A tag generates a pseudonym ID code with its secret key and sends this ID code, which a normal reader (a reader which is not generally allowed to access this specific tag and therefore does not own the secret key) does not understand. The reader passes this ID code to the appropriate trusted center which gives information about the real ID of the tag to the reader if it can authorize itself by well-established cryptographic means towards the trusted center. The trusted center has been given all relevant data about the tag, i.e. the secret key, the ID code, access policies etc., on the rollout of the tag. An authorized reader is able to decipher the real ID code by himself. With two responds of a specific tag being never the same, the problem of traceability is solved, because an attacker can not link two sightings of the same tag.
The concept which is used here is called *Controlled Delegation* which means, that the trusted center decides whether it gives the information to the reader or not. It is important that the trusted center does not give the key to the reader because this would allow the reader to read the tag for all time, which also creates the possibility of physical attacks on the readers memory to get the key. So the trusted center deciphers the ID and passes it on to the reader. The next time the reader sees the tag, it will not recognize the tag as the one read before.
If the reader should be able to read the tag for a limited number of times, this is possible. Therefore, the trusted center gives the real ID of the tag and the next n pseudonym IDs the tag will respond, where n is the number of times the tag should be readable by this reader.
Ownership transfer is also made secure with this technique. When a tag changes hands, the trusted center simply does not grant access to the old owner anymore and grants access to the new owner.
A method to improve scalability and enhance the delegation between different trust center entities and/or readers, i.e. giving secrets to enable a permanent readability, can also be found in [8].

3 Conclusions and Future Work

RFID technologies have promised multiple benefits for manufacturers, retailers and end users in general. These benefits can only be achieved if quality attributes are addressed properly. In this quest, the research community has proposed different techniques to ensure security in RFID implementations, while considering every party's privacy concerns. We have analyzed existing point solutions from a high level, which allowed us to criticize them and ultimately understand the involved trade-offs. We aim to continue updating this catalog, further specifying the applicable context to facilitate an off-the-shelf selection of privacy and security mechanisms.

4 References

[1] G. Avoine and P. Oechslin. RFID Traceability: A Multilayer Problem. In *Procs. Financial Cryptography and Data Security FC'05*, Roseau, The Commonwealth of Dominica, Feb 2005.

[2] M. Bhuptani and S. Moradpour. *RFID Field Guide*. Prentice Hall, 2005.

[3] C. Bornhovd, T. Lin, S. Haller, and J. Schaper. Integrating Smart Items with Business Processes: An Experience Report. *Procs. 38th Hawaii International Conference on System Sciences*, 08:227c, 2005.

[4] C. Castelluccia and G. Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In *Procs. International Conference on SmartCard Research and Advanced Applications CARDIS'06*, Tarragona, Spain, Apr 2006.

[5] G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In *Procs. 1st. IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, Sep 2005.

[6] F. Kahn. Can Zero-Knowledge Tags Protect Privacy? Cryptology ePrint Archive, Report 2005/049, Nov 2005.

[7] G. Karoth and P. Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. *Procs. ACM Workshop on Privacy in Electronic Society*, Nov 2005.

[8] D. Molnar, A. Soppera, and D. Wagner. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. In *Procs. Workshop on RFID and Lightweight Crypto*, Graz, Austria, Jul 2005.

[9] D. Molnar, A. Soppera, and D. Wagner. Privacy For RFID Through Trusted Computing. In *Procs. Workshop on Privacy in the Electronic Society WPES'05*, Alexandria, VA, USA, Nov 2005.

[10] D. Ranasinghe, D. Engels, and P. Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Procs. Auto-ID Labs Research Workshop*, Zürich, Switzerland, Sep 2004.