9

Privacy-enhanced RFID Tag Search System

Ji Young Chun[1], Jung Yeon Hwang[2] and Dong Hoon Lee[3]
[1]*Graduate School of Information Management and Security,Korea University*
[2]*Electronics and Telecommunications Research Institute (ETRI)*
Republic of Korea

1. Introduction

Radio frequency identification (RFID) technology is used to identify RFID-tagged objects automatically. An RFID system generally consists of three components: an RFID tag, an RFID reader, and a backend system. An RFID tag is a small device for identification, which is attached to or embedded in an object. It has an unique identifier and may optionally hold additional product information for the object. An RFID reader is a device used to interrogate RFID tags. It can be fixed or portable. It passes communication messages between an RFID tag and a backend system. A backend system stores and manages the online data which are associates with RFID tags. Since the communication between an RFID tag and an RFID reader occurs without optical line of sight, RFID tags can be read much longer and much faster than other automatic identification and data capture (AIDC) technologies such as Bar-codes and smartcards. Thanks to these advantages, RFID technology has various applications.

Fig. 1. RFID Tag Search System

Recently, RFID technology has been applied to many real-life applications such as asset management, supply chain, and product maintenance, etc. Especially, RFID tag search system

which can be used to find RFID-tagged objects is one of the promising applications of RFID technology. For example, this system can be used to search for missing children and find books in a library (See Fig. 1). This system also can be used to find and monitor an offender who has an electronic tag. Consider the situation which can easily happen in the library. Everyday librarians arrange books in order in its place. However, since they may be handled by many people, books are constantly misplaced on the shelves. When someone wants to borrow a book which is not checked out, if the book is not where it should be one must scan the entire shelves to find the misplaced book. Fortunately if the book is nearby, the search is quickly ended. Otherwise, one should do an exhaustive search. This is too time-consuming. If RFID tag search system is used in the library, one can efficiently find the misplaced book among extensive RFID-tagged books.

Although RFID technology provides various benefits because of its convenience, there is growing concern about RFID security and privacy. When someone holds RFID-tagged objects, attackers can discover his personal information which is stored in RFID tags and can track his movement using IDs of RFID tags. Besides these attacks, there are many security and privacy threats. Therefore, when we implement RFID technology, we should consider security and privacy threats. There are numerous researches focusing on RFID security and privacy issues (Burmester et al., 2008; Gilbert et al., 2008; Juels & Weis, 2005; Ohkubo et al., 2003; Paise & Vaudenay, 2008; Rotter, 2008; Rieback et al., 2006; Tsudik, 2006; Vaudenay, 2007). Recently, secure protocols for RFID tag search system are proposed for the first time (Tan et al., 2007; 2008). After that, various RFID tag search protocols have been proposed (Ahamed et al., 2008;a; Hoque et al., 2009; Won et al., 2008; Zuo, 2009). Even though these protocols are designed to enhance the security and privacy of RFID tag search system with its own requirements, there still exist vulnerabilities. Therefore, we first analyze the vulnerabilities of the previous works and then discuss the corresponding countermeasures.

The remainder of this chapter is organized as follows. We introduce RFID tag search system in Section 2 and classify some protocols which have been proposed in this area in Section 3. In Section 4, we point out the vulnerabilities of the previous works, and then analyze the security and privacy requirements of the RFID tag search system in Section 5. Finally, we conclude the chapter with future works in Section 6.

2. RFID Tag search system

In this section, we describe the RFID tag search system and the threat model in RFID systems. Before describing the threat model, we describe system configurations and the basic RFID tag search protocol to clarify the roles of three components in RFID tag search system. We then describe the threat model in RFID systems.

2.1 System configurations

RFID tag search system also consists of three components: an RFID tag, an RFID reader, and a backend system.

- RFID Tag: RFID tags are categorized into two groups, active and passive, according to whether they have their own battery or not. While an active tag has its own battery, a passive tag does not have an internal battery and passively obtain the operating power from an RFID reader. In RFID tag search system, it is reasonable that tags are assumed to be passive. Since tags are usually attached to cheap objects like books or goods, passive tags are more suitable

than rather expensive active tags in RFID tag search system. We assume that tags are passive in this chapter. It is known that the communication range of passive tags is $3m$ or less (OECD, 2007).

- RFID Reader: An RFID reader can interrogate RFID tags and transfer communication messages between an RFID tag and a backend system. It supplies the operating power to passive tags. To give enough operating power to passive tags, the signal strength of an RFID reader should be strong. Therefore, the communication range of an RFID reader is much stronger than that of a passive tag, it is about $100m$ (OECD, 2007). There are two kinds of RFID readers, fixed and portable. Fixed reader is installed where data capture is required and it sends and receives RFID tag data to a backend system through the wired networks (See Fig. 2). Portable reader which can be mounted in a mobile phone or personal digital assistant (PDA) uses the wireless networks to communicate with a backend system (See Fig. 3). Therefore, fixed reader can be assumed that it has a persistent connection with a backend system while a persistent connection between portable reader and a backend system cannot be guaranteed due to unstable wireless connection or distance limitation, etc.

- Backend System: A backend system stores and manages online data of RFID tags. It is assumed to be trusted and do not compromised.

Fig. 2. Fixed Reader

Fig. 3. Portable Reader

2.2 Basic RFID tag search protocol

RFID tag search is to find a particular RFID tag using an RFID reader. In more detail, an RFID reader can determine whether a particular tag exists nearby the RFID reader using RFID tag

search system. Next we present a simple protocol to realize 'RFID tag search'. This basic RFID tag search system operates as follows:

(1) $B \leftarrow R$	:	Search request about a particular tag
(2) $B \rightarrow R$	:	A tag identifier ID_j
(3) $R \rightarrow T^*$	:	ID_j
(4) T^*	:	Check $\mathsf{ID}^* = \mathsf{ID}_j$
(5) $R \leftarrow T_j$	:	Reply

Fig. 4. Basic RFID Tag Search Protocol

(1) When the reader R wants to find a particular tag, it sends a request message about a particular tag to the backend system B.

(2) The backend system B sends a tag identifier ID_j which the reader wants to find to the reader R.

(3) After receiving ID_j, the reader R broadcasts ID_j to find the tag.

(4) One of arbitrary tags T^* nearby the reader R replays when its own identifier is equal to the broadcasted identifier ID_j.

(5) If the reader receives the reply from the tag T_j, the reader R can know the existence of the tag T_j.

Despite the simplified structure for a tag search the above basic protocol does not have any considerations for RFID security and privacy problems. There exist various threats through malicious attacks in RFID systems. We should consider RFID security and privacy problems to use RFID tag search system in real-life.

2.3 Threat model

In this subsection, we describe various security and privacy threats in RFID systems and analyze the basic RFID tag search protocol in terms of these threats. An adversary can mount the following attacks.

- Eavesdropping Attack: An adversary can eavesdrop all the communication messages between an RFID reader and RFID tags. When a portable reader is used, an adversary can also eavesdrop all the communication messages between a portable reader and a backend system.

- Intercept Attack: An adversary can intercept the messages in transmission between RFID readers and RFID tags. If a message from a reader is intercepted, a tag cannot get this intercepted message.

- Replay Attack: An adversary can replay the messages which were previously eavesdropped or intercepted.

- Tampering Attack: An adversary can modify, add, and delete data stored in RFID tags.

- Physical Attack: An adversary can compromise RFID tags. Once tags are compromised physically, an adversary can know all the secret information stored in RFID tags. An adversary

can also do a physical attack to portable readers, since portable readers can be easily lost or stolen. However, a backend system and fixed readers are not compromised.

Using these attacks, an adversary threatens security and privacy in RFID systems as follows.

- Impersonation: An adversary can impersonate a legitimate tag or a legitimate reader. After an adversary intercepts valid messages from a legitimate tag/reader, she replays these intercepted messages to a legitimate reader/tag.

- Information Leakage: An adversary can identify a specific tag using eavesdropping attacks. This attack can breach the privacy of a tag holder.

- Tracking: An adversary can track the movements of an RFID-tagged object such as a tag or a portable reader using eavesdropping attacks.

- Cloning: An adversary can clone a specific tag using physical and tempering attacks. To make a clone tag, an adversary physically accesses the secret information of a tag, and then creates a fake tag which stores this secret information. Using this attack, the adversary can change an expensive product into a cheap one.

- Denial of Service (DoS): An adversary sends a large amount of requests to a backend system to disable the RFID tag search system. Under this attack, a backend system cannot respond to the request of readers.

- Desynchronization: An adversary can make a tag and a backend system/reader be desynchronized by intercepting communication messages. Once a desynchronization happens, a tag and a backend system/reader cannot communicate with each other any more.

In the basic RFID tag search protocol in Fig. 4 an adversary can eavesdrop all communication messages between R and T^*. An adversary can impersonate a legitimate tag T_j after eavesdropping the communication messages in step (3) and (5). An adversary can also impersonate a legitimate reader R just by replying identifier, ID_j. The basic protocol leaks the information of tags like IDs. This leads the privacy breaches of a tag holder. An adversary can know the sensitive information of a tag holder, such as what a tag holder has and what a tag holder wears. More serious problem of the basic protocol is location tracking. If an adversary constantly observes the replies of a particular tag, she can track the movements of this tag and also the movements of a tag holder. Another security problem is tag cloning since low-cost passive tags cannot be protected with a temper-proof mechanism. The basic protocol is vulnerable to DoS attacks. If a backend system is disabled because of DoS attacks, then R cannot get any tag identifier in step (1) and (2), and so the RFID tag search system cannot be available.
These threats are general threats in RFID systems. However, there may exist other threats to be considered especially in the RFID tag search system. For instance, in the RFID tag search system, it could be important information to an adversary whether an RFID reader finds a specific tag or not. This threat is restricted to the RFID tag search system. Therefore, to design secure protocols in the RFID tag search system, we need to identify threats which are restricted to the search system. We will analyze previous RFID tag search protocols in the next section and then identify threats in the RFID tag search system.

3. Classification of previous RFID tag search protocols

In this section, we classify previous RFID tag search protocols (Ahamed et al., 2008;a; Hoque et al., 2009; Tan et al., 2007; 2008; Won et al., 2008; Zuo, 2009) which are designed to overcome various threats in the previous section.

3.1 Criteria for classification

We classify previous RFID tag search protocols according to the following criteria which reflect fundamental design considerations.

1) Movement of Readers: What kinds of RFID readers are used? Fixed or Portable?
2) Secret Update: Does each tag update its own secret value after every session?
3) Response of Tags: Do all tags respond to the request of an RFID reader? or Does the specific tag respond to the request of an RFID reader while the others keep silent?
4) Reveal Reader ID: Does an RFID reader reveal its identifier without any manipulation?

We will describe each criterion in more detail.

3.1.1 Movement of readers

As we described in Section 2, fixed readers use wired networks while portable readers use wireless networks. Since portable readers are hardly assumed that they have a persistent connection with a backend system, the search protocol with portable readers should consider this situation when portable readers cannot connect to a backend system. Another problem is that portable readers are easily lost or stolen. Once the readers are compromised, all the secret information in readers are revealed. Therefore, the search protocol with portable readers should also consider this situation.

3.1.2 Secret update

When each tag updates its own secret value after every session, a backend system should update the secret value of this tag at the same time. In this case, synchronization between a tag and a backend system is important. If a tag and a backend system are desynchronized, then this tag cannot be searched any more. Secret update is necessary to be secure against a physical attack. If an adversary is assumed to be able to mount a physical attack, an adversary can get the secret information of a tag. After that, an adversary can trace the communication messages of the tag in previous sessions using the current secret value of a tag if each tag does not update its own secret value after every session in the search protocol. This means that the protocol does not provide forward secrecy.

3.1.3 Response of tags

In the RFID tag search protocol, if the specific tag which an RFID reader wants to find responds to the request of an RFID reader, an adversary can learn whether the reader finds the specific tag or not. However, if all the tags including the specific tag respond to the request of an RFID reader, an adversary cannot decide whether the reader finds the specific tag or not. Therefore, by adjusting the number of responses of tags, we can protect the privacy of an RFID reader holder. Beside this problem an adversary can trace a tag. If only a specific tag always responds to a particular message, by sending this particular message repeatedly to the tag, an adversary

can trace this tag. However, if all tags respond to a particular message, an adversary cannot trace the tag.

3.1.4 Reveal reader ID

This criterion is about whether an RFID reader reveals its own ID or not. This is only for the protocols using portable readers. Since fixed readers passively relay communication messages between tags and a backend system, tags do not have to know IDs of fixed readers. However, since portable readers should handle the situation that portable readers cannot connect to a backend system, they should store secret information of tags. Therefore, tags have to know IDs of portable readers to communicate with them. To let tags know an ID of a portable reader, a portable reader sends its own ID to tags. In some circumstance, a revealment of reader's ID is not desirable. If an RFID reader sends its own ID without any manipulation, an adversary can identify this reader and also trace the movement of the reader holder.

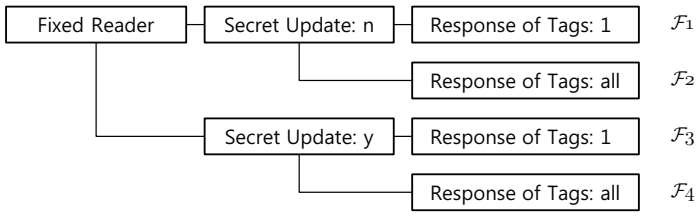


Fig. 5. Classification of Previous RFID Tag Search Protocols with Fixed Readers

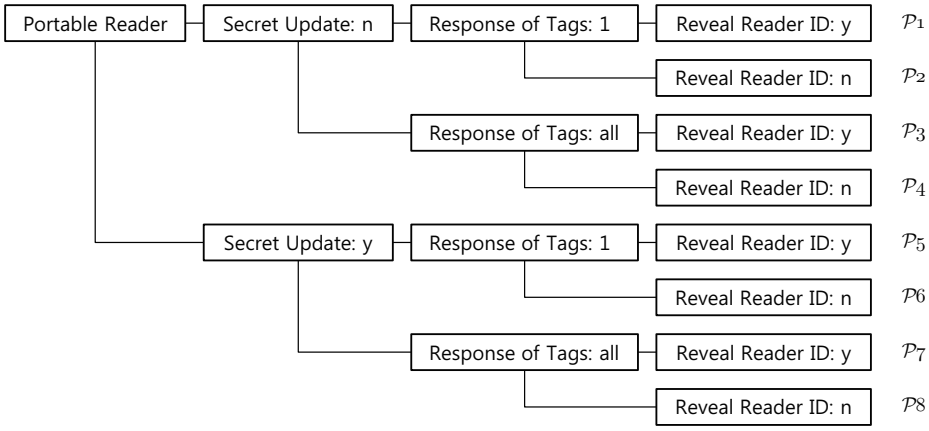


Fig. 6. Classification of Previous RFID Tag Search Protocols with Portable Readers

Fixed Reader		Portable Reader			
Secret Update: n	Secret Update: y	Secret Update: n			Secret Update: y
		3): 1		3): all	
		4): y	4): n	4): y	
$\mathcal{F}1$	$\mathcal{F}3$	$\mathcal{P}1$	$\mathcal{P}2$	$\mathcal{P}3$	$\mathcal{P}8$

Table 1. 6 kinds of previous protocols

3.2 Classification

The classification of RFID tag search protocols based on criteria is shown in Fig. 5 and 6. In Fig. 5 and 6, "Secret Update: y/n" means that each tag updates/does not update its own secret value after every session in RFID tag search protocol. When all tags respond to the request of an RFID reader, this is denoted by "Response of Tags: all". If the specific tag responds to the request of an RFID reader, this is denoted by "Response of Tags: 1". "Reveal Reader ID: y/n" means that the reader ID is revealed/is not revealed from the communication messages in RFID tag search protocol. This means that an RFID reader sends its own ID to tags without any manipulation. Based on these criteria, search protocols are divided into 12 categories. Protocols using fixed readers have 4 categories from $\mathcal{F}1$ to $\mathcal{F}4$ and protocols using portable readers have 8 categories from $\mathcal{P}1$ to $\mathcal{P}8$.
There are 6 kinds of previous protocols in (Ahamed et al., 2008;a; Hoque et al., 2009; Tan et al., 2007; 2008; Won et al., 2008; Zuo, 2009) (See Table 1). We select one protocol from each type as follows.

- Protocol 1 in category $\mathcal{F}1$: Protocol one in (Zuo, 2009)
- Protocol 2 in category $\mathcal{F}3$: Protocol three in (Zuo, 2009)
- Protocol 3 in category $\mathcal{P}1$: First protocol in (Tan et al., 2008)
- Protocol 4 in category $\mathcal{P}2$: Fourth protocol in (Won et al., 2008)
- Protocol 5 in category $\mathcal{P}3$: RFID search protocol in (Tan et al., 2008)
- Protocol 6 in category $\mathcal{P}8$: Enhanced search protocol in (Hoque et al., 2009)

In Table 1, 3) means the third criterion, Response of Tags and 4) means the fourth criterion, Reveal Reader ID.

4. Analysis of previous RFID tag search protocols

In this section, we analyze previously selected RFID tag search protocols. We do not present the protocols in detail but describe main features and drawbacks.

4.1 Protocol 1 in $\mathcal{F}_1$

In (Zuo, 2009), there is no mention about the movement of readers. However in the Protocol 1 disconnection of an RFID reader is not considered. This is why we classify Protocol 1 as $\mathcal{F}1$. Since tags do not update their secret information, Protocol 1 does not provide forward secrecy. That is, an adversary can trace the movement of a tag T_i in the previous sessions using compromised secret information k_i and id_i of a tag T_i. The secret information can be obtained through physical attacks. If an adversary stored all communication messages in the

Reader R		Tag T^*
calculate $F_{k_i}(id_i \oplus H(n_1))$		
send $\theta = F_{k_i}(id_i \oplus H(n_1))\|n_1$	$\xrightarrow{\theta}$	calculate $F_{k^*}(id^* \oplus H(n_1))$
		test if $F_{k^*}(id^* \oplus H(n_1)) = F_{k_i}(id_i \oplus H(n_1))$
		if so, calculate $H(id_i\|F_{k_i}(n_1))$
verify $H(id_i\|F_{k_i}(n_1))$	$\xleftarrow{\lambda}$	send $\lambda = H(id_i\|F_{k_i}(n_1))$

Fig. 7. Protocol 1

previous sessions, she can check whether a previous communication message (θ, λ) is from a tag T_i or not. After she gets n_1 from θ, she can check whether $\lambda = H(id_i\|F_{k_i}(n_1))$.
Besides the tracing problem through physical attacks, there is another tracing problem through replay attacks in the protocol. If an adversary repeatedly sends the same request θ, a tag T_i always sends same response λ. Therefore an adversary can trace a specific tag. If all tags except a tag T_i respond to the request of a reader with random values, then Protocol 1 becomes secure against replay attacks. This modified protocol can be classified as $\mathcal{F}2$.

4.2 Protocol 2 in $\mathcal{F}_3$

Reader R		Tag T^*
calculate $F_{k_i}(id_i \oplus H(n_1))\|F_{k_i^N}(id_i \oplus H(n_1))$		
send $\theta = F_{k_i}(id_i \oplus H(n_1))\|$		
$F_{k_i^N}(id_i \oplus H(n_1))\|n_1$	$\xrightarrow{\theta}$	calculate $F_{k^*}(id^* \oplus H(n_1))$
		test if $F_{k^*}(id^* \oplus H(n_1)) = F_{k_i}(id_i \oplus H(n_1))$
		or $F_{k^*}(id^* \oplus H(n_1)) = F_{k_i^N}(id_i \oplus H(n_1))$
		if either condition is true,
		calculate $H(id_i\|F_{k_i}(n_1))$
verify $H(id_i\|F_{k_i}(n_1))$	$\xleftarrow{\lambda}$	send $\lambda = H(id_i\|F_{k_i}(n_1))$
if k_i was used to verify λ		update $k_i \leftarrow H((k_i \gg L)\|n_1)$
update $k_i \leftarrow H((k_i \gg L)\|n_1)$		
if k_i^N was used to verify λ		
update $k_i \leftarrow H((k_i^N \gg L)\|n_1)$		

Fig. 8. Protocol 2

Protocol 2 is similar to Protocol 1, but each tag updates its own secret key after every session. Therefore this protocol satisfies forward secrecy. Since each tag's secret key is updated using a hash function like SHA-1, an adversary cannot know the previous secret key because of the one-wayness of a hash function. However, the protocol should consider the synchronization between a reader and a tag. If an adversary mounts an intercept attack to the communication message λ, a tag T_i and a reader are desynchronized. To be secure against intercept attacks, k_i^N is used for the situation when T_i updated the secret key but a reader did not update the

secret value. Therefore a reader should store two secret keys of a tag T_i, current key and next should-be key.
We can simply modify Protocol 2 to be secure against replay attacks using the same response technique in the Protocol 1. Then the modified protocol can be classified as $\mathcal{F}_4$.

4.3 Protocol 3 in $\mathcal{P}_1$

Reader R_j		Tag T^*
calculate $h(f(r_j, t_i)\|\|n_r) \oplus id_i$		
send $\theta = h(f(r_j, t_i)\|\|n_r) \oplus id_i\|\|n_r\|\|r_j$	$\xrightarrow{\theta}$	calculate $h(f(r_j, t^*)\|\|n_r)$
		if $id^* = h(f(r_j, t^*)\|\|n_r) \oplus h(f(r_j, t_i)\|\|n_r) \oplus id_i$
		calculate $h(f(r_j, t_i)\|\|n_t\|\|n_r) \oplus id_i$
verify $h(f(r_j, t_i)\|\|n_t\|\|n_r) \oplus id_i$	$\xleftarrow{\lambda}$	send $\lambda = h(f(r_j, t_i)\|\|n_t\|\|n_r) \oplus id_i\|\|n_t$

Fig. 9. Protocol 3

This protocol provides serverless RFID search which does not require a persistent connection to a backend system. A holder of a portable reader may go to a remote location where a portable reader cannot connect to a backend system to find an RFID-tagged object. To overcome this problem, if portable readers download all the secret information of tags, then portable readers can always find particular tags even if they cannot connect a backend server. However, this approach is not secure against physical attacks. Since portable readers are easily lost or stolen, an adversary can know all the secret information of tags. Therefore, in Protocol 3, a portable reader R_j stores the information $f(r_j, t_i)\|id_i$ of each tag T_i where r_j and id_i are IDs of a portable reader R_j and a tag T_i, respectively, and t_i is a secret key of a tag T_i. Even if an adversary gets the information $f(r_j, t_i)\|id_i$ of each tag T_i from compromised portable reader R_j, she cannot get a secret key t_i of a tag T_i due to the one-wayness of the function $f(\cdot, \cdot)$.
This protocol is vulnerable to replay attacks. By sending an eavesdropped message θ repeatedly, an adversary can trace a specific tag. The responses λ of a specific tag vary in every session, but a specific tag always sends a response to the same request.
In Protocol 3, a portable reader R_j sends its own identifier r_j. This breaches the privacy of the reader holder. An adversary can trace the movement of a reader holder just eavesdropping an ID of a portable reader. Since the signal strength of a reader is much stronger than that of a tag, an adversary can eavesdrop a message from a reader more easily. Therefore, revealing IDs of readers may be more serious than revealing IDs of tags in RFID tag search system, since tags are usually attacked to goods while portable readers are handled by people in RFID tag search system.

4.4 Protocol 4 in $\mathcal{P}_2$

This protocol does not reveal IDs of readers, hence this protocol protects the privacy of a reader holder. To let tags know an ID of a reader, the authors use a symmetric encryption (Feldhofer & Wolkerstorfer, 2007). By decrypting a received message with its own identifier, a tag can know an ID of a reader. This protocol is also secure against replay attacks. Since each tag stores *ltime* which is the last time to communicate with a reader, tags can check whether a received message is replayed or not using this value. If *ctime* from a received message is less than *ltime*, tags do not respond to the request of a reader.

Reader R_j		Tag T^*
generate $ctime$		
calculate $S_1 = E_{id_i}(ctime \oplus r_j)$		
calculate $S_2 = E_{ctime \oplus r_j}(E_{t_i}(r_j \oplus id_i))$		
send $\theta = ctime \| S_1 \| S_2$	$\xrightarrow{\theta}$	if $ctime > ltime$ then
		calculate $D_{ownid}(S_1) \oplus ctime = r_j$
		calculate $D_{ownt}(D_{ctime \oplus r_j}(S_2)) \oplus r_j = id_i$
		if $id_i = ownid$ then
		generate n_t
		calculate $S_3 = E_{ownid \oplus n_t}(S_1)$
verify $S_1 = D_{id_j \oplus n_t}(S_3)$	$\xleftarrow{\lambda}$	send $\lambda = S_3 \| n_t$
		$ltime \leftarrow ctime$

Fig. 10. Protocol 4

While $ctime$ is useful to defeat replay attacks, it can be used for malicious attacks. After stealing a portable reader, an adversary sends a request message θ with $ctime'$ which is much bigger than current time. A tag T_i accepts this message since $ctime'$ is much bigger than $ltime$. And then updates $ltime$ with $ctime'$. After that, a tag T_i cannot communicate with honest portable readers until $ctime'$.

4.5 Protocol 5 in $\mathcal{P}_3$

Reader R_j		Tag T^*
calculate $h(f(r_j, t_i) \| n_r) \oplus id_i$		
send $\theta = h(f(r_j, t_i) \| n_r) \oplus id_i \| n_r \| r_j$	$\xrightarrow{\theta}$	calculate $h(f(r_j, t^*) \| \| n_r)$
		if $id^* = h(f(r_j, t^*) \| \| n_r) \oplus h(f(r_j, t_i) \| \| n_r) \oplus id_i$
		calculate $\lambda = h(f(r_j, t_i) \| \| n_t) \oplus id_i$
	$\xleftarrow{\lambda}$	then send $\lambda = h(f(r_j, t_i) \| \| n_t) \oplus id_i \| n_t$
		else choose random number $rand$ and n_t
	$\xleftarrow{\lambda}$	then send $\lambda = rand \| n_t$
verify $h(f(r_j, t_i) \| \| n_t) \oplus id_i$		with the predefined probability

Fig. 11. Protocol 5

Protocol 5 improves Protocol 3 in that Protocol 5 is secure against replay attacks. Since all tags respond to the request of a reader with the predefined probability, an adversary cannot trace a specific tag using replay attacks. However, alike Protocol 3, Protocol 5 has the privacy problem that the protocol reveals the IDs of readers. And Protocol 3 and Protocol 5 do not provide forward secrecy for such a reason as mentioned in section 4.1.

Reader R_j		Tag T^*
calculate $\mathcal{P}(seed_{T_i})$		
send $n_i = \mathcal{P}(seed_{T_i})$	$\xrightarrow{n_i}$	calculate $a = \mathcal{P}(seed_{T*})$
		if $a = n_i$ then
		calculate $k = \mathcal{M}(seed_{T*})$, $x = \mathcal{P}(k)$
		and $seed_{T_i} = \mathcal{M}(k)$
	$\xleftarrow{x}$	send x
		else choose random number $rand$
calculate $s = \mathcal{M}(seed_{T_i})$ and $m = \mathcal{P}(s)$	$\xleftarrow{rand}$	send $rand$ with probability λ
if $m = x$, $seed_{T_i} = \mathcal{M}(s)$		

Fig. 12. Protocol 6

4.6 Protocol 6 in $\mathcal{P}_8$

Protocol 6 does not reveal an ID of a reader and provides forward secrecy. And the protocol is also secure against replay attacks since all tags respond to the request of a reader. However, Protocol 6 is not secure against intercept attacks. If an adversary intercepts a communication message x, a tag T_i and a reader R_j are desynchronized. After this session, they cannot communicate with each other. If Protocol 6 uses the technique in Protocol 2, Protocol 6 can become secure against intercept attacks.

Another drawback of the protocol is a storage cost. In the protocol, tags should store seeds as many as the number of portable readers. This can be a burden to resource constraint tags. This protocol is not designed for scalability. To use a new portable reader R', all tags should store a seed for the reader R'. This may take much time when huge tags are used in this search system.

5. Security & privacy requirements in RFID tag search system

We previously described threats in RFID systems in Section 2. These threats are still major threats in RFID tag search system. However, there may exist other threats to be considered in RFID tag search system. In this section, we analyze security and privacy requirements in RFID tag search system based on the analysis of previous protocols.

We first simply describe security and privacy requirements which are analyzed based on the threats in Section 2.

1) Authentication: A backend system and a portable reader must be convinced that tags who communicate with them are legitimate. If authentication is not provided in the protocol, an adversary can impersonate a legitimate tag using malicious attacks such as intercept attacks and replay attacks.

2) Confidentiality: An adversary should not be able to extract any information from eavesdropped messages. If an RFID tag search protocol does not provide confidentiality, the protocol leaks secret information.

3) Anti-tracking: An adversary should not be able to trace the movements of RFID-tagged objects.

4) Anti-cloning: An adversary should not be able to make cloned tags.

5) Anti-DoS attacks: Even if an adversary mounts DoS attacks, an RFID tag search system should not be disabled.

6) Synchronization: Tags and a backend system/ a reader are always synchronized even if an adversary tries to break the synchronization.

To find a particular tag, both fixed reader and portable reader can be used. A fixed reader is installed at location where searches of RFID-tagged objects are required. Therefore a fixed reader can find a specific tag that is nearby a fixed reader. For example, to cover all area in a library, 15 fixed readers are needed (See Fig. 13). However portable reader provides more flexible searches. To find a particular tag, a user just moves around with a portable reader.

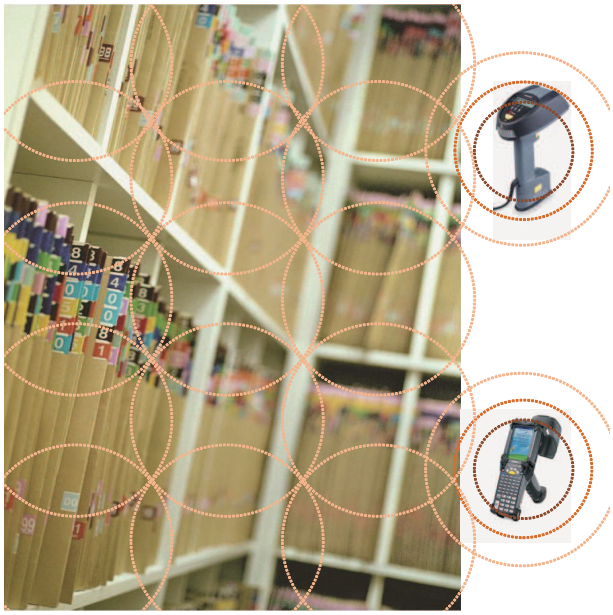


Fig. 13. Fixed reader and Portable reader

When a portable reader is used in RFID tag search system, we should consider the privacy of an RFID reader holder. The communication range of a tag is $3m$, while the communication range of a reader is $100m$ (See fig. 14). The area where an adversary can eavesdrop a message from a tag is $9\pi m^2$ and the area where an adversary can eavesdrop a message from a reader is $10000\pi m^2$. Therefore, a message from a reader can be eavesdropped much easier than a message from a tag. Moreover, since tags usually are attached to goods in RFID tag search system while readers are handled by people, the privacy breaches of a portable reader can be more serious than that of a tag.

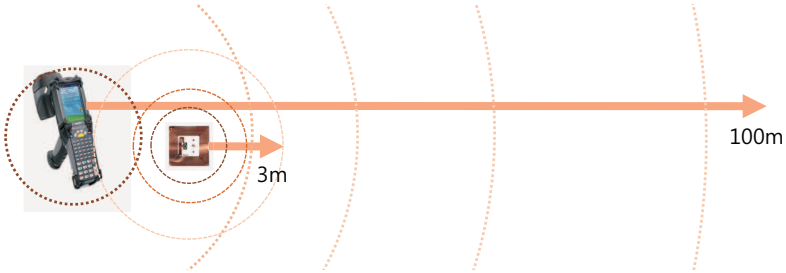


Fig. 14. Communication ranges of a tag and a reader

Requirements	P 1	P 2	P 3	P 4	P 5	P 6
1) Authentication	x	√	x	√	√	√
2) Confidentiality	√	√	√	√	√	√
3) Anti-tracking	x	√	x	√	√	√
4) Anti-cloning	x	x	x	x	x	x
5) Anti-DoS attacks	x	x	√	√	√	√
6) Synchronization	–	√	–	–	–	x
7) Reader ID privacy	–	–	x	√	x	√
8) Availability	–	–	√	√	√	√
9) Leakage Resilience	–	–	√	√	√	√
10) Protect response of tags	x	x	x	x	√	√

Table 2. Security and Privacy Properties

Besides the security and privacy requirements which are mentioned above, additionally required requirements in RFID tag search system are as follows.

7) Reader ID privacy: In an RFID tag search protocol, an ID of a reader should not be revealed. If a portable reader sends its own ID in every session, an adversary can identify the reader and trace a portable reader holder using this static value.

8) Availability: Even if a portable reader cannot connect to a backend system, an RFID reader should be able to find a particular tag which a reader wants to find.

9) Leakage Resilience: Even if a portable reader is compromised, an adversary should not be able to know secret information of tags.

10) Protect response of tags: If a particular tag responds to the request of a reader, an adversary can trace this tag using replay attacks. Therefore, an RFID search protocol protects the response of tags.

The security and privacy properties of selected 6 protocols are summarized in Table 2.
The only one requirement which is not satisfied by selected 6 protocols is anti-cloning. To design a secure protocol against cloning, physical unclonable functions (PUFs) are proposed (Tuyls & Batina, 2006). PUFs are used as a secure memory to store a secret key on a tag. It will

be an interesting work to design an RFID tag search protocol secure against cloning using the idea of PUFs.

6. Conclusion

In this chapter, we introduce privacy-enhanced RFID tag search system. After describing the threat model in RFID systems, we classify previous RFID tag search protocols which are designed to overcome various threats. And we analyze these protocols and draw security and privacy requirements in RFID tag search system based on the analysis. Our analysis is helpful to researchers who want to design secure protocols in RFID tag search system. Our future work is to improve some protocols which have drawbacks in 6 selected protocols.

7. References

Ahamed, S.I.; Rahman, F.; Hoque, E.; Kawsar, F. & Nakajima, T. (2008). S3PR: Secure Serverless Search Protocols for RFID, *Proceedings of Information Security and Assurance(ISA)*, pp. 187-192, Apr. 2008.

Ahamed, S.I.; Rahman, F.; Hoque, E.; Kawsar, F. & Nakajima, T. (2008) Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol, *International Journal of Security and Its Applications*, Vol. 2, No. 4, pp. 57-66, Oct. 2008.

Burmester, M.; Medeiros, B. & Motta, R. (2008) Provably Secure Grouping-Proofs for RFID Tags, *Proceedings of CARDIS*, LNCS 5189, pp. 176-190, Sep. 2008.

Feldhofer, M. & Wolkerstorfer, J. (2007) Strong crypto for RFID tags-A comparison of low-power hardware implementations, *Proceedings of IEEE International Symposium on Circuits and Systems(ISCAS)*, pp. 1839-1842, May. 2007.

Gilbert, H.; Robshaw, M. & Seurin, Y. (2008) HB ♯: Increasing the Security and Efficiency of HB+, *Proceedings of Advances in Cryptology - EUROCRYPT*, LNCS 4965, pp. 361-378, Apr. 2008.

Hoque, Md.E.; Rahman, F.; Ahamed, S.I. & Park, J.H. (2009) Enhancing Privacy and Security of RFID System with Serverless Authentication and Search Protocols in Pervasive Environments, *Proceedings of Wireless Personal Communications*, pp. 1-15, Jul. 2009.

Juels, A. & Weis, S.A. (2005) Authenticating Pervasive Devices with Human Protocols, *Proceedings of Advances in Cryptology - Crypto*, LNCS 3621, pp. 293-308, Aug. 2005.

Ohkubo, M.; Suzuki, K. & Kinoshita, S. (2003) Cryptographic Approach to "Privacy-Friendly" Tags,*RFID Privacy Workshop*, Nov. 2003.

Paise, R. & Vaudenay, S. (2008) Mutual authentication in RFID: security and privacy, *Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, pp. 292-299, Mar. 2008.

Rotter, P. (2008) A Framework for Assessing RFID System Security and Privacy Risks, *IEEE Pervasive Computing*, Vol. 7, No. 2, pp. 70-77, Apr. 2008.

Rieback, M.R.; Crispo, B. & Tanenbaum, A.S. (2006) The Evolution of RFID Security, *IEEE Pervasive Computing*, Vol. 5, No. 1, pp. 62-69, Jan. 2006.

Tuyls, P. & Batina, L. (2006) RFID-tags for Anti-counterfeiting, *Proceedings of CT-RSA*, LNCS 3860, pp. 115-131, Feb. 2006.

Tsudik, G. (2006) YA-TRAP: Yet Another Trivial RFID Authentication Protocol, *Proceedings of Pervasive Computing and Communications(PerCom) Workshops*, pp. 640-643, Mar. 2006.

Tan, C.; Sheng, B. & Li, Q. (2007) Serverless Search and Authentication Protocols for RFID, *Proceedings of Pervasive Computing and Communications(PerCom) Workshops*, pp. 3-12, Mar. 2007.

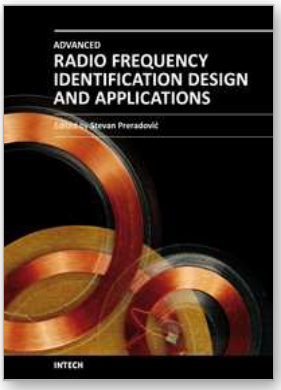
Tan, C.; Sheng, B. & Li, Q. (2008) Secure and Serverless RFID Authentication and Search Protocols, *Proceedings of IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1400-1407, Apr. 2008.

Vaudenay, S. (2007) On Privacy Models for RFID, *Proceedings of Advances in Cryptology - ASIACRYPT*, LNCS 4833, pp. 68-87, Mar. 2007.

Won, T.Y.; Chun, J.Y. & Lee, D.H. (2008) Strong Authentication Protocol for Secure RFID Tag Search Without Help of Central Database, *Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Vol. 2, pp. 153-158, Dec. 2008.

OECD (2007) Radio Frequency Identification (RFID): A Focus on Information Security and Privacy, OECD Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)9/FINAL, 70 pages, Jan. 2008.

Zuo, Y. (2009) Secure and private search protocols for RFID systems, *Information System Frontier*, Vol. 0, pp. 0-0, August. 2009.



Advanced Radio Frequency Identification Design and Applications

Edited by Dr Stevan Preradovic

ISBN 978-953-307-168-8
Hard cover, 282 pages
Publisher InTech
Published online 22, March, 2011
Published in print edition March, 2011

Radio Frequency Identification (RFID) is a modern wireless data transmission and reception technique for applications including automatic identification, asset tracking and security surveillance. This book focuses on the advances in RFID tag antenna and ASIC design, novel chipless RFID tag design, security protocol enhancements along with some novel applications of RFID.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Ji Young Chun, Jung Yeon Hwang and Dong Hoon Lee (2011). Privacy-enhanced RFID Tag Search System, Advanced Radio Frequency Identification Design and Applications, Dr Stevan Preradovic (Ed.), ISBN: 978-953-307-168-8, InTech, Available from: http://www.intechopen.com/books/advanced-radio-frequency-identification-design-and-applications/privacy-enhanced-rfid-tag-search-system

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