An Enhanced Security Protocol for Fast Mobile IPv6

Ilsun YOU††, Kouichi SAKURAI††, and Yoshiaki HORI††, Members

SUMMARY Recently, Kempf and Koodli have proposed a security protocol for Fast Mobile IPv6 (FMIPv6). Through the SEcure Neighbor Discovery (SEND) protocol, it achieves secure distribution of a handover key, and consequently becomes a security standard for FMIPv6. However, it is still vulnerable to redirection attacks. In this paper, we propose an enhanced security protocol, which improves Kempf-Koodli’s protocol and consequently becomes a security standard for FMIPv6. However, it is still vulnerable to redirection attacks since it does not protect the additional messages and round trip times. The protocol is based on the Cryptographically Generated Address (CGA) method. With the help of the AAA infrastructure, it is supposed that during the bootstrapping step, the MN shares the message protection secret K(1) with the first access router AR(1) through the Authentication, Authorization, and Accounting (AAA) infrastructure [3],[8]. This assumption is reasonable because the AAA infrastructure is widely used for the network access authentication in Mobile Internet environment. Moreover, we assume that there is a secure channel between access routers.

2. Proposed FMIPv6 Authentication Protocol

2.1 Notations and Preliminary

- \textit{Msg(address1, address2)} means that the message \textit{Msg} is sent from \textit{address1} to \textit{address2}.
- \textit{E(K, M)} denotes a function that encrypts the message \textit{M} with the given key \textit{K}, where \textit{K} can be a secret key or a public key.
- \textit{SIGN(K, M)} denotes a function that digitally signs the message \textit{M} with the private key \textit{K}.
- \textit{MN} denotes a mobile node.
- \textit{AR(i)} denotes the \textit{i}th access router which the \textit{MN} visits, and its IPv6 address, where \textit{i} > 0.
- \textit{CoA(i)} is the \textit{i}th care-of address of the \textit{MN}, where \textit{i} > 0.
- \textit{PU_X} is the \textit{X}’s public key from which the CGA is derived.
- \textit{PR_X} is the \textit{X}’s private key which corresponds to \textit{PU_X}.
- \textit{HK(i)} is the \textit{i}th handover key, where \textit{i} > 0.
- \textit{K(i)} is the \textit{i}th message protection secret, where \textit{i} > 0.
- \textit{CGA - PARAM_X} is the \textit{X}’s parameters which are used to verify the \textit{X}’s CGA is derived from \textit{PU_X}.

It is assumed that the \textit{MN} has a public/private key pair \textit{PU_MN/PR_MN} and its address is a CGA, which derived from \textit{PU_MN}. And it is supposed that during the bootstrapping step, the \textit{MN} shares the message protection secret \textit{K(1)} with the first access router \textit{AR(1)} through the Authentication, Authorization, and Accounting (AAA) infrastructure [3],[8]. This assumption is reasonable because the AAA infrastructure is widely used for the network access authentication in Mobile Internet environment. Moreover, we assume that there is a secure channel between access routers.

2.2 Operation

As illustrated in Fig. 1, this protocol is composed of three phases: handover key negotiation, fast binding update and new network attachment phases.

During the handover key negotiation phase, the \textit{MN} negotiates a new handover key \textit{HK(i)} with the current access router \textit{AR(i)} through its public key \textit{PU_MN}. Especially, in order to protect the \textit{RtSolPr} and \textit{PrRtAdv} messages, the \textit{MN} and the \textit{AR(i)} adopt the HMAC method instead of the public key based digital signature. That makes it possible...
for them to defend against the DoS attack while reducing the heavy computation overhead caused by the asymmetric cryptographic operations. For the HMAC method, a message protection secret $K(i)$, derived from its related handover key and nonces, is introduced. Note that during the bootstrapping step, the first message protection secret $K(1)$ is shared between the $MN$ and the $AR(1)$ with the help of the AAA infrastructure as mentioned above. Once the shared handover key $HK(i)$ has been constructed, the $MN$ starts the fast binding update phase by sending the $FBU$ message to the $AR(i)$ when a link-specific handover event occurs. If the $FBU$ message is valid, the $AR(i)$ can believe that the $MN$ truly owns both $CoA(i)$ and $PU_{MN}$ because it can get $HK(i)$ in the only case that $PR_{MN}$ belongs to itself. With such belief, the $AR(i)$ starts to act as a temporary home agent for the $MN$ while exchanging the $HI$ and $HACK$ messages with the next access router $AR(i+1)$. Note that the $HI$ message includes the $(i+1)$th message protection secret $K(i+1)$. Thus, the $AR(i)$ allows the $AR(i+1)$ to securely share $K(i+1)$ with the $MN$. After that, the $AR(i)$ returns the $MN$ the $FBA$ message while stating to tunnels the traffic sent to $CoA(i)$ on its link to $CoA(i+1)$ on the $AR(i+1)$’s link. If the $FBA$ message is valid, the $MN$ assumes that data packets are being forwarded to its new location. As soon as the $MN$ handovers to the $AR(i+1)$’s link, it announces its attachment by sending the $UNA$ message to the $AR(i+1)$. This is the new network attachment phase. In order to secure the $UNA$ message, the proposed protocol uses both the digital signature, $SIGuna$, and the HMAC value, $MACfna$. Especially, the digital signature is adopted to provide the handover key independence. When the $MN$ cannot send the $FBU$ message or receive the $FBA$ message on the $AR(i)$’s link (the reactive mode), the $AR(i+1)$ performs the fast binding update phase on behalf of the $MN$ before verifying the $UNA$ message.

3. Analysis

In this section, the proposed protocol is formally analyzed through BAN-logic [9]. After that, the protocol’s security properties and computation overhead are discussed.

3.1 Formal Verification by BAN-Logic

Since introduced by Burrows, Abadi and Needham in 1989, BAN-logic has become the best-known and widely used method for verifying security protocols due to simplicity and robustness. For details on notations and logical postulates of BAN-logic, refer to [9]. As the first step of this verification, we define the goals as follows:

Goal1: $AR(i) \equiv FBU$

Goal2: $AR(i+1) \equiv UNA$

Goal3: $MN \equiv MN \xrightarrow{K(i+1)} AR(i+1)$

For the next handover, the validity of $K(i+1)$ should be believed by both the $MN$ and the $AR(i+1)$. Because the $AR(i)$, who controls $K(i+1)$, sends the secret to the $AR(i+1)$ through their secure channel, we can assume that the $AR(i+1)$ believes that the secret is valid and fresh. Thus, we provide the assumptions A4 and A6 in addition to Goal3.

Also, we use the following definition besides the basic rules of BAN-logic. It is clear from the meaning of the definition that it is intuitively true.

Definition1: $A \equiv \xrightarrow{PR} A, A \equiv B \equiv \{M\}PU_{A}, A \equiv B \equiv M$
(1) $MN \rightarrow AR(i): < m_i >_{K(i+1)}$
(2) $AR(i) \rightarrow MN: < (MN \leftrightarrow AR(i), MN \leftrightarrow AR(i+1))_{PU_{MN}}, m_i, n_i >_{K(i)}$
(3) $MN \rightarrow AR(i): < FBU, seq>MN \leftrightarrow AR(i)_{PK_{MN}}$
(4) $AR(i) \rightarrow MN: < FBA, seq>MN \leftrightarrow AR(i)_{PK_{MN}}$
(5) $MN \rightarrow AR(i+1): \{H(UNA)\}_{PK_{MN}} < UNA, MN \leftrightarrow AR(i+1) >_{K(i+1)}$

Fig. 2 Idealized protocol.

A1: $MN \equiv AR(i) \Rightarrow MN \leftrightarrow_{PK_{MN}} AR(i)$
A10: $AR(i+1) \equiv_{PK_{MN}} MN$
A2: $MN \equiv AR(i) \Rightarrow MN \leftrightarrow_{PK_{MN}} AR(i-1)$
A11: $MN \equiv_{PK_{MN}} MN$
A3: $AR(i) \equiv MN \leftrightarrow_{PK_{MN}} AR(i)$
A12: $MN \equiv_{PK_{MN}} MN$
A4: $AR(i+1) \equiv MN \leftrightarrow_{PK_{MN}} AR(i+1)$
A13: $MN \equiv \#(m_i)$
A5: $AR(i) \equiv \#(MN \leftrightarrow_{PK_{MN}} AR(i))$
A14: $AR(i) \equiv \#(n_i)$
A6: $AR(i+1) \equiv \#(MN \leftrightarrow_{PK_{MN}} AR(i+1))$
A15: $MN \equiv \#(seq)$
A7: $MN \equiv MN \leftrightarrow_{PK_{MN}} AR(i)$
A16: $AR(i) \equiv MN = FBU$
A8: $AR(i) \equiv MN \leftrightarrow_{PK_{MN}} AR(i)$
A17: $AR(i+1) \equiv MN = UNA$
A9: $AR(i) \equiv_{PK_{MN}} MN$

Fig. 3 Assumptions.

Once the assumptions are made, we can now proceed with the analysis (where R1 denotes the message-meaning rule, R2 denotes the nonce verification rule and R3 denotes the jurisdiction rule).

From the $RtSolPr$ message, we derive by:
(1) $AR(i) \equiv MN \vdash m_i$ [by A8, R1]

From the $PrRtAdv$ message, we derive:
(2) $MN \equiv AR(i) \vdash (MN \equiv AR(i), MN \equiv AR(i+1))_{PU_{MN}}, m_i, n_i$ [by A7, R1]
(3) $MN \equiv \#(MN \leftrightarrow_{PK_{MN}} AR(i), MN \leftrightarrow_{PK_{MN}} AR(i+1))_{PU_{MN}}, m_i, n_i$ [by A5]
(4) $MN \equiv AR(i) \vdash (MN \leftrightarrow_{PK_{MN}} AR(i), MN \leftrightarrow_{PK_{MN}} AR(i+1))_{PU_{MN}}$ [by (2), (3), R2]
(5) $MN \equiv MN \equiv_{PK_{MN}} AR(i)$ [by A11, (4), Definition1, A1, R3]
(6) $MN \equiv MN \equiv_{PK_{MN}} AR(i+1)$ [by A11, (4), Definition1, A1, R3]

From the $FBU$ message, we derive:
(7) $AR(i) \equiv MN \equiv_{PK_{MN}} FBU$ [by (5), R1, A5, R2]
(8) $AR(i) \equiv FBU$ [by (7), A16, R3]

From the $FBA$ message, we derive:
(9) $MN \equiv AR(i) \equiv_{PK_{MN}} FBA$ [by (5), R1, A15, R2]

From the $UNA$ message, we derive:
(10) $AR(i+1) \equiv MN \equiv_{PK_{MN}} UNA$ [by A4, R1, A6, R2]
(11) $AR(i+1) \equiv UNA$ [by (9), A17, R3]

Note that only the right part of the $UNA$ message can leads to the formula (11). However, the left part of the message is required to prove the handover key independence. By the formulas (6), (8), (11), we can conclude that the proposed protocol achieve the given goals.

3.2 Security Analysis

(1) Tight binding between $HK(i)$ and $CoA(i)$: In the proposed protocol, the $AR(i)$ encrypts $HK(i)$ with the $MN$’s public key $PU_{MN}$, which corresponds to $CoA(i)$. If the $FBU$ message, protected by $HK(i)$, is valid, the $AR(i)$ can be sure that the $MN$ truly owns $PR_{MN}$ and $CoA(i)$. Thus, there exists the tight binding between $HK(i)$ and $CoA(i)$.

(2) Handover key independence: In the proposed protocol, each handover key is not used for generating or distributing other handover keys. Therefore, even if one handover key is compromised, the previous or successive handover keys are not compromised.

(3) Preventing Denial of Service attacks: The proposed protocol adopts the HMAC method to protect the $RtSolPr$, $PrRtAdv$, $FBU$, $FBA$ and $UNA$ messages. Especially, each involved entity validates the related HMAC value such as $MAC1$, $MAC2$ or $MACuna$ before performing its public key operation. In this way, it can defend against the DoS attacks.

(4) Secure $UNA$ messages: In the proposed protocol, each $UNA$ message is protected by both the public key based digital signature and HMAC methods. Because of not knowing $K(i+1)$ and $PR_{MN}$, an attacker cannot fabricate $UNA$ messages and launch session hijacking attacks by just eavesdropping. Note that though the message can be protected by only the HMAC method, the digital signature method is used to protect the proposed protocol even though handover keys are compromised. Like our approach, Kempf-Koodli’s protocol can use the digital signature based on the CGA method to protect the $UNA$ messages. However, in this case, its computational costs can be considerably increased due to the expensive assymmetric operations.

3.3 Computational Cost Comparison

Table 1 compares the computational cost of the proposed protocol with that of Kempf-Koodli’s one. As described in it, while the $MN$ reduces ($V+H$) at the expense of $3HM$, the $AR(i)$ and $AR(i+1)$ reduce $S$ at the expense of $3(H+HM)$. In addition to such an advantage, the proposed protocol exploits the existing messages of the FMIPv6 protocol to present an FMIPv6-seamless structure. Therefore, it does not introduce new signaling messages and additional round trip times.

4. Conclusion

A new security protocol for FMIPv6 was proposed. The proposed protocol uses the message protection secret to solve the drawbacks of Kempf-Koodli’s one. Through the HMAC
Table 1  Computational cost comparison (S: the cost for the one signature generation, V: the cost for verifying the one signature, H: the cost for one hash operation, HM: the cost for one HMAC operation, E: the cost for one public key encryption, D: the cost for one public key decryption, MN∗ and AR∗: the nodes of Kempf-Koodli’s protocol, MN and AR: the nodes of the proposed protocol).

<table>
<thead>
<tr>
<th>Message</th>
<th>MN∗</th>
<th>AR∗</th>
<th>MN</th>
<th>AR</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIS olPr</td>
<td>S</td>
<td>2H+V</td>
<td>HM</td>
<td>HM+2H</td>
</tr>
<tr>
<td>PrRlAdv</td>
<td>2H+V+D</td>
<td>E+S</td>
<td>HR+D</td>
<td>E+HR</td>
</tr>
<tr>
<td>FBU</td>
<td>HM</td>
<td>HM</td>
<td>HM</td>
<td>HM</td>
</tr>
<tr>
<td>FBA</td>
<td>HM</td>
<td>HM</td>
<td>HM</td>
<td>HM</td>
</tr>
<tr>
<td>UNA</td>
<td>0</td>
<td>0</td>
<td>S+H+HM</td>
<td>3H+HM+V</td>
</tr>
</tbody>
</table>

*Values 86,035 K 46,061 K 84,009 K 4,070 K

* The parameters provided in [10] are applied to compute the values. It is assumed that the size of the message is 100 byte message and the used algorithms are SHA, HMAC – SHA and RSA. The values are measured in cycles.

values computed with this secret, it can prevent the DoS attacks while minimizing the public key operations. Note that the first message protection secret is negotiated between the MN and its first AR with the help of the AAA infrastructure. By using BAN-logic, the proposed protocol’s correctness is formally verified. From security analysis and computational cost comparison, we can conclude that the protocol is more secure and efficient than Kempf-Koodli’s one.

Acknowledgments

This paper is supported by JSPS RONPAKU Program (ID No.KOSEF-10910).

References