LETTER

Cryptanalysis of a Handover Authentication Scheme Using Credentials Based on Chameleon Hashing

Eun-Jun YOON[†a)], Muhammad Khurram KHAN[††b)], *and* Kee-Young YOO[†c)], *Members*

SUMMARY Quite recently [IEEE Commu. Letters, Vol.14, No.1, 2010], Choi et al. proposed a handover authentication scheme using credentials based on chameleon hashing, claiming to provide several security features including Perfect Forward/Backward Secrecy (PFS/PBS). This paper examines the security of the scheme and shows that the scheme still fails to achieve PFS/PBS unlike their claims.

key words: *handover authentication, chameleon hashing, security, forward/backward secrecy*

1. Introduction

Developing a secure and efficient handover authentication scheme is a very important topic in various wireless networks such as WLAN, WiMAX, and 3GPP. For a secure handover, when a Mobile Node (MN) moves from the current Attachment Point (AP) to a new AP, it needs to authenticate securely the MN to protect itself from illegitimate users or attackers who are not paying for using the wireless networks. Moreover, a secure session key should also be established between the MN and the AP to protect user's communication data against passive and active attacks. For an efficient handover, it needs to provide low-cost cryptography operations and to minimize the communication overheads for a fast handover authentication.

In 2010, Choi et al. [1] proposed a handover authentication scheme using a credential based on chameleon hashing [2], claiming to have achieved robust key exchange and efficiency in terms of delay time and energy consumption. In the scheme, a short-term credential C, which is signed with a chameleon hash value $CH_y(m,r)$, is used for mutual authentication and authenticated ephemeral Diffie-Hellman (DH) key exchange [3] only between an MN and an AP. Choi et al. insisted that the proposed scheme can provide Perfect Forward/Backward Secrecy (PFS/PBS). PFS/PBS means that even if a long-term secret key is compromised at any point in time, it never reveals all the preceding and following session keys. Therefore, PFS/PBS are very important security requirements in DH key exchange. This paper examines the security of the Choi et al.'s scheme and shows that the scheme still fails to achieve PFS/PBS unlike their claims. In particular, knowing a long-term secret key of MN or AP, an adversary can simply compute the session Pairwise Master KEY (PMK) that is used to protect user data over the air interface.

2. Review of Choi et al.'s Scheme

This section reviews the handover authentication scheme using credentials based on chameleon hashing proposed by Choi et al. [1]. The scheme is composed of two phases: initial full authentication and handover authentication. Throughout the paper, notations are employed in Table 1.

2.1 Initial Full Authentication Phase

In this phase, an MN performs an initial full authentication with an AAA server during a bootstrapping procedure and receives a short-term credential C from the AAA server after every initial full authentication. The AAA server also issues the credential C to APs after every expiration time of the credential. Figure 1 depicts the initial full authentication phase, which works as follows. Assume that the AAA server sets up a RSA key pair and all nodes hold the RSA public key of it. The expression $(\bmod p)$ is omitted to simply represent.

Table 1 Notation used in protocol.

$h(\cdot)$	A strong one-way hash function.
ID_x	An identity of node x.
PK_x^-/PK_x^+	The private/public key of the traditional RSA.
T_{Exp}/T_{Curr}	The expiration/current time.
$\alpha(i)_x$	A secret (hashing) key of node x for finding collision and DH secret key, where $\alpha(i)_x \in Z_q^*$.
$r(i)_x$	A hash value $r(i)_x = h(g^{\alpha(i)_x}(\bmod p)\|T_{Curr})$ of node x, where $r(0)_x \in Z_q^*$.
$m(i)_x$	A random value computed by the equation $m(0)_x + \alpha(0)_x r(0)_x = m(i)_x + \alpha(i)_x r(i)_x$, where $m(0)_x \in Z_q^*$.
$y(i)_x$	A public (hashing) key $y(i)_x = g^{\alpha(i)_x}(\bmod p)$.
$CH_y(m,r)$	A chameleon hash function $CH_y(m,r) = g^m y(i)^r$ $(\bmod p)$.
C_x	A signature value $Sign(CH_y(m,r)\|T_{Exp})$ of node x with the RSA private key of AAA server.

1. MN→AAA Server: $CH_{y(0)_{MN}}(m(0)_{MN}, r(0)_{MN})$

   After performing the initial full authentication (e.g.,

Manuscript received June 1, 2010.
Manuscript revised August 11, 2010.

[†] The authors are with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702–701, South Korea.

[††] The author is with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Kingdom of Saudi Arabia.

a) E-mail: ejyoon@knu.ac.kr
b) E-mail: mkhurram@ksu.edu.sa
c) E-mail: yook@knu.ac.kr

DOI: 10.1587/transinf.E93.D.3400

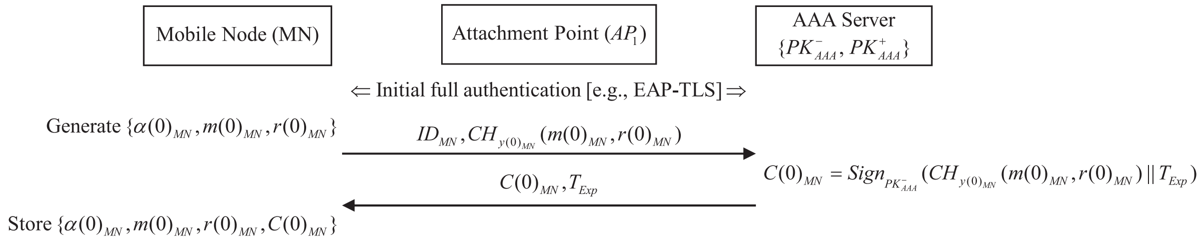
Mobile Node (MN)
Attachment Point (AP_1)
AAA Server $\{PK^-_{AAA}, PK^+_{AAA}\}$
⇐ Initial full authentication [e.g., EAP-TLS] ⇒
Generate $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}\}$
$ID_{MN}, CH_{y(0)_{MN}}(m(0)_{MN}, r(0)_{MN})$
$C(0)_{MN} = Sign_{PK^-_{AAA}}(CH_{y(0)_{MN}}(m(0)_{MN}, r(0)_{MN}) \| T_{Exp})$
$C(0)_{MN}, T_{Exp}$
Store $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}, C(0)_{MN}\}$

Fig. 1 The initial full authentication phase of Choi et al.'s scheme.

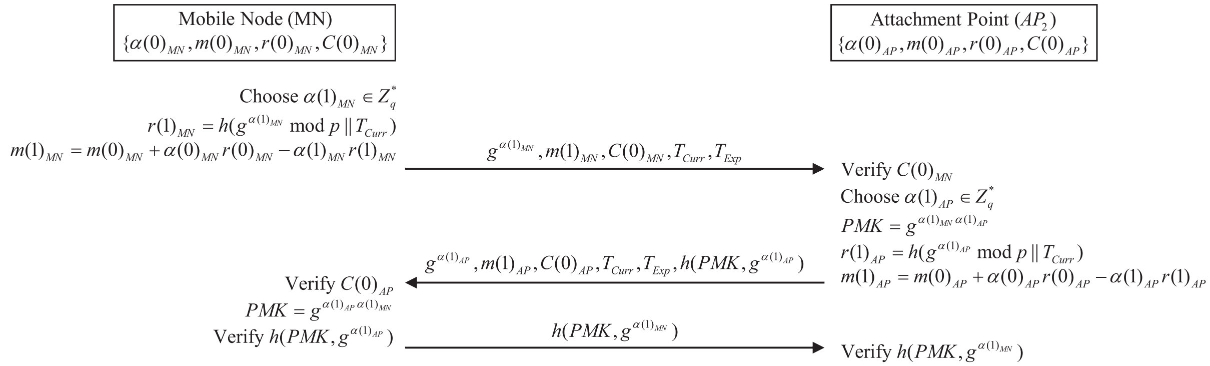
Mobile Node (MN) $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}, C(0)_{MN}\}$
Attachment Point (AP_2) $\{\alpha(0)_{AP}, m(0)_{AP}, r(0)_{AP}, C(0)_{AP}\}$
Choose $\alpha(1)_{MN} \in Z_q^*$
$r(1)_{MN} = h(g^{\alpha(1)_{MN}} \bmod p \| T_{Curr})$
$m(1)_{MN} = m(0)_{MN} + \alpha(0)_{MN} r(0)_{MN} - \alpha(1)_{MN} r(1)_{MN}$
$g^{\alpha(1)_{MN}}, m(1)_{MN}, C(0)_{MN}, T_{Curr}, T_{Exp}$
Verify $C(0)_{MN}$
Choose $\alpha(1)_{AP} \in Z_q^*$
$PMK = g^{\alpha(1)_{MN}\alpha(1)_{AP}}$
$r(1)_{AP} = h(g^{\alpha(1)_{AP}} \bmod p \| T_{Curr})$
$m(1)_{AP} = m(0)_{AP} + \alpha(0)_{AP} r(0)_{AP} - \alpha(1)_{AP} r(1)_{AP}$
$g^{\alpha(1)_{AP}}, m(1)_{AP}, C(0)_{AP}, T_{Curr}, T_{Exp}, h(PMK, g^{\alpha(1)_{AP}})$
Verify $C(0)_{AP}$
$PMK = g^{\alpha(1)_{AP}\alpha(1)_{MN}}$
Verify $h(PMK, g^{\alpha(1)_{AP}})$
$h(PMK, g^{\alpha(1)_{MN}})$
Verify $h(PMK, g^{\alpha(1)_{MN}})$

Fig. 2 The handover authentication phase of Choi et al.'s scheme.

EAP-TLS), MN itself generates chameleon hashing parameters $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}\}$, computes $CH_{y(0)_{MN}}(m(0)_{MN}, r(0)_{MN})$, and sends them to the AAA server.

2. AAA Server→MN: $C(0)_{MN}, T_{Exp}$

   AAA server computes the credential $C(0)_{MN}$ for the future handover authentication of the MN as follows.

   $$\begin{aligned} C(0)_{MN} &= Sign_{PK^-_{AAA}}(CH_{y(0)_{MN}}(m(0)_{MN}, r(0)_{MN}) \| T_{Exp}) \\ &= Sign_{PK^-_{AAA}}(g^{m(0)_{MN}} g^{\alpha(0)_{MN} r(0)_{MN}} \| T_{Exp}) \end{aligned}$$

   It then sends the message $C(0)_{MN}, T_{Exp}$ including the necessary data to the MN through a secure channel.

3. MN keeps the $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}\}$ as its secret key.

2.2 Handover Authentication Phase

When the MN moves into a new AP (AP$_2$), the handover authentication phase should be performed as shown in Fig. 2.

1. MN→AP$_2$: $g^{\alpha(1)_{MN}}, m(1)_{MN}, C(0)_{MN}, T_{Curr}, T_{Exp}$

   MN chooses a new random value $\alpha(1)_{MN} \in Z_q^*$ as its DH secret key and secret hashing key, and computes

   $$r(1)_{MN} = h(g^{\alpha(1)_{MN}} \| T_{Curr}),$$
   $$m(1)_{MN} = m(0)_{MN} + \alpha(0)_{MN} r(0)_{MN} - \alpha(1)_{MN} r(1)_{MN}.$$

   It then sends the necessary parameters to the AP$_2$.

2. AP$_2$ →MN: $g^{\alpha(1)_{AP_2}}, m(1)_{AP_2}, C(0)_{AP_2}, T_{Curr}, T_{Exp}, h(PMK, g^{\alpha(1)_{AP_2}})$

   AP$_2$ first computes $CH_{y(1)_{MN}}(m(1)_{MN}, r(1)_{MN})$ using the received parameters and verifies the credential $C(0)_{MN}$ using the PK^+_{AAA} as follows.

   $$\text{Verify}_{PK^+_{AAA}}(C(0)_{MN}) \equiv (CH_{y(1)_{MN}}(m(1)_{MN}, r(1)_{MN}) \| T_{Exp})$$

   If successful, AP$_2$ chooses a new random value $\alpha(1)_{AP_2} \in Z_q^*$, and computes its DH half-key $g^{\alpha(1)_{AP_2}}$ and Pairwise Master Key PMK = $(g^{\alpha(1)_{MN}})^{\alpha(1)_{AP_2}}$ that is used to protect user data over the air interface. Then, it computes

   $$r(1)_{AP_2} = h(g^{\alpha(1)_{AP_2}} \| T_{Curr}),$$
   $$m(1)_{AP_2} = m(0)_{AP_2} + \alpha(0)_{AP_2} r(0)_{AP_2} - \alpha(1)_{AP_2} r(1)_{AP_2}.$$

   It then sends these values with the necessary parameters for mutual authentication to MN.

3. MN→AP$_2$: $h(PMK, g^{\alpha(1)_{MN}})$

   MN computes the AP$_2$'s $CH_{y(1)_{AP_2}}(m(1)_{AP_2}, r(1)_{AP_2})$ and verifies the credential $C(0)_{AP_2}$ using the PK^+_{AAA} as follows.

   $$\text{Verify}_{PK^+_{AAA}}(C(0)_{AP_2}) \equiv (CH_{y(1)_{AP_2}}(m(1)_{AP_2}, r(1)_{AP_2}) \| T_{Exp})$$

   If successful, it computes the PMK = $(g^{\alpha(1)_{AP_2}})^{\alpha(1)_{MN}}$. Finally, MN checks the hash value $h(PMK, g^{\alpha(1)_{AP_2}})$ of the PMK and response to confirm the PMK agreement as $h(PMK, g^{\alpha(1)_{MN}})$.

4. AP_2 checks the hash value $h(PMK, g^{\alpha(1)_{MN}})$ of the PMK. If successful, they agree same ephemeral DH session key such as $g^{\alpha(1)_{AP_2}\alpha(1)_{MN}}$ and authenticate each other successfully.

3. Cryptanalysis of Choi et al.'s Scheme

This section shows that Choi et al.'s scheme is not provide Perfect Forward/Backward Secrecy (PFS/PBS). PFS/PBS means that even if a long-term secret key is compromised at any point in time, it never reveals all the preceding and following session keys. Therefore, PFS/PBS is a very important security requirement in evaluating a strong security protocol. For example, the well-known Diffie-Hellman key agreement scheme can provide PFS/PBS.

In the Choi et al.'s scheme, the Pairwise Master KEY (PMK) $g^{\alpha(1)_{AP_2}\alpha(1)_{MN}}$ is used as a ephemeral DH session key to encrypt all further communications in the session. They support this claim with the argument that says: *In our scheme, the DH secret keys are the ephemeral random values $\alpha(i)_{MN}$ and $\alpha(i)_{AP_2}$ of an MN and an AP, respectively. They guarantee the freshness of the DH session key if two nodes have chosen their random exponents properly.* However, this argument may hold if the ephemeral random values $\alpha(i)_{MN}$ and $\alpha(i)_{AP_2}$ are not send through open network channel. Note that all messages in handover authentication phase are transmitted via an insecure channel such as over the air interface. Therefore, knowing a long-term secret key of MN or AP, an adversary can simply compute the session Pairwise Master KEY (PMK) $g^{\alpha(1)_{AP_2}\alpha(1)_{MN}}$ and hence previous communication messages will be learned.

Suppose that MN's long-term secret key $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}\}$ is compromised to an adversary $\mathcal{A}$ and then he/she intercepts the transmitted values $g^{\alpha(1)_{MN}}, m(1)_{MN}, C(0)_{MN}, T_{Curr}, T_{Exp}$ in step (1) and $g^{\alpha(1)_{AP_2}}$, $m(1)_{AP_2}$, $C(0)_{AP_2}$, T_{Curr}, T_{Exp}, $h(PMK, g^{\alpha(1)_{AP_2}})$ in step (2) of the handover authentication phase, respectively. It is easy to obtain this information since it is readily available over the open network. Then, $\mathcal{A}$ can compute the session PMK $g^{\alpha(1)_{AP_2}\alpha(1)_{MN}}$ by performing the following operations.

1. Let the computed value $m(0)_{MN} + \alpha(0)_{MN}r(0)_{MN}$ from the compromised long-term secret key $\{\alpha(0)_{MN}, m(0)_{MN}, r(0)_{MN}\}$ of MN be denoted as $SKey$. By using the intercepted $m(1)_{MN} = m(0)_{MN} + \alpha(0)_{MN}r(0)_{MN} - \alpha(1)_{MN}r(1)_{MN}$ form the step 1 of handover authentication phase, $\mathcal{A}$ first computes $-(m(1)_{MN} - SKey)$ to obtain $\alpha(1)_{MN}r(1)_{MN}$ as follows.

$$\begin{aligned}\alpha(1)_{MN}&r(1)_{MN}\\ &= -(SKey - \alpha(1)_{MN}r(1)_{MN} - SKey) \qquad (1)\\ &= -(m(1)_{MN} - SKey)\end{aligned}$$

2. By using the intercepted DH half-key $g^{\alpha(1)_{MN}}$ and T_{Curr}, $\mathcal{A}$ computes $r(1)_{MN}$ as follows.

$$r(1)_{MN} = h(g^{\alpha(1)_{MN}} \| T_{Curr}) \qquad (2)$$

3. By using the above results of the equations (1) and (2), $\mathcal{A}$ extracts the ephemeral random value $\alpha(1)_{MN}$ of the MN as follows.

$$\alpha(1)_{MN} = \alpha(1)_{MN}r(1)_{MN}r(1)^{-1}_{MN} \qquad (3)$$

where $r(1)^{-1}_{MN}$ is an inverse value of $r(1)_{MN}$ in the equation (2) such as $r(1)_{MN} \cdot r(1)^{-1}_{MN} \equiv 1$.

4. By using the obtained ephemeral random value $\alpha(1)_{MN}$ and the intercepted DH half-key $g^{\alpha(1)_{AP_2}}$ of AP_2, $\mathcal{A}$ can compute the session PMK as follows.

$$g^{\alpha(1)_{AP_2}\alpha(1)_{MN}} = (g^{\alpha(1)_{AP_2}})^{\alpha(1)_{MN}} \qquad (4)$$

When the AP_2's long-term secret key $\{\alpha(0)_{AP_2}, m(0)_{AP_2}, r(0)_{AP_2}\}$ is compromised to $\mathcal{A}$, he/she can also compute the same session PMK $g^{\alpha(1)_{AP_2}\alpha(1)_{MN}}$ by performing the above attack procedure. As a result, if a long-term secret key of MN or AP is compromised at any point in time, it reveals all the preceding and following session keys by the adversary $\mathcal{A}$. Obviously, Choi et al.'s scheme is not provide Perfect Forward/Backward Secrecy (PFS/PBS) unlike their claims.

4. Conclusions

This paper demonstrated that Choi et al.'s handover authentication scheme using credentials based on chameleon hashing fails to achieve Perfect Forward/Backward Secrecy (PFS/PBS) unlike their claims. As a result, there is no quick tweak that can be applied to make Choi et al.'s scheme provide PFS/PBS since the ephemeral random value $\alpha(i)_x$ is easily obtained from $m(i)_x$. It means that the scheme must not be based on the chameleon hash function to provide PFS/PBS. It is the subject of our future work to design a secure handover authentication scheme without using the chameleon hashing.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments in improving this manuscript. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No.2010-0010106).

References

[1] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," IEEE Commun. Lett., vol.14, no.1, pp.54–56, 2010.

[2] H. Krawczyk and T. Rabin, "Chameleon signatures," Proc. NDSS, 2000, pp.143–154, 2000.

[3] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol.IT-22, no.6, pp.644–654, 1976.