

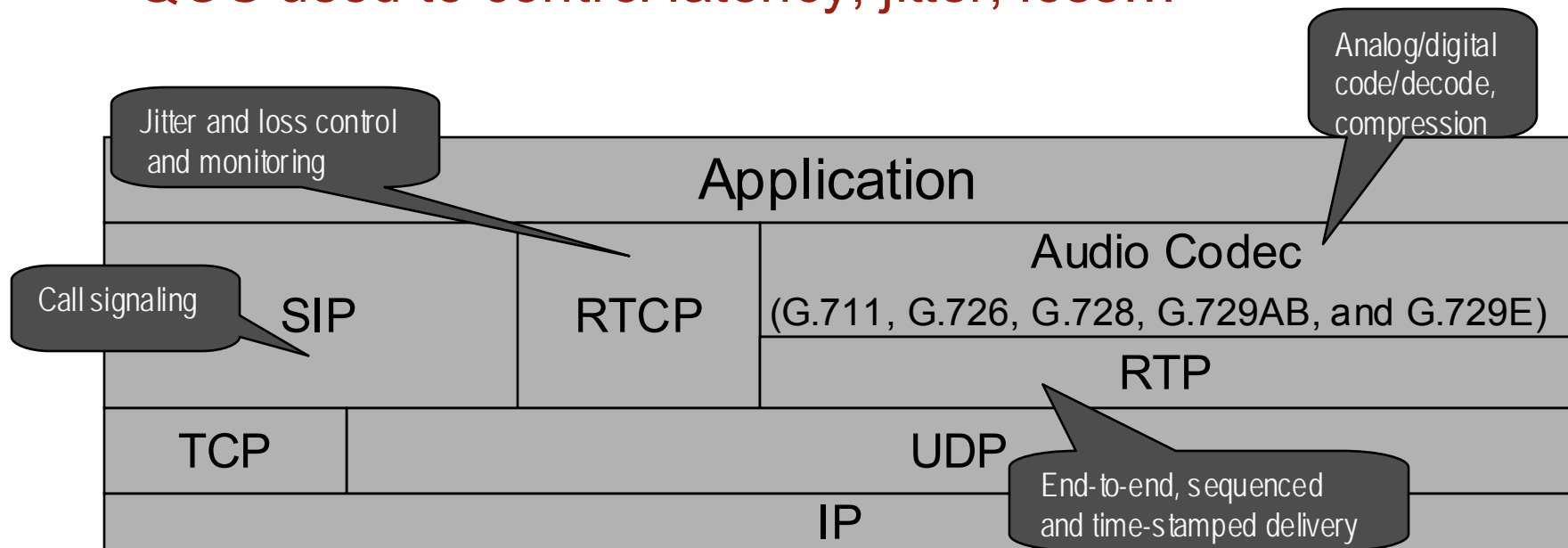
IP Telephony Security Risks

Dave Piscitello
Core Competence

60 Second Primer on IPT

VOIP/IPT

- Place phone, fax, modem calls over IP-based networks
- Analog voice is digitized, compressed sent in tiny ☺ ☺ packets
- QOS used to control latency, jitter, loss...



New targets, old objectives

- Whether POTS or Voice over IP, attackers have common goals:
 - Hurt the carrier
 - Disrupt or degrade service (e.g., deny dial tone)
 - Steal service (e.g., toll fraud)
 - Damage infrastructure (e.g., destroy LUDs)
 - Hurt the subscriber
 - Identity fraud (e.g., use a stolen phone, access card)
 - Steal information (e.g., eavesdrop)
 - Compromise information (e.g., change voice mail)

Hurting the carrier (Examples)

- **IPT control packet floods**
 - H.323 GRQ, RRQ, URQ packets to UDP/1719
- **IPT control packet eavesdropping**
 - Capture unencrypted identities, PINs, phone numbers, ...
- **IPT application data theft/alteration/damage**
 - Use stolen credentials to access directories, voicemail, databases
- **Rogue device & toll fraud**
 - Connect phone to unprotected wall jack, use stolen credentials to place calls or (WORSE) tunnel modem connection over IPT
- **Voice mail hacks**

Hurting the customer (Examples)

- IPT Call data flood (exhaust resources)
- IPT packet injection, modification, replay
 - inject RTP packets into active call containing noise, gaps, speech
- IPT QOS modification
 - Twiddle 802.1q or IP TOS bits to alter engineered QOS
- Call hijacking
 - redirect a call to a different phone (e.g., SIP re-invite), to “social engineer” caller to enter PIN, etc.
- Call eavesdropping
 - Use packet capture tools over shared media

New targets, classic attacks

- Attacking endpoint devices
 - Exploit IPT operating systems on phones, PCs
 - Exploit IPT and Internet protocols
- Attacking IPT infrastructure
 - Exploit IPT servers (gateways, call managers)
 - Exploit media servers (e.g., voicemail)
 - Exploit transmission services
(Ethernet, WAN/Internet access, WLAN,...)

Attacking endpoints

- Packet floods, OS and “stack” DOS exploits
 - “jolt/jolt2” IP fragmentation attacks
 - RTP SSRC collision, forged RTCP BYE, forged CCMS
- IPT implementation exploits
 - Malformed H.323 packets exploit memory leak
- IPT viruses
- Endpoint admin privilege exploits
 - Web-based admin pages: no SSL, weak authentication
- Exploits listening services on IPT endpoints
 - tftp on IPT phone, XP services on PC

Attacking (new) infrastructure

- Attack media (application) servers, call managers, gateways:
 - Packet floods and DOS attacks
 - OS, IPT, application implementation exploits
 - IPT call redirection
 - ARP poisoning, address spoofing
 - Implementation privilege exploits
 - Exploits against listening services
 - telnet, snmp, web, ftp

Summary

From a black hat perspective, IPT is

- A phone service: exploit it as you would POTS and cellular service
- An IP-based service: see if implementations are vulnerable to traditional protocol exploits
- Medium-agnostic: it may be possible to attack underlying services (e.g., WLAN)
- A set of data applications: they run on commercial and new operating systems, and both are exploitable
- A green field for new applications: assume IPT application software is not “secure code”

Now that I've scared you, Jason will comfort you