Guidelines for Securing Your VoIP PBX

Unregistered436 / Patrick McNeil – July 2015

DEF CON 23

Installment TWO of the PBX mysterys series!!

Information Leakage Prevention (Confidentiality)

- Block scanners with firewall rules or a VoIP security appliance that matches on signatures of known scanners and/or credential cracking behaviors (See our iptables rules).
- Change the User-Agent value to something generic or even to that of an alternate type of system to trick attackers into the wrong approach. Ex: “Asterisk” becomes “Avaya CM”.
- Set or change the default SIP realm.
- If possible, use a different set of audio prompts than the system default.
- Take a packet capture and look for identifying fields (and investigate how to change them).
- Consider a Session Border Controller (SBC) to anchor sessions, perform NAT, and filter out identifying fields with header manipulation rules (topology hiding).

DoS (Availability)

- Use DoS mitigation devices to block volumetric attacks and challenge setup of new TCP and UDP sessions.
- Consider combining on premises detection and cleaning with a cloud scrubbing capability.
- Use a security appliance that can enforce SIP message format and session state to prevent out of state floods as well as oddly formatted messages that crash the system.
- Apply rate limiting on edge routers.
- Apply BCP 38 / RFC2827 to ban private IP ranges as public source IPs (sometimes used in attacks).
- Use iptables and fail2ban to apply rate limiting on the host in case edge protections are not sufficient
- Consider high-availability or multi-site deployment for critical systems.

Management & Services Assurance (Integrity)

- Follow vendor specific hardening guides like **THIS**
- Don’t put PBX admin interfaces on the Internet. Block access to management IP address ranges and/or protocols on the edge router or firewall.
- Require VPN access for management functions.
- SIP usernames should never match extensions.
- Use long passwords, and change ALL of them!
- Use a secure encrypted management protocol for everything (no telnet/FTP), and audit the encryption algorithms configured for use (HTTPS, SSH, etc). Note that “None” is a valid HTTPS algorithm, meaning NO encryption is performed!
- Don’t assume that the vendor’s out of band management ports are safe because they are out of band. An attacker can “pivot” from a compromised internal network to a management network.
- Don’t use a monolithic PBX distribution OR be diligent about auditing what software you really need to be running. Shut down unnecessary services. Ex: Do you NEED AMI?
- PATCH! Sign up for vendor security notifications.
- Where feasible, use TLS to protect VoIP signaling, and SRTP to protect media. Do not re-use existing vendor certificates, and always issue your own or buy a public certificate.
- For TLS, employ mutual authentication so client and server need to validate each other. This prevents “man in the middle” attacks and encryption downgrades. Client certificates can be time consuming to administer, but even a single organizational cert will greatly increase security.

Detection & Prevention of Fraud & Abuse

- Don’t use three digit extensions, which are the default for SIPVicious. If using something longer, don’t start with “1000”.
- Ask your telecom provider what fraud protections they offer. If asked, many have default settings or paid services to block certain types of calls, cap spending, or eliminate calls to high-cost destinations.
- Limit (or eliminate) use of call forwarding, voicemail callback, and dialing out from voicemail.
- Block international dialing when possible, and require a pin code for accessing international trunks. Remember that there are international destinations that are in the North American Numbering Plan. See **NANPA** for the complete list.
- Delete or administratively disable unused extensions. Once cracked, unused extensions can be abused longer than active ones.
- Audit user passwords by trying to crack them.
- Enforce application (SIP) message rates and number of active sessions using thresholds and blacklisting.
- Watch real-time signaling for fraud patterns, using a fraud detection system that is either in-line or in monitor / tap mode if possible, and NOT ON the PBX. Call Detail Records can be modified if a system is sufficiently compromised.
- Security or fraud management systems should be capable of learning normal traffic baselines and watching for changes in ratio, frequency, or direction.