Carrier VoIP Security

Nicolas FISCHBACH
Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - http://www.securite.org/nico/
COLT and VoIP

- COLT Telecom
  - Voice, Data and Managed Services, Tier 1 ISP in EU
  - 14 countries, 60 cities, 50k business customers
  - 20 000 km of fiber across Europe + DSL
- VoIP “experience”
  - 3 major vendors
    - One “we're coming from the TDM world”
    - One “we're coming from the IP world”
    - One “we're a VoIP company”
- Internet and MPLS VPN-based VoIP services
- Own network (fiber + DSL) and wDSL
- Going PacketCore + NGN + IMS
VoIP Network Architecture

VoIP Core
- Billing
- OSS/BSS
- IP PBX
- SBC
- Softswitch
- MGW

TDM / PSTN
- MGW
- SBC
- IP PBX

IP / MPLS
- H.323/RTP
- H.323/MGCP/RTP

Internet
- SIP/RTP
- H.323/RTP

Carrier
- PBX
- CPE

Softswitch
- MGW
- SBC
- IP PBX

Carrier
- CPE
- PBX

MGW
- MGW
- MGW
- MGW

SBC
- SBC
- SBC
- SBC

IP PBX
- IP PBX
- IP PBX
- IP PBX

Softswitch
- Softswitch
- Softswitch
- Softswitch

Billing
- Billing
- Billing
- Billing

WEB
- WEB
- WEB
- WEB

DB
- DB
- DB
- DB

FW
- FW
- FW
- FW
VoIP Protocols

- **H.323**
  - ITU, ASN.1, CPE/Phone<->Gatekeeper
  - H.225/RAS (1719/UDP) for registration
  - H.225/Q.931 (1720/TCP) for call setup
  - H.245 (>1024/TCP – or over call setup channel) for call management

- **MGCP** (Media Gateway Control Protocol)
  - IETF, Softswitch (CallAgent)<->MGW
  - CallAgents->MGW (2427/UDP)
  - MGW->CallAgents (2727/UDP)
  - Used to control MGWs
  - AoC (Advise Of Charge) towards CPE
VoIP Protocols

- SIP
  - IETF, HTTP-like
- RTP
  - Media stream (one per direction)
  - RTCP: control protocol for RTP
  - SRTP: Secure RTP (w/ MiKEY)
  - Often 16000+/UDP or default NAT range, but can be any UDP>1024
  - Can be UA<->UA (risk of fraud) or UA<->MGW<->UA
Session Border Controller

- What the role of an SBC?
  - Security
  - Hosted NAT traversal (correct signalling / IP header)
  - Signalling conversion
  - Media Conversion
  - Stateful RTP based on signalling

- Can be located at different interfaces:
  Customer/Provider, inside customer LAN,
  Provider/Provider (VoIP peering)

- What can be done on a FW with ALGs?
- What can be done on the end-system?
- Is there a need for a VoIP NIDS (especially with SIP-TLS)
VoIP Hardware

- Mix of software and hardware (mostly DSPs)
  - Softswitch: usually only signalling
  - MGW (Media Gateway): RTP<->TDM, SS7oIP<->SS7
  - IP-PBX: Softswitch+MGW

- Operating systems
  - Real-time OSes (QNX/Neutrino, VxWorks, RTLinux)
  - Windows
  - Linux, Solaris

- Poor OS hardening

- Patch management:
  - OSes not up-to-date
  - Not “allowed” to patch them
Security challenges

- VoIP protocols
  - No, VoIP isn't just SIP
  - SIP is a driver for IMS services and cheap CPEs
  - H.323 and MGCP rock the carrier world

- Security issues
  - VoIP dialects
  - Only a couple of OEM VoIP stacks (think x-vendor vulnerabilities)
  - FWs / SBCs: do they solve issues or introduce complexity?
  - Are we creating backdoors into customer networks?
  - CPS and QoS
VoIP dialects: result

- No way to firewall / ACL (especially if non-stateful) based on protocol inspection
- Vendors who never heard of timeouts and don't send keep-alives

Result:
- Clueful: Permit UDP <port range> <identified systems>
- Half clueful: Permit UDP <port>1024> any
- Clueless: Permit UDP any any

End-result:
- 0wn3d via exposed UDP services on COTS systems
- Who needs RPC services (>1024/UDP)?
(Not so) Lawful Intercept

- Lawful Intercept
  - Re-use existing solutions: TDM break-out
  - Install a sniffer (signalling+media stream)
  - Re-route calls (but hide it in the signalling)

- Eavesdropping
  - Not a real threat (own network)
  - Entreprise network: Needs to be a part of a global security strategy
    - Clear text e-mail
    - Clear text protocols (HTTP, Telnet, etc)
    - Clear text VoIP
    - Etc
  - vomit, YLTI, VOIPONG, scapy (VoIPoWLAN): easy way to show how insecure it is
Phones

- Crashing IP Phones
  - This is no news :)  
  - Quite easy (weak TCP/IP stacks and buggy software implementation)  
  - Mostly an insider threat  
    - DHCP server  
    - TFTP server (phone configuration)  
    - Credentials (login + PIN)  
  - VoIP doesn't mean that you need to move to IP Phones  
    - PBX with E1 (PRI/BRI) to router and then VoIP  
    - PBX with IP interface towards the outside world (but do you really want to put your PBX on the Internet)?  
    - Means that you have to maintain two separate networks, but “solves” the QoS issues on a LAN  
    - What about soft clients?
Phones: Try this at home :) 

- Lots of IP phones with PoE
- CDP exchange: VLAN mapping + PoE information
- What if you write a worm that tells the switch to send you 48V to your non-PoE Ethernet NIC on your PC?
Denial of Service Threat

- Generic DDoS
  - Not a real issue, you can't talk to our VoIP Core
    - ACLs are complex to maintain use edge-only BGP blackholing
  - We are used to deal with large DDoS attacks :)"
Security Challenges

- Online services
  - Call Management (operator console)
  - IN routing
  - Reporting / CDRs

- Security issues
  - Multi-tenant capabilities
  - Have the vendors ever heard of web application security?
  - Who needs security or lawful intercept if a kid can route your voice traffic via SQL injection
  - WebApp FWs are really required...
Security Challenges

- TDM / VoIP: two worlds, two realms, becoming one?
  - Security by “obscurity” / complexity vs the IP world
  - Fraud detection

- Security issues
  - New attack surface for legacy TDM/PSTN networks
  - No security features in old Class5 equipment
  - No forensics capabilities, no mapping to physical line
  -Spoofing and forging

Abusing NMS/Operations

- VoIP is damn complex
- Only way to debug most of the issues: VoiceEng + IP/DataEng + SecurityEng on a bridge/online chat
- Requirement: be able to sniff all traffic
- Tool: Ethereal(-like)
- Attacker: Just use any of the protocol decoder flaw in the sniffer
- Make sure your sniffers are on R/O SPAN ports, in a DMZ which only allows in-bound VNC/SSH
- If the guy is really good and can upload a rootkit over RTP: let him take care of the system, he's probably better than your average sysadmin ;-))
Carrier/Carrier VoIP Security

- Aka “VoIP peering” / Carrier interconnect
- Already in place (TDM connectivity for VoIP carriers/Skype{In, Out})
- Connectivity: over the Internet, IX (public/private), MPLS VPN or VPLS (Ethernet)
- No end-to-end MPLS VPN, break the VPN and use an IP-IP interface
- Hide your infrastructure (topology hiding), use {white, black}listing and make sure only the other carrier can talk to you
- Signalling/Media conversion (SBC)
Encryption / Authentication

- Do we want to introduce it?
  - Vendor X: “We are compliant”. Sure.
  - Vendor Y: “It's on our roadmap”. Q1Y31337 ?
  - Vendor Z: “Why do you need this?”. Hmmm...

- IPsec from CPE to VoIP core
  - Doable (recent HW with CPU or crypto card)
  - What about CPE<->CPE RTP ?
  - Still within RTT / echo-cancellation window

- May actually do mobile device<-> IPsec -> VoIP core
  - Bad guys can only attack the VPN concentrators
  - Not impact on directly connected customers
Future: IMS services

- IMS = IP Multimedia Subsystem
- Remember when the mobile operators built their WAP and 3G networks?
- Mostly “open” (aka terminal is trusted)
- Even connected with their “internal”/IT network
- IMS services with MVNOs, 3G/4G: overly complex architecture with tons of interfaces
- Firewalling: complex if not impossible
Carrier VoIP Security

- Conclusion
- Q&A