CHAPTER

Final thoughts

9

CHAPTER OUTLINE

BEFORE WE START

This chapter is a summary of the thoughts discussed herein as well as a different way of looking at things. There can be no simple "one-size-fits-all" solution to securing a VoIP network or a VoIP service. Internet telephony service providers, VoIP component manufacturers, and end users alike all look for a single solution, but to no avail. So perhaps the best way to close this book out is to try and summarize the thoughts and suggestions contained in the preceding chapters. It should not be a surprise that there will be some redundancies in this summary. To paraphrase a saying that was used in different training sessions: "I am going to tell you what I am going to tell you and then I am going to tell you what I told you!" So please understand that these final thoughts are more of a reiteration and a statement of the importance of the facts that have been laid out here. The intent of any book like this is to spur the thought process and hopefully encourage you, the reader, to take a hard look at the service and network to find any holes that still might exist. Things change too fast to document any guidelines that will stay current for any length of time. So this section will try to give you an opportunity to rethink your network.

WHAT WE HAVE ALREADY COVERED

A few of the things already covered include the following:

1. Encryption of the network control and signaling information as well as the media stream (RTP) is a must. AES encryption, either 192 or 256, is the best choice today. Move beyond DES and triple DES.
2. VPNs should be used to carry the VoIP in a secure tunnel whenever possible. SSL VPNs work well with the VoIP systems as well as software-based VPN clients.

3. IPSec delivers the strongest security today when it can be deployed. Refer to the RFC for this great tool.
4. Autoregistration of telephones on an IPPBX should be turned off to prevent a rogue device from registering on the network. If used, autoregistration can be used for bulk deployments but then turned off.
5. Wherever possible use dedicated servers for TFTP, music on hold (MOH), and XML to isolate these in a walled garden away from the normal servers. Moreover, offload these functions from the PBX servers.
6. Use multiple layers of administration so that a nonessential account cannot get access to security, and additions and changes to the operating systems.
7. Be aware of extension mobility, such that before a phone can be moved to a different place on the network, it must use port authentication on the switch (L2/L3) as well as user authentication.
8. One of the single largest problems with VoIP is toll fraud. Use a good prevention program to eliminate or at least minimize the risk. This includes the exploits of call forwarding all calls, restricted access to voice mail ports, and prevention of transferring calls to extension "9011."
9. Use separate DHCP servers when possible, one for voice and one for data.
10. Protect the signaling gateways, media gateways, and session border controllers from remote access. Use a strong password and use a VoIP aware firewall. Consider any device that sits out on the network and build in the necessary protection.
11. Application layer gateways will aid in preventing unauthorized access and DoS attacks as listed.

Vendor issues

As stated earlier, trying to get multiple vendor solutions to play well together can be a daunting challenge. This in no way is reflecting poorly on the vendor; it means that the end user must be proactive when dealing with vendors.

1. Become an active part of the team; don't leave all the work and decisions to the vendor(s) alone.
2. Ask tough questions regarding the way that the system works and what the potential risks are. Most of the vendors know what the issues are with their systems and with interoperability. This should not be the very first installation they are doing; they should have a series of past experiences and lessons learned.
3. Ask how long it normally takes them to rectify a problem (either known or a new issue that surfaces). What has their track record been in solving and securing their systems?
4. Ask the vendors what standards they support and what RFCs they follow. For example, RFC 3261 defines how SIP works and how to assure interoperability with most vendors. RFC 3261 is the updated version of RFC 2543 and there are approximately 150 differences between the two RFCs. Does the vendor support the 3261 over the original 2543? Has the vendor complied with the changes to allow interoperability between vendors?

5. How does their system deal with SIP support? Does it use a GUI to ease its use?
6. Does their system offer high availability and possibly load balancing throughout the system? This is a measure of not just uptime but also performance. Does the system use a form of clustering? (Preferably yes.)
7. How does the system handle IP defragmentation on all standard and nonstandard ports? The goal here is to find out how the vendor handles the networking of the system and the mitigation of a DoS attack. The ping of death may be an example to consider here in how the vendor system handles this component.
8. Does the vendor system allow the setting and defining of separate rules and actions to follow for different media types, or is a one-size-fits-all approach used?
9. Can the end user track individual calls through the system to mitigate DoS and hijacking? Can the vendor offer support against "zero-day" attacks and advanced persistent threats?
10. Can redirection of the signaling protocols be disabled to prevent misuse of this feature?
11. Can the reinvite messages, hold, and conference calling features be limited? This can prevent abuse of number of connections attacks.
12. Does the system allow static NAT for incoming and outgoing calls as an option? Can NAT be hidden from the calling/called parties?
13. Does the system offer extensive reports and logging capabilities (registration attempts/failures; call detail recording logs, etc.)? Is a Syslog server used for offloading the reports for later analysis?
14. Does the system support fill QoS features and prioritization? Will the system integrate with the parameters of the network resources in providing QoS as an integrated service?
15. How adaptable is the system to implement a toll bypass scheme? Can legacy systems (key systems, TDM PBXs, etc.) be integrated into a toll bypass arrangement, and then migrated to an IPPBX solution over time?
16. How does the system facilitate telecommuters in the network? Are there any special considerations or constraints? How many users will the system support?

The above list is not all inclusive, but these are some of the areas that would have to be discussed with each vendor providing a component or a "total solution." It may be wise to have a joint meeting with all vendors providing any component in a VoIP network. From a personal perspective, by allowing all vendors to come together and discuss your networking plans and goals, they get to hear about how each other's products work and how they may have to integrate together. Then, there is no excuse if they promise a solution and do not fulfill it; moreover, this helps to minimize the finger-pointing when something does not play well with another vendor's products. The time to learn what will and will not work together is before the system is bought and installed. At that point, the vendors still have a vested interest in full disclosure. This predeployment approach should be first on the agenda.

Controlling the risks

Without saying, one of the first things to control risks in voice mail and PBX systems includes reading the documentation. This may sound somewhat general knowledge but it is often a skipped step by end users and providers alike. Voice system manuals will (should) provide a lot of step-by-step procedures and instructions on how to properly configure the system and secure it. There is also a publication by NIST 800-24[1] that addresses finding the holes in your PBX that makes for good reading. Although the NIST publication does not address the VoIP world, it addresses many of the same issues.

Another area that needs to be considered is the way to integrate the VoIP system into the IT security plans. VoIP has very similar network issues as the data network, but it also includes many protocol-specific and device-specific issues on its own that go beyond the data network. As for internal audits and control there should be a mechanism to:

1. Centralize all of the telephony and telecommunications service requests so that stringent control can be maintained.
2. The VoIP telephony or IT management should develop policies and procedures for the systems and where possible integrate them into the IT security policy so that the wheel is not reinvented here.
3. Assessments need to be performed. Check the vendor instructions and documentation on what to test and how often.
4. Periodically test and recheck everything as new exploits are discovered regularly.

When evaluating the effectiveness of the security there may be a few added benefits offered by the vendor (either at a cost or free) such as reporting instructions on how to surface a potential issue. The same hold true in a multivendor environment (or third-party arrangement).

1. Look for and report unusual patterns that show up in real time or in the logs.
2. Consider consolidating the logs (here is where the Syslog server can come into play) so that a single point of logging can be readily reviewed.

Consider an option from either the long-distance supplier or third-party insurer if toll fraud insurance is available. Remember this is the single largest exploit on VoIP at the time and the numbers can be staggering.

Incorporate and/or add a PBX disaster recovery and continuity plan to the security measures. Remember confidentiality, integrity, and availability are the three keys to maintaining security on VoIP. Availability falls under the category of a recoverable system in the event of some disaster such as virus, malware (including ransomware), and a malicious physical attack on the hardware or software of the system. There can be no substitute to a good plan in place to recover in the event of a major breach. This process therefore includes maintaining control over physical access to the system and components. The data processing center is locked and controlled via secure card access. Think of the closets spread around the building where

[1]This is a bit dated but it has some good information in it. It was produced in 2001.

the data switches and patch panels are located. Are they also secure? Now think of the closets used for telephone connections. Are they as secure as the closets housing the data processing equipment?[2] Now that the systems are converging, they need to be controlled as much as the data components.

PBX best practices

From the perspective and at a minimum here are a few things that should be done at little or no cost, but that will provide a great return for the effort:

1. Eliminate unnecessary modems or access ports.
2. Use a centralized architecture (or centralized cluster) if possible.
3. When a distributed architecture is used lock it down.
4. When vendors use remote access for diagnostics and patches, turn the access off when not needed.
5. Centralize and protect any remote access systems.
6. Audit the use of any remote system access (this includes access to remote IPPBXs, voice mail systems, conference bridges, call centers, gateways/gatekeepers, SBC, firewalls/NAT, ALGs, proxies).
7. Whenever anyone needs to access these systems or components make sure they must authenticate before getting on. Use strong passwords and make them unique.[3] Always reset the default passwords and authentication practices.
8. When possible consider using a two-factor authentication or better (i.e., SecurPBX tokens and/or biometric capabilities).
9. Use a telephony firewall that can filter traffic between the PSTN/gateways and the PBX/IP network.
10. Already mentioned but included in the IPPBX strategy is to use separate DHCP servers: one for the voice network and one for the data network. Consider also using access control procedures that only allow certain ports to be used for DHCP requests and a different DHCP port for the DHCP response. Use a DHCP snooping feature to handle these requests and responses. This will aid in preventing a DHCP spoofing attack.
11. Along with item number 10 above, consider using a MAC filter to monitor and manage MAC addresses within the voice segment of the network. This filtering should limit devices in unknown segments from connecting to the IPPBX.

Some steps that may assist in developing a security plan like any other plan include:

1. Use a business strategy, because the plan has to protect the business from unknown adversaries.
2. Plan the network with security in mind, segment where possible, and isolate where it makes sense.

---

[2]Remember the discussion of a janitor closet where the telephone panels are located. The telephone systems were never controlled the same as the data closets.

[3]It is remarkable how many organizations still leave the default passwords in place and the default authentication.

3. Appoint a project manager as a liaison between the groups.
4. Conduct a network assessment of existing network infrastructure.
5. Add to the network plan a VoIP architecture design as an integrated system, not just an overlay.
6. Implement the VoIP and test it every step of the way.
7. Optimize the VoIP network and document the operation.

Some additional recommendations include:

1. Don't use any form of a shared media device (such as a hub or low-end switch).
2. Conduct regular inspections and look for any snooping devices.
3. Ensure VoIP sent out across a public network is encrypted. End-to-end encryption is not the only option; consider link-level encryption too.
4. Lock down any VoIP server that contains confidential information (i.e., usernames, employee IDs, department IDs, etc.) and treat the servers like any other confidential database server.
5. Possibly place the IPPBX or the telephony server on a separate segment of the network protected by a VoIP aware firewall.
6. Build redundancy into the VoIP network. This does not mean that two networks are required but critical components should be backed up with suitable redundancy.
7. QoS, scalability, manageability, and security of IP telephony should be logically deployed on logically different IP segments. Ideally, two separate networks would be used, but this conflicts with the goal of convergence.
8. Voice and data segmentation and switched architectures enhance security and aid in the eavesdropping attacks known today.
9. While separate VLANs help, filtering and routing between them is better.
10. Configure access control lists in the layer 3 switches to limit ports and addresses that can access the voice VLAN. A possibility of a VLAN Management Policy Server (VMPS) allows the switch to dynamically assign VLANs to users based on the MAC address. This is an added benefit.

SUMMARY

Suffice it to say that no network is safe. When looking at the network build the protection in layers so that a compromise of any one system or component/feature does not compromise the whole system. Recognize that a sound VoIP security strategy is dependent on a sound data security strategy. Understand that the only pure security system is a rock. Everything else is a balance between risk avoidance and cost. Finally filter all of the systems and packet flows as much as possible.

The bottom line is that:

1. VoIP security is a user's responsibility.
2. Vulnerabilities of voice and data networks and systems carry over to a VoIP network and system, only more so.

3. The risks are far too large to ignore; no action is not a solution.
4. No Holy Grail exists; there is no one solution that fits all systems and networks and for the most part there is no single solution that addresses all components of a network.
5. It is up to the organization to implement security best practices with unique VoIP security measures.

Therefore, a wrap-up of thoughts to consider might include the following:

1. Make sure that the network and security infrastructure (including all the components) are voice optimized/aware and capable of including all the unique needs of a VoIP system. Normal policies and procedures used for a TDM architecture will not work for a VoIP system. Various protocols that must open ports dynamically to establish a call require opening and closing these ports on demand. When using a NAT device, inspection of the traffic protocols is required at the network layer as well as the application layer. Thus, a VoIP aware NAT device is essential.
2. Bandwidth, latency, and QoS are crucial for network security. Theft of bandwidth is a high risk in the network today, causing severe latency that may cause dropped calls, or worse yet frustrate the end users because of poor QoS causing them to seek alternative services that are expensive and dilute the security of the organization.
3. No matter what has already been done, new exploits are discovered everyday leaving system exposed and vulnerable. Because the IPPBX system is at the heart of the VoIP network, make sure that updates and patches are conducted regularly. Where possible a test bed may be needed to install the patches and updates and be assured that these will not conflict with other ongoing systems. The last thing that should happen is a flash update causing a new vulnerability being exposed because of the patch. Isolate the system (server) from the rest of the network and test the changes.
4. Conduct regular security audits. Think like the "bad guy" who is trying to penetrate the network.
5. When any flaw or vulnerability is uncovered remediation, immediately if possible, is a must.
6. Always secure the remote access from employees; use a VPN wherever practical.
7. Eliminate any backdoors in the systems that are used by vendors for diagnostics and testing. Secure the access and turn it off when not needed.
8. Disable any unsecure features such as FTP and Telnet; disable local administration and management accounts when not needed.
9. Use encryption whenever the VoIP is crossing the internet. Wherever encryption, authentication, and authorization are optional, use them.
10. Set up the network to take advantage of separate VLANs for voice and data. Although this does not totally eliminate risk from a savvy internal user, it does aid in minimizing the overall risks.

Test it, test it, and test it again. Good luck.