VOIP Security Essentials

Jeff Waldron

Traditional PSTN

- PSTN (Public Switched Telephone Network) has been maintained as a closed network, where access is limited to carriers and service providers.
- Entry to the PSTN has traditionally been a protected by price, as the annual costs exceed $100,000 (USD).
- These two characteristics of the PSTN (closed network and very high cost of access) have established the false perception that the PSTN is a secure network.
- This claim is quickly discredited once someone starts to analyze the security controls, or lack of, that are available in the PSTN.

PSTN “Trust”

- The PSTN is comprised of thousands of interconnected network elements over dedicated circuit switched facilities that use the SS7 (Common Channel Signaling System No.7, SS7 or C7) which relies upon a model of trusted neighbors.

Voice Over Internet Protocol (VOIP)

- Voice over IP – the transmission of voice over packet-switched IP networks – is one of the most important emerging trends in telecommunications.
- VOIP introduces both security risks and opportunities.
- VOIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues.
- Lower cost and greater flexibility are among the promises of VOIP for the enterprise

VOIP Advantages

- Cost Savings (toll charges, PBX vendor costs, moves-adds-changes)
  - A study by The Yankee Group noted VOIP systems were 22% less expensive to operate than circuit-switched networks.
  - Most saving is found within new site facilities only needing one copper infrastructure.
- Almost all organization have existing IP infrastructure.
- VOIP can run over wired or wireless infrastructure
- Mobility (routing phone numbers to dynamic IP address)

VOIP Disadvantages

- Initial start-up cost.
  - Phone
  - VOIP equipment (call center, gateway)
- Additional training for IT staff to support.
- Power outage.
  - All components supporting VOIP system need UPS protection
- Voice Quality and QOS Requirements

  Network and Codecs affect voice quality
  - Latency (acceptable delay < 150 ms)
  - Jitter (variations in delay)
  - Packet loss
- New security requirements to deal with:
  - Denial of Service, Eavesdropping, Misuse/fraud, Impersonation
  - Softphones

VOIP Security Basics

- Secure the VOIP gateways (or call centers)
  - Ensure anti-virus is installed and updated/current.
  - Configure the devices securely
  - Apply patches
- Apply security settings/configurations at boundaries and devices
- Ensure VOIP Gateway is behind enterprise firewall
- Segment voice and data traffic on separate VLANS
- UPS is key to availability

VOIP Architecture

- PBX Replacement
  - Vendors are no longer offering the traditional PSTN on the new offerings of PBX devices. Organizations will be forced to migrate to VOIP.
- Media Servers and Gateways
  - Connect calls within VOIP system
  - Connect calls between PSTN and VOIP
- End Nodes
  - VOIP capable phones (wired or wireless)
  - Softphones
  - IM Clients
  - Video Clients

VOIP Protocols

- Current VOIP systems use either a proprietary protocol, or one of two standards, H.323 and the Session Initiation Protocol (SIP).
- Although SIP seems to be gaining in popularity, neither of these protocols has become dominant in the market yet, so it often makes sense to incorporate components that can support both.

Skype

- With over 29 Million Skype users online at one time as of June 2006, Skype is a technology to be dealt with
  - A peer-to-peer VOIP client
  - Secured using 256 bit AES encryption
  - PGP authentication

VOIP in the News

- VoIP theft nets $1M, two arrests
  Published: 2006-06-09
  (http://www.securityfocus.com/brief/225)
  - At least 15 Internet phone companies were hacked --one of which suffered as much as $300,000 in loses as a result of the attacks. The group sold more than ten million minutes of telephone time for as little as 0.4 cents per minute

VoFi [Voice-over-WiFi]

- While it's still very early for voice-over-802.11 handsets, users and vendors alike will have to think hard about security issues -- particularly since vendors are scheduled to bring a wave of new dual-mode handsets to market, creating the potential for many more of these devices entering the workplace, often without the IT department knowing about it.

VOIP Security Issues

- There are Four main issues of VoIP security.
  - *Authentication:* Is the party who answered the call the intended destination?
  - *Nonrepudiation:* Once a destination accepts a call, is there anything in place that prohibits it from denying receipt of the connection?
  - *Privacy:* Is the call content secure?
  - *Availability:* Users expect to hear a dial tone when they pick up the phone.

VOIP Ready for Primetime?

- May not be ready for external Enterprise use – depending on industry/staff knowledge.
- Could be used to connect branch offices/agents to a corporate headquarters.
- Requires a different mindset to implement within a business structure.
- Works well in the home environment.

Summary

- Standards are maturing and there are so many of them to choose from
- OK for home use. Will reduce or eliminate long-distance bills
- Good option for use by mobile users depending on the nature of the calls. Cell phone might still be an option.

Conclusion

- VOIP is still an emerging technology, so it is difficult to develop a complete picture of what a mature worldwide VOIP network will one day look like. As the emergence of SIP has shown, new technologies and new protocol designs have the ability to radically change VOIP.