IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

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):

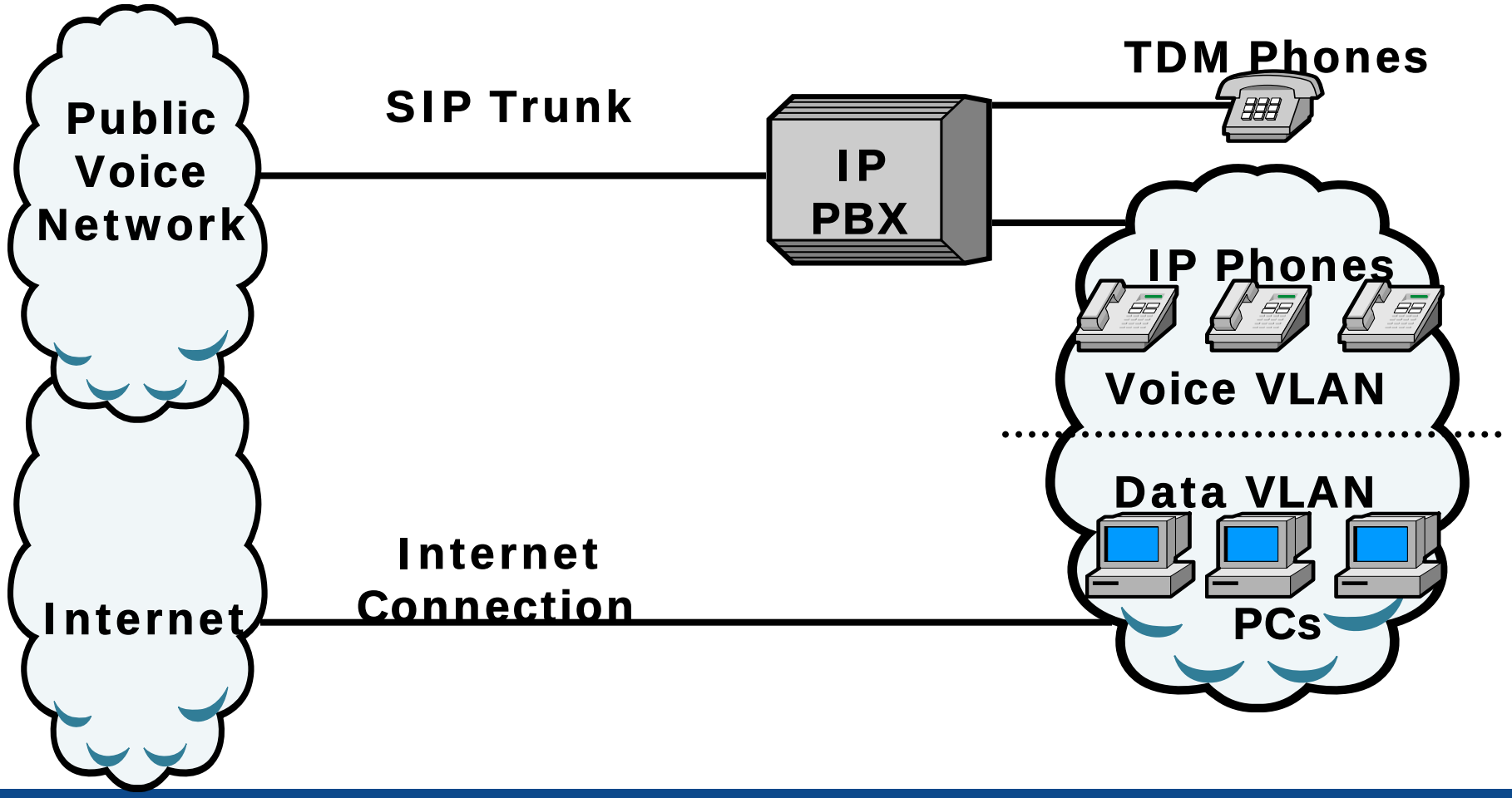
- Is a general-purpose protocol for managing sessions
- Can be used for any type of session
- Provides a means for voice signaling
- Defined by the IETF (looks like an Internet protocol)
- Resembles HTTP
- ASCII requests/responses

SIP Introduction

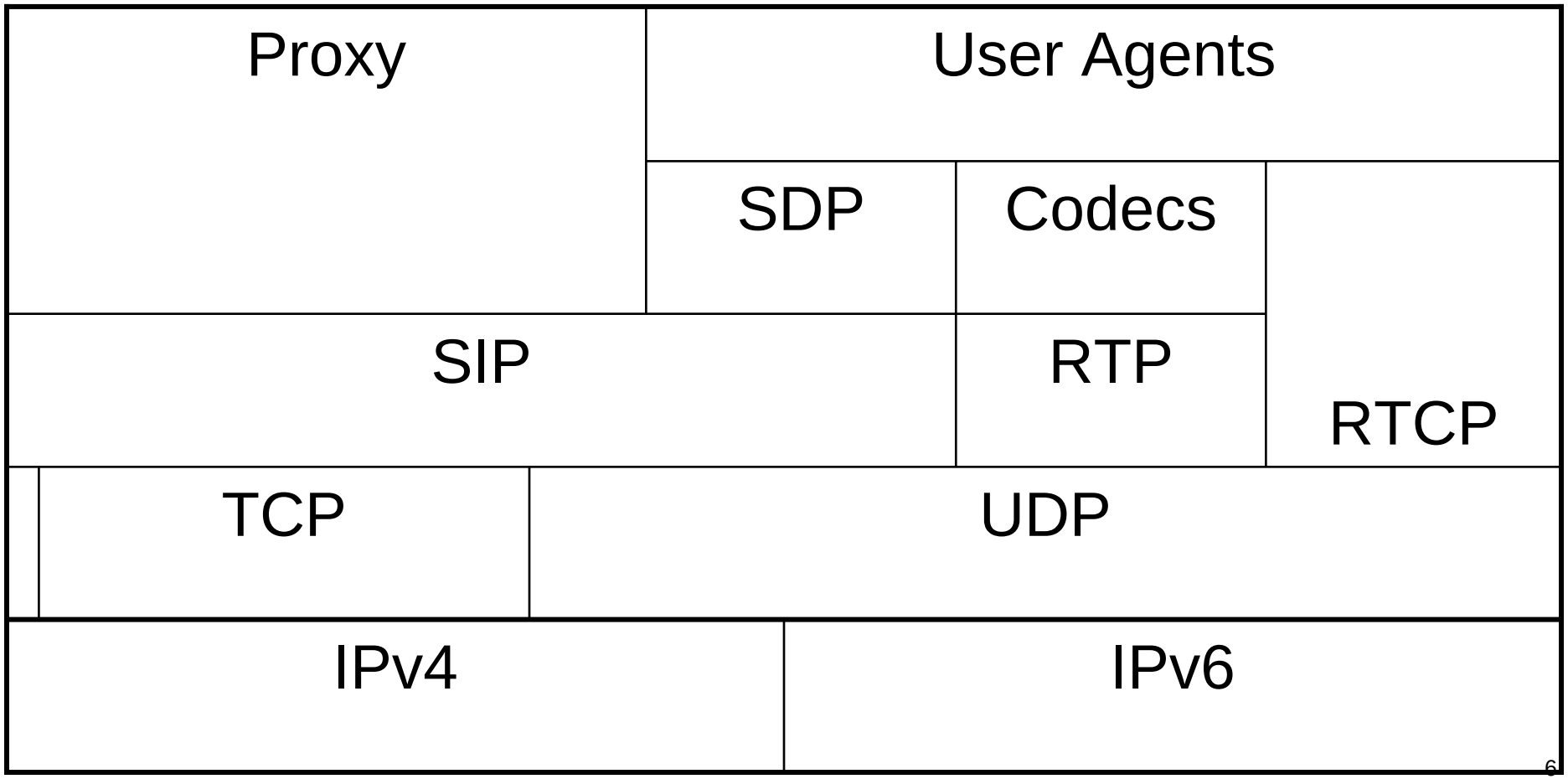
Why is SIP important:

- 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

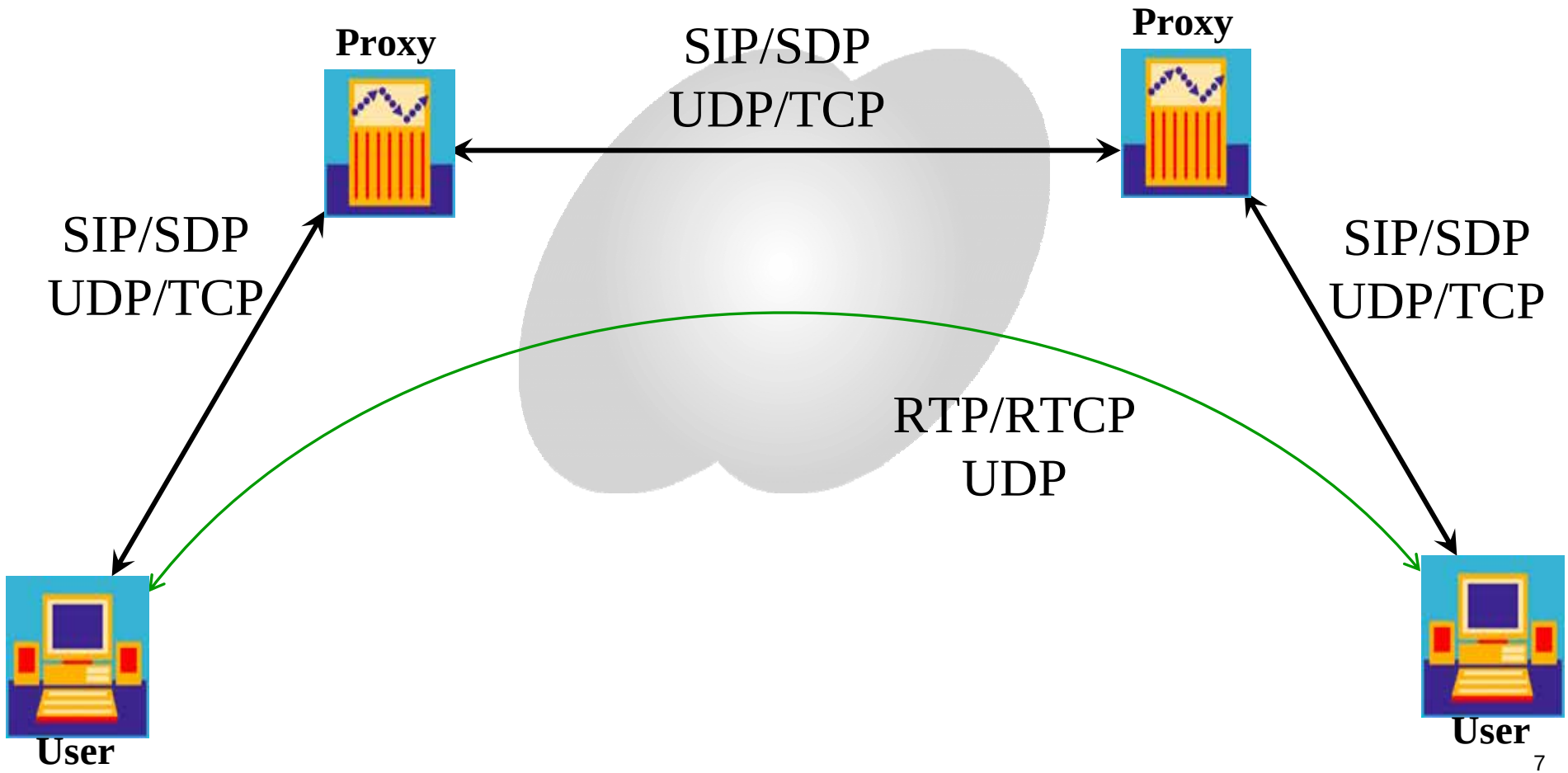
SIP Introduction



SIP Components



SIP Call Flow



SIP Vulnerabilities

Security issues with SIP:

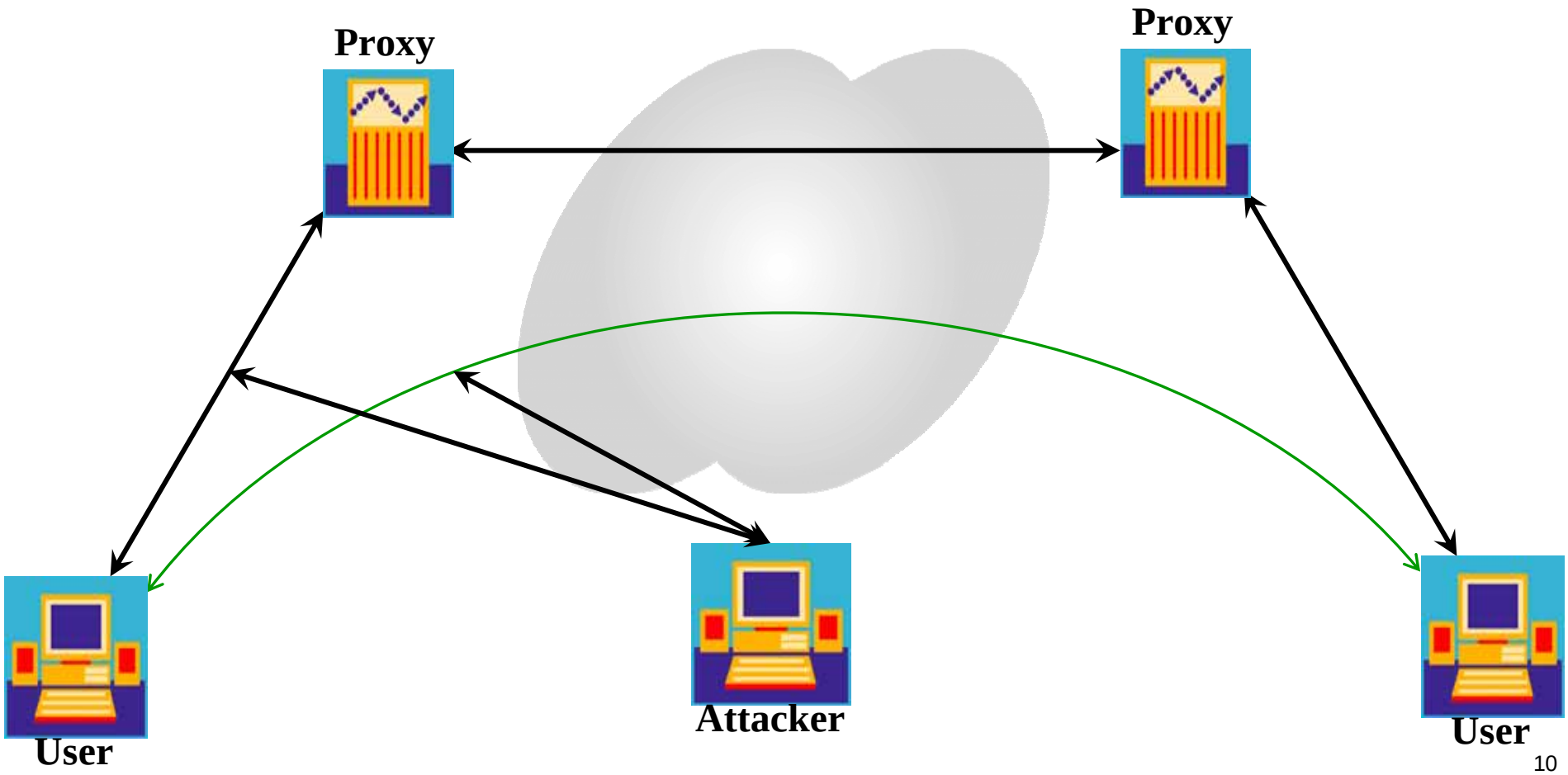
- SIP is a complex, free format protocol
- SIP itself does not require any security
- Security mentioned in SIP RFC, but not required
- Security degrades to common feature set
- Security is not mandatory even if available
- UDP is commonly used for SIP transport
- Network Address Translation (NAT) breaks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

SIP Vulnerabilities

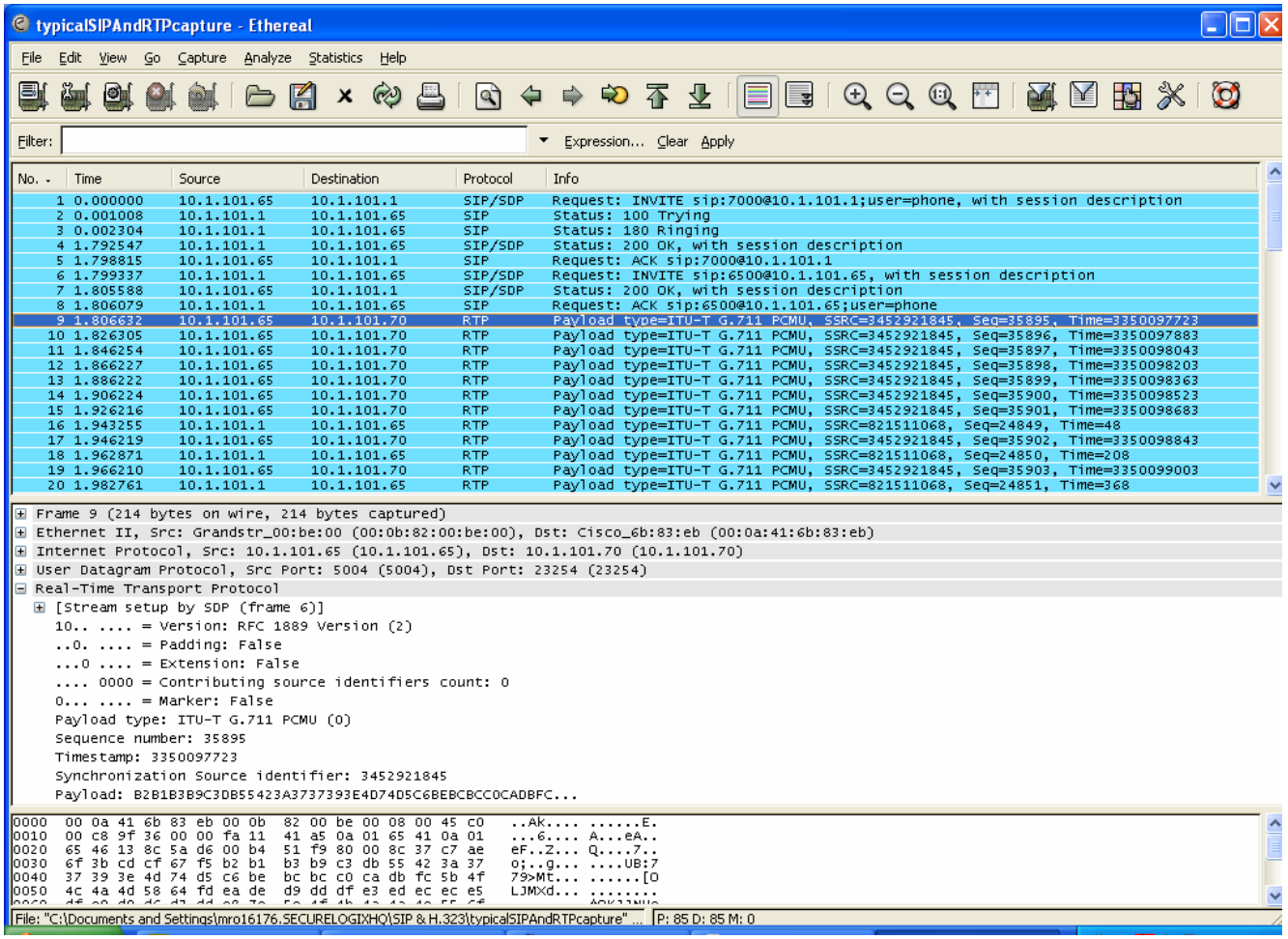
SIP-Specific Vulnerabilities:

- 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

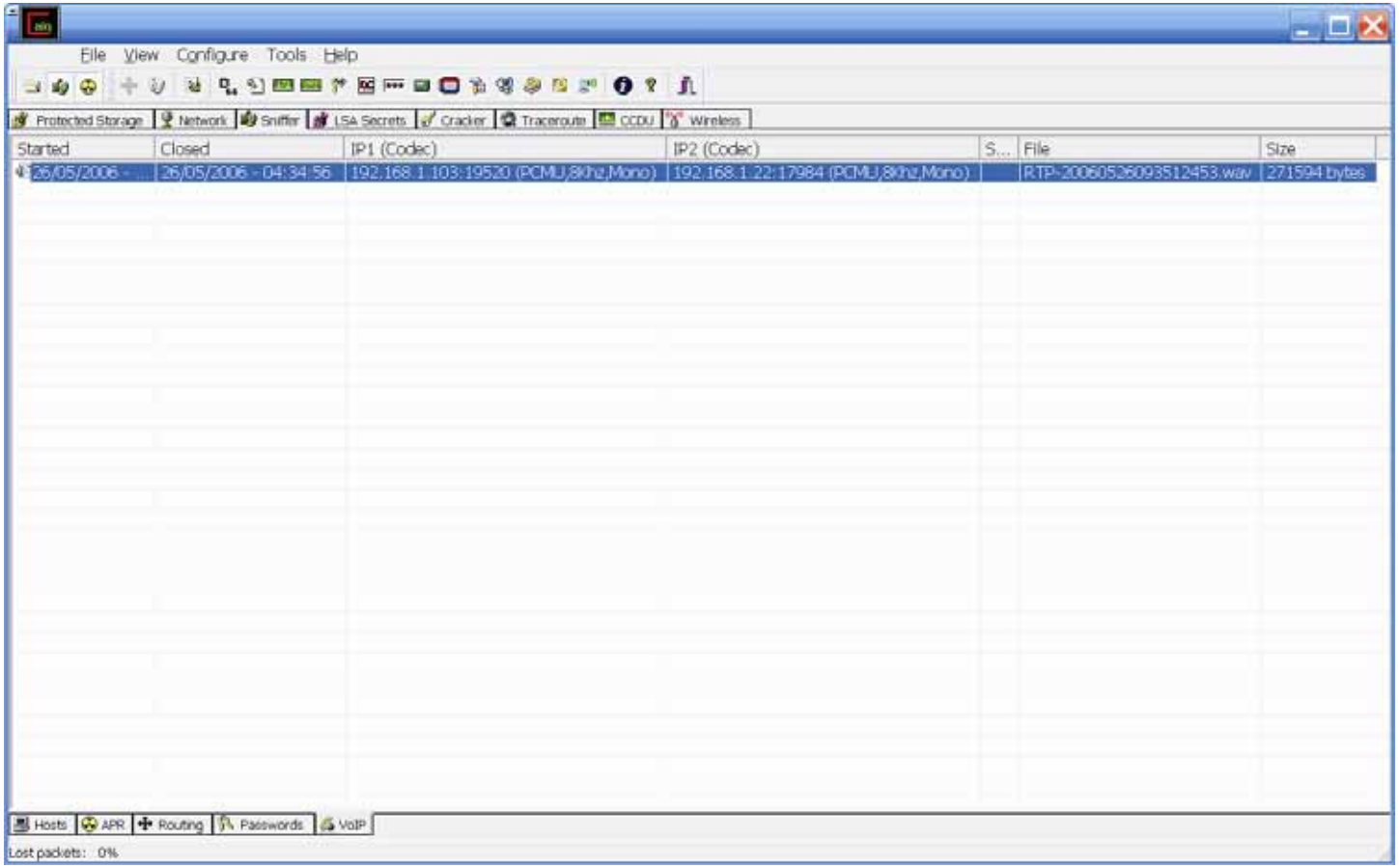
Eavesdropping



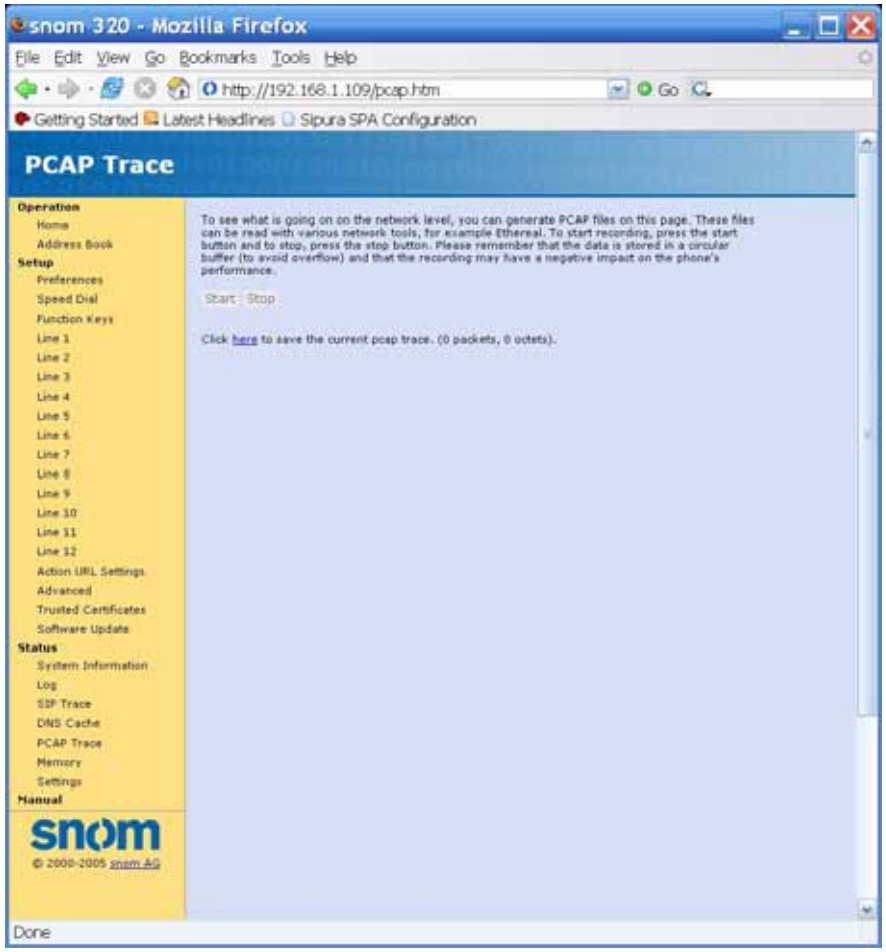
Eavesdropping Tools



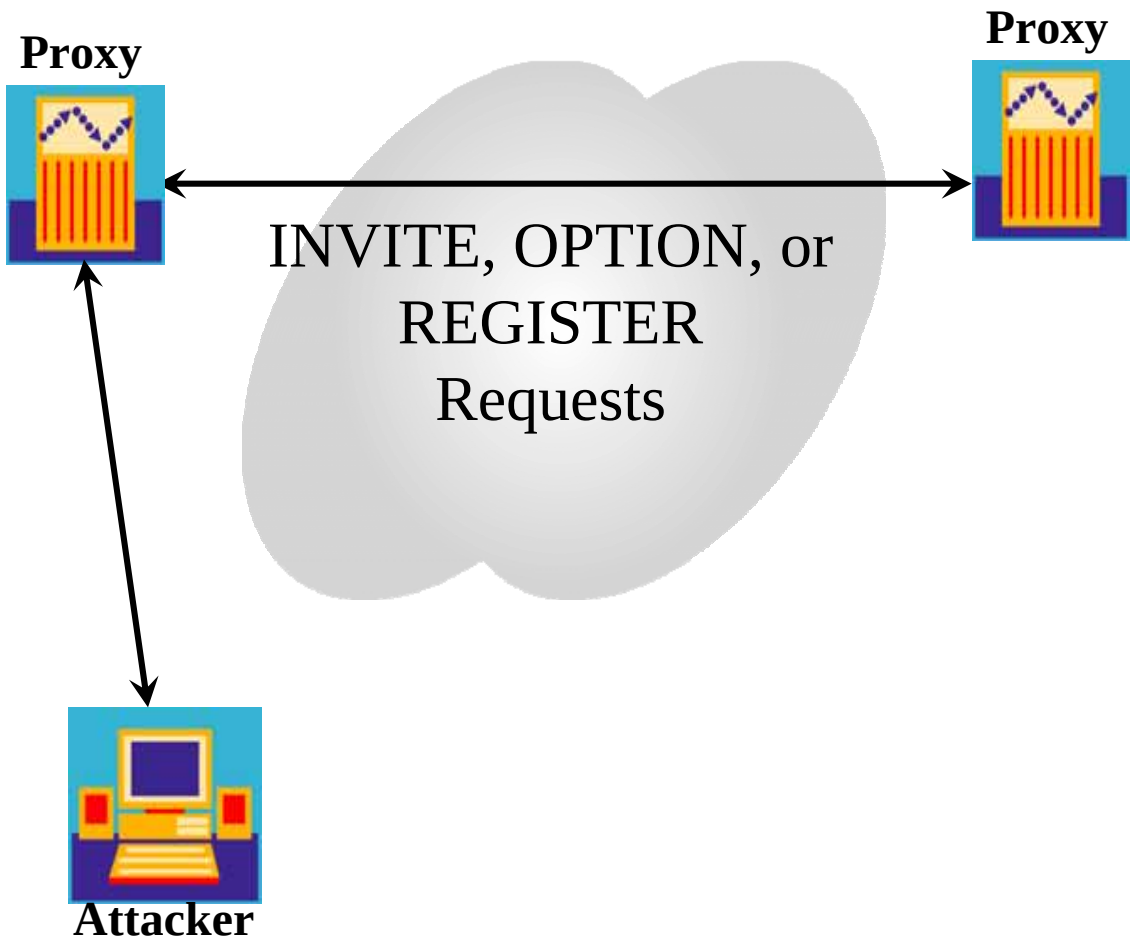
Eavesdropping Tools



Eavesdropping Tools



General/Directory Scanning

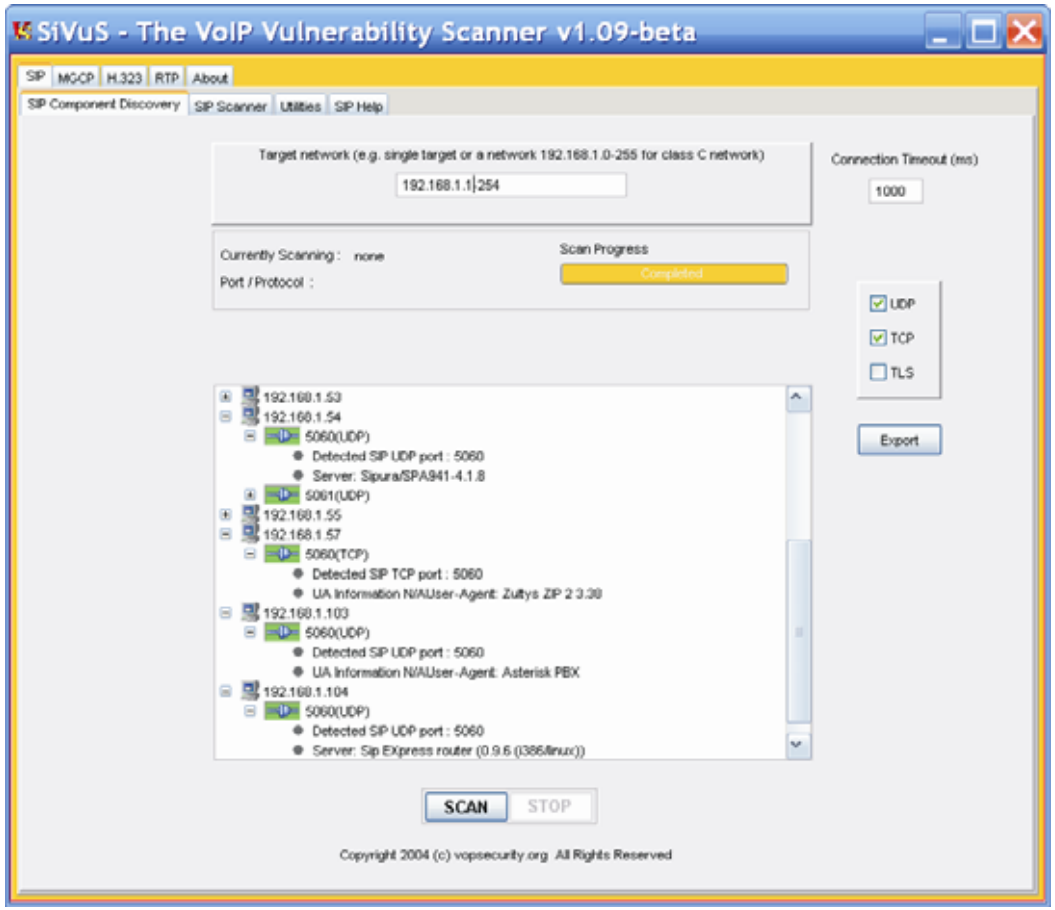


General Scanning Tools

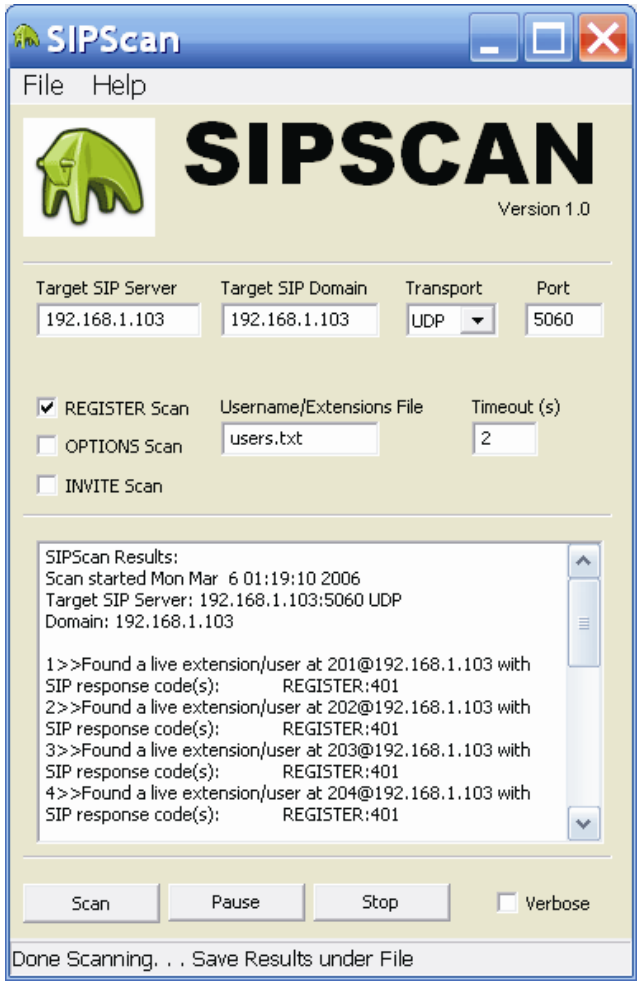
Nmap has the best VoIP fingerprinting database

```
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

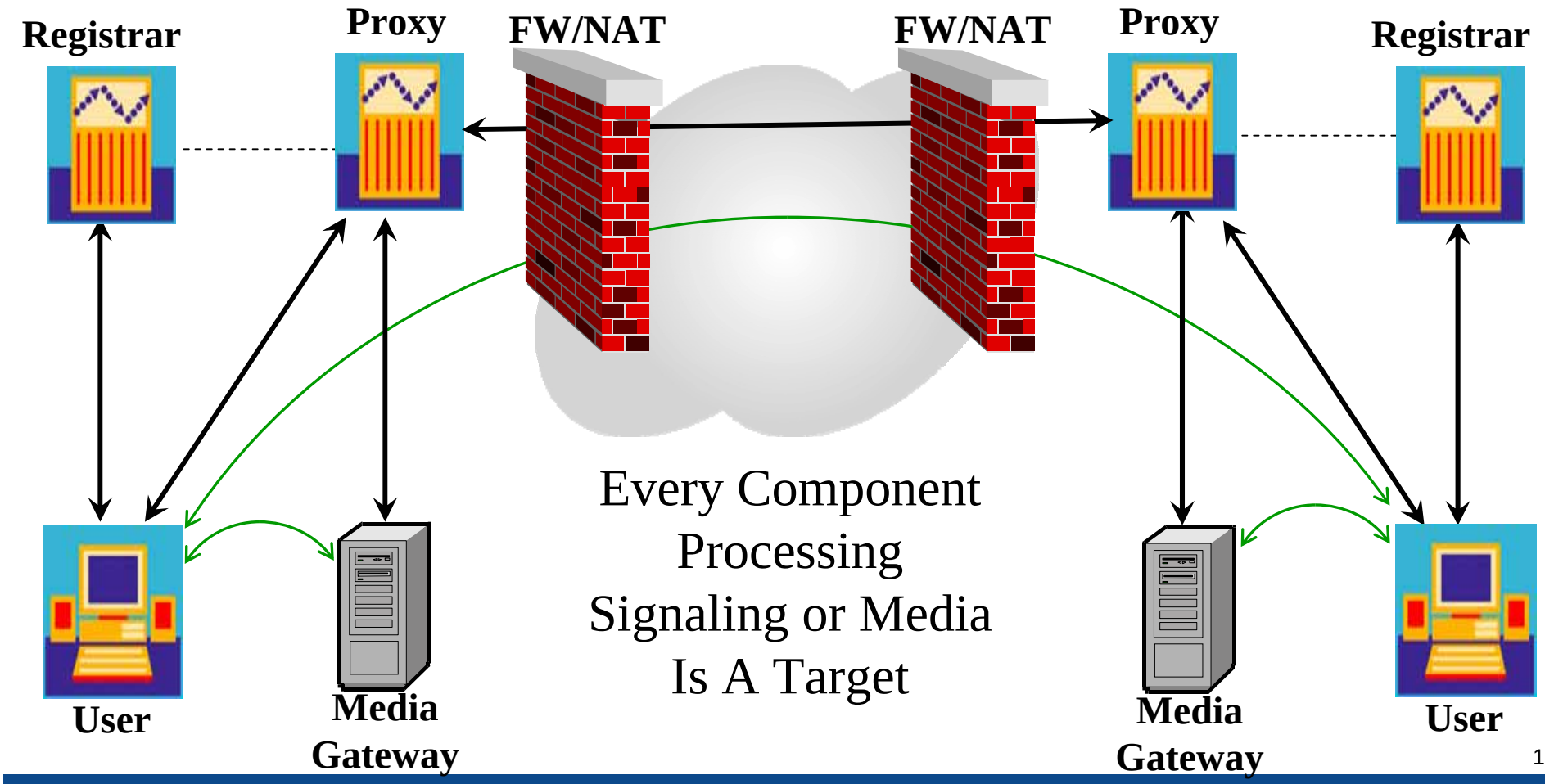


Directory Scanning Tools

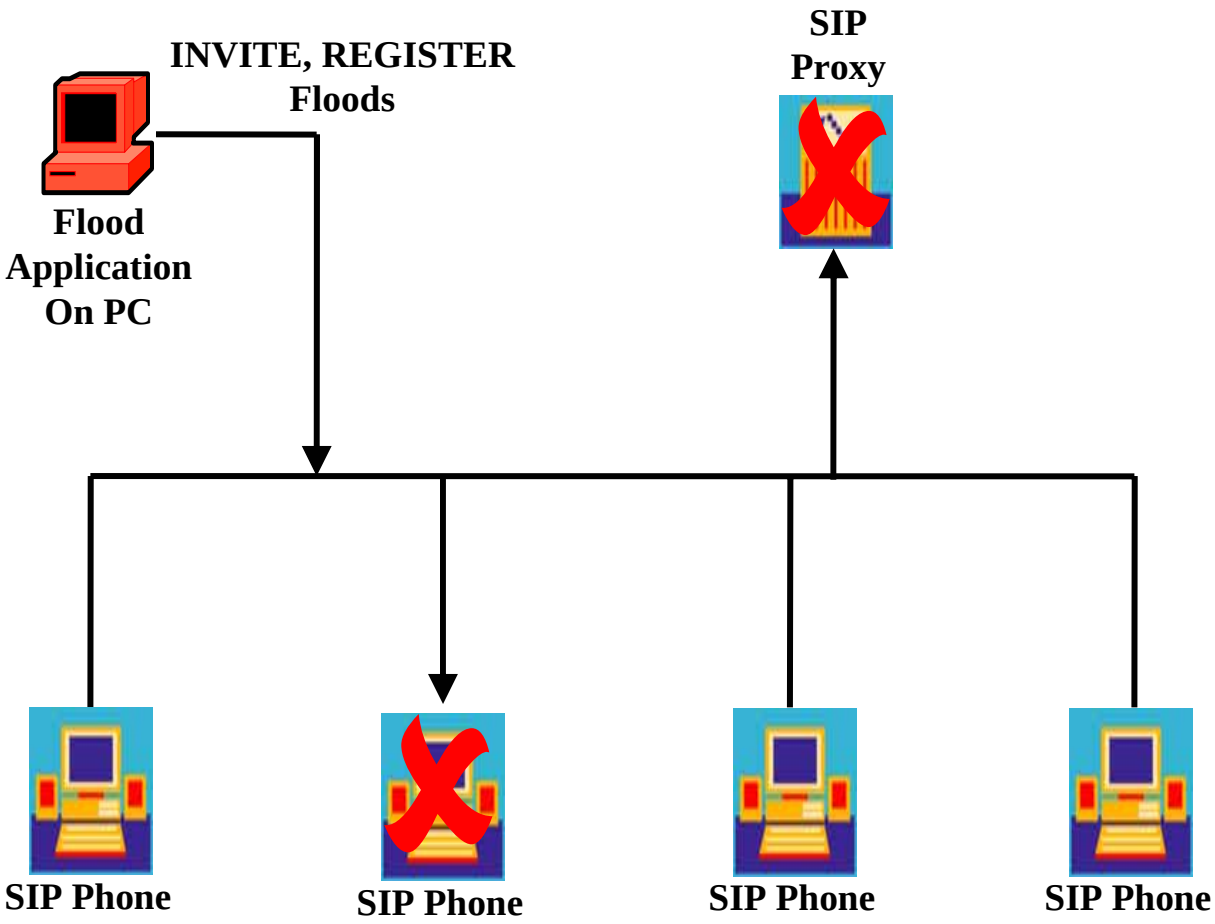
Linux tools:

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

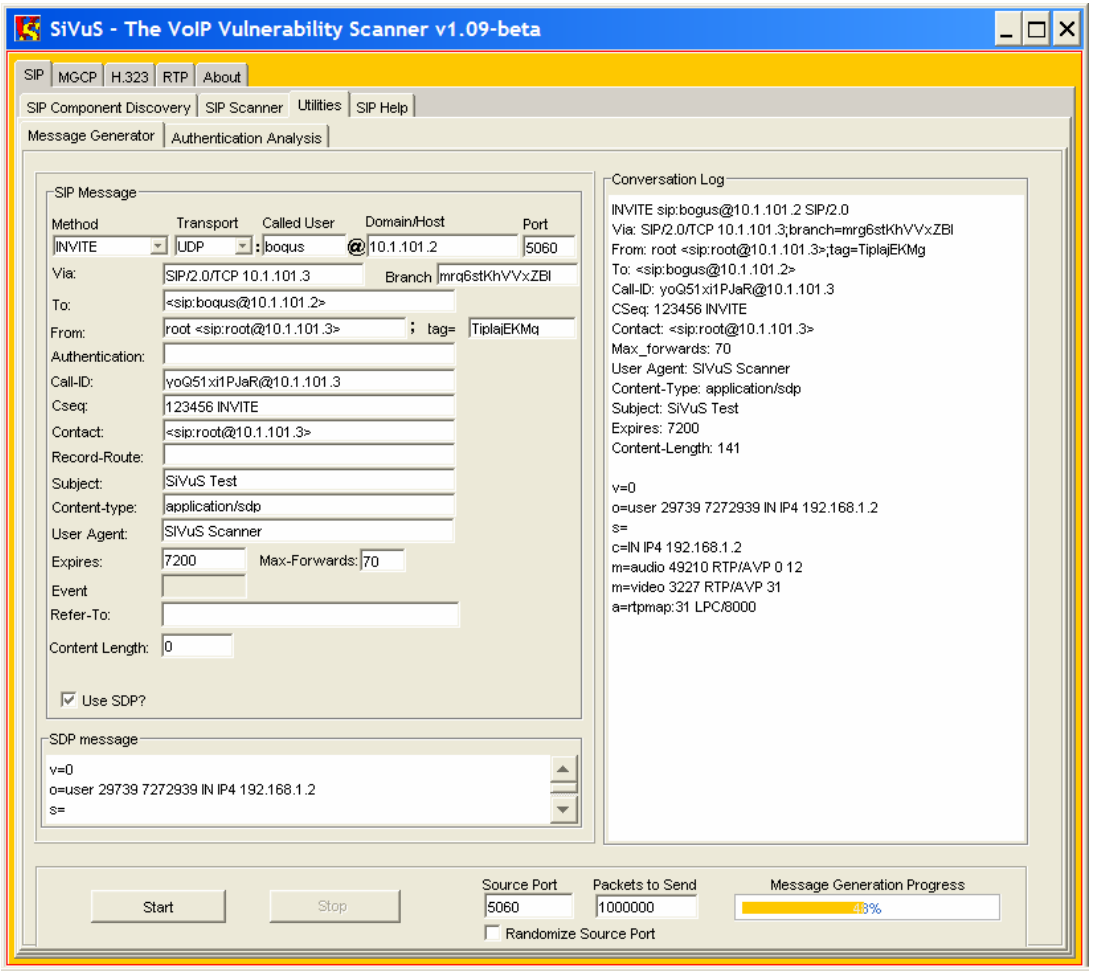
Denial of Service



Flood-based Denial of Service



Flood-based Denial of Service Tools



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: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
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: 9656141892590 9@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

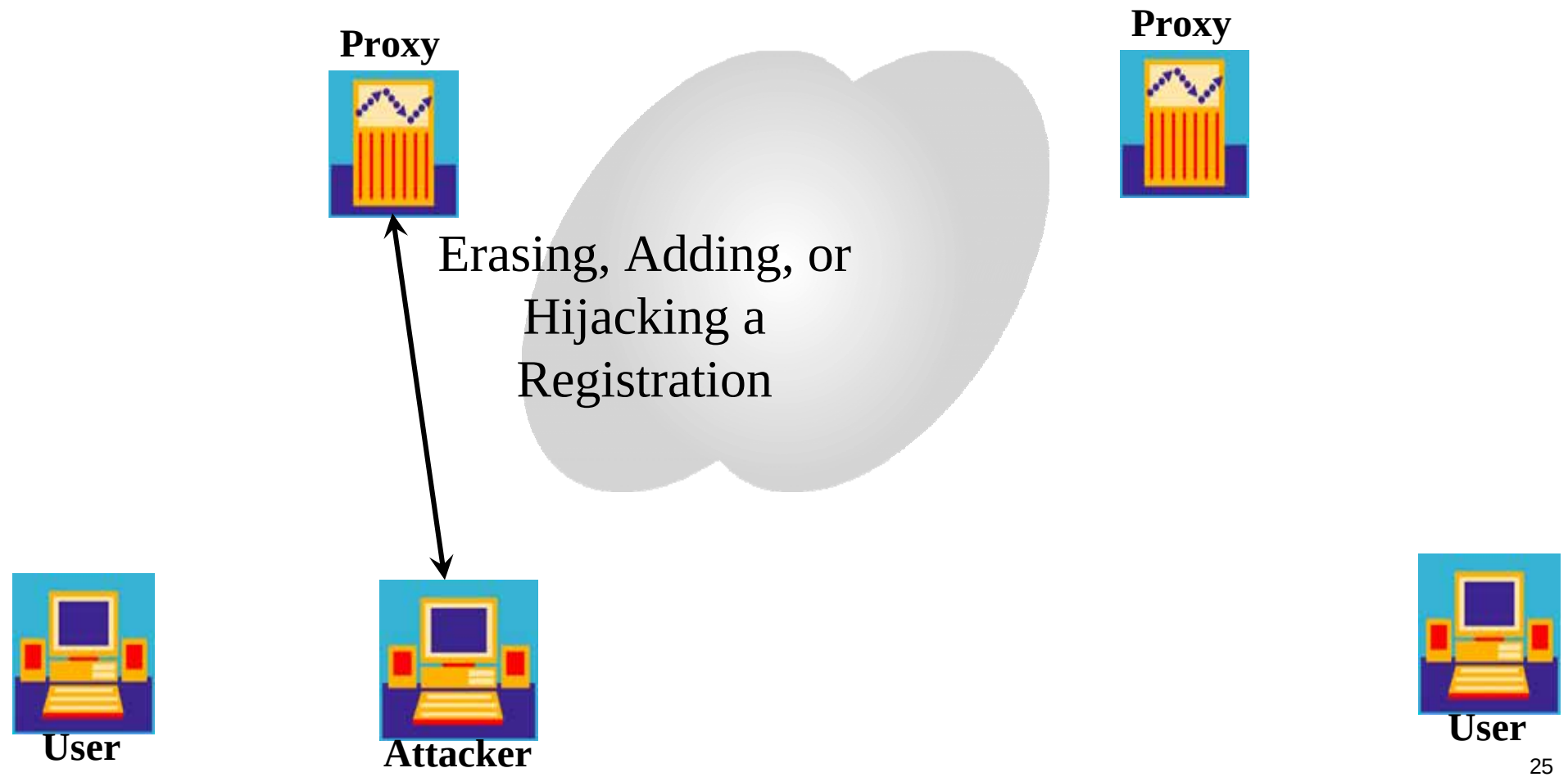
Linux tools:

- protos SIP test suite

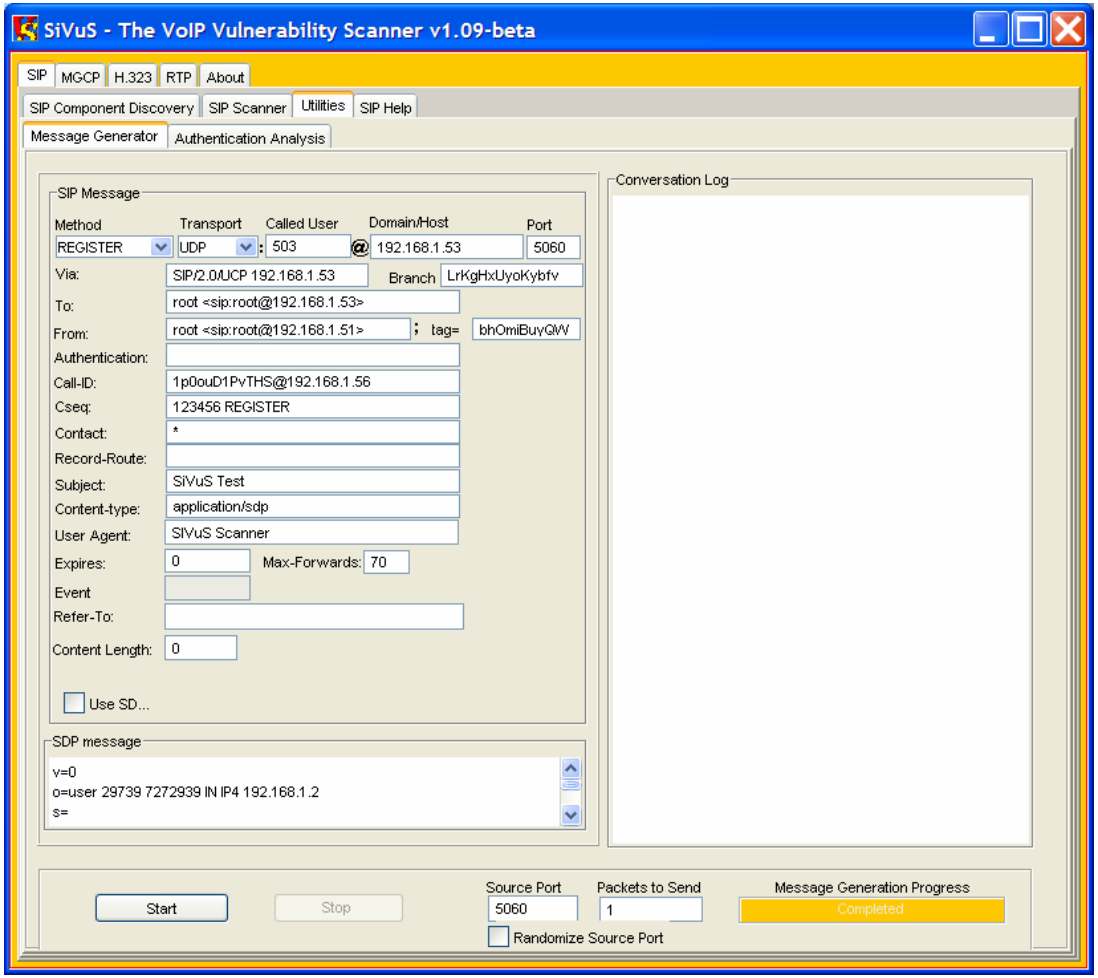
Commercial tools:

- Codenomicon

Registration Manipulation



Registration Manipulation Tools

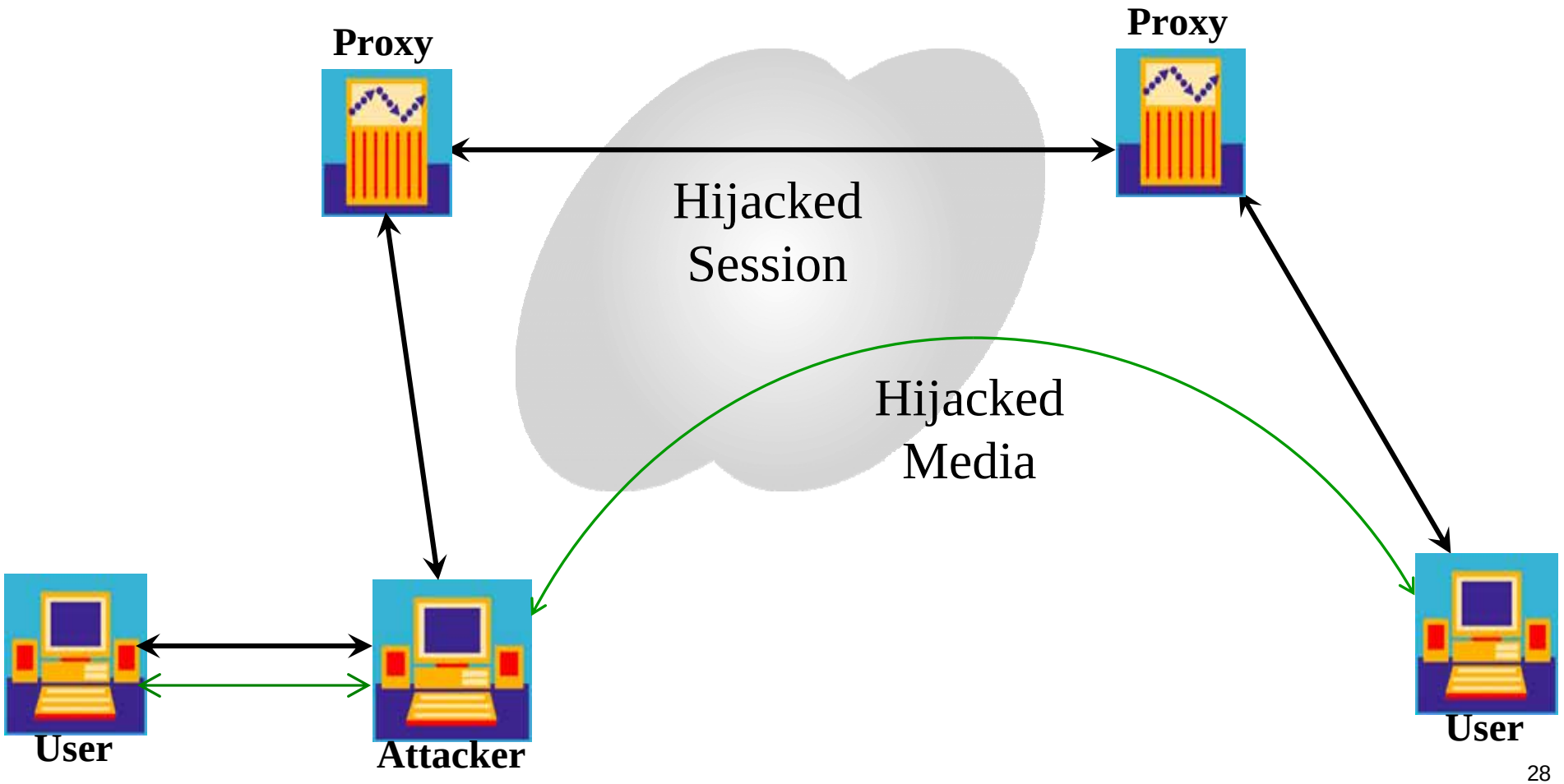


Registration Manipulation Tools

Linux tools:

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

Registration Hijacking

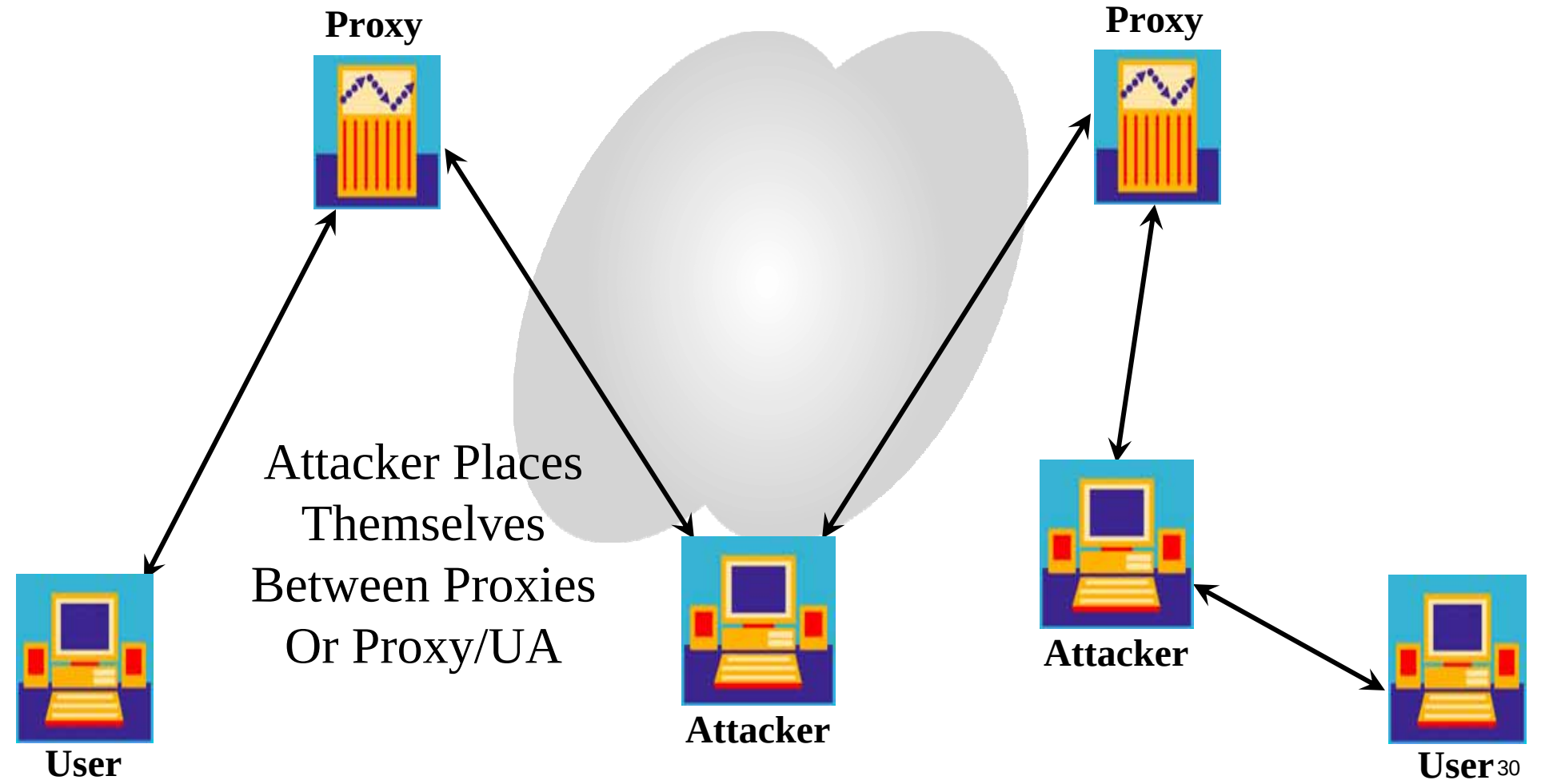


Registration Hijacking Tools

Linux tools:

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

Application Man-in-the-middle

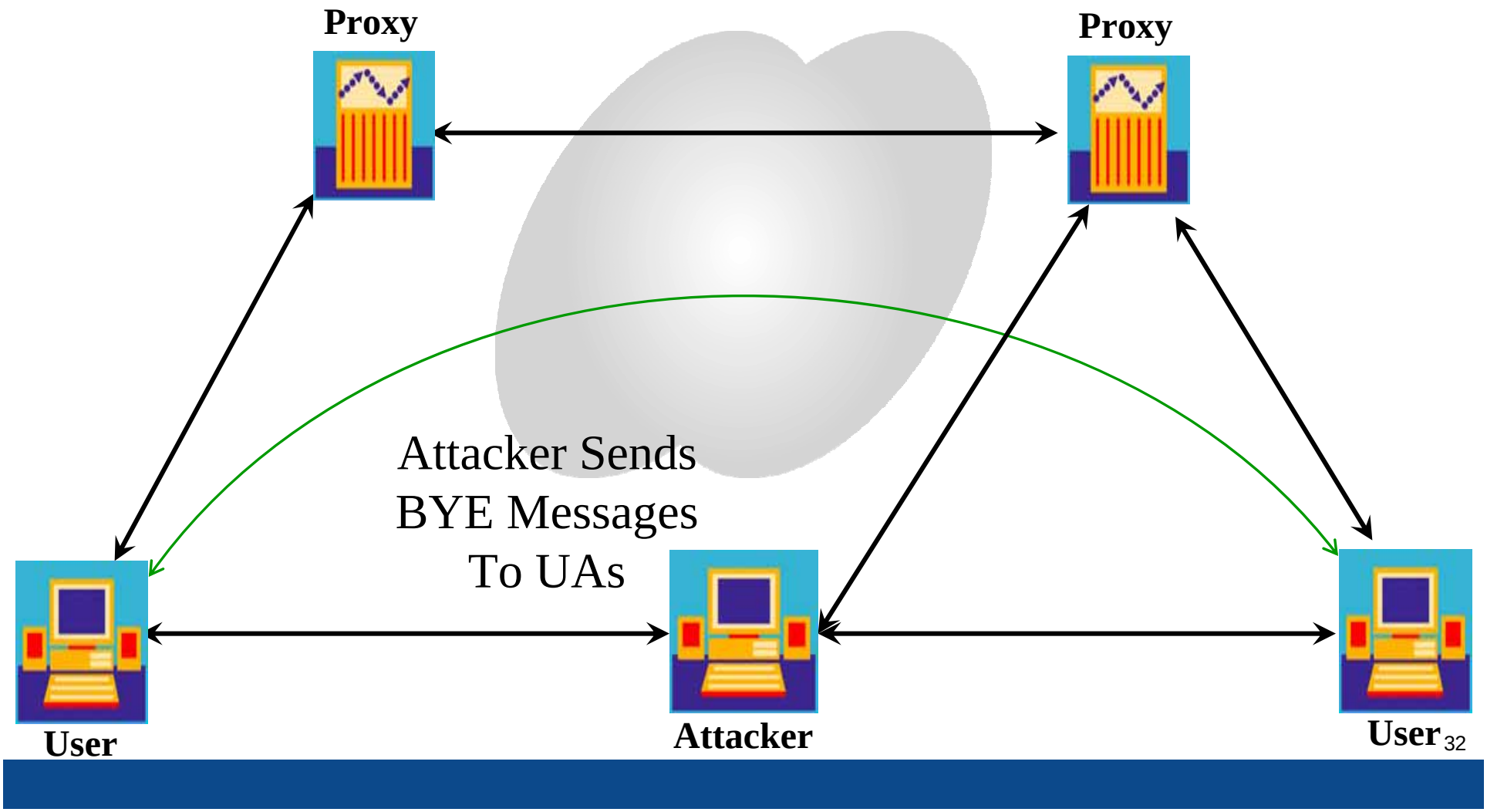


Application Man-in-the-middle Tools

Linux tools:

- sip_rogue – rogue SIP proxy or B2BUA

Session Tear Down

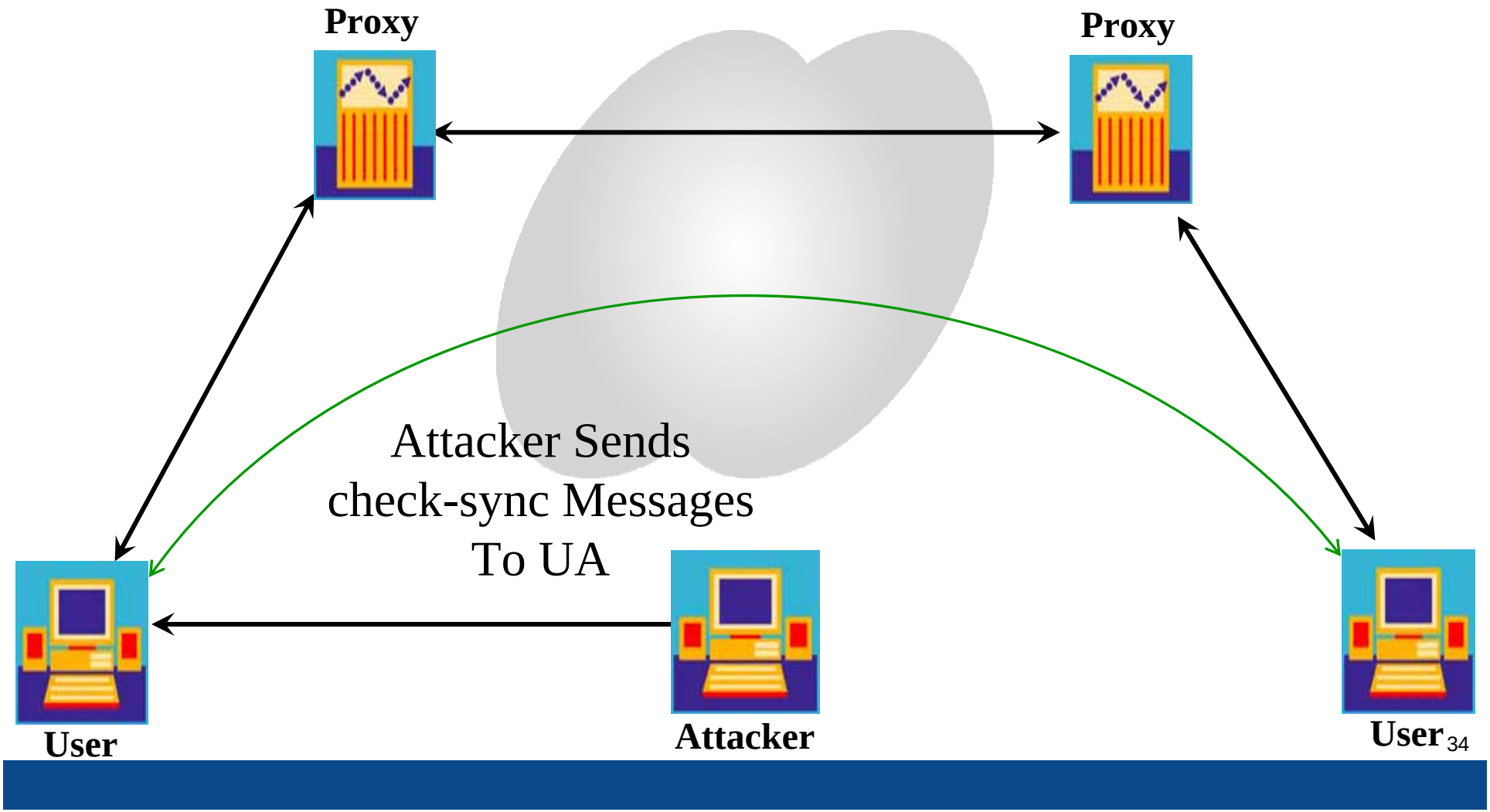


Session Tear Down Tools

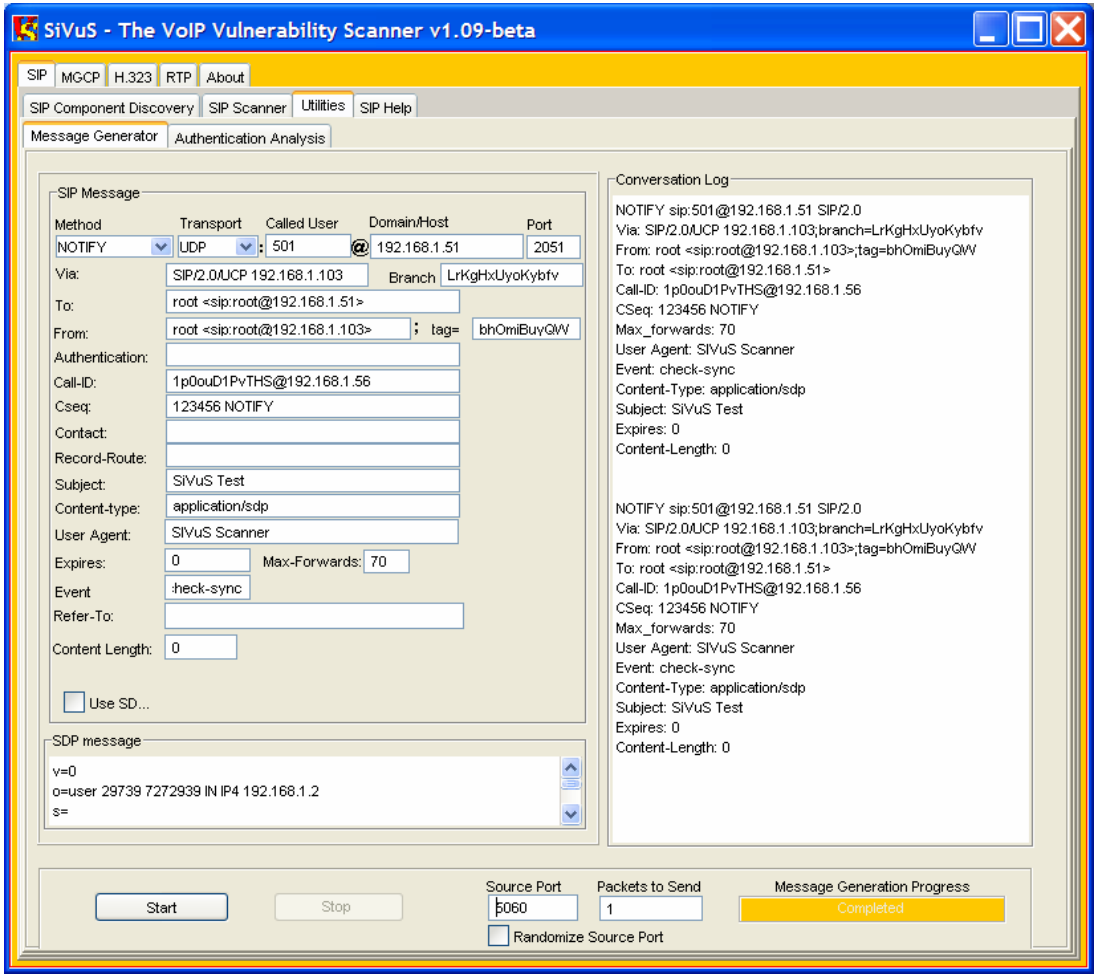
Linux tools:

- teardown – used to terminate a SIP call

Check-sync Reboot



Check-sync Reboot Tools

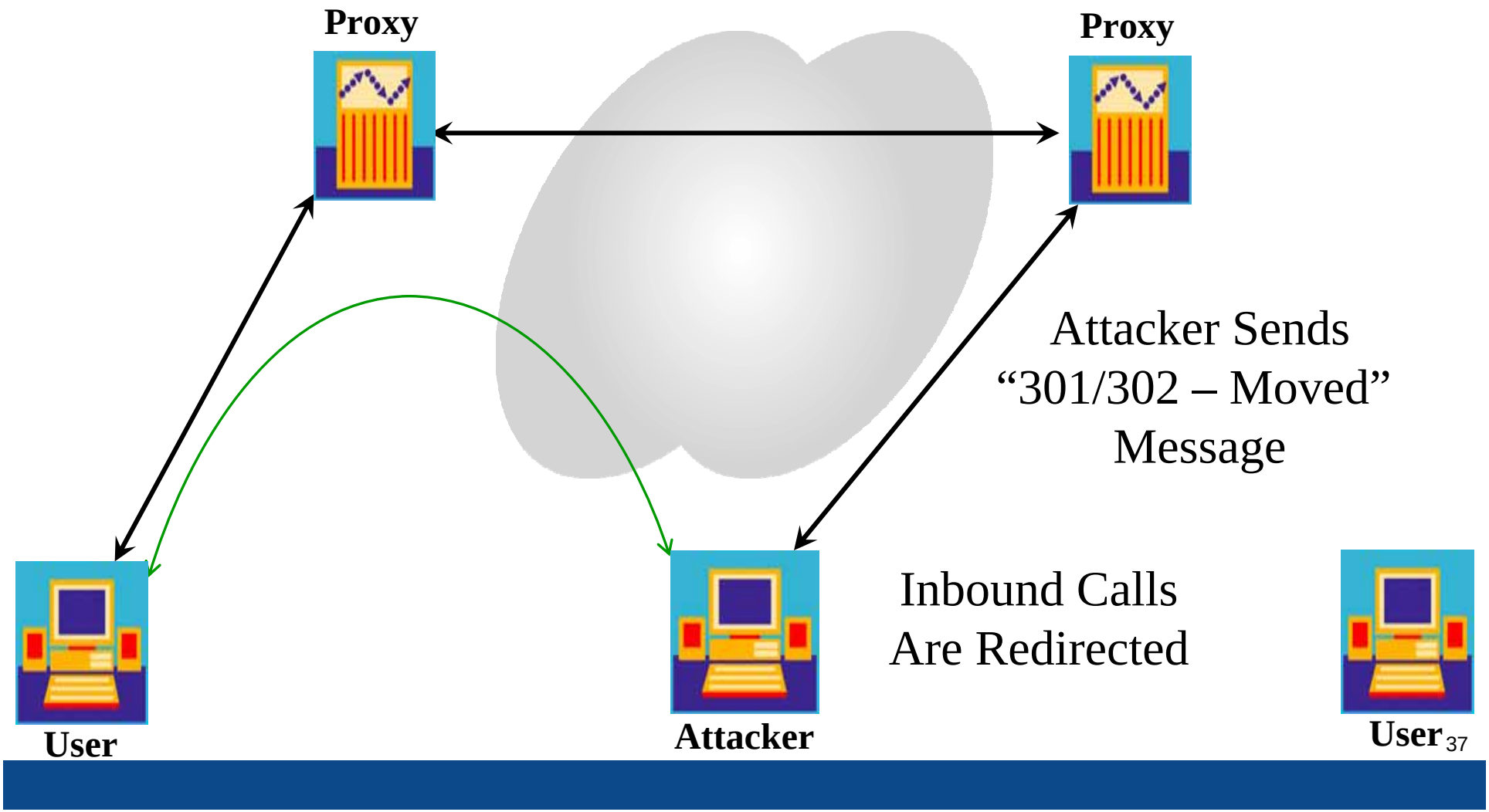


Check-sync Reboot Tools

Linux tools:

- check_sync – causes a SIP phone to reboot

Redirection

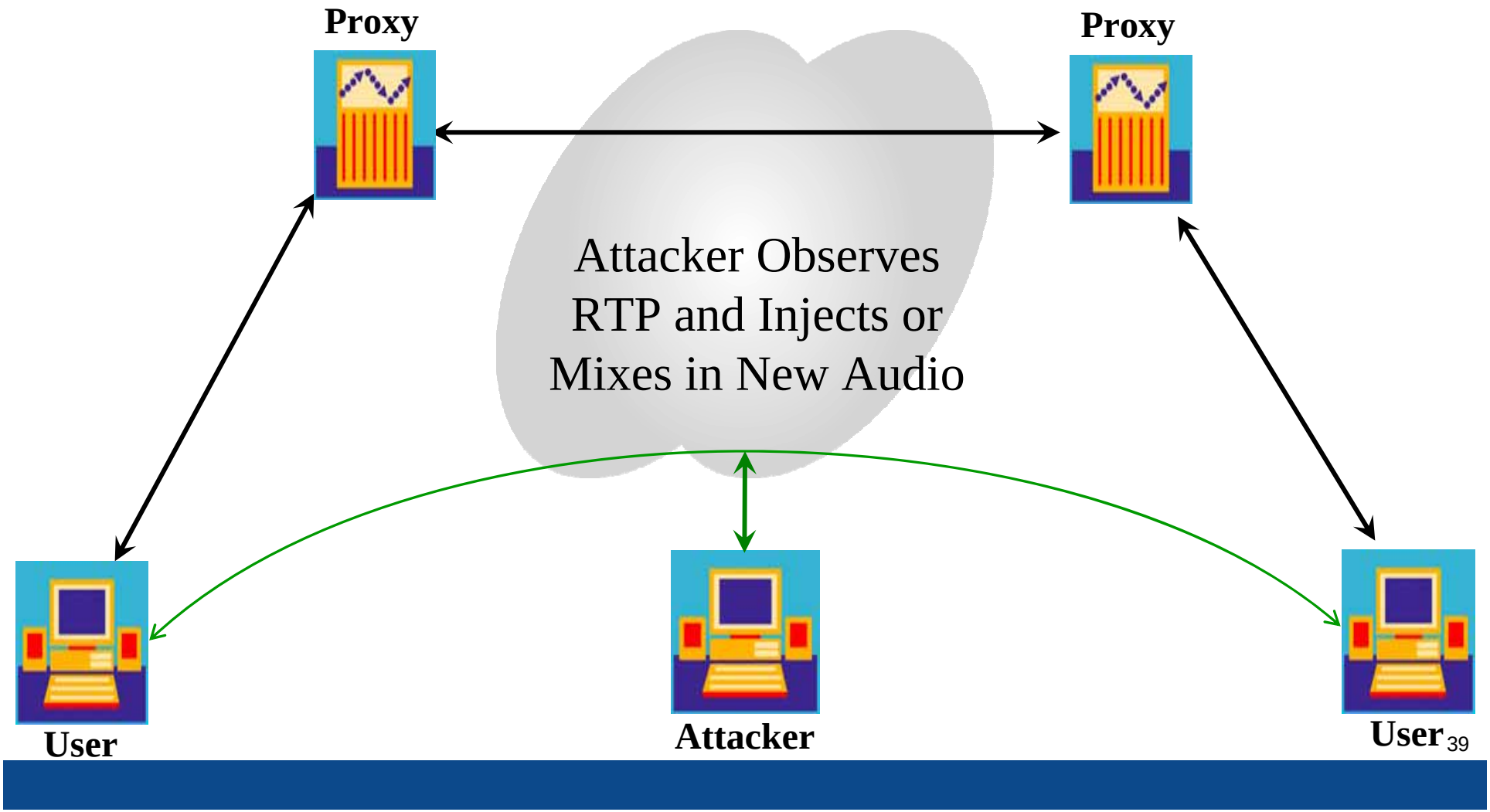


Redirection Tools

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
Pfizer
3 pills - 100mg
$85
ORDER


4 film-coated tablets
Cialis 20 mg
film-coated tablets
tadalafil


GARANTIE
SPANISH FLY
Voedingssupplement
Dietary supplement
15 ml


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!

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
- ethereal – www.ethereal.com
- wireshark – www.wireshark.com
- SiVuS – 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
- Asterisk – www.asterisk.org
- Trixbox – 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

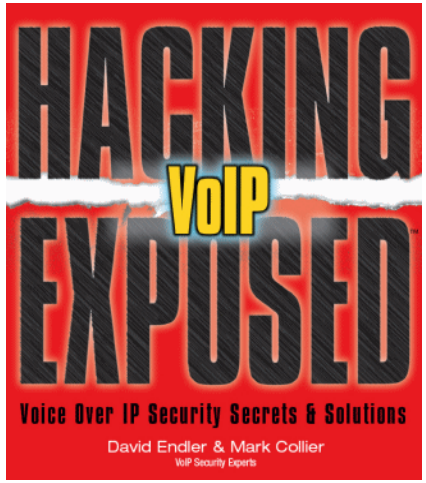
Key Points to Take Home

- 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

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

QUESTIONS?

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



SECURELOGIX®
CORPORATION