Asterisk and Security

Kevin P. Fleming
Director of Software Technologies
Digium, Inc.
kpfleming@digium.com

Basics

- Understand the tools and platform you are deploying!
- Try to avoid off-the-shelf 'complete' operating system distributions
- If you must use one, do a thorough audit of all services and processes that are installed; disable the ones that are not required for the VoIP deployment
- Learn the available tools for monitoring your network's usage and performance
- Don't install Asterisk on a system shared with normal users :-)

Security Challenges

- Denial of Service (DoS)
- Interception (wiretapping)
- Theft of Resources
- Identity Management

Denial of Service

- Simple: firewalls, intrusion detection
- Complex: excessive call length, routing calls through unnecessary hops
- Security vulnerabilities
- These issues apply to endpoints as well, not just VoIP servers; various SIP phones are susceptible to crashes or other unexpected behavior through simple exploits

Interception (LAN)

- When possible, segregate voice traffic onto a separate VLAN
- Use intelligent network switches that can prohibit ports from joining VLANs they are not allowed to use; using 802.1x for maximum control of devices, not just ports
- Use port-based MAC address filtering to isolate endpoint traffic to the voice VLAN, thereby eliminating the chance for MAC address spoofing to intercept traffic
- Learn how to use traffic interception tools on purpose; you will need them for voice quality monitoring and debugging of service problems

Interception (WAN/Internet)

- When traffic must pass over a public network link, use some form of encryption
- OpenVPN is a simple-to-deploy and reliable choice for creating encrypted point-to-point or point-to-multipoint links
- IPSEC is somewhat harder to deploy but is standards-based and available on a large number of platforms
- Asterisk's IAX2 protocol can provide AES encryption between Asterisk servers with no need for an encrypted tunnel

Theft of Resources

- Users will do unusual,crazy, innovative things to try convince your communication system to do things you never intended!
- Simple example: softphones on client systems can frequently be used by other applications on that system for bulk call generation
- Complex example: users can call-forward calls through multiple extensions on the system, and to outside destinations, causing increased channel usage without obvious impacts (until you run out of channels!)
- Be extremely diligent when building your dialplan, especially if you allow Direct Inward System Access

Identity Management

- Never, ever, ever allow caller identity (CLID and CNAM) information provided by an endpoint to be used as 'trusted' information by your VoIP network
- When possible, use SSL certificates for endpoint authentication to the VoIP network; if not possible, ensure that passwords are highly random, long and composed of alphabetic, numeric and punctuation characters
- Don't use a simple, predictable authentication naming scheme for endpoints on the network; doing so allows attackers to easily guess the name for another user's endpoint
- If you deploy softphones, learn how to centrally provision them and then lock them down

Thank You!