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 compared to traditional phone call
  ○ VoIP offers 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 be 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 vulnerable
- Cooperate with
  - Session Description Protocol (SDP)
  - Real-time Transmission Protocol (RTP)
How SIP works

1. Calling Party sends an INVITE (SDP) message to the SIP Gateway.
2. The SIP Gateway sends a 100 Trying message to the Called Party.
3. The Called Party sends a 180 Ringing message to the SIP Gateway.
4. The SIP Gateway sends a 200 OK message to the Calling Party.
5. The Calling Party sends an ACK message to the SIP Gateway.
6. The SIP Gateway sends an RTP Stream message to the Called Party.
7. The Called Party sends a BYE message to the SIP Gateway.
8. The SIP Gateway sends a 200 OK message to the Calling Party.

SIP Signaling and SDP (UDP or TCP)
Bearer or Media (UDP)
RTP

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


Thank you