Session Initiation Protocol (SIP) Vulnerabilities

Mark D. Collier
Chief Technology Officer
SecureLogix Corporation
What Will Be Covered

- Introduction to SIP
- General SIP security
- SIP vulnerabilities and attack tools
- Recommendations
- Links
SIP Introduction

Session Initiation Protocol (SIP):

- Is a general-purpose protocol for managing sessions
- Can be used for any type of session
- Provides a means for voice signaling
- Defined by the IETF (looks like an Internet protocol)
- Resembles HTTP
- ASCII requests/responses
SIP Introduction

Why is SIP important:

- Generally viewed as the protocol of the future
- Designed to be simple (it’s not) and extensible
- Supported by major vendors (sort of)
- Used by many service providers
- Provides a foundation for application support
- Will be used for public VoIP access
SIP Introduction

Public Voice Network

Internet

SIP Trunk

IP PBX

TDM Phones

IP Phones

Voice VLAN

Data VLAN

PCs

Internet Connection
## SIP Components

<table>
<thead>
<tr>
<th>Proxy</th>
<th>User Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SDP</td>
</tr>
<tr>
<td></td>
<td>Codecs</td>
</tr>
<tr>
<td>SIP</td>
<td>RTP</td>
</tr>
<tr>
<td>TCP</td>
<td>UDP</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv6</td>
</tr>
</tbody>
</table>
SIP Call Flow

SIP/SDP UDP/TCP

RTP/RTCP UDP

SIP/SDP UDP/TCP

User

Proxy

Proxy

User
SIP Vulnerabilities

Security issues with SIP:
- SIP is a complex, free format protocol
- SIP itself does not require any security
- Security mentioned in SIP RFC, but not required
- Security degrades to common feature set
- Security is not mandatory even if available
- UDP is commonly used for SIP transport
- Network Address Translation (NAT) breaks security
- Data firewalls do not monitor SIP
SIP Vulnerabilities

SIP-Specific Vulnerabilities:

- Eavesdropping
- General and directory scanning
- Flood-based Denial of Service (DoS)
- Fuzzing Denial of Service (DoS)
- Registration manipulation and hijacking
- Application man-in-the-middle attacks
- Session tear down
- check-sync reboots
- Redirect attacks
- RTP attacks
- SPIT
Eavesdropping

Proxy

Attacker

User

Proxy

User
# Eavesdropping Tools

![Image of Eavesdropping Tools](image)

## Typical SIP and RTP Capture - Ethernet

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>SIP/SIP</td>
<td>Request: INVITE $fo$sip:7080@10.1.101.100;username, with session description</td>
</tr>
<tr>
<td>2</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>SIP/SIP</td>
<td>Status: 100 TryRing</td>
</tr>
<tr>
<td>3</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>SIP/SIP</td>
<td>Status: 200 OK, with session description</td>
</tr>
<tr>
<td>4</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>SIP/SIP</td>
<td>Request: ACK sip:7080@10.1.101.100;username, with session description</td>
</tr>
<tr>
<td>5</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>SIP/SIP</td>
<td>Status: 200 OK, with session description</td>
</tr>
<tr>
<td>6</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>10.1.101.65</td>
<td>SIP/SIP</td>
<td>Request: ACK sip:7080@10.1.101.100;username, with session description</td>
</tr>
</tbody>
</table>

- Frame 9 (214 bytes on wire, 214 bytes captured)
- ethernet Eth1, src: d0:aa:01:02:03:04 (decode: d0:aa:01:02:03:04), dst: cisco:xmb:xmb (decode: cisco:xmb:xmb)
- Internet Protocol, Src: 10.1.101.65 (10.1.101.65), Dst: 10.1.101.70 (10.1.101.70)
- User Datagram Protocol, Src Port: 1604 (5604), Dst Port: 23064 (23064)
- Real-Time Transport Protocol

<table>
<thead>
<tr>
<th>[Stream sent by SIP (Frame 9)]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ... = Version: mrc user version (2)</td>
</tr>
<tr>
<td>... = Padding: False</td>
</tr>
<tr>
<td>... = Extension: False</td>
</tr>
<tr>
<td>2. 0 = Contributing source identifiers count: 0</td>
</tr>
<tr>
<td>... = Bearer: False</td>
</tr>
<tr>
<td>Payload: Type: T.3105 PMU (0)</td>
</tr>
<tr>
<td>Sequence number: 33964</td>
</tr>
<tr>
<td>Timestamp: 10000000723</td>
</tr>
</tbody>
</table>

- Synchronization Source Identifier: f4512f7846
- Payload: 8023b32c3a005123d77291e47456968b00cc0a0bfc...

- Data: 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff
Eavesdropping Tools
Eavesdropping Tools
General/Directory Scanning

Proxy → INVITE, OPTION, or REGISTER Requests → Proxy

Attacker
General Scanning Tools

Nmap has the best VoIP fingerprinting database

```
nmap -O -P0 192.168.1.1-254
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-20 01:03 CST
Interesting ports on 192.168.1.21:
(The 1671 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)
Device type: VoIP phone
Running: Cisco embedded
OS details: Cisco IP phone (POS3-04-3-00, PC030301)

Interesting ports on 192.168.1.23:
(The 1671 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:15:62:86:BA:3E (Cisco Systems)
Device type: VoIP adapter
Running: Cisco embedded
OS details: Cisco VoIP Phone 7905/7912 or ATA 186 Analog Telephone Adapter

Interesting ports on 192.168.1.24:
(The 1671 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0E:08:DA:DA:17 (Sipura Technology)
Device type: VoIP adapter
Running: Sipura embedded
OS details: Sipura SPA-841/1000/2000/3000 POTS<->VolP gateway
```
General Scanning Tools
Directory Scanning Tools
Directory Scanning Tools

Linux tools:

- `dirscan` – uses requests to find valid UAs
- `authtool` – used to crack digest authentication
Denial of Service

Every Component Processing Signaling or Media Is A Target
Flood-based Denial of Service

INVITE, REGISTER Floods

Flood Application On PC

SIP Proxy

SIP Phone
SIP Phone
SIP Phone
SIP Phone
Flood-based Denial of Service Tools
Flood-based Denial of Service Tools

Linux tools:

- inviteflood – floods target with INVITE requests
- registerflood – floods registrar with REGISTER requests
Fuzzing Denial of Service

INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
From: UserAgent<sip:6710@192.168.22.36:6060;user=phone>
To: 6713<sip:6713@192.168.26.180:6060;user=phone>
Call-ID: 96561418925909@192.168.22.36
Cseq: 1 INVITE
Subject: VovidaINVITE
Contact: <sip:6710@192.168.22.36:6060;user=phone>
Content-Type: application/sdp
Content-Length: 0
Fuzzing Denial of Service Tools

Linux tools:
- protos SIP test suite

Commercial tools:
- Codenomicon
Registration Manipulation

Erasing, Adding, or Hijacking a Registration
Registration Manipulation Tools
Registration Manipulation Tools

Linux tools:

- `eraseRegistrations` - removes a registration
- `addRegistrations` - adds one or more bogus registrations
Registration Hijacking

Proxy

Hijacked Session

Proxy

Hijacked Media

User

Attacker

User
Registration Hijacking Tools

Linux tools:

- reghijacker – hijacks a registration, even when using authentication
- authtool – cracks digest authentication
Application Man-in-the-middle

Attacker Places Themselves Between Proxies Or Proxy/UA
Application Man-in-the-middle Tools

Linux tools:
- sip_rogue – rogue SIP proxy or B2BUA
Session Tear Down

Proxy

Attacker Sends
BYE Messages
To UAs

User

Proxy

Attacker

User
Session Tear Down Tools

Linux tools:

- teardown – used to terminate a SIP call
Check-sync Reboot

Attacker Sends check-sync Messages To UA
Check-sync Reboot Tools

SiVuS - The VoIP Vulnerability Scanner v1.09-beta

Message Log:

NOTIFY sip: 901@192.168.1.51 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.103;branch=+r3e-hk843fky9ty
From: sip:901@192.168.1.103;tag=92b188156
To: sip:901@192.168.1.51
Call-ID: 192.168.1.51f
Cseq: 3245590 NOTIFY
User-Agent: SiVuS Scanner
Event: check-sync
Content-Type: application/sip
Subject: SiVuS Test
Expires: 0
Content-Length: 0

NOTIFY sip: 901@192.168.1.51 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.103;branch=+r3e-hk843fky9ty
From: sip:901@192.168.1.103;tag=92b188156
To: sip:901@192.168.1.51
Call-ID: 192.168.1.51f
Cseq: 3245590 NOTIFY
User-Agent: SiVuS Scanner
Event: check-sync
Content-Type: application/sip
Subject: SiVuS Test
Expires: 0
Content-Length: 0

Additional Message Log:

Message Generation Progress:

Completed
Check-sync Reboot Tools

Linux tools:

- `check_sync` - causes a SIP phone to reboot
Redirection

Attacker Sends “301/302 – Moved” Message

Inbound Calls Are Redirected
Redirection Tools

Linux tools:

- redirector – used to redirect calls from a SIP UA
RTP/Audio Injection/Mixing

Attacker Observes RTP and Injects or Mixes in New Audio
RTP/Audio Injection/Mixing

Linux tools:

- rtpinjection - monitors an RTP session and injects or mixes in new audio
SPIT Tools

Linux tools:

- Asterisk – a free, easily installed SIP PBX that makes it easy to generate SPIT
- spitter – a tool that creates SPIT files for Asterisk
Links

- SIP attack tools – [www.hackingvoip.com](http://www.hackingvoip.com)
- ethereal – [www.ethereal.com](http://www.ethereal.com)
- wireshark – [www.wireshark.com](http://www.wireshark.com)
- SiVuS – [www.vopsecurity.org](http://www.vopsecurity.org)
- Cain and Abel - [http://www.oxid.it/cain.html](http://www.oxid.it/cain.html)
- Codenomicon – [www.codenomicon.com](http://www.codenomicon.com)
- Asterisk – [www.asterisk.org](http://www.asterisk.org)
- Trixbox – [www.trixbox.org](http://www.trixbox.org)
Recommendations

- Establish policies and procedures
- Follow best practices for data security
- Secure the platforms, network, & applications
- Use standards-based security, such as TLS and SRTP
- Use SIP firewalls
- Continue to protect legacy networks
- Use knowledgeable security consultants, to design, test, and secure your network
Key Points to Take Home

- SIP is an important VoIP protocol
- SIP will be used for public VoIP access
- SIP is vulnerable to attacks
- There are tools available to implement these attacks
- There are steps you can take to improve security
QUESTIONS?

Contact:
Mark D. Collier
mark.collier@securelogix.com
www.securelogix.com
(210) 402-9669