SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2008; **1**:511–520
Published online 16 October 2008 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.62

Early security key exchange for encryption in Mobile IPv6 handoff

Tin-Yu Wu[1*,†], Chi-Hsiang Lo[2,3] and Han-Chieh Chao[2,3,4]

[1]*Department of Electrical Engineering, Tamkang University, Taipei, Taiwan*
[2]*Institute of Computer Science & Information Engineering, National Ilan University, Ilan, Taiwan*
[3]*Department of Electronic Engineering, National Ilan University, Ilan, Taiwan*
[4]*Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan*

Summary

Wireless equipment has become ubiquitous. However, in facing various software attacks, wireless linked networks are more vulnerable than wire linked networks. The general problem with Mobile IPv6 (MIPv6) (Table I) is the long handover latency period. To reduce the security latency, we propose early security key exchange for encryption in MIPv6 handoff. In our approach, two issues are addressed in dealing with the latency within the encryption technology during the handover. First, we extend the Early Binding Update (EBU) method to deal with the long security exchange negotiation time for the MIPv6 handoff. Second, we adopt the Security Access Gateway (SAG) to solve the limited computing and memory in the Mobile Node (MN). Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: SAG; MIPv6; security handover latency

1. Introduction

Mobile IPv6 (MIPv6) provides mobile techniques for new IP-based services over wireless networks, allowing users to access on-line services while Roaming. MIPv6 offers more advantages than Mobile IPv4 (MIPv4). In MIPv6, the Mobile node (MN) uses Route Optimization (RO) permits talking directly to its peers while retaining the ability to move around and change the currently used IP addresses. The packets go through a shorter route instead of a triangle route with the other end on the Home Agent (HA). Therefore, MIPv4 confronts extra delays due to the triangular routing and the lack of addresses and high signaling load [1].

The security risks occur because of the binding process. Therefore, under the end-to-end principle, MIPv6 designed a procedure called Return Routability (RR), RFC3775, and RFC3776 to compensate for the differences in trust relationships and authentication between these nodes. Return Routability Binding Updates (BUs) sent to Corresponding Node (CN) do not require a security configuration association or an authentication infrastructure between the MN and CN. Nevertheless, RR has some disadvantages. For instance, RR cannot provide a satisfactory security level or deal with fixed CN while another node is dealing with a mobile CN. This is based on a simple BU signal protection. Furthermore, there must be additional Internet Key Exchanges (IKE) and IP

*Correspondence to: Tin-Yu Wu, Department of Electrical Engineering, Tamkang University, Taipei, Taiwan.
†E-mail: tyw@mail.tku.edu.tw

Table I. Acronyms.

AAA	Authentication, Authorization, Accounting
AR	Access Routers
BUs	Binding Updates
CoA	Care-of-Addresses
CBU	Certificate-based Binding Update
CN	Corresponding Node
CN_{HA}	Correspondent Home Agent
CN_{MN}	Correspondent Mobile node
DKM	Directed Key Migration
EBA	Early Binding Acknowledgement
ECBU	Extended Certificate-Based Update Protocol
EEBU	Extended Early Binding Update
FA	Foreign Agent
HA	Home Agent
HoA	Home of Address
HMIPv6	Hierarchical Mobile IPv6
IETF	Internet Engineering Task Force
IKE	Internet Key Exchanges
IPSec	IP Security
MAP	Mobility Anchor Point
MH	Mobile Host
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
ML-IPSec	Multi-layered IPSec
PKD	Proactive Key Distribution
QoS	Quality of Service
REQ	Request
RO	Route Optimization
RR	Return Routability
SA	Security Associations
SAG	Security Access Gateway
SAG-CN	Security Access Gateway-Corresponding Node
SAG-MN	Security Access Gateway-Mobile Node

Security (IPSec) to deal with the higher security requirement. IKE requires heavy computing overhead, making it unsuitable for mobile devices [2–4].

Today, numerous researches have focused on authentication and data encryption during handover. Only a few inventions protect all traffic between the MN and CN with limited computing and memory equipment. Wireless networks have major weaknesses due to the handoff latency. Additional secret protocols increase the latency and this is a critical problem in real-time traffic.

We therefore propose an early security key exchange for encryption during MIPv6 handoff. This process is designed to reduce the handover latency. According to the present statistics, additional security procedures will double the encryption latency. Our design is aimed at reducing the latency from encryption technology during the handover. The Extended Early Binding Update (EEBU) procedure is used to deal with the long-term security exchange negotiation in MIPv6 handoff. The IPSec tunnel protects all traffic between the MN and CN.

In our approach three aspects are expressed as follows: (1) define and present how all traffic is protected between the MN and CN; (2) how the Security Access Gateway (SAG) is used to solve the limited MN computing power and memory; and (3) reduces the security exchange latency over handoff [7–9].

Section 2 introduces the related works. Section 3 illustrates the early security key exchange for encryption in MIPv6 handoff and the performance evaluation. Section 4 describes whether the CN is a MN or not. Section 5 presents the performance analysis. The conclusion and the future studies are elaborated in Section 6.

2. Related Works

A brief overview of the EBU process is given. The mobile Multi-layered IPSec (ML-IPSec) supplies MIPv4 handoff security between the HA and Foreign Agent (FA). The Extended Certificate-based Update (ECBU) Protocol is the HA that handles strong authentication for its MNs and the authentication process between wired devices. Finally, we present two similar researches.

2.1. Early Binding Update [3,4,7]

The RFC 3775 describes the MIPv6 protocol roaming procedure in detail. However, the MN has a weakness; the latency during handover, such as packet loss, latency and out of sequence packets. The above-mentioned situations will become serious within a long-term handover period. When the RR precedes the MN it must wait for both address tests to conclude before it can be registered at a new care of address. The EBU can improve these problems. EBU presents an optimization for MIPv6 correspondent registrations to reduce the latency of both address tests. Generally, three phases are used throughout the performance evaluation: Pre-handover phase, Critical phase, and Post-handover phase.

Figure 1 shows that the EBU uses Pre-handover phases to Pre-procedure Home Keygen Token. Home Keygen Token delivers the MN to the legitimate owner of the home address. During handover, the approach needs to send a HoTI and also to receive a HoT and therefore carry home-address test through the Pre-handover phase.

2.2. Mobile Multi-layered IPSec [10]

In IP layer, security data confidentiality and integrity are measured. The IPSec is usually adopted to encrypt end-to-end data. However, some services are not

DOI:10.1002/sec

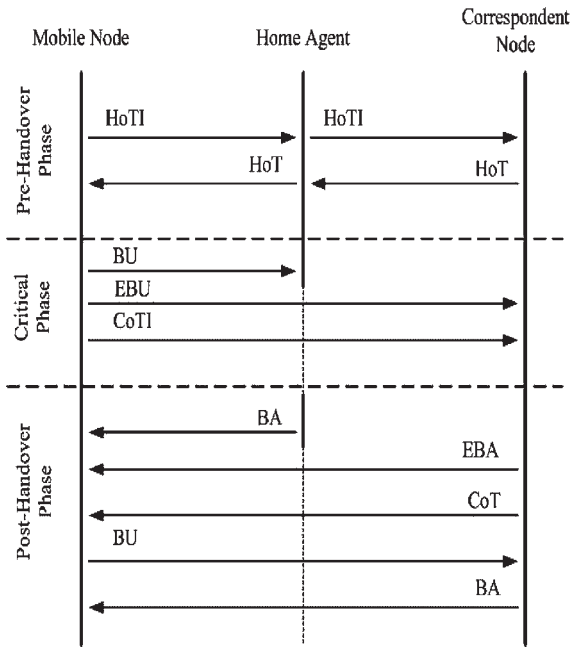

Fig. 1. Early binding updates.

provided; for example, TCP acknowledgment information is not available if the end-to-end encryption is in use or mobile routers cannot use IPSec because the information needed by these algorithms resides inside the encrypted packet. Therefore, the ML-IPSec modifies IPSec so that certain portions of the datagram may be exposed to intermediate network elements.

These authors define and present performance measurements for an efficient key distribution protocol to enable fast ML-IPSec session initialization. There are two protocols that support mobility, Proactive Key Distribution (PKD) and Directed Key Migration (DKM). The PKD focuses on fast handoff by pre-distributing keys through FA. PKDs are neighbors of the current FA. The advantage of this mechanism is that the overhead and handoff latency during handover are reduced and decreased. The disadvantage is that the active key information must be stored in more nodes. The DKM is stored only in the FA, which actively serves the mobile host (MH). When the MH moves to a FA area, the DKM migrates from the old FA to the new FA in a secure manner.

2.3. Extended Certificate-based Update Protocol [11,12]

MIPv6 proposed RR to process BUs. The Internet Engineering Task Force (IETF) suggests bundling IKE to improve the authentication ability and to protect the communication channel MN-HA. The RR provides a simple way to protect the BU signals. The authors proposed the ECBU protocol such that one function of the HA is to act as the security proxy for its MNs. The authentication is based on the HA's certificate and the secret session keys are generated by strong cryptosystems. This approach avoids many security obstacles in the RR protocol and provides a simple, integrated, and efficient security solution for mobile communication and based on a Certificate-based Binding Update (CBU) protocol. Figure 2 shows that the ECBU protocol is able to protect all communication channels in MIPv6 networks.

2.4. Forwarding Scheme Extension for Fast and Secure Handoff in Hierarchical MIPv6 [5]

In this paper, the authors propose that the Hierarchical Mobile IPv6 (HMIPv6) and Authentication, Authorization, Accounting (AAA) protocol has ineffective authenticating and BU procedures that limit its Quality of Service (QoS). Thus, the authors propose a forwarding scheme extension for fast and secure handoff which can reduce a handoff delay while

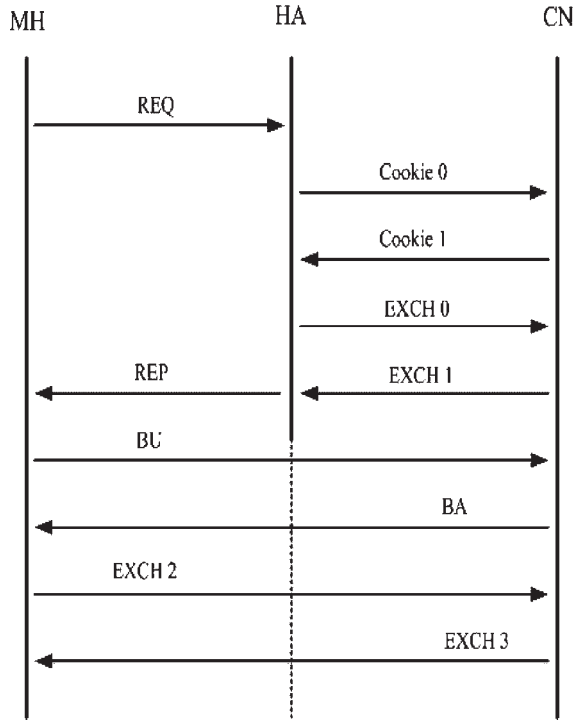

Fig. 2. Extended certificate-based binding update.

DOI:10.1002/sec