Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Often Overlooked: PBX and Voice Security in a Networked World

My goal is to bring you up to speed on some of the common risks and specific attacks/countermeasures associated with voice systems. This paper assumes some familiarity with basic PBX terminology and architecture. If you would like a primer, Brian Waldrop has written an excellent SANS article including pbx overviews, history, and common terms that can be found in the SANS Reading Room. As I have researched this topic, I felt there was a noticeable gap for a resource that pulled information on securing voice systems toge...

Copyright SANS Institute
Author Retains Full Rights

AD

Chris Herrera
GSEC Practical Assignment
Version 1.4b

Often Overlooked: PBX and Voice Security in a Networked World

Many IT security professionals may have read the title of this paper and decided this was not in the scope of their job description. They were hired to secure computers, network elements, and perhaps client/server applications from script kiddies and malicious hackers. With the exception of war dialing for open modems, voice security is the responsibility of the PBX administrator down the hall with his monochrome terminal connection to the switch and punch-down tool in his back pocket. Whatever our pre-conceptions about this section of the IT department, the bottom line is that every company or organization has a phone system. These may range between large internal pbx's with thousands of circuits, to a simple configuration of analog POTS lines, but they are there and they can cost your organization money, time, and credibility. The universal adoption of voice systems makes it is easy to forget what a core technology it is. The install rate for vpn, digital certificates, wireless networks, and biometrics varies greatly across different organizations. However, it is almost guaranteed that most organizations have some sort of phone system installed at their location.

Abstract

My goal is to bring you up to speed on some of the common risks and specific attacks/countermeasures associated with voice systems. This paper assumes some familiarity with basic PBX terminology and architecture. If you would like a primer, Brian Waldrop has written an excellent SANS article including pbx overviews, history, and common terms that can be found in the SANS Reading Room.[i] As I have researched this topic, I felt there was a noticeable gap for a resource that pulled information on securing voice systems together in one place. My goal is to provide a concise, but informative summary of voice security for a typical security administrator or manager to quickly review and act upon. Accordingly, I have assembled a checklist of what I feel every security professional needs to take into account when pulling voice systems under their security umbrella. My hope is that this list will serve as a basis for other security professionals to build and expand upon as they learn more about voice security in our networked world.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Part I:

Why you should care

Potential economic loss is a big factor for advocating the need to maintain vigilance on voice networks and devices. The telecommunications industry estimates $4 billion per year is lost to phone fraud.[ii] It would be one thing if this were just a carrier problem, but the FCC and court systems have taken the stance that when a business voice system is compromised and used to generate fraudulent traffic, the customer is liable rather than the carrier.[iii] This means that bottom line charges for that customer can quickly add up – an average reported toll fraud incident costs around $40,000.[iv] If an IT department does not annually budget for toll fraud, these unanticipated bills can eat into your planned budget virtually overnight and your department may be forced to cut security training or software monies elsewhere to stay within budget. To protect your overall department and security budget priorities, it makes sense to include pbx security in your list of responsibilities and become familiar with the architecture and basic countermeasures that can be put in place.

Additionally, phone networks can provide the same sort of revenge outlet for a disgruntled current or former employee as data networks. Denial of service and defacement activities can also be carried out on your voice infrastructure just as on data networks to wreak havoc on business operations. This type of activity generally garners executive attention and can be potentially embarrassing to the entire organization as well as your department. Assuming no preparations were in place, the logical reaction would be for management to dictate pbx security be addressed, possibly by external resources. Proactively including voice systems in your security plans can help avoid outside costs and organizational embarrassment. If you will end up examining voice security in the long run, do it now rather than waiting for the mandated reaction due to a security incident.

Phone hackers are just as smart as their IP counterparts and are out to immediately make money or cause harm through extortion or defacement. Furthermore, pbx technology has been around for such a long time, phone hackers (also called “phreakers”) have had years or decades to seek out potential vulnerabilities. So, what continues to make voice systems an attractive target? While data and internet products often receive budget dollars and personnel strictly earmarked for security, the pbx is often viewed as only needing regular maintenance to keep it running. However, since there are a relatively small number of players in the pbx equipment arena, an attacker that takes the time to learn two or three brands of pbx systems can have critical knowledge to attack over 70% of the possible targets.[v] Voice systems certainly seem deserving of much more attention than most IT security departments have allocated in the past.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Common vulnerabilities

Let's look at some of the existing hacks that are well-known and may be tried first against your voice systems.

- Administration and Maintenance Ports.

Voice systems usually have lines or terminal connections into the switch to allow administrators to make changes and diagnose trouble. For similar reasons, it is not unusual for an outside vendor to require access to the production switch to apply upgrades or troubleshoot problems. While this may seem unusual to those with computer or data network backgrounds, it is a way of life for pbx administrators. These dial-up lines provide necessary direct access into your switch, but represent the number one unauthorized entry point for hackers.[vi] In the underlying architecture of the system, some pbx systems use terminals connected to the exact same type of ports that are used to carry voice traffic. These could be switched to a voice or outside port with little notice, but using dedicated ports for admin terminals can help reduce this risk by requiring administrative access to alter the connected ports.[vii] The next step would be to make sure relatively complex passwords are in place rather than a default or blank password. Also, many of the tools and strategies we use to secure data networks can be applied to protect our admin/maintenance ports. Call-back systems, RADIUS authentication, and inactive session timeouts can be set up on some systems to provide an additional level of security. However, the most effective counter-measure is to physically unplug the lines to your maintenance ports when not in use. This will not only eliminate the possibility of this entry point the majority of the time, it will also force a vendor to schedule authorized maintenance times with you and not have free reign to dial into your switch whenever they would like.[viii]

- Account/system maintenance.

Most security professionals realize the importance of staying on top of your data network id inventory. Similarly, PBX extensions and voicemail should be rolled into whatever termination and audit process you use for data ids. Extensions and voicemail boxes for terminated employees should be de-activated just as quickly as their network ids. One of the best methods for counteracting breaches in your voice security is the end user reporting unusual occurrences or when something "just doesn't seem right." By leaving numerous "dead" extensions or mailboxes in service, you take away that supplemental security component. A hacker could then take over an extension or mailbox with a much reduced chance for discovery. If you don't coordinate data and voice network termination it can lead to information theft of existing messages and contacts, voicemails re-directing customers to the former employee's new company, abusive and slanderous messages to remaining employees, and abuse of toll or DISA (Direct Inward System

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Access) facilities. Good password architecture is also important. You are at a disadvantage with voicemail passwords since there are only 10 possible characters to use per digit. However, you should try and counteract this by making voicemail passwords as long and set to change as frequently as your organization can stomach.

Another area to be cautious is in applying system software and maintenance patches. If there are options to run production software in RAM or other hardware component, this should be chosen over a floppy disk or other removable media. This reduces the chance of someone swapping media undetected and creating backdoors to voice systems. In addition, it is important that some sort of integrity checking be done to verify any received manufacturer updates before they are loaded onto the system. Given today's sophisticated hacking community, regular checksums or CRC's are not enough to verify authenticity. Strong error detection based on cryptography must be used. This way, modifications down to the bit level can be detected and the software update aborted if inconsistencies exist.[ix] The goal is to defeat a hacker who may be trying to impersonate a manufacturer through social engineering or fake packaging to install altered code of their choice. Putting these safeguards in place should help insure only legitimate and authorized software makes it onto your production voice systems.

- Voicemail systems.

Voicemail represents an attractive target for industrial espionage. With some basic information such as the general access voicemail number and a target mailbox, common software can be used to launch semi-attended hacks. The resulting benefits to the attacker could range from sending unauthorized messages from executive mailboxes to making large numbers of long distance phone calls via any enabled thru-dialing features. The following script is provided as a proof of concept on Stephan Barnes' website for automated dialing of a target mailbox (5019) to a main voicemail access number (18005551212) while assuming the system will allow three attempts before terminating the current session.

```
"ASP/WAS script for Procomm Plus Voicemail Hacking
"Written by M4phr1k, www.m4phr1k.com, Stephan Barnes
proc main
transmit "atdt*918005551212,,,,,5019#,111111#,,5019#,222222#,,"
transmit "^M"
WAITQUIET 37
HANGUP
transmit "atdt*918005551212,,,,,5019#,333333#,,5019#,555555#,,"
transmit "^M"
WAITQUIET 37
HANGUP
```

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
transmit "atdt*918005551212,,,,,5019#,666666#,,5019#,777777#,,"
transmit "^M"
WAITQUIET 37
HANGUP
endproc
```
[x]

While this hack is not fully automated, since the attacker must listen for a good response, it is not hard to imagine additional scripting that could take these responses into account and on which Stephan theorizes in his article. He also provides some insight into the numerical theory of where to begin the hack for maximum chances of success in a minimal timeframe. Care should also be taken to avoid two common configuration choices that could make your voicemail system much easier to hack. First, using fixed length passwords should be avoided. Forcing the user to enter the * or # character before the system will respond can keep password length hidden. Second, systems should not allow entry if the password is supplied as part of a larger string of numbers. It should be confined to only accept a stand-alone password. By allowing access if the password is part of a larger string, the length of the sequence needed to guess a four-digit password is reduced by a factor of five.[xi]

Another common voicemail hack is to pre-script responses for a collect call service and then provide the compromised number in a billed to third party call. With the proper pauses, many operators and automated systems can be fooled into believing this is a legitimate response, rather than a pre-scripted voicemail greeting. Another counter-measure can be put in place to reduce this risk. Program your voicemail system with a global greeting that can't be bypassed and plays before a user's personal greeting – "You have reached the ACME global voicemail system." This simple sentence could save you thousands of dollars should a hacker break into your voicemail system and want to use it for third party calls. This should allow operators and the majority of automated systems to realize it is a bogus call and not grant the billing request. Additionally, and as noted above, all voicemail systems should be configured to disconnect callers after a certain number of failed attempts to log into a mailbox. This will extend the time needed to crack your voicemail passwords.

- Fax machines.

Fax machines are an easily overlooked component of a modern information infrastructure. It is relatively old technology that by and large is a secure form of transport. However, many sensitive documents and transactions still require the use of fax machines. This technology has become such a fixture in the workplace that people trust fax machines to make a point to point connection and transfer unencrypted data across the public phone network without pause. Surprising outcomes can result from a simple fax transmission. "For example, the Brother 780-MC fax machine allows faxes to be recorded and forwarded to another

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

telephone number. If you can guess the 3-digit password, remote access can be used to dial call-forwarding information into the telephone company, which in turn reroutes the line." [xii] By using this method for this particular fax machine, copies of all faxes could be sent to another phone number without the knowledge of the original sending party. This attack can be countered by disabling call forwarding with your service provider or the feature on the local fax device. While this type of vulnerability seems to be the exception rather than the rule, the growing popularity of fax functional products may change all of this. Fax servers, and especially all in one printing products, put the onus of securing an analog phone line and an Ethernet connection within the same machine back on the hardware vendor. While no widespread vulnerabilities have been reported, it stands to reason given recent vulnerabilities in SNMP that someone will find a way to exploit the device architecture to hack into all-in-one devices and use as an entry point to voice or data networks.

- Thru dialing features (VM, DISA, and auto-attendant)

Many pbx systems allow for some sort of thru dialing capability. This basically allows calls to be placed to an outside number from the pbx if you identify yourself as an authorized user through the voicemail system. After entering a simple code, or no code at all, you can then place outside calls. This is often the end target of phone hackers for attacking voicemail systems as described above. As one hacker explained: "The whole point of hacking Meridians is the out dial function. Once you have successfully gotten into the VMB [voicemail box] dial '0*' (Zero-Star) …This is the jackpot. With this you can call ANYWHERE (hopefully) for free, any time (unless the VMB has hours [...some do...])"[xiii] They can then sell this information and rack up as many fraudulent calls as possible in a short amount of time. The city of East Palo Alto is one documented target, "They say an AT&T investigation revealed that it was the work of high-tech hackers who managed to break into the city's phone system and rack up $30,000 in unauthorized calls before the city's long-distance carrier detected the fraudulent activity."[xiv] The majority of these calls were made over one weekend.
Direct Inward System Access (DISA) lines allow employees to call a local or toll-free line into the pbx and once entering a code dial long distance calls that are billed to the main pbx location. These can be a great benefit for traveling employees, but present a risk of being compromised. The best counter-measure is to issue calling cards to employees for off-site long distance calling. However, if it is not practical to distribute calling cards, consider long DISA access codes (8+ digits) and a number that is outside your normal dial plan to counter this risk.[xv]

An automated attendant system (automated directory) can sometimes be exploited in the same way – with a special code entry allowing outside ld calls to be placed. Restricting auto-attendant to only forward to internal extensions is the best practice.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- 700, 809 Area Code, and other ld scams

700 numbers are generally assigned to conference call companies. This service exists to provide on the fly conferencing for those who don't contract with one company for conference services. The downfall is that operators can be used to place conference calls to just about anywhere in the world and bill back to the originating number. This is another dialing scheme that attackers will try and take advantage of if regular toll or international calling is restricted. "…this is done by dialing a known 700 conference number and programming or requesting a conference-call arrangement. Subsequent calls may then be placed to both international and North American destinations, and the victim's PBX receives the bill."[xvi] Accordingly, calls to 700 number destinations should be blocked. Arrange for a standard service offering with a carrier that uses 1-800 services. This can be rolled out as a benefit to your users and limit the vulnerability of allowing 700 number dialing from your pbx.

Direct dial international long distance calls should be limited to only those employees that require regular access, and if possible, be bundled with an individual account code when used. In addition, there are multiple area codes that fall into the North American dial plan (10 digits), but actually terminate in foreign countries. It would be a mistake to assume that only allowing 10 digit long distance dialing will restrict all international toll charges. Attackers who successfully breach voice security often call Caribbean destinations. This is because in many Caribbean nations, numbers that bill you back for calling them (similar to 900 numbers in the U.S.) are interspersed throughout the dial plan. Paging individuals in your company or leaving cryptic voicemails and e-mails is one way the owners of these numbers attempt to profit from unwitting users. Just like 900 numbers, these calls bill by the minute and a successful call will result in a charge. In addition, as a phone number shortage took grip in the 1990's, the 809 area code was split into several other codes. So, while long experience may have taught you to block all calls to the 809 area code, this change means you have some catching up to do. I've included a list of the common Caribbean island area codes in my checklist for blocking consideration.

- Social Engineering

Just as with data security, the best technical precautions in the world can often be defeated by unknowing or apathetic insiders. Phreakers have the advantage of voice systems not being considered high-value assets in many cases. While most employees would not give a stranger their network password without proper authorization, they may not feel the same sense of suspicion if asked for their voicemail password. Employees need to know that voice systems are an important part of the IT infrastructure and should be treated as such. Potential scams should be communicated to them on an on-going basis via e-mail or voicemail. Receptionists or call center employees should especially have their knowledge of potential scams re-enforced. As maintainers of high volume and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

often published phone queues, phreakers may try and test these employees' abilities more than any other. They should be made aware that callers asking for extension "9000", "9100", or whatever your outside line prefix may be, are dead giveaways for voice attacks. These callers are basically asking the employee to open an outside line for them and connect them to an operator where they could bill all manner of services. Walk your receptionists through this hack once and it will likely leave the necessary impression. It is also a good practice to have them refrain from giving out extensions to unknown callers and instead just complete transfers for callers. It would be very easy for an attacker to build their own company directory of numbers and voice mailboxes to focus their attacks on if receptionists happily give up extensions as a time saving tactic. Much time is then saved for the attacker since they can drop names for senior management gleaned from your website or annual report and only focus on compromising the executive extensions provided to them from receptionists.

- Preventative logging and auditing

Good news in the otherwise daunting task of securing voice systems is that most platforms contain some sort of rudimentary logging facility that can help you identify suspect activity. While most of these features will require regular reviews to establish a baseline, they will allow you to notice basic changes in call patterns that could mean some sort of security breach is taking place. "Most PBX systems have within its security parameters the method to record, in memory, items such as system activity logs, journal files, exception reports, software errors, hardware errors, and operations and measurements parameters. These parameters or files should be constantly checked and updated, both manually and automatically."[xvii] Logs of administrative sessions and changes, call duration, originating numbers, destination numbers, and length of calls are some standard call reporting features that can tip you off to an intruder if normal calling patterns change greatly. Much of this destination information can be found in the cdr (call data record) reporting option in your pbx package. This takes some basic information from each call and allows you to extrapolate system wide data and reports. "Reports can be configured to capture data based on call type, trunk groups, extensions, and authorization codes just to name a few."[xviii] One scenario would be to examine call duration times for excessive or drastically longer duration 800 number calls. "Some companies break the law by charging improperly for entertainment and information services that you reach by dialing an 800 or 888 number. For example, some services ask you during the course of a call to simply 'Press 1' to be charged automatically."[xix] While you can't review the exact content of the call in your reports, you could determine that one or two numbers with hours of charges could be suspect and then dial those numbers to verify legitimacy. In addition, numerous integration packages are available for purchase to elevate the level of reporting, auditing, and notification available to the administrator and security staff.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Finally, your long distance and local phone companies will have some sort of fraud investigation program in place. They will monitor some of the same items mentioned above from the telecom side, but given the high volume of calls they must analyze, it stands to reason that you should review your own logs for potential signs of fraud. While your carrier's fraud department does not absolve you of needing to secure your systems, it helps to know what services they are regularly performing and to develop a relationship with the fraud department. This may help you gain a better understanding of fraud events at the carrier level and arrange to be notified of suspect activity or early warnings. I like to think of this part as similar to the relationship you may have with your anti-virus vendor. It's far from a cure-all, but a little extra protection never hurts.

- Phone Hack (Phreaking) Web Sites

One of the best ways to know what's going on in the voice hacking community is to read their forums. You can get plugged into the latest hacks and vulnerabilities along with the Phreaking community. They also provide excellent historical information. PBX technology does not evolve as quickly as computer hardware or software. Many 15 to 20 year old hacks and exploit methods still work. Some of the sites I have discovered that provide relevant hacks or extensive background info are:

Phrack - http://www.phrack.org
Australian Phreak Scene (Archive) - http://web.textfiles.com/ezines/APS/
Phreaking Portal for Belgium and Europe - http://www.phreak.be/
America's Least Wanted - http://www.americasleastwanted.com/
UK Hackers and Phreaker's Guide - http://www.exegesis.uklinux.net/gandalf/index.htm
Northern Arizona Phreaks United - http://napu.8m.com/main.html
Phone Losers of America - http://www.phonelosers.org/
State Lookup for local U.S. phreak sites - http://phonelosers.org/state_list.html

In conclusion, I have compiled the next section – An Initial Checklist for Securing Voice Systems. Even though I have tried to do a thorough job, this is really the tip of the iceberg and is only designed to help you get up to speed quickly – i.e. if you are preparing for an upcoming audit or in a reactionary mode after a successful attack on your voice systems. Once you identify all pbx components in your environment, you can begin identifying specific, targeted vulnerabilities for your platform. By following the checklist, you should be able to identify most of the common entry points casual phreakers may employ. However, only by narrowing your research to specific hardware platforms can you attempt to counteract the truly professional attacker.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Part II - An Initial Checklist for Securing Voice Systems

Section 1. Disaster Recovery Considerations

- Detail the plan for extended loss of the main or satellite pbx devices.

- Detail the plan for extended loss of one or multiple voicemail systems.

- Review fire and power system preparedness. Are the same precautions for data infrastructure applied to your voice systems including UPS capacity and monitoring?

- Are recent configurations saved on a nearline or tape backup device? This is useful in the event corruption of PBX data occurs.

- Review PBX backup strategy. Is it happening regularly? Are tapes stored off-site for recovery purposes? Look to your data backup policies and model similar provisions for voice devices.

Section 2. Essential Documentation

- Assemble current physical location maps. Include detail for each core pbx device.

- Review documentation for phone room layout and all crucial wiring.

- Are contact lists current for wiring, hardware, and software vendors if the need for priority installation/repair arises?

- Review the mechanism to inventory installed systems.

- Are all long-haul and local carrier contact numbers current in the event their infrastructure needs to be repaired or re-installed? Are d-marc points to these carriers clearly identified and documented?

- Document warranty information for each asset and review monthly for upcoming renewals.

- Document main software and feature revision levels.

- Do you have a strong policy for remote access to pbx equipment for internal or vendor use?

- Review common product installation and configuration standards (build docs) and verify they are current for your production hardware and software.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

• Review documented procedures for updating/moving/decommissioning hardware and software.

• Are voice related systems appropriately represented in your corporate security policy?

• Are guidelines clearly spelled out on how to handle abusive phone calls – both incoming and outgoing? Are one or more people designated to work with law enforcement on investigations/subpoenas?

Section 3. Security Procedures

• What physical security is in place for the pbx or admin terminals? Physical security is just as important on a pbx as it is on a router or switch. Make changes if needed.

• What procedures are used to verify software updates are legitimate and have not been tampered with?

• Are there automated alerts for voice network or pbx component failures? Even basic monitoring should be possible using free SNMP or Linux Mon utilities. Any off-line time should be investigated in the event someone has breached your physical security and installed an update that required disconnecting all ports, re-initializing, or re-booting.

• Remote administration ports on the pbx and voicemail systems should be protected with a third-party security device or dial-back features. Better yet, remote administration ports should only be connected and used when absolutely necessary.

• Does a voice incident response plan exist to define the procedure/approvals needed to reduce services or sever connections in the event of a security incident?

Section 4. Countermeasures to known hacks/illicit use

• Record an automated greeting "You have reached the XYZ company voicemail system" that is played before all mailbox personal greetings. This will stop most 3rd party collect call billing attempts.

• Review voicemail password strength and change policies. Make adjustments if necessary to insure passwords are changing on a regular basis. Insure a # or * is needed at the end of all password entries so that length is not given away. Also verify a password must be entered on its own rather than as part of a larger string of characters.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

• Disable all out dialing or thru-dialing functionality. If this is absolutely necessary, try and put as many restrictions as possible on the system – only certain users, certain times, etc. by using class of service tables within most pbx systems. Budget for a two-factor integration platform such as SecurePBX from RSA to help safeguard this feature, if it is absolutely needed.

• Block all international calls, or greatly reduce the number of users that can dial internationally to the bare minimum. This should reduce the monetary damage a hacker can do in the event your security is breached.

• Block Caribbean area codes for the same reason as above. An area code lookup for all North American exchanges is available at http://www.nanpa.com The following is a starter list for suspect Caribbean nations. :

242 Bahamas
246 Barbados
264 Anguilla
268 Antigua & Barbuda
284 British Virgin Islands
340 U.S. Virgin Islands
345 Cayman Islands
441 Bermuda
473 Grenada
649 Turks and Caicos Islands
664 Montserrat
758 St. Lucia
767 Dominica
784 St. Vincent and Grenadines
787 Puerto Rico
809 Dominican Republic
868 Trinidad and Tobago
869 St. Kitts and Nevis
876 Jamaica

• Is your Helpdesk trained to recognize the early signs of toll fraud or a pbx intrusion – excessive hang-ups, wrong number calls, and locked out voicemail boxes? Do they know how, who, and when to escalate suspect events as callers alert them of potential problems?

• What tools are available for dealing with PBX incidents? Are these likely to prevent or limit the damage that will be done by an attacker in real time? If not, research outside products that may be able to supplement current tools with more thorough and responsive information.

• For all important outside access numbers – central voicemail, DISA lines, remote administration lines – is each device programmed to wait several

© SANS Institute 2003, Author retains full rights.

seconds after answering before responding? Many hackers will look for tones or standard greetings during war-dialing activities.

• Are inactive/idle timeout values set on core devices? Using low values reduces the amount of time these sessions are available if an administrator forgets to log out or is unexpectedly called away from an administrative session.

• Verify how administration and maintenance ports are configured. Are appropriate passwords in place? Are dedicated ports in use, if possible? Are remote access lines kept inactive or unplugged unless needed?

• What is the logging situation with respect to all major voice systems? First, are thorough logs generated for administrative and billing issues that may arise later? Is logging centralized to one console, or is a process in place to easily review separate logs for trending and suspicious activity? If logs are to a mainframe printer, is this device secured from view from all but administrative staff?

• Is receiving and evaluating vendor and CERT advisories formally assigned as a work task to one or more individuals? If so, what mechanism is in place to verify compliance?

• Are DISA lines in use? If so, are the access numbers out of range of the normal corporate dial plan to prevent discovery via war-dialing? Is there a regular process in place to change this number from time to time? Are access codes sufficiently long to prevent random hacking and are they changed on regular basis?

• If automated attendant programs are used, are they restricted to only forward calls to internal extensions?

• Review allowed call forwarding in the environment. Is call forwarding limited to internal extensions only? If outside forwarding is allowed, is it restricted to local numbers only? If not, a number could easily be forwarded to provide free long distance services for an attacker or rogue employee.

• Are direct trunks accessible via security codes from end stations? If so, consider restricting this feature so that no regular user could guess the code and receive an outside dial tone, bypassing your pbx security and logs.

• Are 1010 dialing and outside operator assisted calls blocked? This is another way intruders can attempt to work around any long distance and international blocks you have put in place.

• Are any services or equipment shared with other tenants or companies? If so, are proper security and confidentiality agreements in place to protect both parties?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References.

[i] Waldrop, Brian L., "Securing the Other System: Basic PBX Functionality and Vulnerabilities", April 24, 2001, http://rr.sans.org/telephone/PBX.php

[ii] AT&T, "AT&T Fraud Education", 2002, http://www.att.com/fraud

[iii] Working Assets, "Securing Your Office Phone System from Voice and Data Network Fraud", 2002, http://www.workingassets.com/business/fraud.cfm

[iv] Bergman, Steven R., "Toll Fraud", October 1994, http://www.teleconvergence.com/art_tollfraud.html

[v] Jainschigg, John, "Securing Your Switch", April 2002, http://www.cconvergence.com/article/CTM20020404S0012

[vi] Jainschigg, John, "Securing Your Switch", April 2002, http://www.cconvergence.com/article/CTM20020404S0012

[vii] National Institute of Standards and Technology, "PBX Vulnerability Analysis", August 2000, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

[viii] Working Assets, "Securing Your Office Phone System from Voice and Data Network Fraud", 2002, http://www.workingassets.com/business/fraud.cfm

[ix] National Institute of Standards and Technology, "PBX Vulnerability Analysis", August 2000, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

[x] Barnes, Stephan, "M4phr1k's House of Voodoo – Voicemail Hacking Section", October 2002, http://home.mminternet.com/~barneshouse/Voicemail.htm

[xi] National Institute of Standards and Technology, "PBX Vulnerability Analysis", August 2000, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

[xii] Cohen, Dr. Frederick B., "Protection and Security on the Information Superhighway – Ch. 5", 1995-97, http://www.all.net/books/superhighway/aspects.html

[xiii] Goku, Sen - ed., "Australian Phreak Scene, vol. 1 issue 2, 4/10/1995, http://web.textfiles.com/ezines/APS/apsv1i2.txt

[xiv] Walker, Thai, "Thieves rack up city's phone bill", November 4, 2002, http://www.bayarea.com/mld/mercurynews/news/local/4439758.htm

[xv] Working Assets, "Securing Your Office Phone System from Voice and Data Network Fraud", 2002, http://www.workingassets.com/business/fraud.cfm

[xvi] Milligan, Bernie, "Gateways to Toll Fraud", 1996, http://www.claypro.com/CTF/GATEWAY.html

[xvii] National Institute of Standards and Technology, "PBX Vulnerability Analysis", August 2000, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

[xviii] Waldrop, Brian L. "Securing the Other System: Basic PBX Functionality and Vulnerabilities", April 24, 2001, http://rr.sans.org/telephone/PBX.php

[xix] Federal Trade Commission, "Toll-Free Telephone Number Scams", May 1997, http://www.ftc.gov/bcp/conline/pubs/tmarkg/tollfree.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced