Intro to VoIP

Zhengtang Cao
Zihao Gu
Jialin Sun

VoIP Basic/Application

- Voice over IP
  - A suite of IP-based communications services.
  - Provides multimedia communications over IP networks
  - Enable “voice” to be transported using the Internet Protocol (IP).

- Applications
  - Skype, Viber, Avaya, and 8x8
  - Microsoft Net meeting, ohphone, gphone

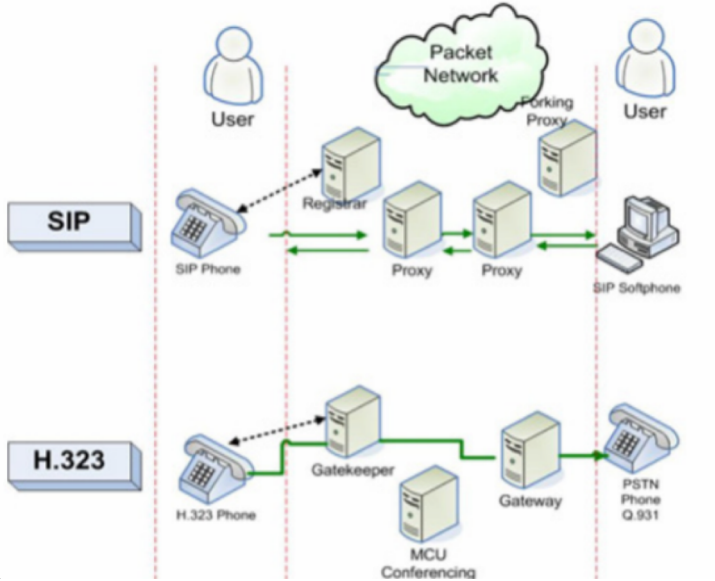
VoIP Advantage/Disadvantage

- Advantage:
  - Less cost compare to traditional phone call
  - VoIP offer providers with easy IT management and reduced operating costs
  - VoIP technology is feature rich to support multimedia application
    - share files
    - video/audio conferences

- Disadvantage:
  - Security Concerns
  - Reliability problem: sound quality might not stable as traditional phone call
  - Might not support emergency calls

VoIP overview – Signaling Protocols

- Locate User
- Session Establishment
- Session Setup Negotiation
- Modify Session
- Teardown Session



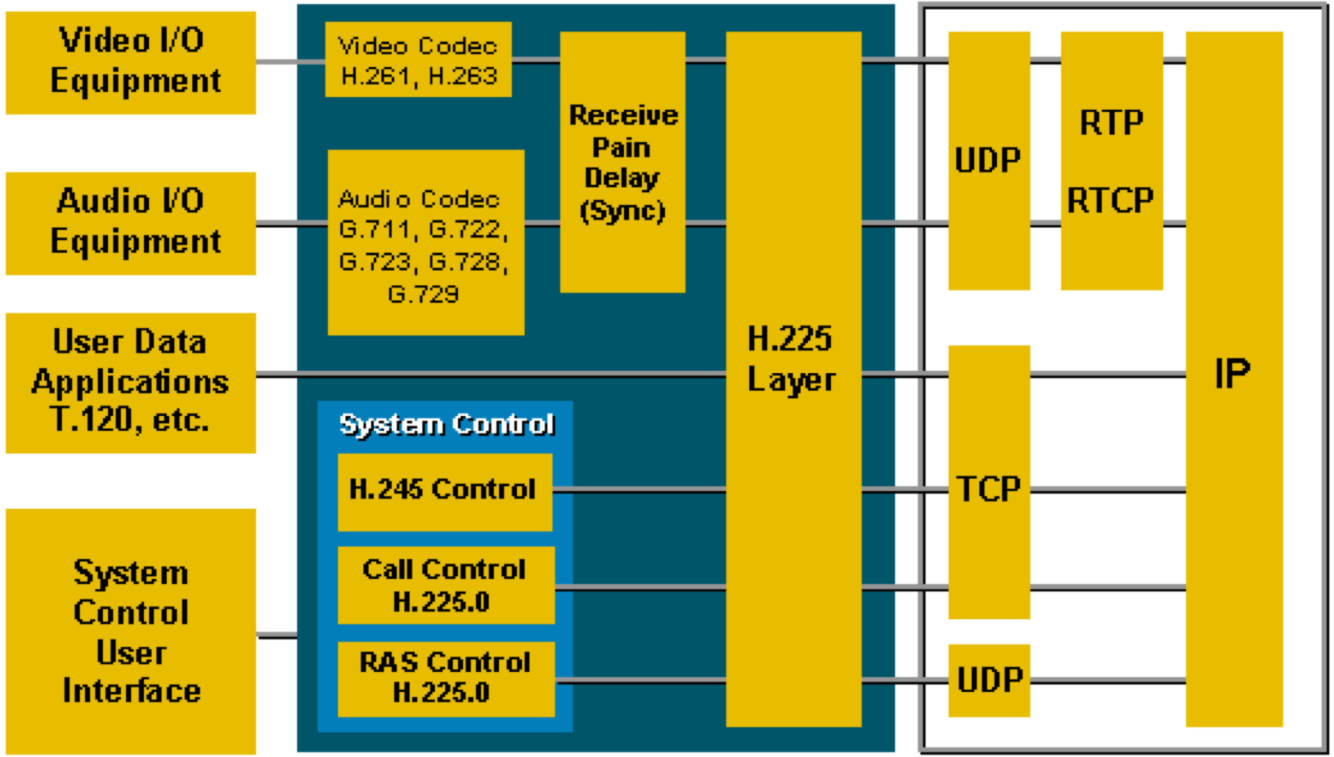
VoIP protocols

- SIP
  - SIP is a signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP).
- H.323
  - H.323 is an ITU Telecommunication Standardization Sector (ITU-T) recommendation that defines protocols to provide audio-visual communication sessions on all packet networks.
  - Widely used in IP based videoconferencing, Voice over Internet Protocol (VoIP) and Internet telephony.

H.323

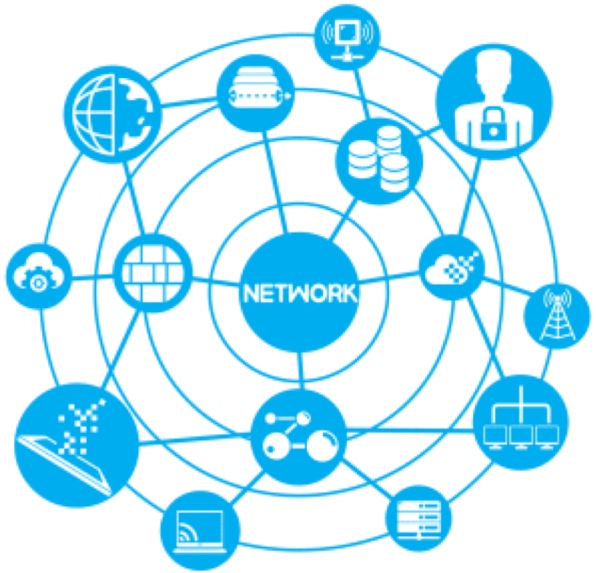
- Focus on multimedia conferencing
- A system specification describing the use of several ITU-T and IETF protocols
- **core** of a H.323 system:
  - H.225.0 Registration, Admission and Status (RAS)
  - H.225.0 Call Signaling
  - H.245 Control protocol for multimedia communication
  - Real-time Transport Protocol (RTP)
  - optional supplementary services supports

Architecture of H.323

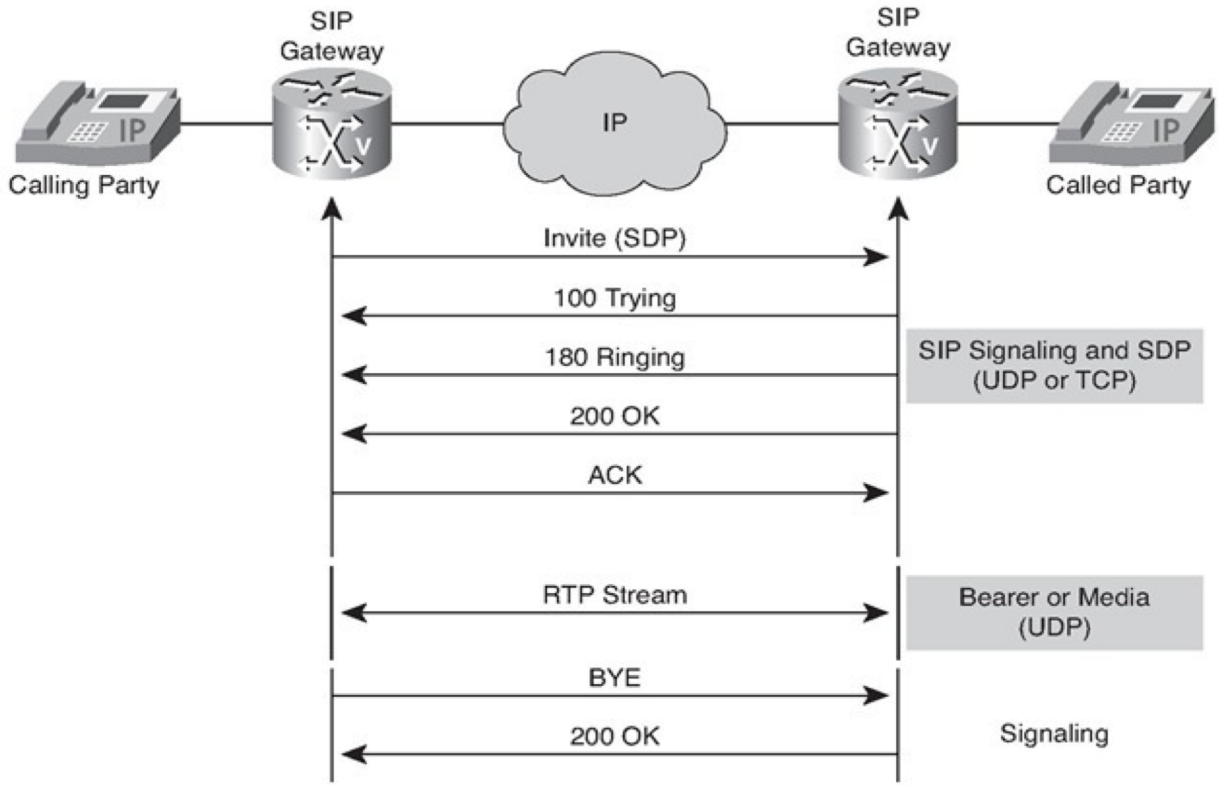


SIP

- Session Initiation Protocol
- widely used in multiple areas:
  - instant messaging
  - file sharing
  - multimedia communicating
  - online gaming
- More complex, hence more vulnerabe
- **Cooperate** with
  - Session Description Protocol (SDP)
  - Real-time Transmission Protocol (RTP)

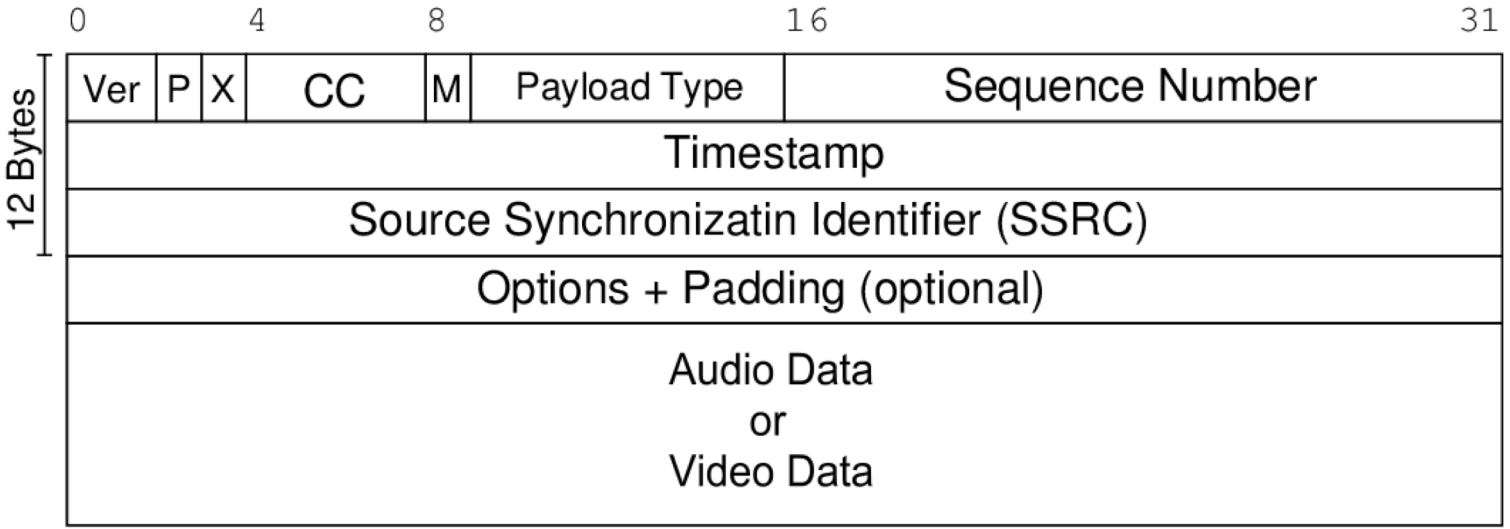


How SIP works



RTP

- Real-Time Transmission Protocol
- Delivers audio and video over IP networks
- runs over User Datagram Protocol (UDP)
- **Cooperate** with RTP Control Protocol (RTCP)



GERNERAL ATTACK TYPE

- Denial-of-service
- Call hijacking
- Resource exhaustion
- Eavesdropping
- Message integrity
- Toll fraud

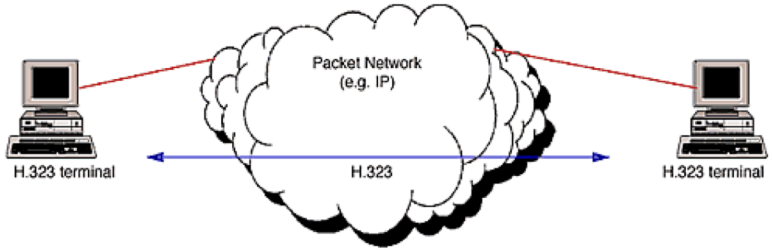
SIP attack

- **SIP message payload tampering:**
  - SIP is a text-based protocol and messages are transported usually in clear text. Attackers can try to **inject harmful content** into a message
- **SIP message flow tampering:**
  - A special case of DoS attacks in real time communication networks are attacks that disturb the ongoing communication between users
- **SIP message flooding:**
  - attacks that overwhelm a victim’s resources

H323 Vulnerabilities

https://www.symantec.com/connect/articles/h323-mediated-voice-over-ip-protocols-vulnerabilities-amp-remediation

- **H.225 (denial of service; execution of code)**
  - These failures result from insufficient bounds checking of H.225 messages as they are parsed and processed by affected systems.
- **H.245**
  - including terminal switching capabilities and information such as opening and closing logical channels



SRTP

- The **Secure Real-time Transport Protocol** (**SRTP**)
- Based on Real-time Transport Protocol (RTP)
- Provide:
  - encryption
  - message authentication and integrity
  - replay attack protection

  on RTP data

Reference

H.323. Retrieved from: https://zh.wikipedia.org/wiki/H.323.

Session Initiation Protocol. Retrieved from: https://en.wikipedia.org/wiki/Session_Initiation_Protocol.

Real-time Transport Protocol. Retrieved from https://en.wikipedia.org/wiki/Real-time_Transport_Protocol

SIP DoS classifications. Retrieved from https://security.stackexchange.com/questions/57040/sip-dos-classifications.

H.323 Mediated Voice over IP: Protocols, Vulnerabilities & Remediation: Symantec Connect. (n.d.). Retrieved from https://www.symantec.com/connect/articles/h323-mediated-voice-over-ip-protocols-vulnerabilities-amp-remediation.

SRTP. Retrieved from https://en.wikipedia.org/wiki/SRTP.

Introduction to VOIP Security - OWASP. (n.d.). Retrieved from https://www.owasp.org/images/b/b6/VOIP_Security_basics.pdf.

Ransome, J. F., & Rittinghouse, J. W. (2005). VoIP Security Best Practices. *Voice over Internet Protocol (VoIP) Security*, 235–302. doi: 10.1016/b978-155558332-3/50011-x


PASSWORD
Thank you