20

The Study on Secure RFID Authentication and Access Control

Yu-Yi Chen[1] and Meng-Lin Tsai[2]
[1]Department of Management Information System
National Chung Hsing University
[2]Department of Computer Science and Engineering
National Chung Hsing University
Taiwan

1. Introduction

In recent years, Radio Frequency Identification (RFID) technology is rapid progress and has been widely used in daily life. RFID systems consist of three components: radio frequency (RF) tags, RF readers and a back-end database server. A passive RFID tag is a microchip capable of transmitting a static identifier or serial number for a short distance. Readers query tags for their contents by broadcasting an RF signal. Tags respond with resident data, such as a unique serial number. Tag data may be read automatically without line of sight. RFID systems have many applications in supply chain managements, inventory control, anti-counterfeiting, ticketing systems, healthcare and smart home developments.

However, it may bring up some privacy threats. Anyone can easily access tagged items and collect data without line of sight that personal privacy under threat. The most concerned issues are the tracking and the location privacy. Based on the characteristic of outstanding traceability, the history of the tag's location might be identified as a tag's information is intercepted and collected by the attacker in different location. For instance, the unique tag's EPC data can be used to trace a person or an object carrying a tag in time and space. The collected information can be merged and linked in order to generate a person's profile. It will be a serious problem as RFID tags are widely used.

Without privacy protection, a person with carried RFID tags can be tracked and profiled by unauthorized people. The unique information of the items may be indicated that a customer carrying those tags is subject to track from unauthorized readers.

Ideal RFID systems used in product lifecycle should satisfy high confidentiality, anonymity, integrity and high availability (Gao et al., 2004; Pisarsky, 2004). The product life cycle is a procedure that the product from manufacture to be recycled. This procedure from the perspective of commerce can be divided into five stages(Figure 1): (1)&(2) are the stage of "production to retail store" (business-to-business) , (3) is the stage of "retail store to customer" (business-to-customer), (4) is the stage of "individual sales" (customer-to-customer), (5)&(6) are the stage of "after-sales service", and (7) is the stage of "recycling" (reverse logistics). Since a tag is embedded in the product, security risks such as privacy threats may be occurred in each stage of the product life cycle.

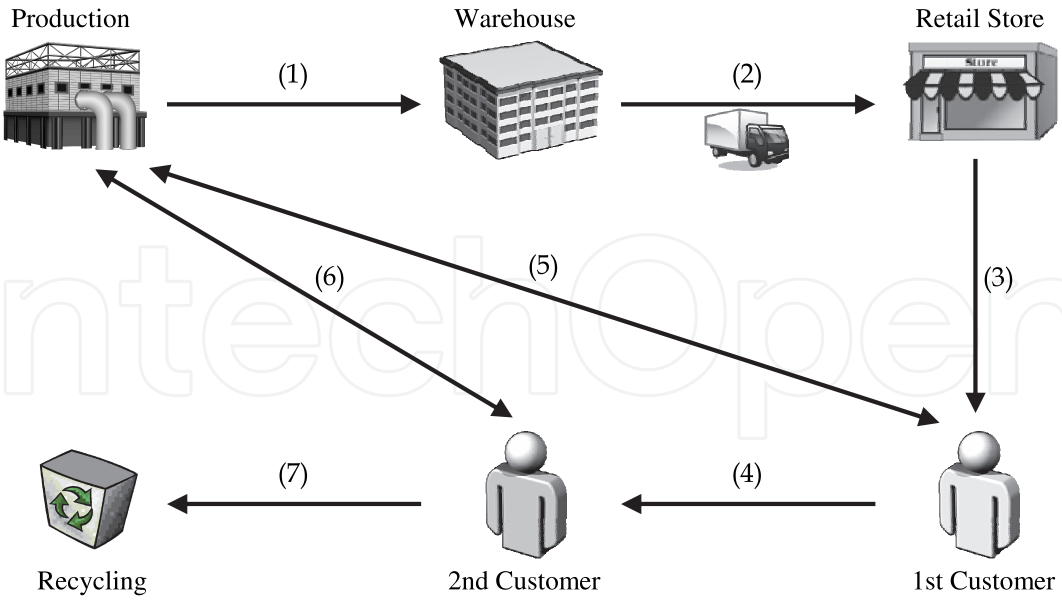


Fig. 1. The product life cycle.

To our desirable point, researchers need to pay more effort to develop object identication throughout the life cycle with guaranteeing the corporate and personal privacy, illegal tracking, unauthorized profiling, impersonating, cloning, and illegal reading/writing. This article is not purpose of an exhaustive literature survey but summarizes some aspects of RFID authentication and access control in the proposed studies.

2. Basic RFID tags

In most RFID systems, tags automatically emit their unique serial numbers upon reader interrogation without alerting their users. The challenge in providing security for RFID tags is such kinds of low-cost device unable to perform basic cryptographic operations. Basic RFID tags just have a little rewritable memory, even have no programmable-supported computing capability. At best, such RFID tags may include security functions supporting keyed reads and keyed writes which essentially just like PIN-controlled data accesses. In this section, we show how privacy and authentication may be considerably improved in low-cost RFID tags with only a small enhancement of their capabilities.

2.1 Killing and sleeping

The “kill command” method is a straightforward approach to make a tag no longer functional. This approach proposed by the AutoID Center is indeed for tags to be killed upon purchase of the tagged product. A tag can be killed by sending it a special “kill command” with a short PIN (Sarma et al., 2002; Weis et al., 2003). As the tag receives the “kill” command, its state changes into the inoperative state. Kill the tag technique is to restrict the use of a tag by removing its identity. As shown in Fig. 2, the killed tag has no way to change back to the inventoried state. It cannot be identified for more detailed information again. For example, purchased goods would be killed at checkout clerks such that no one would contain active RFID tags for protecting the consumer privacy. This solution is simple and effective but the tag can not be reused. Clearly, the tag’s lifecycle is end and it cannot be applied for after-sale purposes.

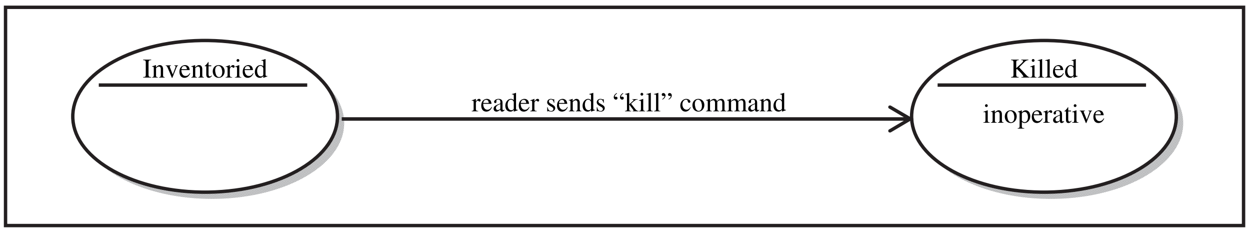


Fig. 2. The state changing of the tag in killing approach

Another kind of solution is using the "sleeping" mechanism. As the reader sends a "sleep" command to the tag, the tag will temporarily inactive. The sleeping tag can be waked as the tag receives PIN from the reader. The state changing of the tag is shown in Fig. 3. The tag's state can be switched between inventoried and sleep. For controlling the tag's access, the tag's owner has to manage the PINs of all tags on purchased good. Unfortunately, passwords may be overheard or collected by spoofing a tag. This approach also pose other problems: a set of tags use a single generic PIN which can be easily defeated, but each tag use a unique PIN which could be uniquely identified by the adversary.

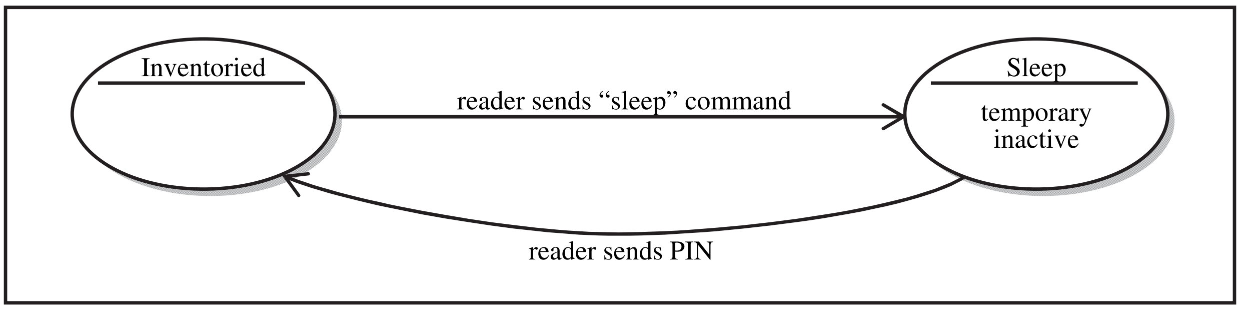


Fig. 3. The state changing of the tag in sleeping approach

2.2 Renaming approach

The solutions of relabeling or re-encrypting the tag's serial number were proposed for minimal security requirements. This approach takes into account the natural computational limitations of RFID tags, it involves no computational operations but only relatively little storage. The relabelled or re-encrypted serial number is overwritten to the tag at checkout for protecting the consumer's privacy. This is possible for current generation tags and would prevent the unauthorized compilation of bibliographic directories. However, even if the relabelled or re-encrypted identifier emitted by an RFID tag has no intrinsic meaning, it can still be tracked since the relabelled or re-encrypted identifier is just a static meta-identifier. Therefore, point-to-point tracking is possible if the meta-identifier is not changed over time. For this reason, this approach does not solve the problem of privacy.

2.2.1 Relabeling

Sarma et al. (2003) proposed an idea to protect the tracking problem (Sarma et al., 2003). As a customer purchases goods, the reader sends a "delete" command at the point of sale such that the tags' unique serial number is erased. Only the product code information of the tag is retained for later use. The state changing of the tag is shown in Fig. 4. However, the tracing problem is still existed to distinguish individual by a fixed group RFID-tagged products. For example, someone is a fan of a particular brand will always take the brand's shoes, watch and bag such that tracking is still possible by associating these kinds of particular tag types with holder identities.

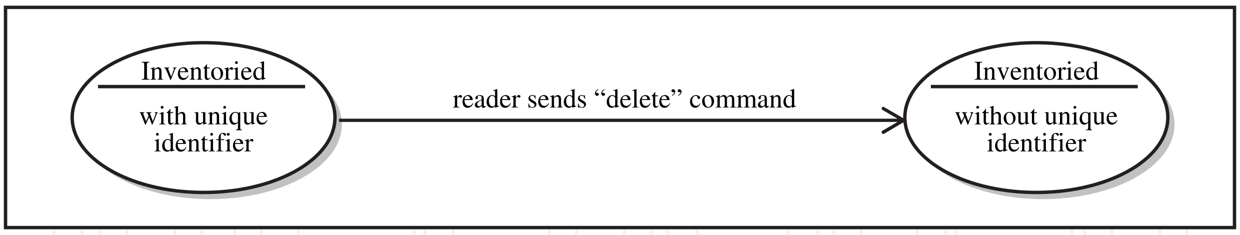


Fig. 4. Sarma's idea for erasing the tag's unique identifier

Inoue & Yasuura (2003) proposed another relabling approach to offer users the identifier's controllability for protecting privacy (Inoue & Yasuura, 2003; Inoue et al., 2002). Each tag has a read-only memory (ROM) and an electrically-erasable programmable read-only memory (EEPROM). These two memories are used exclusively. The state changing of the tag is shown in Fig. 5. A unique and permanent identity is stored in the tag's ROM by the producer. As the tag remains on ROM mode, the permanent identity can be read. The tag can provide unlimited identification with ROM mode for total management at its production, distribution, and sale stage. For purchased goods, the owner can set a private and temporary identity in EEPROM. As switching to EEPROM mode, the tag cannot operate the permanent object identification. Even the temporary identity can be read by anyone, no one can recognize the tag since the information about the object in the network is distributed accompanying the permanent identity on the ROM as a key. Therefore, the adversary has nothing to do with the temporary identity. The object can be identified only by the owner. Moreover, the tag can be switched to ROM mode again by certificating the owner or restricting the change only via contacted communication. This approach remains the permanent identity for life cycle of the object. As the object is discarded, the scrap merchant can make the tag to be switched to ROM mode to operate the permanent object identification and utilize it for recycling. However, the temporary identity is unique and cannot avoid the point-to-point tracing problem since it could be uniquely identified by the adversary.

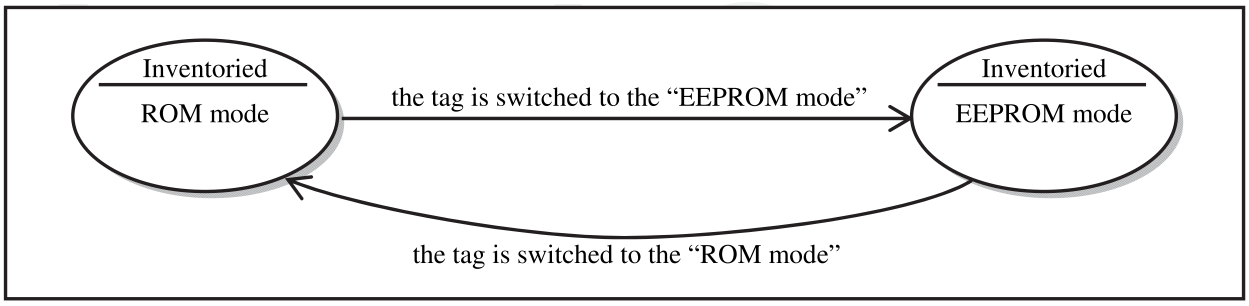

Inventoried
ROM mode
the tag is switched to the "EEPROM mode"
Inventoried
EEPROM mode
the tag is switched to the "ROM mode"

Fig. 5. Inoue's double mode tag

Kinosita et al. (2003) proposed another approach to rewrite the tag (Kinosita et al., 2003). As a customer purchases the product on checkout, the reader rewrites a new random number to the tag. Fig. 6 shows the state changing of the tag. However, the random identifier is unique and cannot avoid the point-to-point tracing problem since it could be uniquely identified by the adversary.

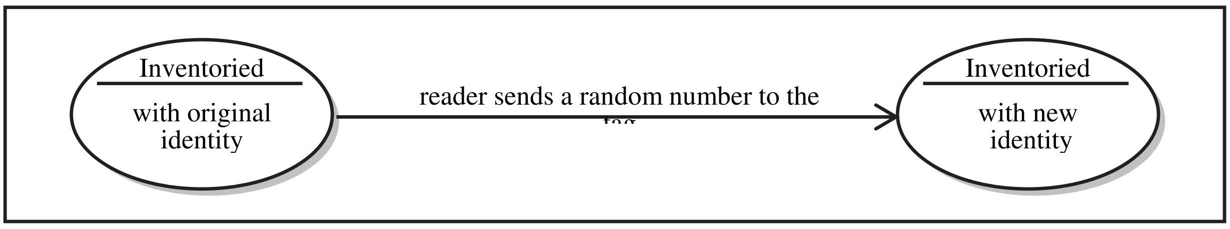


Fig. 6. Kinosita's approach to rewrite the tag

2.2.2 Re-encryption

Juels & Pappu's (2003) proposed an approach based on re-encryption concept (Juels & Pappu, 2003). The public key cryptosystem is used in this scheme. The data of a banknote is arranged into optical and radio frequency areas. A unique serial number and a signature are printed on the banknote. The banknote serial number and signature are encrypted by the law-enforcement's public key. The resulting ciphertexts are stored in the banknote's tag. Clearly, the tag can be authenticated as the ciphertexts are decrypted by the law-enforcement for verifying the signature of serial number. For rendering multiple appearances of the tag unlinkable, these ciphertexts are re-encrypted with a new encryption factor by the law-enforcement's public key after each access session. The encryption-operation requires high computational loading which is performed by the reader not the tag. The change in each appearance is designed for preventing the tracing problem. Fig. 7 shows the state changing of the tag. However, the ciphertexts keep constant (Ohkubo et. al, 2003) such that the tag still can be traced between twice re-encryptions. It means the tag must be rewritten often. This makes re-encryption approach unsuitable in practical. Basing on the re-encryption concept, a similar scheme proposed by Golle et al. (Golle P et al., 2004) known as universal re-encryption mechanism. It is essentially a special extension of the ElGamal cryptosystem (Elgamal T., 1985) in which re-encryption is possible without knowledge of public keys. However, this universal re-encryption mechanism has a practical drawback of requiring the role of agent to perform re-encryption.

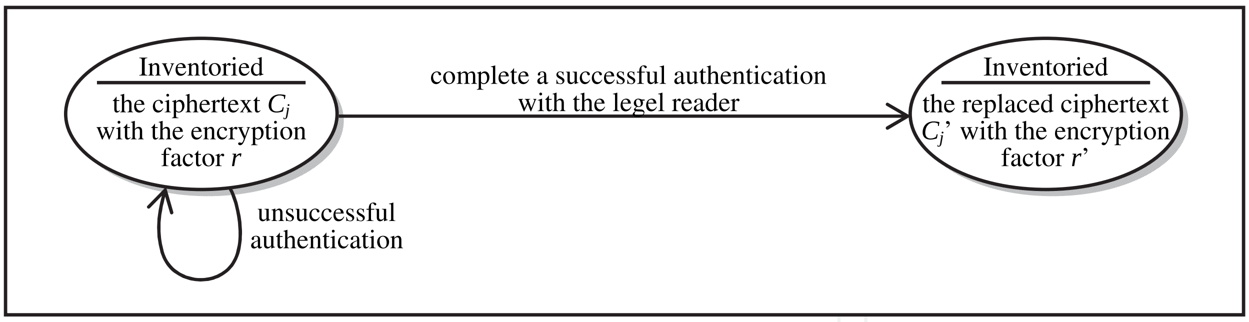

Inventoried
the ciphertext C_j with the encryption factor r
complete a successful authentication with the legel reader
Inventoried
the replaced ciphertext C_j' with the encryption factor r'
unsuccessful authentication

Fig. 7. Juels & Pappu's re-encryption approach

2.3 Distance measurement

Fishkin et al. proposed an approach to measure the distance between the reader and the tag (Fishkin et al., 2004). An adversary usually interrogates the tag in the far distance. Fishkin et al. observes and analyzes the energy of the received signal by the tag. The distance between the reader and the tag can be estimated by the signal-to-noise ratio. This distance information is used as a variable in a tiered authentication scheme, where the tag releases general or specific information to the reader according to the distance variable. Fig. 8 shows the state changing of the tag.

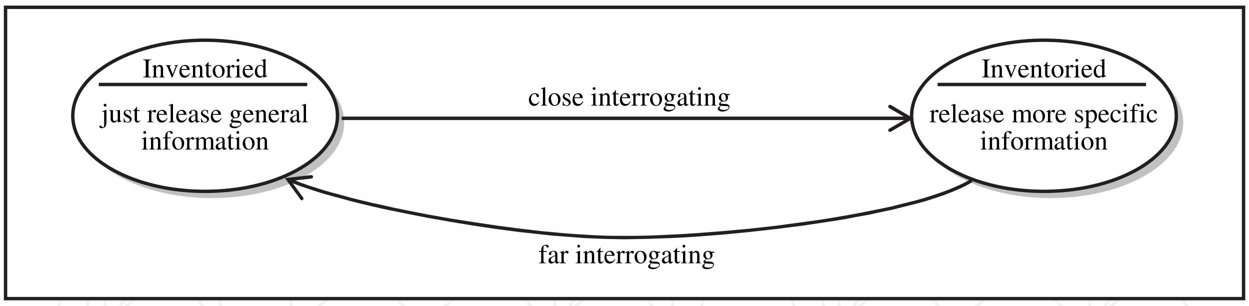

Inventoried
just release general information
close interrogating
Inventoried
release more specific information
far interrogating

Fig. 8. Fishkin's approach

2.4 Blocking & soft blocking

Juels et al's (2003) proposed a mechanism to interfere with the readers' interrogation by a blocker tag (Juels et al., 2003). The blocker tag simulates all possible RFID tags to prevent the malicious identification of the target tag. This privacy protection scheme depends on adding a privacy bit to the tag. While inside a store, the tag's privacy bit usually is set to 0, indicating public access to the tag's identification. While during checkout, this privacy bit is changed to 1, denoting the tag is entering restricted access. Then the tag must interact with another tag known as the "blocker tag" (Juels et al., 2003). The blocker tag broadcasts radio signals to block/disrupt nearby RFID readers could work. It is accomplished through non-standard interaction with the anti-collision protocols employed in tag-reading session (Auto-ID Center, 2003; Sarma, 2001). The blocker tag will manipulate the query result of a normal tag by scrambling the bits of certain tags determined by their privacy bit (Juels & Brainard, 2004). The state changing of the tag is shown in Fig. 9. As the privacy bit is set to 0, the tag can be unrestricted scanned and the blocker tag doesn't interrupt the reading of tag. As the privacy bit is set to 1, the tag is private with restricted access under the cover of blocker tag. Juels and Brainard proposed an enhancement mechanism called soft blocking (Juels & Brainard, 2004). The soft blocker tag transmits a policy statement to enforces and monitors the reader not violate the security policies. However, blocker tag is expensive (Cavoukian, 2004) and suffers from the heterogeneity of current RFID systems using different frequencies, air protocols, etc. The blocker tag and its variants have limited applicability.

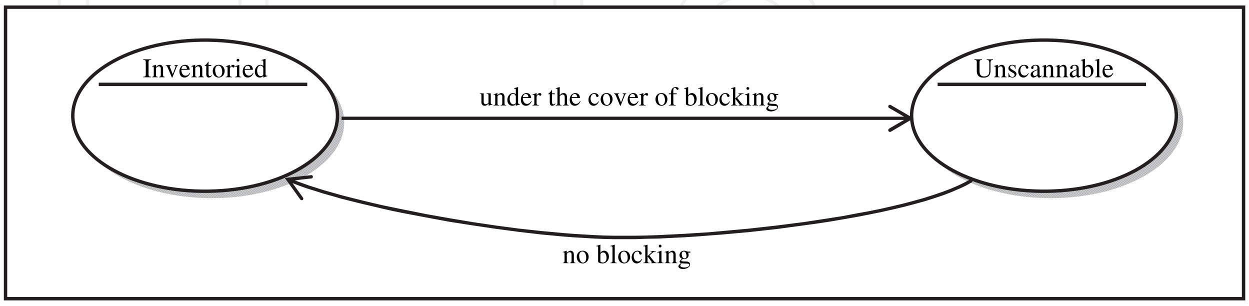


Fig. 9. Blocking approach

3. Symmetric-key tags

Symmetric-key tags are considered as the type of security obtainable with a small amount of rewritable memory, but very limited computing capability. Such RFID tags may be expected to perform some basic computational operations, but not conventional cryptographic ones. Many approaches have been proposed to achieve private authentication in such RFID systems. The proposals usually include hash function, silent tree-walking, or other light cryptography-based approaches to prevent the unauthorized reading of RFID tags. Most researchers devoted to show that standard cryptographic functionality is not needed to achieve stronger security in RFID tags. Since the communication between the reader and the tag is using RF signals, which make an RFID system vulnerable to various attacks such as eavesdropping, traffic analysis, spoofing and denial of service. Within the scanning range, a malicious reader can perform bogus authentication with detected tags to retrieve sensitive information. The sensitive information may be disclosed and hence infringe on the user's privacy. Traceability is another type of privacy violation, the relation between the user and the tag can be found will cause the tracing of the tag makes the tracing of the user possible (Avoine & Oechslin, 2005). The proliferation of RFID applications (Ni et al., 2003) raises an emerging requirement – protecting user privacy (Robinson & Beigl, 2003) in RFID authentications.

As the relationship is illustrated (Fig. 10) in Weis's paper (Weis et al, 2003), the forward channel (reader-to-tag) is assumed to be easily monitored by an adversary since the signal broadcasted by the reader is strong enough, the backward channel (tag-to-reader) is relatively much weaker and may only be monitor by an adversary within the tag's shorter operating range. The reader-to-tag (forward) channel and the tag-to-reader (backward) channel are assumed not secure, but eavesdroppers may only monitor the forward channel without detection.

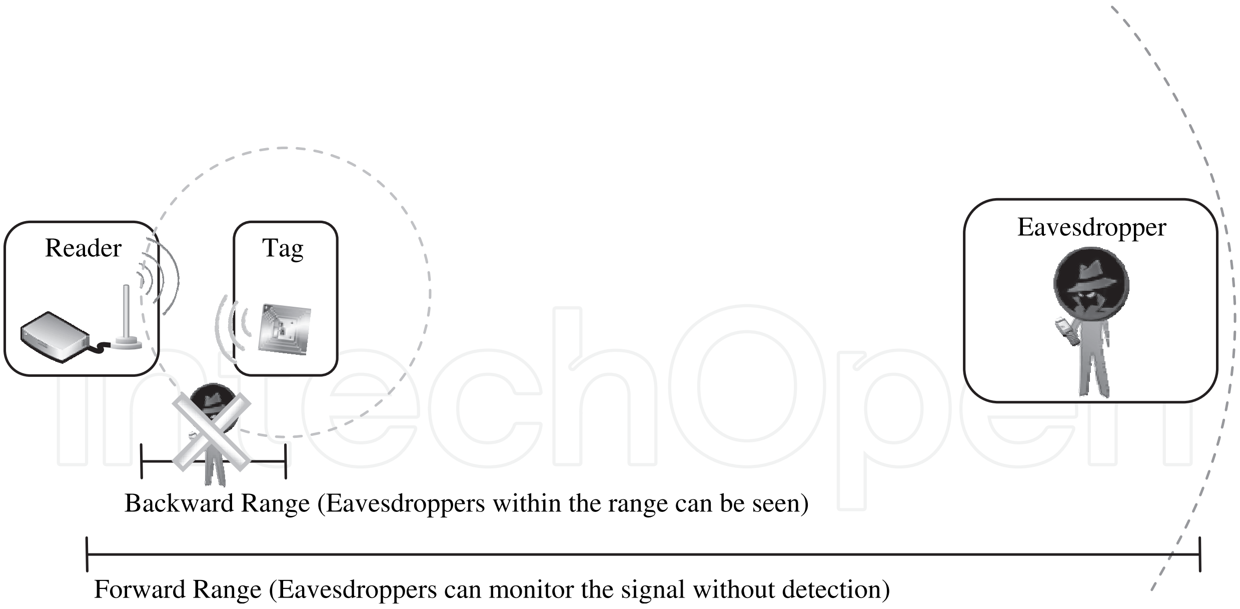

Reader
Tag
Eavesdropper
Backward Range (Eavesdroppers within the range can be seen)
Forward Range (Eavesdroppers can monitor the signal without detection)

Fig. 10. Forward vs. backward channels

In this section, we show how privacy and authentication may be considerably developed. It needs to take into account the natural computational limitations and the likely attack scenarios. The challenge in providing security for low-cost RFID tags is that they are computationally weak devices, unable to perform even basic symmetric-key cryptographic operations.

3.1 Non-indexed key-search approach

The general approach of key search for RFID-tag identification was proposed by Weis et al. (2003). Upon receiving a query from the reader, the tag first sends the hash value of its key with a random nonce. Without any index, the reader must compute for all keys until it identify the tag. As the tag responds with different values every time, the reader must exhaustively search until it finds the matched one. The scheme is not scalable for a huge number of tags since many computations must be performed at the back-end.(Rhee et al., 2005; Weis et al., 2003)

Weis et al. (2003) proposed two simple hash-based access control protocols, the hash-lock scheme and the randomized hash-lock scheme (Weis et al., 2003). Fig. 11 shows the randomized hash-lock scheme. Each tag has its initial ID_i is issued by the back-end database server. As the reader tries to access the tag, the tag's response is a hash value $\alpha = h(ID_i || R)$ generated by hashing the tag's ID_i concatenated with a random number R. If the reader is legal, it can ask the back-end database server to provide all tags' identities. Then the reader performs a brute-force searching comparison between α and $h(ID_k || R)$ to find the corresponding record. This scheme is not scalable since the reader's computational loading is $O(n)$.

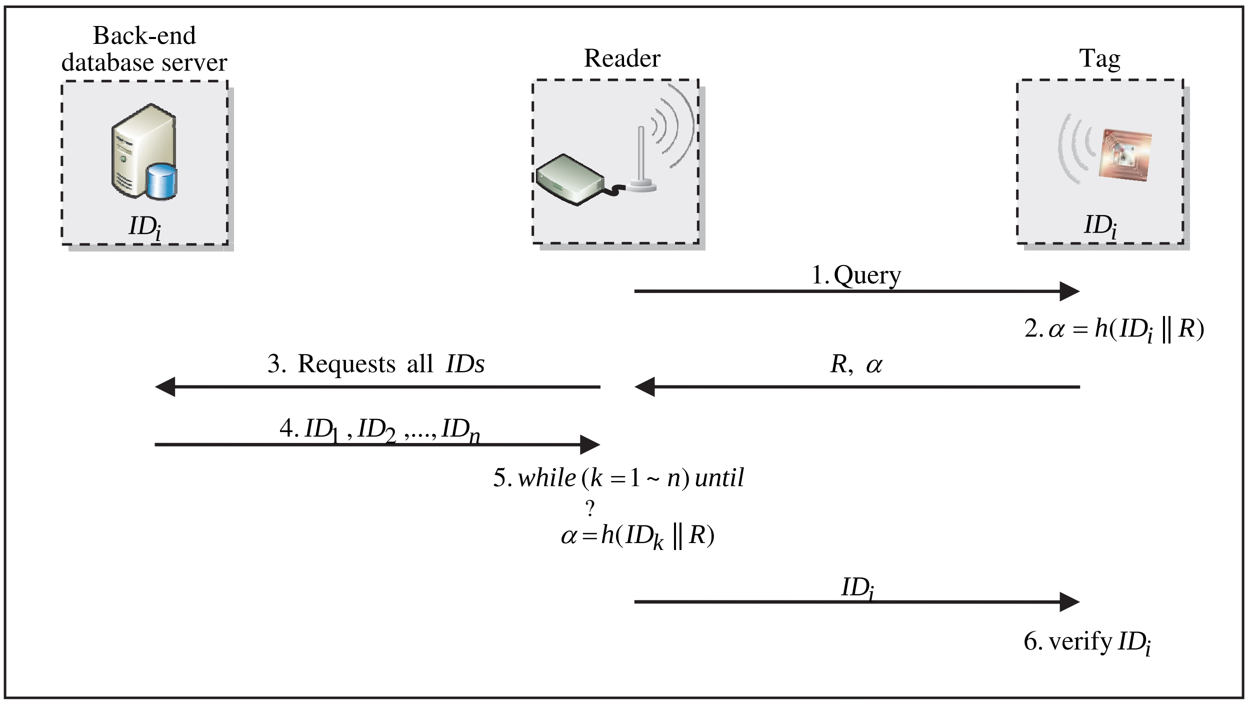

Back-end database server
ID_i
Reader
Tag
ID_i
1. Query
2. $\alpha = h(ID_i \| R)$
3. Requests all IDs
R, α
4. $ID_1, ID_2, ..., ID_n$
5. $while\ (k = 1 \sim n)\ until$
$\alpha \overset{?}{=} h(ID_k \| R)$
ID_i
6. verify ID_i

Fig. 11. Weis's randomized access control scheme

The motivation of this scheme is to make the tag's response message not predictable to prevent the tracing of individual. To randomizes tag responses instead of a invariable tag response in order to protect location privacy. However, the tag still can be traced as shown in the following use-case diagram (Fig. 12). An adversary can eavesdrop on the legal reader's broadcasts ID_i for collecting to its own database. As the target tag's identity is collected, the adversary immediately realizes the tag had appeared on the location. In addition, the adversary may interrogate a tag to get its response message (R, α) for making a brute-force searching comparison between α and $h(ID_i \,||\, R)$ to figure out which collected identity ID_i is matched. Therefore, any collected identity can be traced.

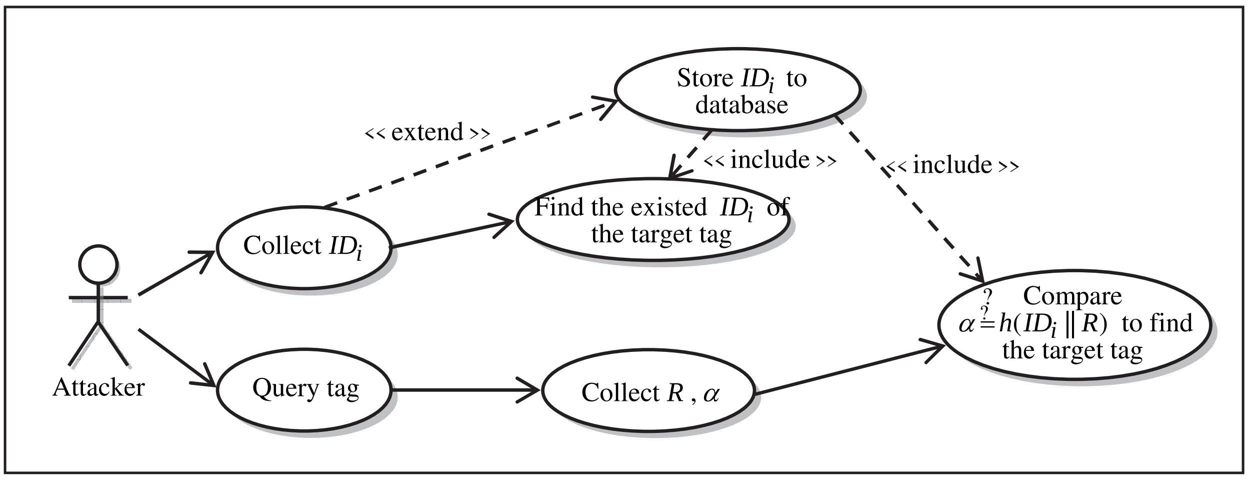


Fig. 12. The attack on Weis's randomized access control scheme

3.2 Indexed key-search approach

The major sticking point with the non-indexed key-search approach is that the reader's computational loading is $O(n)$. Under the practical consideration, it is not scalable since the process of key search can be prohibitively costly if the set of tags is large. For reducing the cost of key search, the tag's first reply message must be the index for key-searching. As the reader has sent the right response being the "key", then the tag reveals its identity. Unfortunately, the invariable index value will cause the tag traceable. (Chien, 2006; Huang, 2009; Weis et al., 2003)

3.2.1 Weis's hash-based access control scheme

Weis et al. (2003) proposed the hash-lock scheme (Weis et al., 2003), shown in Fig.13. Each tag has a hash value $metaID_i$ of its Key_i as it is issued by the back-end database server. The

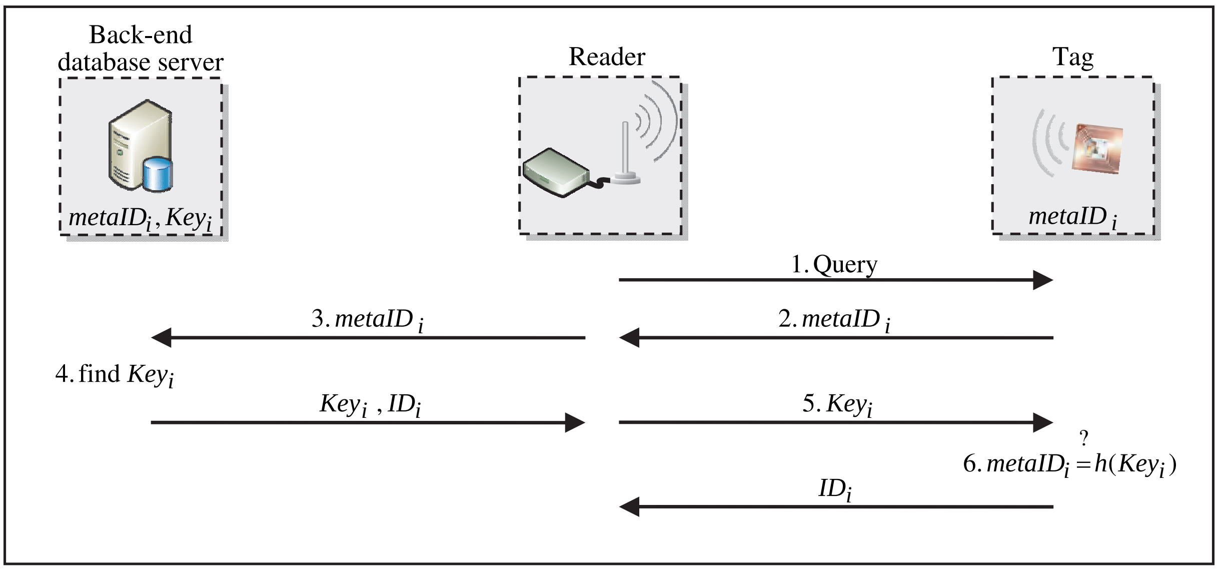


Fig. 13. Weis's hash-based access control scheme

reader can only get this hash value $metaID_i$ as it tries to access the tag. If the reader is legal, it can ask the back-end database server to retrieve the corresponding Key_i. After the tag receives the correct Key_i from the reader, the tag's information can be accessed by the reader. Unfortunately, the scheme not offers location privacy since the tag can be uniquely identified by its hash value. Another drawback is that the plain key is sent over the forward channel which can be eavesdropped in the RF-signal range.

In this scheme,the tag can be traced as shown in the following use-case diagram (Fig. 14). The adversary can eavesdrop on the legal reader's broadcasts Key_i for collecting to its own database. As the target tag's key is collected, the adversary realizes the tag had appeared on the location. Moreover, the adversary may interrogate a tag to get its response message $metaID_i$ for making a comparison between $metaID_i$ and $h(Key_i)$ to figure out which collected Key_i is matched. Since a tag's response message is an invariable $metaID_i$, it can be treated as an identifier, for the adversary to trace individuals. This scheme supports data privacy but can not protect location privacy of the tag since the invariable hash value is used in each time.

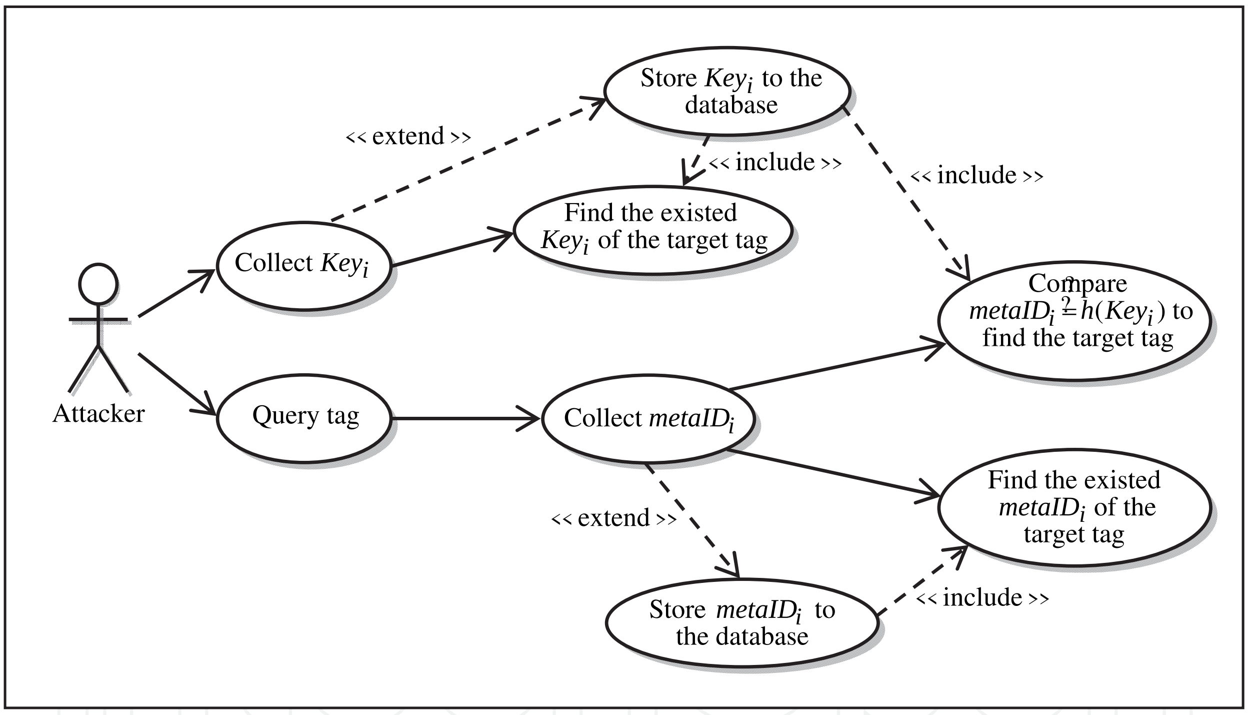

Store Key_i to the database
<< extend >>
<< include >>
<< include >>
Find the existed Key_i of the target tag
Collect Key_i
Compare $metaID_i \overset{?}{=} h(Key_i)$ to find the target tag
Attacker
Query tag
Collect $metaID_i$
<< extend >>
Find the existed $metaID_i$ of the target tag
Store $metaID_i$ to the database
<< include >>

Fig. 14. The attack on Weis's hash-based access control scheme

3.2.2 Chien's hash-based access control scheme

Chien (2006) proposed another hash-based access control scheme (Chien, 2006), shown in Fig. 15. The back-end database server's master secret key is K_{svr}, and each tag's unique key is $Key_i = h(K_{svr} \,||\, ID_i)$ Each tag has a hash value $metaID_i$ of its Key_i as it is issued by the back-end database server. As the reader tries to access the tag, it can get this hash value $metaID_i$ and the current $date$. If the reader is legal, it can ask the back-end database server to retrieve the corresponding ID_i for generating the right Key_i. Then the reader generates a hash value $h(Key_i \oplus date)$ by the tag's Key_i and the received current $date$. After the tag receives the correct hash value $h(Key_i \oplus date)$ from the reader, the tag's information can be accessed by the reader.

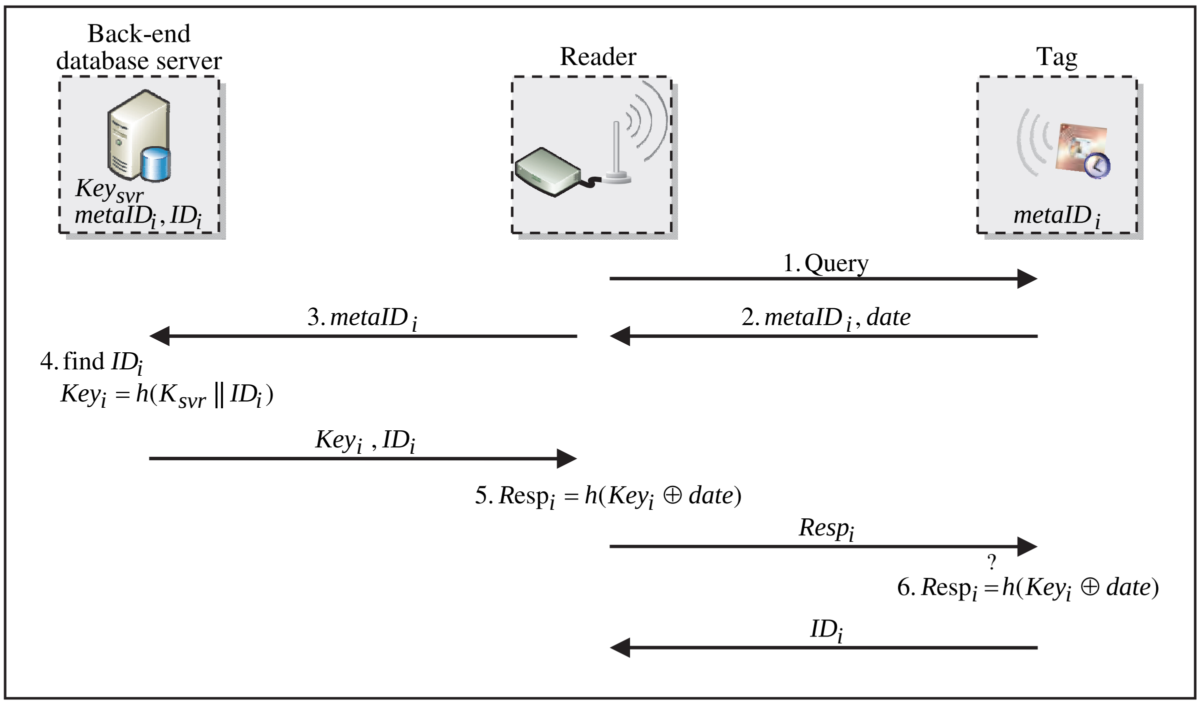


Fig. 15. Chien's hash-based access control scheme

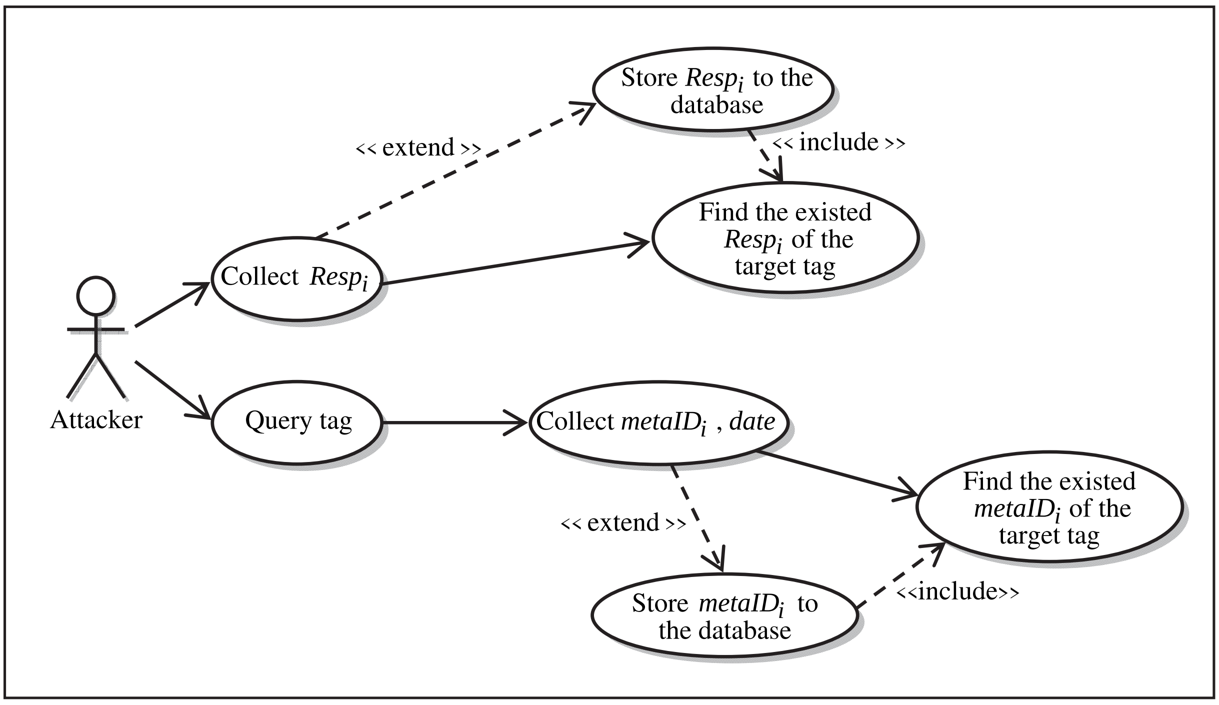

Store $Resp_i$ to the database
<< extend >>
<< include >>
Find the existed $Resp_i$ of the target tag
Collect $Resp_i$
Attacker
Query tag
Collect $metaID_i$, $date$
Find the existed $metaID_i$ of the target tag
<< extend >>
Store $metaID_i$ to the database
<<include>>

Fig. 16. The attack on Chien's hash-based access control scheme

Fig. 16 shows the use-case diagram of this scheme's weaknesses. The adversary can eavesdrop on the legal reader's broadcasts $Resp_i$ for collecting to its own database. As the target tag's response is collected on the same day, the adversary realizes the tag had appeared on the location. Moreover, the adversary may interrogate a tag to get its response message ($metaID_i$, $date$). Since a tag's response message has an invariable $metaID_i$, it can be treated as an identifier for the adversary to trace individuals.

3.3 Synchronization approach

The general idea is to change the tag's identifier after each access session. By refreshing both of the tag's identifier and the corresponding back-end database record in each session, the identifier cannot be employed for tracking purposes. The adversary can only eavesdrop or intercept a single, unreliable message exchange, it seems to provide the tag with location privacy. The literature explores several variants of this principle. Ohkubo, Suzuki, and Kinoshita (OSK) propose the conceptually simplest approach. Henrici and Müller propose to resolve the synchronization problem. Dimitriou proposes a scheme that eliminates the issue of desynchronization entirely. (Avoine & Oechslin, 2005; Dimitriou, 2005; Henrici & Muller, 2004; Joaquin et al., 2011; Juels, 2004; Lee et al., 2005, 2006; Ohkubo et al., 2003; Osaka et al., 2006)

3.3.1 Henrici & Muller's hash-based ID variation scheme

Henrici & Muller (2004) proposed a hash-based ID variation scheme (Henrici & Muller, 2004), shown in Fig. 17. A tag with initial ID_i, transaction number TID_i and last successful

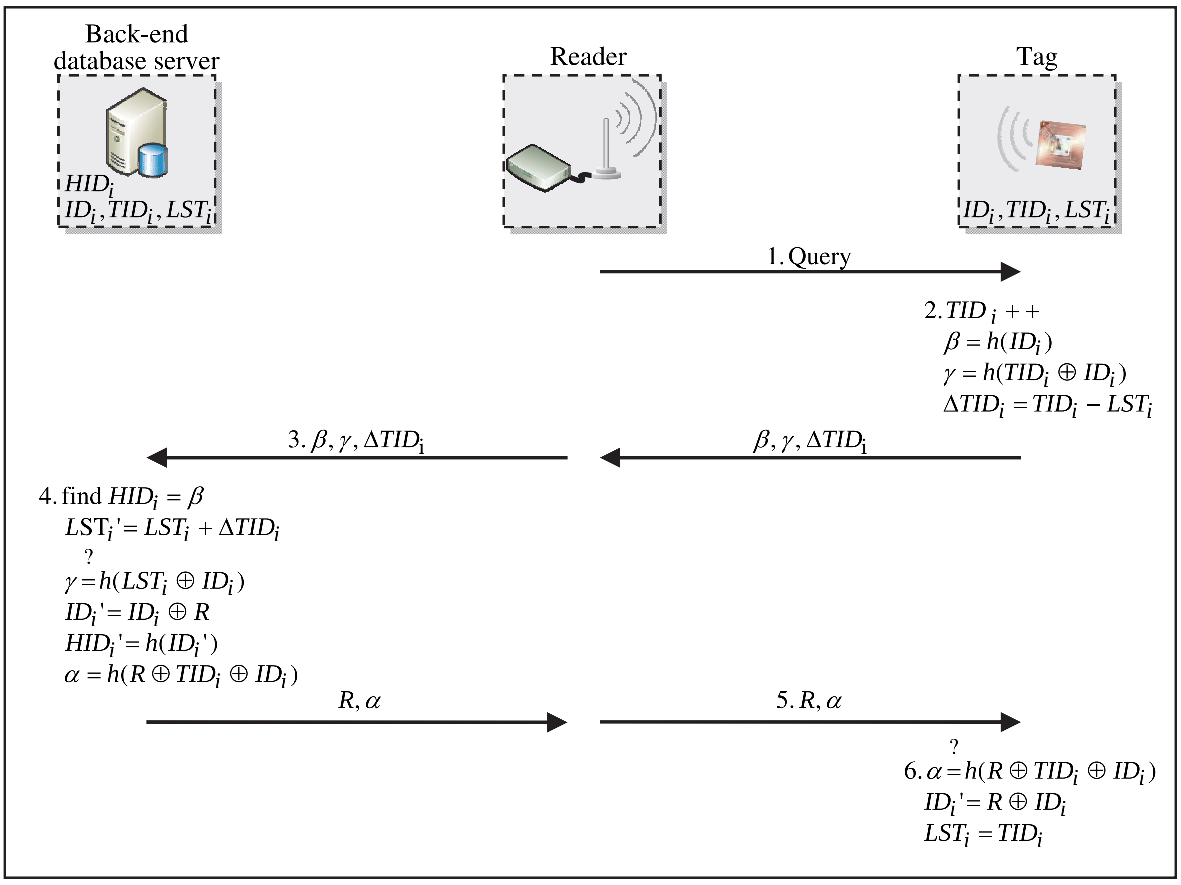

Back-end database server
Reader
Tag
HID_i
ID_i, TID_i, LST_i
ID_i, TID_i, LST_i
1. Query
2. TID_i ++
$\beta = h(ID_i)$
$\gamma = h(TID_i \oplus ID_i)$
$\Delta TID_i = TID_i - LST_i$
3. $\beta, \gamma, \Delta TID_i$
$\beta, \gamma, \Delta TID_i$
4. find $HID_i = \beta$
$LST_i' = LST_i + \Delta TID_i$
$\gamma \overset{?}{=} h(LST_i \oplus ID_i)$
$ID_i' = ID_i \oplus R$
$HID_i' = h(ID_i')$
$\alpha = h(R \oplus TID_i \oplus ID_i)$
R, α
5. R, α
6. $\alpha \overset{?}{=} h(R \oplus TID_i \oplus ID_i)$
$ID_i' = R \oplus ID_i$
$LST_i = TID_i$

Fig. 17. Henrici & Muller's hash-based ID variation scheme

transaction number LST_i are issued by the back-end database server. As the tag is queried, the tag's transaction number TID_i is increased progressively and the message ($\beta = h(ID_i)$, $\gamma = h(TID_i \oplus ID_i)$, $\Delta TID_i = TID_i - LST_i$) is responded to the reader. If the reader is legal, it can ask the back-end database server to use $\beta = h(ID_i)$ identifying the tag. Then the back-end database server's response is the hash value $\alpha = h(R \oplus TID_i \oplus ID_i)$ generated by the transaction number TID_i, tag's identity ID_i, and a random number R. After the tag receives the correct hash value α from the reader, the tag's information can be accessed by the reader.

In this scheme, the tag updates its ID_i after each successful access. It seems to make the tag's response message $\beta = h(ID_i)$ not predictable to prevent the tracing of individual. However, the design of identity variation not really guarantees the location privacy. Fig. 18 shows the use-case diagram of this scheme's weaknesses. The adversary may interrogate a tag to get its response message $\beta = h(ID_i)$ and $\Delta TID_i = TID_i - LST_i$ for collecting to its own database. If $\Delta TID_i \geq 2$, it means the last transaction is not successful and the tag's identity ID_i is not updated. As the target tag's hash value $\beta = h(ID_i)$ once again collected, the adversary immediately realizes the target tag appeared.

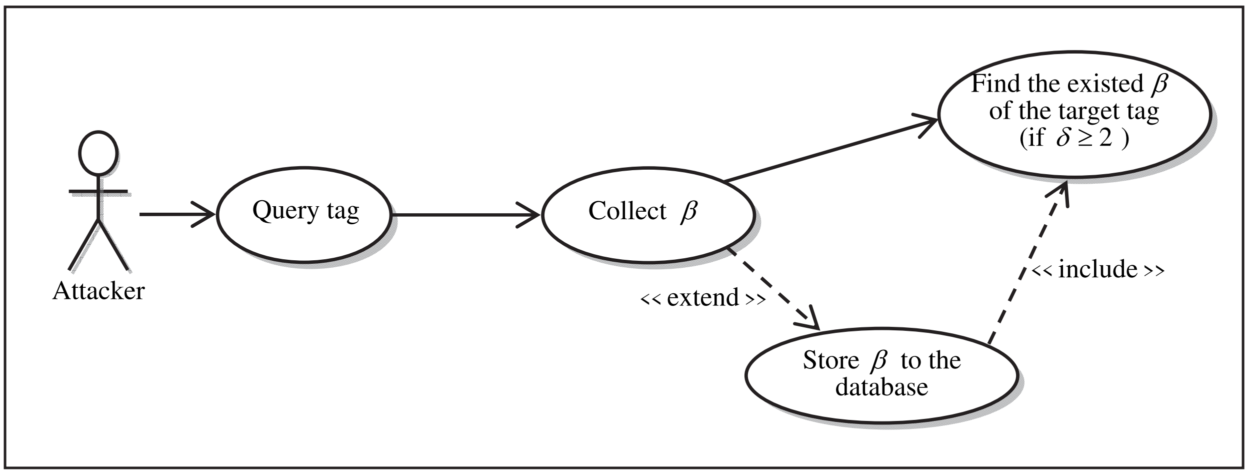

Attacker
Query tag
Collect β
Find the existed β of the target tag (if $\delta \geq 2$)
<< extend >>
<< include >>
Store β to the database

Fig. 18. The attack on Henrici & Muller's hash-based ID variation scheme

3.3.2 LCAP scheme

Lee et al. (2005) proposed a low-cost RFID authentication protocol (LCAP) (Lee et al., 2005), shown in Fig.19. A tag with initial ID_i is issued by the back-end database server. The back-end database server always maintains a previous-session record and a current-session record for a tag. Each record has the fields (*HaIDi*, *IDi*, *TDi*). *HaIDi* value is the hash value of *IDi* used for identifying or addressing the tag. *TDi* is used to link the previous-session record and the current-session record each other in order to synchronize the tag and the database in case of incompletion of the current session. As the reader tries to query the tag with a random number R, the tag emits a hash value $\beta = h(ID_i)$ and the left-half hash value $\alpha_L = f_L(h(ID_i \,||\, R))$. If the reader is legal, it can ask the back-end database server to use $\beta = h(ID_i)$ identifying the tag. Then the back-end database server's response is the right-half hash value $\alpha_R = f_R(h(ID_i \,||\, R))$. After the tag receives the correct right-half hash value α_R from the reader,the tag's information can be accessed by the reader.

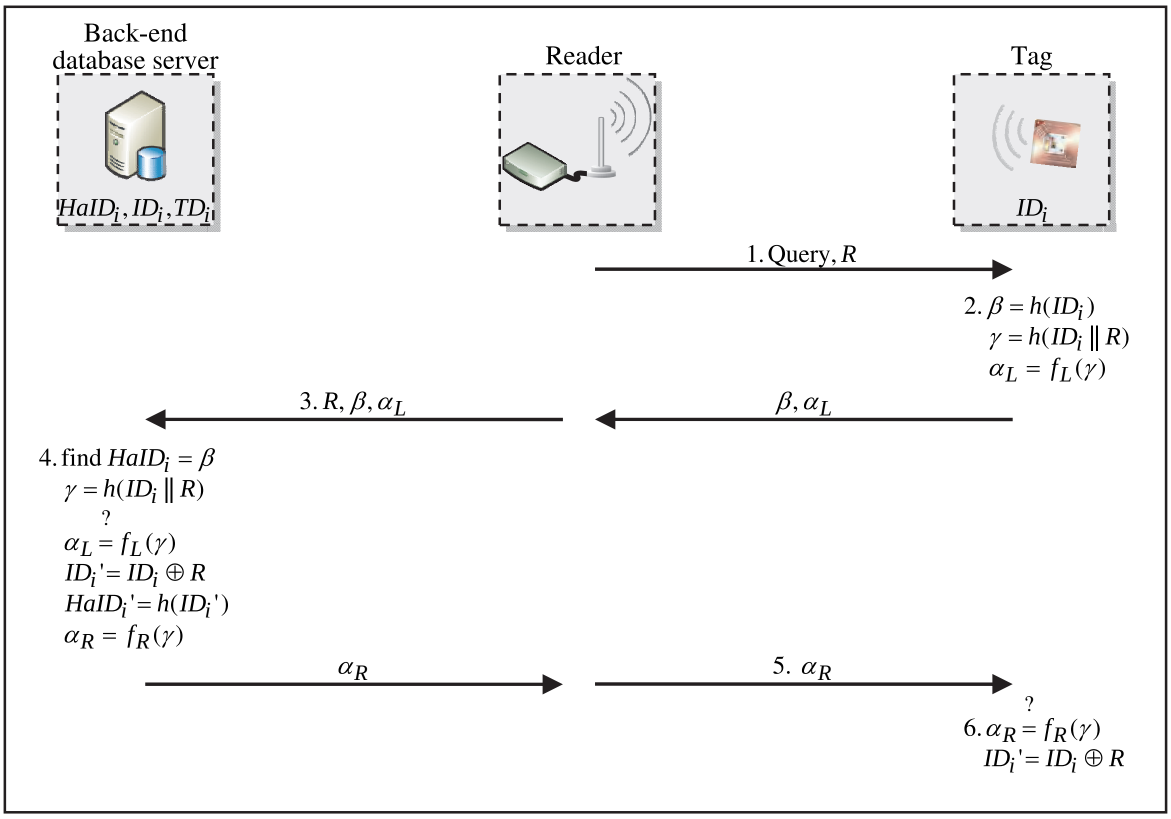


Fig. 19. LCAP scheme

In this scheme, the tag's identity ID_i is refreshed simultaneously by the tag and the back-end database server after each successful access. It seems to make the tag's response message $\beta = h(ID_i)$ not predictable to prevent the tracing of individual. However, the design of "dynamic" identity not really guarantees the location privacy. Fig. 20 shows the use-case diagram of this scheme's weaknesses. Gildas Avoine and Philippe Oechslim had described an attack based on refreshment avoidance (Lee et al., 2005). In the attack, an adversary always makes a tag unable to refresh its identity and hence can trace the tag. For example, the adversary interrogates all tags with the same number R to get the response message $\beta = h(ID_i)$ and the left-half hash value $\alpha_L = f_L(h(ID_i \,||\, R))$ for collecting to its own database. As the target tag's hash value $\beta = h(ID_i)$ once again collected, the adversary immediately realizes the target tag appeared.

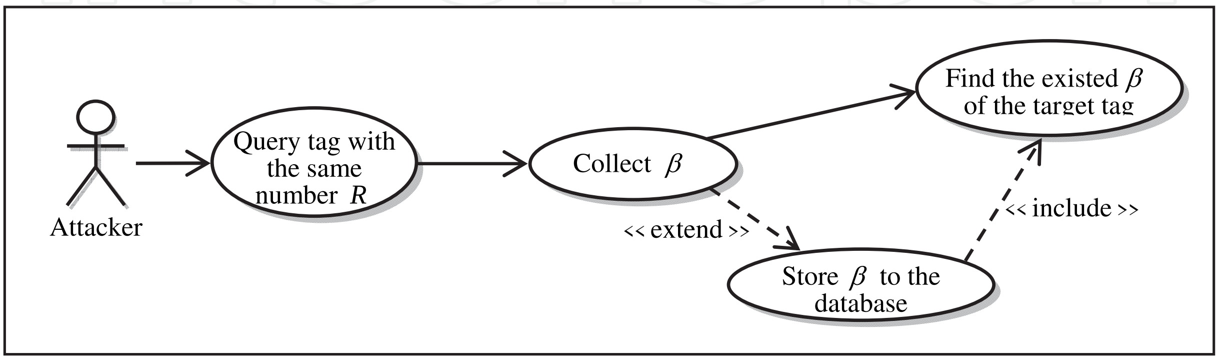

Attacker
Query tag with the same number R
Collect β
Find the existed β of the target tag
<< extend >>
<< include >>
Store β to the database

Fig. 20. The attack on LCAP

3.4 Tree-based approach

In the tree-based approach, each tag is not just assigned with a single key but associated with a unique leaf node. In fact, a sequence of keys from the root to the leaf node are defined for the associated tag. The tag's authentication response is performed by the sequence of keys such that it can be identified by the reader using a breadth-first search in the key tree. Based on the logarithmic complexity of tree-based key search, the tree-based identification is efficient to support a large scale system. (Bringer et al., 2008; Dimitriou, 2006; Lu et al., 2007; Molnar & Wagner , 2004; Molnar et al., 2005; Wang et al., 2007; Yeh et al., 2008)

3.4.1 Dimitriou's tree-based tag identification scheme

Dimitriou (2006) proposed a tree-based tag identification scheme (Dimitriou, 2006). Each edge is defined with a secret value Key_i . Key_i in the path from the root to the leaf node are hereby distributed to this tag. If the tree depth is d , each tag contains d keys. Fig. 21 shows a binary key tree with eight tags. For example, T_4 has keys k_4^1, k_4^2 and k_4^3.

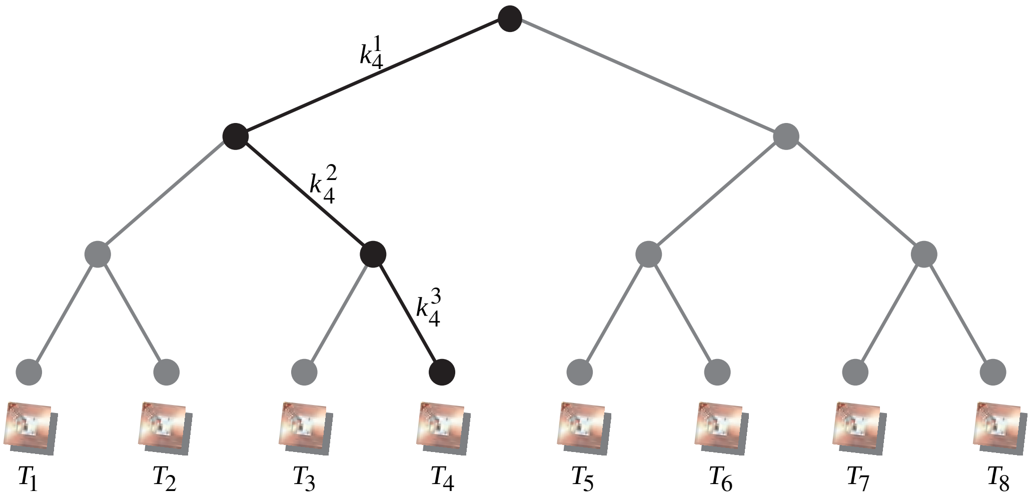


Fig. 21. A binary key tree with eight tags

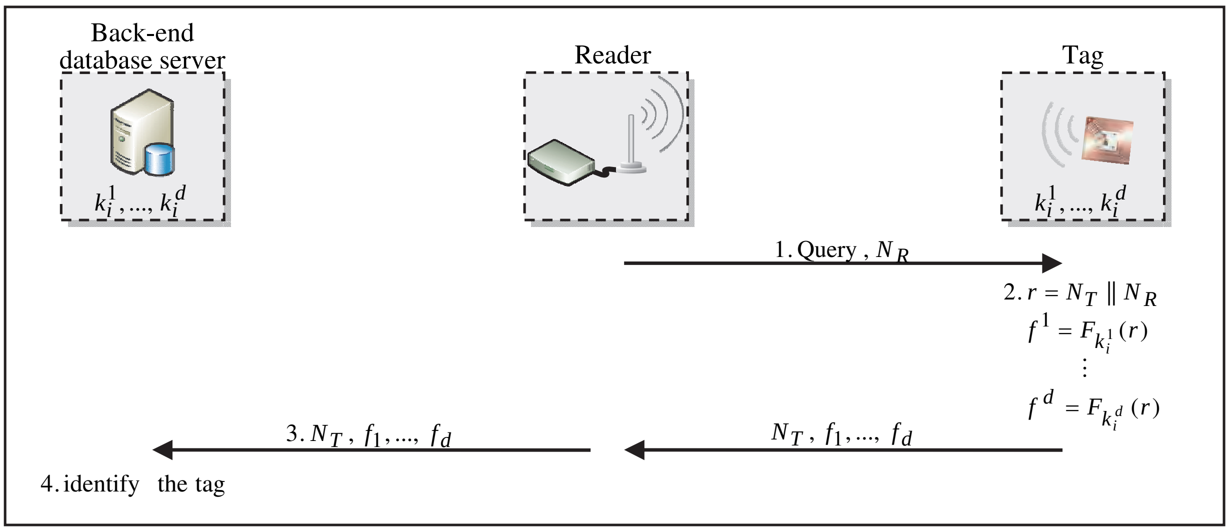


Fig. 22. Dimitriou's tree-based tag identification scheme

The procedure of Dimitriou's tree-based tag identification scheme is shown in Fig. 22. As the reader tries to query the tag with a random number N_R, the tag generates a random number N_T and computes the message ($f^1, f^2, \ldots, f^d$) by all its keys. The back-end database server has to find out the keys in the trees from the root to the leaf node for identifying the tag. If the path exists, the back-end database server regards the tag as a valid tag.

In this scheme, tag searching using the idea of the tree walking algorithm is efficient for the reader. However, it may not be afforded for low-cost tags without enough computing capability to generate the responses by the sequence of keys in a transaction.

3.4.2 Wang et al.'s tree-based authentication scheme

Wang et al.'s (2007) proposed a Storage-Aware Private Authentication protocol (SAPA) (Wang et al, 2007). This scheme uses a sparse tree structure to organize keys of all tags. In the tree, only the root and the leaf node store a key. Each tag T_i is arranged to a leaf node and has a key triple (k_h, k_m, k_r). k_h, is the key assigned to the root. k_r is the key assigned to the leaf node. k_m represents the path from the root to the leaf node which is expressed in 0 and 1. For example fig.23 shows a sparse binary tree of three levels, the key triple (k_h, k_m^2 and k_r^2) is assigned to T_2.

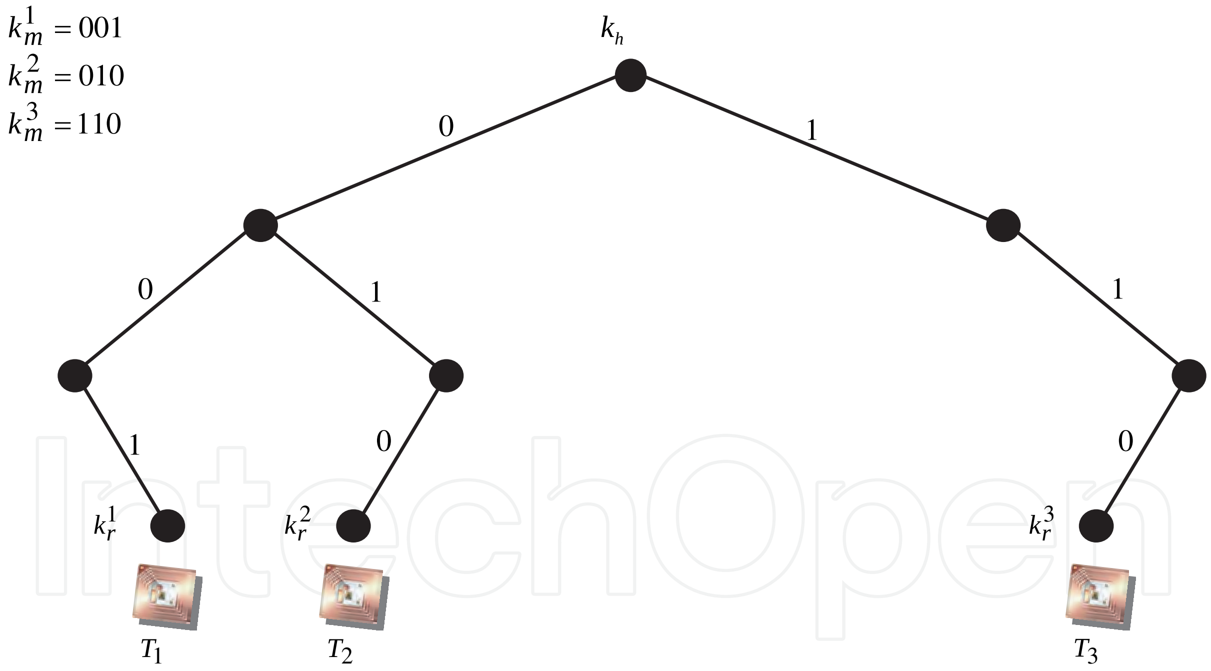


Fig. 23. A sparse binary tree of three levels

The procedure of Wang et al.'s tree-based authentication scheme is shown in Fig. 24. As the reader tries to query the tag with a random number r_1, the tag generates a random number r_2 and computes a sequence of hash chains ($M_0, M_1, \ldots, M_l, M_i$). Then the back-end database server first verifies the message M_0 to authenticate the tag. After, the back-end database server performs a recursive algorithm to identify the tag through the path.

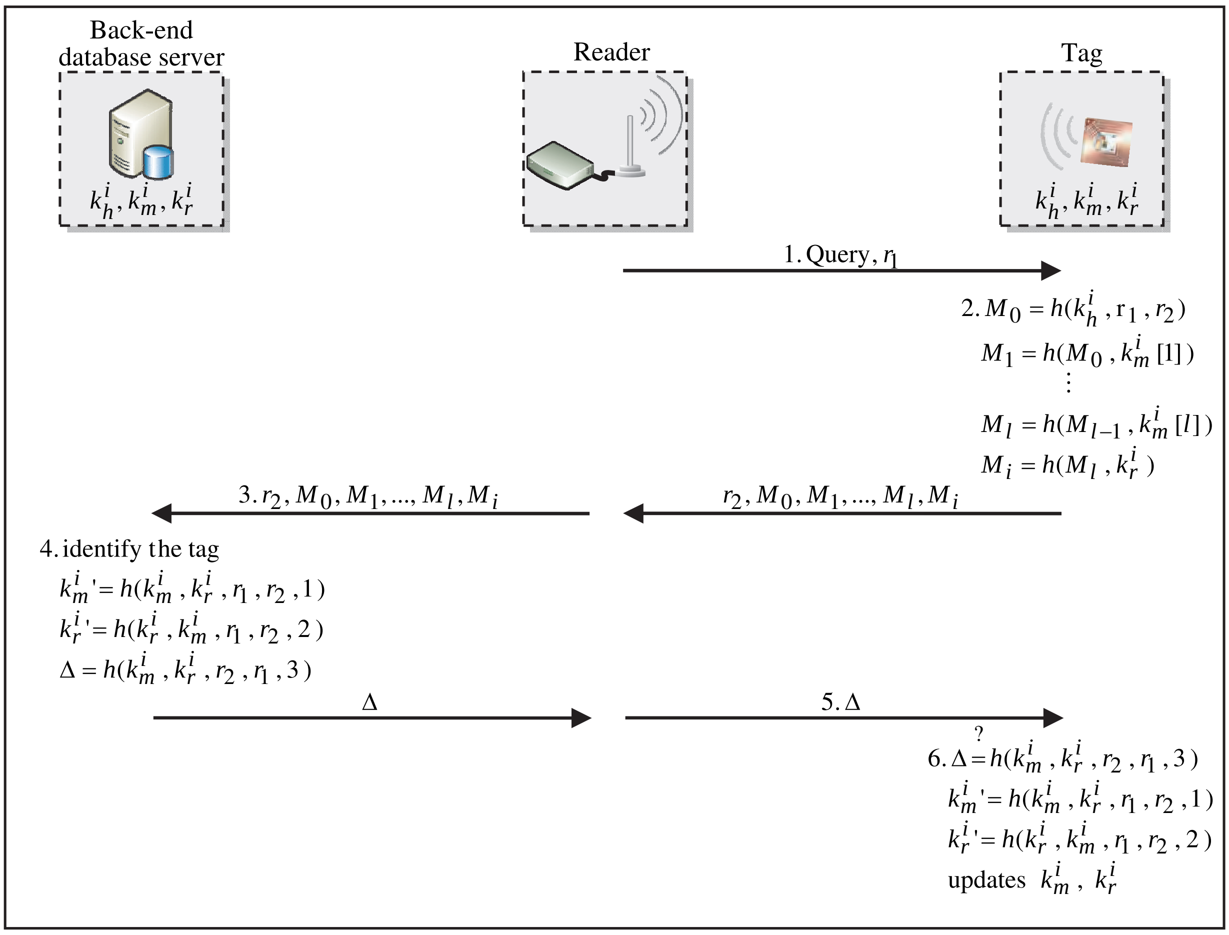

Back-end database server
Reader
Tag
k_h^i, k_m^i, k_r^i
k_h^i, k_m^i, k_r^i
1. Query, r_1
2. $M_0 = h(k_h^i, r_1, r_2)$
$M_1 = h(M_0, k_m^i[1])$
$\vdots$
$M_l = h(M_{l-1}, k_m^i[l])$
$M_i = h(M_l, k_r^i)$
$r_2, M_0, M_1, ..., M_l, M_i$
3. $r_2, M_0, M_1, ..., M_l, M_i$
4. identify the tag
$k_m^i{}' = h(k_m^i, k_r^i, r_1, r_2, 1)$
$k_r^i{}' = h(k_r^i, k_m^i, r_1, r_2, 2)$
$\Delta = h(k_m^i, k_r^i, r_2, r_1, 3)$
Δ
5. Δ
6. $\Delta \overset{?}{=} h(k_m^i, k_r^i, r_2, r_1, 3)$
$k_m^i{}' = h(k_m^i, k_r^i, r_1, r_2, 1)$
$k_r^i{}' = h(k_r^i, k_m^i, r_1, r_2, 2)$
updates k_m^i, k_r^i

Fig. 24. Wang et al.'s tree-based authentication scheme

In this scheme, both the tag and the back-end database server update key triple (k_h, k_m', k_r') for each successful authentication. It may cause a collision for the new path k_m' assigned to the tag. The asynchronous attack may happen as the adversary blocks Δ sent back to the tag. These drawbacks cause the scheme impractical.

3.5 Chen et al.'s indefinite-indexed approach

Chen et al. (2011) proposed the indefinite-indexed access control scheme (Chen et al., 2011), shown in Fig.25. As a tag is issued by the back-end database server, the $index_i$, Key_i and a square matrix ω are stored in the tag. The tag's serial number $index_i$ is specified as a pair of values (x_i, y_i) which can also be regarded as a coordinate. For the purpose of keeping the tag's location private, the serial number cannot be emitted directly. Infinite possibilities exist to select two un-parallel lines crossed on the coordinate. If the tag is allowed to freely determine the two un-parallel lines, it means $index_i$ can be represented randomly. The first line can be determined by the tag's serial number (x_i, y_i) and any point (x_1, y_1). Then the second point (x_2, y_2) can be randomly selected on this line. Later, the other two points (x_3, y_3) and (x_4, y_4) can also be determined similarly. The values of these four coordinates will be re-arranged into a matrix π and performs the matrix product $\pi \cdot \omega$ as the response for the reader. Therefore, only the back-end database server holds the inverse matrix of ω can obtain the matrix π and figure out the tag's serial number.

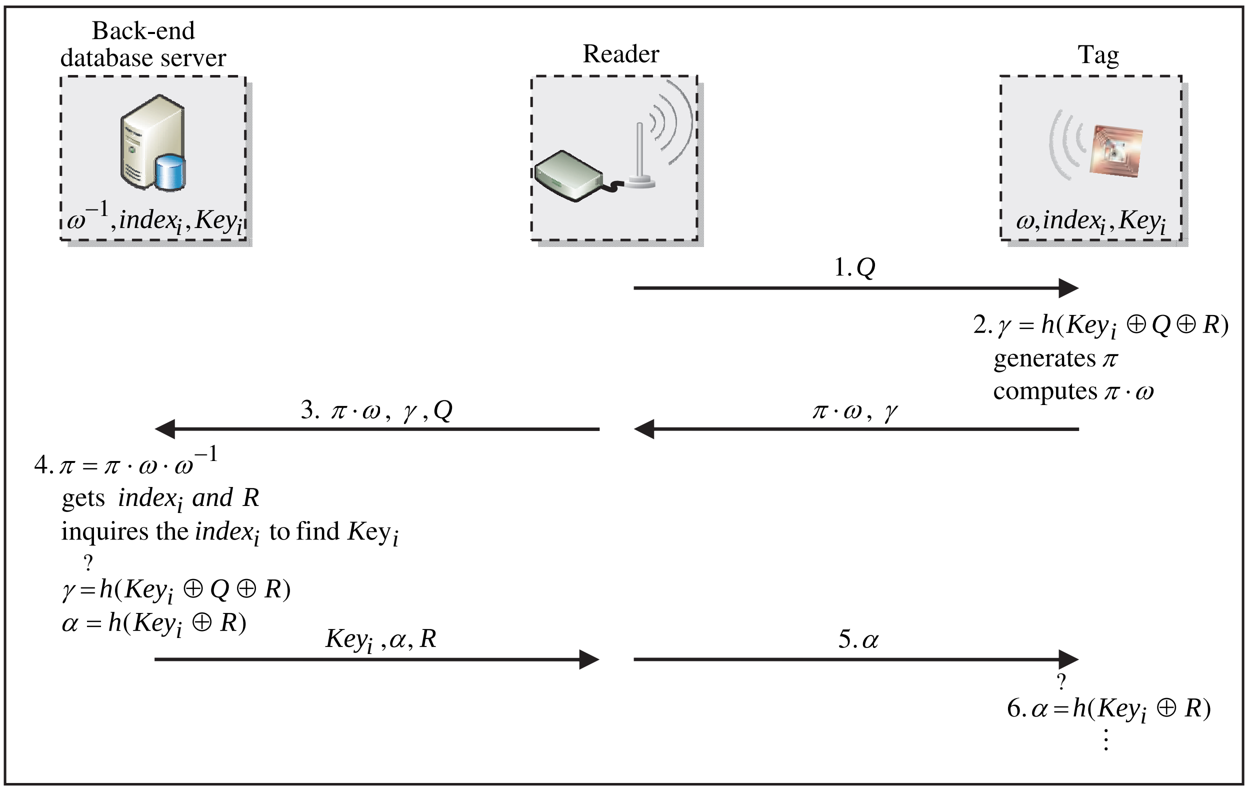

Back-end database server
Reader
Tag
$\omega^{-1}, index_i, Key_i$
$\omega, index_i, Key_i$
$1. Q$
$2. \gamma = h(Key_i \oplus Q \oplus R)$
generates π
computes $\pi \cdot \omega$
$3.\ \pi \cdot \omega,\ \gamma, Q$
$\pi \cdot \omega,\ \gamma$
$4. \pi = \pi \cdot \omega \cdot \omega^{-1}$
gets $index_i$ and R
inquires the $index_i$ to find Key_i
$\gamma \overset{?}{=} h(Key_i \oplus Q \oplus R)$
$\alpha = h(Key_i \oplus R)$
Key_i, α, R
$5. \alpha$
$6. \alpha \overset{?}{=} h(Key_i \oplus R)$
$\vdots$

Fig. 25. Chen's indefinite-indexed access control scheme

The motivation of this scheme is to make the tag's response message not predictable to prevent the tracing of individual. In other word, the tag's response message in each access cannot be recognized it is emitted by the same tag. In this scheme, the tag's serial number is regarded as a coordinate. Infinite possibilities exist to select two un-parallel lines crossed on the coordinate. Therefore, the tag's serial number can be represented differently in each access and not useful to identify the tag. Moreover, the other messages emitted between the tag and the reader are also randomized and not useful to trace the tag. Therefore, the tag's location privacy can be guaranteed. In addition, this scheme also guarantees mutual authentication and resists the man-in-the-middle attack, the spoofed reader attack, and the spoofed tag attack.

4. Conclusions

Modern RFID systems are creating a new era of ubiquitous information society. It allows almost everything to be uniquely numbered by embedding a RFID tag. Then the process automation efficiency and usability could be improved (Chang, 2005; Garfinkel et al., 2005). It allows objects to be scanned and identified without the need for visual or physical contact. However, due to the powerful tracking capability of RFID tag, it poses a potentially widespread threat to consumer privacy (McCullagh, 2003). In the world of RFID tags widespread deployment, anyone with an RFID reader can potentially discover individuals' informational preferences without their permission.

Without access control, anyone can read the information stored on current generation RFID tags. The static unique identifiers stored on tags can be traced for linking the tagged items to the individuals who carry the item. Therefore, security and privacy in RFID systems are an important aspect that needs particular attention. Current researches in RFID technology not just concentrate on the identification scheme. Secure and efficient authentication and access control mechanisms have received much attention in the proposed researches. This article examines the main privacy concerns: information leakage of a tag, traceability of the person and impersonation of a tag. The impersonation problem is always the first one to be analyzed and solved in each scheme. Otherwise, the adversary can collect the information sent by the tag and the adversary can try a spoofing or replay attack to impersonate a target tag. For further consideration, the disclosure of information arising during a transmission of data possibly reveals various personal details without awareness of the holder. Most of the proposed schemes were well designed to prevent the problem of tag's information leakage. However, most of the proposed schemes can not really avoid the problem of traceability. The adversary may try to distinguish whether the response is transmitted by the target tag or not. Once a link is established between the response and the target tag, the adversary can monitor the person's location. For those schemes analyzed in this article, state diagram and use-case diagram are used to figure out the schemes' weaknesses. Through this way, the security requirements in RFID applications can be clearly understood to know which mechanism actually brings which feature. We expect it is more beneficial those researchers as just devoting to the RFID security studies.

5. References

Auto-ID Center (2003). 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interference Specification: Recommended Standard, Version 1.0.0, Technical Report, Auto-ID Center.

Avoine G. (2004). Privacy Issues in RFID Banknote Protection Schemes, *in Proc. 6th Conference on Smart Card Research Advanced Application*, pp. 33–48.

Avoine G. & Oechslin P. (2005). A Scalable and Provably Secure Hash Based RFID Protocol, *2nd IEEE International Workshop on Pervasive Computing and Communication Security*, pp. 110-114.

Avoine G. & Oechslin P. (2005). *RFID Traceability: A Multilayer Problem, Financial Cryptography*.

Bringer J., Chabanne H. & Icart T. (2008). Improved Privacy of the Tree-Based Hash Protocols Using Physically Unclonable Function, *Proc. of the 6th International Conference on Security and Cryptography for Networks – SCN 2008*, pp. 77-91.

Cavoukian A. (2004). Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology, Information and Privacy Commissioner/Ontario.

Chang G.C. (2005). A Feasible Security Mechanism for Low Cost RFID Tags, *International Conference on Mobile Business*, pp. 675–677.

Chen Y.Y., Tsai M.L. & Jan J.K. (2011). The Design of RFID Access Control Protocol using the Strategy of Indefinite-Index and Challenge-Response, *Computer Communications*, Vol. 34, No. 3, pp. 250-256.

Chien H.Y. (2006). Secure Access Control Schemes for RFID Systems with Anonymity, *Proceedings of the 7th International Conference on Mobile Data Management (MDM 2006)*.

Dimitriou T. (2005). A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks, *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 59-66.

Dimitriou T. (2006). A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete, *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, Mar. 13-17.

Elgamal T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory, Vol. 31, pp. 469–472.

Fishin K., Roy S. & Jiang B. (2004). Some Methods for Privacy in RFID Communication, *in Proc. 1st Eur. Workshop on Security in Ad-hoc and Sensor Networks*.

Gao X., Xiang Z., Wang H., Shen J., Huang J. & Song S. (2004). 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.*

Garfinkel S.L., Juels A. & Pappu R. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions, *IEEE Security & Privacy*, pp. 34–43.

Golle P., Jakobsson M., Juels A. & Syverson P. (2004). Universal Re-encryption for Mixnets, *in Proc. RSA Conference - Cryptographers' Track (CTRSA)*, pp. 163–178.

Good N., Han J., Miles E., Molnar D., Mulligan D. & Quilter L. (2004). Radio Frequency Id and Privacy with Information Goods, *in Proc. Workshop on Privacy in the Electronic Society*, pp. 41-42.

Henrici D. & Muller P. (2004). Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 149-153, Mar.

Huang Y.C. (2009). Secure Access Control Scheme of RFID System Application, *Proceedings of the 2009 Fifth International Conference on Information Assurance and Security*, pp. 525-528.

Inoue S. & Yasuura H. (2003). RFID Privacy using User-Controllable Uniqueness, *in Proc. RFID Privacy Workshop*, Nov.

Inoue S., Konomi S. & Yasuura H. (2002). Privacy in the Digitally Named World with RFID Tags, *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing.*

Joaquin G.A., Guillermo N.A., Ana C. & Jean L. (2011). Secure and Scalable RFID Authentication Protocol, 5th International Workshop on Data Privacy Management and Autonomous Spontaneous Security, pp. 231-243.

Juels A. (2004). Minimalist Cryptography for Low-Cost RFID Tags, *Security in Communication Networks*, pp. 149-164.

Juels A. & Brainard J. (2004). Soft Blocking: Flexible Blocker Tags on The Cheap, *in Proc. Workshop on Privacy in the Electronic Society*, pp. 1–7.

Juels A. & Pappu R. (2003). Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, *in Proc. Financial Cryptography, Lecture Notes in Computer Science*, Vol. 2742, pp. 103-121.

Juels A., Rivest R.L. & Szydlo M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, *in Proc. 8th ACM International Conference on Computer Communication Security*, pp. 103–111.

Kinosita S., Hoshino F., Komuro T., Fujimura A. & Ohkubo M. (2003). Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection, *to appear in CSS 2003 in Japanese.*

Lee S.H., Asano T.Y. & Kim K.G. (2006). RFID Mutual Authentication Scheme Based on Synchronized Secret Information, *Symposium on Cryptography and Information Security*, January.

Lee S.M., Hwang Y.J., Lee D.H. & Lim J. I. (2005). Efficient Authentication for Low-Cost RFID Systems, *International Conference on Computational Science and its Applications - ICCSA 2005*, pp. 619-627.

Lu L., Han J., Hu L., Liu Y. & Ni L.M. (2007). Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems, *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, pp. 13-22, Mar. 19-23.

McCullagh D. (2003). RFID Tags: Big Brother in Small Packages, *CNET News*, http://news.com.com/2010-1069-980325.html.

Molnar D. & Wagner D. (2004). Privacy and Security in Library RFID: Issues, Practices, and Architectures, *Conference on Computer and Communications Security – CCS 2004*, pp. 210–219.

Molnar D., Soppera A. & Wagner D. (2005). A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags, *Selected Areas in Cryptography – SAC*, pp. 276-290, Aug..

Ni L.M., Liu Y., Lau Y.C., & Patil A. (2003). LANDMARC: Indoor Location Sensing Using Active RFID, *in Proceedings of IEEE PerCom*.

Ohkubo M., Suzuki K. & Kinoshita S. (2003). Cryptographic Approach to Privacy-Friendly Tag, *RFID Privacy Workshop*, MIT, MA, USA, November.

Osaka M., Takagi T., Yamazaki K. & Takahashi O. (2006). An Efficient and Secure RFID Security Method with Ownership Transfer, *2006 International Conference on Computational Intelligence and Security*, pp. 1090-1095, Nov. 3-6.

Pisarsky G.M. (2004). RFID Technology: An Analysis of Privacy and Security Issues, *20th Computer Science Seminar*, pp. 1–5.

Rhee K., Kwak J., Kim S. & Won D. (2005). Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment, *International Conference on Security in Pervasive Computing - SPC 2005*, pp. 70-84.

Robinson P. & Beigl M. (2003). Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments, *in Proceedings of SPC*.

Sabaragamu Koralalage K.H.S., Mohammed Reza S., Miura J., Goto Y., & Cheng J. (2007). POP Method: An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism, *Proceedings of the 2007 ACM Symposium on Applied Computing*, pp. 270-275, Mar. 11-15.

Sarma S.E.(2001). Towards The Five-Cent Tag, Technical Report, Auto-ID Center.

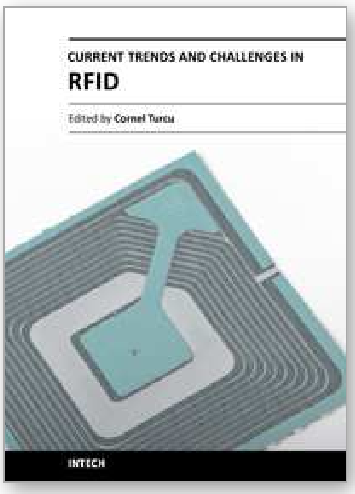
Sarma S.E., Weis S.A. & Engels D.W. (2002). Radio-Frequency Identification Systems, Workshop on Cryptographic Hardware and Embedded Systems – CHES’ 02, LNCS, Vol. 2523, pp. 454–469.

Sarma S.E., Weis S.A. & Engels D.W. (2003). RFID Systems and Security and Privacy Implications, *In Workshop on Cryptographic Hardware and Embedded Systems*, pp. 454-469.

Wang W., Li Y., Hu L. & Lu L. (2007). Storage-Awareness: RFID Private Authentication based on Sparse Tree, *Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)*, July 19.

Weis S., Sarma S., Rivest R. & Engels D. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *in 1st Intern. Conference on Security in Pervasive Computing (SPC)*, pp. 50-59, March.

Yeh K.H., Lo N.W. & Winata E. (2008). An Efficient Tree-Based Tag Identification Protocol for RFID Systems, *22nd International Conference on Advanced Information Networking and Applications – Workshops*, pp. 996-970, Mar. 25-28.



Current Trends and Challenges in RFID
Edited by Prof. Cornel Turcu

ISBN 978-953-307-356-9
Hard cover, 502 pages
Publisher InTech
Published online 20, July, 2011
Published in print edition July, 2011

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821