


## CHAPTER

# 19

## Voice over IP (VoIP) and PBX Security



Although often overlooked even by large organizations, the security of enterprise voice, telephony, and streaming multimedia systems (such as video conferencing and webcast and multicast systems) is a critical component of a sound overall security strategy that deserves special consideration. Attackers have been targeting computing systems for the last 25 years or so using intentionally exploitative behavior such as hacking and denial of service attacks. However, telephony exploits (originally referred to as *phone phreaking* but now included as part of mainstream hacking) have been used by clever individuals and organizations as far back as the 1960s to do everything from gaining free long distance to secretly passing malicious data right under the sensorial noses of otherwise diligent security systems. In the worst cases, both low-tech efforts (cable cuts) and high-tech means (sophisticated SS7 protocol attacks, described in further detail later in this chapter) have been used, sometimes in conjunction with each other, to cause massive disruption of public telecommunications network (PTN), up to and including the crippling or total disruption of critical infrastructure emergency systems.

In the animal kingdom, the Monarch butterfly is not typically eaten by birds and other would-be butterfly predators because it has a chemical in its body that is poisonous and makes it taste horrible. The Viceroy Moth is not at all poisonous and would be a nice snack for some of the same hunters, but it has adapted to look almost identical to the Monarch—which makes it less likely to be eaten. By camouflaging itself an otherwise easy prey protects itself. Similarly, one of the most practical approaches to both VoIP and non-VoIP telephony system security is to make yourself the least attractive target. You should also consider the different threat vectors from which an attacker may target the components of your telephony infrastructure.

This chapter covers best practices for protecting voice communications. In modern telecommunication infrastructures, many protocols are used, and nearly all of them cross over onto the data communication network. There is no longer a strict delineation between voice and data, and as a result, the risks to both data networks and voice networks consist of a superset of the risks to each. We will focus on the various components of modern telecommunication infrastructure, the threats to those components both old and new, and best practices for securing each of those components. We'll also look at what can be done to protect hosted telecom environments. Rounding up the technology perspective, we'll

consider securing classic PBX-based telecom systems. Finally, we will look at telecom expense management systems, and how they can complement security defenses by providing the ability to detect security problems.

## Background

Today businesses of all sizes are compromised in a variety of ways through their voice systems. Global telecom fraud costs a fortune for carriers and enterprises. Surprisingly, many “tricks of the trade” from the early days of phone phreaking still work and are used, often in alarmingly easy ways. When you layer a VoIP system on top of an IP network, you combine the risks associated with both, creating a superset of new risks as of result. Here are two examples:

- Many VoIP systems are server-based and rely on common operating systems (mainly Windows and Linux) to run their hardware interface. Therefore, they are susceptible to a class of problems that from a voice systems perspective were not previously a threat.
- IP-based voice protocols, while providing low-cost, advanced end-user features and reliable transport mechanisms for voice traffic, also give attackers a new method for exploiting voice systems and additional avenues for compromising data networks in general.

Consider the components of a modern enterprise IP-based phone or video system:

- Call control elements (call agents)
  - Appliance or server-based call control—Internet protocol private branch exchange (IPPBX)
  - Soft switches
  - Session border controllers (SBCs)
  - Proxies
- Gateways and gatekeepers
  - Dial peers
- Multi-conference units (MCUs) and specialized conference bridges
- Hardware endpoints
  - Phones
  - Video codecs
  - Other devices and specialized endpoints
- Soft clients and software endpoints
  - IP phones
  - Unified messaging (UM) integrated chat and voice clients
  - Desktop video clients
  - IP-based smartphone clients

- Contact center components
  - Automated call distribution (ACD) and interactive voice response (IVR) systems
  - Call center integrations and outbound dialers
  - Call recording systems
  - Call center workflow solutions
- Voicemail systems

Also consider the variety of protocols that are used to run enterprise, consumer, and carrier systems, each with their own unique behaviors, vulnerabilities, and exploits. Here is an abridged list of protocols commonly used on enterprise networks, the PTN, and Internet:

- H.248 (also known as Megaco)
- Media gateway control protocol (MGCP)
- Session initiation protocol (SIP)
- H.323
- Skinny call control protocol (SCCP) and other proprietary protocols
- Session description protocol (SDP), real-time protocol (RTP), real-time control protocol (RTCP), and real-time streaming protocol (RTSP)
- Secure real-time transport protocol (SRTP)
- Inter-Asterisk eXchange protocols (IAX and IAX2)
- T.38 and T.125
- Integrated services digital network (ISDN)
- Signaling system number seven (SS7) and SIGTRAN
- Short message service (SMS)

In traditional carrier networks (as defined by AT&T to support direct distance dialing or DDD ... this was “in the beginning” for telephony), switches were defined by a class hierarchy that separated them into five different roles. This standard was U.S.-centric, but most international models were similar or identical—consider that the first European exchanges were opened under Bell patents in London and Manchester in 1878.

- **Class 1** International gateways handing off and receiving traffic from outside the U.S and Canadian networks
- **Class 2** Tandem switches interconnecting whole regions
- **Class 3** Tandem switches connecting major population centers within a region
- **Class 4** Tandem switches connecting the various areas of a city or towns in a region
- **Class 5** Switches connecting subscribers and end-users

Anything below this level was considered a PBX (private branch exchange, fully featured but owned and managed by a private entity) or key system (a small, multiline system with typically less than 50 users). This architecture allowed very close and effective control of toll centers and long distance, but limited the availability of extended features

such as least-cost routing. Large companies with networked PBXs and many connects could use least-cost routing, but it was complicated to set up and manage and, overall, was not really low-cost, but merely lower cost. It was also primarily a closed system, using the SS7 protocol to manage call control effectively without significant security facilities—owing to the lack of interaction with non-AT&T (or Bell)-controlled systems.

While this served the population well for many decades, some flaws in the approach have required new thinking as these entities and the SS7 protocol were brought into the IP world—many famous SS7 hacks and compromises illustrate the weaknesses in the approach.

The portability of IP and flexibility of VoIP have allowed enterprises to provide their own transport across significant geographical distances, as they are no longer relegated to the functions and features of a PBX. A new set of security and regulatory concerns not previously encountered has also been introduced. Some of the main drivers behind the development of VoIP technology are the opportunities for cost savings, from lowering the cost of structured cabling by sharing Ethernet connections to advanced features like VoIP backhaul and global tail-end hop-off.

These very same features have introduced new and significant challenges for the enterprise trying to protect its intellectual property and maintain regulatory and legal compliance. For example, there is a very thin line between “toll bypass” (legal) and “toll evasion” (illegal), and businesses need to be mindful of any regulations in their areas of operation prior to using these types of features. Entire books are dedicated to understanding these nuances, but here is the critical point to consider: today’s enterprise VoIP systems perform functions that span all classes of the legacy switch hierarchy, from end-user connectivity to international routing, including functionality previously reserved for Local Exchange Carriers (LECs) and Competitive Local Exchange Carriers (CLECs), the “official” telephone companies.

THE NEXT LEVEL OF EDUCATION

## VoIP Components

By taking a quick walk-through of the evolution of VoIP systems, you can easily understand how the convergence of fixed wire line, wireless, and mobile technologies has supported the rapid evolution of VoIP. Let’s examine how the modern systems are constructed as a first step toward understanding how to secure them.

### Call Control

The call control element (the “brains” of the operation) of a VoIP system can be either a purposed appliance, a piece of software that runs on a common or specialized server operating system, or a piece of network hardware embedded or integrated into another networking component such as a switch blade or software module (soft switch).

In the enterprise, the original IP phone systems were traditional digital time-division multiplexing (TDM) systems with an IP-enabled component, designed like digital systems. They eventually evolved into full IP-based systems (IPPBX). They have now evolved far beyond the early designs that mimicked the “old thinking” of voice networks by leveraging the tools and resiliency available in IP networking, high-availability server architecture, and virtualization.

Primarily responsible for call setup and teardown, signaling, device software serving, and feature configuration, call control is one of the easier pieces of the voice infrastructure to protect. This does not mean that security for this component should be taken lightly.

Call control is critical to the infrastructure, particularly if any part of your business's revenue is dependent on phone calls (customer service, call centers, etc.). If your shop runs an IP phone system that you manage internally, this hardware sits well within your physical and logical security perimeter and should be relatively straightforward to secure. Following best practices related to patching, backup, and configuration management is paramount, but as long as this component is not exposed to the outside world, it is a difficult target to all but internal threats.

If you use a hosted or SaaS-based VoIP system, take the time to analyze how the provider manages security and ensure that its vulnerability management program supports the level of risk you are willing to accept. Should your enterprise require external services for any reason (users' functional requirements, you are a VoIP provider, etc.), there are special types of call control elements such as session border controllers (SBCs) and voice proxies that are designed to be exposed to or interface with systems under a different administrative domain. Much like edge or border routers, these elements are specifically designed to function as border elements interfacing with someone else's infrastructure, whether a B2B-type connection to a provider backbone or a dial tone to customers via the Internet. SBCs can also perform functions frequently required by regulations such as emergency call prioritization and lawful intercept. It would be wise to use one of these (read: insane not to) and to ensure they are hardened, particularly if you allow VoIP-to-PSTN calls.

Network access control lists (ACLs) and firewalls can be employed to help protect these and other elements of the voice infrastructure that must be exposed, and many advanced stateful firewalls now have built-in application-level gateway (ALG) capabilities designed specifically for voice protocols. For these elements, testing is required to ensure that the security elements function and interact with the voice systems in the way that you expect and need them to. More on *why* this is important in the next section about gateways.

## Voice and Media Gateways and Gatekeepers

The voice (or media) *gateway* is the pathway to the outside world. This component is what allows termination to a PSTN, transcoding between TDM and IP networks, media termination, and other types of analog/digital/IP interface required in today's multimedia-rich IP infrastructures. Gateways are configured to use *dial peers* (defined as "addressable endpoints") to originate and receive calls. Some gateways are directly managed by the call control elements via a control protocol (MGCP or H.248), whereas others operate in a more independent, stand-alone capacity (H.323 or SIP). Voice gateways can also run soft switches and perform primary (or survivable) call processing or "all-in-one" functions, an approach commonly used in the SMB space.

The critical piece to consider about voice gateways is that, in stark contrast to the call control components, the gateways are nearly *always* exposed to the outside world in some way. Although not universally true based on the specific application, in an enterprise, voice gateways are the termination points for the PSTN and, as such, need to be carefully protected. Always ensure strong authentication methods are used to access the device itself, and pay special attention to disabling unneeded services on a gateway, especially H.323 and SIP, if they are not being used.

Some systems have these protocols enabled by default, which is a recipe for disaster if they are exposed unprotected to the Internet. For example, even if you are not running SIP on your network, a voice gateway with an Internet connection, a PSTN connection, and SIP

services enabled could fall victim to a dial peer hack, which would allow attackers to compromise the router in such a fashion that they could make calls to and from the router via the Internet or PSTN, or bridge one to the other. This could, at best, be an inconvenience, utilizing resources that would otherwise be available for legitimate purposes and, at worst, embarrassing or damaging, incurring unanticipated costs in the form of utilization and long distance. Depending on what country you are in, your local LEC, CLEC, or ISP may or may not be obligated to help you track down this fraudulent behavior, potentially leaving an enterprise stuck with huge costs. Plugging the term “voice gateway hacked” into your favorite search engine will turn up not only several clever methods for doing this, but also a slew of horror stories from administrators managing devices that they thought were secure.

*Gatekeepers*, not to be confused with gateways, provide intelligence and control certain routing and authentication, authorization, and accounting (AAA) security functions. They can also perform and assist with certain types of address translation, and can consolidate administrative control elements such as call detail records (CDR), communication with monitoring and management systems, and bandwidth management for a given zone (a term which is used here generically for illustrative purposes, although “zone” is specific to H.323 terminology). Certain environments do not have a gatekeeper function, such as pure SIP environments, and others practically require it, such as large video codec deployments. A compromised gatekeeper would give an attacker full control over all of your multimedia endpoints registered to that gatekeeper, so following the same practices as you would for your call control elements is critical.

## MCUs

Conferencing and collaboration is used extensively within and across all enterprises as part of the fundamental communications capability that connects all users to each other. At the heart of this technology is the conference bridge, or multi-conference unit (MCU), a multiport bridging system for audio, video, and multimedia collaboration. The trend between internally hosted MCUs and provider-hosted MCUs has been stuck in the yoyo of corporate decision making, with each specific situation warranting one direction or the other based on cost to own, cost to operate, features, and security. Special attention should be paid to MCU functionality, whether they are hosted on premise or externally, in order to make sure they are secure.

Consider the following:

- The easier it is to use, the more people will use it—even the ones you don’t want to use it.

One large semiconductor company was famous for having a very easy to use audio bridge with global dial-in capability, where each department (and some individuals) had their own bridge codes with no additional unique information required to join a conference. They used the same bridge codes for everything from ad-hoc conferences to critical secret strategy meetings. The flaw in this convenience was pointed out inadvertently by someone dialing in to the wrong meeting by accident—they found themselves listening to sensitive information while remaining completely incognito. A Good Samaritan might mention this to the security team; anyone else would have unauthorized access to confidential information.

- Convenience and ease of use need to be balanced with secure practices.

A secondary flaw in the same bridge at the same large semiconductor company was that the codes were rarely or never changed, even when employees left the company. Some former employees joked that they could always plan ahead of time what to do with their stock because they could eavesdrop on the finance calls prior to the earnings release—while it sounds like a no-brainer, this is a real situation and occurs more frequently than most people would like to imagine.

- A problem with an MCU can affect a lot of users at once.

Like gateways, MCUs are frequently exposed to the outside world, and are commonly used by everyone in the organization up through executive level. Turn off those unneeded services; advise business folks of both best practices for using this service and possible repercussions if they do not maintain proper security practices while leveraging this functionality.

- MCUs can connect different types of media; require those facilities to be secured.

Although the trend is moving rapidly toward IP video, there are still thousands of systems with ISDN connections standing by patiently waiting for calls. ISDN is arguably more secure than IP due to the maturity of implementation and length of time it has been in service, but this in no way guarantees that administrators are actually following those best practices for ISDN (CHAP, dial-back, PPP, etc.). The IP and ISDN sides of a video MCU are susceptible to both annoyances (video SPAM) and compromises. If you can, hire a reputable outside service to perform penetration testing specifically on your exposed MCU services on a regular basis (depending on how often you make changes) to ensure their security.

An off-premise MCU provided by an experienced third party is often more easily secured than an internally hosted MCU that is exposed, as the service providers have had some practice at securing MCSs, but that implies you trust their practices. Like anything, much of the security of the overall system is in how it is used. If security features are offered—one-time passwords, two-factor authentication—evaluate what level of security is appropriate for the application and then ensure it is met.

## Hardware Endpoints

Endpoint compromises today are frequently targeted at mobile devices, and much of the attention in the industry right now is focused on how to secure the mobile environment. The hardware phone or video codec, sitting quietly idle in the office but running 24/7, may, however, become an important tool for advanced corporate espionage, eavesdropping, or denial of service attacks. Modern VoIP phones have a fair bit of intelligence built into them and offer a previously unavailable avenue—some phones have a built-in layer two switch and are capable of executing XML scripts or Java code locally. Video codecs run all kinds of custom code required for video conferencing and content sharing and are sometimes directly exposed to the Internet. None of these devices have particularly robust mechanisms for authenticating to their control components, unless a diligent administrator goes out of his or her way to enable them. Generally, these local capabilities are used to make the devices more interactive and functional, but they can be exploited in a variety of ways.

According to the research firm Gartner, XML-based attacks are the next big thing, based on comments released after a disclosure of vulnerabilities related to remote code



execution and DoS ability from exploited XML code. Part of what makes this a problem for the enterprise is the sheer number of endpoints connected to the system—a single phone system may manage tens of thousands of endpoint devices, offering a massive exploitable base from which to wreak havoc via DDoS or other types of disruptive attacks. With VoIP in place, this not only disables your ability to make phone calls and causes productivity loss, but also can compromise your entire enterprise network from within.

Specialized endpoints are also employed for a variety of situations. Ensure that the vendors or OEMs supplying these components or devices have a suitable approach to security and understand their responsibility in the security of the overall infrastructure. It is important to recognize in this context that one phone can be the snowflake that starts the avalanche.

## Software Endpoints

Enterprise desktop strategy focuses on convergence and extending simple, useful technologies to end users. This focus is intended to increase overall productivity and collaboration. One component of this strategy is the soft phone or voice and video-enabled chat client. This is a piece of software that runs on a PC or mobile device and acts like a hardware endpoint by registering to the call control element(s) as a device.

Why would you install a soft client on a mobile device, which already has mobile capability? Two reasons: Cost is, of course, the first one. In many places, data usage on a cell phone is less costly than calling minutes, and by running a soft client, you convert what would otherwise be cellular usage minutes into an IP data stream (thank the “unlimited data plan” for this being a viable option). Second, by running the soft client, you can extend your enterprise features to the mobile user, including functionality not typically available on mobile devices such as consolidated extension-based or URI dialing. Some enterprises are even using direct inward system access (DISA) features or forking in order to make the mobile device itself an augmentation of the desk phone, creating a Single Number Reach (SNR) environment and automatically employing intelligent features like tail-end hop-off without direct user invocation.

System administrators need to consider the fact that, although enabling these types of features is great for users and allows unprecedented ability to control cost, the virtual voice security perimeter now extends well beyond the physical perimeter they are charged with managing, sometimes reaching around the globe and well outside of the traditional realms of control. Additionally, this trend mandates that much more granular attention be paid to the end-user computing environment.

As it stands, audio streams are rarely encrypted on a corporate LAN (or anywhere else for that matter) and can be easily sniffed; with a soft phone, both the means to eavesdrop and the source of what you want to listen to can be accessed via the same NIC, even when SRTP is used. Although SaaS-based chat and IM infrastructure is out of the scope of this chapter, there is a trend toward federating internal and external systems and enabling cross-federation calling via soft clients and “pervasive” B2B video. Lock this down as much as possible by only explicitly allowing the control systems to communicate with each other and only with the required ports and services.

## Call and Contact Center Components

Call centers have made a remarkable evolutionary leap, from initially being used as a place to take orders and field complaints, to being a strategic asset that most enterprises cannot



survive without. Within the last decade, call centers have morphed into “contact centers” and “centers of excellence.” Trusted to sustain 24/7/forever operation and provide all levels of support to customers across every industry imaginable, these highly complex distributed systems, which now support millions of agents worldwide, have taken advantage of VoIP technologies in new and exciting ways—or, for the security administrator, in completely frightening ways. Their complexity has increased exponentially as the expectations of agents and customers alike have increased in sophistication.

The two core components of any call center are automatic call detection (ACD) and interactive voice response (IVR). Simply put, the ACD moves calls around, and the IVR collects information from the caller and queues those calls in the appropriate places, based on defined variables such as agent skills. Whereas some systems simply queue calls and route them when an agent is available, others have advanced speech recognition capability and complicated algorithms predicting variables such as wait time for the next agent. Because of the complexity of these systems, it is especially important to ensure that they are patched and updated on a regular basis. A compromise of ACD or IVR could spell disaster for the victim, up to and including unrecoverable brand damage.

Increasingly, these systems are being integrated with SaaS-based external solutions, especially CRM and other customer experience database systems. Although this offers the ability to drive a valuable and unique customer experience by having a single source of truth for customer data, it also warrants heavy scrutiny from a trained security professional. Many call centers employ predictive dialers or low-tech outbound dialers, which are powerful tools in the wrong hands unless best practices are followed to ensure that they are only allowed to call the numbers you want them to dial.

Call recording and workflow management solutions can be very helpful for the overall productivity of your agent workforce, but they can also present a liability—these systems should have a known, published policy for how they are used, how long data is stored, how archives are maintained, and what practices are used if data must or must not be destroyed.

## Voicemail Systems

The last, but certainly not least, major component of a VoIP-based telephony system is the voicemail system. Auto attendants, direct inward system access (DISA) features used for manual call forwarding, automatic call forwarding, and other voicemail features are a “standard” component of enterprise life, which nearly everyone has come to expect and rely on. Unfortunately, they have historically been one of the easiest systems to abuse for three main reasons:

- Access to mailboxes is typically numeric-only, and people find long strings of numbers difficult to remember. Easy (and often default) passwords are commonplace. War dialers can be set up to target these systems and record successful logins for attackers to return to later. Anyone who has ever built a voicemail system knows the practice of initially setting everyone’s default password to their extension, or perhaps the last four digits of their direct inward dialing (DID) phone number, or some other easy-to-figure-out formula. This is a good opportunity to stretch your creative brain muscle and come up with something better.

- Since voicemail systems have never really been considered a “key” component of an enterprise infrastructure, much less attention has been paid to securing these systems than to, say, the enterprise ERP or financial systems. Keep in mind, access to this type of functionality in the wrong hands can cause permanent damage to an organization in financial (and worse) ways.
- More often than not system-level access to and from the outside world is not carefully controlled or audited, as some of a voicemail system’s convenience “features” need outside access in order to work properly.

To preserve the sanctity of your voicemail system, always deactivate (and preferably delete) unused mailboxes, never leave default passwords in place, consider requiring more than a four-digit access code (every digit you add makes a brute-force attack that much harder, but also adds more challenge for your users), and seriously evaluate how these systems will be used within your infrastructure.

## VoIP Vulnerabilities and Countermeasures

Having outlined the components that may fall under your purview in an enterprise VoIP infrastructure, let’s now consider the three main exploitable paths from which you may be attacked:

- The “low-tech” hacks
- Attacks on server, appliance, or hardware infrastructure
- Advanced threats directed against specific systems or protocols

Telephony systems are frequently targeted partly because of the maturity of their services and partly owing to their sheer numbers. Everyone has a phone system. Here’s what you can do to ensure that you’ve done your due diligence when it comes to protecting your VoIP and multimedia-rich infrastructure.

The following areas require specific attention from security administrators and these are the areas we’ll focus on in this section:

- The original hacks—how to protect yourself from the oldest tricks in the book
  - Adding insult to injury: consider who tries to exploit *voice* services vs. *VoIP* services?
- Vulnerabilities and exploits
  - The network
  - The servers
  - The appliances
  - The “other stuff”
- The protocols—examining specific areas of concern
- System integrators, hosted systems, and TEM as part of an enterprise security posture
- Putting it all together: process makes perfect

## Old Dogs, Old Tricks: The Original Hacks

In the beginning (well ... in the 1960s, that is), John Draper discovered (and exploited) a vulnerability in the Dual-tone multi-frequency signaling (DTMF) dialing systems of the time, when he found that a toy whistle from a cereal box could be used to produce a 2600 Hz sound to manipulate the communication protocol of public phone systems to obtain free long distance. He was sentenced to two months in prison.

You might think that telephone companies would have immediately fixed the vulnerability so other people couldn't repeat the exploit. But, in reality, low-tech approaches like this worked for many phone systems (including carrier systems) around the globe well into the 1980s (for instance, Telstra's "big grey phones," which were some of the first mobile phones, were a common target).

While most modern IP-based systems are smart enough not to fall for the old DTMF tricks (sort of ... many voicemail systems are still susceptible), you want to take precautions against equally simple attacks that will probe your defenses on a daily basis. Information on exploits of various systems is so readily available, that taking advantage of open relays is a common recreational and for-profit activity. In addition, the security of a fixed location, such as a land line, is no longer a reliable way to ensure that you know where a call is originating from, an important part of understanding what someone is trying to do.

The portability of public IP address space means that spoofing the physical location of a phone is a relatively easy matter, and tracking it down can be quite difficult. The VoIP predator's basic approach is to sell a VoIP service to end customers and then use compromised systems to route those calls for free from and to virtually anywhere. The predator charges for a service on the front end, but gets a free service (hopefully not from you) on the back end. There's always a phone bill—but it is generally left up to the victim to settle, as the victim's carrier has to pay their partner provider for the calls regardless.

In the enterprise, the trick is to not become one of those relays. Often, people or businesses think they are subscribing to a legitimate service, as there are hundreds, even thousands, of exploited gateways. Of little help is the fact that hiding voice transit and routing among other IP-based traffic is easy.

## Assessment Audit

Create a risk profile for low-tech hacks in your organization by doing the following audit.

- What is your externally facing profile?
- Are there exposed numbers that can reach internal systems and access them?
- If so, do those internal systems have password or PIN protection? What complexity?
- If simple access is required for any reason, can you audit access?
- Who is responsible for accepting the risk of a breach? Is this person aware of this responsibility and what it means to the organization?
- Have you performed an inventory of all voice protocols enabled on your gateways for use later? If not, do so now.
- Is DISA enabled?

- Given that some organizations prefer a “live answer” experience for their internal and external customers, have the operators been trained and given process documentation to follow in the event of a suspected malicious call?
- War dialers are still out there ... do you have the capability to determine if someone is *trying* to breach your defenses? Then use it. Enlist the phone company’s help in tracking down malicious behavior before the culprit finds an opening.
- Do you have a Telecom Expense Management (TEM) program that tracks and reports on the costs of phone usage and identifies which phones have the largest bills?

## Action Steps

1. Create a scorecard from the information you’ve gathered from your audit in order to identify your most significant risks and areas in need of attention; prioritize high-risk items with a standard likelihood and severity graph or matrix.
2. Know your dial-in numbers; only publish them for those who may need to use them, and ensure the executive team is aware of the risk of offering this service.
3. Enforce password requirements for system access.
4. Delete old and unused mailboxes as soon as possible.
5. Use restrictions (like secondary authorization codes) to prevent DISA from being used for long distance and international calling; if not possible or if the feature is needed, ensure that all calls made via DISA are logged and auditable and users with access to the service are educated on the risks.
6. Limit exposure where possible by using fewer external dial-in numbers; enforce a business process that requires security team review and approval prior to enabling new services.
7. Do not offer all user features to all users by default, unless your security program can support the ongoing use, auditing, and management of these features for the full user population.
8. Pay attention to call forwarding and who is allowed to use the feature to send calls outside of your perimeter.
9. Determine how your TEM program can flag abnormal patterns or utilization in order to give you visibility into when you may have a problem.

## Vulnerabilities and Exploits

For our purposes in this section, *vulnerability* means a weakness that has not yet been used to compromise a perimeter, whereas *exploit* is a compromised vulnerability.

### Network

Security administrators need to understand how to strike a balance between functionality and security, particularly when their peers (network and systems administrators) have the job of trying to move traffic in an unobstructed fashion across common multiaccess networks as

fast as possible. Inspecting packets takes resources and adds transit time, which can lead to an adversarial relationship between the teams working to move packets from place to place seamlessly and the teams trying to ensure that legitimate data is contained within those packets. Sit down with the parties responsible for the network and the voice systems, and using a cooperative approach citing the greater good, discuss the following topics:

- What protocols will be allowed and used for VoIP on the network?
- What protocols should be explicitly blocked?
- How much bandwidth is “normal” for your call volumes?
  - If you’re using a G.711 codec, you should expect ~80 kb per call.
  - G.729 can vary depending on compression used and specific subprotocol.
- Can you create segregated security areas (zones) for your voice components?
  - Subnets for voice control and voice gateways.
  - Subnets for phones (many network switches now have a *voice VLAN* command that allows the phone to exist on a different VLAN than the device attached behind the phone).
  - Only allow the protocols in and out that you need; if a system integrator (SI) is implementing the system for you, have them provide this information, or consult your system documentation from the manufacturer.
- Can you define and configure the system to allow calling only to locations where needed and warranted by the business?
  - Explain the benefits of a permit-by-exception model vs. explicit denial.
  - It is much better to start from a more secure configuration and open features or access once it is requested than to allow all by default and experience a compromise.
  - Although some users may be frustrated by having to request the ability to call certain places, you should keep control of this and spend the time educating people about the risks and why voice security is important, specifically ensuring that other IT administrators are on the same page
  - Do you have a way to determine if any “extra” data is being passed in voice streams? This is a more advanced capability and implies that an exploit is already in place allowing an attacker to access your system; visibility may be difficult ... e.g. if an RTP stream is using 768 kb, can you verify if it is video or something else legitimate, or could it be a malicious embedded data transfer? Determining this requires deep packet inspection capability to evaluate the UDP payload, which many modern firewalls can do to some extent via ALGs.

Basic documentation you may want to have in place and keep updated on a regular change-driven or scheduled basis should include layer one, layer two, and layer three diagrams indicating the location of all voice system components in the network, and both physical and logical topology.

## Servers

As with any server-based system, understand your key weaknesses and most vulnerable areas. As described in the previous section, having updated diagrams and an inventory of all of the components of your voice platform will help ensure that those assets can be secured in a reasonable way. Documentation is a critical but frequently overlooked part of a security management strategy, which applies to VoIP as well.

For any server-based system that runs on a commodity OS (typically Windows or Unix), ensure that your network or server teams are prepared to follow patch management procedures for these resources along with the rest of the environment. With companies like Microsoft enabling features like enterprise voice services and voicemail, system administrators have the added responsibility of ensuring that Windows servers are patched for these in addition to the rest of their KB patches. In addition, many contact center and workforce productivity solutions, some of which have special versions supported only by the manufacturer, also run on Windows under the hood.

## Appliances

Once upon a time, when DTMF ruled the voice world, dialogic boards were the key for interpreting dialed digits, and every voice system had them in either the PBX controller or voicemail system. Back then, nearly all voice systems would have been considered “custom appliances” by today’s standards. The common modern practice for many manufacturers today is to buy OEM hardware from one of the big server suppliers and to run either a proprietary OS or custom version of a commodity operating system to create their “appliance.” Some voice hardware providers still make their own application-specific integrated circuit (ASIC) chips and hardware chassis, but this is becoming less common as standardization and virtualization gain adoption in the voice space.

The real relevance for security administrators is in the amount of customization the provider does in order to offer their features. In one sense, a certain “security by obscurity” is achieved with highly customized platforms because there are generally fewer of them in the field and they present a less attractive target than something more widely deployed (which is additionally true for proprietary protocols). Inversely, an exploit specific to a unique platform may remain undiscovered for a longer period of time, as you are dependent on the manufacturer or specific product community to identify such vulnerabilities.

## Everything Else

There’s a lot that falls into the “other stuff” category, from hosted systems to all of the components that are not considered call control. Hosted systems are covered later, as they require special considerations. The two most commonly exploited systems in the “other stuff” category are DISA-enabled voicemail servers and gateways that allow connections from the Internet. No matter what brand of phone system you are running, keep the following information handy:

For the voicemail system:

- Use a least-privilege model in which administrators do not have mailboxes accessible via external means; require a VPN and strong authentication.
- Delete unused mailboxes.
- Force complexity requirements for voicemail passwords and access codes.



- Carefully consider the risks of allowing remote call forwarding or other call forwarding features, particularly those that can be enabled remotely; if a feature is not absolutely necessary for your users, do not allow it.
- Use strong authentication for “remote destination” calling or calling-card type features.

For the voice gateways:

- Explicitly *disable* unused services, especially those with Internet-facing connections.
- Lock down via ACL or firewall what systems are allowed to communicate with the gateways via IP; use a secondary system (IPS) to watch what the gateways are doing if you are running SIP or a similar protocol.

## The Protocols

At the heart of the family of VoIP technologies are the specific protocols that enable the transit and real-time conversations that IP networks were not originally designed to handle. While this book is not an authoritative reference for VoIP protocols, it is a good primer and guideline for what to consider and where to look for more information when securing networks leveraging VoIP.

Security filtering and analysis for most network-based communications has become quite advanced, but VoIP-specific capability has not kept up with the rest of the industry. While current-generation firewall ALGs can tell you that a VoIP conversation is, in fact, a valid protocol (RTP, RTSP) and an “audio data stream,” they cannot

- Tell you what is taking place in that conversation
- Guarantee that no one else is listening in
- Determine that a voice conversation is the only thing taking place over that communication channel

Outside of the U.S. Department of Defense or Department of Homeland Security (or other state-sponsored and government agencies), advanced heuristic electronic listening is not widely employed for security purposes.

Realistically and within the reach of ordinary organizations, the following section lists the mechanics of the protocols you’ll encounter on an enterprise network, some associated risks, and practical suggestions for protecting them.

### Protocol: H.248 (Megaco)

**Governing Standards** RFC 3015 (obsolete), RFC 3525 (obsolete), RFC 5125 (current)

**Purpose** Gateway control protocol: IETF and ITU-T standards-based method for meeting the requirements intended to be addressed by the development of a Media Gateway Control Protocol (MGCP), including security considerations.

**Function** Controls decomposed multimedia gateways, enabling separation of call control and media transcoding and conversion; supports a broad range of network types.

**Known Compromises and Vulnerabilities** DoS attacks using malformed packets targeted at port 2944 / sctp. This port can also be used to pass H.248 text. A result of an exposed gateway can lead to DoS via a large number of packets being directed at the default ports, making the gateway too busy to process legitimate traffic. H.248 has no built-in security and relies on lower layer protocol support for security such as IPSec or TLS, but these are frequently not used as crypto processing introduces latency to a very latency- and jitter-sensitive application (voice).

**Recommendations** Consider the requirements for performance, signaling security, and media security if you are going to use this protocol for gateway control. A suitable approach is to use encryption for call setup (signaling protection), which adds some processing time for call setup, but prevents replay attacks, spoofing, and barge-in, and to use SRTP to protect the audio streams (media protection). Remember that both of these will add time and can affect the number of simultaneous call flows that your system can process.

## Protocol: MGCP

**Governing Standards** RFC 2705 (obsolete), RFC 3435 (obsolete), RFC 3660 (current), RFC 3661 (current). Media Gateway Control Protocol (MGCP) is the de facto standard in the industry for gateway control implementations.

**Purpose** Packaged gateway control protocol currently deployed and implemented in many different voice and media systems—RFC 3435 specifically describes an API and corresponding protocol used between elements of a decomposed multimedia gateway.

**Function** Controls decomposed multimedia gateways, enabling separation of call control and media transcoding and conversion; supports a broad range of network types. Default port for MGCP devices is UDP 2427.

**Known Compromises and Vulnerabilities** Interference with authorized calls or setup of unauthorized calls via barge-in or intercept, and rerouting or dropping legitimate calls-in-progress. DoS attacks occur via directing a large volume of traffic to UDP port 2427, preventing the device from processing legitimate requests. Possibility of a device crash via sending a specifically malformed packet directed to UDP port 2427. Some vendor-specific implementations have targetable vulnerabilities (including Cisco's ASA UDP inspection engine; see Cisco Advisory ID: cisco-sa-20120314-asa).

**Recommendations** Because a system will use MGCP if running gateways controlled by a call agent, ensure that you research the specific platform and any known bugs or code vulnerabilities that may exist. The OEM or vendor should also be able to furnish this on request. Many MGCP exploits are targeted at systems other than the VoIP systems themselves, and as no security mechanisms are designed into the MGCP protocol itself, it would be wise to consider reviewing RFC 2705, which refers to using IPSec (AH or ESP) as a protection. In fact, RFC 2705 recommends that MGCP *only* be implemented with IPSec and that MGCP messages only be carried over secure connections. In practice, this advice is not always heeded, so do not assume that a system was implemented according to the RFC recommendations.

## Protocol: SIP

**Governing Standard** The Session Initiation Protocol (SIP) standards and extensions are so numerous that an RFC is dedicated to identifying all of the other SIP RFCs (Hitchhiker's Guide to SIP, RFC 5411), and there are books to help navigate the situation. For the basics, RFC 3261 is the core SIP standard. SIP is a highly complex set of protocols—really a protocol suite with volumes dedicated to implementing, managing, and securing the entire stack based on different use cases. This overview is not a substitute for deeper research on how SIP is being used within an enterprise and the methods required to ensure it has been securely implemented and suitably protected.

**Purpose** Application layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. Sessions include Internet telephone calls, multimedia calls and distribution, and multimedia conferencing. In plain English: SIP is used for all kinds of voice and multimedia applications and is prolific both on corporate networks and the Internet, sometimes appearing unintentionally in enterprise environments via voice-enable chat clients that are both sponsored (e.g. Lync, Connect, Jabber, etc.) and unauthorized (Yahoo messenger, AIM, etc.).

**Function** SIP is a session-based protocol, using SIP invitations that are used to create sessions. These carry session descriptions that allow participants to negotiate a set of compatible media types (in the event that different endpoints or devices have different capabilities). SIP makes use of proxy servers to route requests to a user's registered location ("current" location), authenticate and authorize services, implement provider call-routing policies, and provide features. SIP also provides a registration function that allows users to upload their current locations for use by SIP proxies. SIP runs on top of several different transport protocols and relies on a variety of different mechanisms for security.

**Known Compromises and Vulnerabilities** Because there are so many SIP-related vulnerabilities that exist based on the different implementations of the protocol and extensions, it is worth classifying them into the following categories:

- Control-system and SIP proxy
- Device-based (including mobile device)
- DoS, DDoS, flooding
- SPAM over Internet Telephony (SPIT)
- Vishing (the criminal practice of using social engineering over a telephony system, widely facilitated by VoIP and SIP-based systems)
- Spoofing, bargaining, and redirection
- Replay and interception

**Recommendations** If you're going to allow SIP on the network or enable SIP-based enterprise applications, either for voice and video (or other converged services) or for less specific uses (third-party IM clients, etc.), seriously consider the minimum level users *need* in order to function. Discuss this with whoever in your organization is responsible for the services that use SIP and ensure that they understand the risks of this highly dynamic protocol.

If your policy doesn't allow use of third-party IM clients and there is no requirement to support a SIP-based enterprise function, turn SIP services off on all network devices and explicitly block it at your edge inbound and outbound. SIP can use a variety of ports statically or dynamically depending on the application (the defaults are typically TCP and UDP 5060 or 5061, but, like HTTP, SIP can be configured to use any ports), so, if possible, block it via protocol recognition.

If SIP is required, and particularly if such a requirement includes SIP services be available via the Internet, ensure you are using a device that has the capability to inspect the traffic (a firewall with inspection or ALG capability, an IDS, or other sniffer or analyzer) and validate that the information in the SIP header is correctly formed and is accurate (SIP header construction is alarmingly easy to spoof). This is the easiest way to tell if there is a spoof attempt or other malicious activity in process.

Because SIP adoption is increasing owing to its ease of use, ability to implement quickly, and compatibility with a variety of devices, the pressure to secure the protocol itself and know how it is being used is increasing. SIP is possibly the single easiest threat vector to exploit due to lack of awareness and attention paid to what it is being used for on a network. Complete books are dedicated to SIP and securing it; consider getting one of these if you have critical services delivered via SIP or if you are going to allow it to run on the network. Best practices are always to turn off any unneeded services for any protocol, which is certainly true for SIP as well, but as adoption continues to increase more attention needs to be paid to how and where this particular protocol is being used.

## Protocol: H.323

**Governing Standard** H.323 may actually have more reference material than SIP, as it is itself a “standard” currently in ITU-T revision 7 (H.323 v7). It is a component of the “H-series” ITU-T recommendations for Audiovisual and Multimedia Systems specifically addressing systems and terminal equipment for audiovisual services. The overall H-series recommendations cover a wide variety of different aspects of multimedia networking.

**Purpose** Standardized approach for terminals and other entities that provide multimedia communications services over packet-based networks that may not provide a guaranteed quality of service. Audio support is mandatory, but entities may support real-time video and/or data communications as well. If video and data are supported, the ability to use a common mode of operation is required, so that all terminals supporting the media type can interact. H.323 has dozens of subprotocols, including a specific security subprotocol, H.235 (currently in revision .9 which is the 13<sup>th</sup> revision of the protocol—note, the numbering scheme was changed mid-lifecycle; the order of numbering is H.235v1, H.235v2, H.235v3, H235.0 [which was v4], H.235.1, H.235.2, H.235.3 ... etc. to current, H.235.9).

**Function** H.323 entities may be integrated into PCs or implemented in standalone devices (videoconferencing codecs, IP cameras, MCUs, for example) and support many types of networks and internetworking, including point-to-point, multipoint, broadcast, or multiaccess networks (see ITU-T H.332). Methods for internetworking with other networks are supported, including terminals on B-ISDN, N-ISDN, guaranteed quality-of-service LANs, GSTN, and wireless networks, and other specific types of terminals and networks through the use of

gateways. Today, H.323 is the most commonly used approach for videoconferencing over IP, and it is gaining traction as more enterprises focus on saving costs by reducing travel, replacing the face-to-face interactions with room-based videoconferencing and video-to-the-desktop.

**Known Compromises and Vulnerabilities** Like SIP, there are far too many compromises and vulnerabilities to list them specifically ... there are no less than 50 different implementations of H.323 by different vendors—and there are probably many, many more. Several of these implementations contain vendor-specific intellectual property to enable certain features or functions. In general, you will want to dig in if you support H.323-based services and understand what the specific risks are around the supported devices and platforms. Also, like SIP, there are full volumes addressing H.323 security, but the most common and impacting types of H.323 vulnerabilities are

- DoS, DDoS, flooding
- Gateway compromises (probably the most common, relevant, dangerous, and potentially damaging from a risk perspective)
- Remote code execution and arbitrary code execution

**Recommendations** If you're not using it—turn it off! Do not assume that the capability to communicate via this protocol suite over your network is disabled by default. Many devices are shipped with these protocols enabled for convenience—so it will “just work” if you introduce a new device into the network. Leaving H.323 enabled on an Internet-facing gateway can lead to disaster—a specific compromise is covered earlier in this chapter to which H.323 gateways are particularly susceptible. Although SIP is an IEEE-provided set of recommendations and H.323 is from the ITU-T, they have many overlapping capabilities and functions. If it is at all possible to standardize on the use of one versus the other for the enterprise, focus on security, but it is unlikely that this will be the case in today's vendor-centric multimedia technology world.

## Protocol: SCCP and Other Proprietary Protocols

**Governing Standard** Skinny Call Control Protocol (SCCP) (aka “skinny”) is a Cisco-proprietary protocol; other vendors have also developed closed protocols implemented ahead of or outside of the IETF, IEEE, and ITU-T standards.

**Purpose** Lightweight protocol for session signaling and endpoint call control in a Cisco Call Manager environment. There are many protocols specific to an OEM or equipment vendor.

**Function** Call control, signaling, and other functions as defined on a per-vendor (OEM) basis.

**Known Compromises and Vulnerabilities** Because SCCP is a category of protocol, the specific SCCP vulnerabilities are not listed. It is, however, critical to engage the supplier or manufacturer and require them to disclose and keep you apprised of all specific vulnerabilities or exploits that their platforms are susceptible to, including from the open standard protocols.

**Recommendations** Although not a common practice, it would be wise to require an SLA for an OEM to fix any exploitable vectors that exceed a specified or defined level of severity within an agreed (preferably, contractually agreed) amount of time. At a minimum, find out what the OEM or manufacturer's processes are around patching, vulnerability management, and exploit discovery in their products. When it comes to large vendors like Cisco and Avaya, they have mechanisms in place to publish alerts related to vulnerabilities in their products via specific community support forums or dedicated support sites. Visit these on a regular basis or sign up for email-based notification if they offer it in order to stay on top of vulnerabilities that may affect platforms on your network.

## Protocol: SDP/RTP/RTCP/RTSP

### Governing Standard

- **Session Description Protocol (SDP)** RFC 2327 (obsolete), RFC 3266 (obsolete), RFC 4566 (current)
- **Real-Time Protocol (RTP)** RFC1889 (obsolete), RFC 3550 (current, but updated by RFC 5506, RFC 5761, RFC 6051, RFC 6222)
- **Real-Time Control Protocol (RTCP)** RFC 3605
- **Real-Time Streaming Protocol (RTSP)** RFC 2326 (extensions part of RFC 6064)

### Purpose

- **SDP** A format description for standardized conveyance of media details, transport addresses, and session description metadata (relies on other protocols for actual transport).
- **RTP** A protocol providing end-to-end network transport functions for real-time data applications over unicast or multicast networks.
- **RTCP** An extension of SDP supporting NAT traversal
- **RTSP** A protocol for streaming audio and video multimedia

**Function** Various; these form a core set of protocols used for describing how media transport should work and actually moving the media across the network.

**Known Compromises and Vulnerabilities** Most specific vulnerabilities related to these protocols will either be related to a particular piece of equipment or exploited via a method (e.g., RTP interception and redirection). As advised previously, ensure that whichever VoIP or multimedia platform you are using is regularly evaluated, tested, patched, and audited, along with the rest of the network.

**Recommendations** Use secure protocols where available, such as SRTP, to support the functionality requirements provided by the listed protocols. In some cases, no secure transport protocols are available as built-in options, so other protocol suites or families such as IPSec should be used to protect the required VoIP and multimedia control traffic.



## Protocol: SRTP

**Governing Standard** RFC 3711 (current)

**Purpose** Secure Real-Time Transport Protocol (SRTP) is a profile of RTP, which can provide authentication, confidentiality, replay protection, and protection to the RTCP traffic.

**Function** SRTP provides a framework for authenticating and encrypting RTP and RTCP streams, including definition of a default set of transforms and extensibility for inclusions of future transform sets. SRTP offers high throughput and low packet expansion, both critical considerations for any protection mechanism of a real-time media capability.

**Known Compromises and Vulnerabilities** Although using SRTP is significantly better than not using anything, it is not by itself a catch-all or complete security mechanism for protecting voice or multimedia traffic. The default settings are susceptible to brute-force attacks, as in many implementations, SRTP only requires DES encryption, which is relatively easy to crack by modern computing standards. On top of this, key management is critical, as a compromised key negates the relevance of even strong encryption.

**Recommendations** Following security best practices ensures that the default encryption requirements that SRTP negotiates are suitably strong to prevent brute-force attacks, and a key management program helps guarantee that keys are changed frequently to preserve the integrity of the encryption in place.

## Protocol: IAX and IAX2

**Governing Standard** RFC 5456 (IAXv2, current), RFC 5457 (IANA considerations for IAX). All modern references to IAX refer to IAX2.

**Purpose** Inter-Asterisk eXchange Protocol (IAX) was developed to minimize bandwidth utilization over slower network links, with support for trunking and multiplexing, and ability to traverse firewalls and NAT.

**Function** IAX is an “all-in-one” application layer control protocol for creating, modifying, and terminating multimedia sessions over IP networks from server-to-server and server-to-client. Although primarily targeted at VoIP, IAX can be used for other multimedia applications including streaming video. IAX is somewhat unique in its “in-band” approach, delivering both control and media services together. IAX uses a single static-port UDP data stream that simplifies NAT traversal, a problem for some other voice control protocols. The intent is to simplify firewall and network management. IAX is also compact and efficient, and as an open protocol, supports future additional payload types and services, although to be incorporated, features have to be added to the protocol.

**Known Compromises and Vulnerabilities** As with all real-time systems, risks of resource exhaustion or DoS-type attacks are ever present. For IAX, because of the well-known single static port and risk of added processing time to the nonlatency-tolerant media streams, this risk should not be taken lightly. Additionally, some known vulnerabilities for the IAX2 libraries allow remote code execution via a truncated frame exploit. However, the most

significant risk from IAX, in particular, is also one of the protocol's main benefits—its efficiency and ability to support many different traffic streams in a multiplexed fashion over a firewall. While most IAX issues will be a result of the implementation versus the capability of the protocol, organizations with sensitive data or intellectual property that may be subject to corporate espionage or other commercial for-profit exploitation should carefully evaluate whether they want to support a protocol that makes it easier for someone to smuggle data outside the walls in an almost steganography-derived way.

**Recommendations** IAX was designed for use with Asterisk but is also available for use with some other IPPBX systems. If deploying Asterisk as an enterprise VoIP solution, it would be wise to consult one of the many volumes available relating specifically to Asterisk, some of which have entire sections or chapters covering security. If deploying IAX as a protocol solution for a non-Asterisk-based system, seriously consider the risk of not being able to determine whether the streams contain audio or something else (without access to very advanced equipment and software, that is. If you're working for the DoD, these capabilities may be available to you). Alternatively, evaluate the functional balance of using IAX with what it might take to support other protocols such as H.323 or SIP and what your overall exposure profile might look like. Your VoIP security posture must include both the risk of running this protocol, along with consideration of having run other protocols instead. After modeling any realistic situations you may encounter, which leaves you with the least amount of residual risk?

## Protocol: T.38

**Governing Standard** RFC 3362 (T.38, current), ITU Recommendation T.38

**Purpose** SDP media descriptor for transmitting MIME subtype image and T.38 facsimile transmissions over an IP network.

**Function** Allows fax over IP in real time via either TCP or UDP.

**Known Compromises and Vulnerabilities** This is worth researching in some detail for your particular application. Some known Asterisk vulnerabilities allow a remote system crash while negotiating T.38 parameters over SIP.

**Recommendations** Although a less commonly exploited mechanism, ensure that your OEM or provider can detail any T.38 issues you may face prior to implementation.

## Protocol: ISDN

**Governing Standard** Too many to list

**Purpose** Integrated Systems Digital Networks (ISDN) are the foundation of many of the modern TDM networks that support the PTN and PSTN, and while not really part of VoIP technologies, are worth a mention.

**Function** As related to VoIP, ISDN networks are either used for IP-based transport or are linked via gateways to VoIP networks for PSTN access.

**Known Compromises and Vulnerabilities** ISDN has been around for some time and is a cornerstone of today's global voice transport capabilities; consider how ISDN might play into your overall VoIP and multimedia systems. Although dozens of books, magazines, and research papers are dedicated to ISDN and many of them cover security in detail, the main security consideration for an enterprise is the touch point the between internal VoIP networks and the PSTN: the gateway. It is common to see exploits tried from IP-networks attempting to bridge the PSTN network; but it is also possible to compromise a gateway from the PSTN and create a hairpin, which is just as damaging to long-distance bills (and can be worse if you pay for inbound minutes as well).

**Recommendations** Audit all gateways on a regular basis that have both VoIP networks and PSTN networks connected to them. If using ISDN for videoconferencing, utilize the stronger authentication methods built in to the PPP protocol (CHAP), and preferably control who is allowed to dial in via ISDN. You can also use well-documented features like call back in order to prevent spoofing.

## Protocol: SS7 and SIGTRAN

**Governing Standard** Too many to list

**Purpose** Signaling System No. 7 (SS7) is the signaling standard for the PTN, and SIGTRAN is the adoption for allowing SS7 to function over IP networks.

**Function** Signaling and control for PTN voice networks, largely outside the scope of VoIP considerations, but worth mentioning for awareness and familiarity.

**Known Compromises and Vulnerabilities** Research this if the environment is actually running these protocols. Many published vulnerabilities and exploits for SS7 are addressable via best practices.

**Recommendations** Typically, you will not have to support these types of protocols unless you are an exchange or voice carrier, although sometimes these protocols are used specifically for backhaul over IP networks, which should be specifically understood and addressed in relation to the overall security posture.

## Protocol: SMS

**Governing Standard** 3GPP TS 23.040 (sort of ... SMS was developed as part of the international cooperative GSM project)

**Purpose** Short Message Service (SMS) is a methodology for sending text messages via cellular or other mobile technologies, but is now being adopted and integrated into other multimedia applications.

**Function** Everyone today uses SMS with or without realizing it, but adoption in enterprise environments is increasing at an incredible rate for business communications.

**Known Compromises and Vulnerabilities** While SMS is not strictly related to enterprise VoIP, understanding the trend toward owning and operating corporate SMS gateways is relevant. *Direct text marketing* and other methods of text SPAM/unsolicited/unregulated SMS messaging will become a tool in the black hat's toolkit in the near future (if it has not already come to pass). The same sophisticated social engineering tricks that can leverage SIP so easily can also use SMS as another convenient launch medium.

**Recommendations** Specifics related to securing the operation of SMS are unique and need special consideration. The IP multimedia subsystem (IMS), part of the next-generation network (NGN) developed as a replacement for GSM by 3GPP, added support for SMS in release 11, and both this and other cellular network technologies (4G LTE for example) either support today or will support SMS. If interacting with or supporting cellular networks, ensure that the considerations for SMS make it into the overall risk assessment, and the specifics of the installation are defined, measured for risk, and evaluated on an ongoing basis as the services and uses evolve.

## Security Posture: System Integrators and Hosted VoIP

How much does the system integrator or vendor that's chosen really know about the selected VoIP or multimedia platform? Are they experts on security or on securing this specific system? How many times have they implemented a similar system, and have any of those systems been compromised? If deploying an off-premise solution, how will we guarantee the integrity of sensitive corporate conversations? What capabilities do we have to ensure that our phone bills are actually correct? These questions—and many more—need to be answered if your organization is in the process of evaluating or deploying a new VoIP technology. The three specific areas alluded to in these questions can be outlined as detailed in the following sections.

For hosted VoIP:

- Should I consider a hosted option for enterprise use?
- Where does the responsibility lie for the security of a hosted system?
- Is it possible to integrate an off-premise solution with something internally hosted and managed, and is this a good idea?

For TEM:

- What is TEM and what does it do for the enterprise?
- How does TEM relate to security?

## System Integrators

The trend across IT departments today seems to be toward perpetually figuring out how to do more with less. Although running lean can provide some benefits to the financial bottom line, it also creates new risks to the environment. Using a system integrator (SI) can be cost-effective, but how can you ensure that you will improve your security rather than create additional vulnerabilities that will need to be addressed? There are a few questions you should ask your vendors that will help ensure you that they both know what it will take to

provide a secure system and keep your best interests in mind. Before starting, ask yourself these questions:

- How can I choose a quality integrator and determine if the integrator has the necessary skills to implement the system?
- What questions can I ask in order to determine if one integrator is more security-aware than another if they are both technically competent?
- Does the network require other attention prior to a VoIP deployment?

When evaluating a new system, if you don't already have one, create a scorecard by which you can measure vendors against each other. It does not need to be complicated, but should give you the ability to rate vendors relative to their ability to implement the solution via a point system and one versus another. You want both objective and subjective metrics—if you've used a vendor in the past and had great experiences, then that should count for something. Alternatively, if you have had poor experiences with an SI in the past but they have proven to your satisfaction that they can do a better job for you, that thinking should be incorporated as well. The Balanced Scorecard approach offers an easy-to-use template, or you can create something simple, like the one shown in Figure 19-1.

In addition to the scorecard, carefully evaluate the vendor's Statement of Work (SOW) and understand exactly what they are proposing they do and what they are asking you to do. Often, small items are included in an SOW that are expected of the customer but aren't necessarily considered up front—these can become a big deal later. Make sure the responsibilities and tasks that the vendor needs you to complete to be successful are spelled out in very clear detail, preferably in one place.

Your company name		Go/No-Go Criteria		Metric Weight/ Importance		Vendor A		Vendor B		Vendor C		Vendor D		Additional notes		Total
Short project description/what you are trying to accomplish		Raw score	Weighted Score	Raw score	Weighted score	Raw score	Weighted score	Raw score	Weighted score	Raw score	Weighted score	Raw score	Weighted score			
1	Project schedule can be met															
2	Budget/project cost															
3	SOW terms defined by business owner															
4	Success criteria defined by business owner															
5	Success criteria															
<b>Vendor requirements</b>																
6	Qualified to do this work															
7	References															
8	Version/revision control system															
9	Ability to execute															
10	Financial stability															

Figure 19-1 Vendor scorecard

For example, is the vendor providing project management, or will you handle it internally? Project management (PM) may not seem to be directly related to security, but in the bigger picture, having PM involvement helps ensure that things are organized in a way that explicitly defines the task-level expectations from a security perspective, and can ensure that things like suitable documentation are delivered after the project is closed. Quiz the vendors about their general practices around security, get a feel for their general approach, and ensure that you discuss what your expectations are from a baseline security perspective. You can ask things like:

- How many deployments of the specific system have you completed?
  - Are you familiar with this code revision and any security-related release notes and default setting changes for the version to be deployed?
- Have any of the systems you've previously installed been compromised?
  - If so, why? Were you involved in the root cause analysis?
  - What did you learn and what internal processes have you changed as a result of that experience?
- At what point do you change passwords during the install process?
- What are the basic ACLs or protections you put in place for every deployment, by default, without specific customer request?
- Which sets of security standard practices are you familiar with and which do you employ in your planning, installation, and deployment processes?
- A question for yourself: Since you're going to *rely* on this SI to perform work that you will have to put your seal of approval on and possibly attach your name to ... do you have a sense of confidence that the vendor will to “do the right thing” or do what you would do given a difficult choice?

Do some advance research to understand what the best practices are for baseline security for whatever system you're about to deploy. Particularly with voice, security is important and often neglected. Ask the vendor about past mistakes or things that didn't go so well—if the vendor is willing to be open and humble about things that they've learned from in the past, you may get an idea of how well the vendor will address anything that does fall through the cracks.

There are conflicting ideas between VoIP functionality and preserving perimeter security, and sometimes a network needs to be “prepped” for voice. This consideration isn't strictly about how to configure your QoS—you also want to be aware of your visibility into what voice protocols are being used on the network and how they are being used. The SI should document and provide exactly what the net add is going to be, both in traffic volume and type, along with recommendations for anything that needs to be investigated or completed in the security systems (firewalls, IDS and IPS, analyzers, monitoring platforms, etc.).

## Hosted VoIP and Off-Premise Systems

Between the cost of capital, the capital itself, and the ongoing cost of operations, many organizations are looking at ways to stretch the dollars spent on their telecommunication systems. Phones and telecom are part of the bottom-line functionality that business cannot survive without, which sounds obvious, but frequently means that many assumptions are made about the cost aspects for procuring and operating voice platforms.



Thanks to the extensibility and low cost of VoIP technologies, the cost of computing power to support multitenancy, the “cloud” movement, and Moore’s law basically holding true for the cost of bandwidth (which means you can get double the bandwidth for the same cost every 18 months), a relatively new market has emerged—the hosted VoIP phone system. Off-premise solutions available to businesses offer a complete suite of enterprise features and functionality previously reserved for only enterprise-level highly complex PBX systems.

For most organizations, cost is often a primary decision driver. Because low cost and high security are often competing ideas, defining a set of “relevance factors” may help you qualify whether a hosted system is a good idea for your organization. Understanding what is important to your business helps you make a recommendation as to whether a cloud-based or off-premise VoIP solution is a suitable choice for your environment.

Questions you should ask both yourself and the prospective provider include the following: Should I consider a hosted system for my organization? What security methods or solutions are available to ensure that these systems are protected? How security-aware is the provider? Can administrative functions be segregated? Some voice hosting providers, specifically smaller start-up types, provide cost-effective solutions by offering multitenancy on the back-end systems. Considering that business process is the last thing to be developed in a small shop and human error is responsible for most outages and security breaches of any type globally, are you willing to bet on the robustness of your provider’s processes and the skill of its administrators to protect your data from other customers?

Some providers do have high-quality solutions that preserve the integrity and confidentiality of each of their customers’ information from each other, but how can they demonstrate this? Build a questionnaire for potential providers that helps you drill in to how they operate the systems you’re signing up for. Pay special attention to the following:

- How is multitenancy managed?
- Where are the separations between customers?
  - Are they logical or physical?
  - How are the provider’s networks built and protected?
  - Is there firewalling between different customers’ environments?
- Is a dedicated circuit required to deliver its services?
  - Is this on a private network or delivered via the Internet?
  - If delivered via the Internet, is it a dedicated Internet link or shared with other production traffic?
  - Are techniques like IPSec employed for header and payload encryption of the actual voice traffic, or is only payload protection available?
- Are SLAs being offered, and do they cover security events?
- Do the provider’s work processes and change processes preserve the segregation between your environment and someone else’s?
- Is the staff of the hosting provider able to maintain a least-privilege model and other best practices for supporting the back end?

Based on answers to some of the previous questions, if the system is administered largely outside of the organization's walls and outside the realm of administrative control by badged employees, with only endpoints actually on your network, who is responsible for the overall security of the system? This can be a sticky question, especially if you're ever in a data-breach situation. Ensuring you have strong underpinning contracts supporting the internal customer-facing SLAs will ensure that the vendor is accountable for simple things like moves, adds, and changes, but a data breach will still land squarely in the lap of the security group.

Understanding the needs of your organization's unique security environment and matching those with provider capabilities is an important exercise. Not everyone needs DoD levels of protection, so balancing your actual requirements against cost considerations and stakeholder interests is critical. If involved in the front end of the project or deployment, develop a risk profile with the potential threats you could face. If joining mid-cycle, consider performing an audit of the system and its functions, review the tickets for suspicious or security-related items, and generate an audit findings report that gets everyone (especially executives, customers, stakeholders) on exactly the same page.

Implementing a new system from the ground up, either on premise or hosted, is relatively straightforward (not simple ... but straightforward). It can be significantly more complicated, however, to integrate an existing internally managed solution with a hosted one. A few typical scenarios would warrant such an activity:

- **Scenario A** Your organization is planning to migrate from one system to another over a period of time, and the situation does not allow for a direct cutover; user functionality and consolidated dialing must be preserved during the migration. In this scenario, you control both systems with the same group of administrators.
- **Scenario B** A new organization or interest has been acquired, and cost and/or other reasons dictate preserving both systems, but you are required to allow direct calling and dialing between the systems. You may, at some point, control both systems with the same group, but initially they are separately administered.
- **Scenario C** There are enough dollars spent on telecom services with a particular organization (perhaps a customer or major supplier) that it makes sense to perform some level of integration in order to save money on both sides but bypassing the PTN. You only control one system but still need to integrate with another.
- **Scenario D** Some users within your environment do not have the same set of use requirements for the system, and you can deliver packaged services to a group or type of user more cost effectively by delivering certain types of user access via a third-party system versus an internal system (or vice versa). You have a cost advantage in offering different levels of service to different types of users either by function or geography.

Each of these four scenarios has certain specific details that you need to pay attention to in order to protect the sanctity of your environment.

In scenario A, where you control both systems in the long term and you're only supporting integration for dial-plan purposes for some period of time, pay the most attention to which services will be run on which system and when, and how those services will affect the rest of the environment, but both systems are technically within your electronic perimeter—a direct

integration may be possible (for example, if the old system and new system are of the same type, you may be able to use system tools and features to integrate them securely).

Scenario B, which could be a merger or acquisition situation, may dictate that you have some level of segregation or a trust boundary between the systems for a defined period of time, which you could choose to keep in place indefinitely depending on the specifics. In this situation, you really want to consider the use of a gateway or SBC and a security device of some type sitting between the systems and offering some type of stateful inspection (SBCs and other devices can do both). Even if you have a clearly defined plan for network integration, this can be an unintended early data connection between networks that can allow nasty things in under your nose. SIP gateways are being used more and more often in this type of situation, so remember that SIP does not carry any of its own security mechanisms, relying on IPSec (which, in turn, relies on your practices and implementation) for security.

Scenario C—two systems permanently under different administrative domains—most certainly requires both a gateway and firewall, and you may want to look carefully at which traffic you allow and how it is accessed. A trunk access code via a gateway is one way to easily and securely connect to a third-party system, where calls to the other entity are allowed based on a specific dialed digit sequence (and an optional but recommended forced authorization code), or there may be other methods or features based on your system. When connecting to a third party like this, also consider where within your environment the other party needs to be able to call, as you could inadvertently become a remote gateway for someone to exploit—any connection like this creates an implied trust relationship between you and whatever system you are connecting to. As much as possible, make these allowed pathways explicit and specifically controlled by IP address, port, protocol, and service type.

Scenario D is really gaining popularity as globalization continues to grow and penetrate industries previously never considered “worldwide,” with voice and data communication capability being the cornerstone enabler for this multinational corporate foundation. Whereas the term “global company” was once only used to refer to the megalopolis or huge transnational organization of the Fortune 500, SMBs and enterprises of any size are now able to globalize with a mix of creative in- and outsourcing. Understanding what it costs to deliver complete enterprise telephony services on a per-head basis can be difficult but is worth understanding, as someone will inevitably ask the question, “What are we getting for those dollars?” This question is often followed by “This set of workers does not need all of those features; how can we deliver a subset of services to them at a lower price point?” The aware security administrator will hopefully see this thinking on the horizon and be in a position to offer some proactive advice on the matter as soon as it comes up: yes, we can securely integrate with a third-party system on a permanent basis in the following ways:

- We need to understand what the third party will provide—a phone only? Any integration to other systems? Voicemail? Remote access and DISA?
- We need to develop a suitable “interface” that preserves our security perimeter and have a firewall with ALG capability proposed as part of the design.
- We need to create dial-plan space or use a trunk access code to dial between the systems, and carefully evaluate whether we will allow features like tail-end hop-off (remember, toll bypass and toll evasion are similar, but one is illegal and one is not ... be aware of the laws in the country or state you’ve provided dial tone to).

When it comes down to it, you need to evaluate your overall mission and understand if the features and services a hosted VoIP provider is offering fit in with the expectations of your stakeholders. Not everyone needs their voice system to be run from Fort Knox, and paying attention to the other relevant details, in addition to how the back end is hosted, will help you preserve a suitable overall security posture.

## PBX

A Private Branch Exchange (PBX) is a computer-based switch that can be thought of as a local phone company. Following are some common PBX features:

- Multiple extensions
- Voicemail
- Call forwarding
- Fax management
- Remote control (for support)

### Hacking a PBX

Attackers hack PBXs for several reasons:

- To gain confidential information (espionage)
- To place outgoing calls that are charged to the organization's account (and thus free to the attacker)
- To cause damages by crashing the PBX

This section briefly reviews some common attacks, without delving into details.

### Administrative Ports and Remote Access

Administrative ports are needed to control and diagnose the PBX. In addition, vendors often require remote access via a modem to be able to support and upgrade the PBX. This port is the number one hacker entry point. An attacker can connect to the PBX via the modem; or if the administrative port is shared with a voice port, the attacker can access the port from outside the PBX by calling and manipulating the PBX to reach the administrative port. Just as with administrative privileges for computers, when attackers have remote administrative privileges, "they own the box" and can use it to make international calls or shut down the PBX.

### Voicemail

An attacker can gain information from voicemail or even make long-distance phone calls using a "through-dial" service. (After a user has been authenticated by the PBX, that user is allowed to make calls to numbers outside the PBX.) An attacker can discover a voicemail password by running an automated process that "guesses" easy passwords such as "1111," "1234," and so on.

## Denial of Service

A PBX can be brought down in a few ways:

- PBXs store their voicemail data on a hard drive. An attacker can leave a long message, full of random noises, in order to make compression less effective—whereby a PBX might have to store more data than it anticipated. This can result in a crash.
- An attacker can embed codes inside a message. (For example, an attacker might embed the code for message rewinding. Then, while the user listens to the message, the PBX will decode the embedded command and rewind the message in an endless loop.)

## Securing a PBX

Here is a checklist for securing a PBX:

- Connect administrative ports only when necessary.
- Protect remote access with a third-party device or a dial-back.
- Review the password strength of your users' passwords.
- Allow passwords to be different lengths, and require the # symbol to indicate the end of a password, rather than revealing the length of the password.
- Disable all through-dialing features.
- If you require dial through, limit it to a set of predefined needed numbers.
- Block all international calls, or limit the number of users who can initiate them.
- Block international calls to places such as the Caribbean that fraudsters tend to call.
- Train your help desk staff to identify attempted PBX hacks, such as excessive hang-ups, wrong number calls, and locked-out mailboxes.
- Make sure your PBX model is immune to common DoS attacks.

## TEM: Telecom Expense Management

Phone bills can be more complex to read than ancient hieroglyphs, and there has been little progress made on simplifying or decoding them for the average consumer or telecom manager. Understanding what is on your phone bill so you can tell whether your voice providers are doing the right thing is important (there are alarming statistics on the error percentage in consumer and corporate phone bills). But that's the job of your telecom group—why would a security professional care about phone bills? Your phone bill can have some clues to other problems in your environment, and a TEM program can help automate the process of getting to the goodies, the high-quality information you need to tell quickly if you have a security problem related to your phone system.

TEM is a relatively new discipline in the telephony space, gaining major adoption within the last decade. There are many firms armed with specialized software ready to help you collect, organize, understand, interpret, and audit your telephone bills, all for a modest

gain-share or percentage of savings fee (an interesting side note and case in point, that's how bad telecom bills are—companies will *guarantee* that they will save you *so* much money that they will derive their compensation purely from a percentage of the money they save you or get back for. And TEM firms are doing quite well, illustrating the level of opportunity out there). While effort (hopefully someone else's) is involved in the setup and optimization of the billing, once you've reached the point where a TEM firm can actually audit bills, you're likely to have a useful tool to spot irregular or suspicious activity that may otherwise be tough to catch.

At some point in his or her career, every security professional gets pulled into a conversation about some malicious phone calls or fraudulent billing. Even if the administrator hasn't had much to do with telecom prior to that, suddenly he or she has to figure out how the telephone fraud happened. With TEM in place, the security administrator has a powerful tool to search for precursors or other suspicious activity that could be related to the exploited vector the attacker used and can help identify where it may happen again.

If, for example, an unexpected \$100,000 phone bill arrives out of nowhere with calls to countries your users have no reason to call, and through investigation you determine that it was the result of a gateway compromise, you could use the TEM capability to check the rest of the PRI or voice services globally to determine if any of the same suspicious or exploited numbers were being called and to help determine if there are other potentially compromised gateways. You would, of course, also want to do an internal network audit of the services and security on the gateways themselves, as you'll want to plug the holes you know about at the same time that the TEM and audit function is checking for leaks elsewhere for you.

Although phone bills are generally not directly related to the security group's main role, it is the objective of every security group to protect stakeholder interests, and TEM can help a security group detect anomalous behavior and operate more quickly and effectively when they are called in to action for this type of an issue.

## Summary

"Process makes perfect." Similar to the maxim "location, location, location" for realtors, successful security administrators should keep this mantra in mind in all things that they do: process, process, process. Having solid, repeatable processes to support any efforts on which they embark can not only help to build trust in the security group, but also help elevate the level to which security supports and enables the business. Specifically with voice systems, investing the time to create a process cycle for evaluating new voice initiatives and maintaining updated documentation will pay dividends in the long run. There are arguably more exploitable threat vectors in modern converged multimedia platforms than any other area of technology, and this area is also the least understood and most often neglected. Having defined, documented processes established to support decisions that capture the relevant risk factors will provide a tangible ongoing value. Voice systems warrant special attention from security groups, and this chapter attempts to identify some areas that require thorough consideration when introducing this family of technologies into an environment.



## References

Androulidakis, Iosif. *PBX Security and Forensics*. Springer, 2012.

Dwivedi, Himanshu. *Hacking VoIP: Protocols, Attacks, and Countermeasures*. No Starch Press, 2008.

Endler, David, and Mark Collier. *Hacking Exposed VoIP: Voice over IP Security Secrets & Solutions*. McGraw-Hill, 2006.

Kuhn, Richard. *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*. Diane Publishing, 2003.

Park, Patrick. *Voice over IP Security*. Cisco Press, 2008.

Porter, Thomas, and Jan Kanclirz, Jr. *Practical VoIP Security*. Syngress, 2006.

Thermos, Peter, and Ari Takanen. *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*. Addison-Wesley, 2007.



# E-next

THE NEXT LEVEL OF EDUCATION