

# **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):

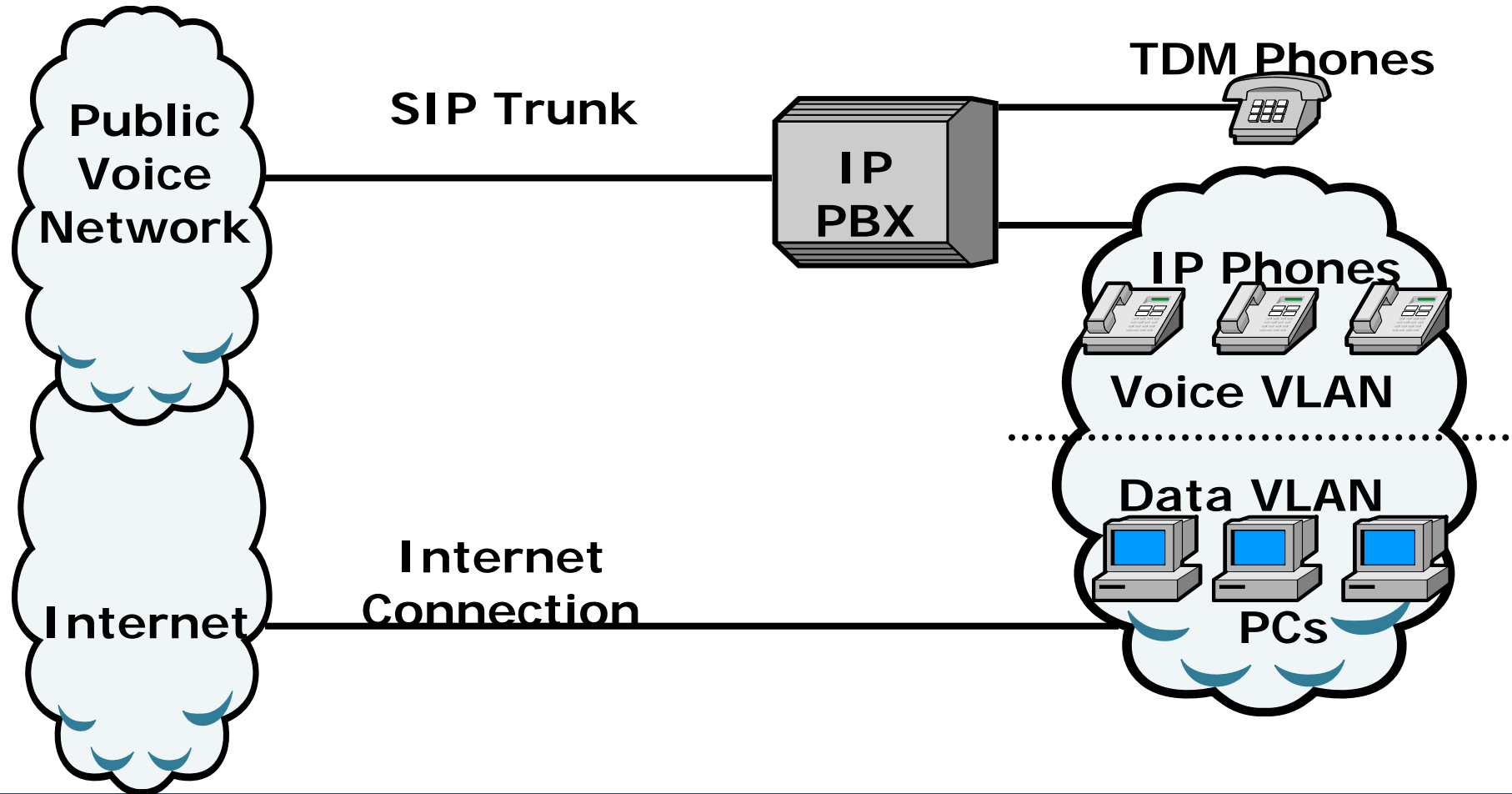
- ◆ Is a general-purpose protocol for managing sessions
- ◆ Can be used for any type of session
- ◆ Provides a means for voice signaling
- ◆ Defined by the IETF (looks like an Internet protocol)
- ◆ Resembles HTTP
- ◆ ASCII requests/responses

## SIP Introduction

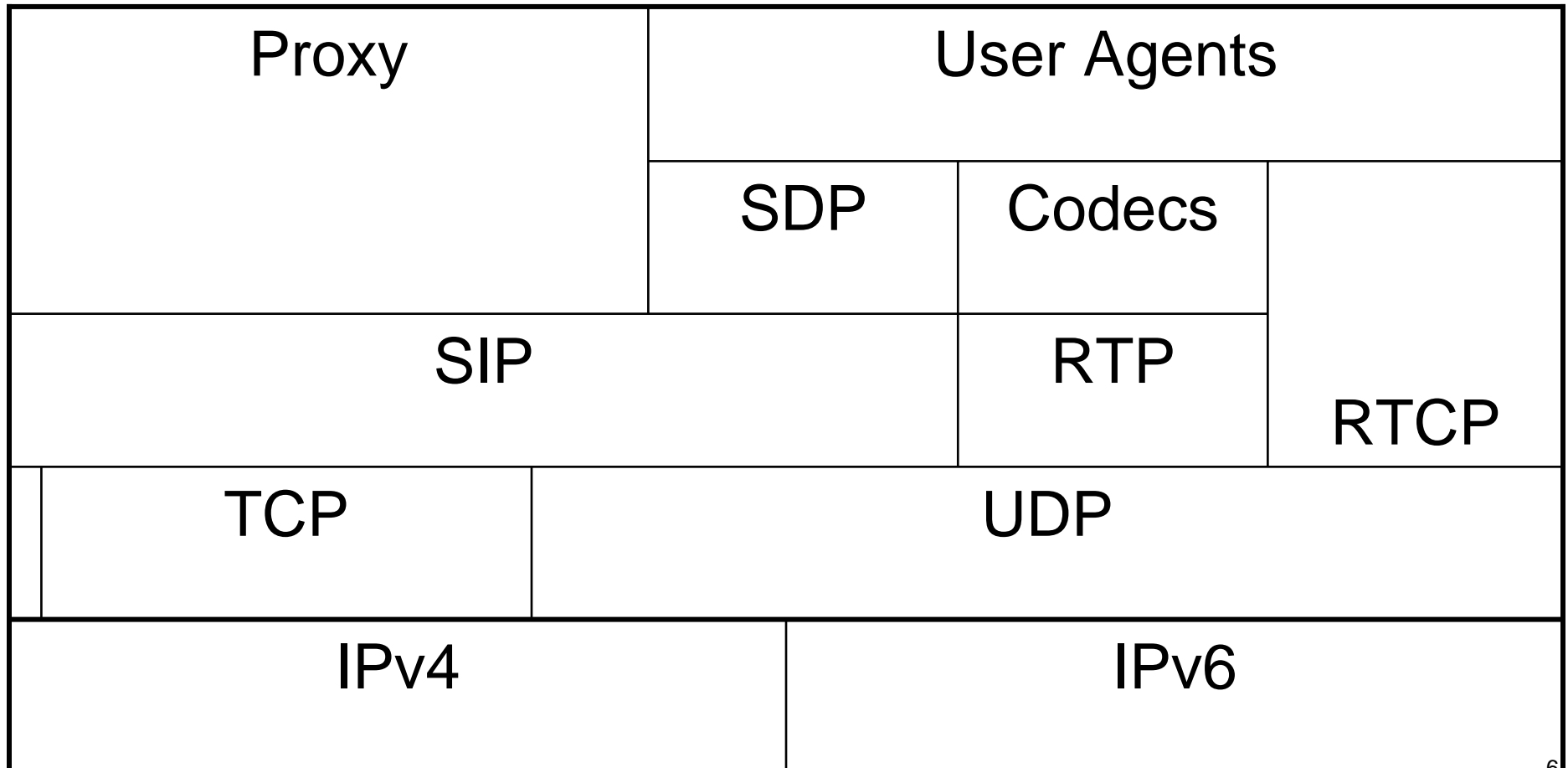
Why is SIP important:

- ◆ 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

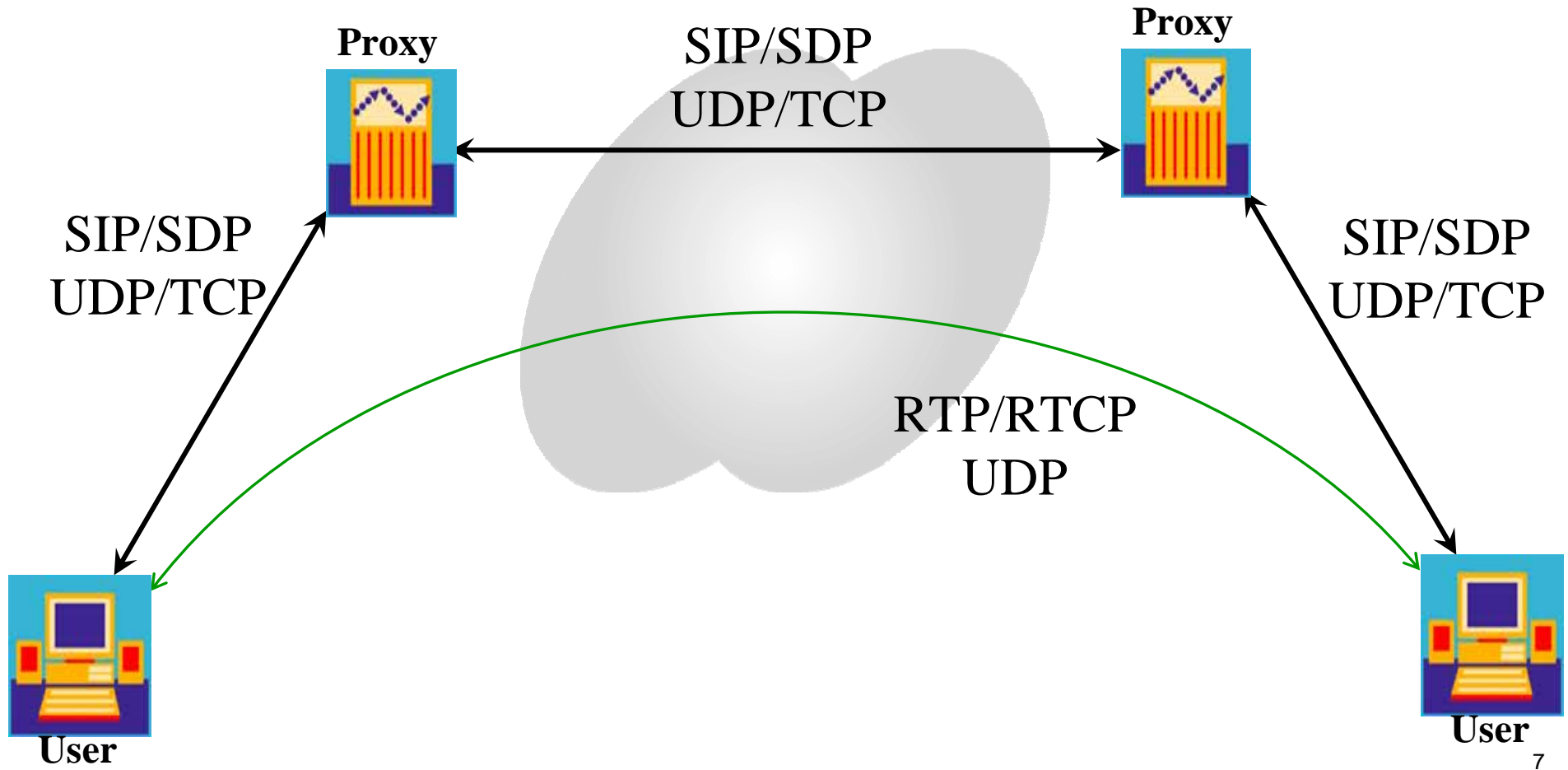
## SIP Introduction



## SIP Components



## SIP Call Flow



## 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

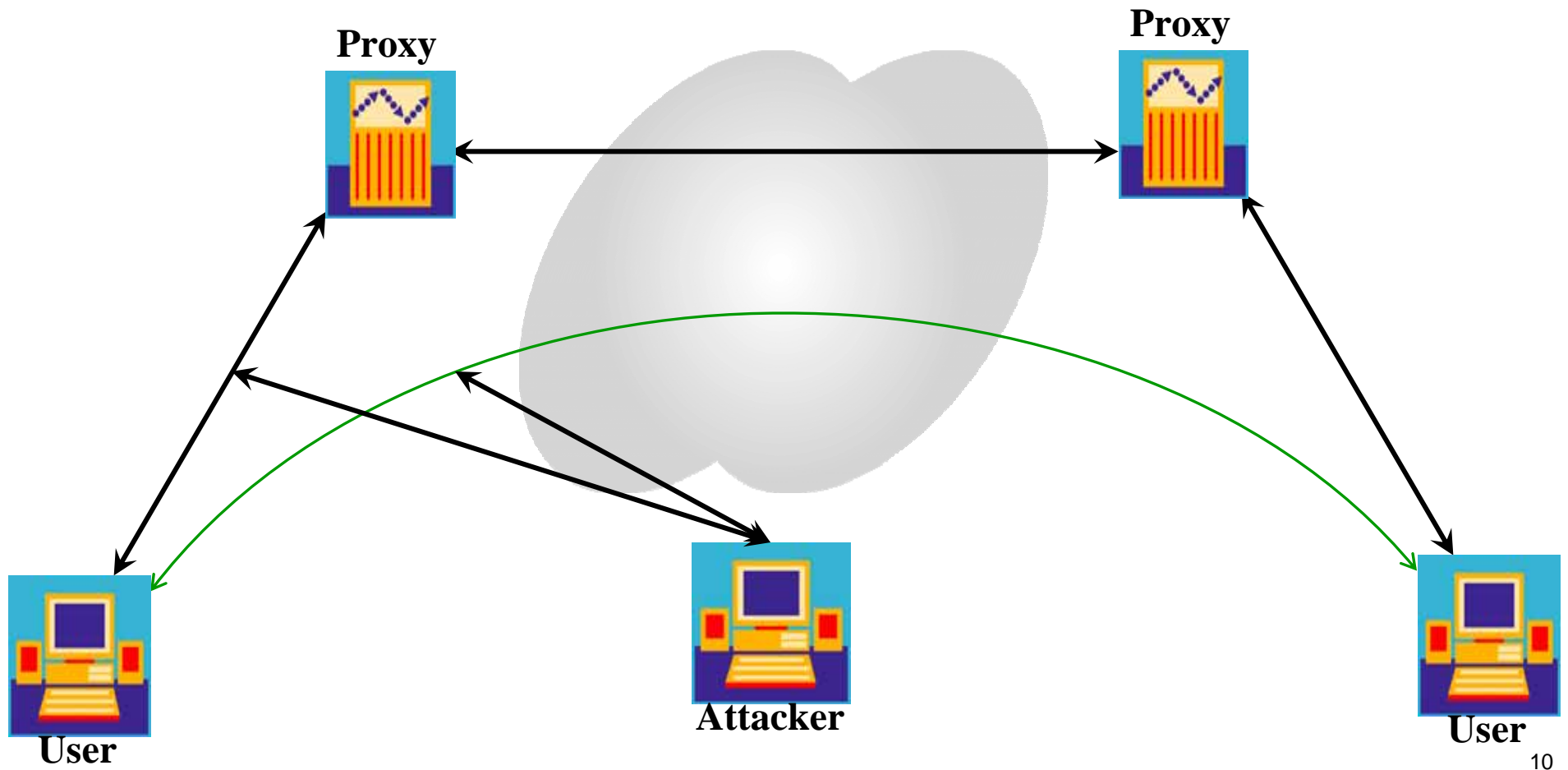


## SIP Vulnerabilities

### 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



# Eavesdropping Tools

The screenshot shows the Wireshark interface with a capture titled "typicalSIPAndRTPcapture - Ethereal". The main pane displays a list of captured packets:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.101.65	10.1.101.1	SIP/SDP	Request: INVITE sip:7000@10.1.101.1;user=phone, with session description
2	0.001008	10.1.101.1	10.1.101.65	SIP	Status: 100 Trying
3	0.002304	10.1.101.1	10.1.101.65	SIP	Status: 180 Ringing
4	1.792547	10.1.101.1	10.1.101.65	SIP/SDP	Status: 200 OK, with session description
5	1.798815	10.1.101.65	10.1.101.1	SIP	Request: ACK sip:7000@10.1.101.1
6	1.799337	10.1.101.1	10.1.101.65	SIP/SDP	Request: INVITE sip:6500@10.1.101.65, with session description
7	1.805588	10.1.101.65	10.1.101.1	SIP/SDP	Status: 200 OK, with session description
8	1.806079	10.1.101.1	10.1.101.65	SIP	Request: ACK sip:6500@10.1.101.65;user=phone
9	1.806632	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35895, Time=3350097723
10	1.826305	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35896, Time=3350097883
11	1.846254	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35897, Time=3350098043
12	1.866227	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35898, Time=3350098203
13	1.886222	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35899, Time=3350098363
14	1.906224	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35900, Time=3350098523
15	1.926216	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35901, Time=3350098683
16	1.943255	10.1.101.1	10.1.101.65	RTP	Payload type=ITU-T G.711 PCMU, SSRC=821511068, Seq=24849, Time=48
17	1.946219	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35902, Time=3350098843
18	1.962871	10.1.101.1	10.1.101.65	RTP	Payload type=ITU-T G.711 PCMU, SSRC=821511068, Seq=24850, Time=208
19	1.966210	10.1.101.65	10.1.101.70	RTP	Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35903, Time=3350099003
20	1.982761	10.1.101.1	10.1.101.65	RTP	Payload type=ITU-T G.711 PCMU, SSRC=821511068, Seq=24851, Time=368

The packet details pane for packet 9 shows the following structure:

- Frame 9 (214 bytes on wire, 214 bytes captured)
- Ethernet II, Src: Grandstr\_00:be:00 (00:0b:82:00:be:00), Dst: Cisco\_6b:83:eb (00:0a:41:6b:83:eb)
- 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: 5004 (5004), Dst Port: 23254 (23254)
- Real-Time Transport Protocol
  - [Stream setup by SDP (frame 6)]
  - 10... .. = Version: RFC 1889 Version (2)
  - ..0. .... = Padding: False
  - ...0 ... = Extension: False
  - .... 0000 = Contributing source identifiers count: 0
  - 0... .. = Marker: False
  - Payload type: ITU-T G.711 PCMU (0)
  - Sequence number: 35895
  - Timestamp: 3350097723
  - Synchronization Source identifier: 3452921845
  - Payload: B2B1B3B9C3DB55423A3737393E4D74D5C6BEBCCOCADBFC...

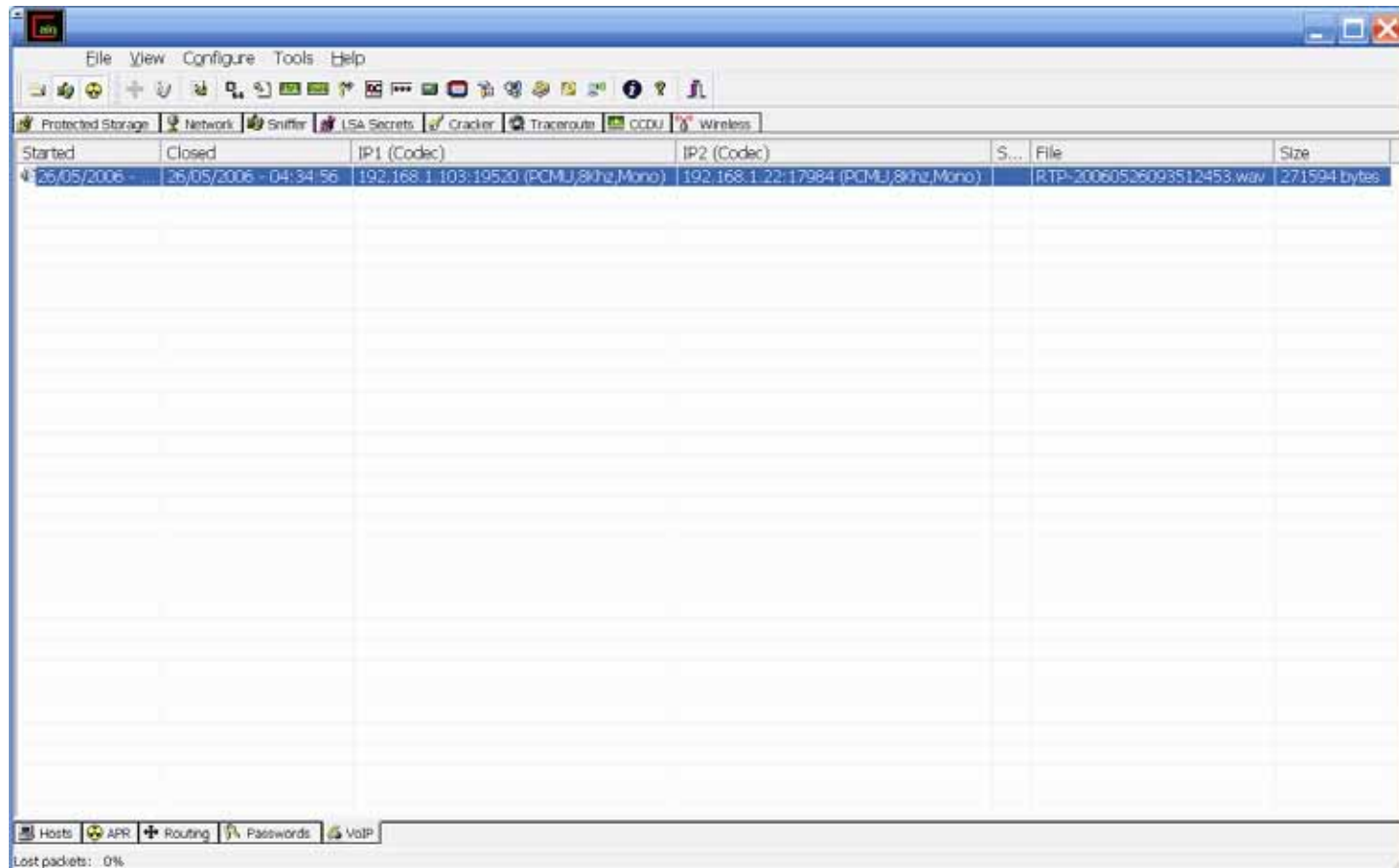
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

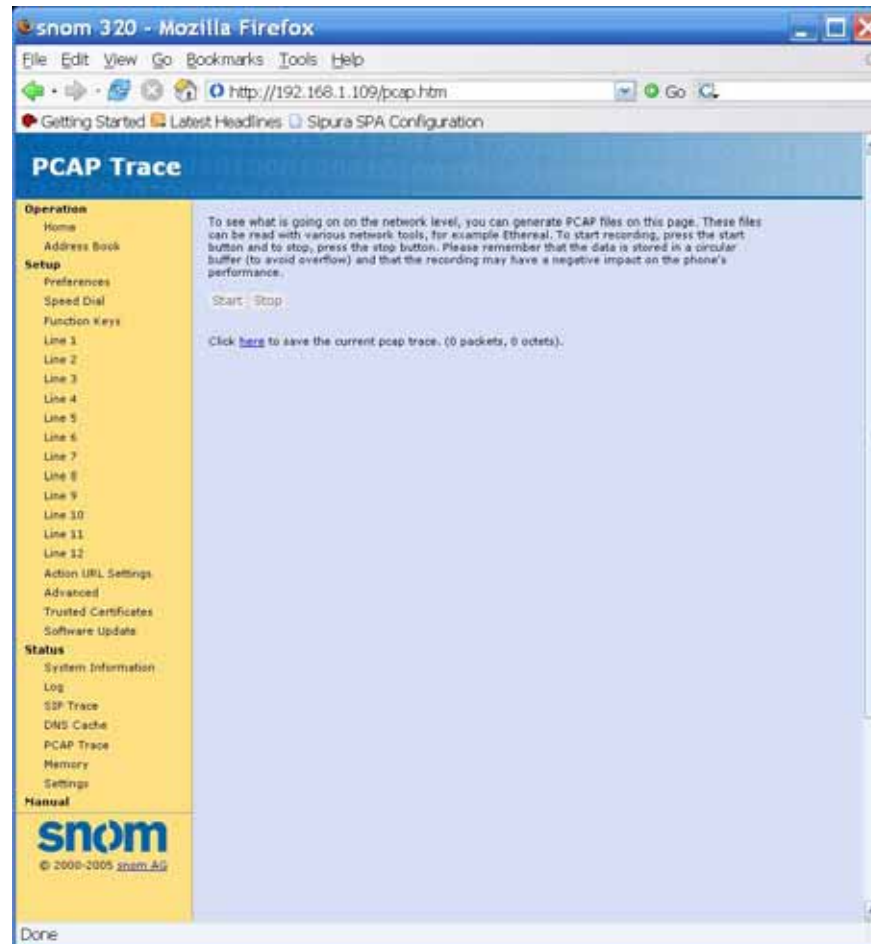
0000 00 0a 41 6b 83 eb 00 0b 82 00 be 00 08 00 45 c0 ..AK....E.
0010 00 c8 9f 36 00 00 fa 11 41 a5 0a 01 65 41 0a 01 ..6....A...eA..
0020 65 46 13 8c 5a d6 00 b4 51 f9 80 00 8c 37 c7 ae eF..Z...Q...7..
0030 6f 3b cd cf 67 f5 b2 b1 b3 b9 c3 db 55 42 3a 37 0;..g...:...UB:7
0040 37 39 3e 4d 74 d5 c6 be bc bc c0 ca db fc 5b 4f 79>Mt...[O
0050 4c 4a 4d 58 64 fd ea de d9 dd df e3 ed ec e5 LJMxd...[O

```

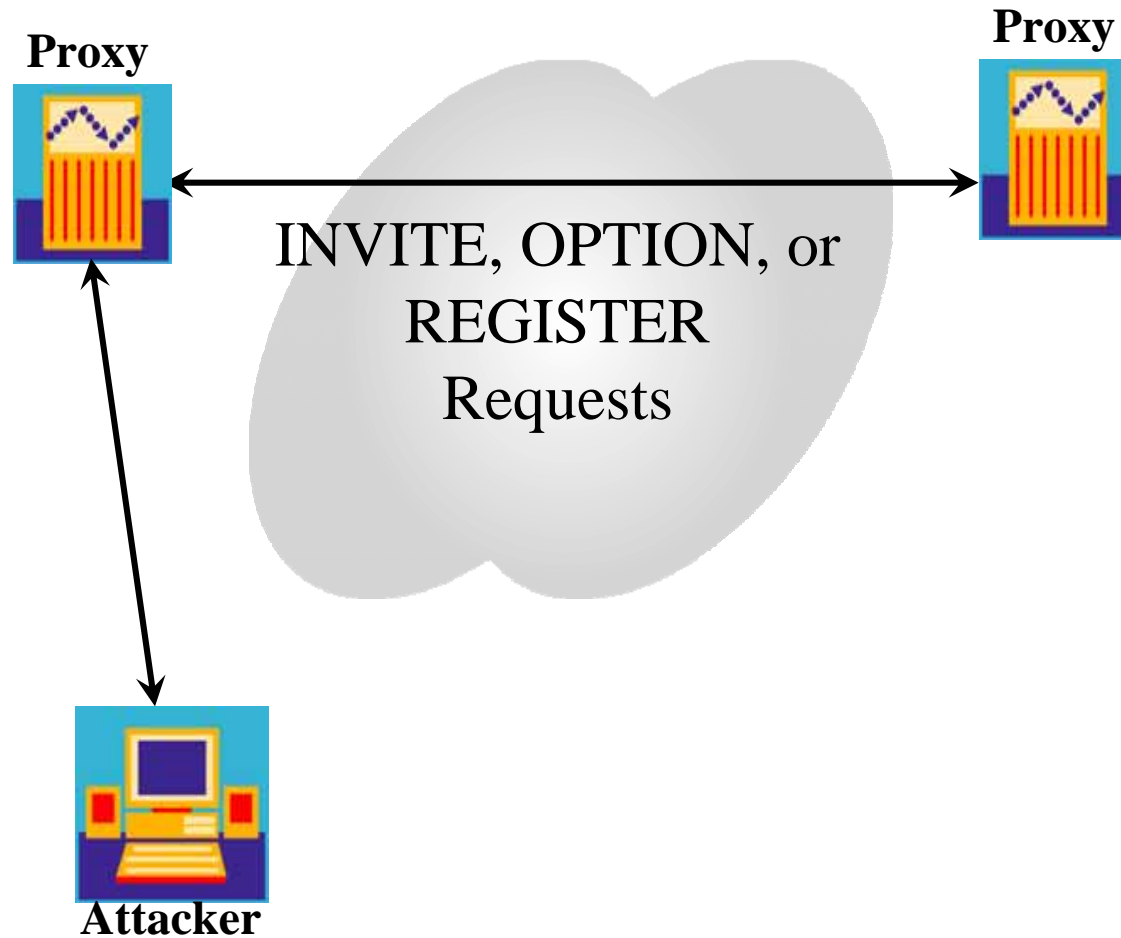
## Eavesdropping Tools



# Eavesdropping Tools



## General/Directory Scanning

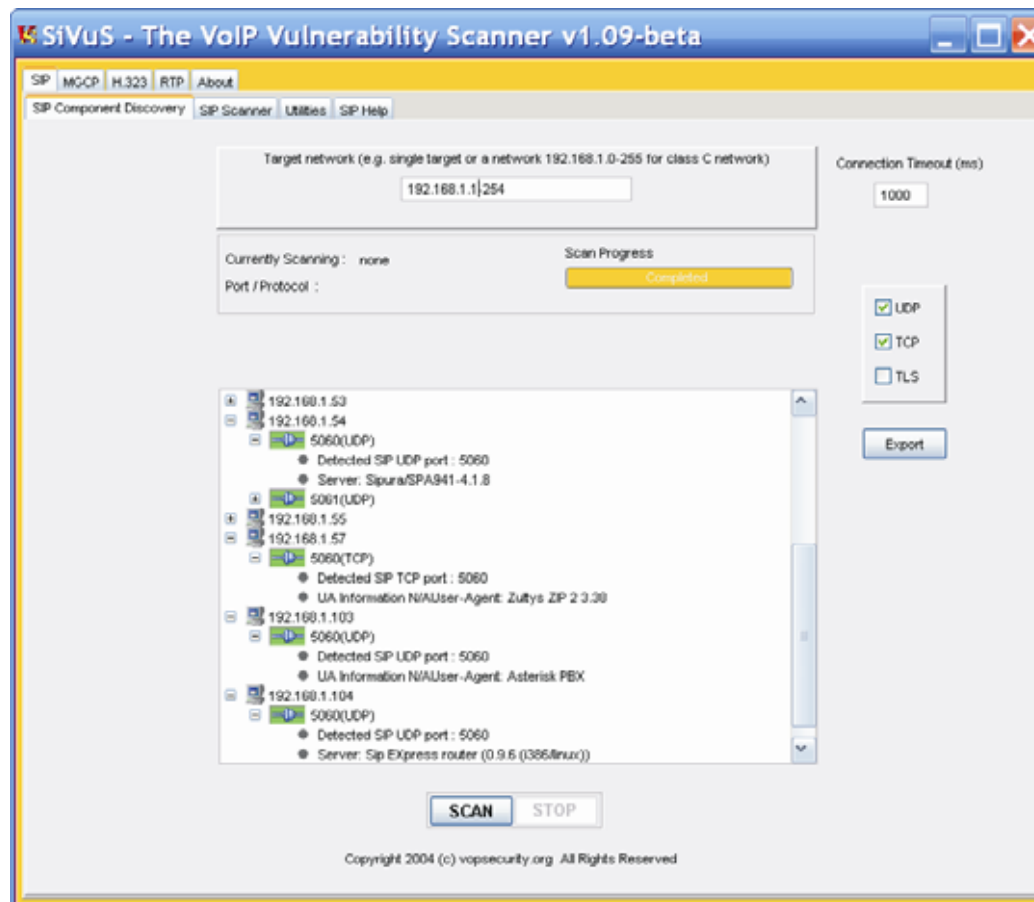


## General Scanning Tools

### Nmap has the best VoIP fingerprinting database

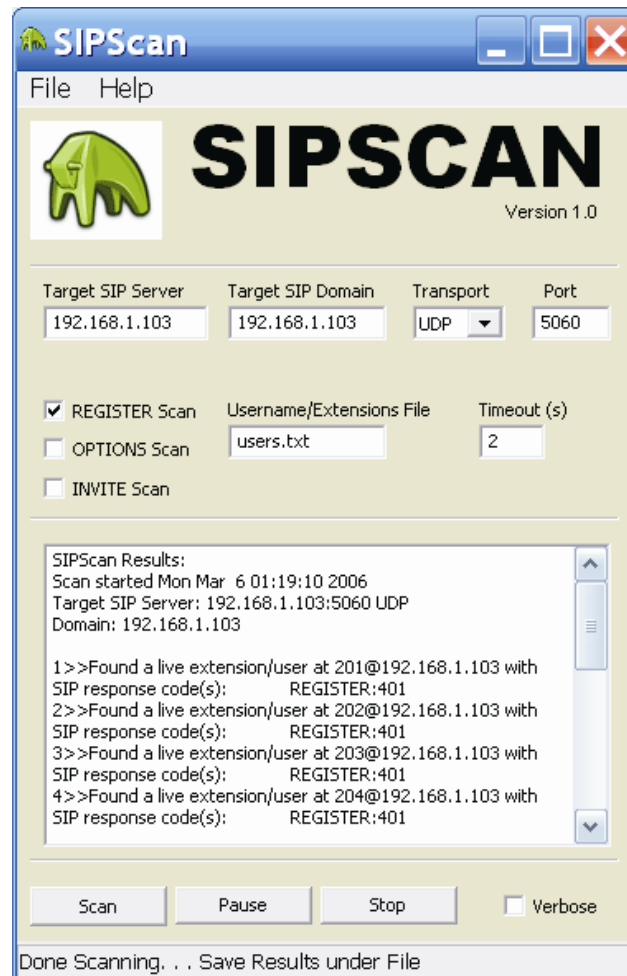
```
nmap -O -P0 192.168.1.1-254
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-20 01:03 CST
Interesting ports on 192.168.1.21:
(The 1671 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)
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 phone|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<->VoIP gateway
```

## General Scanning Tools





## Directory Scanning Tools

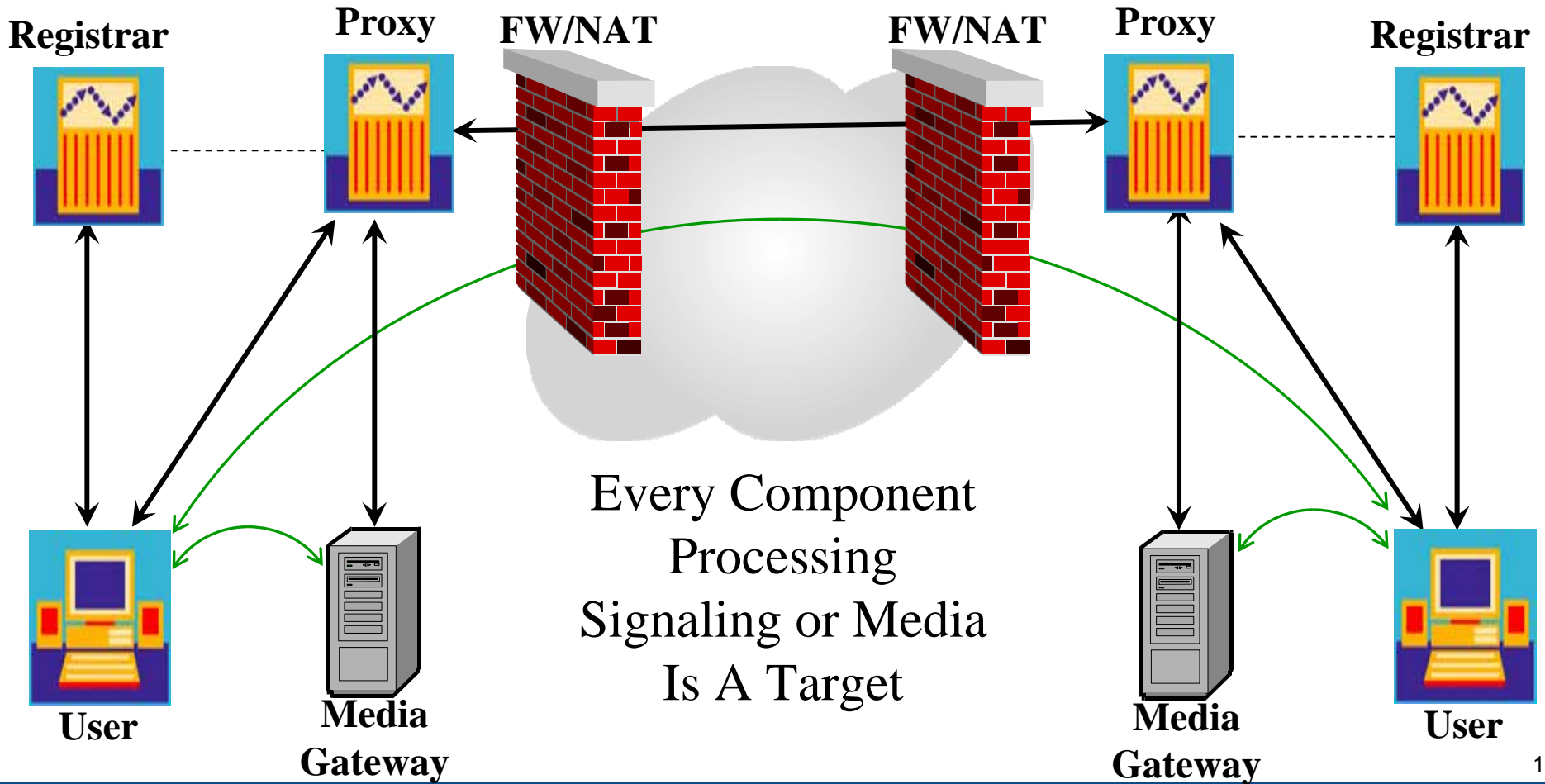


## Directory Scanning Tools

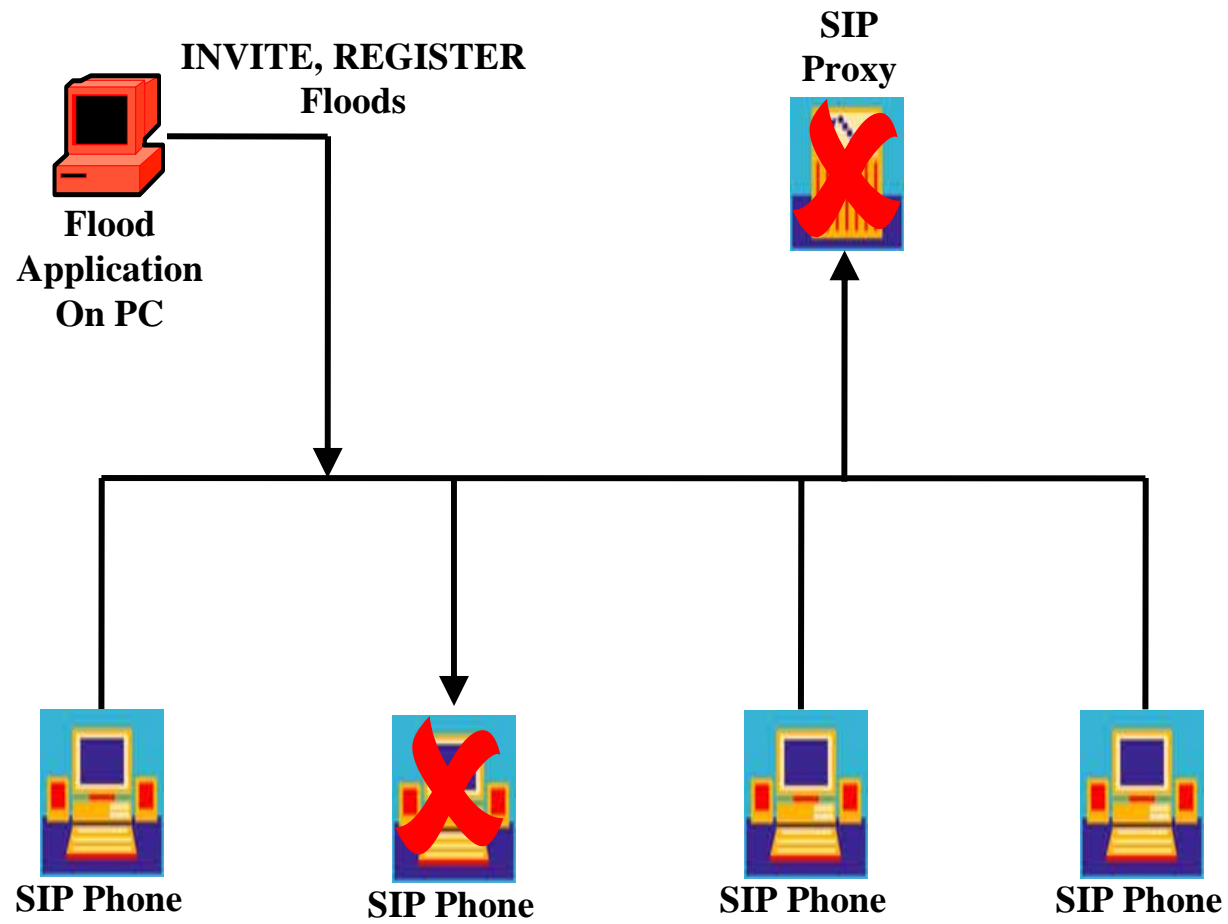
Linux tools:

- ◆ dirscan – uses requests to find valid UAs
- ◆ authtool – used to crack digest authentication

## Denial of Service



## Flood-based Denial of Service



# Flood-based Denial of Service Tools

The screenshot displays the SiVuS application interface. The main window is titled "SiVuS - The VoIP Vulnerability Scanner v1.09-beta". It features a menu bar with options like SIP, MGCP, H.323, RTP, and About. Below the menu bar, there are tabs for "SIP Component Discovery", "SIP Scanner", "Utilities", and "SIP Help". The "SIP Scanner" tab is active, showing a "Message Generator" section with "Authentication Analysis" selected.

The "SIP Message" configuration area includes fields for Method (INVITE), Transport (UDP), Called User (boqus), Domain/Host (10.1.101.2), and Port (5060). Other fields include Via (SIP/2.0/TCP 10.1.101.3), To (<sip:boqus@10.1.101.2>), From (root <sip:root@10.1.101.3>), Authentication, Call-ID (yoQ51xi1PJaR@10.1.101.3), Cseq (123456 INVITE), Contact (<sip:root@10.1.101.3>), Record-Route, Subject (SiVuS Test), Content-type (application/sdp), User Agent (SiVuS Scanner), Expires (7200), Max-Forwards (70), Event, Refer-To, and Content Length (0). A checkbox for "Use SDP?" is checked.

The "SDP message" field contains the following text:

```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```

The "Conversation Log" on the right shows the generated INVITE message details, including headers like Via, From, To, Call-ID, CSeq, Contact, Max\_forwards, User Agent, Content-Type, Subject, Expires, and Content-Length. It also shows the SDP body:

```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
c=IN IP4 192.168.1.2
m=audio 49210 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC/8000
```

At the bottom, there are "Start" and "Stop" buttons, a "Source Port" field set to 5060, a "Packets to Send" field set to 1000000, and a "Message Generation Progress" bar showing 43% completion. A checkbox for "Randomize Source Port" is present and unchecked.

## 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: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaa...
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:

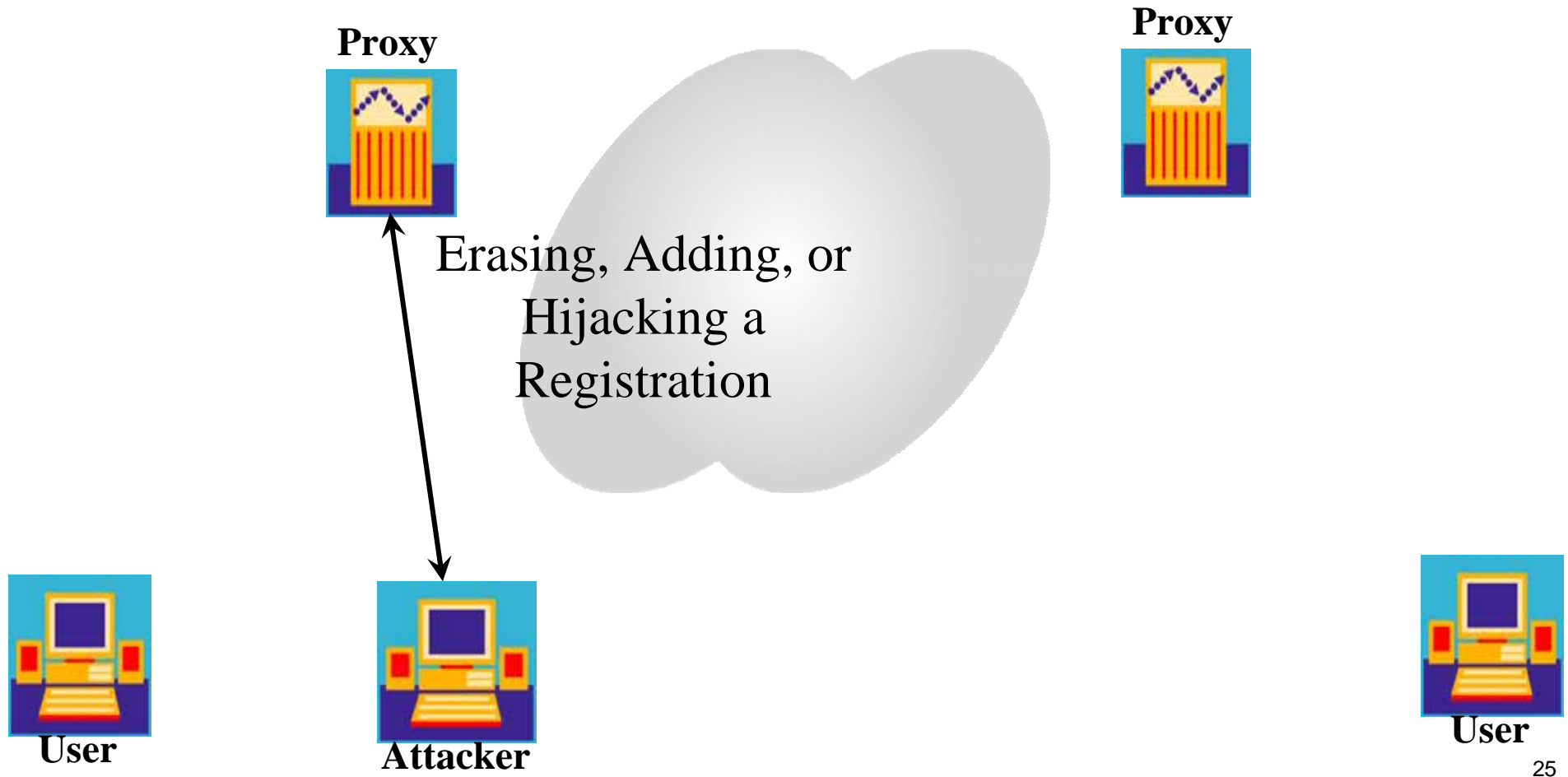
- ◆ protos SIP test suite

Commercial tools:

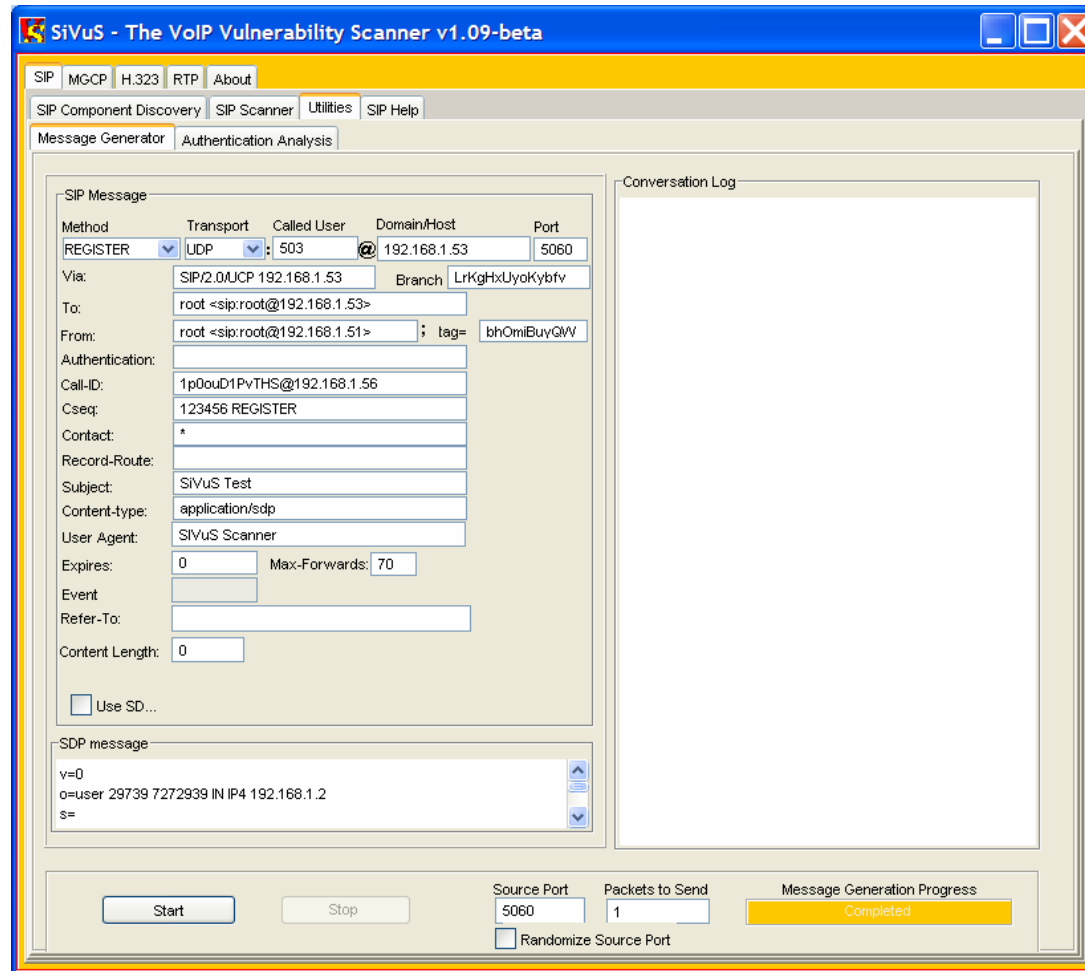
- ◆ Codenomicon



## Registration Manipulation



# Registration Manipulation Tools

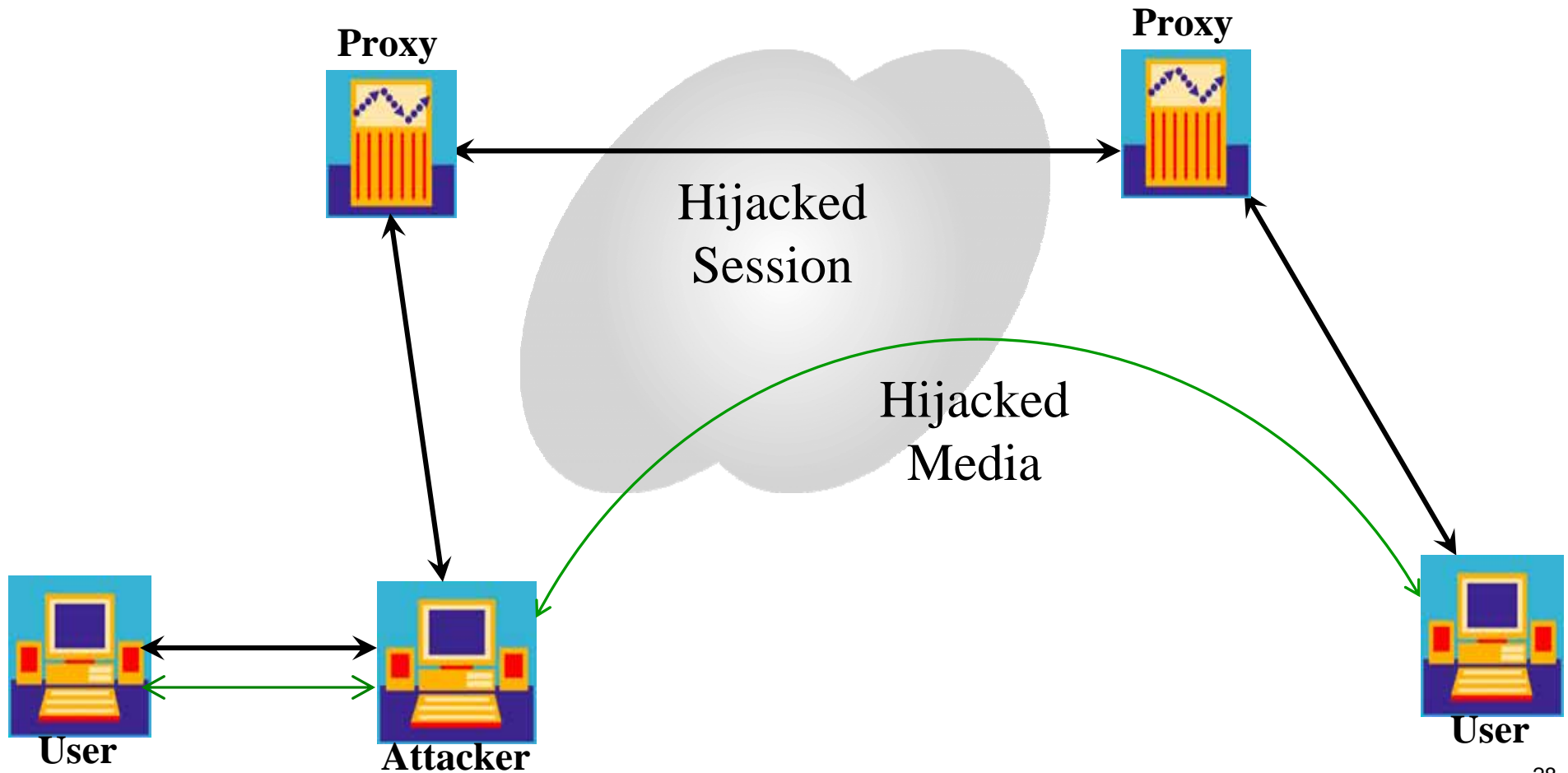


## Registration Manipulation Tools

Linux tools:

- ◆ `erase_registrations` – removes a registration
- ◆ `add_registrations` – adds one or more bogus registrations

## Registration Hijacking

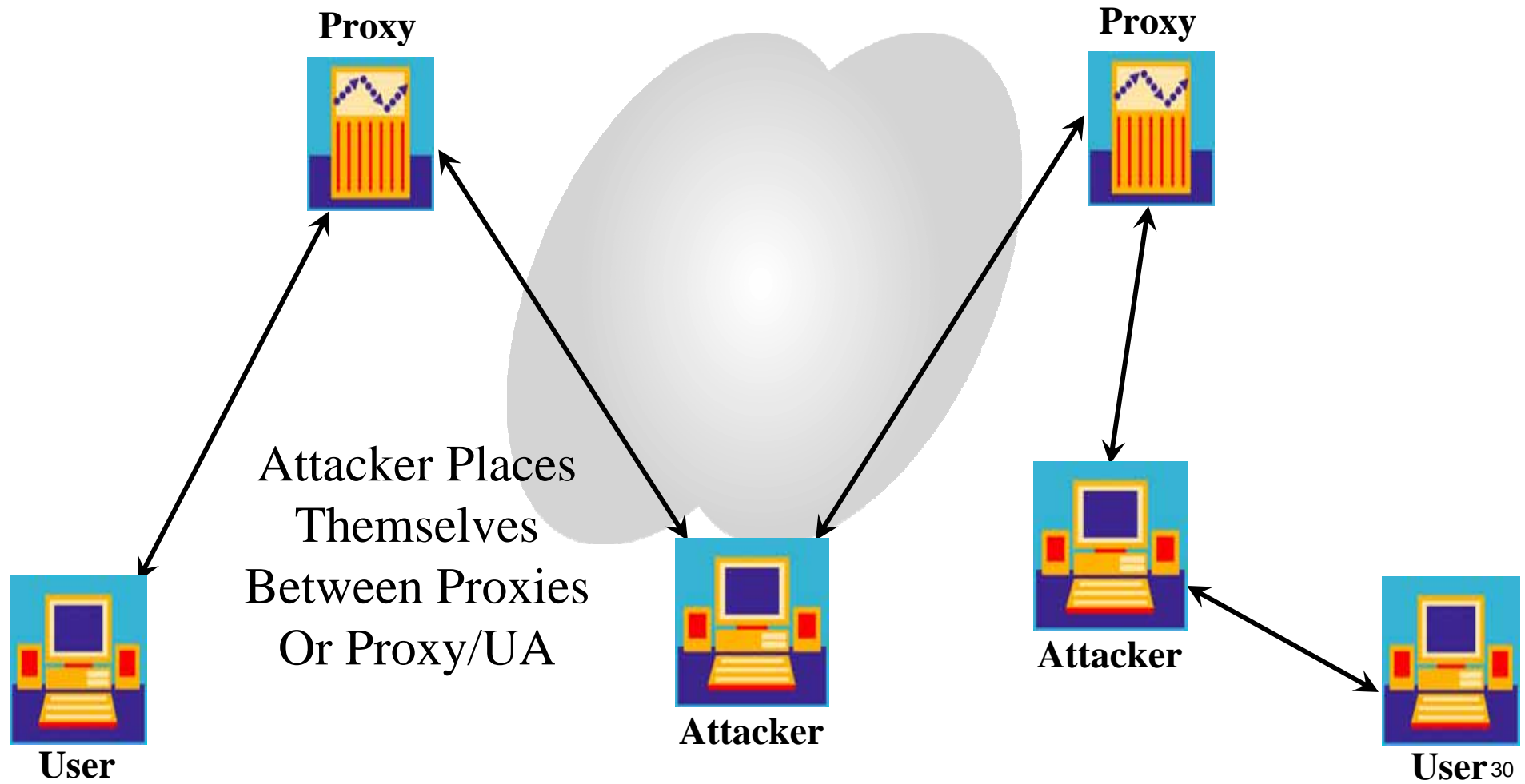


## Registration Hijacking Tools

### Linux tools:

- ◆ reghijacker – hijacks a registration, even when using authentication
- ◆ authtool – cracks digest authentication

## Application Man-in-the-middle

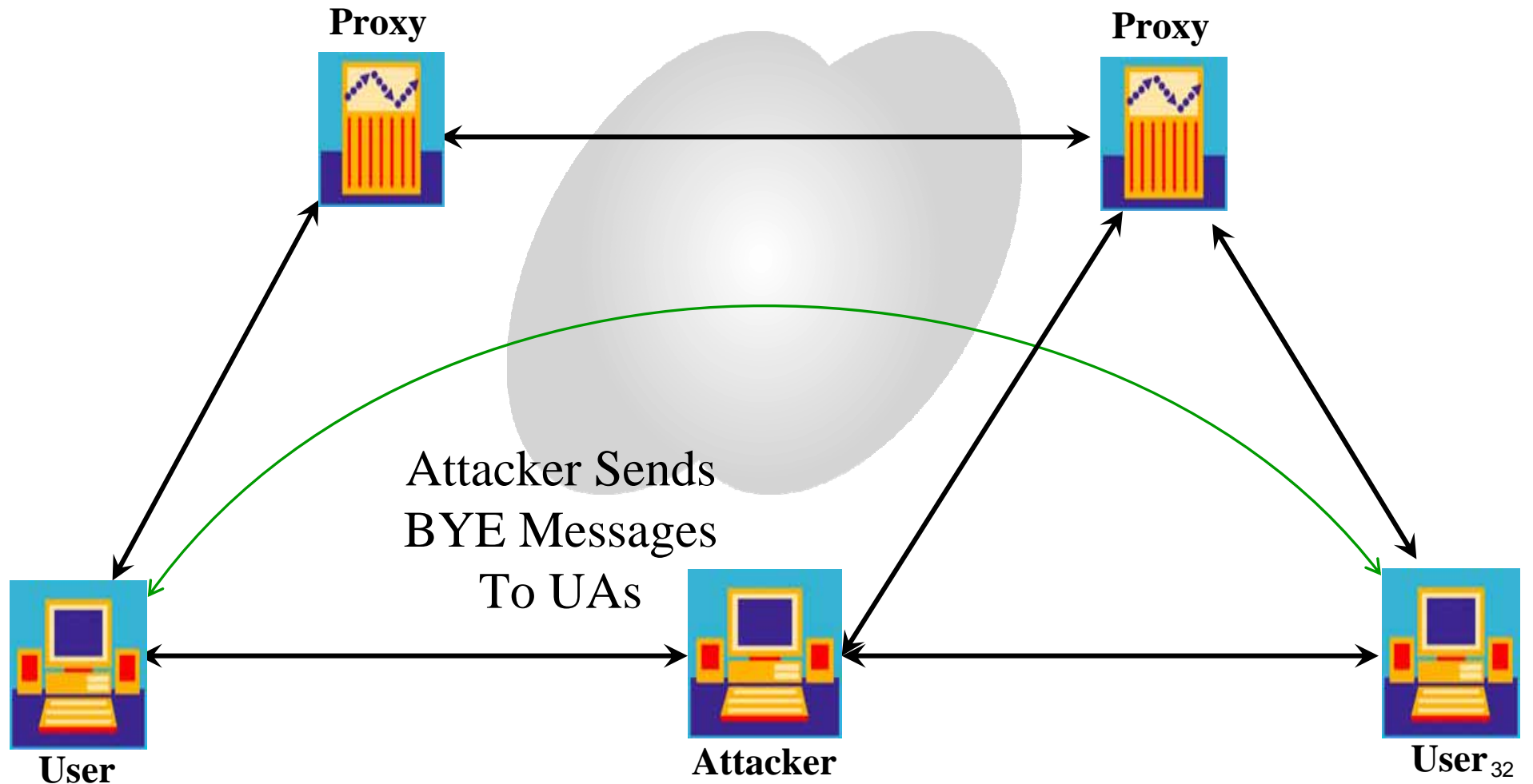


## Application Man-in-the-middle Tools

Linux tools:

- ◆ sip\_rogue – rogue SIP proxy or B2BUA

## Session Tear Down



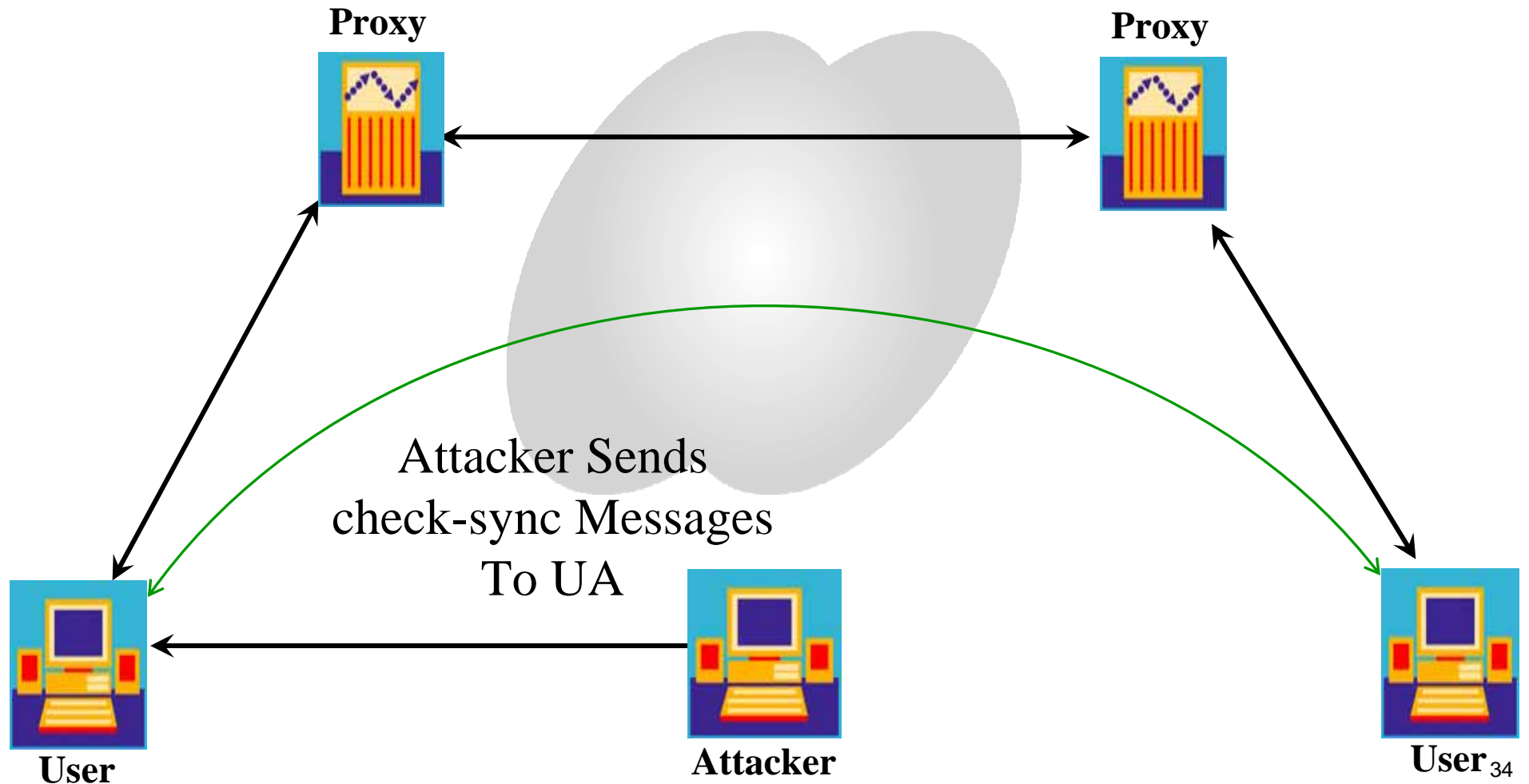


## Session Tear Down Tools

Linux tools:

- ◆ teardown – used to terminate a SIP call

## Check-sync Reboot



# Check-sync Reboot Tools

The screenshot displays the SiVuS - The VoIP Vulnerability Scanner v1.09-beta application window. The interface is divided into several sections:

- Navigation:** Includes tabs for SIP, MGCP, H.323, RTP, and About. Below these are sub-tabs for SIP Component Discovery, SIP Scanner, Utilities, and SIP Help. Further down are Message Generator and Authentication Analysis.
- SIP Message Configuration:** A form with fields for Method (NOTIFY), Transport (UDP), Called User (501), Domain/Host (192.168.1.51), and Port (2051). Other fields include Via (SIP/2.0/UJCP 192.168.1.103), To (root <sip:root@192.168.1.51>), From (root <sip:root@192.168.1.103>), Authentication, Call-ID (1p0ouD1PvTHS@192.168.1.56), Cseq (123456 NOTIFY), Contact, Record-Route, Subject (SIVuS Test), Content-type (application/sdp), User Agent (SIVuS Scanner), Expires (0), Max-Forwards (70), Event (.heck-sync), Refer-To, and Content Length (0). There is a checkbox for "Use SD..." and a text area for "SDP message" containing:
 

```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```
- Conversation Log:** Displays two log entries for NOTIFY messages. The first entry shows:
 

```
NOTIFY sip:501@192.168.1.51 SIP/2.0
Via: SIP/2.0/UJCP 192.168.1.103;branch=LrKgHxUyoKybvf
From: root <sip:root@192.168.1.103>;tag=bhOmiBuyGW
To: root <sip:root@192.168.1.51>
Call-ID: 1p0ouD1PvTHS@192.168.1.56
CSeq: 123456 NOTIFY
Max_forwards: 70
User Agent: SIVuS Scanner
Event: check-sync
Content-Type: application/sdp
Subject: SIVuS Test
Expires: 0
Content-Length: 0
```

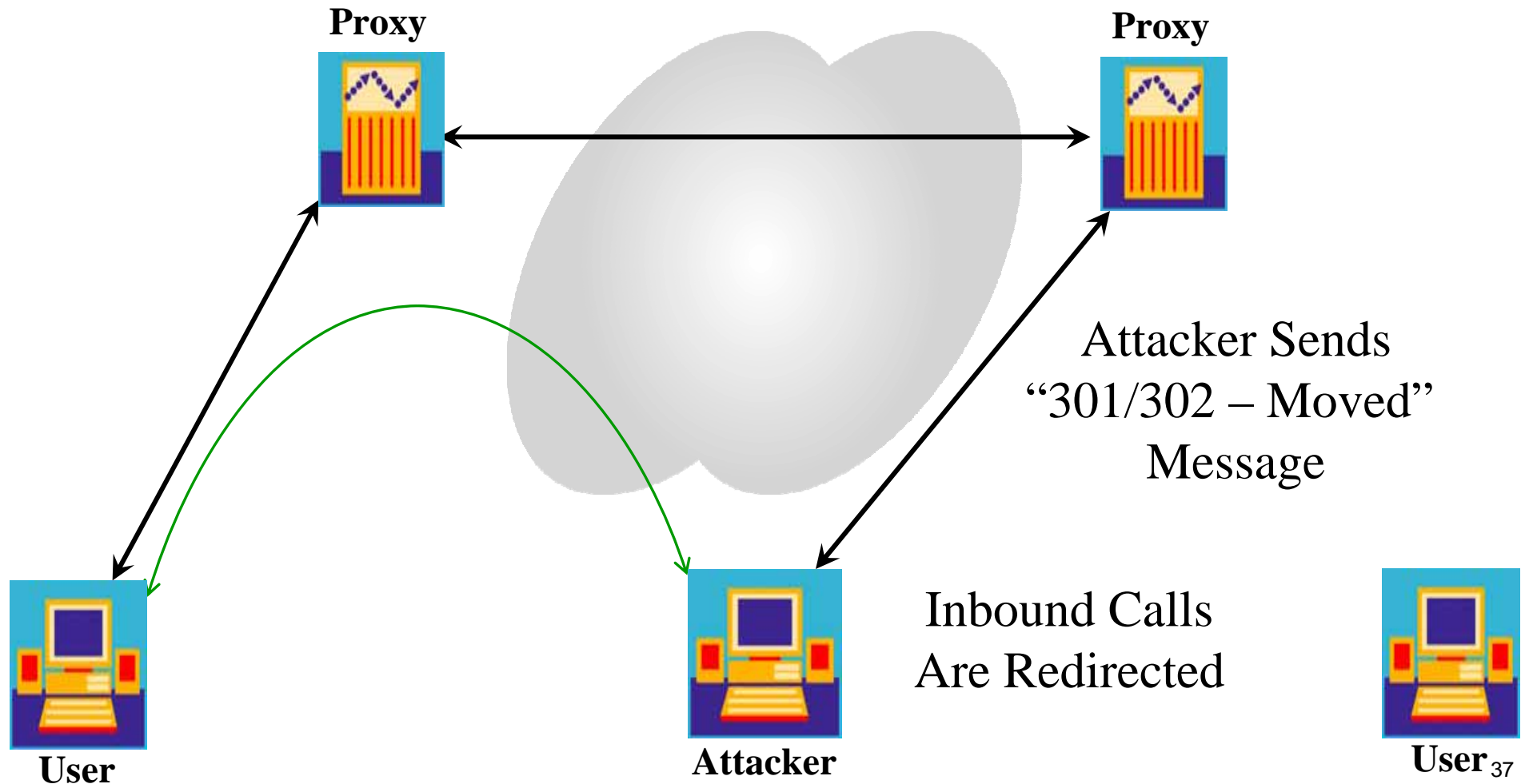
 The second entry is identical.
- Control Panel:** Features a Start button, a Stop button, a Source Port field (5060), a Packets to Send field (1), and a Message Generation Progress bar (Completed). There is also a checkbox for "Randomize Source Port".

## 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



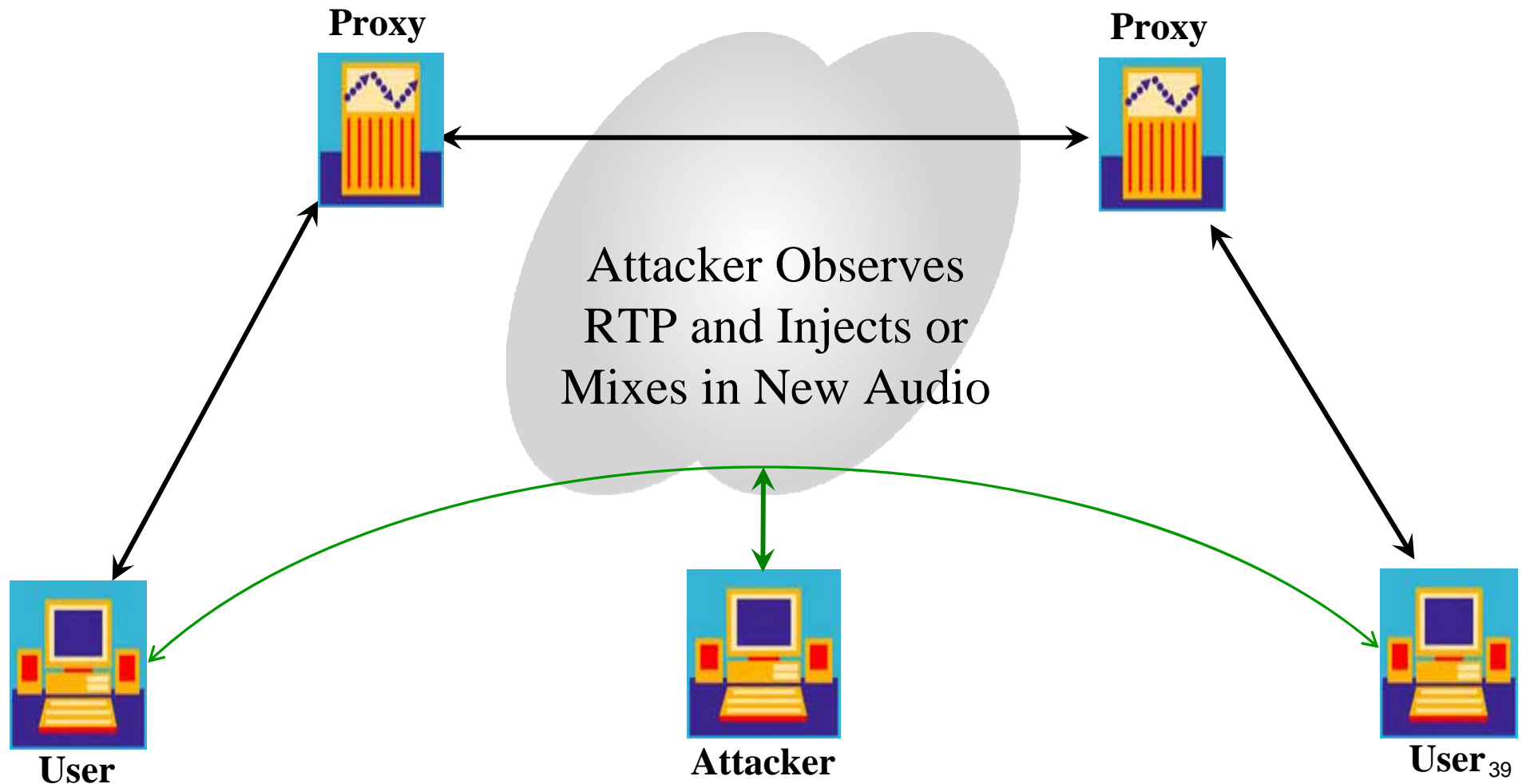
User<sub>37</sub>

## Redirection Tools

Linux tools:

- ◆ redirector – used to redirect calls from a SIP UA

## RTP/Audio Injection/Mixing



## RTP/Audio Injection/Mixing

Linux tools:

- ◆ rtpinjector – monitors an RTP session and injects or mixes in new audio



# SPIT

**VIAGRA**



3 pills - 100mg

**\$85** [ORDER](#)



**DROWNING IN DEBT?**



**WE CAN HELP...**

**The Honest To Goodness  
INTERNET  
Get Rich  
Quick Book!**

The Final Authority For Making  
Big Money On The Web!



By The \$100-Million Roundtable Group

## 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>
- ◆ Fuzzing - <http://www.ee.oulu.fi/research/ouspg/protos/index.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](mailto:mark.collier@securelogix.com)

[www.securelogix.com](http://www.securelogix.com)

(210) 402-9669

