ITSPA

Internet Telephony Services Providers' Association

Recommendations for secure deployment of an IP-PBX

Version 2

November 2013

Contact: admin@itspa.org.uk

Contents

Introduction

ITSPA takes the safety of its customers seriously. Telephony systems using VoIP bring many benefits in cost and flexibility, but in common with many of today's advanced technologies, there are also threats. In 2010, ITSPA formed a security committee to discuss best practice and create advice for its own members and for customers of IP telephony systems. We distilled some of the best practical advice from service providers, security experts and vendors and used it to create this document.

The security measures outlined in this document include configuration measures that should be implemented on an IP-PBX installed in customer's premises as well as Service Provider support available from ITSPA members to assist in the identification and avoidance of an attack.

The recommendations in this document are relevant for IP-PBX installations; please refer to the ITSPA Security Documents for recommendations to secure Hosted Telephones.

ITSPA has its own Quality Mark that recognises ITSPA members that aspire to be the best in their field. Part of qualifying for this Quality Mark is the adherence to best practices, and this includes the area of VoIP security. When you choose a service provider with the ITSPA Quality Mark, you are choosing a partner that has a deep understanding of VoIP issues, and a commitment to delivering services of the highest quality and safety.

Health Warning!

Before you set off to build your own VoIP PBX you need to be aware that whilst it's relatively easy to set up a PBX, keeping it safe is not at all easy.

Because your PBX can make almost unlimited chargeable calls very quickly, it is a high worth target for professional hackers. All VoIP PBXs are found and scanned for weaknesses within hours of connecting to the internet and continuously thereafter.

So, unless you, or your engineer, fully understand what you're doing and are prepared to keep your PBX permanently maintained, you are putting yourself at financial risk and you should go no further.

Instead, think about using a hosted VoIP or fully managed service from an established ITSPA member where any risk is borne by them, not by you.

Checklists

During Setup

1. Subscribe to security mailing lists for all vendors that your solution encompasses.
2. Set up a regular calendar of maintenance that is relevant to your installation
3. Keep a list of all hardware and software assets with versions of software / firmware.

Regular Checks (ideally daily)

1. Check security mailing lists for new vulnerabilities and apply recommend fixes
2. Check firewall logs
3. Check call logs for any unexpected call traffic
4. Check network graphs for any unexpected traffic

We hope that you enjoy this paper, which gives our practical security advice and recommendations for VoIP systems. We of course welcome your feedback.

The Current Situation

There are industrial-grade scanners operating around the clock to find and exploit IP-PBX's and hosted handsets that are not secured or running the latest firmware.

Any PC or Network with direct access to the Internet must be secured, using strong passwords, network security, firewalls and by disabling unnecessary services; deploying an IP-PBX is no different.

Before exposing an IP-PBX on the Internet you *must* ensure that it is secured against malicious attacks.

a. Current Security Issues and Attacks

The following security issues and attacks have been observed on many standard VoIP implementations.

- General scanning and directory scanning (including extension enumeration).
- Phone Hacking (for example, discovering account secret or exploiting software vulnerability).
- Man-In-The-Middle attacks (including eavesdropping and injection of audio).
- Denial-of-Service, DoS, (including SIP *INVITE*/*REGISTER* flooding and fuzzing).
- Session manipulation (including hijacking, tear down and redirect).
- Equipment reboot (including *NOTIFY*/*check-sync* messages sent to *User Agent*, causing a reboot).
- SPIT, Spam over Internet Telephony (e.g. unsolicited audio sent to phones or voicemail)

b. Current Vulnerabilities that Contribute to Security Issues

The following vulnerabilities significantly contribute to the current security issues associated with VoIP.

- Relying on implicit trust relationships; there is no mutual authentication as standard.
- Plain text signalling protocol (SIP); there is no method of obfuscation or encryption as standard.
- Raw media protocol (RTP); there is no method of encryption or obfuscation as standard.

- DoS possibilities at multiple levels; disrupting the network and/or application layer.

Network Security

If you have a network that connects to the Internet, then this is a potential door for attackers to get in. It is worth considering a few basic aspects of security to protect yourself as much as possible.

- **Firewalls**. A firewall sits at the border between your network and the Internet. It limits what attackers on the Internet can "see" inside your network, and controls the kinds of traffic that can flow in and out of the network. Some firewalls provide reporting and statistics so that you can see what is going on. ITSPA highly recommends that you use a firewall. This could be a general purpose IP firewall or a specialist security gateway.

- **Passwords**. Never leave any system with the default or factory password. Attackers know these passwords, and this is the simplest attack. If your users choose their own passwords and PINs then try to discourage them from using obvious passwords, or ones that are easy to guess if you know a little about the person (e.g. car registration, partner's name etc.). PIN numbers like 1111 or 1234 are obviously a bad idea. Here are a few strategies for picking "strong" passwords:
  - Join two or more words, perhaps that tell a story that the owner will remember, e.g. bonsaitreecare, blacklabrador
  - Include numbers as well as letters in the password, e.g. 10terhooks, 5after12
  - Use longer passwords, 8 characters is a minimum, 12 or more is better. These types of password are more resistant to "dictionary" attack, where an automated system tries to log on many times, using a list of common words and logins, e.g. 12345, pa33word, etc.

- **VPN**. An encrypted Virtual Private Network is a way for remote users (e.g. home workers) to access your network securely. Access is via a password, and traffic is encrypted so that no-one on the Internet can monitor and capture your data.

- **Management Interfaces**. Any device that has a configuration console or remote control of some kind should be secured behind your firewall and accessed via VPN. Control ports left 'open' on the Internet can easily be found, in some cases even using a simple Google search.

- **Patches**. Keep systems up-to-date with operating system patches. New system vulnerabilities are being found every week, so it is important to patch systems regularly.

- **Unused Services**. Disable any unused services in order to avoid misuse. For example, if you don't use the voicemail system, disable it, as an attacker might exploit a weakness to gain access to further services.

- **WiFi**. Wireless brings its own set of system vulnerabilities. If you allow WiFi access, make sure that you use a secure encryption system (like WPA2) to make it difficult for strangers to join your network, and choose a secure passphrase (see passwords, above).

Remember that there is always trade-off between security and convenience. Allowing remote use of systems (such as VoIP phones for home workers) creates new and flexible ways of working. Shutting off remote VoIP phones makes the system much more secure, but also removes a lot of value from your organisation. It is better to strike a reasonable balance.

VoIP Security

In general, people attack voice systems because they represent a source of money. This is nothing new and hackers (crackers, phreakers, call them what you will) have been attacking company telephone systems for decades, even before VoIP came along. An attacker may just be trying to get some free long distance calls for himself, but there are also organised criminals who want to use your telephone system to route international calls at your cost. Some may route calls to premium rate numbers (which they have set-up) in order to make money. In any case, the result is the same: your phone bill is increased, and the money is in their pocket. Attacks to get free calls are known as toll fraud attacks, whereas attacks to call premium rate numbers are known as revenue share fraud, and usually International Revenue Share Fraud (IRSF).

To make VoIP secure, you should first make sure that you have basic network security. Your VoIP system consists of elements like a PBX (for example Asterisk), and VoIP phones or ATA's (devices that convert a conventional phone to VoIP). Each of these devices are often fully functional computing devices that have web interfaces and configuration screens, and you need to consider how to secure each device as you would secure a desktop PC. ITSPA thinks that these are the most important issues to consider:

- **Passwords.** Secure all VoIP devices that have a configuration interface, including phones, PBX's and ATA's. See section 3 for advice on choosing secure passwords. Reinforce the use of strong passwords on VoIP phones with a policy on the PBX to require passwords on all phones. Leaving just a single phone with a default password, weak password or worse still no password significantly increases the risk of a toll-fraud attack.

- **Management Interfaces**. Secure VoIP systems (PBX, phone, etc.) behind your company firewall. Remember if someone can reconfigure these systems remotely, then there is a possibility to reroute calls to international destinations or to premium numbers.

- **Mobile VoIP**. If you use VoIP from smartphones (which is increasingly common), then do configure the access PIN on the phone. Mobiles get lost and stolen, so you should prevent the phone being used (for services including VoIP) with a PIN. Many phones have a feature to automatically erase phone content after a PIN has been incorrectly entered a number of times. Consider using encryption services for remote VoIP phones, especially if these remote phones connect via public WiFi hotspots. Even if you not consider that your phone calls are sufficiently confidential to need this level of secrecy, encrypting VoIP traffic can provide some valuable additional security controls.

- **Mobility Services**. Think carefully about services that you want users to have access to remotely. For example, it can be very useful for remote users to be able to reconfigure call forwarding features, so that calls are forwarded to home or mobile numbers. The flipside of this is that an attacker might use the same feature to reroute calls to a premium number. Any service that allows a remote caller to get back to the PBX "dial tone" has potential for making unauthorised calls at your expense.

- **Lock down the PBX**. Potentially a VoIP phone can register with a PBX from anywhere in the world. You may choose to limit registrations to within your own office network, or only allow preconfigured VoIP phones access. You may be able to secure phones via password, IP address or MAC (physical) address. A good policy to grant access to specified users, i.e. deny access by default, and create exceptions for authorised users.

- **Unused Services.** Disable any unused services on your VoIP PBX in order to avoid misuse.

- **Patches**. Just as with network systems (see section 3), VoIP components also have vulnerabilities that can be fixed with periodic software/firmware updates. Your ITSP may have recommended firmware versions; check with them.

- **Call Limits**. Your Internet telephony service provider (ITSP) may be able to provide services that protect you from overspend on your telephony service. For example, they may be able to limit calls to premium rate and international destinations. Some ITSPs can detect patterns of fraud, e.g. uncharacteristic repeated calls to overseas destinations and automatically prevent calls until you authorize the extra spend.

Your Internet telephony service provider (ITSPA member) will be able to provide more detailed information on any of these topics, and may also be able suggest companies that can help you to secure your systems.

Using Firewalls to Protect Traffic

All VoIP interconnections should be protected by a firewall. ITSPA considers a firewall to be the absolute minimum requirement for security, but beyond this minimum you should consider a layered approach, as we describe in this document. There are a number of different types of firewall ranging from network firewalls designed primarily to secure data applications to specialist devices designed for VoIP and specifically for the Session Initiation Protocol (SIP). These specialist devices are sometimes described as enterprise SBCs. The appropriate choice will depend on the types and origins of VoIP interconnections. All customers will need to handle VoIP traffic to and from their service provider, but an increasing number are using VoIP to provide connectivity to remote offices or to home users or roaming users. Each of these interconnections pose different security threats.

Configuring a network firewall to handle VoIP traffic is not as simple as allowing other services such as web and email. This is because VoIP protocols are more complex, because VoIP is sensitive to Network Address Translation (NAT) and because VoIP uses dynamic ports. Some customer organisations having strict security policies governing their firewall configuration may find that the configuration needed to enable the required VoIP services falls outside of this policy. These customers or any customer finding it difficult to correctly configure their firewall should consider a specialist security device.

Network Firewalls

The following guidelines apply to service providers, PBX equipment and user agents.

a. Secure Connections from Dynamic IP Addresses

It is not always possible to limit VoIP interconnects to static IP addresses. Most home workers will use a standard domestic broadband connection, virtually all of which use dynamic IP addresses. Roaming users connecting from WiFi hotspots and users running VoIP apps on mobile devices will all connect from dynamic IP addresses. Where connections from dynamic IP addresses cannot be avoided ensure that authentication for all user accounts is enabled and those robust passwords are chosen as discussed elsewhere in this document. Check that you PBX requires and enforces authentication for a wide a range of operations as possible. At a minimum, user agent registration (SIP REGISTER), and call set-up (INVITE) must be authenticated. Other operations such and as call termination (BYE) and presence and voice mail notification (SUBSCRIBE/NOTIFY) should also require authentication. These authentication requirement apply to accounts used for both internal IP phones and for remote users, an attacker will target both categories. If you PBX cannot authenticate the full range of protocol operations or if for other reasons is not practical to configure it to do so, consider using as specialist security gateway that can provide the full range of authentication services.

For additional security consider enabling encryption for remote and roaming users. The firewall can then be configured to allow only encrypted VoIP traffic from dynamic IP addresses. VoIP encryption is discussed in more detail in section X.

b. Connections to Trunk/Interconnect Providers

Where possible use a direct, dedicated connection for trunk/interconnect connections with your provider. A direct dedicated connection will greatly reduce the risk of a range of security threats.

Whether using a direct dedicated connection or the Internet, you should use a firewall. Configure the firewall to allow only authorised interconnect traffic to and from the trunk/interconnect provider; this reduces the risk of unauthorised access to your PBX.

c. Restrict the Media Port Range

VoIP calls are established by a signalling protocol (SIP) which sets up the call and negotiates the network ports used for the media streams. The ports used for the media streams are chosen dynamically. A firewall must be configured to allow the media streams otherwise there will be no audio on calls. The simple approach to this is to allow the full UDP port range, 1 to 65535. Opening such a large port range weakens the firewall's security controls and in many organisations will not be permitted by the established security policy. Where possible restrict the range of ports used by media streams. Most IP-PBXs can be configured to set and upper and lower limit for the media ports. Set a range appropriate for the expected maximum number of concurrent calls (allowing to ports for each call) and configure the firewall to allow only the selected port range.

For additional security, consider using a specialist VoIP security gateway that monitors the signalling (call setup) traffic and dynamically opens the media ports used by validated and authenticated calls.

d. Protecting Management Interfaces/Control Ports

In telephony systems, we use a variety of management interfaces/control ports to configure devices, including user agents and PBX equipment. It is essential to protect these from unauthorised access.

ITPSA recommends using a firewall to protect management interfaces, which greatly reduces the risk of unauthorised access. Configure your firewall to allow access to these management interfaces only from authorised IP addresses.

Advanced Firewall Appliances

The following guidelines apply to both PBX equipment and user agents.

a. SIP Security Gateways

SIP Security Gateway appliances have been designed to be aware of how SIP/VoIP communication works; in this way, they offer a wider range of security benefits over traditional firewall types. A good SIP Security Gateway will offer a number of enhanced security controls including:

- Dynamic IP Firewall controls avoiding the need to configure a large open port range
- Application level security controls recognising common attacks
- Blacklisting know sources and call patterns
- Enhanced authentication services
- Call encryption
- Transparent network address translation and far-end NAT traversal processing.

The features and capabilities offered by SIP security gateways vary between models. We therefore recommend that you seek advice from vendors or security specialists before deploying one.

b. VoIP Encryption

The SIP standard allows both signalling (call set-up) and media (audio or video streams) to be encrypted. The standard specifies the use of TLS for signalling encryption and SRTP for media encryption. TLS is the same as the protocol used to sure access to website providing on-line banking or other services needing encryption. SRTP is designed specifically for encrypting VoIP calls. It is a light weight but secure encryption protocol that avoids the overhead associated with VPN technologies designed primarily for data. Many IP phone vendors now offer call encryption and most soft-phone available for laptops, mobile phones and tablets include encryption. While only some IP-PBXs support encryption, a good SIP Security Gateway will handle encrypted calls.
Encrypting VoIP calls provides many benefits including:

- Additional security for remote and roaming users connecting from dynamic IP addresses.
- Protection against a wide range of attacks that rely on monitoring VoIP calls, these include off-line password recovery attacks, call termination attacks and a range of denial of service attacks.
- Protection against unauthorised eavesdropping.

Call encryption is an area where VoIP can offer a superior service over fixed line and cellular networks. There are a number of documented, although illegal, techniques for monitoring calls on cellular networks. Where call privacy is important VoIP offers a simple and cost effective mechanism to encrypt calls.

Security Tips for VoIP Devices

Most IP-PBX installations use VoIP telephones installed on workers' desks. One of the great benefits of VoIP is that you can take your telephone anywhere in the world, plug it into the Internet and it will work exactly as it did back home or in your office, which has many advantages but it also brings with it some security concerns.

Additionally, VoIP telephones and adapters are powerful online computers so need some protection from external attack, just like your PC.

But don't worry, the security precautions you need to consider are simple and common sense and you already have what you need to apply them. (NB: almost everything discussed below applies also to users of softphones on PCs and Macs.)

1. Use an ITSPA member with a Quality Mark as your service provider. You can then be certain that your service provider follows industry best practice.

2. Any modern router (that connects you to the Internet) will have some kind of integrated firewall. This means that you start off with a high level of protection against attacks from the outside world. (But if your router is getting on a bit it may be worth getting a modern one and certainly worth checking that its firmware is up to date.)

3. Your device normally contains a username or account number plus a password, which it uses to log itself into your service provider's telephone network. Keep this password safe because it can be used by anybody anywhere to make phone calls from their own phone if they can get their hands on it. See section 3 for advice on passwords/PINs.

4. If you dispose of a phone, you should remove your username/password first. Log-on to the device's web page and remove this information. A factory reset is even better, as it also removes the calling directory and records of your calls.

5. 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.

6. Change your password on your VoIP service itself and, if you are no longer using their service, delete any credit cards they hold for you and cancel the account.

7. Keep the software on both your PC and phone patched up-to-date (see section 3).

Service Provider Support

In most IP-PBX attacks, the motive is fraud. The attacker will make expensive calls, including calls to international destinations or to premium rate numbers from which they profit.

If your IP-PBX has been compromised, any local policies you have in place to restrict calls will almost certainly be rendered useless. It is therefore important to work with your service provider to add an additional, external layer of protection.

ITSPA members are well versed in the area of security and will usually have a number of safeguards in place to help combat fraud. Furthermore, ITSPA Quality Mark holders will have clearly demonstrated, with evidence, their understanding and commitment in this area.

There are a variety of ways in which your service provider should be able to help, some of which are described below. They may also be able suggest companies that can help you to ensure your own systems are secure.

a. Call Barring

You may wish to block calls to/from certain countries, numbers or area codes. If you do not need to make international calls for example, ask your service provider whether the ability to call outside of the UK can be disabled at account level. Similarly, if your service provider allows it, you should prevent calls to UK premium service (09 numbers) to avoid accidental or fraudulent dialling of these numbers.

b. Credit Limits

If your service provider allows it, set your own credit limit so that if someone does find your user details, there are limits on how much they can spend. If your account is operated on a pre-paid basis, it is often advisable to limit the frequency of auto top-ups or simply turn them off all together. Your service provider should be able to send you an alert via email or text at predefined thresholds to let you know if you are nearing your limits.

c. Calling Pattern Analysis

Some providers have the capability to learn your normal pattern of calling and detect when there is activity outside of this (based on time of day, average call length, frequency/volume of calls etc). You should discuss this with your own service provider to see whether this is implemented as standard or available as an optional extra.

d. Blacklists

ITSPA currently maintains a list of known bad numbers (i.e. associated with toll and/or revenue share fraud) which is periodically distributed amongst those members who subscribe. In turn, members who detect fraudulent activity on their own networks will each add these numbers to the list in a combined effort against the fraudsters.

There is also an ITSPA study group looking into how such lists might be shared in real-time between service providers in a concerted response to organised fraud.

VoIP Checklist

This is a list of key issues that you should check off to ensure that your IP-PBX is VoIP Ready:

Item	Description	Checked
1	**Server**: Ensure the server you want to deploy the IP-PBX on is hardened, with un-needed services disabled, SSH Root access disabled with SSH login via Secure Key and default ports changed, i.e. use 4245 for SSH not 22, etc.	
2	**Software:** Ensure that your servers operating system and ALL associated software that you are installing is latest version with ALL the latest security patches enabled.	
3	**Passwords**: Change ALL the default passwords and ensure that ALL passwords, including extension passwords are complex.	
4	**Access**: Limit external access to known IP's only.	
5	Limit your extension registration source IP: For all extensions that are not public facing, define that those extensions are only accessible via your internal network. This ACL type limitation can be done at both extensions and trunk levels. On extensions, you have something called the "deny" and "permit" and "host" definition in your trunk settings	
6	Limit Max Trunk calls and Max calls per extension to your requirements	
7	Enable logging and check the logs!	
8	Enable a backup routine	