Analysis and Signature of Skype VoIP Session Traffic

Sven Ehlert  
Sandrine Petgang  
Fraunhofer FOKUS, Berlin, Germany  
July 25th, 2006

Students : Amine.Boukioud@ensimag.fr  
Lamya.Boumert@ensimag.fr

Course Link : https://ensiwiki.ensimag.fr/index.php/4MMSR
Authors

- **Sven Ehlert**:
  - Fraunhofer Society
  - Engineering, Networks & Communications, Security & Privacy, SIP/VoIP Security and research

- **Sandrine Petgang**:
  - Fraunhofer Society
  - Skype research
Skype?

- Skype allows its users to place voice calls and send text messages to other users of Skype clients.
- Similar to MSN and Yahoo IM but it has better voice quality and uses different protocols.
Analysis and signature of skype voip session traffic

Introduction

Analyzing network traffic with the goal to detect patterns that are intrinsic to the Skype protocol

Creating a security operator to detect, monitor, or filter Skype traffic
Table of contents

I. Introduction
II. Skype network entities
III. Analysis methods
IV. Skype components
V. Skype message flow
VI. Detection limitations
IV. Conclusion
Skype network entities

**Skype Login server (LS):**
- ✓ manages the creation of Skype usernames
- ✓ handle user authentication

**Skype Client (SC):** a participating user

**Super Node (SN):** is a SC that has a public IP and enough CPU, can perform:
- ✓ Routing tasks (forwarding requests)
- ✓ Forwarding login requests
- ✓ Providing media proxying capabilities
To detect characteristics of Skype's network behavior, they have modified firewall and NAT at both nodes to gain a broader data set.

**Configuration**

**Firewall**
- No firewall protection at all
- UDP and TCP incoming restrictions
- Incoming and outgoing restrictions

**NAT**
- Public addresses without NAT
- Private addresses behind a NAT
Analysis Methods (2/2)

Goals

- Protocol and port usage
- Packet content
- Packet size
Skype’s components (1/3)

- **Ports:**
  A Skype client (SC) opens a TCP (signalization) and a UDP (media streaming) listening port configured in its connection dialog box.

- **Host Cache (HC):**
  A list of super node IP address and port pairs that SC builds and refreshes regularly.

- **Codecs:**
  A wideband codec [1] allowing frequencies between 50-8KHz.
Skype’s components (2/3)

- **Buddy List**
  - In Windows XP, Skype stores its buddy information in an XML file
  - In Linux, Skype stores the ‘config.xml’ file in `$(HOMEDIR)/.Skype/<skypeuserid>`

- **Encryption**
  - Skype uses 256-bit AES encryption
  - Skype uses 1536 to 2048 bit RSA to negotiate symmetric AES keys

- **NAT and Firewall**
  - SC uses a variation of the STUN and TURN protocols to determine the type of NAT and firewall
Skype’s components (3/3)

**STUN:**
- Simple Traversal of UDP through NAT

**TURN:**
- Traversal Using Relay NAT
Skype message flow analysis

- Three distinct tasks:
  - UDP Probe
  - TCP SN Handshake
  - TCP Authentication
## Skype message flow analysis

### UDP Probe

<table>
<thead>
<tr>
<th>Skype 1.4</th>
<th>Skype 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Su1</strong> = 18 bytes</td>
<td><strong>Su1</strong> varies.</td>
</tr>
<tr>
<td><strong>Su2</strong> = 11 bytes</td>
<td><strong>Su2</strong> = 11 bytes</td>
</tr>
<tr>
<td><strong>Su3</strong> = Su1 + 5 bytes</td>
<td><strong>Su3</strong> = Su1 + 5 bytes</td>
</tr>
<tr>
<td><strong>Su4</strong> = 18, 51 or 53 bytes</td>
<td><strong>Su4</strong> = 18, 51 or 53 bytes</td>
</tr>
</tbody>
</table>

**Analysis and signature of skype voip session traffic**
Skype message flow analysis

UDP Probe

Session identifiers:

- U1 is a initiating message
- The first two bytes contain a session identifier

SI = Session Identifier  TF = First 4-Tuple  TS = Second 4-Tuple
SC = IP of Skype Client  SN = IP of Super Node  xx = varying bytes
Skype message flow analysis

UDP Probe

Function parameter:
- The third byte of a message seems to be a message type encoding.

SI = Session Identifier  TF = First 4-Tuple  TS = Second 4-Tuple
SC = IP of Skype Client  SN = IP of Super Node  xx = varying bytes
Skype message flow analysis

UDP Probe

IP Address exchange:

- U2 (4-7) contains the SC's IP address
- U3 (9-12) contains the SN's IP address.

SI = Session Identifier  TF = First 4-Tuple  TS = Second 4-Tuple
SC = IP of Skype Client  SN = IP of Super Node  xx = varying bytes
Skype message flow analysis

TCP SN Handshake

TCP SN signalling:

<table>
<thead>
<tr>
<th>SC</th>
<th>SN</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP, PSH bit, s = 14</td>
<td>T1, v1.4</td>
</tr>
<tr>
<td>TCP, PSH bit, s varies</td>
<td>T1, v2.0</td>
</tr>
<tr>
<td>TCP, PSH bit, s varies</td>
<td>V2.0</td>
</tr>
<tr>
<td>TCP, PSH bit, s = [22..29]</td>
<td>T2</td>
</tr>
<tr>
<td>TCP, PSH bit, s = 339 or other</td>
<td>T3</td>
</tr>
<tr>
<td>TCP, PSH bit, s = 4, 15, 16 or 17</td>
<td>T4</td>
</tr>
</tbody>
</table>

Analysis and signature of skype voip session traffic
Skype message flow analysis

TCP SN Handshake

TCP Restrictions Applied:

<table>
<thead>
<tr>
<th>SC</th>
<th>SN</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP, PSH bit, s = 72 (p.443)/ var. (p.80)</td>
<td>R1</td>
</tr>
<tr>
<td>TCP, PSH bit, s varies</td>
<td>R2</td>
</tr>
<tr>
<td>TCP, PSH bit, s varies</td>
<td>R3</td>
</tr>
<tr>
<td>TCP, PSH bit, s = [23..27]</td>
<td>T2</td>
</tr>
<tr>
<td>TCP, PSH bit, s = 339 or other</td>
<td>T3</td>
</tr>
<tr>
<td>TCP, PSH bit, s = 4, 15, or 16</td>
<td>T4</td>
</tr>
</tbody>
</table>
Skype message flow analysis

TCP SN Handshake

- **Port 443 Operation**: a modification of the Transport Layer Security (TLS) protocol is used.

```
R1
80 46 01 03 01 00 2d 00
00 00 10 00 00 05 00 00
04 00 00 0a 00 00 09 00
00 64 00 00 62 00 00 08
00 00 03 00 00 06 01 00
80 07 00 c0 03 00 80 06
00 40 02 00 80 04 00 80.
```

```
R2
16 03 01 00 4a 02 00 00
46 03 01 40 1b e4 86 02
ad e0 29 e1 77 74 e5 44
b9 c9 9c b4 31 31 5e 02
dd 77 9d 15 4a 96 09 ba
5d a8 70 20 1c a0 e4 f6
4c 63 51 ae 2f 8e 4e e1
e6 76 6a 0a 88 d5 d8 c5
5c ae 98 c5 e4 81 f2 2a
69 bf 90 58 00 05 00.
```
Skype message flow analysis

TCP SN Handshake

- **Port 80 Operation**: it does not use HTTP
Skype message flow analysis

TCP Authentication

- **Restricting Access to LS**: detect messages L3 and L4 exchanged with a randomly selected SN.
- **SN Restricted TCP Access**: TCP access over port 1024 was not allowed, the SC initiated the same handshake over ports 443 and 80.
- **Automatic Login**: the Skype application stores the credentials and retrieves it the next time the user starts up the application. The users does not have to enter his credentials again for further login attempts.

```
C:\Documents and Settings\<username\Application Data\Skype\user\config.xml`, which contains a section `<Account>` with subsection `<credentials>`
```
Detection limitations

- Skyp’s Peer-To-Peer character, the security network has to install monitoring systems at all network points
- Detection of Skype usage in high traffic scenarios requires powerful monitoring hardware
- Patterns differ between the versions, so the detection requires continuous monitoring
Conclusion

• Skype is a P-2-P technology

• Skype architecture:
  ✓ Skype client
  ✓ Super nodes
  ✓ Login servers

• Skype components:
  ✓ Ports
  ✓ Host cache
  ✓ Codecs
  ✓ Body list
  ✓ Nat firewall (STUN-TURN)

• Skype message flow:
  ✓ UDP Probe
  ✓ TCP Handshake
  ✓ TCP authentication
References


M. Fiedler K. Tutschku T. Hossfeld, A. Binzenhoefer. Measurement and analysis of skype


Analysis and signature of skype voip session traffic

At least One 😊