Vulnerabilities and Improvements on HRAP\textsuperscript{+}, a Hash-Based RFID Authentication Protocol

Seyed Mohammad Alavi\textsuperscript{1}, Behzad Abdolmaleki\textsuperscript{2}, and Karim Baghery\textsuperscript{3}

\textsuperscript{1} Imam Hossein Comprehensive University
Tehran, Iran
malavi@ihu.ac.ir

\textsuperscript{2} Information Systems and Security Lab (ISSL), Sharif University of Technology
Tehran, Iran
b.abdolmaleki.ir@ieee.org

\textsuperscript{3} Information Systems and Security Lab (ISSL), Sharif University of Technology
Tehran, Iran
k.baghery.1988@ieee.org

Abstract
In the last decade, Radio Frequency Identification (RFID) systems are employed in many authentications and identifications applications. In RFID systems, in order to provide secure authentication between RFID users, different authentication protocols proposed. In 2011, Cho et al. proposed a hash-based mutual RFID authentication protocol (HRAP). They claimed that HRAP protocol provides secure communication between RFID users and also it can provide users privacy. In that year, Habibi et al. investigated the security and privacy of HRAP protocol and showed that HRAP protocol has some weaknesses. Then, Habibi et al. proposed an improved version of HRAP protocol (HRAP\textsuperscript{+}) that eliminates all weaknesses of HRAP protocol. In this study, we cryptanalyze the HRAP\textsuperscript{+} protocol and we show that there are some flaws in HRAP\textsuperscript{+} protocol still. It is shown that, an attacker can perform tag impersonation, server impersonation, and replay attacks with success probability greater than $\frac{1}{4}$. Then, in order to omit all mentioned weaknesses, we propose an improved version of HRAP\textsuperscript{+} protocol. Security analysis shows that the improved protocol can improve the performance of HRAP\textsuperscript{+} protocol. In addition, we compare the security of the proposed protocol with some hash-based protocols that proposed recently.

Keywords: RFID authentication protocols, HRAP\textsuperscript{+} protocol, Security, Impersonation Attack.

1. Introduction
RFID systems are increasingly becoming part of our daily life. In many of our daily routines, without realizing it, we use RFID technology that use radio waves for automatic identification applications [1]. RFID technology also is used in different objects for different applications. Mainly, RFID systems consist of three main parts including Tag, Reader and Back-end-server or Database (Shown in Fig. 1). The data included in RFID tags that often are identification numbers, can be collected by the wireless reader. Also the reader can perform some logic processors and change the content of RFID tags. The third part of RFID systems that contains all secret information of tags, is back-end server or database. The reader located between the tags and the back-end server and exchanges data between them. In each run of RFID system, the database performs some certification and authentication processes and provides access to the data [2]. In some applications, communication channels between the readers and the database is insecure [3]. But in some cases, communication channels between the readers and the database is secure [4].

Due to nature of wireless communication between tags and readers, these channels can be eavesdropped by an adversary. As a results, although these systems provide many useful services, they can dangerous for security and the privacy of end-users. In the last few years, in order to protect RFID users against different security and privacy attacks
and provide secure communication between them, different
RFID authentication protocols have been proposed [5-10].
Although, all proposed protocols have been presented to
provide security and privacy of end-users, in some cases it
is shown that the proposed protocols have some weaknesses
and suffer from various attacks. So in order to increase the
security and privacy of the proposed protocols, lots of liter-
ature focused in cryptanalyze of RFID authentication pro-
tocols [5-14].

In 2011, in order to provide secure communication for
RFID users, Cho et al. proposed a hash-based mutual RFID
authentication protocol [5] which referred as HRAP proto-
col in this paper. In HRAP protocol, communication chan-
nel between the reader and the database is secure. Cho et al.
analyzed the security and the privacy of HRAP protocol and
claimed that their protocol can provide security and privacy
of RFID users. In that year, Habibi et al. [6] cryptanalyzed
HRAP protocol and showed that still the security and the
privacy of HRAP protocol has some problems and is not
secure against desynchronization attack, traceability and
backward traceability attacks. Then, Habibi et al. applied
some changes in the structure of tag message (M1) and pro-
posed an improved version of HRAP protocol (HRAP+).
Habibi et al. present some security and privacy analysis for
HRAP+ protocols and claimed that HRAP+ protocol elimi-
nates all weaknesses of HRAP protocol and is resistance
against various attacks.

In this study, we cryptanalyze the HRAP+ protocol and
we show that although Habibi et al. tried to omit all weak-
nesses of HRAP protocol, still HRAP+ protocol has some
security problems and is vulnerable against tag impersona-
tion, server/reader impersonation and replay attacks. In the
HRAP+ protocol, the structure of RID has a problem that
makes it vulnerable against the mentioned attacks. In this
paper, it is shown that how an attacker can use this weak-
ness and impersonate the tag, the back-end server or the
reader. Mentioned attacks are based on an assumption that
is reasonable in many cases. Due to this assumption, the
success probability of mentioned attacks is greater than \( \frac{1}{4} \)
that are given in the section 3 with more details.

Furthermore, in order to increase the performance of
HRAP+ protocol and provide security and privacy of RFID
users, we propose an improved version of HRAP+ protocol.
We analyze the security of the proposed protocol and we
show that with our modifications all weaknesses of HRAP+
protocol removed. Also we compare the security of pro-
posed protocol with some hash-based protocols that pro-
posed recently. Our comparisons, show that the proposed
protocol has sufficient security and privacy and is resistance
against all attacks.

The rest of paper is organized as follows: HRAP+ protocol
is introduced in section 2. In section 3, some attacks on
HRAP+ protocol presented. In section 4, we apply some
changes in HRAP+ protocol and propose an improved ver-
sion of it. The security of proposed protocol is analyzed in
section 5, and it is shown that all weaknesses of HRAP+
protocol are omitted. Also in this section the security anal-
ysis of proposed protocol are compared with some similar
protocols that are hash-based and proposed in recent years.
Finally, we conclude this paper in section 6.

---

<table>
<thead>
<tr>
<th>Server / Reader ( (ID_{old}, S_{old}, ID_{new}, S_{new}) )</th>
<th>Tag ( (ID_i, S_j) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each tuple of ((ID_{old}, S_{old})) and ((ID_{new}, S_{new}))</td>
<td>Generates ( R_i^l ) Randomly</td>
</tr>
<tr>
<td>Generates ( \beta ) and obtains ( R_i^l ) and ( RID_i )</td>
<td>( \text{RID}<em>i = (R_i^l \mod S_j + 1)</em>{10-47} )( \mod (R_i^l + S_j - R_i^l \mod S_j)_{48-95} )</td>
</tr>
<tr>
<td>Verify ( \alpha_i \equiv h(ID_{old}^l \oplus R_i^l \oplus R_i^l \oplus RID_i) )</td>
<td>( \alpha_i = h(ID_i^l \oplus R_i^l \oplus R_i^l \oplus RID_i)<em>{48-95} \mod S_j</em>{10-47} )</td>
</tr>
<tr>
<td>Calculates ( \theta = h(\beta_i \parallel \text{RID}_i) ) and sends it to the tag and updates its secret values as follows:</td>
<td>( \theta \equiv h(\beta_i \parallel \text{RID}_i) )</td>
</tr>
<tr>
<td>( \text{If ID} = ID_{new} )</td>
<td>If ( (\theta = h(\beta_i \parallel \text{RID}_i)) ) server is legitimate and the tag updates:</td>
</tr>
<tr>
<td>( S_{old} \leftarrow S_{new} \leftarrow h(S_{new} \parallel \text{RID}_i) )</td>
<td>( S_j \leftarrow h(S_j \parallel \text{RID}_i) )</td>
</tr>
<tr>
<td>( ID_{old} \leftarrow ID_{new} \leftarrow h(ID_{new} \parallel S_j) )</td>
<td>( ID_{i+1} \leftarrow h(ID_i \parallel S_j) )</td>
</tr>
</tbody>
</table>

**Fig. 2.** The HRAP+ protocol [6].
2. The HRAP+ Protocol

In [6], Habibi et al. proposed an improved version (HRAP+) of HRAP protocol that proposed by Cho et al. in [5]. HRAP+ protocol is similar to HRAP protocol and consists of three phases. The structure of HRAP+ protocol is illustrated in Fig. 2. The notation that are used in HRAP+ protocol are provided in Table 1.

Table 1. The Notations of HRAP+ Protocol

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_j$</td>
<td>The communications key shared by server and tag</td>
</tr>
<tr>
<td>$ID_k$</td>
<td>The group identification code of the $k$th tag</td>
</tr>
<tr>
<td>$R_t$</td>
<td>A random number</td>
</tr>
<tr>
<td>$h(.)$</td>
<td>Hash function</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>Concatenation operation</td>
</tr>
<tr>
<td>A $\oplus$ B</td>
<td>Message A is XORed with message B</td>
</tr>
<tr>
<td>A $\neq$ B</td>
<td>Compare whether A is equal to B or not</td>
</tr>
</tbody>
</table>

3. Security Analysis of HRAP+ Protocol

In this section, the security of HRAP+ protocol is analyzed. It is shown that security of HRAP+ protocol has some weaknesses and does not resist against tag impersonation, reader impersonation and replay attacks. All attacks performed with two assumptions and the success probability of attacks are greater than $\frac{1}{2}$ that in the rest of paper will be explained with more details.

According to the authentication phase of HRAP+ protocol, the value of $RID$ is defined as follows,

$$R_{\text{ID}} = (R_t - R_t \mod S_j + 1)_{[0:47]} \| (R_t + S_j - R_t \mod S_j)_{[48:95]}$$

(1)

now if $R_t < S_j$, the value of $R_{\text{ID}}$ in (1) can be rewritten as follows,

$$R_{\text{ID}} = (R_t - R_t + 1)_{[0:47]} \| (R_t + S_j - R_t)_{[48:95]}$$

(2)

Note that, when $R_t < S_j$, $R_t \mod S_j = R_t$.

3.1 Tag Impersonation Attack

This attack can be performed in two phases as follows.

**Learning phase:** In round $i$th of protocol, the attacker eavesdrops exchanged data between the tag and the server and obtains $R_t^i$, $R_t^i \oplus \beta$ and $\alpha$.

**Attack phase:** In round $(i+1)$th of protocol, when the server send a request message $R_{\text{ID}}^{i+1}$, the attacker impersonate the tag and responds with $\alpha$ and $R_t^i \oplus \beta \oplus R_t^i \oplus R_{\text{ID}}^{i+1}$ to the server. Then, the server performs following operations,

- For each tuple of $(ID_k, S_i)$, the server generates $\beta$ and obtains $R_t^{i+1} = R_t^i \oplus R_t^i \oplus R_{\text{ID}}^{i+1}$ and $R_{\text{ID}}^{i+1}$.
- Then the server uses the values $ID_k^i, R_t^{i+1}, R_{\text{ID}}^{i+1}$ and $R_{\text{ID}}^{i+1}$ and checks that $\alpha = h(ID_k^i \oplus R_t^{i+1} \oplus R_{\text{ID}}^{i+1})$. According to mentioned assumptions $R_t^i < S_j$ and $R_t^{i+1} < S_j$, we can write $R_{\text{ID}}^{i+1} = (1)_{[0:47]} \| (S_j)_{[48:95]} = R_{\text{ID}}^i$.
- Since $R_{\text{ID}}^{i+1} = R_{\text{ID}}^i$, the server authenticates the attacker as a legitimate tag.

**Proof:**

$$h(ID_k^i \oplus R_t^{i+1} \oplus R_{\text{ID}}^{i+1}) = h(ID_k^i \oplus R_t^{i+1} \oplus R_t^i \oplus R_{\text{ID}}^{i+1})$$

$$= h(ID_k^i \oplus R_t^i \oplus R_t^i \oplus R_{\text{ID}}^{i+1}) = \alpha$$

(3)

**Lemma 1:** For two numbers $\lambda$ and $\mu$ that are random numbers from set $\chi = \{0, 1, ..., 2^n - 1\}$ and $\mu > 1$, the probability of inequality $\lambda < \mu$ is greater than $\frac{1}{2}$.

**Proof:** Provided in appendix.

**Lemma 2:** For three numbers $\lambda$, $\mu$ and $\kappa$ that are random numbers from set $\chi = \{0, 1, ..., 2^n - 1\}$ and $\mu > 1$, the probability of inequality $\lambda \oplus \kappa < \mu$ is greater than $\frac{1}{2}$.

**Proof:** Provided in appendix.

According to the Lemma 1 and Lemma 2, the inequalities $R_t^i < S_j$ and $R_t^{i+1} < S_j$ hold with probability greater than $\frac{1}{2}$. Therefore, this attack will be successful with probability greater than $\frac{1}{4}$.

3.2 Server Impersonation and Reply Attacks

In this section, we aim to show that in HRAP+ protocol, an attacker can perform replay attack and impersonate the server. This attack can be summarized as follows,

- Firstly, the attacker eavesdrops first session of protocol and obtains $h(\beta \parallel R_{\text{ID}}^i)$. Also in this session, the attacker blocks third phase of protocol (transmit message from the server to the tag). As a result the tag does not update its secret values.
- Now, the attacker acts as a legitimate server and sends a random number $R_{\text{ID}}^i$ to the target tag.

Copyright (c) 2014 Advances in Computer Science: an International Journal. All Rights Reserved.
In response, the tag generates a random number \( R_i^{t+1} \) and calculates \( R_i^{t+1} \oplus \beta_i + 1 = h(ID_i^{[48-95]} \| S_j) \), then sends them to the attacker.

Then, the attacker sends eavesdropped message \( h(\beta_i \| RID_i) \) to the target tag.

Since the target does not receive its secret values, \( \beta_i = h(ID_i^{[48-95]} \| S_j) \). Using assumptions \( R_i^t < S_j \) and \( R_i^{t+1} < S_j \), it can be asserted that \( RID_i + 1 = (1)_{[0-47]} \| (S_j)_{[48-95]} = RID_i \). As a result \( h(\beta_i \| RID_i) = h(\beta_i \| RID_i) \) and the tag authenticates the attacker as a legitimate server.

In this attack also, according to the Lemma 1 and Lemma 2, the inequalities \( R_i^t < S_j \) and \( R_i^{t+1} < S_j \) hold with probability greater than \( \frac{1}{2} \), as a result the attacker will impersonate the server with probability greater than \( \frac{1}{4} \).

4. Improved Version of HRAP* Protocol

In the last section we showed that due to structure of \( RID_i = (R_i - R_i \mod S_j + 1)_{[0-47]} \| (R_i + S_j - R_i \mod S_j)_{[48-95]} \) an attacker could perform tag impersonation, reply attack, and server impersonation attack on HRAP* protocol. In this section, in order to omit mentioned weaknesses of HRAP* protocol, we propose an improved version of HRAP* protocol (Shown in Fig. 3). In the improved protocol, we changed the structure of \( RID_i \) indeed we protect \( RID_i \) via a one-way hash function. The improved protocol can be summarized in two phases as follows.

### 4.1 Initial Phase

In this phase, some secret values such as \( ID_k \) and \( S_j \) are stored in the specific tag. Also a one-way hash function is saved in all tags. In the server, for each specific tag, the values \( ID_{old}, ID_{new}, S_{old} \) and \( S_{new} \) are stored. Like as all tags, the server uses a one-way hash function in authentication procedures.

### 4.2 Authentication Phase

The authentication of proposed protocol is similar to HRAP* protocol and consists of three phases. This phase can be expressed as follows.

1. Like as HRAP* protocol, the server generates a random number \( R_i^t \) and sends it to the target tag.
2. Firstly, the tag generates random number \( R_i^t \). Then the tag uses \( R_i^t \) and calculates messages \( RID_i, \alpha_i \) and \( \beta_i \) as follows, and send \( \alpha_i \) and \( \beta_i \oplus R_i^t \) to the server.

\[
RID_i = h(R_i^t \oplus S_j)
\]

\[
\alpha_i = h(ID_k^t \oplus R_i^t \oplus R_i^t \oplus RID_i)
\]

\[
\beta_i = h(ID_k^{[48-95]} \| S_j)_{[0-47]}
\]

3. In order to authenticate the tag, the server performs following operations.

- For each tuple of \((ID_k, S_j)\), the server generates \( \beta \) and obtains \( R_i^t \) and \( RID_i \).
- Then the server uses the values \( ID_k^t, R_i^t, R_i^t \) and \( RID_i \) and checks that \( \alpha_i \oplus h(ID_k^t \oplus R_i^t \oplus R_i^t \oplus RID_i) \). If they were the same, the server computes \( \theta = h(\beta_i \| RID_i) \) and sends it to the target tag.

![Table 1](image)

**Table 1.** Improved version of HRAP* protocol.

---

**Fig. 3.** Improved version of HRAP* protocol.
5. Security Analysis of Proposed Protocol

In the last session we proposed an improved version of HRAP* protocol that removes mentioned weaknesses. It this subsection, we aim to analyze the security and the privacy of proposed protocol against various attacks.

5.1 Tag and Server Impersonations Attacks

In section 3, we showed that the main weakness of HRAP* protocol is the structure of $RID = (R_t - R_t \mod S_j + 1) \oplus (R_t + S_t - R_t \mod S_j)$ that makes HRAP* vulnerable against impersonation attacks. In proposed protocol, we changed the structure of $RID$ completely as follows,

$$RID_{new} = h(R_t \oplus S_j)$$ (4)

where $h(\cdot)$ is a one-way hash function. As it can be seen, with this changes, since the values of $R_t$ and $S_j$ change in each run of protocol, and the attacker does not access them directly, so the attacker cannot perform impersonation attacks.

5.2 Replay Attack

In this attack, the attacker tries to perform impersonation attacks to access exchanged messages, modify, and even delete them. In the proposed protocol, we applied some changes in the structure of exchanged data between the tag and the reader, indeed we changed $\beta = ID_k\oplus S_j$ to $h(ID_k\oplus S_j)$. Also, we changed the structure of secret value $RID$ that provided in (4). It can be seen that with these changes, the attacker cannot perform replay attack. Note that, with new values of $\beta$ and $RID$, if somehow the attacker obtains the random number $R_t$, he/she cannot extract secret keys $S_j$ and $ID_k$.

Furthermore, the structure of the proposed protocol is similar to HRAP* protocol, as a result the proposed protocol is secure against other attacks like HRAP* protocol. More analysis about other attacks provided in [6]. In order to more evaluation of the security and the privacy of the proposed protocol, in Table 2, the security and the privacy of proposed protocol compared with some hash-based protocols that proposed in the last few years. It can be seen, that with applied new changes in the proposed protocol, all weakness of HRAP* protocol have been omitted.

Table 2. Security Analysis of Some Hash-based Protocols

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Impers.</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
</tr>
<tr>
<td>Replay Attack</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Reader Impers.</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>DoS Attack</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>Traceability</td>
<td>$\times$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
<td>$\checkmark$</td>
</tr>
</tbody>
</table>

$\checkmark$: Secure $\times$: Insecure

6. Conclusions

In this paper, the security of HRAP* that is an improved version of HRAP protocol, is analyzed. We showed that although the designer of HRAP* tried to remove all weaknesses of HRAP protocol, still HRAP* protocol has some security problems and is not resist against tag impersonation, server impersonation and replay attacks. Mentioned attacks were based on an assumption that in many cases is reasonable. Due to this assumption, the success probability of mentioned attacks was greater than $\frac{1}{4}$. Furthermore, we presented an improved version of HRAP* protocol that removed weaknesses of HRAP* protocol. In order to more evaluation we analyzed the security of proposed protocol and also we compared the security analysis of the proposed protocol with some hash-based protocol that are in the same family and proposed recently.

Appendix

Proof of Lemma 1:

$A := \{(\lambda, \mu)|0 \leq \lambda \leq 2^n, 2 \leq \mu \leq 2^n, and \lambda < \mu\}$

$= \bigcup_{\mu=2}^{2^n-1}\{(\lambda, \mu)|\lambda = 0,1, \ldots, \mu\},$

and

$S := \{(\lambda, \mu)|0 \leq \lambda \leq 2^n, 2 \leq \mu \leq 2^n\}$

as a result,

$$Pr[(\lambda, \mu) \in A] = \frac{|A|}{|S|} = \frac{2^n(2^n + 1) - 3}{2^n(2^n - 2)}$$
\[
\frac{1}{2} + \frac{3}{2(2n - 2)} - \frac{3}{2n(2n - 2)} \geq \frac{1}{2}
\]

Proof of Lemma 2:

\[A_{(\lambda, \mu)} := \{(\lambda, \mu, \kappa) | \kappa = \lambda \oplus r \text{ where } 0 \leq \psi \leq \mu\}\]

Thus, for each \((\kappa, \lambda, \mu) \in A_{(\lambda, \mu)}\) there exist an \(\psi\) such that

\[\lambda \oplus \kappa = \lambda \oplus \lambda \oplus \psi = \psi \leq \mu\]

Now, let

\[A := \bigcup_{0 \leq \lambda \leq 2^n, 2 \leq \mu \leq 2^n} A_{(\lambda, \mu)}\]

Hence, for total numbers \((\lambda, \mu, \kappa)\) such that \(\lambda \oplus \kappa \leq \mu\) and \(\mu > 1\) we have

\[|A| = \sum_{\mu=2}^{2^n-1} \sum_{\lambda=0}^{2^{n-1}-1} |A_{(\lambda, \mu)}| = \sum_{\mu=2}^{2^n-1} \sum_{\lambda=0}^{2^{n-1}-1} (\mu + 1) = 2^n \sum_{\mu=2}^{2^n-1} (\mu + 1) = 2^n \left(\frac{2^n(2^n + 1)}{2} - 3\right)\]

On the other hand,

\[S := \{(\kappa, \lambda, \mu) | 0 \leq \lambda, \mu \leq 2^n - 1, 2 \leq \kappa \leq 2^n - 1\},\]

\[|S| = 2^n 2^n (2^n - 2)\]

Now, the probability that for random \(\kappa, \lambda\) and \(\mu > 1\), \(\lambda \oplus \mu < \kappa\) is equal with

\[Pr[(\kappa, \lambda, \mu) \in A] = \frac{|A|}{|S|} = \frac{1}{2} + \frac{3}{2(2^n - 2)} - \frac{3}{2n(2^n - 2)} > \frac{1}{2}\]

References


