Voice over Internet Protocol (VoIP) can provide cost savings and increased flexibility for your business that other voice systems can't match. But it also comes with a number of potential security threats that need serious consideration. An experienced VoIP provider like IntelePeer can help you minimize your security risks in VoIP environments.

From detailed security threats to best practices to what to expect from a support team, we've created this guide to help you understand how to minimize security risks before making a large investment with any particular service provider.

Pre-Deployment Considerations

Professional hackers have found it extremely profitable to exploit VoIP PBX for weaknesses. When they find them, they have the capability to make almost unlimited chargeable calls very quickly.

Understanding the ins and outs of VoIP security may sound complicated, but it's not as hard as you think. With a little due-diligence and few precautionary steps, your business environment will be fully protected.

Fortunately, IntelePeer has specialized engineers who are able to put a number of measures in place to help minimize risks, ensuring security.

GET STARTED

Common Security Threats

As industrial-grade scanners continuously look to exploit weaknesses in your VoIP environment, you must know which kinds of potential attacks to watch for. Below is a list of the most common types of VoIP PBX attacks.

Call Interception

During setup, data passes – unencrypted – through VoIP gateways. When an attacker identifies the stream's source, he can gain physical access to a segment of the LAN, allowing him to hijack the signal and listen to your calls.

Not surprisingly, unsecured wireless networks are at higher risk for call interception. That's why most enterprises use Ethernet switches, rather than hubs, to limit the number of locations for a possible exploit.

Signaling Manipulation

Hackers use a variety of tools to manipulate signals. Two of the more popular methods are "BYE teardowns" and "equipment reboots."
In the case of a BYE Teardown an attacker notices a call signal, then spoofs a "BYE" message to each user agent (UA) on the call, effectively ending or "tearing down" the call.

Another popular manipulation technique is to signal an equipment reboot. This is achieved by the attacker sending a NOTIFY/check-sync signal to the UA, causing phones to reboot. This renders most devices inoperative.

Denial of Service Attacks

A DoS attack – achieved by flooding the network with large amounts of data to disrupt services – is an attempt to make your network unavailable to users.

Some DoS attacks are carried out by multiple computers to achieve a far more devastating effect. These are referred to as a "distributed denial of service" attacks (DDoS). A DDoS attack may target different areas of your network leaving some unharmed; however, if your VoIP infrastructure is directly connected to the primary network, it may be affected as well.

While these attacks may not bring down the entire network, they will cause increased latency, jitter, and packet loss, creating delays or loss of service.

Caller ID Spoofing

Put simply, this is the practice of making fake phone numbers appear on caller ID to appear to be from trustworthy sources. Open source software has not only reduced the cost of spoofing, but has also made it easier than ever.

Seeing a seemingly legitimate number – like one from a financial institution – on their caller ID, victims willingly share personal or confidential information that can be used in future data breaches.

Spamming over Internet Telephony (SPIT)

Capitalizing on the ubiquity of computer-based VoIP systems, spamming over Internet telephony (SPIT) is the process of sending massive amounts of voice spam to large numbers of VoIP users. Much like email spam, unsolicited messages are delivered in bulk to VoIP users.

Difficulty to trace these calls over IP networks means high fraud potential. Session initiation protocol (SIP) is often the most exploited system.

Vishing

Phishing is a term long used to describe the practice of "baiting" unknowing victims into providing personal information such as credit card numbers, social security numbers, and passwords by pretending to be a trusted source. Voice Phishing – Vishing – takes this concept a step further.

Because of the public's trust in landline services, vishers are able to manipulate common VoIP features like caller ID (providing false numbers) and interactive voice response systems (IVR) to trick victims into providing sensitive information. These types of attacks are extremely difficult to trace.

Viruses and Malware

Malware is an all-encompassing term used to describe a variety of malicious and intrusive software. Viruses, spyware, adware, worms, and trojans are just a few example of malware.

These programs are capable of leaking VoIP credentials or opening backdoors, giving hackers the capability to take down entire VoIP networks.

Registration Hijacking

Registration hijacking occurs when an attacker disables a valid SIP registration and replaces it with their IP address. This lets them intercept, reroute, replay, or terminate calls as they wish, all without the user knowing the call has been hijacked.

Man-In-The-Middle Attacks

By inserting himself in the middle of a conversation, the attacker secretly relays messages between two parties, neither knowing the hacker has entered the conversation. The eavesdropping attacker is able to gather sensitive data meant for someone else, with both parties none-the-wiser.

War Dialing

War Dialing is a method of auto-dialing large volumes of phone numbers in an attempt to identify and sort out computer answering systems, fax numbers, and humans. Depending on the number of rings before an answer, the system makes a note, providing hackers with a more defined list of potential entry-points. This allows them easier access to breach and corrupt entire systems and networks.

Exfiltration of Data

Unlike other packet formats, it's hard to detect hidden content or data in VoIP packets without causing delay to the entire data stream. Because of this, attackers are able to use VoIP trojans to extract confidential data from corporate networks during RTP sessions. These types of attacks are extremely difficult to prevent, as firewalls allow VoIP traffic to pass unimpeded.

Security Best Practices

As long as telephone lines have existed, people have been finding ways to attack them. Now, with the emergence and growth of VoIP, those attacks are becoming more frequent, and in some cases, easier to pull off.

Whether attackers are looking to reroute calls, steal free minutes, or enact fraudulent schemes, you must take precautions to safeguard your and your customers' personal information and data.

Now that you understand the types of threats your VoIP network faces, it's time to start protecting yourself. The following list of security best practices can help.

Importance of Session Border Controllers (SBCs)

Session border controllers manage the signals coming into your VoIP devices, like a guard at the castle gates. Developed explicitly for voice traffic, SBCs have the same built-in security features as a standard network firewall, giving your VoIP services an added level of protection. Despite some dissenting opinions, SBCs are still the best way to protect your VoIP environment.

General Security Measures

Session border controllers manage the signals coming into your VoIP devices, like a guard at the castle gates. Developed explicitly for voice traffic, SBCs have the same built-in security features as a standard network firewall, giving your VoIP services an added level of protection. Despite some dissenting opinions, SBCs are still the best way to protect your VoIP environment.

VPN

Using an encrypted Virtual Private Network (VPN) is a safe way for remote users (e.g. home workers) to access your network securely. With a VPN, employees access the network using a specific password. Traffic is encrypted to prevent would-be hackers from monitoring and capturing data from remote locations.

Patches

As new system vulnerabilities are discovered – oftentimes weekly – it's becomes extremely important to run the newest operating system patches. Check regularly for software/firmware updates. PBX manufacturers or resellers often provide recommended firmware versions; check with them.

Unused Services

Attackers looking for weaknesses may be able to exploit unused services. Disabling unused services will help to fortify your system from any unnoticed attacks. For example, if your voicemail system isn't being used, disable it.

Wi-Fi

Open wireless access presents its own set of vulnerabilities. Be sure to use secure encryption systems like WPA2 to keep unknown users off your network. Using password best practices will also help to ensure security (see above).

Management Interfaces

Attackers can find "open" ports in your network, sometimes through a simple Google search. Secure all VoIP systems (PBX, phone, etc.) behind an SBC (see above) to prevent remote access or call rerouting from hackers.

Passwords

Any VoIP device with a configuration interface – phones, PBXs, IP phones, soft clients, workstations, and other networked devices – needs to implement strong password practices to remain protected. This can be achieved in a number of ways:

- ☑ Create a strong password policy requirement for all PBXs
- ☑ Change default passwords immediately
- ☑ Encourage employees to create unique passwords by:
  - Joining two or more familiar words that tell a memorable story (e.g. itrimtrees, mydogskippy)
  - Include numbers and letters (e.g. 10derh3art, 5plus2equals7)
  - Use an 8 character minimum. 12 or more is better.

Using weak or default passwords – or worse, no password at all – will leave your system vulnerable to attackers. Simple passwords like strings of numbers (1111 or 1234) or personal numbers (home address, partner's name, car registration) can be easily guessed or discovered by would-be attackers and should be avoided at all costs.

Mobility Services

While it may be convenient to forward office calls to home or mobile numbers using remote services, it also creates new vulnerabilities. The same feature that forwards those calls can be used by attackers to reroute calls to premium numbers or make unauthorized calls at the user's expense.

Mobile VoIP

As VoIP use on smartphones becomes more common, so should security considerations. In the event of a lost or stolen phone, configuration of the phone's access PIN can prevent unwanted access to content.

Likewise, the use of encryption services for remote VoIP phones – especially those utilizing public Wi-Fi – will provide additional security.

Call Limits

Asking the Internet telephony service provider (ITSP) to place limits on premium rate and international call destinations may help detect fraudulent activities. If patterns of fraud are detected, a notification is issued to you, asking for authorization of additional spend.

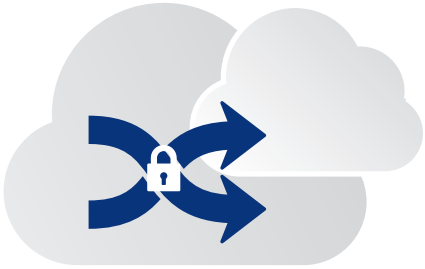
Lock Down the PBX

Because VoIP phones can register with a PBX from anywhere in the world, it's important to consider limiting registrations to a specific office network. Some phones can be secured with passwords, IP addresses, or MAC (physical) address.

It can also be good policy to grant access to specified users or only allow preconfigured VoIP phones access. *To put it another way: deny access by default and create exceptions for authorized users.*

Securing Connections from Dynamic IP Addresses

Users running VoIP apps on mobile, those working from home, and roaming users who connect via Wi-Fi will all connect from dynamic IP addresses – something that cannot be avoided. Fortunately, there are a number of precautions you can take to increase network security:



- ☑ Ensure that authentication for all user accounts is enabled
- ☑ Use password best practices (see above)
- ☑ Check that the PBX requires and enforces authentication for a wide range of operations
  - At a minimum, user agent registration (SIP REGISTER) and call set-up (INVITE) must be authenticated.
  - Other operations such as call termination (BYE), presence, and voice mail notification (SUBSCRIBE/NOTIFY) should also require authentication. These authentication requirements apply to both internal IP phones and remote users, as an attacker will target both.
  - If the PBX cannot authenticate the full range of protocol operations, or if it is not practical for it to do so, consider using a security gateway to provide the full range of authentication services.
- ☑ Whether using a direct dedicated connection or public Internet, you'll want to enable encryption for remote and roaming users through an SBC. Configure it to only allow encrypted VoIP traffic from dynamic IP addresses. This greatly reduces the risk of unauthorized access to your PBX.

VoIP Encryption

VoIP encryption provides additional security for remote and roaming users who connect from dynamic IP addresses. It will also protect against a wide range of attacks that rely on the monitoring of VoIP calls (offline password recovery attacks, call termination attacks, denial of service attacks, etc.) and defend against eavesdropping attempts.

Many VoIP vendors now offer call encryption services that are superior to fixed-line and cellular networks. This includes softphone services available for laptops, mobile phones, and tablets. And while only a few IP-PBXs support call encryption, a good SBC can provide sufficient security.

SIP standards specify the use of TLS for signaling encryption (call set-up) and SRTP for media encryption (audio or video streams).

- ☑ TLS is the same protocol used to access banking websites
- ☑ SRTP is designed specifically for encrypting VoIP calls.

Securing VoIP Devices

The ability to connect to the internet and place calls from anywhere in the world is one of VoIP's greatest advantages. Unfortunately, this capability also presents increased security risks. With a little effort, however, these risks can be minimized.

- ☑ Modern routers and most corporate hotspots have a firewall in place for guest logins. Be sure to ask.
- ☑ Previously set up devices log themselves into the service provider's telephone network using saved account numbers and passwords. Unknown users who obtain this information can use it to login from their own phones. Keep this information secure. (See section three for advice on passwords/PINs.)
- ☑ Usernames and passwords should be erased when phones are discarded. Log-on to the device's web page and remove this information manually. A factory reset is even better, as it also removes the call directory and call records.
- ☑ For softphones, remove the password and then uninstall the application. When disposing of a PC or laptop, it is good practice to format the disk or even to remove and destroy it.
- ☑ If VoIP service is no longer in use, delete any credit cards on file and cancel the account.
- ☑ Keep both PC and phone software up-to-date (see "Patches" section above).

Service Provider Support

Most IP-PBX attacks are fraud-driven. The attacker makes expensive calls to international destinations or to premium rate numbers, profiting from the additional charges. Because these attacks render call restrictions and local policies useless, it is important to work closely with your service provider. Creating additional, external layers of protection is key to your security.

IntelePeer is well versed in VoIP security and has a number of safeguards in place to help combat fraud. Furthermore, IntelePeer has a well-documented record of and commitment to security. Below are two ways IntelePeer supports customer security.

Call Barring

You may wish to block calls to/from certain countries, numbers, or area codes. For example, if you do not need to make international calls, IntelePeer ensures this feature is not available to your business.

Fraud Alerts

IntelePeer monitors its network using practices like proactive call screening and alert procedures to prevent fraudulent abuse, reduce fraud exposure, and prevent unauthorized access. We also share the latest fraud trends with our customers.

If suspicious calling patterns are observed (long duration international calls, international PBX fraud, and calls terminating to known "high fraud" countries), IntelePeer's Customer Service organization makes all reasonable attempts to alert the customer of the suspected fraud.

In the event that the customer does not respond, IntelePeer disables the affected trunk group (to maintain the integrity of the network) until the customer is reached.

Are You Ready?

Check **to see if you're ready for VoIP security with the the complete checklist on the next page.**

IntelePeer's highly trained engineers and fully encrypted network can help you reduce the risk of a cyber-threat or full out attack on your VoIP network. Find out how IntelePeer can enhance and secure your communications.

CONTACT US *to Learn More*

VoIP CHECKLIST

Server

- ❒ Restrict access to those services which you do not use.
- ❒ Harden the IP-PBX server for deployment, with unnecessary services disabled.
- ❒ Disable SSH Root access with SSH login via Secure Key and change default ports (i.e. use 4245 for SSH not 22, etc.).
- ❒ Install the IP-PBX system in a secure location with restricted access.
- ❒ Limit max trunk calls and max calls per extension to your requirements.
- ❒ Update your server's operating system and ALL associated software to the latest version. Make sure ALL of the latest security patches enabled.

Passwords & Access

- ❒ Change ALL default passwords to unique passwords
- ❒ Ensure ALL passwords, including extension passwords, are complex. If possible, require alphanumeric passwords with as many digits as the system allows.
- ❒ Limit maintenance port access to those with passwords.
- ❒ equire that passwords and access codes are changed regularly.
- ❒ Delete/change former employees' passwords immediately following separation.
- ❒ Set access PIN on smartphones that will use VOIP.
- ❒ Limit external access to known IP's only.
- ❒ Consider limiting call types (access to international/premium rate numbers) by extension.
- ❒ Limit VOIP registrations to office network.
- ❒ Ensure all non public-facing extensions are only accessible via your internal network (i.e. devices that do not need to use public IPs for registration). This ACL-type limitation can be done at both the extension and trunk levels.
- ❒ Block access to unallocated mailboxes on the system; change default PIN on unused mailboxes.

Security Checks

- ❒ Enable VoIP logging to monitor activity.
- ❒ Check firewall logs weekly to identify potential threats.
- ❒ Be vigilant for evidence of hacking. (The inability to get an outbound line is usually a good indicator of high volumes of traffic through your system. Check for calls outside business hours.)
- ❒ Regularly analyze billed calls by originating extension to identify irregular usage and unexpected traffic.
- ❒ Assess security of all PBX peripherals/applications regularly: platform, operating system, password and permissions scheme. Carefully evaluate the security of any onboard remote management utility (e.g. PC Anywhere) for possible holes.

Enable a backup routine

- ❒ Back-up your system at least once every 30 days.