VoIP Security & Attacks

by

Edgardo Romero Aguero

What Is VoIP?

Routing of voice conversations over IP network

Analogue signal is digitized using CODEC

Compressed and sent over IP network in a packet

Low cost compared to PSTN

VoIP Protocols

Protocols are divided into two roles

Signalling Protocols & Media Transport Protocols

Signalling Protocols

Locate user

Establish & tear down sessions

Session Initiation Protocol (SIP) & H.323

Application level protocols

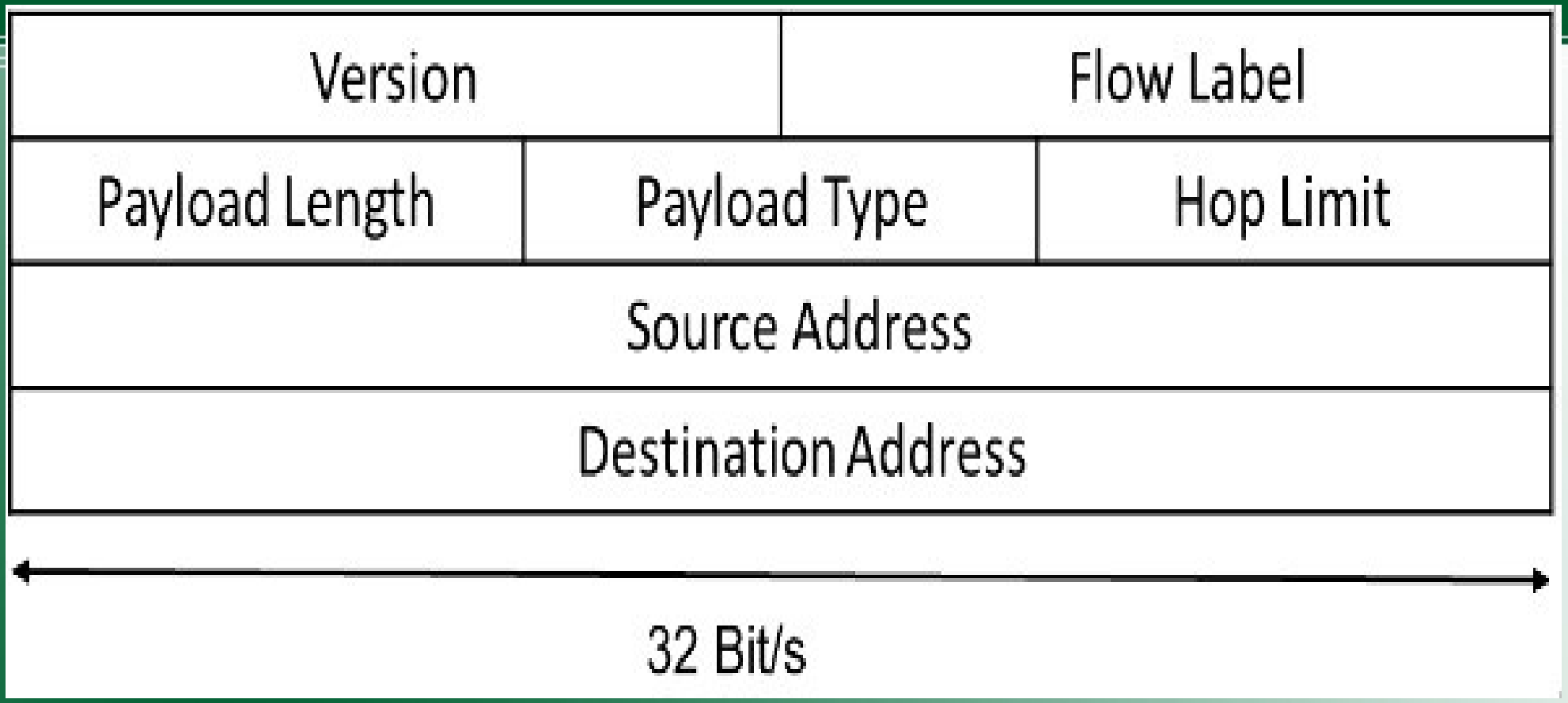
SIP

Used for controlling sessions

Can run over TCP and UDP

Port 5060 for non encrypted traffic

Port 5061 for encrypted traffic using TLS


Version
Flow Label
Payload Length
Payload Type
Hop Limit
Source Address
Destination Address
32 Bit/s

Media Control Protocol

Used for delivering real-time multimedia data

Provides services such as time stamps, sequence numbers, and payload format

Real-time Transport Protocol (RTP)

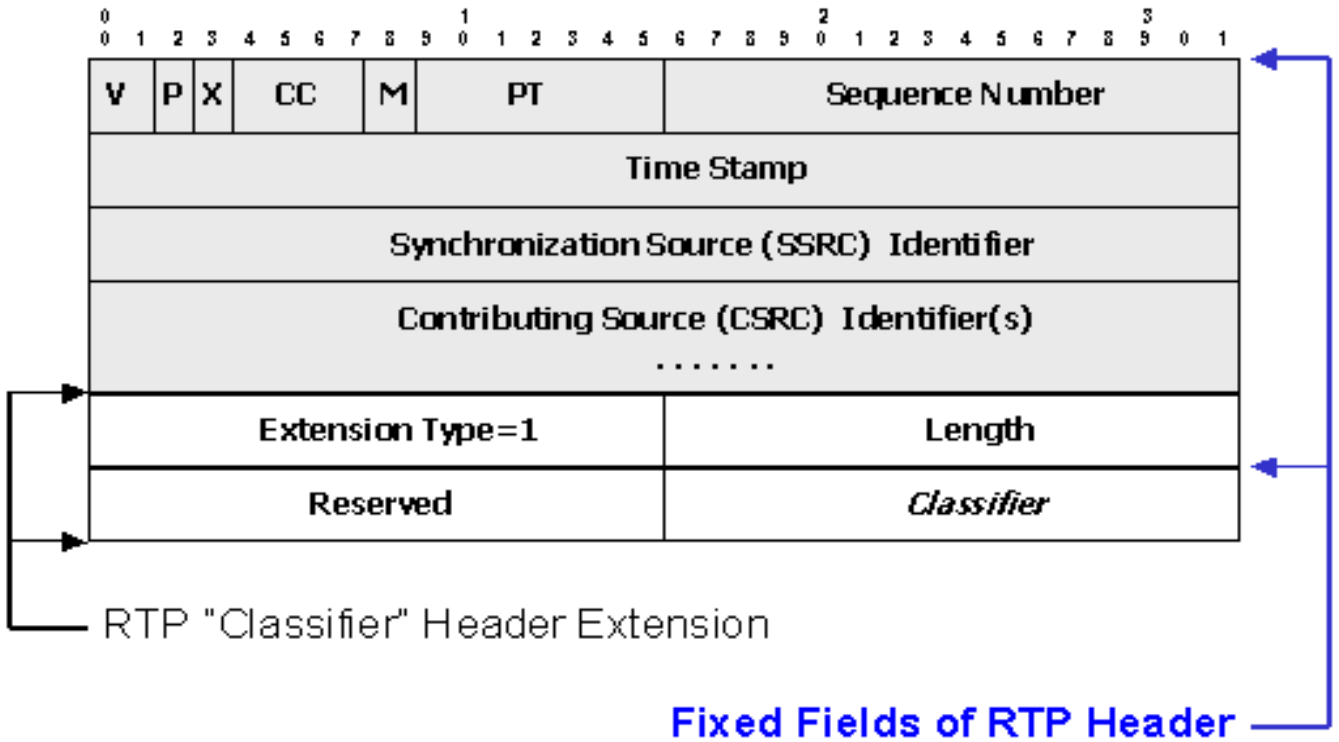
RTP

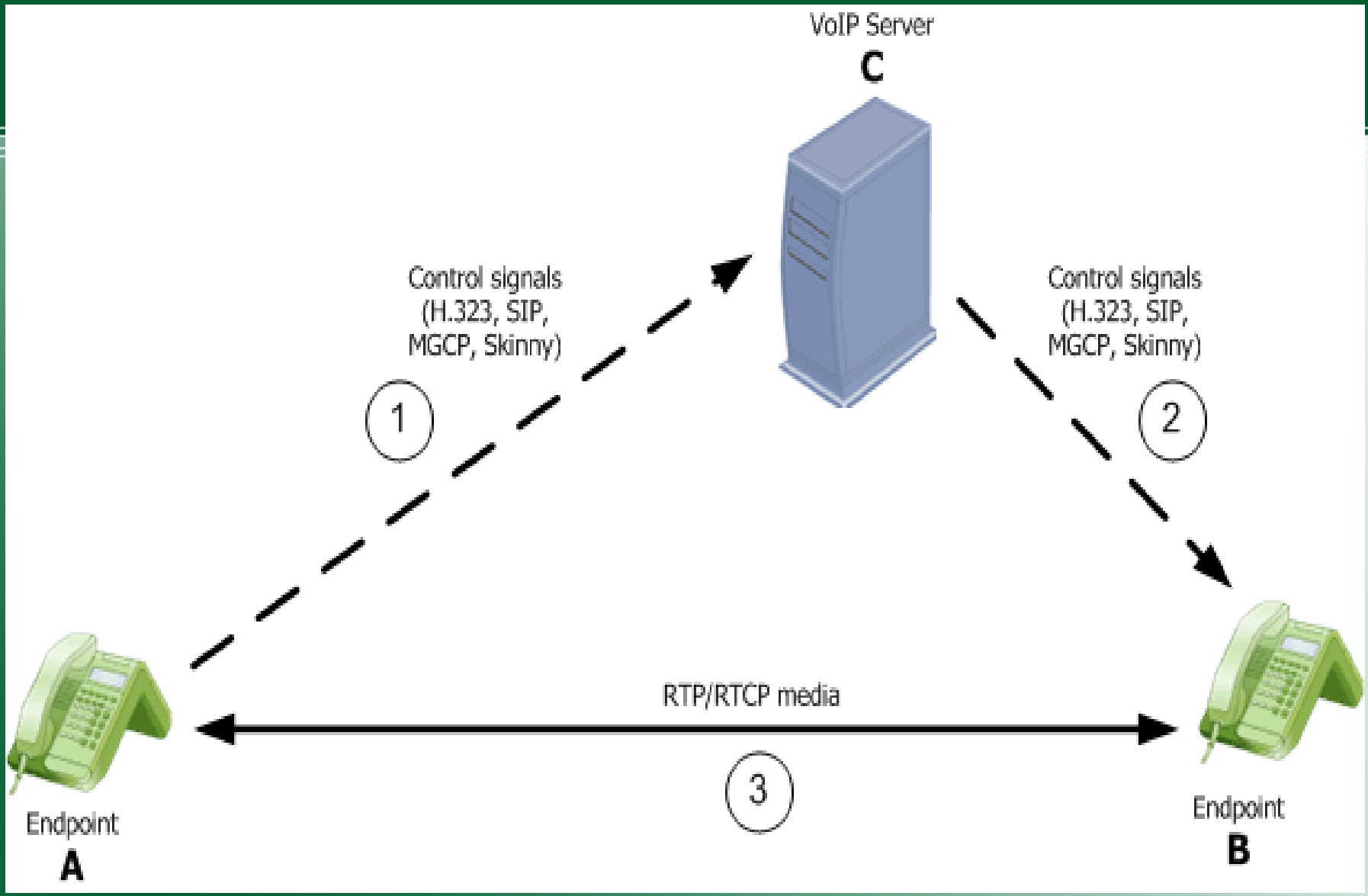
Designed for end-to-end real time transfer of data

Two sub protocols: RTP & RTP Control Protocol

RTCP used to provide feedback on QoS

RTP Header & Extension




VoIP Server
C
Control signals
(H.323, SIP,
MGCP, Skinny)
1
Control signals
(H.323, SIP,
MGCP, Skinny)
2
RTP/RTCP media
3
Endpoint
A
Endpoint
B

VoIP Security

Four attack surfaces

Protocols: unencrypted traffic & unauthenticated requests

Infrastructure: insecure configuration of devices

Architecture: network topology (routing)

Social engineering

VoIP Attacks & Solutions

Denial of Service Attack (DoS)

Flood user with INVITE requests

Use CANCEL, GOODBYE or PORT UNREACHABLE to drop call

VoIP Attacks & Solutions

Filter unwanted traffic using firewalls

Can reduce QoS with time delays

Authentication before forwarding messages

Use a shared secret

VoIP Attacks & Solutions

Eavesdropping

Can eavesdrop using Phrase Spotting

Possible because of Code-Excited Linear Prediction (CELP)

Encryption

VoIP Attacks & Solutions

SPIT & Vishing

Pretend to be trustworthy organization and have user give out their own data

VoIP Attacks & Solutions

Filter traffic based on frequency and duration

Signal protocol analysis

Reputation based spam filtering

Adequate training for employees

VoIP Attacks & Solutions

Man-in-the-middle attack

Alice sends message to Bob

Spoofed message back to Alice (301 moved permanently)

VoIP Attacks & Solutions

Alice sends new message to attacker

Attacker establishes connection with Bob

Sends back code 200 to Alice

VoIP Attacks & Solutions

Device Authentication

Packet integrity checking