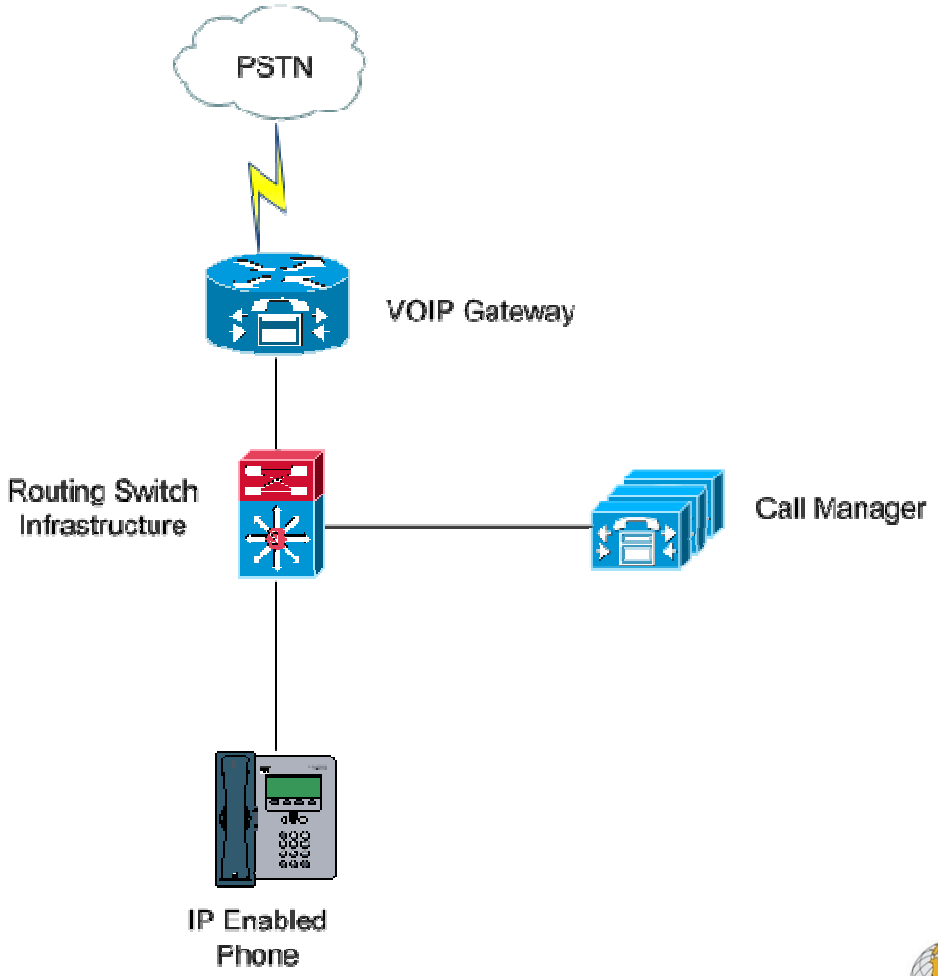
Ron Shuck, CISSP, CISM, CISA, GCIA
Infrastructure Security Architect
Spirit AeroSystems

Voice Over IP Security

Overview

- VOIP Components
- Common Threats
- How Threats are Used
- Future Trends

VOIP Components



Routing and Switching Infrastructure

- Provides basic network connectivity and transport
- Infrastructure services (DHCP, DNS, etc.) provide critical services for the VOIP systems
- Delay, bandwidth, and packet delivery are dictated by these systems
  - Quality of Service (QoS)
  - Service Level Agreements (SLA)
- Provides compartmentalization of information systems

VOIP Gateway

- Provides conversion of calls between the data network and the Public Switched Telephone Network (PTSN)
- Primarily uses trunks for PSTN connectivity
- Can be used to relay call signaling to Internet VOIP providers
- Can provide VOIP termination from systems on the Internet

Call Manager

- Performs the functions of a traditional PBX and is the core of the VOIP system
  - Maps internal extensions
  - Routes calls to VOIP gateways, internal extensions, or external numbers
  - Tracks call utilization
  - Controls call flow on the network
- Cisco Call Manager uses Skinny Client Control Protocol (SCCP) for signaling between the Call Manager and phones
- The Call Manager is an application sitting on a traditional Microsoft Windows or Linux platform

VOIP Enabled Phone

- The VOIP phone provides the user the entry point into the phone system
- Uses various access medias
  - Wired
  - Wireless
  - Softphone
- Encodes voice communications using a codec for encoding and compression
- Contacts the Call Manager for configuration and management
  - Initial configuration via TFTP
  - Reliant on the Call Manager for functionality

Common Threats

- Denial of Service (DoS)
- Eavesdropping
- Interception/Modification

Denial of Service

- DoS attacks are common
  - Unintentional DoS (most common)
  - General Worm/Malware
  - Intentional Insider
  - Intentional Outside
- Signs of a DoS Attack
  - Poor network performance beyond VOIP
  - Inability to make calls
  - Phone service suddenly stops
  - Massive traffic flows
  - IPS/IDS alerts

DoS RSI - Flooding

- Flooding
  - Traditional attacks such as SYN Flooding, Malformed packets, etc
  - Distributed Denial of Service Attack using 'Botnet' to attack public facing services
  - Weaknesses in the network infrastructure equipments underlying operating system or configuration
  - Mis-configured systems that communicate on the network
- Goal is to make voice quality so low it is unusable
- Defenses
  - Network segmentation
  - Implementing QoS
  - Hardening infrastructure to NSA or CIS standards
  - Keeping network Infrastructure patched
  - Proactive network monitoring and management

DoS RSI - QoS Manipulation

- QoS provides network based traffic prioritization used to give VoIP precedence
- Attackers can abuse this functionality to give bogus attack traffic priority
  - Manipulating Differentiated Services Control Point (DSCP) bits
  - Producing bogus RTP, SCCP, SIP, or other traffic that may be protected by VOIP systems
- Goal to render QoS ineffective and lessen the resources needed for the attack
- Defenses
  - Network segmentation
  - QoS trust mechanisms
  - Proactive network monitoring and management

DoS RSI - Infrastructure Attacks

- Attacks against network services used in VOIP
  - DHCP Exhaustion – Requesting DHCP addresses until none remain
  - Attacks Against DNS – DNS poisoning, UDP flooding, or other attacks
  - Compromise network infrastructure
    - Device Access
    - Exploit routing protocols
    - Implement Access Control Lists
- Goal is to render the network infrastructure unable to support VOIP applications
- Defenses
  - Use DCHP Snooping (Cisco)
  - Harden DNS Servers
  - Harden network infrastructure according to NSA or CIS guidelines
  - Use secure routing protocols and practices

DoS VOIP Gateway

- Vulnerable to many of the same attacks as the routing and switching infrastructure
- Additional vulnerabilities
  - Flooding SIP requests to user resources or tie up PSTN trunks
  - Flooding SIP requests to tie up resources
- Goal is to make the PSTN inaccessible to the voice network
- Defenses
  - Network segmentation
  - Infrastructure hardening
  - Proactive monitoring and management

DoS - Call Manager

- Vulnerable to network, OS, and application level DoS attacks
- DoS vulnerabilities include
  - Flooding attacks discussed for infrastructure
  - Single packet attacks
  - Weaknesses in the Call Manager software or OS
  - Flooding registration requests
- Goal is to render the Call Manager unable to service calls
- Defenses
  - Patch management for Call Manager servers
  - Network Segmentation
  - Network Intrusion Prevention System (NIPS)
  - Host-Based Intrusion Prevention (HIPS)

DoS - VOIP Enabled Phones

- VOIP phones are vulnerable to many of the same attacks as the RSI & CM
- Unique vulnerabilities
  - Registration attacks
  - DHCP exhaustion
  - Phone configuration weaknesses
- Goal is to render the phone inoperable
- Defenses
  - Network segmentation
  - Strong phone authentication
  - Harden network infrastructure

Eavesdropping

- VOIP networks are inherently easier to eavesdrop on than traditional phone systems
  - Traditional techniques used to sniff networks can be used to intercept conversations
  - Attacks can be executed in a switched environment to intercept conversations
  - Trivial for insiders in an IT group to intercept conversations
- Numerous threats exist from eavesdropping
  - Espionage
  - Extortion/Blackmail
  - Unauthorized information disclosure
  - Wiretapping and unauthorized employee monitoring

Eavesdropping RSI by IT

- IT network administrators have easy access to tap traffic undetected
  - Using managed switch functionality (SPAN, RSPAN)
  - Insert sniffer on device in the normal traffic flow
- Tools such as Wireshark, Cain & Able, and various other sniffing tools exist that reassemble traffic flow
- Goal to monitor network conversations as they traverse the network
- Defenses
  - Background checks on potential IT staff
  - Traditional counter intelligence methods
  - Encrypting VOIP communications
  - If eavesdropping is suspected by IT, communicate items out of band
  - Perform regular 3rd party audits of IT

Eavesdropping RSI by Outside Attacker

- An outside attacker must first gain access to the network to intercept traffic
  - Unsecured wireless access points
  - Remote Access (VPN, SSL, Dial-up)
  - Compromised system
  - Physical access to the facility
  - Malicious software
- Interesting traffic is intercepted
  - Segment sniffing
  - SPAN ports
  - ARP cache poisoning, ARP flooding, & DNS poisoning can be used to sniff in a switched network

Eavesdropping RSI by Outside Attacker (Cont)

- Goal is to covertly gather VOIP traffic for analysis
  - Private information/Espionage
  - Helpdesk password changes
  - Call/number harvesting
  - Decode Dual Tone Multi-Frequency (DTMF) tones
    - Credit card, Social security numbers, Voicemail password
- Defenses
  - Network segmentation
  - Encryption of VOIP traffic
  - Using network infrastructure features such as DHCP snooping, ARP protection, MAC limits, and other protection mechanisms
  - Harden infrastructure according to NSA or CIS guidelines
  - Defense-in-depth security program

Eavesdropping Call Manager

- An attacker must have access to the network & the Call Manager
  - Using an exploit
  - Username or password guess
- Methods to Eavesdrop
  - Redirect calls through bogus VOIP proxy
  - Review Call Manager logs to view source and destination of calls
  - View other call log information
- Goal is to gather basic usage patterns and manipulate phone behavior
- Defenses
  - Patch management of the Call Manager
  - Host & Network based IPS
  - Network segmentation

Eavesdropping VOIP Gateway

- Eavesdropping from the inside network facing interface is a key target
- If the VOIP gateway terminates call from the Internet, those calls can be easily intercepted
- Goal is to intercept call from the primary network exit point to the PTSN
- Defenses
  - Identical to RSI
  - Additionally if calls are allowed from the Internet, VPN should be used to secure communications

Eavesdropping VOIP Enabled Phone

- The configuration of the phone is sent via TFTP which transmits configuration information in clear text
  - Identify Call Manager
  - Identify phone extension
  - Gather detailed configuration information
- Phone configuration information can be used to retrieve dialing information
- Goal is to gather phone configuration information and view calling behavior
- Defenses
  - Use Transport Layer Security (TLS) or other cryptography for phone to call manager connectivity
  - Network segmentation

Interception/Modification RSI

- Interception of VOIP traffic can be used to launch a Man-In-The-Middle (MITM) attack
  - Attacker relays traffic between victim and itself
  - Repackages traffic and forwards it to the destination
- This can be used to manipulate voice traffic
  - Replay, insert, or omit voice conversations
  - Redirect calls to a different destination
  - Directing traffic to a non-existent destination
- Goal is to manipulate traffic without the users knowledge
- Defenses
  - Use Transport Layer Security (TLS) or other cryptography for phone to call manager connectivity
  - Harden network infrastructure to NSA or CIS standards
  - Use switch features such as ARP inspection, DHCP spoofing, and MAC address control

Interception/Modification
VOIP Gateway

- If an attacker can control the VOIP gateway they can;
  - Redirect calls going to the PSTN to alternate numbers
  - Redirect or monitor inbound calls
  - Manipulate Caller ID information
  - Bypass Call Manager defined dialing rules
- If the gateway is accessible from the Internet, mis-configured access rules can allow attackers to route calls through the PSTN
- Goal is to control the flow of voice traffic to and from the PSTN
- Defenses
  - Harden VOIP gateways
  - Monitor gateways for abuse
  - Network segmentation
  - Don't allow connections from the Internet without VPN

Interception/Modification
Call Manager

- The Call Manager is the nerve center for the VOIP network and the most valuable target for an attacker
  - Provides phone management
  - Provides call routing
  - Provides call rules
  - Provides call accounting
- Unique Security Issues
  - The Call Manager is dependent on the host OS security & its subcomponents
  - Some VOIP vendors do not release critical patches at the same time as the operating system vendor
  - Limits to the system hardening that can be performed
- Control of the Call Manager can be gained through exploiting the operating system, applications, or configuration
  - Software vulnerabilities
  - Weak configurations

Interception/Modification
Call Manager (Cont)

- The Call Manager can be manipulated to
  - Direct calls both inside and outside of the network
  - Control phone configuration
  - Bypass call rules
  - Manipulate call accounting
  - Change security parameters
- Goal is to have control of the VOIP system
- Defenses
  - Patch management
  - Host & Network Based Intrusion Prevention
  - Network Segmentation
  - Proactive network monitoring and management

How These Threats Are Used

- Fraud
- Theft of Service
- Espionage
- Sabotage
- Extortion

Fraud

- Manipulation of phone system for verifications to provide bogus authorization or reversed to get consumer information
  - Credit card approval
  - Wire transfer approval
  - Vendor fraud
- Manipulation of Caller ID
  - Support traditional fraud (boiler rooms)
  - Securities fraud
- Manipulate outbound calling
  - Direct calls to 900 numbers
- Gather consumer information though eavesdropping

Theft of Service

- Open VOIP gateways with ports open to the Internet
  - Hackers locate through scanning
  - Direct calls through your gateway and PSTN
- Create extensions that are not logged in the accounting system
  - Obscure source of call
  - Employee long distance abuse
  - Facilitating insider trading
- Insider resell of long distance using remote access

Espionage

- Wiretapping with the purpose of intercepting calls to provide a competitive advantage for an outside organization
  - Tapping VIP phones
  - Getting access to VIP voicemail
  - Tapping helpdesk or IT lines for further system access
- Providing unauthorized access to conference call bridges through Call Manager manipulation
- Using call history to profile the organization
- Masking extensions to facilitate social engineering

Sabotage

- Using DoS attacks to drop phones at critical times
  - Launch DoS during disaster against first responders
  - DoS attack for phone intensive organizations
  - Drop phones in commodities trading
- Disgruntled employees
  - Manipulate QoS settings to provide poor call quality
  - Create scripts to randomly assign extensions
  - Redirect inbound or outbound calls
- Malware based DoS from general malice

Extortion/Blackmail

- Use of information gathered from eavesdropping
  - Phone records
  - Conversations
  - Voicemail
- Threats of DoS attack if a ransom is not paid
  - Major threat for commodities trading organizations
  - Call centers can lose millions during down time
- Use by disgruntled IT staff with access to these systems
- System can be used to make ransom requests that are difficult to trace

Future Threats

- SPAM Over Internet Telephony
- Integrating VOIP into Traditional Crime
- Physical/Electronic Attacks

SPAM Over Internet Telephony

- The expansion of VOIP will lead to gateway to gateway calling over the Internet
  - Reduces long distance cost to the cost of bandwidth
  - Long distance calling will be the same price as an email
- SPAM over Internet Telephony will explode as email SPAM has with email
  - High volume of telemarketing calls
  - Filtering mechanisms will have to be implemented

Integrating VOIP into Traditional Crime

- Mobility of VOIP technology can allow highly mobile call centers
  - Use of compromised networks for boiler room operations
  - Rapid setup/tear down with Internet access being the only requirement
- Use of VPN and VOIP by organized crime for secure communications
  - Use of compromised networks for high profile activities
  - Compromise of VOIP networks and resell of phone service for illicit use
  - Use of system 'hopping' to thwart law enforcement

Physical/Electronic Hybrid Attack

- Combing physical and electronic attacks to facilitate high profile crime
- For example we'll consider a robbery
  - Five minutes before robbery a DoS attack is launched against the Video over IP camera system
  - All calls to 911 or security are directed to a confederate in a van outside with an IP phone that is configured as an extension on the company's phone system connected via wireless access points
  - Inbound calls to security are directed to the confederate as well
  - All calls from security are configured to call a phantom extension

Conclusion

- VOIP Technology can provide many positive benefits for organizations, but the risks must be evaluated
- Before implementing VOIP
  - Perform a risk assessment
  - Design security into your deployment plan
  - Use defense-in-depth
  - Develop a strategy for monitoring and management

ISSA™ Information Systems Security Association CENTRAL PLAINS CHAPTER