

Securing IP Telephony Systems – Best Practises

Defining Threats

By definition VOIP traffic is vulnerable to the same threats as data traversing the IP network... The most common threats are from Denial-of-Service attacks, "Malware", and deliberate intrusion.

It is imperative that there is a holistic approach to IT security, so that the voice system is included in overall security risk analysis and applies "best practices" as deemed appropriate, aligned to data system security measures as a minimum. In practical terms this would typically include the implementation of following security measures:

- Use deep packet inspection techniques – IDS/ IPS or Firewall Systems at WAN / Internet ingress points to prevent multi-layered attacks breaching the core network.
- Implementing robust wireless security mechanisms such as strong authentication, strong encryption and rogue access point detection.
- Deploy endpoint security on Servers and Hosts to enforce network attached devices to conform to defined enterprise and desktop security policy.

However, organisations should also be aware of the potential need to harden specific IP Telephony components to protect the integrity and availability of voice services in particular.

Securing Network Infrastructure

There are several recommended techniques for securing the network infrastructure:

- **Employ Separate Voice and Data VLANs - Mandatory**

Keeping the voice and data traffic separate through the use of 802.1Q VLANs has several advantages. The inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network attached PCs cannot initiate a direct attack on voice components.

This does not mean that there should be no interaction between Voice and Data VLANs - for example Unified Messaging solutions need access to both voicemail and email systems – but VLANs will offer a different level of control allowing Access Control and restricting 'Global' access between voice and data environments.

Additionally, organisations should employ a separate Voice Server VLAN for key Call Processing Servers so they can be secured from un-solicited access; it follows that IP phones are place in specific IP phone VLANs following normal VLAN conventions for broadcast and management control.

- **Use Secure Network Management Techniques – Highly Desirable**

All network device and server management should be encrypted to ensure confidentiality and authenticated, for example using SSH v2. A central facility that offers secure authentication, authorisation and accounting facilities would ensure that only recognised administrators can make changes to the network configuration.

This recommendation is desirable regardless of VOIP. Again SSH v2 traffic and network management applications should be managed within a dedicated Management VLAN.

- **Authenticate Network Access - Desirable**

Wireless LANs, Teleworking, and PDAs have all contributed to a widening of the network perimeter such that traditional boundary security measures may be circumvented. In order to protect the core it is desirable to authenticate any node that attempts to join the network, before allowing access to any network resource.

Implementing the network authentication standard, standards based IEEE 802.1x network access control mechanisms may be desirable where the LAN deployments allow separate 802.1x controls to be applied to voice and data VLANs – NB. IP phones typically don't support 802.1x so this should be disabled for the voice VLAN.

By ensuring any Host (wireless or wired) that attempts to gain access to the IP network must pass an integrity check; for example be check for the latest antivirus signatures; then by default the network becomes more secure for voice applications also; since Hosts that fail to pass the checks are isolated from the main network thereby protecting the core network from a potentially compromised Host machine or PDA.

- **Use “Voice Aware” Firewalls - Optional**

Stateful awareness of voice signalling protocols is essential for firewalls to maintain a secure boundary whilst being able to inspect voice traffic for potential anomalies. Not all firewalls have this capability and technicians should ensure that such firewalls support secure inspection of protocols such as SIP and H.323. Firewalls also need to treat VOIP traffic with 'precedence' so they do not impede voice, in terms of delay or jitter or packet loss.

Most organisations define internal risks as low and therefore rarely employ Firewalls internally in their IP infrastructures; employing Firewalls for perimeter security to the outside 'World'. Since the outside 'World' for voice systems is the PSTN then most IP Telephony calls will never need to traverse a Firewall.

If a Firewall boundary is deemed necessary along a VOIP path; perhaps governing VPN connections for Teleworkers; then the Firewall deployment should not only be voice aware for SIP and H.323 but the deployment itself should ideally not represent a single point of failure for the Telephony system.

IP Telephony – Security Specifics

IP Telephony security should follow a risk assessment of the probability and implications of any given threat on the Telephony system. Threats are essentially common to both voice and data systems, so industry best practices should prevail within any given organisation.

However, although the threats and type of attack methods may be similar, the implications of loosing part of or the entire phone system will be different in terms of a risk to business operations and costs.

For example, in terms of IP Telephony DoS attacks can be targeted at Call Processors, Call Routing Servers, or other IP enabled voice systems. Malware attacks can exhaust the resources

on Voice Servers and PCs running Softphone applications. Determined hackers can potentially target the IP Telephony system to either snoop on private conversations or transfer incoming calls to pay-per-use services.

Securing VOIP Equipment

Having performed a risk assessment on the implications of any given threat on the business it may be necessary to consider these additional security enhancements for the IP Telephony system:

- **Harden IP Telephony Call Processing Servers – Highly Desirable**

The voice servers' operating systems must be hardened against the possibility of direct attack. In practise this means that all non-essential network services (e.g. TFTP and Web services) should be disabled, administrator accounts secured with strong password protection and if possible that Host based IDS / IPS software agents should be installed.

- **Harden IP Phones - Desirable**

IP phones should be protected from local configuration modifications that may compromise the security of the voice system. In addition, most IP phones act as an Ethernet switch, requiring only one LAN outlet to connect both the desktop PC and phone. Whilst this is convenient, it often means that voice traffic is copied across to the PC port. It is desirable to prevent the voice traffic being copied by ensuring the Voice VLAN on the PC port of the IP phone is disabled if this is not done by default by the phone hardware itself.

- **Encrypting voice traffic – Optional**

Some IP Telephony solutions now provide an option to encrypt VOIP calls so that they can remain private and can not be snooped by LAN Analysers in the voice path. Additionally, the network devices themselves could ensure the confidentiality and integrity voice (as with data) for traffic that traverses less secure WAN infrastructures such as the Internet.

- **Authenticating Telephone Users – Optional**

As with conventional Digital PBX Systems it may be desirable to force Telephone Users to logon to the phones themselves – using features like Extension mobility – and providing only basic internal dialling capabilities (Phone CoS) if a valid User profile is not initiated.

Conclusion

It is imperative to take a holistic approach to securing the voice and data infrastructure. In most cases this means following a suitable security policy for the entire network, taking a layered approach to security, in particular securing network boundaries and continuously monitoring and reviewing the effectiveness of these safeguards.

Never-the-less, organisations need to assess the risks of any given security threat differently for voice and data systems as they may have different business implications. Here hardening key voice components may be desirable as well as providing conventional network based security controls.