2010 International Conference on Broadband, Wireless Computing, Communication and Applications

Comments on a One-Way Hash Chain based Authentication for FMIPv6

Ilsun You
School of Information Science, Korean Bible University
Seoul, Korea
Email: isyou@bible.ac.kr

Jong-Hyouk Lee
IMARA Team, INRIA
Rocquencourt, France
Email: jong-hyouk.lee@inria.fr

***Abstract*—In this paper, we analyze a one-way hash chain based authentication scheme proposed by Haddad and Krishnan. The authentication scheme has been introduced for improving handover performance in Fast Mobile IPv6 (FMIPv6), but as we argue in this paper the authentication scheme is vulnerable to redirect and DoS attacks. We present strengths and weaknesses of the authentication scheme. In addition, a possible extension to NEtwork MObility (NEMO) is suggested.**

***Keywords*-Authentication; Hash; FMIPv6; NEMO.**

I. Introduction

Mobility support for mobile nodes (MNs) is a fundamental requirement for future networks. Mobile IPv6 (MIPv6) had been standardized in the Internet Engineering Task Force (IETF) as a base mobility management protocol [1]. Then, extensions to MIPv6 have been introduced. One of the extensions is FMIPv6 that reduces handover latency and prevents packet loss [2]. However, the specification of FMIPv6 only defines operations for involved entities. Without securing the operations, FMIPv6 cannot be deployed in real mobile networks. To address this security problem, a public-key cryptography based authentication scheme has been standardized [3], but it requires resource-constrained MNs to process expensive computational overheads of public-key cryptography. Another authentication scheme introduced by Haddad and Krishnan [4] relies on a one-way hash chain, which leads lightweight computational overheads to resource-constrained MNs.

In this paper, we focus on Haddad and Krishnan's authentication scheme. Hereafter, we call it as HKA. A handover key in HKA is efficiently exchanged between an MN and its access router (AR) without an involvement of public-key cryptography operations. HKA also provides an independence of handover keys and a tight binding between a handover key and a care-of address (CoA). However, as we reveal in this paper, HKA is vulnerable to redirect and DoS attacks because 1) it has been designed to protect only fast binding update (FBU) and fast binding acknowledgment (FBA) messages; and 2) cryptographically generated address (CGA) [5] based SEcure Neighbor Discovery (SEND) [6] is required for the first handover or for the update of one-way hash chain. The strengths and weaknesses of HKA are explored. A possible extension to NEMO [7] is also suggested in this paper.

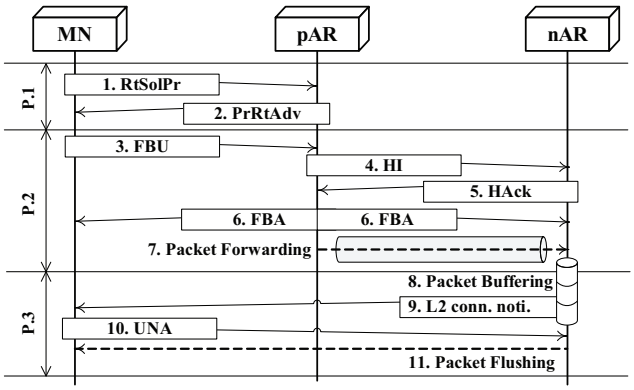

Figure 1. Operations of Predictive FMIPv6.

The rest of this paper is structured as follows. First, we discuss the operations of FMIPv6 and possible threats in detail in Section II. In Section III, we explore Haddad and Krishnan's one-way hash chain based authentication scheme, i.e., HKA. In Section IV, we present a possible extension of HKA to NEMO and then conclude this paper in Section V.

II. FMIPv6 and Threats

A. FMIPv6

Handover latency and packet loss are the most important performance criteria for mobility management protocols. FMIPv6 has been standardized as an extension to MIPv6 to improve handover performance, i.e., reducing handover latency by utilizing the L2 handover trigger and preventing packet loss by adopting packet buffering at ARs [2].

FMIPv6 has two different operation modes, i.e., predictive mode and reactive mode. The predictive mode is achieved when an MN successfully receives a FBA message from its current AR before the MN attaches to a new AR, whereas the reactive mode is started when an MN cannot receive a FBA message from its currnet AR and attaches to a new AR. In this paper, we only consider the predictive mode of FMIPv6 due to the limited space. Fig. 1 shows the operations of predictive FMIPv6.

An MN in Fig. 1 sends a router solicitation for proxy advertisement (RtSolPr) message to a previous AR (pAR), where the MN is currently attached, to obtain the infor-

978-0-7695-4236-2/10 $26.00 © 2010 IEEE
DOI 10.1109/BWCCA.2010.84

mation about neighboring networks. The RtSolPr message can be triggered by the L2 trigger, i.e., link-specific event for handover. In response, the pAR sends a proxy router advertisement (PrRtAdv) message containing the information of neighbor networks such as neighbor ARs' link-layer addresses, IPv6 addresses, network prefixes, wireless link parameters, etc. Suppose the PrRtAdv message includes the information of a new AR (nAR). Then, the MN can prepare its handover to a new network managed by the nAR while it still attaches to the pAR.

The MN generates a new CoA (nCoA) based on the network prefix obtained from the PrRtAdv message. Note that the MN uses a previous CoA, which has been generated based on the network prefix of the pAR, while it attaches to the pAR. The MN sends a FBU message to authorize the pAR to bind the pCoA to the generated nCoA. As the pAR receives the FBU message from the MN, it sends a handover initiate (HI) message to the nAR. In response, the nAR sends a handover acknowledge (HAck) message to the pAR. The HAck message includes a status value for fast handover, e.g., acceptance of the MN's fast handover. Then, the pAR sends FBA messages to the MN and nAR. Packets destined for the MN are being forwarded from the pAR to the nAR.

As soon as the MN establishes link connectivity with the nAR, it sends an unsolicited neighbor advertisement (UNA) message to the nAR in order to explicitly inform its attachment. The nAR sends buffered packets to the MN. Accordingly, the MN achieves its seamless handover thanks to 1) the L2 trigger; 2) the information about neighboring networks obtained while it is still attached to the pAR; and 3) packet buffering and forwarding services provided by ARs. Note that the MN is required to inform its location change by sending a binding update message to its home agent (HA) after it attaches to the nAR, but in Fig. 1 such a home registration is omitted.

B. Possible Threats on FMIPv6

FMIPv6 improves handover performance by reducing handover latency and preventing packet loss, but it suffers from various threats. Here, we divide the operations of predictive FMIPv6 into three phases as shown in Fig. 1 and then present the identified threats for each phase.

- P.1 (RtSolPr and PrRtAdv messages): In P.1, the MN obtains the neighboring network information by exchanging the RtSolPr and PrRtAdv messages with its pAR. Suppose an attacker sends a fake PrRtAdv message including the bogus information about neighboring networks. For instance, the attacker easily inserts the information of poor neighbor networks, e.g., overloaded AR's information or far-off AR's information. If the MN accepts this fake PrRtAdv message, it sends a FBU message to its pAR in order to inform its handover to one of poor neighbor networks. This threat makes worse QoS of the MN. This threat is also possible even the FBU message is securely protected. In addition, if the attacker successfully deceives multiple MNs to choose a poor neighbor network, this threat also aggravates the status of the poor neighbor network, e.g., increasing loads to an AR managing the poor network for processing MNs.
- P.2 (FBU, FBA, HI, and HAck messages): In P.2, the messages between the infrastructure nodes, i.e., the pAR and the nAR, are assumed to be secure. On the other hand, the messages between the pAR and the MN are vulnerable. Suppose an attacker sends a fake FBU message indicating a false information, e.g., the MN performs its handover to a new network. As the pAR receives this fake FBU message, the pAR and the nAR exchange the HI and HAck messages for the MN. As the attacker increases the number of such fake FBU messages, both of the pAR and the nAR are overloaded to process those HI and HAck messages. Especially, per HI message sent from the pAR, the nAR should perform a duplicate address detection process to verify the uniqueness of the nCoA included in the HI message.
- P.3 (UNA message): In P.3, the MN explicitly announces its attachment to the nAR by sending an UNA message, which is vulnerable. Suppose an attacker is between the MN and its nAR. Upon receiving the UNA message, the attacker obtains the address information, i.e., nCoA and link-layer address. At the same time, while masquerading as the nAR, the attacker sends the MN a false neighbor advertisement acknowledgment (NAACK) message indicating that the nCoA included in the UNA is invalid. As a result, the MN performs an address configuration or uses a bogus nCoA included in the NAACK message. At this point, the attacker possibly intercepts the MN's packets forwarded from the nAR through the MN's original address information.

There may be other threats not identified and attackers may launch combined attacks.

III. HKA: One-way hash chain based authentication scheme for FMIPv6

HKA is a lightweight authentication scheme that enables an MN to efficiently exchange a handover key with its AR.

A. HKA Operations

Fig. 2 shows the operations of HKA. Note that each message presented in Fig. 2 includes the information required for fast handover, but in Fig. 2 the values related to the operations of HKA are mainly presented. Suppose that the MN now attaches to the pAR and will perform its handover to the nAR. In Fig. 2, the handover from the pAR to the nAR is assumed to be the first handover of the MN.

The MN generates its one-way hash chain V in which each value is 128 bits; $V_0, V_1, ...V_n, V_i = H(V_i + 1)$. Then,

the MN sends its RtSolPr message including the first hash value V_0, CGA parameters C_{MN} including its public key PUK_{MN}, and signature S_{MN} [4], [5], [6]. As the pAR receives the RtSolPr message sent from MN, it verifies this message according to [5], [6]. The pAR generates the handover vector HV in which each value of this handover vector is 64 bits; $HV_0, HV_1, ...HV_n, HV_{i+1} = H(V_i)$. The pAR sends the MN the PrRtAdv message including the first handover vector HV_0, its CGA parameters C_{pAR}, and signature S_{pAR}.

In P.1 of Fig. 2, the RtSolPr and PrRtAdv messages are used to exchange V_0 and HV_0 between the MN and the pAR. Because this is the first handover of the MN, the CGA based SEND is used to protect the RtSolPr and PrRtAdv messages. In other words, C_{MN} included in the RtSolPr protects V_0, while HV_0 is encrypted with PUK_{MN}. Note that the CGA parameters includes the message sender's public key [5].

In P.2, the MN sends its FBU message to the pAR. The FBU message includes the nCoA address $nCoA$, the hash extension HE, and the HMAC value for this FBU message $HMAC_{FBU}$. Here, $nCoA$ is generated as a concatenation of the network prefix of nAR obtained from the PrRtAdv message and the one-way hash chain based interface identifier $HIID$, which is computed as follows:

$$HIID = Left(64, V_1) \text{ XOR } HV_1,$$

where HV_1 is computed as $HV_1 = H(HV_0)$ and XOR means an exclusive OR operation. HE included in the FBU message is computed as follows:

$$HE = Right(64, V_1) \text{ XOR } HV_1.$$

Then, $HMAC_{FBU}$ included in the FBU message is computed as follows:

$$HMAC_{FBU} = HMAC(V_1, FBU),$$

where V_1 is used as a handover key and FBU is the FBU message in which the source address and the destination address are the pCoA of the MN and the address of the pAR, respectively.

As the pAR receives the FBU message sent from the MN, it decodes $HIID$ and HE by using HV_1. The next steps are hashing the concatenation of the two decoded values and comparing the result 128 bits hash value with V_0. If this verification is successful, the pAR uses V_1 to authenticate the FBU message sent from the MN. In order words, V_1 is used as a handover key to check $HMAC_{FBU}$. This successful verification makes the pAR believes that the MN's $nCoA$ and its association with V_1. Then, the pAR sends the HI message including V_1 and HV_1 to the nAR. As the pAR receives the HAck message indicating acceptance of the MN's fast handover, it sends FBA messages to the MN and nAR. The FBA message sent from pAR to the MN includes the HMAC value $HMAC_{FBA}$, which is computed as

$$HMAC_{FBA} = HMAC(V_1, FBA),$$

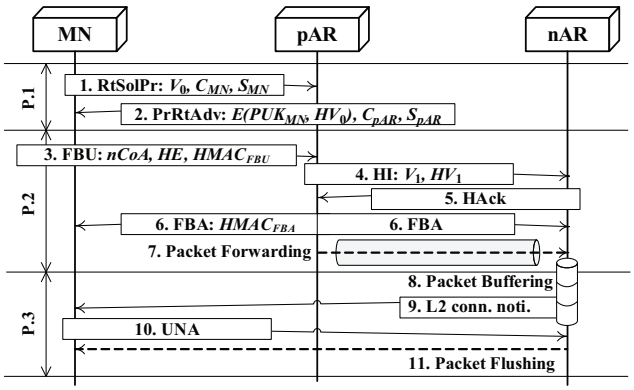

Figure 2. Operations of HKA on Predictive FMIPv6.

where FBA is the FBA message sent from the pAR. As the MN receives the FMA message including $HMAC_{FBA}$, it verifies the FBA message with V_1.

In P.3, the UNA message is sent from the MN to the nAR which is involves any security protection.

B. Strengths and Weaknesses

Compared to public-key cryptography based authentication schemes, HKA requires lightweight computational overheads to resource-constrained MNs. The followings are the strengths of HKA:

- HKA utilizes the one-way hash chain to protect FBU and FBA messages.
- HKA provides the tight binding between the MN's handover key and CoA by inserting the first 64-bit part of the handover key to the CoA.
- HKA guarantees an independence of handover keys by restricting that each generated handover key by the MN is only used once per handover. That is, a compromise of the past keys has no security impact on HKA.
- HKA does not require additional message exchanges for securing its handover.

However, HKA has the following weaknesses:

- Each handover key is computed by an exclusive OR operation with the corresponding handover vector. As each AR can use its handover vector to compute the successive ones, it can easily recover the next handover keys. That is, even though only one of the pARs is compromised, its next handover keys can be revealed just by eavesdropping.
- Only FBU and FBA messages are protected in HKA. Other messages such as RtSolPr, PrRtAdv, and UNA messages are not protected. It means that HKA suffers from the threats, which can be launched in P.1 and P.3. Note that the SEND enabled RtSolPr and PrRtAdv messages are only used for the first handover or updating of one-way hash chain.

- Because HKA utilizes the SEND protocol for the first handover or updating of one-way hash chain, it is still vulnerable to DoS attacks on P.1.

IV. Extension to NEMO

FMIPv6 is a mobility management protocol for a host. In other words, this protocol cannot support mobility service for a set of hosts efficiently. NEMO defined in [7] is rated as a base mobility management protocol for a set of hosts. In NEMO, a mobile router (MR) is introduced as a main entity for providing mobility service for a set of hosts, i.e., mobile network nodes (MNNs), attached to the MR. The MNNs configure their addresses based on a mobile network prefix (MNP) provided from the MR. As the MR involving its MNNs changes its attachment, it registers its current location to the HA. Since the MR acts as a routing gateway for the MNNs, data packets for the MNNs are routed via a bi-directional tunnel established between the MR and the HA. That is, the MNNs attached to the MR do not need to register individually to the HA.

Here, we consider a moving train consisting of passenger carriages as a possible environment for HKA. Each passenger carriage is equipped with an MR that provides mobility services for wireless devices of passengers. Suppose that each MR installed in a passenger carriage is connected each other by a wired link. Then, HKA can be easily applied into this environment. For instance, as a passenger gets in his passenger carriage, the MR of the passenger carriage would be the first AR. When the passenger moves to other passenger carriages for telephones and food services, HKA can enable the wireless device of the passenger to efficiently exchange a handover key for seamless handover authentication between different MRs. Note that the considered environment here assumes that a set of MRs installed in the train moves while they are connected.

Due to characteristics of NEMO, the following issues must be considered when we apply HKA into NEMO based vehicular networks:

- Fast Handover and Tunnel Management between MRs: In the considered environment, a set of MRs is installed in the train. Then, they are connected via wired links that the specification of NEMO does not support such a case. Accordingly, a mechanism for fast handover and tunneling management between MRs is required to be developed for reducing handover latency and packet loss. This can be implemented by adopting FMIPv6 functionalities into the MRs.
- Mobility Rate: In NEMO, an MNN does not need to register its location to the HA for every movements while the MNN attaches to its MR. However, as the MNN attaches to another MR, data packets destined for the MNN must be forwarded from the previous MR to the current MR. In other words, as the time for which the MNN stays in a foreign MR is increased, the performance for data packet routing is decreased. This is mainly related with mobility rate and cannot be pre-determined for an individual MNN.
- Route Optimization: Route Optimization (RO) for NEMO has been widely studied for years, but this is still an undergoing research topic. Note that RO can improve the performance for data packet routing and also eliminate the unnecessary data packet forwarding from the previous MR to the current MR. If RO based on individual location update for MNNs is considered, authentication and authorization for location update must be also considered.

V. Conclusion

In this paper, we have analyzed a one-way hash chain based authentication scheme, i.e., HKA. This authentication scheme has been introduced for improving handover performance in FMIPv6 while enabling efficient handover key exchanging between an MN and its AR. However, as we presented, HKA is still vulnerable to various threats due to its limitations. Our next study is to develop an improved one-way hash chain based authentication scheme, which is free from the weaknesses of HKA for NEMO based vehicular networks.

References

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *IETF RFC 3775*, June 2004.

[2] R. Koodli, "Fast Handovers for Mobile IPv6," *IETF RFC 5268*, June 2008.

[3] J. Kempf and R. Koodli, "Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND)," *IETF RFC 5269*, June 2008.

[4] W. Haddad and S. Krishnan, "Authenticating FMIPv6 Handovers," *draft-haddad-mipshop-fmipv6-auth-02*, September 2006.

[5] T. Aura, "Cryptographically Generated Addresses (CGA)," *IETF RFC 3972*, March 2005.

[6] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "SEcure Neighbor Discovery (SEND)," *IETF RFC 3971*, March 2005.

[7] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," *IETF RFC 3963*, January 2005.