Securing RFID systems by detecting tag cloning

Mikko Lehtonen[1], Daniel Ostojic[2], Alexander Ilic[1] and Florian Michahelles[1]

[1] Information Management, ETH Zürich, 8092 Zurich, Switzerland,
mlehtonen@ethz.ch, ailic@ethz.ch, fmichahelles@ethz.ch,
[2] Pervasive and Artificial Intelligence Research Group, Department of Informatics,
University of Fribourg, Switzerland,
daniel.ostojic@unifr.ch

Abstract. Cloning of RFID tags can lead to financial losses in many commercial RFID applications. There are two general strategies to provide security: prevention and detection. The security community and the RFID chip manufacturers are currently focused on the former by making tags hard to clone. This paper focuses on the latter by investigating a method to pinpoint tags with the same ID. This method is suitable for low-cost tags since it makes use of writing a new random number on the tag's memory every time the tag is scanned. A back-end that issues these numbers detects tag cloning attacks as soon as both the genuine and the cloned tag are scanned. This paper describes the method and presents a mathematical model of the level of security and an implementation based on EPC tags. The results suggest that the method provides a potentially effective way to secure RFID systems against tag cloning.

Key words. Security, clone detection, low-cost, EPC, RFID

1 Introduction

Radio frequency identification (RFID) is taking its place as a pervasive everyday tool for automatic identification (Auto-ID) of physical objects. Various industries use it to facilitate the handling of physical goods. RFID is also an enabling technology behind the the Internet of Things (IoT) [1]. IoT connects physical objects to networks and databases and makes use of sensors and actuators to enable new levels of measuring and processing accuracy of real-world processes.

RFID is changing the way security is engineered in Auto-ID applications. On the one hand, RFID brings improvements to security vis-a-vis older Auto-ID technologies by providing increased visibility and the possibility to use cryptography [2]. While an object tagged with a non-serialized barcode can be reliably authenticated only with the help of an additional security feature, such as a hologram or special taggants, an RFID tag can enable both identification and authentication of the tagged object. On the other hand, security is needed in many RFID applications. RFID tags are used to grant access to buildings [3], ski resorts [4], and highways [5], as tickets to public transports [6] and Olympic games [7], and in mobile payment [8]. Moreover, RFID is being adopted as a product authentication technology to secure supply chains from counterfeit products

[9]. In all these applications cloning and impersonation of RFID tags could be financially lucrative for occasional hackers or professional criminals, and severely damaging for the licit companies' revenues and reputation. The potential losses due to security breaches are furthermore amplified by the high level of automation allowed by the technology. Therefore security is not only added value that RFID provides vis-a-vis older Auto-ID technologies – it is also a requirement.

From the point of view of RFID technology, the most challenging security threats in commercial RFID applications are tag cloning and tag impersonation. The research community addresses these threats primarily by trying to make tag cloning hard by using cryptographic tag authentication protocols [2]. The fundamental difficulties of this research revolve around the trade-offs between tag cost, level of security, and performance in terms of reading speed and distance; it is not very hard to protect an RF device from cloning today, but it is extremely challenging to do it using a low-cost barcode-replacing RFID tag. These tags will be deployed in numbers of several millions and the end-user companies have a strong financial incentive to minimize the tag cost and thus the features the tags provide. To illustrate these rigid hardware constraints, according to Sanjay Sarma, the co-founder of the Auto-ID center at MIT, you *can't do anything beyond hashes in passive RFID tags* [10].

Though the research community always provides incremental improvements to the aforementioned trade-offs, there are reasons to believe that low-cost RFID tags cannot be completely protected from cloning in the foreseeable future. Today it takes the computational and physical complexity of approximately a smart card to implement a mobile device that can be considered reasonably secured against most known threats, including side-channel attacks and physical attacks [42]. Low-cost tags are computationally much weaker devices than smart cards, they can use only a fraction of a smart card's energy and power budget, they lack the physical protection, and furthermore even stronger and better protected devices have been cracked. As a result, it is disputable whether it is possible to come up with a truly secure RFID device that addresses all known vulnerabilities without coming up with a device that effectively has the cost and/or performance (i.e. reading speed and distance) of a wireless smart card.

This paper investigates an approach to secure low-cost RFID systems against tag cloning and impersonation based on detection of cloning attacks – an approach that is far from being fully exploited today. Instead of relying on the strength of the weakest and cheapest devices within the system, the tags, this approach relies on the visibility the tags provide. The underlying technical concept is simple and it has already been proposed for ownership transfer and access control [31–33] (cf. Section 2). However, it has not been included in review papers (e.g. [2]), and we think that it merits a recognition. Therefore our major contribution is not the idea development itself but innovative application and thorough evaluation of the concept with respect to cloning of RFID tags.

Our focus on low-cost RFID tags stems from two motivations. First, also low-cost tags are used in security-sensitive applications where cloning of tags could lead to big damage. For instance, Pfizer uses low-cost HF and UHF tags as authentication features for their most counterfeited drug product Viagra [9]. Second, if also low-cost tags can be properly secured, RFID could be applied also in security sensitive domains where the cost of cryptographic tags cannot be justified.

This paper is organized as follows. We first provide a structured review of related work in Section 2. We then study the potential of the presented approach by presenting a statistical model of the provided level of security in Section 3, our implementation based on standard off-the-shelf EPC tags in Section 4, and we discuss the pros and cons of the method focusing on anti-counterfeiting and access control applications in Section 5. Section 6 finishes with the conclusions.

1.1 Introduction to RFID

RFID systems include tags that are affixed to objects, interrogators that read and write data on tags, and back-end systems that store and share data. Passive tags get all their power from the reader while more expensive active tags have a battery. The most important standard for networked RFID is overseen by EPCglobal Inc.[3] The focus of the EPC system is on information in databases associated with EPCs. EPC standards are driven by the retail industry and they focus on passive low-cost UHF tags [11]. Moreover, UHF tags are important in logistics applications due to their higher read range compared to LF and HF tags.

While cryptographic RFID tags are currently widely available in the HF band (e.g. Mifare Desfire[4]), today there are no cryptographic tags commercially available in the UHF band. However, the need for security products in the UHF market is emerging and the first implementations exist (e.g. [12, 13]).

2 Related work

In very general terms, security is the process of protecting assets against adversaries' actions and it comprises steps of prevention, detection, and response [15]. In the following we review related work by mapping countermeasures to the three steps in the process of securing an RFID system against tag cloning and impersonation. This resulting overall process is illustrated in Fig. 1.

2.1 Prevention

Prevention is about building barriers that must be broken or bypassed so as to materialize a threat. It constitutes the first level of defense and the most obvious target for adversaries' attacks. A mundane example of preventive security measures is a lock in a house's front door. Strength of the preventive measures is characterized by their Cost to Break (CtB) that is the minimum effort to

[3] http://www.epcglobalinc.org

[4] http://mifare.net/products/mifare_desfire.asp

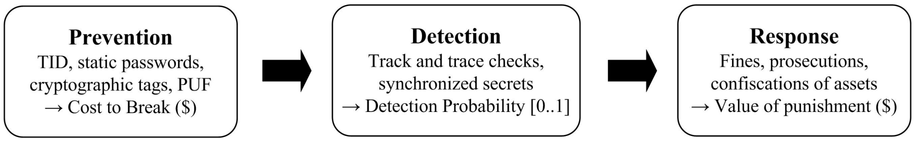

Prevention
TID, static passwords, cryptographic tags, PUF
→ Cost to Break ($)
Detection
Track and trace checks, synchronized secrets
→ Detection Probability [0..1]
Response
Fines, prosecutions, confiscations of assets
→ Value of punishment ($)

Fig. 1. Process of securing an RFID system against tag cloning and impersonation (the small arrows indicate the outcome and metric of each step)

find and exploit a vulnerability [16]. Once preventive measures are broken, the exploitation can normally be repeated with a small marginal cost.

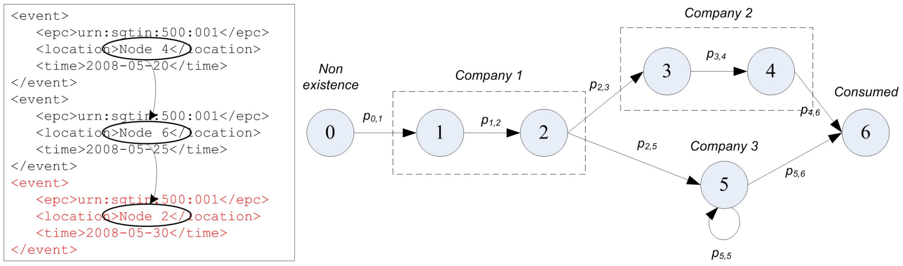
Basic preventive measures of standard EPC tags include unique factory programmed, read only, transponder ID (TID) numbers [11] that are somewhat similar to the network card MAC addresses, and password-protected ACCESS and KILL commands (e.g. [18]). The basic measures, however, are vulnerable to eavesdropping and thus they provide only modest protection against tag cloning.

Cryptographic measures include reader-to-tag and tag-to-reader authentication. Several tag-to-reader authentication protocols have been proposed in the literature, usually based on cryptographic primitives like bitwise operations and pseudo-random numbers (e.g., [17, 19, 20]) or hash-functions (e.g., [22–24]). Also different symmetric encryption-based tag authentication protocols exist, for example based on AES algorithm (e.g., [14, 12, 25]). Asymmetric encryption is currently very challenging on RFID tags but due to advances in elliptic curve cryptography (ECC) it is becoming feasible [26, 27]. Moreover, key distribution that is a big future challenge of secure RFID. Another way to authenticate an RFID tag is to use a Physical Unclonable Function (PUF) [28] that is a one way function implemented using minimalistic hardware overhead.

2.2 Detection

Detection is about minimizing the negative effects of materialized threats and increasing the adversaries' probability of getting caught. A video surveillance system is a typical example of detective measures. In some cases detection enables an immediate response that nullifies the negative effects of the materialized threat, and the result is effective prevention of the negative effects. This is analogous to an intrusion detection system that detects the intruder immediately when the intrusion occurs and blocks the intruder before he can do any harm. In other cases there is a delay before detection leads to a response and the materialized threat leads to harmful effects. For instance, this is the case with burglar alarms that do not immediately seize the harm from happening.

In RFID systems, detection-based measures do not require cryptographic operations from the tags but they make use of visibility to detect cloned tags or changes in the tag ownership. The efficiency of a detection based measure is characterized by the probability to detect a threat. In contrast to preventive



```
<event>
   <epc>urn:sgtin:500:001</epc>
   <location>Node 4</location>
   <time>2008-05-20</time>
</event>
<event>
   <epc>urn:sgtin:500:001</epc>
   <location>Node 6</location>
   <time>2008-05-25</time>
</event>
<event>
   <epc>urn:sgtin:500:001</epc>
   <location>Node 2</location>
   <time>2008-05-30</time>
</event>
```

Fig. 2. Illustration of how cloned tags can be detected from track and trace data (left): since transition from Node 6 to Node 2 ($p_{6,2}$) is not possible according to the supply chain model (right), the last event in Node 2 must be generated by a cloned tag [30]

measures, detective measures can generate *false alarms* where a genuine tag is classified as an impersonator.

Juels [2] noted that serial level identification alone without secure verification of the identities can be a powerful anti-counterfeiting tool. Koh *et al.* [34] made use of this assumption to secure pharmaceutical supply chains by proposing an authentication server that publishes a *white list* of genuine products' ID numbers. Staake *et al.* [29] were among the first to discuss the potential of track and trace based product authentication within the EPC network and they point out some problems that occur when the back-end no longer knows where the genuine object is. Mirowski and Hartnett [3] developed a system that essentially detects cloned RFID tags or other changes in tag ownership in an access control application using intrusion detection methods. To address the problem of limited visibility, Lehtonen *et al.* [30] applied machine learning techniques to automatically detect cloned tags from incomplete location data (cf. Fig. 2).

Ilic *et al.* [31] made use of a similar synchronized secret approach, but the application focus was on ownership transfer and access control. Also Grummt and Ackermann [32] presented the idea behind synchronized secrets approach in an RFID access control application in a scheme called *chosen, temporarily valid secrets*. In addition, Koscher *et al.* [33] describe the same principle in a technical report as a way of increasing the security of ACCESS code based authentication of EPC tags. However, none of the authors discussed and evaluated how the synchronized secrets approach could be applied to address tag cloning attacks.

2.3 Response

Response is what happens after a materialized threat is detected. It comprises of all the actions that minimize the negative effects for the process owner [35] and maximize the negative effects for the adversary in terms of punishments. In commercial RFID applications this can mean, for example, confiscation of the illicit goods, prosecution of the illicit players on contract breaches and illegal activities, and ending business relationships. The lack of effective law enforcement can severely cripple the strength of responsive measures, especially in developing countries. Moreover, small companies have less power to deliver hefty punishments than big companies, making them potentially more lucrative targets.

Responsive measures define the expected value of the punishment and they contribute an important component to the overall *deterrent* effect of security that can be characterized by change in the expected payoff from attempted illicit activities. According to the deterrence theory, the lower the overall payoff including the risk of getting caught, the less willingly and often adversaries attempt to realize the threat. In particular, an asset worth of $100 is safe from rational, risk-neutral, and financially motivated thieves if the cost and risk factor of an attempted theft sum up to more than $100. However, because of asymmetric information, different risk perceptions, irrational decisions, and lack of reliable data, researchers have often failed to find empirical evidence of deterrence decreasing the supply of crime in practice [36].

2.4 Effect of security

Given the structured view of security, we can now model the overall effect of a system's all security measures on an adversary. Such modeling can be used to evaluate the effect of security on financially motivated thieves, but it is less useful for occasional hackers who are motivated by intellectual challenges, fame, reputation etc. When E denotes the expected net value of an attempted attack for an adversary, CtB the cost to break the preventive measures, P_{det} the probability the an attack is detected by the detective measures, P_{pun} the probability that the adversary is punished if the attack is detected, F the value of the punishment, and L the value of the loot, the process of security affects an adversary's payoff as defined by Equation 1.

$$E = (1 - P_{det})(L - CtB) - P_{det}P_{pun}(F + CtB) \tag{1}$$

This model bases on Schechter's work on how much security is enough to stop a thief [37] and it shows how both preventive and detective measures can make an adversary's payoffs negative through high CtB or high P_{det}, respectively. In particular, owing to the risk of punishment, a detective measure does not need to have a 100% P_{det} in order to make $E < 0$. This means that a high-enough detection rate is enough to destroy the business model of a thief.

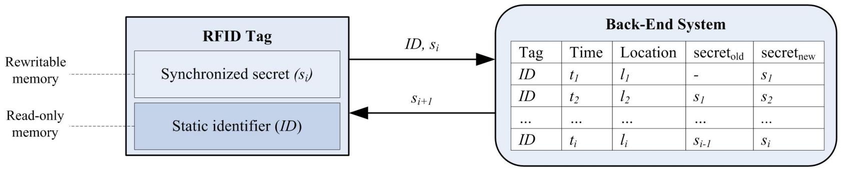
3 Detecting cloned tags with synchronized secrets

The available methods to secure low-cost RFID tags from cloning are limited. In particular, cryptographic approaches proposed in the literature cannot be used with the existing standard UHF tags since they require changes in the chip's integrated circuit, and existing detective measures do not perform well under limited visibility. The presented method described in this section attempts to partially address these problems. Though the method is simple and it has already been proposed in other RFID applications ([31–33]), it has not yet been applied and evaluated to address tag cloning attacks.

3.1 Proposed method

The presented method makes use of the tags' rewritable memory. In addition to the static object and transponder identifiers (e.g. EPC, TID [11]), the tags store a random number that is changed every time the tag is read. We denote this number a *synchronized secret* since it is unknown to all who do not have access to the tag and it can also be understood as a one-time password. A centralized back-end system issues these numbers and keeps track of which number is written on which tag to detect synchronization errors.

Every time a tag is read, the back-end first verifies the tag's static identifier. If this number is valid, the back-end then compares the tag's synchronized secret to the one stored for that particular tag. If these numbers match, the tag passes the check – otherwise an alarm is triggered. After the check, the back-end generates a new synchronized secret that the reader device writes on the tag. This principle is illustrated in Fig. 3.



Tag	Time	Location	secret$_{old}$	secret$_{new}$
ID	t_1	l_1	-	s_1
ID	t_2	l_2	s_1	s_2
...	...	...	...	...
ID	t_i	l_i	s_{i-1}	s_i

Fig. 3. Illustration of the protocol

If a tag has an outdated synchronized secret, either the tag is genuine but it has not been correctly updated (desynchronization) or someone has purposefully obtained and written an old secret to the genuine tag (sophisticated vandalism), or the genuine tag has been cloned and the cloned tag has been scanned. Since unintentional desynchronization problems can be addressed with acknowledgments and the described form of vandalism appears somewhat unrealistic in today's commercial RFID applications, an outdated synchronized secret is as a strong evidence of a tag cloning attack. If a tag has a valid static identifier but a synchronized secret that has never been issued by the back-end, the tag is likely to be forged.

An outdated synchronized secret alone does not yet prove that a tag is cloned; if the cloned tag is read before the genuine tag after cloning attack occurred, it is the genuine tag that has an outdated synchronized secret. Therefore an outdated synchronized secret is only a proof that tag cloning attack has occurred, but not a proof that a tag is cloned. As a result, the presented method pinpoints the objects with the same identifier but it still needs to be used together with a manual inspection to ascertain which of the objects is not genuine.

To protect the scheme against man-in-the-middle (MITM) attacks and malicious back-ends and readers, the back-end and the readers need a reliable way to prove their authenticity to each other. The protocol itself is agnostic to how this is achieved, and it can be done using for example a trusted reader platform [38] and standard public key infrastructure (PKI).

In addition to knowing that a cloning attack has occurred, the back-end can pinpoint a time window and a location window where the cloning attack happened. Thus the method makes it also hard to *repudiate* tag cloning to parties who handle the tagged objects. This is a security service that preventive measures do not provide and it can support the responsive actions.

3.2 Level of security

The level of security of a detection based security measure is characterized by its detection rate (cf. subsection 2.2). In this subsection we evaluate the level of security of the presented method with a statistical model.

We assume a system which consists of a population of tags that have a static identifier and non-volatile memory for the synchronized secret. The tags are repeatedly scanned by readers that are connected to the back-end. The probability that a tag will be scanned sometimes in the future at least once more is constant and denoted by Θ. When a tag is scanned its synchronized secret is updated both on the tag and the back-end as described above in subsection 3.1. The time between these updates for a tag is denoted by a random variable T_{update}. An adversary can copy any tag in the system and inject the cloned tag into the system. The time delay from the copying attack to when the copied tag is scanned is denoted by a random variable T_{attack}. In addition, an adversary can try to guess the value of the synchronized secret.

The system's responses can be statistically analyzed. First, the probability to successfully guess a genuine tag's synchronized secret is $1/(2^N)$, where N denotes the length of the synchronized secret in bits. Even with short sizes, e.g. $N = 32$, guessing the synchronized secret is hard (ca. 2×10^{-9}) and the system can thus be considered secure against guessing attacks[5]. Second, when a copying attack occurs, three mutually exclusive outcomes are possible (cf. Fig. 4):

- **Case 1:** The genuine tag is scanned before the copied tag and an alarm is thus triggered when the copied tag is scanned.
- **Case 2:** The copied tag is scanned before the genuine tag and an alarm is thus triggered when the genuine tag is scanned.
- **Case 3:** The genuine tag is not scanned anymore and thus no alarm is triggered for the copied tag.

In Case 1 the cloned tag is detected as soon as it is scanned the first time and the negative effect of the attack can be prevented. In Case 2 the cloned tag passes a check without raising an alarm but the system detects the cloning attack when the genuine tag is scanned. In Case 3 the security fails and the cloning attack goes unnoticed. The system's level of security is characterized by the probability of Case 1 that tells how often threats are prevented, and by the probability of Case 1 or Case 2 that tells how often threats are detected.

[5] N.B.: There is no brute-force attack to uncover this number

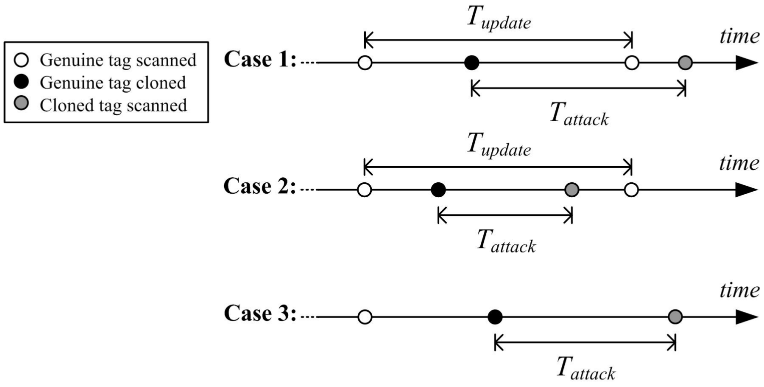


Fig. 4. An illustration of the possible outcomes of a cloning attack

$$\text{Prevention rate} = \Pr(\text{Case 1}) \tag{2}$$

$$\text{Detection rate} = \Pr(\text{Case 1} \vee \text{Case 2}) \tag{3}$$

The probability of Case 1 equals the probability that the genuine tag is scanned at least once more, Θ, multiplied by the probability that the genuine tag is scanned before the cloned tag. Let us assume that the time when the cloning attack occurs is independent of when the genuine tag is scanned and uniformly distributed over the time axis, so the average time before the genuine tag is scanned after the copying attack is $T_{update}/2$. We can now estimate the probability of Case 1 as follows:

$$\Pr(\text{Case 1}) = \Theta \cdot \Pr\left(\frac{T_{update}}{2} - T_{attack} < 0\right) \tag{4}$$

Assuming that $T_{update} \sim N(\mu_{update}, \sigma^2_{update})$ and $T_{attack} \sim N(\mu_{attack}, \sigma^2_{attack})$, we can estimate the probability of Case 1 using a new random variable $Z = \frac{T_{update}}{2} - T_{attack}$ as follows[6]:

$$\Pr(\text{Case 1}) = \Theta \cdot \Pr(Z < 0) \tag{5}$$

Distribution of Z can be calculated using these rules: if $X \sim N(\nu, \tau^2)$, then $aX \sim N(a\nu, (a\tau)^2)$, and if $Y \sim N(\kappa, \lambda^2)$, then $X + Y \sim N(\nu + \kappa, \tau^2 + \lambda^2)$.

$$Z \sim N\left(\frac{\mu_{update}}{2} - \mu_{attack}, \frac{\sigma^2_{update}}{4} + \sigma^2_{attack}\right) \tag{6}$$

[6] N.B.: Since T_{update} and T_{attack} cannot be negative, these assumptions yield viable estimates only when the mean values are high and variances low

Equation 4 shows that the level of security of the synchronized secrets method depends on the frequency in which the genuine tags are scanned with respect to the time delay of the attack, and on the probability that the genuine tag is scanned once more. The same finding is confirmed from equations 5 and 6 which show more clearly that, in the case of normally distributed time variables, $\lim_{\mu_{attack}-\mu_{update}\to\infty} \Pr(\text{Case } 1) = \Theta$.

After the last transaction of the genuine tag, a single cloned tag will always go unnoticed (Case 3). We assumed above a statistically average adversary who does not systematically exploit this vulnerability. However, a real-world adversary who knows the system is not likely to behave in this way. Therefore this vulnerability should be patched by flagging tags that are known to have left the system.

4 Implementation

This section presents our experimental implementation of the presented method using UHF tags conforming to the EPC standard [11]. These tags are relatively low-cost (ca. 0.10-0.20 USD), provide only basic functionalities (e.g. 96-bit rewritable identifier, password-protected access, 16-bit pseudo random number generator), and are therefore expected to be employed in large volumes for tracking various kinds of physical objects.

EPC standards define a user memory bank where the synchronized secret can be stored [21]. To illustrate the real hardware constraints of low-cost RFID tags, many existing EPC tags do not have any user memory. To overcome this problem, one can alternatively re-write the 32-bit access-password in the reserved memory bank to store the synchronized secret, or use a part of the EPC memory bank if it is not completely needed for the object identifier.

The protocol between the back-end system, the reader, and the tag is presented in Fig. 5. In the illustration, s^i denotes the current synchronized secret, s^{i+1} the new synchronized secret, RND_{32} a new 32-bit random number, *alarm* a boolean value whether an alarm is triggered or not, and *ack* an acknowledgment of a successful update of the synchronized secret. Step 6 is dedicated to establishing a secure connection between the reader and the back-end to mitigate MITM attacks, malicious back-end systems, and to protect the integrity of the back-end.

4.1 Set-up

We have implemented the presented method using EPC Class-1 Gen-2 tags from UPM Raflatac that use Monza 1A chips manufactured by Impinj. The reader device is A828EU UHF reader from CAEN and it is controlled by a laptop that runs the local client program. The back-end system was implemented as a web server that stores the EPC numbers, synchronized secrets, and time stamps in a MySQL database. The hardware set-up is shown in Fig. 6.

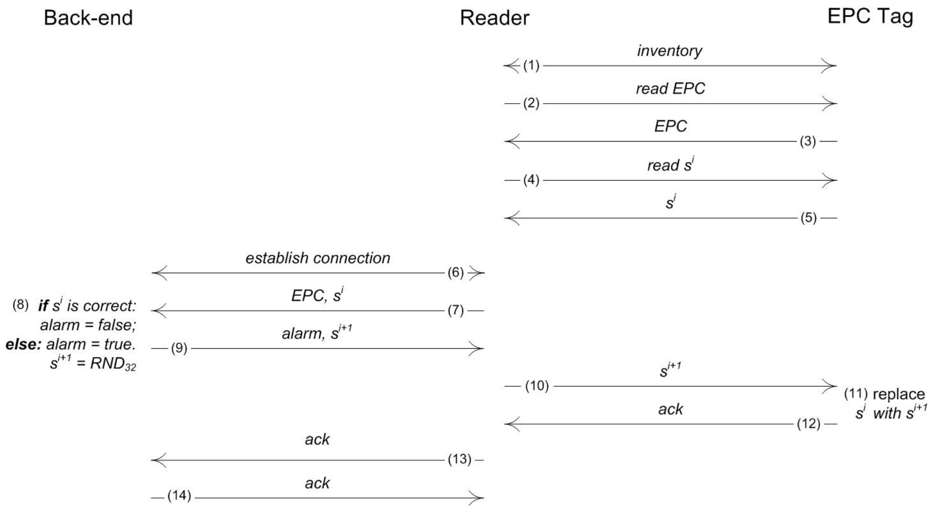


Fig. 5. Implemented protocol

Given that an RFID infrastructure is in place and tags have a modest amount of user memory, the only direct cost of the presented method is the time delay of verifying and updating the synchronized secrets, i.e. steps 4-14 of the protocol (cf. Fig. 5). We have measured this overhead time from 100 reads where the tagged product faces the antenna in 5 cm distance[7].

4.2 Performance

The average overall processing time of one tag was 864 ms. This includes 128 ms for the inventory command, 181 ms for reading the EPC number, and the remaining 555 ms is the time overhead of the synchronized secrets protocol. The measured average times and standard deviations are presented in Fig. 7. The results show that the time overhead of the protocol increases one tag's processing time approximately by a factor of 300%, after the inventory command. Even though the time overhead is short in absolute terms, it makes a difference in bulk reading where multiple products are scanned at once. A closer look on the times of different steps reveals that writing a new synchronized secret on the tag is only a slightly slower than reading a secret from the tag, and that the biggest variance is experienced within the back-end access (steps 6-9).

The performance depends on implementation and has potential for improvement through optimization of reader and back-end software. In addition, variance in web server latency makes the time overhead hard to predict. Despite these

[7] Steps 13-14 of the protocol are omitted from the measurements since they do not increase a tag's processing time

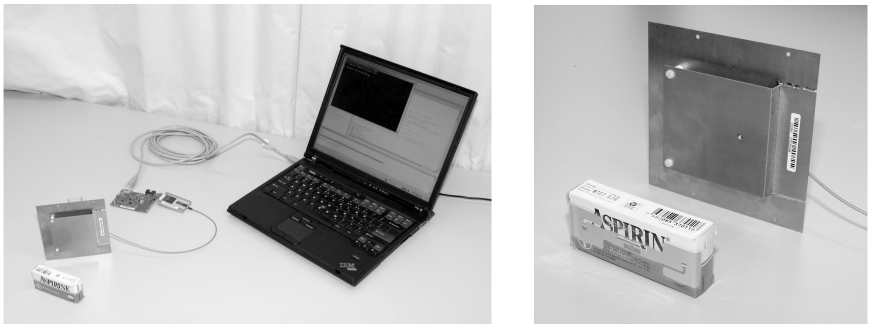


Fig. 6. The hardware set-up

limitations, this simple experiment provides evidence that the overhead time can limit the usability of the presented method in time-constrained bulk reading.

5 Discussion

The challenge of the system designers is to engineer the systems to resist not only the occasional hackers, but also the *law of greed* which says that whenever there exist a possibility to gain from unintended or illegal use, sooner or later someone will do it. Since RFID is primarily used for object identification, the first step of protection is to make sure the objects are what they claim they are. This translates into addressing cloning and impersonation of tags.

Uncertainty relating the alarms is inherent in detection-based security measures and an important cost driver of the overall solution since it invokes manual work; in typical intrusion detection systems an alarm indicates that an intrusion *might* have happened and in the synchronized secrets method an alarm indicates

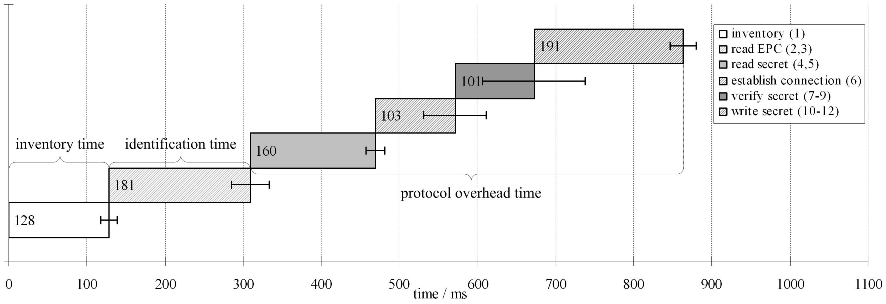


Fig. 7. Measured average times and standard deviations (error bars) of different steps (numbers in brackets) in the implemented protocol

that one of the one of the objects with the same ID is not genuine. Therefore end-users of detective security measures need to implement a verification process that is triggered by every alarm. For the presented method this process includes locating all the physical objects with the same ID and manually verifying these objects. Compared to other detection-based security measures the synchronized secrets method has a major advantage regarding the number of needed manual verification; since an alarm in the synchronized secrets method always indicates a cloning attack – given that desynchronization problems are addressed – the method does not generate any pure false positives. In track and trace based methods, however, alarms can also be generated by any irregular supply chain events such as reverse logistics. This advantage is illustrated with a numeric example in subsection 5.2 below.

The synchronized secrets method does not require sharing of track and trace data, which is a benefit for companies that find this information too sensitive for disclosing. However, if there are large delays between the scans, the synchronized secrets method can trigger an alarm for the cloned tag only after a large delay. In some applications this delay cannot be allowed since it could mean, for example, that a counterfeit medicine has already been consumed. In track and trace based clone detection methods the alarm is triggered – if it is triggered – primarily right after the cloned tag is scanned, and thus similar delays are less likely to occur.

One physical back-end system is unlikely to be scalable enough to run the synchronized secrets protocol for the large numbers of objects that will be tagged. Fortunately, this kind of scalability is also not needed. The back-end can be distributed to virtually an unlimited number of servers by having, for example, one back-end server per product family, per product type, per geographical region, or per a subset of certain kinds of products. This can be implemented either with static lists that map EPC numbers to different back-end systems and that is known by readers, or with the help of EPC Object Naming Service (ONS) or Discovery Services (DS) that provide one logical central point for queries about information and services related to a product [39]. Moreover, the scalability requirements of the presented method are the same as in any RFID system where the back-end knows the current location/status of the items. Additional network requirements of the presented method include strong authentication between the reader devices and the back-end to secure the protocol against MITM attacks.

All EPC tags are potentially vulnerable to tampering of the tag data which can be used as a Denial of Service (DoS) attack against the presented method. This DoS vulnerability can be mitigated with the access passwords of EPC tags [11] by having the reader retrieve the access password and unlock the tag after identification (cf. step 2 in Fig. 5), and lock the tag again after updating the synchronized secret. Moreover, write and read protection of the user memory where the synchronized secret is stored can be used to as a complementing security measure to prevent tag cloning and tampering. In addition, the use of synchronized secrets opens a door for a new DoS attack that makes a genuine tag cause an alarm even when there are no cloned tags in the system; an adversary that is located near to an authorized reader can eavesdrop the static ID number and the synchronized secret of a genuine tag and impersonate this tag to an authorized reader before the genuine tag is scanned. As a result, the genuine tag will raise an alarm next time it is scanned. This results into an unnecessary manual inspection of the genuine tag (which will reveal the time and location of the impersonation attack). This DoS attack is possible only when adversaries have access to an authorized reader device, which is typically not the case in supply chain applications such as anti-counterfeiting. Furthermore, the time and location of this DoS attack are registered, while there are also simpler attacks that achieve the same outcome without leaving any such trace, namely physical or electromagnetic destruction of the tags.

5.1 Anti-counterfeiting

The presented method, complemented by flagging of all sold or consumed products, makes injection of counterfeit products into protected supply chains very difficult; counterfeit products that do not have RFID tags or that have RFID tags with invalid ID numbers are revealed as fakes, and counterfeit products with cloned RFID tags cause a desynchronization that the back-end detects (Case 1 or Case 2). In particular, there is nothing that an adversary can do to a cloned tag that would prevent the system from detecting the cloning attack, given that the genuine and cloned tags will be scanned. In addition to protecting the system from tag cloning, the presented method also provides a proof of when the tags are cloned. This helps further in pinpointing the illicit players and problematic locations. Since the readers and products are located in the premises of the supply chain partners, the risk of above mentioned DoS attacks is low. As a result, the presented method provides a considerable increase in security compared to standard EPC/RFID-enabled supply chains where tag cloning attack is not addressed.

5.2 Access control

Level of security of the presented method depends on how often the tags are scanned and on how much time the adversary needs to conduct the cloning and impersonation attack. We study the scan rates of genuine tags based on a public access control data set [43]. This data set is an activity record of proximity cards within an access control system that controls the access to parts of a building. The probability that a tag was scanned again within this data set is presented in Fig. 8 as a function of time delay from the previous scan. This value equals the probability that a arbitrarily injected cloned tag raises an alarm (Case 1) given the attack delay. For example, an adversary who clones a genuine tag when it is scanned and injects the tag 2 or 24 hours after cloning has a 41% or a 72% chance of raising an alarm upon impersonation, respectively. The overall probability of a tag being scanned again, Θ, was 99.15%, which corresponds to the detection rate (Equation 3). The findings suggest that only very few cloning attacks would potentially go completely unnoticed in the studied application,

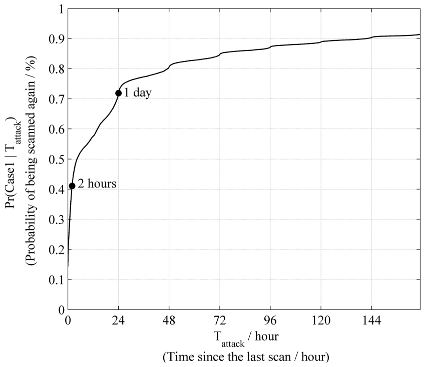


Fig. 8. Time delay between consecutive reads in an access control data set ([43])

and that an adversary needs to conduct the impersonation attack within a few hours after tag cloning to have a relative good chance of not raising an alarm.

Last, we compare the performance of the synchronized secrets method to that of Deckard, a system that was designed to detect cloned tags within the aforementioned data set based on statistical anomalies [3]. In average, Deckard was able to detect 76% of cloned tags with an 8% false alarm rate from simulated attack scenarios within the aforementioned data set. Assuming that 1% of transactions are generated by cloned tags, this means that for each alarm triggered by a cloned tag there are approximately 11 false alarms triggered by genuine tags. As a result the probability that a tag that triggers an alarm is really a cloned one is only 8.4%. Within the synchronized secrets method, however, each alarm indicates a cloning attack and the probability that a tag that triggers an alarm is really a cloned one is 50%, compared to only 8.4% of Deckard. In addition, an alarm would be triggered to 99.15% of cloned tags, compared to 76% of Deckard. This numeric example illustrates the improved reliability of the synchronized secrets method compared to another detection-based RFID security measure.

6 Conclusions

Detecting cloned RFID tags appears attractive for securing commercial RFID applications since it does not require more expensive and energy thirsty cryptographic tags. This paper presents a synchronized secrets method to detect cloning attacks and to pinpoint the different tags with the same ID. The presented method requires only a small amount of rewritable memory from the tag but it provides a considerable increase to the level of security for systems that use unprotected tags. A major benefit of the presented measure is that it can be used with existing standard low-cost RFID tags, such as EPC Gen-2, and it can be applied in all RFID applications where the tags are repeatedly scanned. The additional cost factor of the presented method is manual verifications needed to ascertain which of the tags (objects) with the same ID number is the cloned one, but the number of needed verifications for the presented method is considerably smaller than for comparable detective security measures. Overall, the presented method has the potential to make harmful injection of cloned tags into RFID systems considerably harder using only a minimal hardware overhead.

Acknowledgment

This work is partly funded by the Auto-ID Labs and by the European Commission within the Sixth Framework Programme (2002-2006) projects BRIDGE (Building Radiofrequency IDentification solutions for the Global Environment), IP Nr. IST-FP6-033546. The authors would like to thank the following persons for their comments and help: Michael Fercu and Luke Mirowski.

References

1. Fleisch, E., Mattern, F.: Das Internet der Dinge: Ubiquitous Computing Und RFID in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Springer, Berlin (2005)
2. Juels, A.: RFID security and privacy: A research survey. IEEE Journal of Selected Areas of Communication, **24**(2), pp. 381–894 (2006)
3. Mirowski, L., Hartnett., J.: Deckard: A System to Detect Change of RFID Tag Ownership. International Journal of Computer Science and Network Security, **7**(7) (2007)
4. Michahelles, F., Flörkemeier, C., Lehtonen, M., Hinske, S.: An RFID-tag in Every Ski Item-Level Tagging in the Ski Industry. In: Pervasive Technology Applied - Real-World Experiences with RFID and Sensor Networks, Proceedings of the Pervasive 2006 Workshops, Dublin (2006)
5. Swedberg, C.: RFID Drives Highway Traffic Reports. RFID Journal (2004)
6. IDTechEx: Oyster Transport for London TfL, card UK (2007)
7. RFID News: Olympic tickets to carry wealth of personal info (2008)
8. Texas Instruments: ExxonMobil Speedpass (2008)
9. Bacheldor, B.: Pfizer Prepares for Viagra E-Pedigree Trial. RFID Journal (Feb 2007)
10. Sarja, S.: Introductory Talk: Some issues related to RFID and Security. Keynote Speech in Workshop on RFID Security 2006, Graz (2006)
11. EPCglobal Inc.: Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2. (2005).
12. Feldhofer, M., Aigner, M., Dominikus, S.: An Application of RFID Tags using Secure Symmetric Authentication. In: 1st International Workshop on Privacy and Trust in Pervasive and Ubiquitous Computing, pp. 43-49 (2005)
13. Plos, T., Hutter, M., Feldhofer, M.: Evaluation of Side-Channel Preprocessing Techniques on Cryptographic-Enabled HF and UHF RFID-Tag Prototypes. In: Workshop on RFID Security 2008, Budapest (July 2008)
14. Dominikus, S., Oswald, E., Feldhofer, M.: Symmetric authentication for RFID systems in practice. In: ECRYPT Workshop on RFID and Lightweight Crypto, Graz (2005)

15. Schneier, B.: Beyond Fear. Thinking Sensibly of Security in an Uncertain World. Copernicus Books, New York (2003)
16. Schechter, S. E.: Quantitatively differentiating system security. In: The First Workshop on Economics and Information Security, Berkeley (2002)
17. Juels, A.: Minimalist cryptography for low-cost RFID tag. In: Blundo, C., Cimato, S. (eds.) International Conference on Security in Communication Networks – SCN 2004. LNCS, vol. 3352, pp. 149–164, Springer, Heidelberg (2004)
18. Juels, A.: Strengthening EPC Tags Against Cloning., In: Jakobsson, M., Poovendran, R. (eds.) Proceedings of the 2005 ACM Workshop on Wireless Security, Cologne, Germany. ACM, pp. 67-76 (2005)
19. Vajda, I., Buttyn, L.: Lightweight authentication protocols for low-cost RFID tags. In: Workshop on Security in Ubiquitous Computing, Ubicomp 2003 (2003)
20. Tsudik, G.: YA-TRAP: Yet another trivial RFID authentication protocol. In: IEEE International Conference on Pervasive Computing and Communications, pp. 640-643 (2006)
21. EPCglobal Inc.: Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz v. 1.1.0. (2005)
22. Yang, J., Park, J., Lee, H., Ren, K., Kim, K.: Mutual authentication protocol for low-cost RFID. ECRYPT Workshop on RFID and Lightweight Crypto, Graz (2005)
23. Dimitriou, T.: A lightweight RFID protocol to protect against traceability and cloning attacks. In: IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks SecureComm, Athens, Greece (2005)
24. Avoine, G., Oechslin, P.: A scalable and provably secure hash based RFID protocol. In: IEEE International Workshop on Pervasive Computing and Communication Security, pp. 110-114 (2005)
25. Bailey, D., Juels, A.: Shoehorning Security into the EPC Tag Standard. In: De Prisco, R., Yung, M. (eds.) International Conference on Security in Communication Networks – SCN 2006. LNCS, vol. 4116, pp. 303–320, Springer, Heidelberg (2006)
26. Wolkerstorfer, J.: Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? In: ECRYPT Workshop on RFID and Lightweight Crypto, Graz (2005)
27. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: An Elliptic Curve Processor Suitable For RFID-Tags. Cryptology ePrint Archive, Report 2006/227 (2006)
28. Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., Khandelwal, V.: Design and Implementation of PUF-Based ”Unclonable” RFID ICs for Anti-Counterfeiting and Security Applications. In: IEEE International Conference on RFID 2008, pp. 58–64 (2008)
29. Staake, T., Thiesse, F., Fleisch, E.: Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In: Symposium on Applied Computing, New York, pp. 1607-1612 (2005)
30. Lehtonen, M., Michahelles, F:, Fleisch, E.: Probabilistic Approach for Location-Based Authentication. In: 1st International Workshop on Security for Spontaneous Interaction IWSSI 2007, 9th International Conference on Ubiquitous Computing (2007)
31. Ilic, A., Michahelles, F., Fleisch, E.: The Dual Ownership Model: Using Organizational Relationships for Access Control in Safety Supply Chains. In: IEEE International Symposium on Ubisafe Computing (2007)

32. Grummt, E., Ackermann, R.: Proof of Possession: Using RFID for large-scale Authorization Management. In: Mhlhuser, M., Ferscha, A., Aitenbichler, E. (eds.) Constructing Ambient Intelligence, AmI-07 Workshops Proceedings. Communications in Computer and Information Science, pp. 174–182 (2008)
33. Koscher, K., Juels, A., Kohno, T., Brajkovic., V.: EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. Manuscript (2008)
34. Koh, R., Schuster, E., Chackrabarti, I., Bellman, A.: Securing the Pharmaceutical Supply Chain. Auto-ID Labs White Paper (2003)
35. Mitropoulos, S., Patsos, D., Douligeris, C.: On Incident Handling and Response: A state-of-the-art approach. Computers and Security **25**(5), pp. 351–370 (2006)
36. Cameron, S.: The Economics of Crime Deterrence: A Survey of Theory and Evidence. Kyklos International Review for Social Sciences, **41**(2), pp. 301 - 323 (1988)
37. Schechter, S.E., Smith, M.: How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems and Networks. In: Seventh International Financial Cryptography Conference, Guadeloupe (2003)
38. Soppera, A., Burbridge, T., Broekhuizen, V.: A Trusted RFID Reader for Multi-Party Services. EU RFID Convocation (2007)
39. EPCglobal Inc.: EPCglobal Architecture Framework Version 1.0. (2005)
40. Wang, J., Li, H., Yu, F.: Design of Secure and Low-cost RFID Tag Baseband. In: International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2066–2069 (2007)
41. Sandhu, R.: Good-Enough Security: Toward a Pragmatic Business-Driven Discipline. IEEE Internet Computing **7**(1), pp. 66–68 (2003)
42. Weingart, S.; Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. In: Workshop on Cryptographic Hardware and Embedded Systems, pp. 302-317, Massachusetts (2000)
43. Mirowski, L., Hartnett, J., Williams, R., Gray, T.: A RFID Proximity Card Data Set. Tech. Report University of Tasmania (2008), http://eprints.utas.edu.au/6903/1/a_rfid_proximity_card_data_set.pdf.