Fast Authentication for Secure Internet Service

Kenji FUJIKAWA (ROOT Inc.)
Hitoshi MORIOKA (ROOT Inc.)
Hiroshi MANO (ROOT Inc.)
Overview

• Introduce our MIS Protocol (MISP), a fast authentication protocol on wireless LAN

• Comparison with IEEE802.11 and IEEE802.1x from the point of view of handover latency

• Comparison with IEEE802.11 and IEEE802.1x from the point of view of security
Introduction

• The combination of Wireless LAN and mobile IP is a fast and low-cost mobile communication method.

• But there are some issues.
  – Security Weakness
  – Handover Latency

• So we developed a new link layer protocol, MISP.

• MISP is also adaptable to UPKI or MIAKO.Net
MIS System Architecture

- Home Agent (HA)
- Authentication Servers (AS)
- Mobile Node (MN)
- Base Router (BR)

All APs act as IP routers. So we call them “Base Router”.

MIS Protocol

MISAUTH Protocol
MISP Overview

- MIS protocol is a layer 2 protocol designed for public mobile internet services.
- IPv4/IPv6 are targets as upper layer.
- Lower layer is IEEE802.3 or part of IEEE802.11.
- Features
  - Mutual authentication, session key exchange and network layer setup between a base router (BR) and a mobile node (MN) by ONE ROUNDTRIP PACKET EXCHANGE
  - Effective for fast handover
  - Encryption between AP and STA with periodic key update
  - Authentication of every frame
  - Multiple Service Providers support
- It can be used with MISAUTH protocol (MISAUTHP) which enables remote authentication over IP.
  - based on RADIUS
Layer

In case of using IEEE802.11 as lower layer

- Beacon
- Session Management
- Encryption
- IP Address Assignment
- IEEE802.11 encapsulation
- No DS
- Pseudo Ad-Hoc mode (Ad-Hoc Demo mode)
MISP and MISAUTHP Sequence

Mobile Node

- Channel Scan
- MISP
- Beacon
- Authentication Request
- Authentication Success
- Session Established

Mobile Node

Base Router

- Access Request
- Access Authorization
- Authentication Success

Authentication Server

- MISAUTHP

- Mutual Authentication
- Session Key Sharing
- Assign IP address
Pre-shared Secret Key

- Share a secret key (BR-key)
- Each BR has a different key
- Identified by IP address

- Share an identifier and a secret key (MN-key)
- Each MN has a different key

- No pre-shared information between MN and BR
MIS Protocol Frame Format

• MIS Protocol Control Frame

- IEEE802.11 Header
- IEEE802.2 Header
- MISP Control Message

• MIS Protocol Data Frame (transferring network layer packet)

- IEEE802.11 Header
- IEEE802.2 Header
- MISP Header
- IP Header

Encrypted by MISP

• Ethernet number 0x8893 is assigned for MISP by IEEE.
MIS Protocol Control Message Format

MISP Header

<table>
<thead>
<tr>
<th>Code</th>
<th>Flags</th>
<th>Length</th>
</tr>
</thead>
</table>

Control Message

- Followed by some “objects”

Format of an Object

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value…</th>
</tr>
</thead>
</table>
## Objects

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Name</th>
<th>Beacon</th>
<th>Auth. Req</th>
<th>Auth. Suc</th>
<th>Auth. Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>1</td>
<td>Padding</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>0x02</td>
<td>10</td>
<td>Beacon Timestamp</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>0x03</td>
<td>6</td>
<td>IPv4 Local Address</td>
<td>Optional</td>
<td>Optional</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x04</td>
<td>6</td>
<td>IPv4 Remote Address</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x05</td>
<td>Variable</td>
<td>ICV (Integrity Check Value)</td>
<td>Required</td>
<td>Required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x06</td>
<td>Variable</td>
<td>NAI (Network Access Identifier)</td>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x08</td>
<td>Variable</td>
<td>Session Key Delivery Data</td>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x09</td>
<td>14</td>
<td>Geographical Information</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x0a</td>
<td>3</td>
<td>IPv4 available address number</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x0b</td>
<td>3</td>
<td>IPv4 Source Address Filter</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x0d</td>
<td>4</td>
<td>Error Reason</td>
<td></td>
<td></td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>0xe</td>
<td>2+4n</td>
<td>BR Group</td>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x0f</td>
<td>4</td>
<td>Session Key Valid Time</td>
<td></td>
<td></td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>0x10</td>
<td>4</td>
<td>Serial Number</td>
<td></td>
<td></td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>0x11</td>
<td>4</td>
<td>Beacon Interval</td>
<td></td>
<td></td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>0x12</td>
<td>2+2n</td>
<td>Security Type</td>
<td></td>
<td>Required</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>0x13</td>
<td>8</td>
<td>Uplink Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x14</td>
<td>3</td>
<td>Channel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x15</td>
<td>2+2n</td>
<td>Network Layer Type</td>
<td></td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
Security Types Supported by MISP

• Null (Optional)
  – No security

• HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit (Optional)
  – HMAC-MD5 is used for authentication.
  – HMAC-MD5 is used for delivery of session key.
  – HMAC-MD5 is used for authentication of frame.

• HMAC-MD5/HMAC-MD5/AES-CBC-128bit (Mandatory)
  – HMAC-MD5 is used for authentication.
  – HMAC-MD5 is used for delivery of session key.
  – AES-CBC-128bit is used for data encryption
Beacon

- Beacons are transmitted in 30ms interval.
- Each beacon includes the following information.
  - Timestamp
  - Serial number
  - Beacon interval
  - Group (like SSID)
  - Supported Network layer type
  - Remaining IPv4 addresses
  - Channel
  - Etc…
Behavior of MN

1. An MN makes a list of BRs by scanning channels and receiving beacons. The BRs in the list have corresponding “group (like SSID)”.  
2. The BR list is sorted by the signal strength of the beacon. 
3. The MN try to authenticate to the top of the list of BRs. 
4. If the authentication fails, the MN try to authenticate to the next BR in the list until the end of the list. 
5. After the authentication succeed, the MN can communicate to the network. 
6. The MN makes a registration to the HA. 
7. The MN watches the beacon of connected BR. If the MR cannot receive the beacons of the BR for a certain period or the beacon strength becomes less than the threshold, the MN closes the session and return to 1.
Authentication
(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)
Authentication (Cont.)

(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)
Network Layer Setup

• **IPv4 Configuration**
  – Assign IP address and gateway
  – DNS server, SMTP server, etc. are not assigned because it is premised on mobile IP. In case of using mobile IP, it is enough that fixed servers are installed near the home agent.
  – But it is easy to expand to assign them for non mobile IP users by defining new objects.

• **Other network layer such as IPv6 support is also easy by defining new objects.**
Data Message Format
(HMAC-MD5/HMAC-MD5/AES-CBC-128bit)

- **Code**
- **Flags**
- **Length**

<table>
<thead>
<tr>
<th>Code</th>
<th>Flags</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **IVh**: Upper 8 octets of the Initialization Vector for AES-CBC
- **Payload**: A packet data of the upper protocol
- **Padding**: It makes the payload multiple of 16 octets
- **Protocol ID**: Indicates the network layer protocol

**Encrypted Portion**

- **Padding (variable length)**
- **ICV**
- **Protocol ID**
Encryption, Decryption and Message Authentication (AES-CBC-128bit)

1. 8 octet IVh is randomly generated.
2. Each octet of the IVh rotate 1 bit left. It is IVl.
3. Concatenate IVh and IVl. It is IV.
4. ICV is upper 6 octet of IVh.
5. Encrypt the payload, padding, ICV and Protocol ID by AES-CBC.
6. Make the message by adding MISP header and the IVh.

1. Extract the IVh from the data message.
2. Each octet of the IVh rotate 1 bit left. It is IVl.
3. Concatenate IVh and IVl. It is IV.
4. ICV is upper 6 octet of IVh.
5. Decrypt the data message.
6. Extract the ICV from the decrypted message and compare it to the ICV calculated in 4 to confirm validity.
Session Key Updating

- The session key is identified by the flag in the MISP header.
Communication Blocking in Handover

- Channel Scan
  - Set up link layer and IP layer
- Mobile IP Registration Request
- Detect Disconnection
- Communication Blocking

Signal Strength:
- BR1
- BR2

Time:
- $t_0$
- $t_1$
- $t_2$
- $t_3$
- $t_4$
- $t_5$

HA sends packets to BR1
MN receives packets from BR1

Communication Blocking

Slide 21
Hitoshi MORIOKA, ROOT Inc.
Factors of Communication Blocking

- Channel Scan
- Link Layer Set up
- IP Layer Set up
- Mobile IP registration
IEEE802.11+IEEE802.1x Session Establishment

- 2 roundtrip packet exchanges between MN and AP for association
- 3 roundtrip packet exchanges between MN and AP for authentication.
- 2 roundtrip packet exchanges between AP and RADIUS server for authentication.
- 2 roundtrip packet exchanges between MN and DHCP server for IP layer set up.
Comparison with IEEE802.11, IEEE802.1x and DHCP

Mobile Node → Access Point
- Beacon
- Authentication-Request
- Authentication-Reply
- Associate-Request
- Associate-Accept
- EAPOL-Start
- EAPOL-Request/Identity
- EAPOL-Response/Identity
- EAP-Request/Credentials
- EAP-Response/Credentials
- EAP-Success
- DHCP-Discover
- DHCP-Offer
- DHCP-Request
- DHCP-Ack

Access Point → RADIUS Server
- EAPOL-Request/Identity
- EAPOL-Response/Identity
- RADIUS-Access-Request
- RADIUS-Access-Challenge
- RADIUS-Access-Accept

RADIUS Server → Access Point
- Authentication-Request
- Authentication-Reply
- Access-Accept

Access Point → Authentication Server
- Access-Request
- Access-Authorization
Handover Comparison with IEEE802.11+IEEE802.1x

- If the authentication server is far away from BR(AP), the time needed to establish session is significantly affected by the number of packet exchanges.
- And DHCP needs more time to set up IP layer.
- So MISP has advantage to fast handover because it needs only ONE roundtrip packet exchange between MN and BR, and BR and AS to establish session including IP layer set up.
## Security Comparison with IEEE802.11+IEEE802.1x

<table>
<thead>
<tr>
<th></th>
<th>IEEE802.11+IEEE802.1x</th>
<th>MISP+MISAUTHP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Man-in-the-middle attack</td>
<td>Available by fake EAP success message</td>
<td>Unavailable (avoided by mutual auth.)</td>
</tr>
<tr>
<td>Fake access points</td>
<td>Available</td>
<td>Unavailable (avoided by mutual auth.)</td>
</tr>
<tr>
<td>DoS attack by fake management frame</td>
<td>Available</td>
<td>Depends on implementation</td>
</tr>
<tr>
<td>Session Hijack</td>
<td>Available by MAC address hijacking</td>
<td>Unavailable (avoided by packet auth.)</td>
</tr>
</tbody>
</table>
Most Recent Research

VPN by IPsec6/LIN6/MISP

- Functions for VPN is embedded to Home Residential Gateway (HomeRG)
  - Here, LIN6 is a mobility protocol (instead of MIPv6)
  - MIAKO.Net 4 IMPO

![Diagram of network setup with HomeRG, ForeignRG, and Wireless Terminal connected via a VPN tunnel]
6to4 for interchanging IPv6 packets between HomeRG's
6to4 for interchanging IPv6 packets between HomeRG's (2)
IPv4 connection over IPv6 VPN

NAT

HomeRG
(<HomePref>:<HomeRGID>)

VPN by GIF/IPsec/LIN6/MISP tunnel

ForeignRG

to IPv4 Internet

Wireless Terminal
(<ForeignWLANPref>:<WTermID>)
Advantages of MISP for VPN

- Provides simultaneous access to multiple BR's (base routers, access points)
- Provides fast authentication
- Provides fast handover

Wireless Terminal
(<HomeWLANPref>:<WTermID>,
<ForeignWLANPref1>:<WTermID>,
<ForeignWLANPref2>:<WTermID>)
Multiple Service Providers Support

(a) By BR configuration

(b) By AS proxy
Questions and Comments?