Security Strategies in Web Applications and Social Networking

Chapter 14

Securing Personal and Business Communications

Learning Objective

- Identify store-and-forward and real-time communications, and the threats against them.

Key Concepts

- Store-and-forward communications
- Real-time communications
- Best practices for securing telephone or private branch exchange (PBX) communications
- Best practices for securing Voice over IP (VoIP) communications
- Best practices for securing unified communications (UC)

Store-and-Forward Communication

- Electronic mail (e-mail)
- Voice mail
- Social network site messages
- Web site messages
- Fax messages

Real-Time Communication

- Telephone/VoIP
- Instant Messaging (IM)
- Short Message Service (SMS) or Text Messages
- Multimedia Message Service (MMS) Messaging

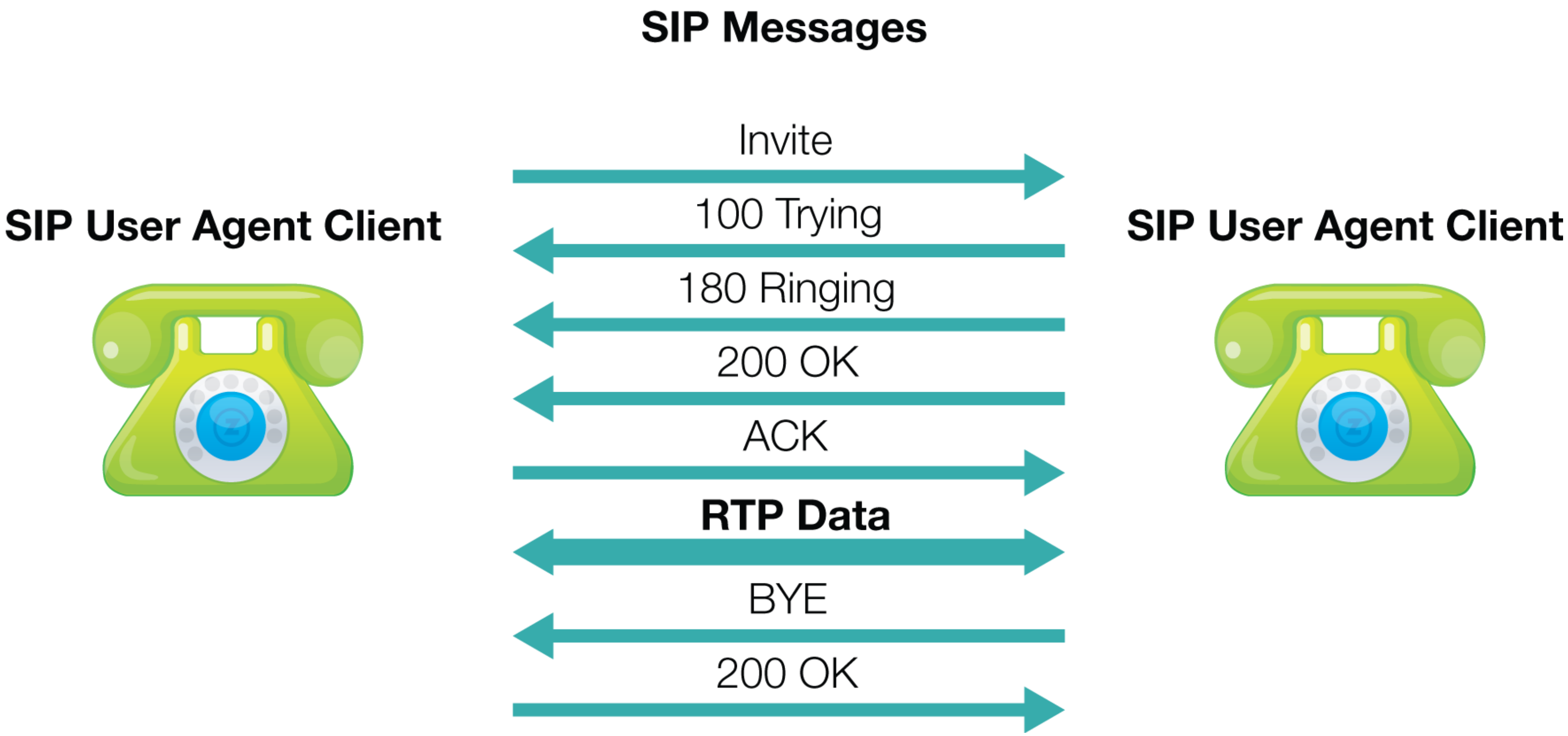
Securing VoIP

- Weigh the network impact
- Train users
- Monitor capacity and usage
- Employ VPNs
- Segregate traffic from data network

Securing VoIP (Continued)

- Protect traffic with VLANs
- Isolate traffic
- Patch programs and use antivirus
- Detect and prevent

SIP Call Between Two Agents



SIP Messages

SIP User Agent Client

SIP User Agent Client

Invite

100 Trying

180 Ringing

200 OK

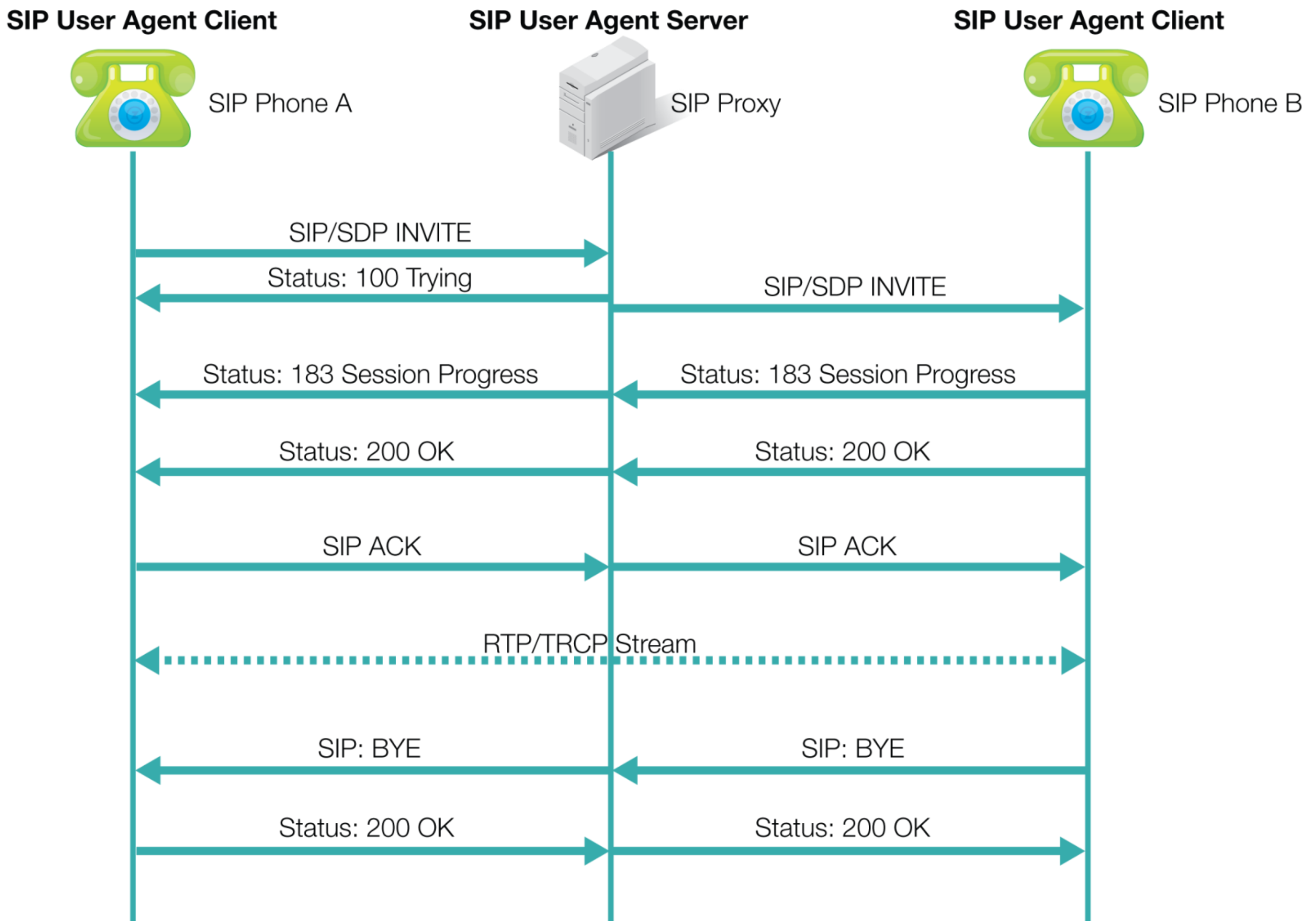
ACK

RTP Data

BYE

200 OK

SIP Call Between Three Agents



Securing SIP/UC

- Patch SIP infrastructure
- Run antivirus on SIP hardware
- Employ application-level gateways in the LAN-to-WAN Domain
- Enforce strong physical security to protect access to areas with SIP infrastructure
- Utilize VLANs to separate SIP traffic network from data network

Securing Telephony/PBX

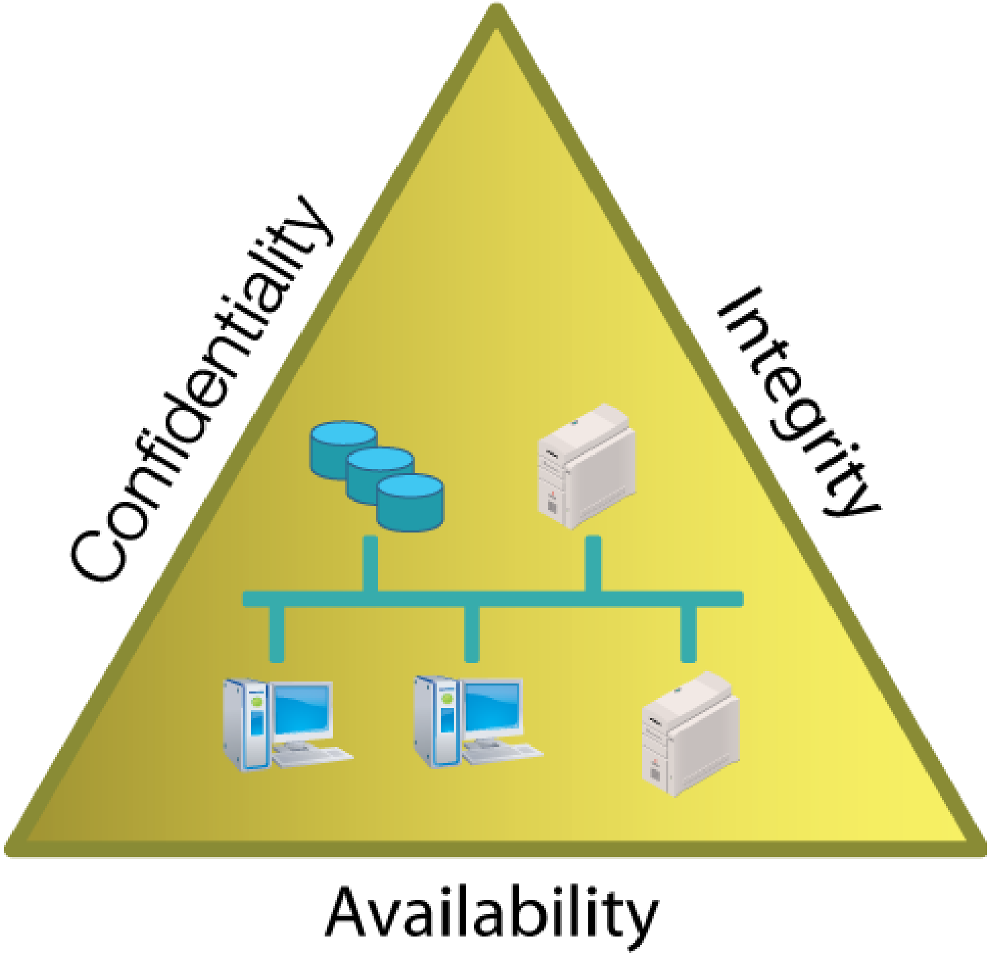
- Physically isolate PBX from unauthorized users
- Disable unused remote management tools
- Use secure protocols or VPN for remote management
- Train systems administrators
- Store PBX documentation in secure area
- Protect again Denial of Service (DoS) attacks

Internet Engineering Task Force (IETF)

- An organized community made possible by the Internet Society (ISOC)
- Develops and promotes Internet standards
- Produces Requests for Comments (RFCs)

IETF strives to keep the quality level of documented standards, policies, and guidelines as high as possible
Achieves goals through peer review and a formalized approval process

Protecting Confidential Data



Protecting Confidential Data (Continued)

- Many organizations do not know at any given moment:
  - Where critical data is stored
  - Who can access the data
  - Who should access the data
- The convergence of technologies only adds to the complexity

Summary

- Store-and-forward communications
- Real-time communications
- Best practices for securing telephone or private branch exchange (PBX) communications
- Best practices for securing Voice over IP (VoIP) communications
- Best practices for securing unified communications (UC)