
**Comms Council UK**

# Recommendations for secure deployment of an IP-PBX

**Version 3**

November 2016

Contact: team@commscouncil.uk

## Contents

# About Comms Council UK

Founded in 2004, Comms Council UK is voice of the next generation communications industry. We are a UK membership-led organisation that represents companies who provide or resell business and residential customers voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video. The membership is a mixture of network operators, service providers, resellers, suppliers and consultants involved in a sector that is diversifying rapidly from just voice services to other innovative IP applications.

# Disclaimer



# Introduction

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, Comms Council UK 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 Comms Council UK members to assist in the identification and avoidance of an attack.

# Health Warning!

Before you set off to run your own VoIP PBX you need to be aware that whilst it's relatively easy to setup 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 commercial risk is often borne by them, not by you.

# The Current Security Threats

The following security issues and attacks have been observed on many standard VoIP implementations (in no particular order):

- General scanning and directory scanning (including extension enumeration).
- Admin interface scanning/brute force attempts (SSH/HTTP/HTTPS)
- Options and Register Requests to gather information on equipment types/versions etc to target attacks
- 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)
- Call Fraud, hackers making unauthorised calls costing the victim many thousands of pounds.

Don’t forget, since many common IP-PBXs run as software applications the underlying operating system’s security also needs to be considered over and above any advice in this document.

## If you are a Victim

If you are unfortunate to be a victim of Telephony Fraud, not matter how large or small, we recommend that you report it to http://www.actionfraud.police.uk using their online Business Reporting Tool.

For more information, see Comms Council UK Telephony Fraud – Reporting Guidance with Action Fraud
http://www.itspa.org.uk/press/itspa-telephony-fraud-reporting-guidance-with-actionfraud

# What you can do to protect yourself

## Considerations for your PBX

### During Setup

1. Use the checklist in Appendix 1 - Checklist for PBX installation
2. Subscribe to security mailing lists for all vendors that your solution encompasses
3. Set up a regular calendar of maintenance that is relevant to your installation
4. 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 and patches
2. Check firewall logs
3. Check call logs for any unexpected call traffic
4. Check PBX logs for unauthorised access attempts which may indicate your firewall is misconfigured or breached
5. Check network graphs for any unexpected traffic

## Considerations for End Points (Phones)

See Appendix 2 Security Tips for VoIP Devices for details.

## Considerations when applying Passwords

See Appendix 3 - Password tips for details.

# Considerations for additional network equipment

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 such as an Enterprise Session Border Controller (SBC).

## 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. You should always send administrative traffic over a VPN and you should also consider routing calls from home devices over a VPN or other encrypted connection.

## Management Interfaces

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

## 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). Also consider setting up your WiFi network with a hidden SSID.

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.

For more details on network protection see Appendix 4 - Network Equipment to Protect Traffic.

# What your Service Provider can do to protect you

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.

Comms Council UK members are well versed in the area of security and will usually have a number of safeguards in place to help combat fraud.

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.

## 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.

## 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 altogether. 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.

## 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.

## Blacklists

Comms Council UK 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 Comms Council UK study group looking into how such lists might be shared in real-time between service providers in a concerted response to organised fraud.

## Comms Council UK Support

Your Internet telephony service provider (Comms Council UK 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.
Comms Council UK is actively compiling lists of security threats and security recommendations for specific IP-PBX's (like Asterisk) and VoIP Devices in the Fraud and Security section of the Members Area within the Comms Council UK website. Please check here for the latest security recommendations and advice.

# Appendix 1 - Checklist for PBX installation

| 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.[AT4] | | |
| 2 | **Software:** Ensure that your server's operating system and ALL associated software that you are installing is latest version with ALL the latest security patches enabled. | | |
| 3 | **Security**: Setup the IP-PBX behind a Firewall or SBC. If not available, use IP-Tables to lock down access to known IP's and enable Fail2Ban to ban IPs associated with intrusions. | | |
| 4 | **Passwords**: Change ALL the default passwords and ensure that ALL passwords, including extension passwords are complex, ideally use a minimum 10-character mixed case password with alphanumeric and special characters. Ensure that every extension configured on your system has a password. | | |

| | | | |
|---|---|---|---|
| 5 | **Access**: Limit external access to known IP's only. | | |
| 6 | Restrict Extensions to LAN side or VPN access only.<br>This will stop your extension credentials being used externally if your system is compromised.<br>On your Extension settings you will see "deny" & "Permit" settings, which can be set as:<br>> Deny: 0.0.0.0/0.0.0.0<br>> Permit: 192.168.1.0/255.255.255.0 (your LAN IP range) | | |
| 7 | Limit Max Trunk calls and Max calls per extension | | |
| 8 | Enable logging and check the logs! | | |
| 9 | Enable a backup routine | | |

# Appendix 2 - Security Tips for VoIP Devices

Most IP-PBX installations use VoIP telephones installed on users' 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.

The security precautions you need to consider are simple and composed primarily of common sense approaches. (NB: almost everything discussed below applies also to users of softphones on PCs and Macs.)

1. 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. (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.) Alternatively, you may want to consider getting a router that has integrated security for VoIP although be careful, not all routers are created equal. You may want to test the device first or talk to your service provider who may be able to offer some advice.
2. 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 as if they were you if they can get their hands on it. See page 10 for advice on passwords/PINs.

3. 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.
4. 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.
5. 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.
6. Keep the software on both your PC and phone patched up-to-date (see page 5).

## Mobile Devices

If you use VoIP from mobile smartphones (which is increasingly common), then make sure you configure the access PIN on the phone lock screen. 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 as well as Remote Erase if a phone gets lost or stolen, both of which should be enabled. Consider using encryption services for remote VoIP phones, especially if these remote phones connect via public Wi-Fi hotspots. Even if you don't 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.

# Appendix 3 - Password tips

Never leave any system with the default or factory password. Attackers know these passwords, and this is the simplest attack.

Ideally use minimum 10 mixed case alphanumerics including special characters, for example:
> ThAs8uh#ez
> 8reCa5ru5*cef2echubra!6ecre4ab
(Note some phones do not handle all special characters)

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, fridayfreepizza5
- Include numbers and non-alphanumeric characters as well as letters in the password, e.g. 10terhooks, 5after12
- Use longer passwords or PINs, 8 characters is a minimum for passwords, 12 or more is better. 6 digits should be a minimum for PINs.
- Some systems allow you to set complexity requirements for passwords and PINs or audit existing passwords. Remember - just because you know what a strong password is, doesn't mean your users do.

  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.

Many systems will offer protection such as disabling accounts and notifying administrators when an incorrect password or PIN has been entered too many times. These should be enabled and monitored as they are often one of the first indicators of an attempted attack.

# Appendix 4 - Network Equipment to Protect Traffic

All VoIP interconnections should be protected by a firewall. Comms Council UK 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.

## 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 your PBX requires and enforces authentication for as 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 as call termination (BYE) and presence and voice mail notification (SUBSCRIBE/NOTIFY) should also require authentication. These authentication requirements apply to accounts used for both internal IP phones and for remote users, an attacker will target both categories. If your PBX cannot authenticate the full range of protocol operations or if for other reasons it is not practical to configure it to do so, consider using a 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 below.

## Session Border Controller

A session border controller (SBC) is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signalling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.

If you wish to maintain a secure and efficient network, that handles the different types of signals produced by different components with ease, it's time to consider a Session Border Controller or specialist VoIP security system for your platform.

While firewalls can provide some security for a VoIP system, most firewalls are unable to detect and block some of the more advanced threats and attacks which could be aimed at your PBX. These threats operate at the application level (signalling and media) and include call fraud, unauthorised call monitoring plus a number of denial of service (DoS) attacks. A good SBC or similar product will provide an additional level of security to protect against these attacks. Regulations and directives recently passed by the European Union will place additional responsibilities on any organisation processing personal data. These regulations, set to come into force in the next two years, apply to any form of data processing or transfer, including VoIP services. The additional level of security provided by a product addressing both network and application level security will help to ensure compliance with these new regulations.

## 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 or equivalent security appliance. 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.

## 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 two 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.

## 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 known 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.

## 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 secure access to website providing on-line banking or other services needing encryption. SRTP is designed specifically for encrypting VoIP calls. It is a lightweight 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 softphones 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, including 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.