



Introduction to VOIP Security

Angad Singh and Rohit Shah
goldfish21@gmail.com
rohit.shah@yahoo.co.in

OWASP

30-October-2010

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation

<http://www.owasp.org>

Agenda

VoIP Basics – An Introduction

VoIP – Call Setup

VoIP Security – Threats, Vulnerabilities, Attacks

VoIP Security – Countermeasures

VoIP Security – Assessing Security Controls

Q&A, Feedback and Closing



VoIP Basics

VOIP Basics

What is Voice Over IP?

The packetisation and transport of classic public switched telephone system audio over an IP network

A suite of IP-based communications services

Provides multimedia communications over IP networks

Operates over any IP network (not just the Internet)

Low-cost alternative to PSTN calling

Few examples . . .

Soft phones : Skype, Microsoft Net meeting, ophone, gphone, Asterisk* etc.

Enterprise : Small IP phone deployments, IP PBX, Cisco Call manager.



VOIP overview - Protocols

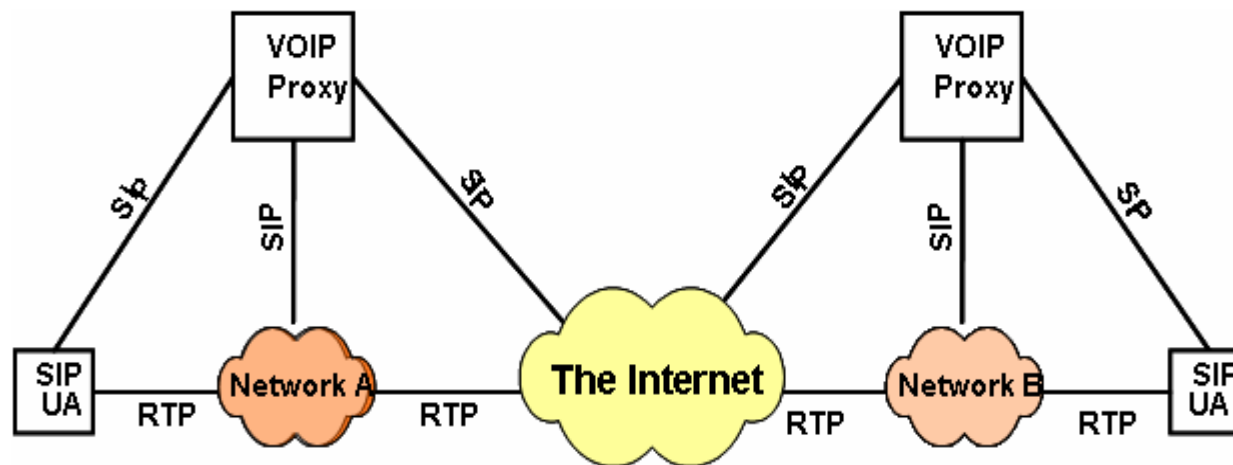
The protocols combining any IP Telephony architecture are divided into the following roles:

Signaling Protocols

Signaling protocols manage the set up, modification and termination of a phone call between the two of them.

Media Transport Protocols

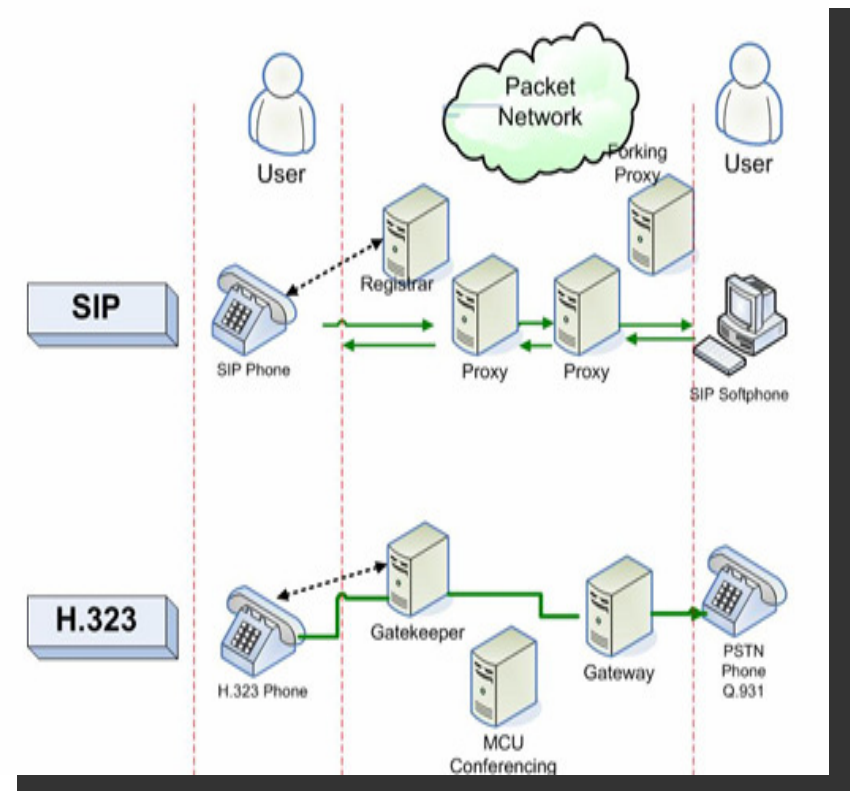
Media transport protocols are used to carry voice samples (such as RTP)



VOIP overview – Signaling Protocols

The VoIP Signaling Protocols perform the following services:

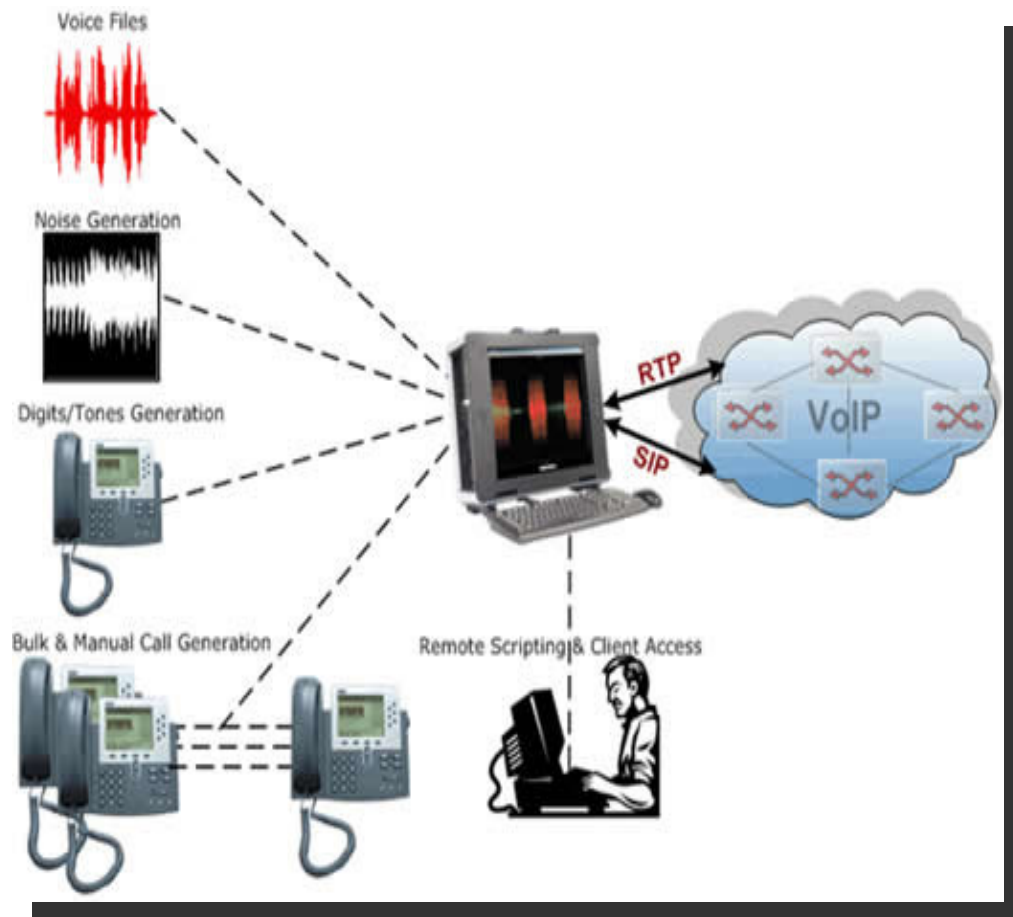
- **Locate User** – The ability to locate another user with whom a user wishes to communicate.
- **Session Establishment** – The ability of the called party to accept a call, reject a call, or redirect the call to another location or service.
- **Session Setup Negotiation** – The ability of the communicating parties to negotiate the set of parameters to be used during the session. This includes, but not limited to, Audio encoding.
- **Modify Session** – The ability to change a session's parameters such as using a different Audio encoding, adding/removing a session participant, etc.
- **Teardown Session** – The ability to end a session.



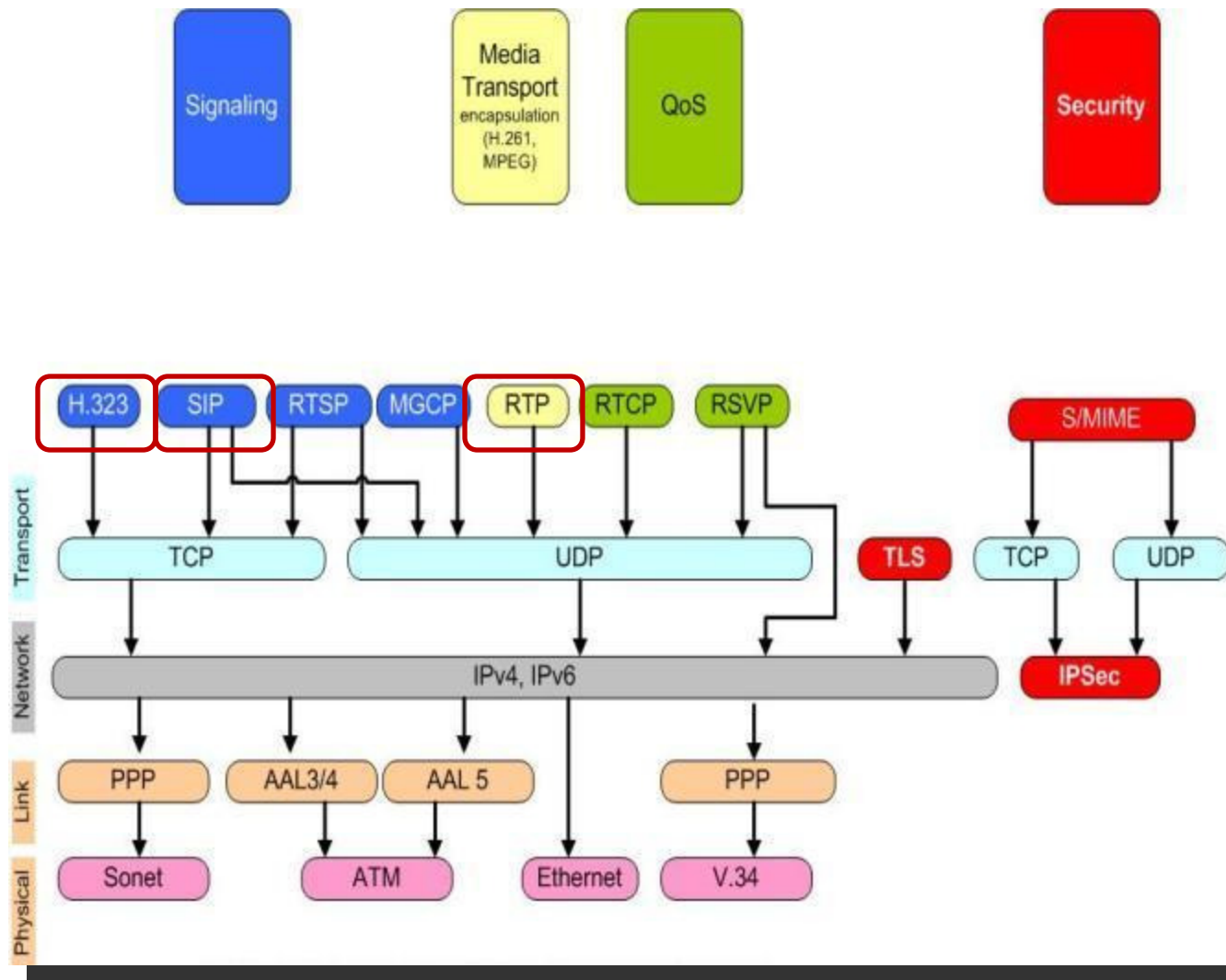
VOIP overview – Media Transport Protocols

The VoIP Media Transport protocols perform the following services:

- **Digitize using CODEC:** The ability to digitize voice using a codec.
- **Compression:** The ability to compress voice into smaller samples.
- **Encapsulation:** The ability to encapsulate the compressed voice samples within an IP transport protocol.
- **Transportation:** The ability to transport the digitized compressed packet over an IP network.



VOIP protocols



SIP

H.323

RTP

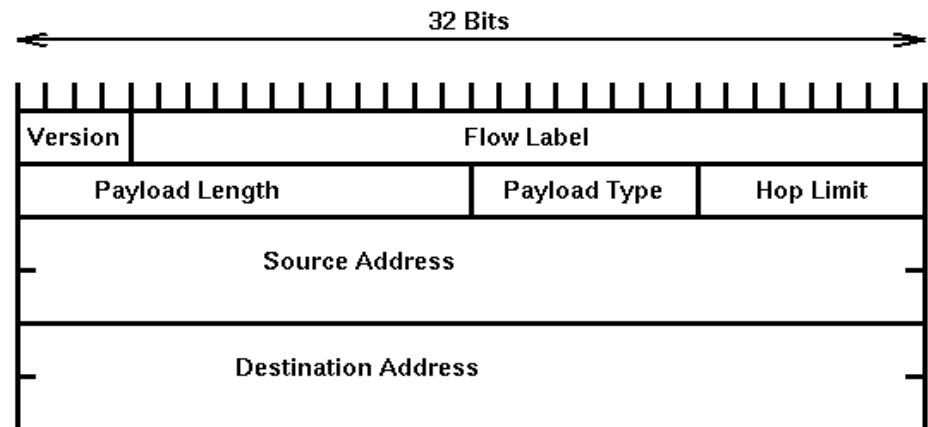
Let's have a look at these
VOIP Protocols in detail ...



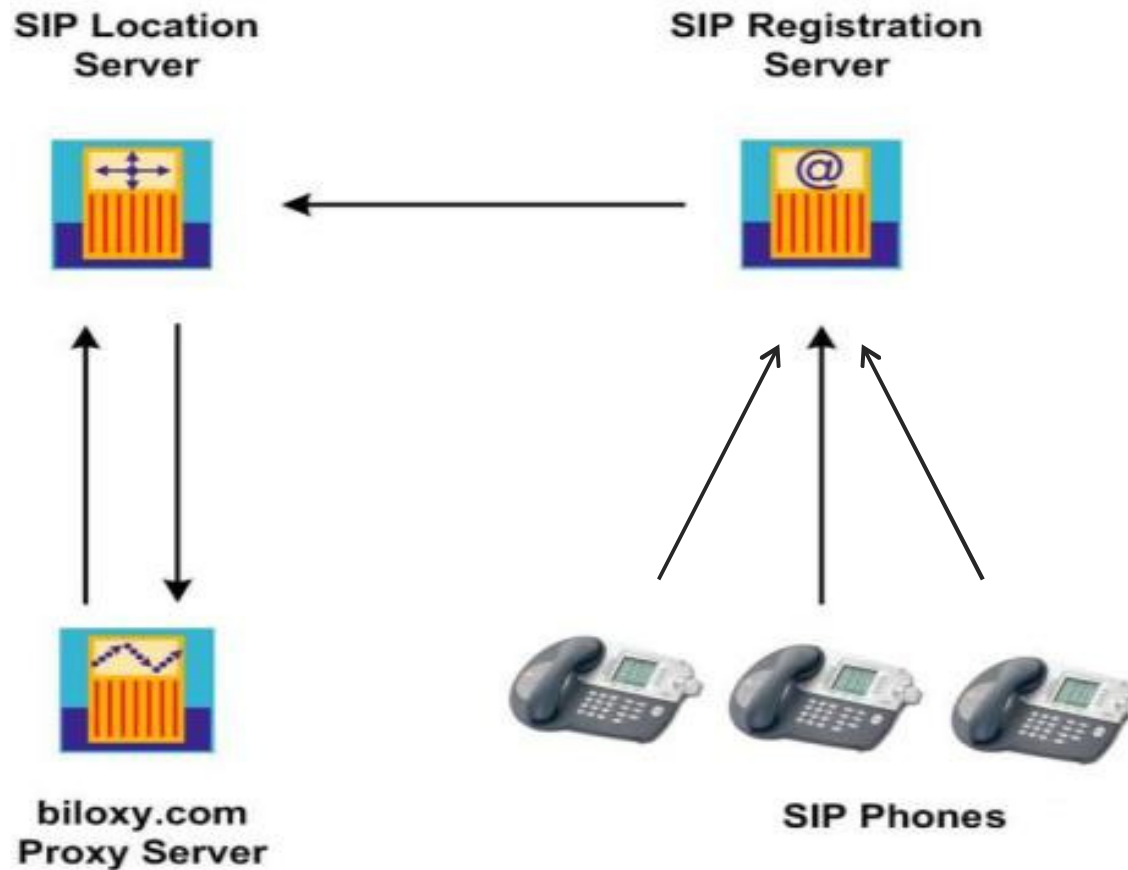
VOIP protocols – SIP overview

- SIP is a **signaling protocol**, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP). It allows two speaking parties to set up, modify, and terminate a phone call between the two of them.
- The SIP protocol is an **Application Layer protocol** designed to be independent of the underlying transport layer; it can run on Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- SIP clients typically use TCP or UDP on port numbers 5060 and/or 5061 to connect to SIP servers and other SIP endpoints. Port 5060 is commonly used for non-encrypted signaling traffic whereas port 5061 is typically used for traffic encrypted with **Transport Layer Security** (TLS).

SIP Header



SIP Architecture Elements



SIP Requests

Following are the SIP Requests that are sent at the time of session establishment:

SIP request	Description	RFC Reference
BYE	Terminates an existing connection between two users in a session.	RFC 3261
OPTIONS	Determines the SIP messages and codecs that the UA or server understands.	RFC 3261
REGISTER	Registers a location from a SIP user.	RFC 3261
ACK	Acknowledges a response from an INVITE request.	RFC 3261
CANCEL	Cancels a pending INVITE request, but does not affect a completed request (for instance, stops the call setup if the phone is still ringing).	RFC 3261
REFER	Transfers calls and contacts external resources.	RFC 3515
SUBSCRIBE	Indicates the desire for future NOTIFY requests.	RFC 3265
NOTIFY	Provides information about a state change that is not related to a specific session.	-

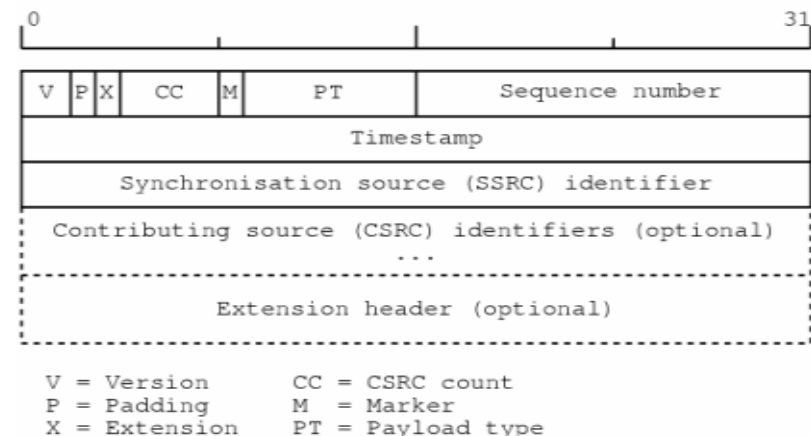
SIP Responses

Following are the SIP Responses that are sent at the time of session establishment:

- 482 Loop Detected
- 483 Too Many Hops
- 484 Address Incomplete
- 485 Ambiguous
- 486 Busy Here
- 5xx responses: Server failure responses
- 500 Internal Server Error
- 501 Not Implemented
- 502 Bad Gateway
- 503 Service Unavailable
- 504 Gateway Time-out
- 505 SIP Version Not Supported
- 6xx responses global failure responses
- 600 Busy Everywhere
- 603 Decline
- 604 Does Not Exist Anywhere
- 606 Not Acceptable

VOIP protocols – RTP overview

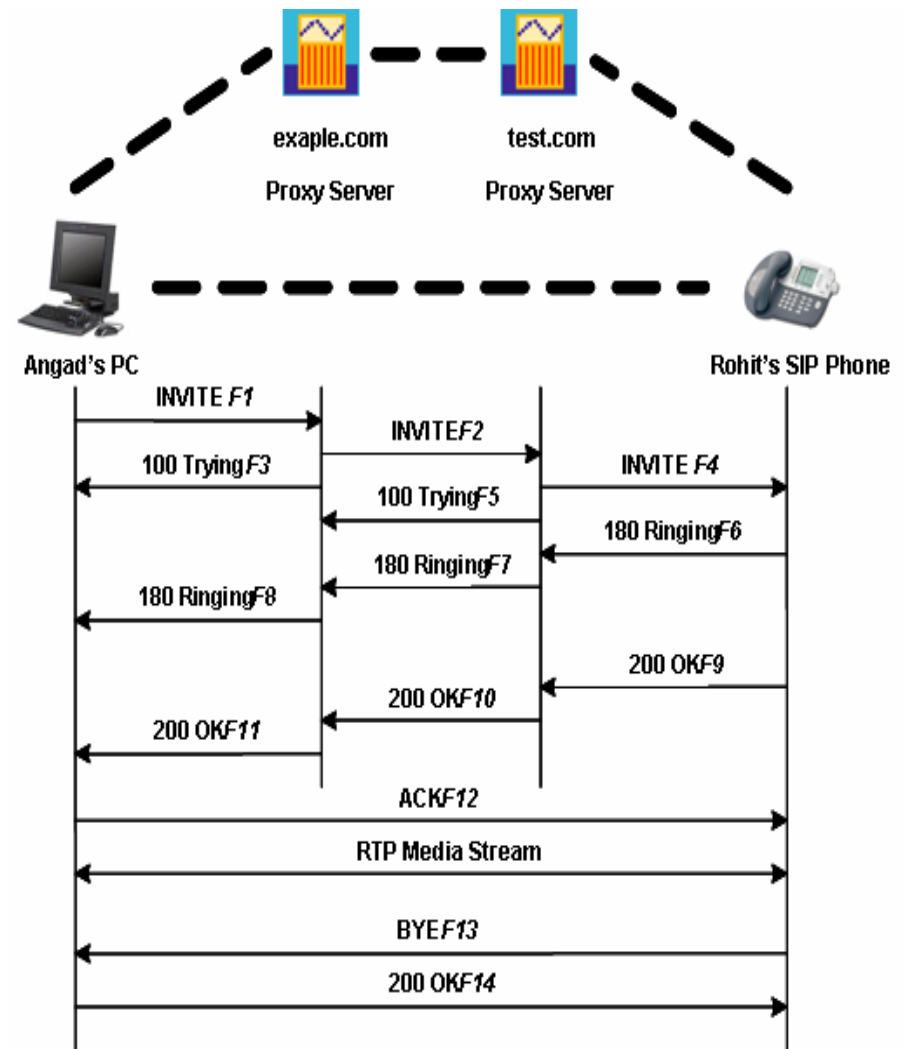
- RTP (Real Time Transmission Protocol) is a data transfer protocol, which deals with the transfer of real-time multimedia data.
- Information provided by this protocol include timestamps (for synchronization), sequence numbers (for packet loss detection) and the payload format which indicates the encoded format of the data.
- RTP does not assure delivery or order of packets. However, RTP's sequence numbers allow applications, such as an IP phone, to check for lost or out of order packets.
- RTP includes the RTP control protocol (RTCP), which is used to monitor the quality of service and to convey information about the participants in an ongoing session.



VoIP –Call Setup

SIP Call Flow – End to End

- ABC uses a **SIP application** on her PC (referred to as a softphone) to call XYZ on his **SIP phone** over the Internet. ABC sends an **INVITE** to User B to initiate a phone call.
- The two **SIP proxy servers** that act on behalf of ABC and XYZ facilitate the session establishment. XYZ **receives** the request (his phones rings).
- While XYZ's phone is ringing, he sends **updates** (TRYING, SESSION PROGRESS, and so on). User B picks up the phone and sends an **OK** response to the caller.
- ABC responds with an **ACK** acknowledgment.
- The conversation via **RTP** is established directly between the two parties.
- XYZ hangs up and sends a **BYE** message.
- ABC accepts the BYE message, and sends an **OK** as an acknowledgment.



Let's have a look at SIP call establishment in detail ...

SIP Call setup – Registration

The proxy server learns about the current location of XYZ, in the previous example through the process of **Registration**.

- F1 REGISTER Bob -> Registrar
- REGISTER sip:registrar.biloxi.com SIP/2.0
- Via: SIP/2.0/UDP
bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
- Max-Forwards: 70
- To: Bob <sip:bob@biloxi.com>
- From: Bob <sip:bob@biloxi.com>;tag=456248
- Call-ID: 843817637684230@998sdasdh09
- CSeq: 1826 REGISTER
- Contact: <sip:bob@192.0.2.4>
- Expires: 7200
- Content-Length: 0



**SIP Registration
Server**



Bob's SIP Phone



**The information
expires after 2 hours**

**Associating Bob's URI
<sip:bob@biloxy.com>
with the machine he is
currently logged (the
Contact information)
<sip:bob@192.0.2.4>**

SIP Call setup – INVITE

INVITE is an example of a SIP method that specifies the action that the requestor (ABC) wants the server (XYZ) to take.

- INVITE sip:bob@biloxi.com SIP/2.0
- Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
- Max-Forwards: 70
- To: Bob <sip:bob@biloxi.com>
- From: Alice <sip:alice@atlanta.com>;tag=1928301774
- Call-ID: a84b4c76e66710@pc33.atlanta.com
- CSeq: 314159 INVITE
- Contact: <sip:alice@pc33.atlanta.com>
- Content-Type: application/sdp
- Content-Length: 142

The Method name

The address which Alice is expecting to receive responses. This parameter indicates the path the return message needs to take

A display name and a SIP or SIPS URI towards which the request was originally directed

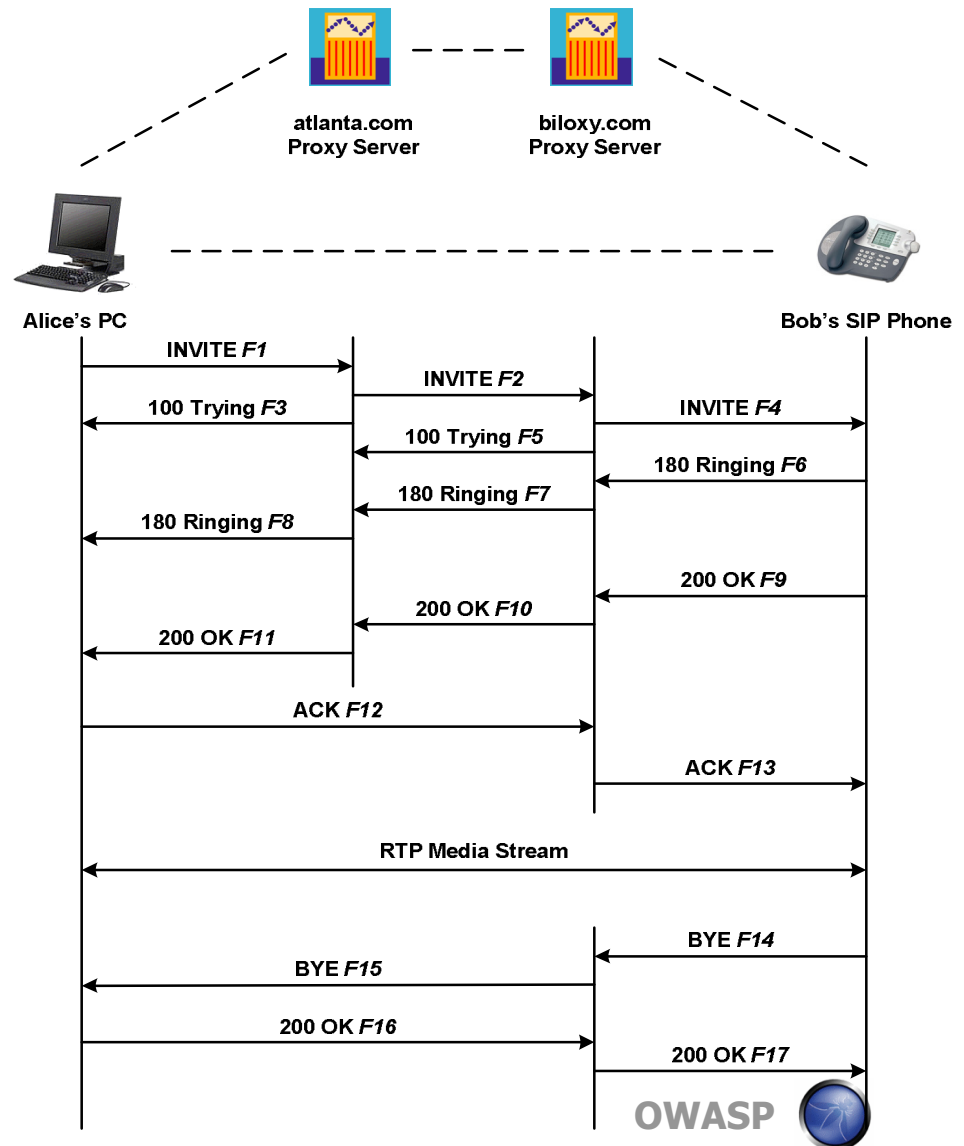
Contains a globally unique identifier for this call

Contains an integer (traditional sequence number) and a method name

Contains a SIP or SIPS URI that represents a direct route to Alice

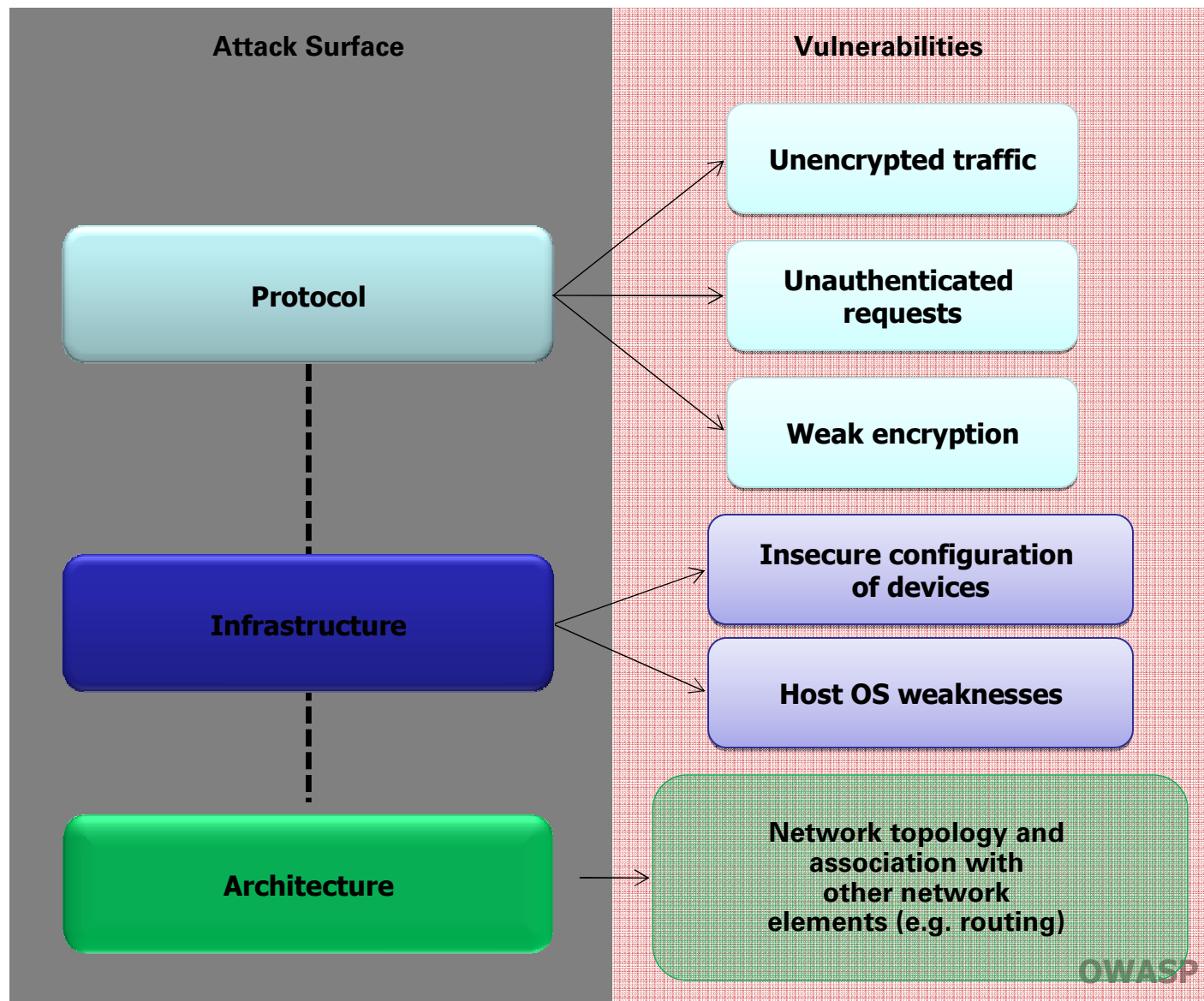
SIP Call setup – Forced Routing

- In the previous example, the example.com proxy server if wished to remain in the SIP messaging path beyond the initial INVITE, it would add to the INVITE a required routing header .
- This header field, known as **Record-Route** contains a URI resolving to the hostname or IP address of the proxy.
- This information would be received by both XYZ's SIP phone and (due to the Record-Route header field being passed back in the 200 (OK)) ABC's softphone and stored for the duration of the dialog.



VoIP Security – Vulnerability, Threats, Attacks

VOIP Vulnerabilities



What are the Threats?

Threats	Attack types	Attack subtypes
Social Threats	SPIT	
	Vishing	
Misrepresentation	Spoofed messages	
	Malformed Messages	
	Caller ID Spoofing	
Interception	Eavesdropping	Text/Fax
	Man in the Middle Attack	Video
		MITM on Proxy server
		MITM on User agent
		MITM on Registration server
		Registration hijacking
Service Disruption	Denial of service	Media Hijacking
		DOS on Proxy server
		DOS on User Agent
		DOS on <u>Registration server</u>
	Fuzzing	

Social Threats – Associated Attacks

Spam over Internet Telephony (SPIT)

What is SPIT?

Anyone using a PC is familiar with email SPAM. Voice SPAM refers to bulk, automatically generated, unsolicited phone calls. Voice SPAM or **SPAM over Internet Telephony (SPIT)** is a similar problem that will affect VoIP.

But how does it effect me?

- SPIT is like **telemarketing** on steroids. You can expect SPIT to occur with a frequency similar to email SPAM.
- As with email SPAM, it is very unlikely that SPIT calls can be identified based on **caller ID** and other information in the signaling.
- Another issue with SPIT is that you **can't analyze the call content** before the phone rings. Current SPAM filters do a reasonable job of blocking SPAM.
- Not an issue yet, but will become prevalent when:
 - The network makes it very inexpensive or **free to generate calls**
 - Attackers have access to VoIP networks that allow generation of a large number of calls
 - It is easy to set up a voice SPAM operation, using Asterisk, tools like “**spitter**”, and free VoIP access



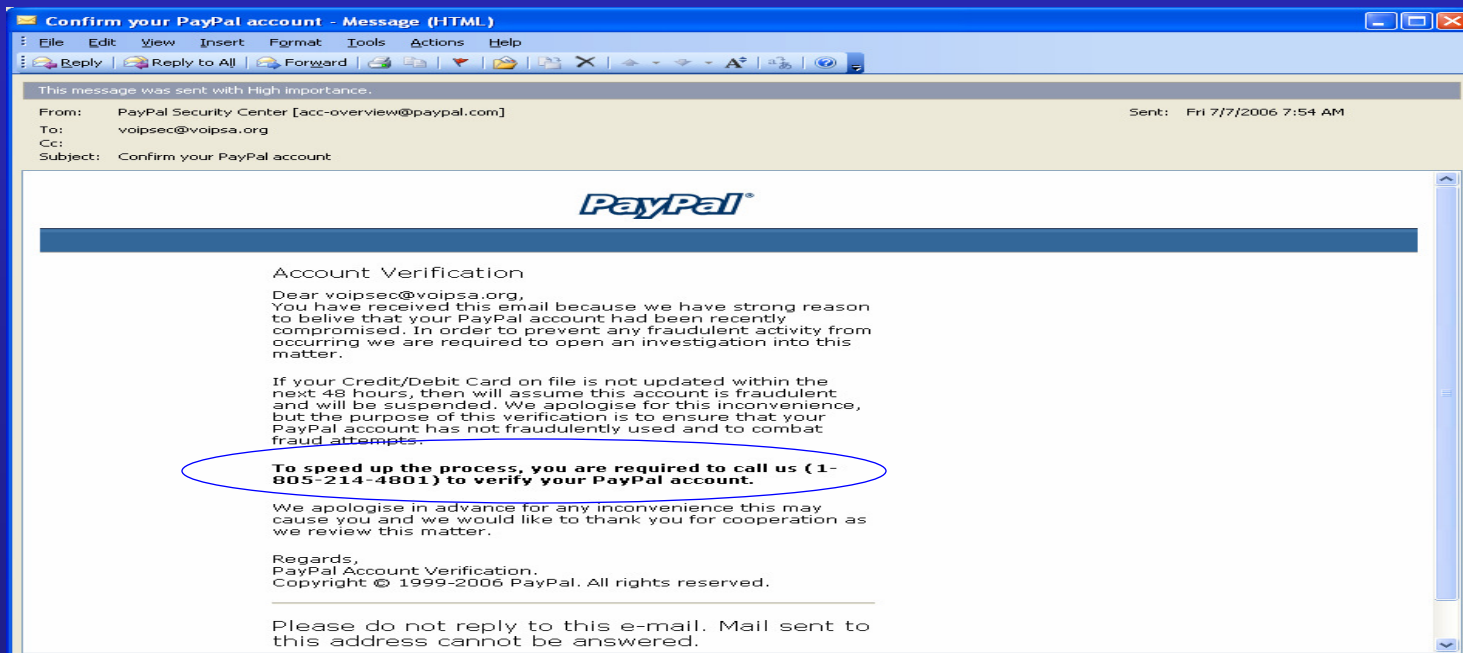
Social Threats – Associated Attacks

Vishing

What is Vishing?

Similar to the Phishing attack, vishing is a type of identity theft attack wherein the attack is delivered through email or voice. Victims are usually lured into the spoofed site and giving up vital information such as passwords, mother's maiden name, credit card numbers, and Social Security numbers.

But how does it effect me?



Misrepresentation – Associated attacks

Spoofed Messages

Spoofed messages

- Due to ignoring the value of '**Call-ID**' and even '**tag**' and '**branch**' while processing **NOTIFY** messages.

Example:

Attacker spoofs the SIP-Proxy's IP, here: 10.1.1.1 Victim 10.1.1.2

UDP-Message from Attacker to Victim:

Session Initiation Protocol

Request-Line: NOTIFY sip:login@10.1.1.2 SIP/2.0

Message Header

Via: SIP/2.0/UDP

15.1.1.12:5060;branch=0000000000000000

From: "asterisk"

<sip:asterisk@10.1.1.1>;tag=0000000000

To: <sip:login@10.1.1.2>

Contact: <sip:asterisk@10.1.1.1>

Call-ID: 0000000000000000@10.1.1.1

CSeq: 102 NOTIFY

User-Agent: Asterisk PBX

Event: message-summary

Content-Type: application/simple-message-summary

Content-Length: 37

Message body

Messages-Waiting: yes\n

Voicemail: 3/2\n



Misrepresentation – Associated attacks

Malformed Messages

An attacker may create and send **malformed messages** to the target server or client for the purpose of service interruption. A malformed message is a protocol message with wrong syntax. The following shows an example with a SIP INVITE message.

INVITE Hi this is a PETER sip:UserB@example.com SIP/2.0

Via: SIP/2.0/UDP userAclient.example.com:5060;branch=z9hG4bK74bf9

Max-Forwards: 70

From: UserA <sip:UserA@example.com>;tag=9fxced76sl

To: UserB <sip:UserB@example.com>

Call-ID: 2xTb9vxSit55XU7p8@example.com

CSeq: 1 INVITE

Contact: <sip:UserA@userAclient.example.com>

Content-Type: application/sdp

Content-Length: 151

v=====0

o=UserA 2890844526 2890844526 IN IP4 userAclient.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

Malformed message Inserted by attacker

Interception – Associated attacks

Man in the middle (MITM) Attacks

What is MITM?

In a VOIP man-in-the-middle attack, the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, or vice versa. Once the attacker has gained this position, he can hijack calls via a redirection server

Which VOIP Elements can be attacked?

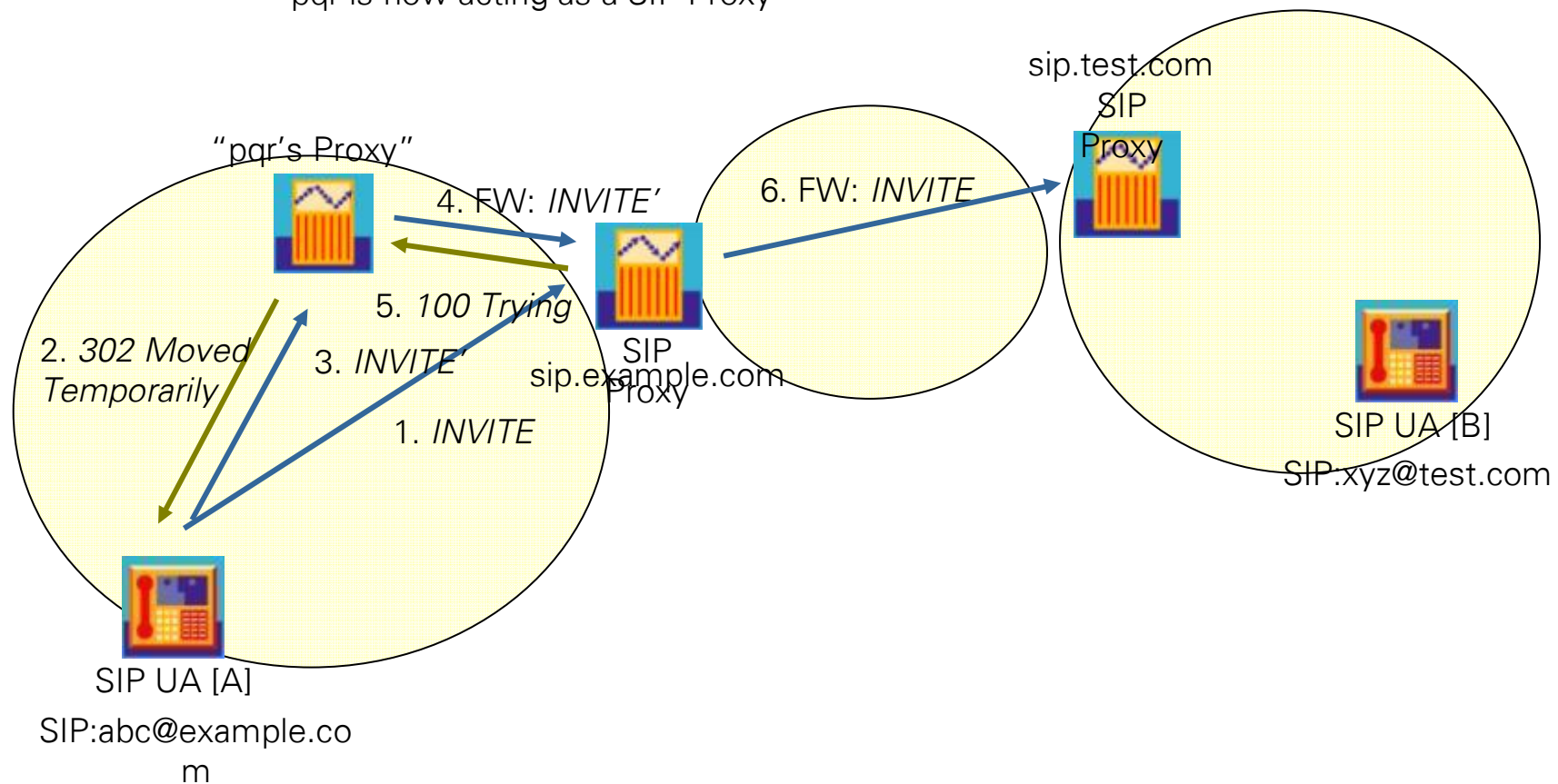
- SIP Registrar
- SIP Proxy Server
- SIP Redirect Server
- SIP UA



Interception – Associated attacks

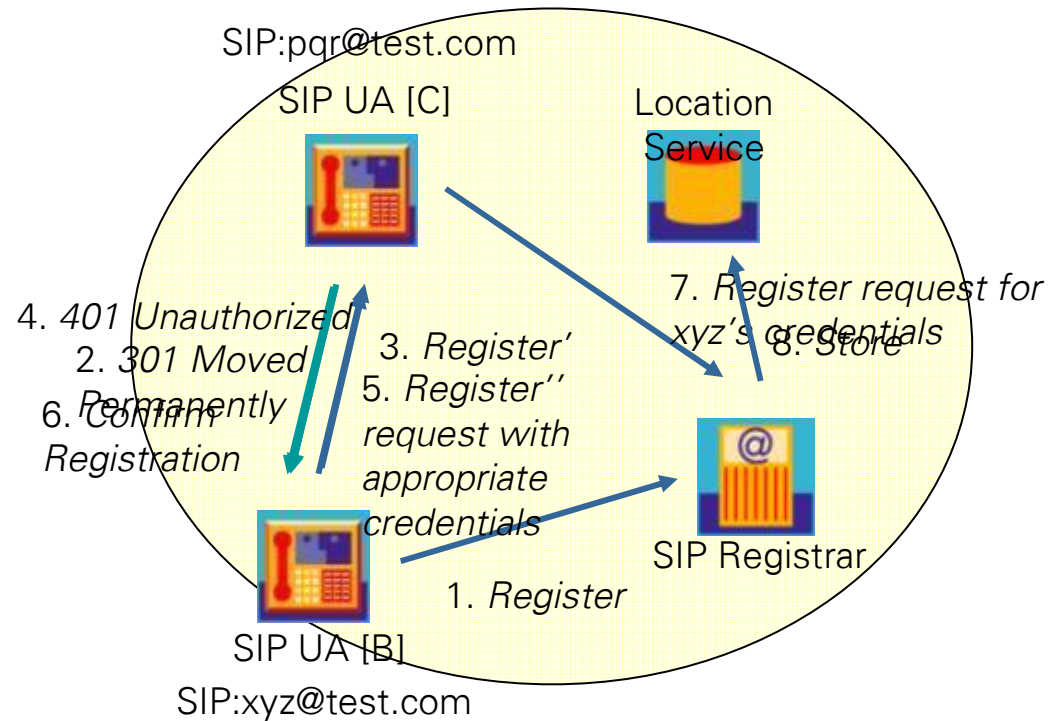
MITM on Proxy – 302 Moved Temporarily

pqr is now acting as a SIP Proxy



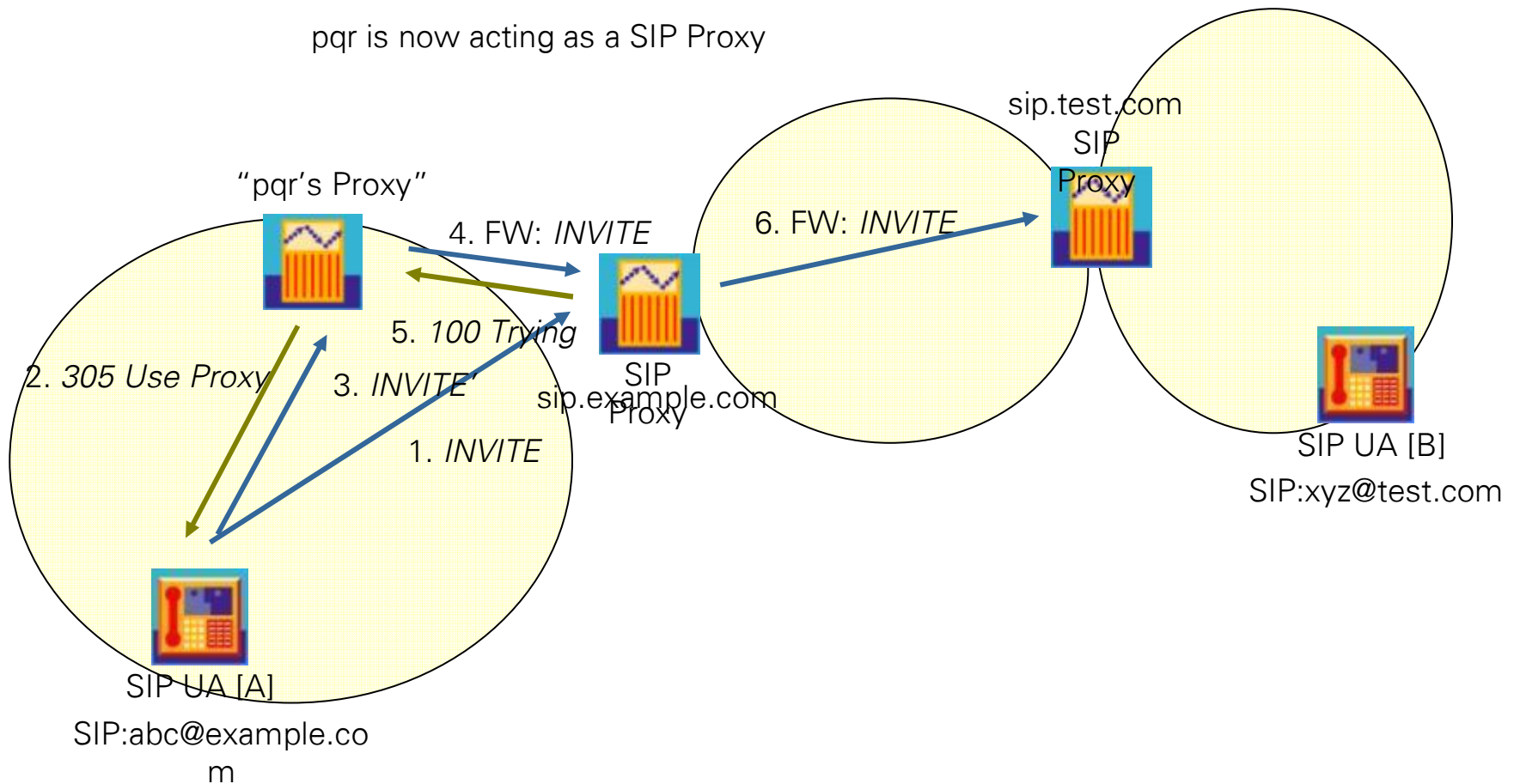
Interception – Associated attacks

MITM on Registrar



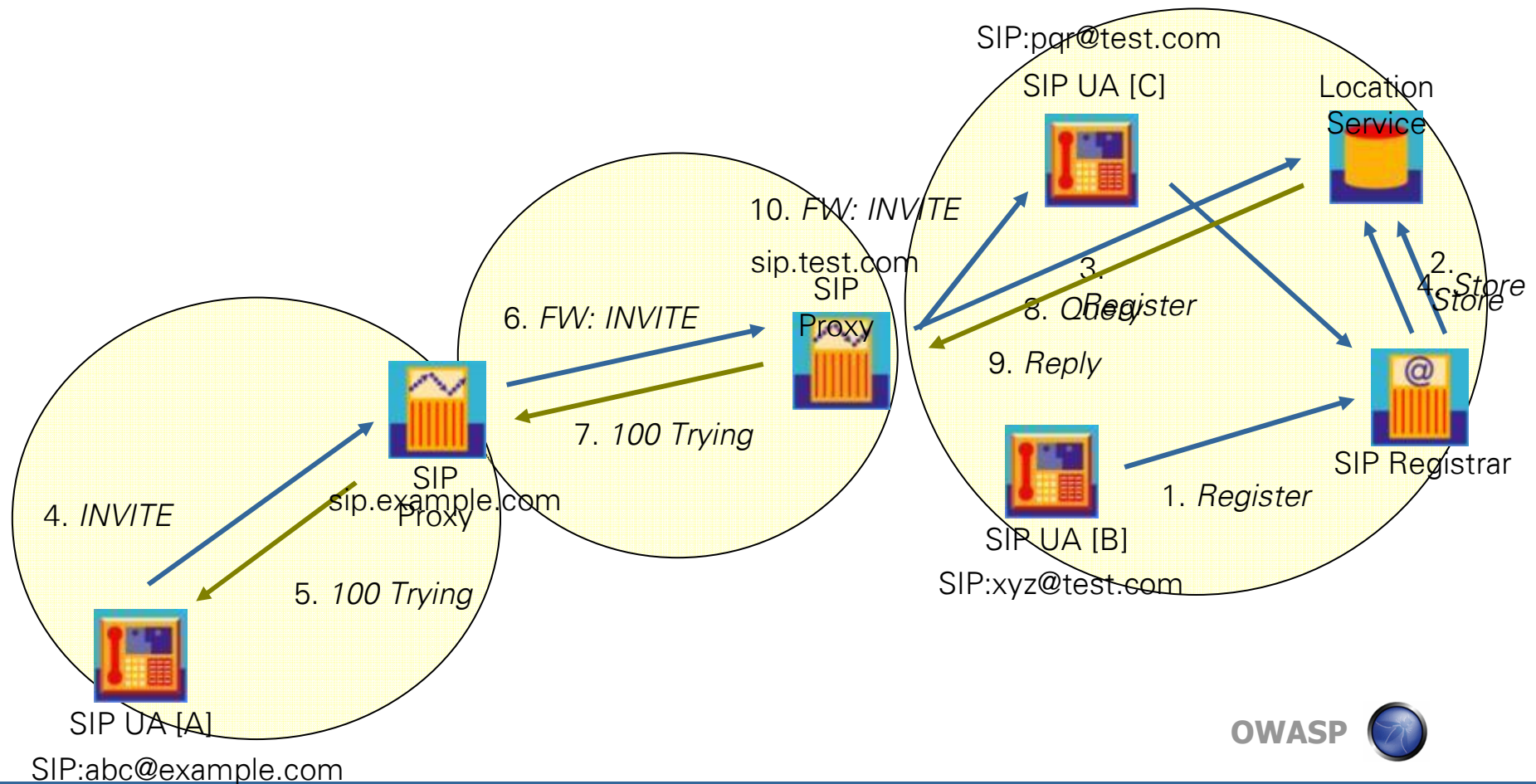
Interception – Associated attacks

MITM on Proxy - 305 Use Proxy



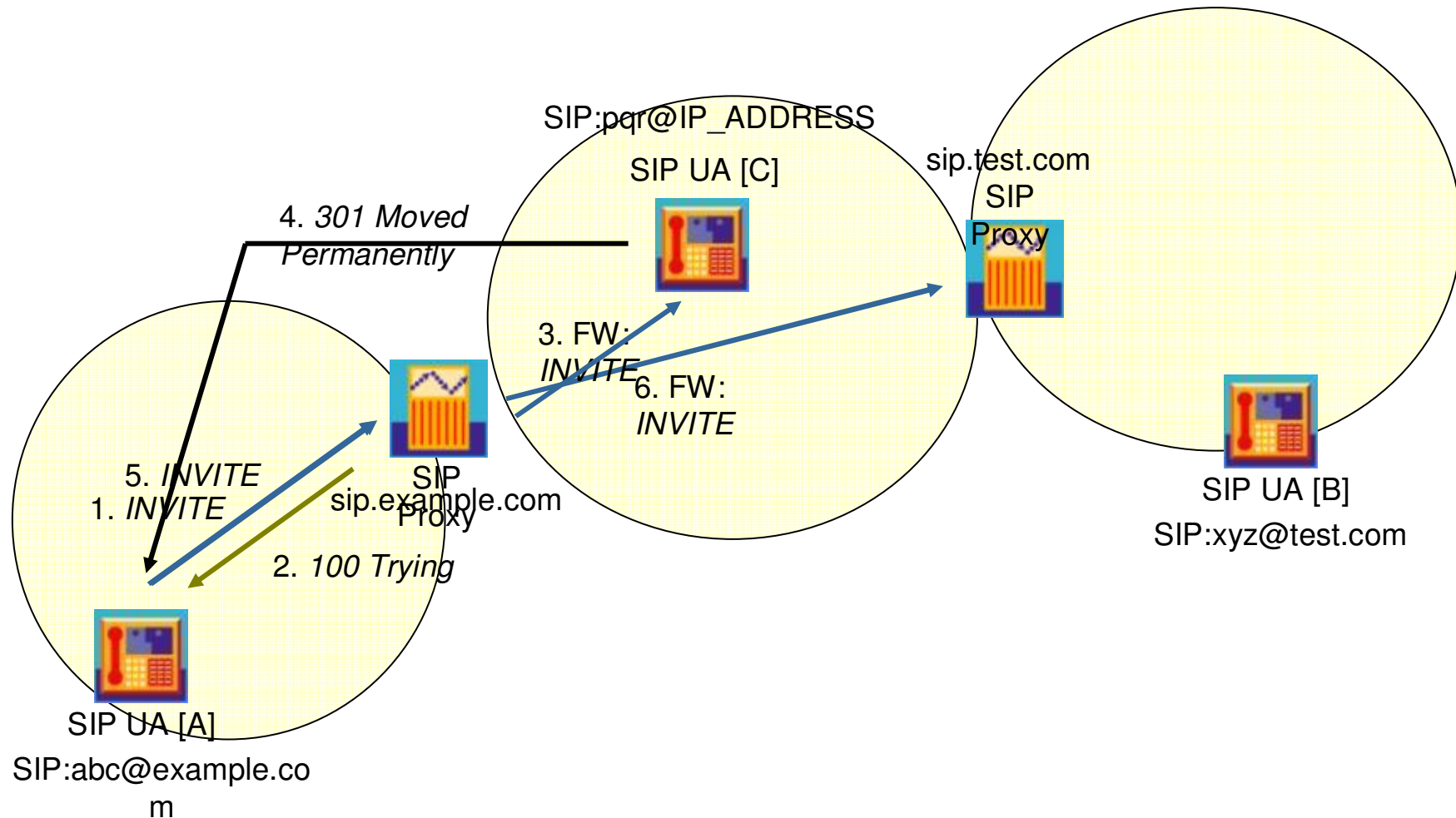
Interception – Associated attacks

Call Hijacking - Using Manipulation of the Registration Records



Interception – Associated attacks

Call Hijacking - Using 301 Moved Permanently Response Code



Service Disruption – Associated attacks

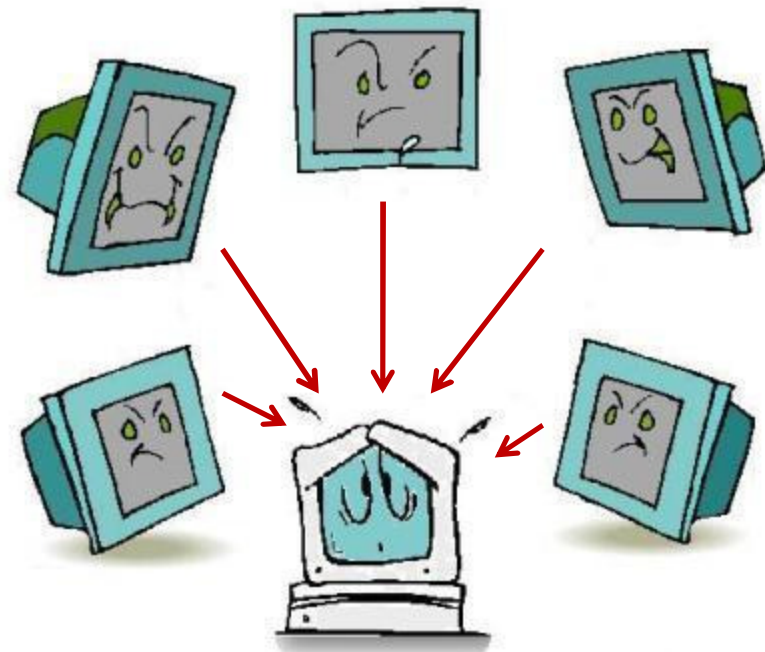
Denial of service

What is Denial of service?

A **denial-of-service** attack (DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

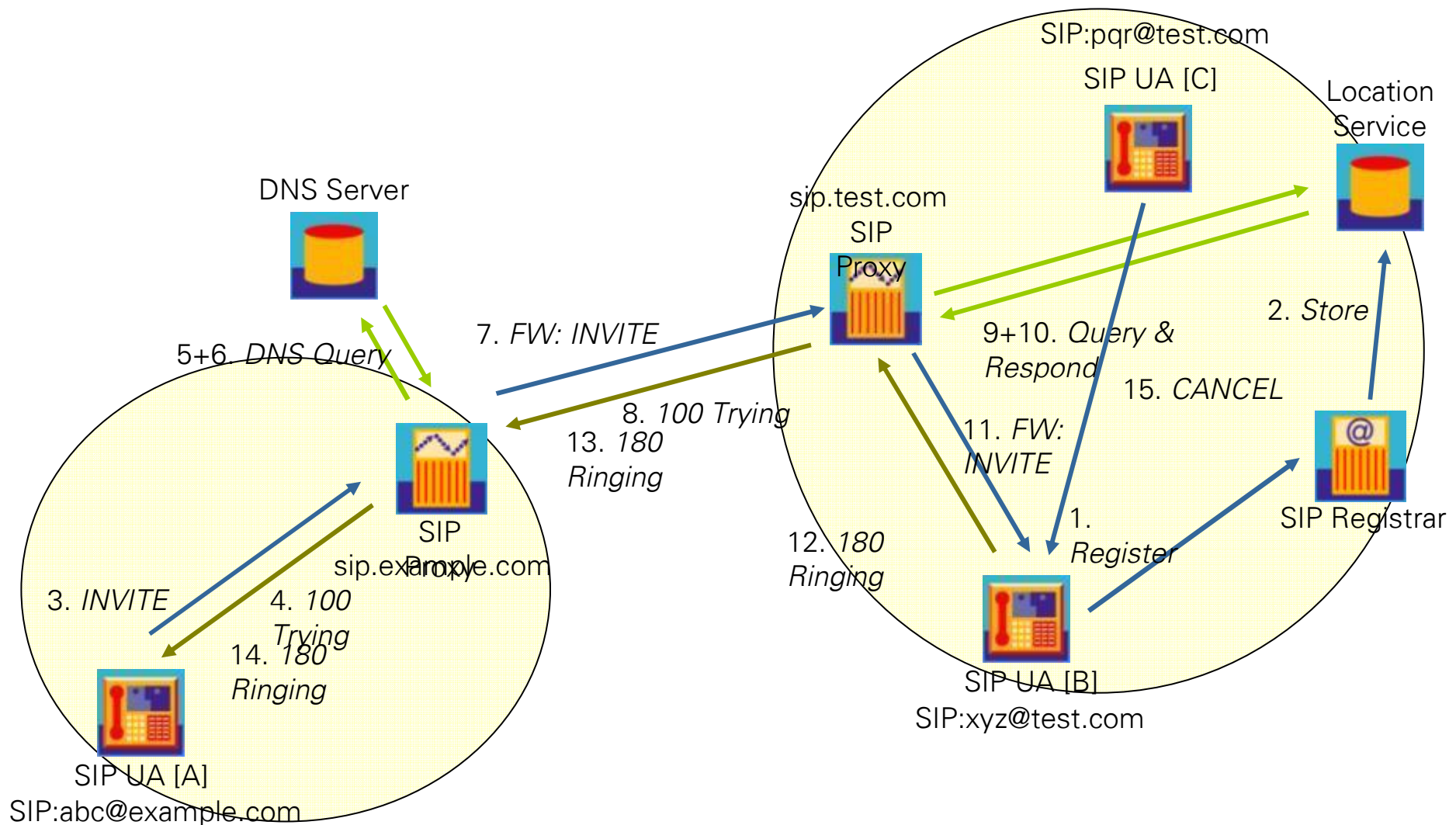
Which VOIP Elements can be attacked?

- SIP Registrar
- SIP Proxy Server
- SIP Redirect Server
- SIP UA



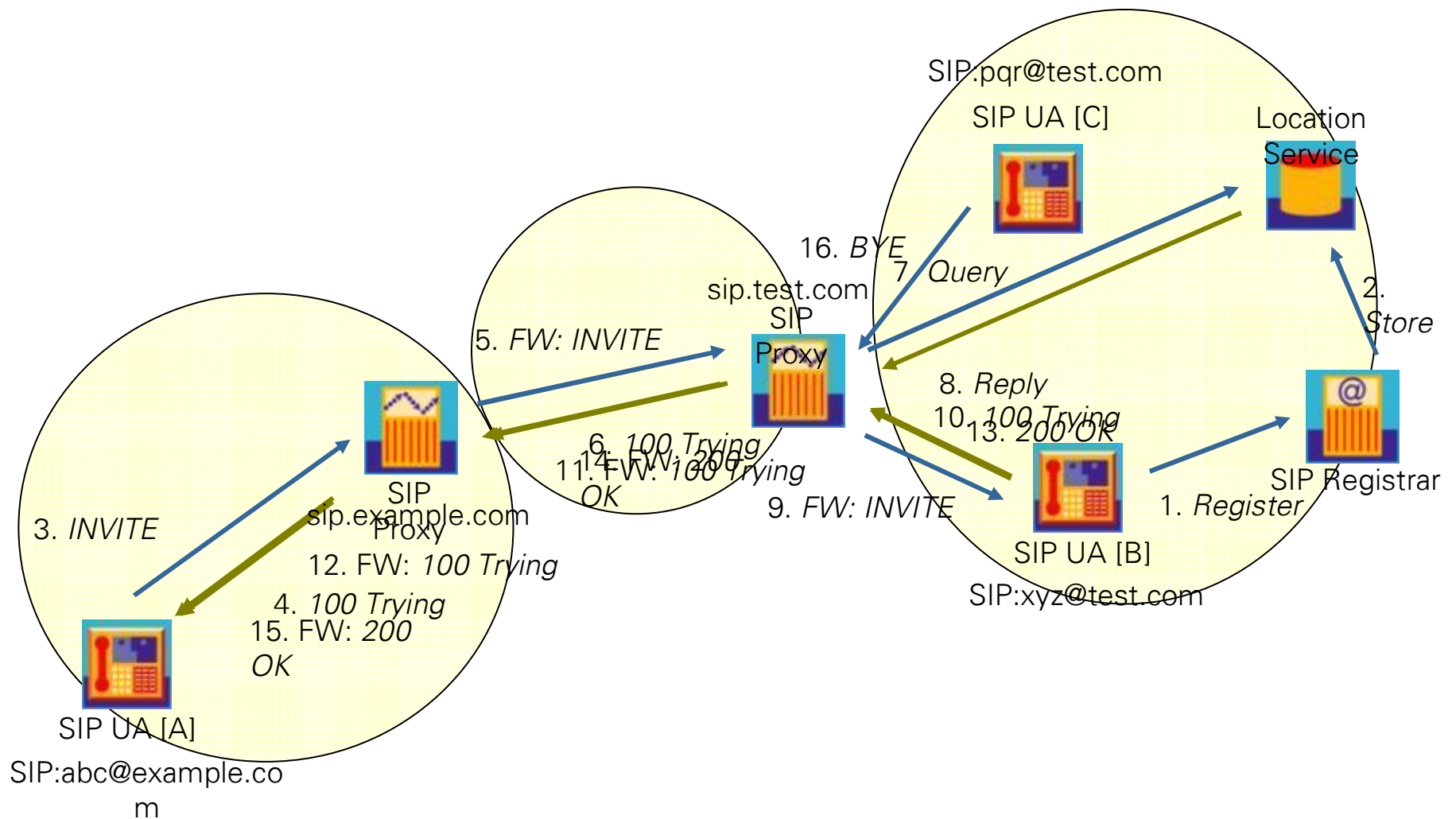
Service Disruption – Associated attacks

DOS on User Agent - DOS Cancel



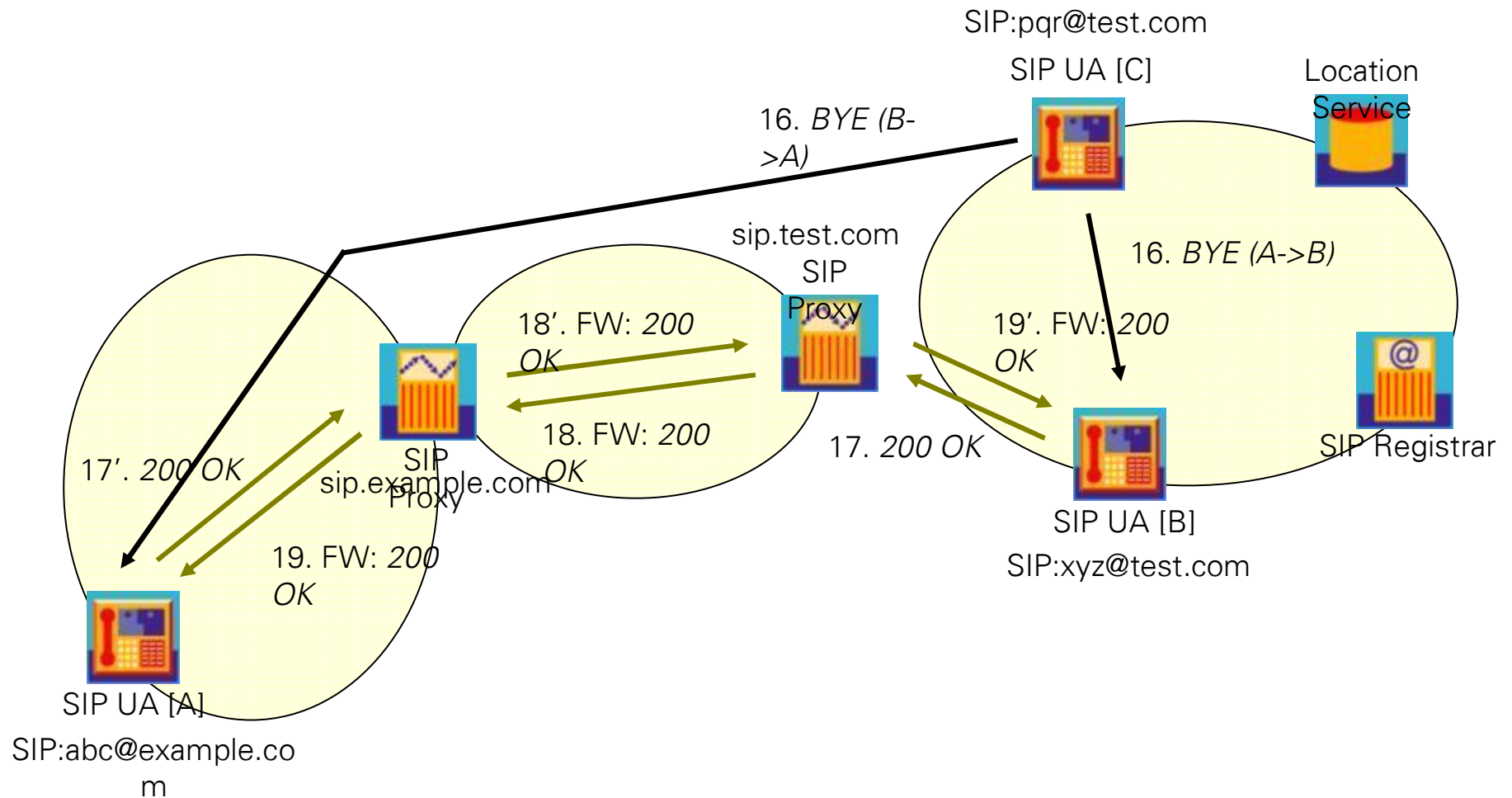
Service Disruption – Associated attacks

DOS on Proxy - DOS BYE



Service Disruption – Associated attacks

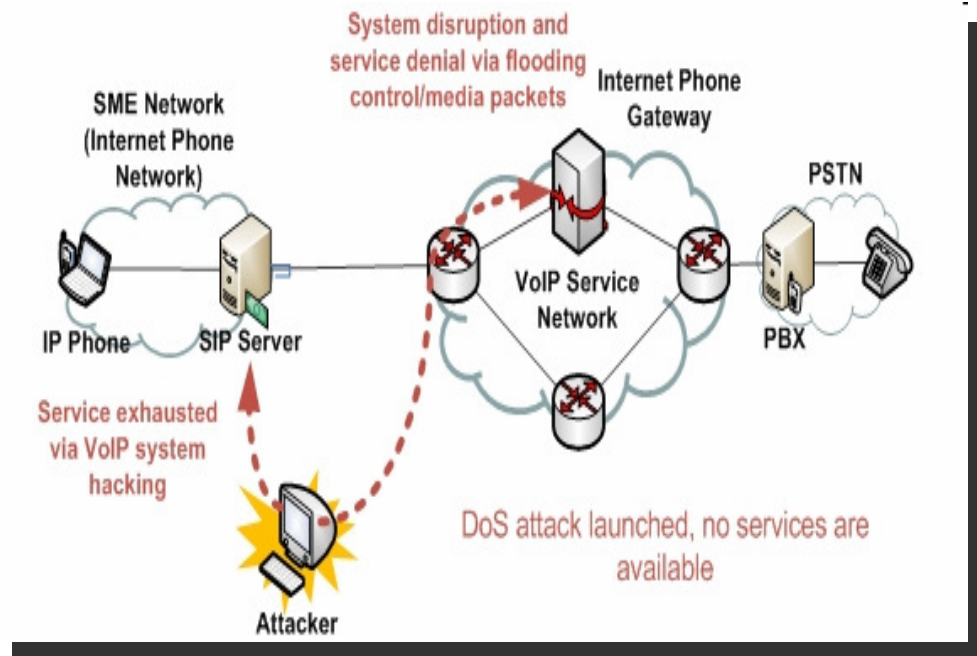
DOS on Proxy - DOS BYE to both



Service Disruption – Associated attacks

VOIP Flooding Attack

INVITE: SIP:u1@2d4fww.hard-to-resolve.domain SIP/2.0
Via: SIP/2.0/UDP 10.147.65.91;
branch=z9hG4bk29FE738
CSeq: 16466 INVITE
To: sip:u1@2d4fww.hard-to-resolve.domain
Content-Type: application/sdp
From: SIP: u2@2d4fww.hard-to-resolve.domain; tag=24564
Call-ID: 1163525243@10.147.65.91
Subject: Message
Content-Length: 184
Contact: SIP: u2@2d4fww.hard-to-resolve.domain
...
<SDP part not shown>



Fuzzing

What is fuzzing?

Fuzzing is a method for finding bugs and vulnerabilities by creating different types of packets for the target protocol that push the protocol's specifications to the breaking point. The practice of fuzzing, otherwise known as robustness testing or functional protocol testing.

Buffer Overflows

Buffer overflow occurs when a program or process tries to store more data in a memory location than it has room for, resulting in adjacent memory locations being overwritten.

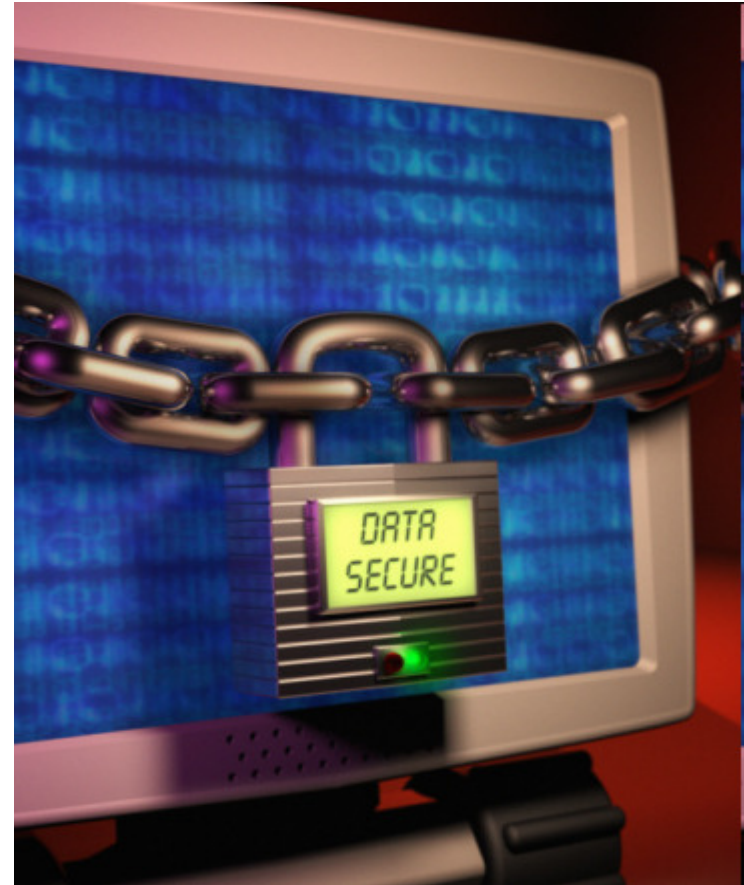
[illegible]

Test case - Incrementally increase the length of the URL until crashing the IIS process

VoIP Security – Countermeasures

Why traditional Logical Controls won't work . . .

- Dynamic assignment of Ports
- Quality of Service
- Firewall Limitations
- Nat Bindings



Countermeasures

Logical Controls

☐ Logical Controls

▶ Protocol

- Authentication
- Selective Encryption
- Authorization

▶ Infrastructure

- Malware protection for host OS
- Timely patching for host OS

▶ Network

- Segregate VoIP and data networks in zones and VLANs
- Deploy Intrusion Prevention/ Detection System
- Filter traffic using application-level Gateway between Trusted and Un-trusted Zones
- Encrypt (VPN) VoIP traffic over critical segments



Countermeasures

Logical Controls - Protocols

● Authentication

- Digest Authentication
 - Used during UA registration
 - Authenticates UA to SIP proxy
 - Similar to HTTP digest from web browser to web server
 - Cannot be used between proxies

● Encryption

- Transport Layer Security (TLS)
 - Used to secure signaling path
 - Authenticates each endpoint on a link
 - Provides encrypted path between each link
 - Non-transitive trust
 - Can be used between proxies
 - Requires X.509 certificates

▶ Authentication and Encryption

- Secure RTP (SRTP)
 - Used to secure the media path
 - Provides end-to-end security
 - Requires X.509 certificates
- Zphone (ZRTP)
 - Used to secure the media path
 - Provides end-to-end security
 - Requires no X.509 certificates
 - Relies on OSI layer 8 authorization

Countermeasures

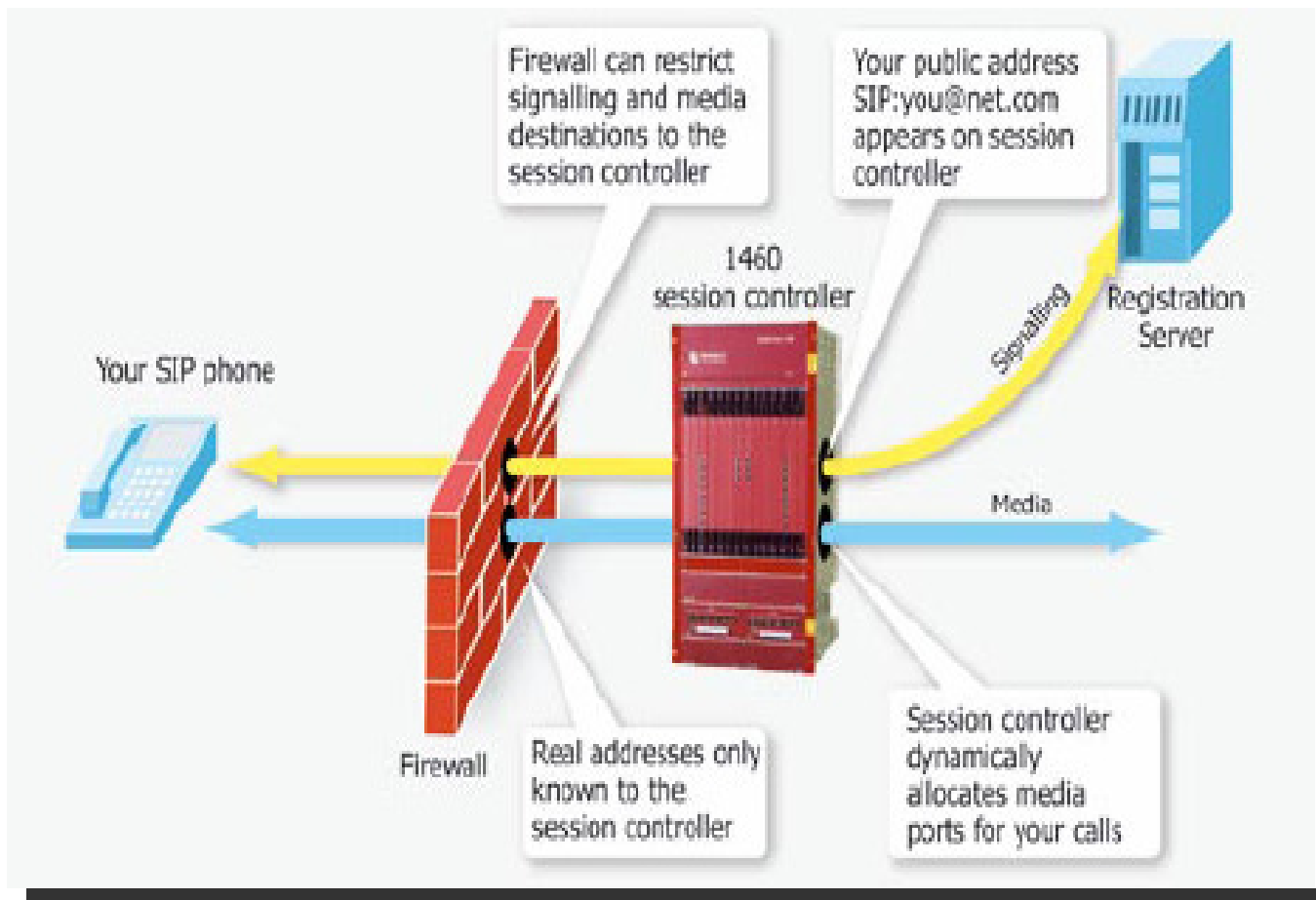
Logical Controls – Application Level Gateway

Application Level Gateways (ALGs) are the typical commercial solution to the firewall/NAT traversal problem. An ALG is embedded software on a firewall or NAT, that allows for dynamic configuration based on application specific information.



Countermeasures

Logical Controls – Session Border Controller

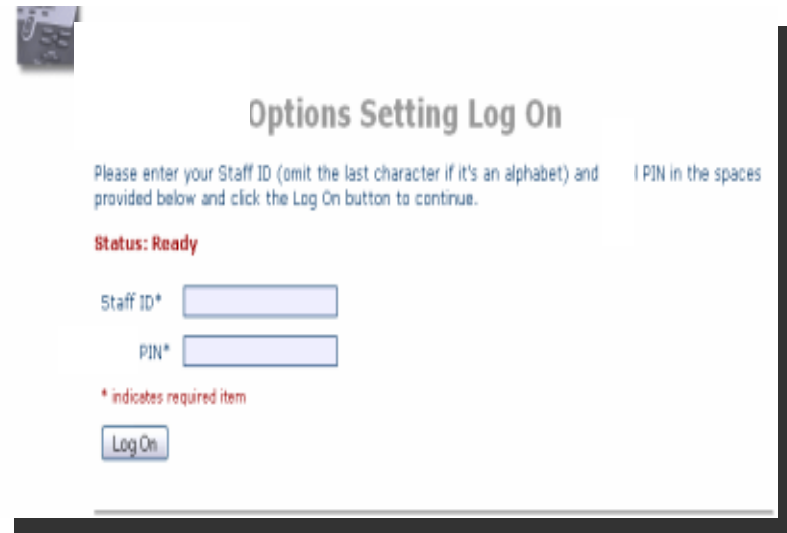


VoIP Security – Assessing Security Controls

Footprinting

Footprinting is usually the first step in gathering information prior to an attack - sensitive details hanging out in the public domain and available to any resourceful hacker who knows how and where to look

- Footprinting does not require network access
- An enterprise website often contains useful information
- Google is very good at finding details on the web:
 - Vendor press releases and case studies
 - Resumes of VoIP personnel
 - Mailing lists and user group postings
 - Web-based VoIP logins
 - ♦ `inurl:"ccmuser/logon.asp"`
 - ♦ `inurl:"ccmuser/logon.asp" site:example.com`
 - ♦ `inurl:"NetworkConfiguration" cisco`
 - ♦ `inurl:sip -intitle:ANNOUNCE -inurl:lists`
 - ♦ `intitle:asterisk.management.portal web-access`



The screenshot shows a web interface for a VoIP system. At the top, there's a header 'Options Setting Log On'. Below it, a message says: 'Please enter your Staff ID (omit the last character if it's an alphabet) and PIN in the spaces provided below and click the Log On button to continue.' There are two input fields: 'Staff ID*' and 'PIN*', both with asterisks indicating they are required. Below the fields is a 'Log On' button. A small red note at the bottom left of the form area says '* indicates required item'.

Scanning

Scanning is probing each IP address in the target range for evidence of live systems and identify the services running on each system. **Nmap** is commonly used for this purpose.

Example: `nmap 192.168.1.2`

- **Open** An application is actively accepting TCP connections or UDP packets on this port.
- **Closed** A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it.
- **Filtered** Nmap cannot determine whether or not the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software.
- **Unfiltered** The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed.
- **open|filtered** Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response.
- **closed|filtered** This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IPID Idle scan.
- **tcpwrapped** TCP Wrapper is a public domain computer program that provides firewall services for UNIX servers and monitors incoming packets.



Scanning

- After hosts are found, scans are used to find running services
 - `nmap -sV 192.168.1.2`
- After hosts are found and ports identified, the type of device can be determined
 - `nmap -O -P0 192.168.1.2`
- Network stack fingerprinting is a common technique for identifying hosts/devices

Example : `nmap -O -P0 192.168.1.2 - UDP PORT STATE SERVICE`

67/udp open|filtered dhcpserver

69/udp open|filtered tftp

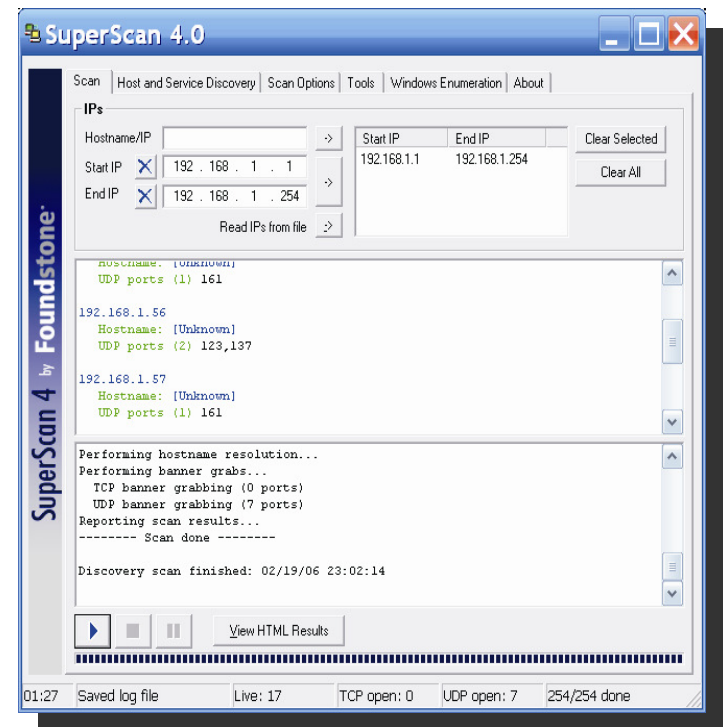
111/udp open|filtered rpcbind

123/udp open|filtered ntp

784/udp open|filtered unknown

5060/udp open|filtered sip

32768/udp open|filtered omad



Enumeration

Enumeration involves testing open ports and services on hosts to gather more information

- Includes running tools to determine if open services have known vulnerabilities
- Also involves scanning for VoIP-unique information such as phone numbers
 - Automated REGISTER, INVITE, and OPTIONS Scanning with SIPSCAN Against SIP Servers
- Includes gathering information from TFTP servers and SNMP

Enumeration TFTP

- Almost all phones use TFTP to download their configuration files
- The TFTP server is rarely well protected
- If you know or can guess the name of a configuration or firmware file, you can download it without even specifying a password
- The files are downloaded in the clear and can be easily sniffed
- Configuration files have usernames, passwords, IP addresses, etc. in them

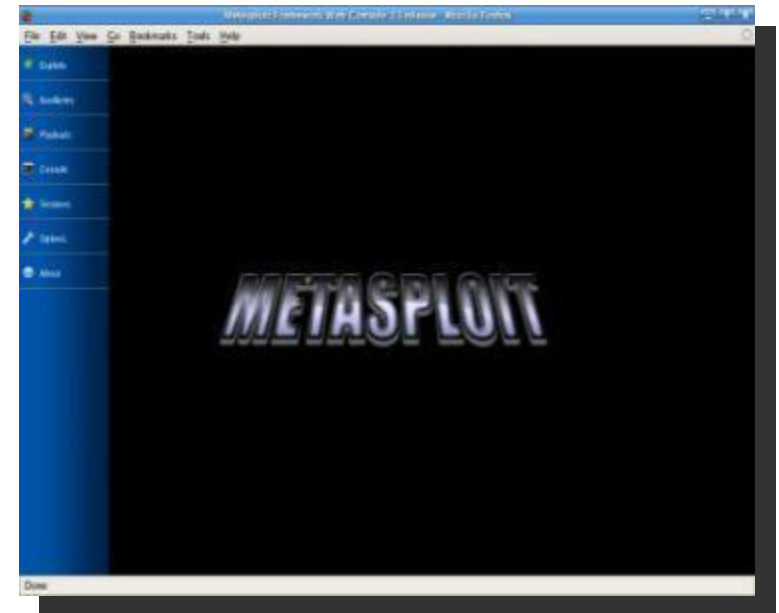


Enumeration

```
[root@attacker]# tftp 192.168.1.2
tftp> get example.cnf
root@attacker]# cat example.cnf
SIP Configuration Generic File (start)
Line 1 Settings line1_name: "502"
Line 1 Extension\User ID line1_displayname "502"
Line 1 Display Name line1_authname: "502"
Line 1 Registration Authentication
line1_password: "test123"
Line 1 Registration Password
```

SNMP Enumeration

- Simple Network Management Protocol (SNMP) version 1 is another inherently insecure protocol used by many VoIP devices
- `snmpwalk -c public -v 1 192.168.1.53 1.3.6.1.4.1`



Tools

- Footprinting
- Google
- ARIN
- APNIC
- Archive.org
- Enumeration
- Netcat
- SiVuS
- Smap
- Scanning
- fping
- Nessus
- nmap
- SNMP walk
- SNSscan
- SuperScan
- Metasploit

Infrastructure Denial of Service

- DNS Auditing tool
- Internetwork Routing Protocol Attack Suite
- UDP Flooder
- Wireshark

Eavesdropping

- Cain and Abel
- dsniff
- VoIPong
- vomit

Network and Application Interception

- arpswatch
- Cain and Abel
- Dsniff
- Ettercap
- siprogue

Fuzzing

- ohrwurm RTP fuzzer
- PROTOS SIP fuzzing suite
- TCPView

References

- NIST
 - ▶ Security Considerations for VoIP Systems
 - ▶ Voice over Internet Protocol (VoIP), Security Technical Implementation Guide (DISA)
- <http://www.ietf.org/html.charters/iptel-charter.html>
- IP Telephony Tutorial, <http://www.pt.com/tutorials/iptelephony/>
- SIP - <http://www.cs.columbia.edu/sip/>
- IP Telephony with SIP - www.iptel.org/sip/
- SIP Tutorials
 - ▶ The Session Initiation Protocol (SIP)
 - ▶ http://www.cs.columbia.edu/~hgs/teaching/ais/slides/sip_long.pdf
 - ▶ SIP and the new network communications model
<http://www.webtorials.com/main/resource/papers/nortel/paper19.htm>
- H.323 ITU Standards - <http://www.imtc.org/h323.htm>

Q & A, Feedback



Question and Answers

Thank you