An Analysis of Fast Handover Key Distribution Using SEND in Mobile IPv6

Chris Brigham
Tom Wang

March 19, 2008

Abstract

In Mobile IPv6 with Fast Handovers, a key is distributed to a mobile node from its access router prior to handover. We examine the security properties of this key distribution protocol using Murphi. By modeling the complete protocol and various decomposed versions, we determine that the SEND-based protocol proposed in the draft is both sufficient and necessary for a secure handover-key exchange.

1 Introduction

In Mobile IPv6, a mobile node must maintain connectivity while moving between access points, which is achieved through a process called handover. In traditional MIPv6 handover, the process involves a burdensome handover latency that is problematic for real-time traffic. Fast MIPv6 handover avoids this latency by defining an alternative handover mechanism [FMIPv6]. This alternative mechanism relies on a protocol for distributing a symmetic handover key for a mobile node and its access router prior to handover [Draft]. Our analysis looks at this protocol–based on SEcure Neighbor Discovery [SEND]–for procuring and distributing the handover key. By modeling the complete draft and decomposed protocols in Murphi [Dill], we determine whether or not the SEND-based protocol is sufficient and necessary for maintaining basic security properties.

2 Security Properties

Our analysis looks at the basic safety properties required to make the handover-key distribution secure. We check authentication and secrecy properties in our Murphi models, and examine key stability–a router implementation detail–by hand.

2.1 Authentication

Authentication properties ensure that protocol participants are who they claim to be. Two such properties were tested in our models: mobile node authentication and access router authentication.

Mobile Node Authentication. *If an honest access router distributes a key and believes it is talking to a mobile node, then that mobile node believes it requested a key from the access router.*

Access Router Authentication. *If an honest mobile node receives a key that was requested from an access router, then that access router received a request from and assigned the key to the mobile node.*

2.2 Secrecy

Secrecy of the handover key is paramount in this key distribution protocol. If the key was made available to an intruder, it could be used to re-route the victims traffic to the endpoint of the intruder's choice.

Handover Key Secrecy. *The handover key for a mobile node and its (previous) access router cannot be known by any other parties until after the key is used in a fast binding update.*

2.3 Key Stability

Due to handover key distribution taking place prior to handover, a healthy amount of time can go by before the key is used in a fast binding update. During this time, the access router must keep track of the procured key assigned to each mobile node.

Handover Key Stability. *Once a handover key has been procured for a mobile node and access router, that key must not change until it expires or a fast binding update occurs.*

The danger here is the possibility of an attacker bombarding the access router with enough unique handover key requests that the space reserved for legitimate requests is depleted. Once depleted, the distributed handover key will be disassociated from the mobile node, causing fast binding update to fail when triggered.

This property depends on the cache management implemented on the access router, making it difficult to check it in our general case model. Instead of looking for a specific vulnerability, we recommend a scheme where the keys are stored in a cache that replaces entries whose addresses have the least amount of recent traffic. With this approach, agents with real-time traffic will not be replaced in the cache, preventing possible disruption during handover. On the other hand, agents with idle connections might be evicted, but they can most likely afford to make an additional handover key request. Keys requested for illegitimate addresses by an attacker will not have any traffic, so they will be the first to be replaced. If the cache is of reasonable size for legitimate activity, then an attacker's key requests will be unable to evict legitmate keys from the cache, since there will be less traffic for the illegitimate addresses.

3 Recommended Protocol Model

Our Murphi model of the protocol proposed in the specification draft abstracts away many details that are irrelevant to the properties in which we have interest. The inner components of SEND's CGA and signature options, for example, have been removed, as has the key algorithm type field, which is not susceptible to a rollback attack. The model is as follows:

$MN \rightarrow AR$: $RtSolPr(sourceAddr, destAddr, hkepk, nonce, sig)$
MN requests a handover key with a signed Router Solicitation for Proxy Advertisement message

$AR \rightarrow MN$: $RtPrAdv(sourceAddr, destAddr, hk, hkepk, nonce, sig)$
AR procures a key, encrypts it with the $hkepk$, and replies with a signed Router Proxy Advertisement message

$MN \rightarrow AR$: $FBU(sourceAddr, hk)$
When MN is ready to handover, it uses the handover key in a Fast Binding Update message

Experiments were run with combinations of multiple mobile nodes, access routers, and intruders. In all cases the network was fixed to support a single message at a time. Increasing the network size caused an exponential blowup in the number of states, since the intruders were able to fill the network with more concurrent combinations of garbage messages that legitimate agents in our model would not process.

Our analysis found no attacks with the complete draft model. Both authentication properies hold, as does the security invariant. We conclude that the proposed SEND-based protocol is sufficient for secure handover-key distribution.

4 Decomposed Models

In addition to determining if the recommended SEND-based protocol is sufficient, we must also determine if each of the pieces which comprise it are necessary. We do this by breaking down the protocol in different ways and rechecking the invariance of each property.

4.1 Reducing Signature Scope

Our first decomposition narrows the scope of the message signature to allow modifications to the source and destination CGAs (cryptographically generated addresses).

An analysis of this model reveals a man-in-the-middle attack, causing the Access Router Authentication property to be violated. This, in turn, can eventually cause the fast binding update to fail.

$$MN \rightarrow AR : RtSolPr(signer : MN, hkepk : MN, nonce : MN) \quad (1)$$
Intercepted by IN
$$IN \rightarrow AR : RtSolPr(signer : IN, hkepk : MN, nonce : MN) \quad (2)$$
AR generates HK for IN, encrypted with $hkepk : MN$
$$AR \rightarrow IN : RtPrAdv(signer : AR, hkepk : MN, hk : IN, nonce : MN) \quad (3)$$
IN forwards unmodified to MN
$$IN \rightarrow MN : RtPrAdv(signer : AR, hkepk : MN, hk : IN, nonce : MN) \quad (4)$$
MN believes it has a legitmate handover key, but AR never assigned a key to it.
$$MN \rightarrow AR : FBU(source : MN, hk : IN) \quad (5)$$
Handover fails, since the handover key was not assigned to the source MN.

In the attack, mobile node MN sends its access router AR a request for a handover key, but the intruder IN intercepts and generate a new request with the MN's handover-key encryption key. When AR generates the handover key for IN and responds, IN cannot decrypt the key, but can can still forward AR's response message to MN. MN has no way to know that the handover key is actually generated for the intruder, so it accepts it. When MN attempts handover later on, the binding update fails.

4.2 No "Noncense"

Our second decomposed model removes the SEND nonce option from the request/response messages. Removing the nonce from the signature scope has the same effect, since if a nonce isn't signed it can be forged en-route. As expected when removing a nonce, a reply attack was found in this model.

$$MN \rightarrow AR : RtSolPr(signer : MN, hkepk : MN) \quad (6)$$
$$AR \rightarrow MN : RtPrAdv(signer : AR, hkepk : MN, hk : IN) \quad (7)$$
IN records (6)
Later, MN reconnects to same AR
$$MN \rightarrow AR : RtSolPr(signer : MN, hkepk : MN) \quad (8)$$
IN intercepts (8), never passes it to AR
$$IN \rightarrow MN : \text{Replay of captured message (6)} \quad (9)$$
$$MN \rightarrow AR : FBU(source : MN, hk : IN) \quad (10)$$
FBU fails, handover key is not valid for MN.

For this attack to work, an intruder need only capture a response message for a particular mobile node at some point in time. Should that mobile node rejoin the access router in the future, the intruder can replay the response, tricking the mobile node into using an invalid handover-key during a binding update.

4.3 CGA Option Removal

Our final decomposed model removes the CGA semantics from the request/response messages. As it turns out, this results in a worst-case scenario. Since the CGA is what binds the public key to the source address,

removing the CGA in effect removes the signature [CGA]. The CGA acts as the certification authority, certifying that the public key is from the source.

The following attack is the worst possible scenario. Both authentication properities are violated, as well as the secrecy property. After the attack, the intruder can initiate handover for the mobile node and hijack whatever packets are meant for the mobile node.

$$MN \rightarrow AR : RtSolPr(signer : MN, hkepk : MN, nonce : MN) \quad (11)$$

Intercepted by IN, signature public key changed, allowing IN to re-sign as MN

$$IN \rightarrow AR : RtSolPr(signer : MN, hkepk : IN, nonce : IN) \quad (12)$$

AR generates HK for IN, encrypted with $hkepk : IN$

$$AR \rightarrow IN : RtPrAdv(signer : AR, hkepk : IN, hk : MN, nonce : IN) \quad (13)$$

IN decrypts handover key (registered to MN), now has handover key!

$$IN \rightarrow MN : RtPrAdv(signer : AR, hkepk : MN, hk : MN, nonce : MN) \quad (14)$$

MN now has real handover key, but secrecy fails!

5 Results

The components of the draft SEND-based protocol are both sufficient and necessary for secure handover key distribution in Fast Mobile IPv6. It is especially important that all message fields, including the destination address, be included in the signature segment of each RtSolPr and RtPrAdv message. Failure to sign all fields can result in an authentication attack, opening the door for an attacker to disrupt handover for participating mobile nodes.

References

[Draft] Distributing a Symmetric FMIPv6 Handover Key using SEND
http://www3.tools.ietf.org/html/draft-ietf-mipshop-handover-key-03

[SEND] RFC 3971: SEcure Neighbor Discovery (SEND)
http://www3.tools.ietf.org/html/rfc3971

[FMIPv6] RFC 4068: Mobile IPv6 Fast Handovers
http://www3.tools.ietf.org/html/draft-ietf-mipshop-fmipv6-rfc4068bis-04

[Dill] Murphi Verification System
http://verify.stanford.edu/dill/murphi.html

[CGA] RFC 3972: Cryptographically Generated Addresses (CGA)
http://www3.tools.ietf.org/html/rfc3972