PBX Security in the VoIP environment

Defending against telephony fraud

Executive Summary

In today's communications environment a voice network is just as likely to come under attack as a data network.

This paper aims to give an understanding of the threat faced by your voice network and looks at some general guidelines for securing your PBX and voice network against telephony fraud.

Terry Regan
SIP Trunk Engineer
White Paper – Rev 1
Spitfire Network Services
March 2013

www.spitfire.co.uk

Introduction

Telephony fraud is the unglamorous cousin of data fraud which rarely comes to the attention of the public, yet the impact to the victim can be just as devastating and sometimes even more costly. It is therefore essential that you secure your voice network and PBX before falling victim to such an attack.

"No matter whether you are a systems installer, maintainer or manager it is essential you consider the security of your voice network before you or your client becomes the victim of telephony fraud."

In the modern PBX/voice network there is no one single point of attack to defend against. Attacks can come from the internet or telephone lines and may try to exploit any number of different vulnerabilities. It is important to take an overall view of your voice security from both the telephony and network viewpoint to try and negate these risks as much as possible.

How you secure a PBX is specific to the manufacturer and voice networks will change from site to site meaning that you cannot apply an explicit set of rules to every site. That said there are some standard procedures/questions/guidelines that are relevant no matter the equipment. As a colleague recently stated "security is less a set of rules, more a state of mind."

The real key to effective security is to understand what you are up against. Once you understand the threat you are in a much better position to deploy security effectively. In this paper we will look at the most common forms of attack and how they are deployed against a PBX/voice network, and suggest some ways to defend against them.

Increase in telephony fraud

Telephony fraud is not a new phenomenon - indeed it has been around almost as long as there have been exchanges. There has however been a marked increase in the number of attacks, both attempted and successful.

This increase is due to several reasons, chief among which are:

- The introduction/increase of VoIP services
  - The introduction and increasing popularity of Voice over IP services has led to the majority of today's PBX's having internet connectivity where traditionally they did not. This has increased the number of attack vectors available to be exploited where they have not been secured.

- The installation of a PBX/voice network by inexperienced persons
    - Pretty much anyone today has the ability to Google a dozen telephone systems and install any one of them on a PC without any experience in telephony. This in itself is no bad thing, but what that installer sometimes lacks is the engineer's experience that would lead him to secure the PBX/voice network against as many "attack vectors" as possible.

- A knowledge gap when voice and data networks converge
    - As voice and data networks become increasingly converged there is sometimes a knowledge gap when an engineer works with equipment that was not traditionally within their remit. For example, an engineer with an IT background may secure the data network but not be aware of potential vulnerabilities that exist on the PBX.

Why attack?

An attack on a customer's data infrastructure can be for several reasons – simple Denial of Service, access to information i.e. corporate theft, malicious damage to systems etc.

"How to make money from telephone fraud."

An attack on a customer's voice infrastructure is predominantly about making money by fraudulently making calls using the customer's phone lines, which the customer is then liable to pay for. Here are the most common ways in which an attacker makes money from these scams:

- Simply making calls for themselves free of charge – usually low level and difficult to detect.

- Premium number and revenue sharing where an operator pays someone for calls terminating on that number. Regulatory control in the UK is pretty tight so most of these revenue shares are to International numbers.

It is worth noting that most attacks take place during the night or over the weekend for the simple reason that you are not there. If the attacker finds a vulnerability they can then exploit it until it is noticed, which could be the whole weekend and cost the customer tens of thousands of pounds.

An example:

The attack occurs over a Bank holiday weekend - Friday night 8pm to Tuesday morning 8am, a total of 84 hours

"How a fraudulent attack can build up call spend."

The customers SIP trunk has 15 channels which are in constant use dialling a premium rate number which charges £2 per minute per call.

This equates to **£1800** per hour or **£151,200** for the full 84 hours.

Attack vectors

An attack vector is the approach or means by which the attacker is able to access the PBX or voice network in order to exploit any vulnerabilities.

Traditionally, many PBX's were not accessible via the internet (indeed some of them had no IP capability at all) which limited the number of attack vectors to those delivered over the external phone lines and those with a physical presence.

As these traditional PBX's have evolved they are often now connected to a network to with external connectivity to make use of newer VoIP services. In addition there are now many server based IP PBX's in production that make use of the SIP protocol and so must also have external IP connectivity. This has introduced a number of attack vectors that can be delivered over the internet.

General Attack Vectors

Here are the most common attack vectors:

Traditional Dial-thru

- Where the attacker dials into the PBX and then uses the functionality of the PBX to generate an outbound call to a premium rate destination in response to their inbound call.

  How is it achieved?

  - Sometimes known as "phreaking", traditional dial-thru is one of the oldest forms of attack. The attacker will simply dial all of your phone numbers, often during the night, looking for a number that is answered by the PBX (i.e. voicemail, Digital Assistant, DISA etc).

- If one is found the attacker will simply redial that number and, once answered by the PBX, will look for a route back out of the PBX. It may be simple number routing (i.e. 9 for line) or make use of a compromised mailbox or DISA (Direct Inward System Access) setup.

- For example if the number is answered by users unprotected mailbox the attacker may attempt to take control of the mailbox and then configure it to forward calls to an external number. Any subsequent calls answered by this mailbox will then generate calls the external number at the expense of the PBX owner.

- Note that this is a valid form of attack on analogue, TDM and VoIP lines.

The person in the room

- This tends to be fraud committed, or at least initiated, from inside the office for low-level personal gain i.e. simply making calls without paying for them. Because it is low level it is often not noticed amongst normal call spend. Even when it is noticed it is often only investigated when it becomes significant. We most often see this type of fraud committed by contract employees working after normal office hours.

How is it achieved?

- As it is a physical presence in the office initiating the fraud they have all the privileges associated with the extensions in the office. This generally means there are a multitude of ways to commit this fraud without the need to bypass any security

  A few examples:

  - Simply dialling premium rate numbers from an extension with those rights
  - Forwarding an extension to an external number
  - Conferencing external parties etc
  - Shared Offices
  - Shared LAN

IP Attack Vectors

PBX Control

- Where the attacker gains full administrative rights to a PBX

How is it achieved?

While still relatively uncommon, the number of incidences is increasing as ever more PBX's use a web interface for administrative control rather than a proprietary programming tool.

There are occasions when there may be a legitimate requirement to access the PBX's administrative interface via the internet. If however there has been no attempt to secure this access then the interface is there for all to see and attempt to log into.

If an attacker is able to gain access they would have full control of the PBX (after changing the password no doubt) and all the capabilities within. It would be a simple matter of re-programming to allow dial-thru or in some cases the attacker could simply force the PBX to generate calls itself.

Any restrictions put in place to prevent fraud can easily be removed as the attacker now has full control over the PBX.

Endpoint control

- Similar to PBX control but where an attacker targets an endpoint for – a SIP handset for example.

How is it achieved?

Many modern IP based handsets have far more intelligence in them than traditional TDM based handsets – in fact some of them are mini systems in themselves.
They are often managed by a web interface and many of them include functionality that allows calls to be generated by this interface. If an attacker can take control of the endpoint they can often use the interface to generate calls directly from the PBX.

This sort of attack is predominantly seen on remote endpoints, i.e. a SIP handset at a home workers premise, where the interface or network has not been secured correctly and unauthorised access has been gained via the internet. A large number of handsets makes for many opportunities.

SIP specific Attack Vector

SIP specific attacks occur when the attacker targets the well known SIP port, 5060. The attacker simply scans the internet looking for IP addresses that have an open port 5060. Once located they then launch a SIP based attack against that IP address.

SIP dial-thru fraud

- This is a SIP based version of dial-thru fraud.

  How is it achieved?

  The attacker will normally use a piece of software to launch a series of SIP calls over the internet against a system that has an exposed port 5060.
  The SIP calls will contain different numbers and the aim is to find a number that is able to dial-thru the system. Once they have discovered one the attack will become much more specific and attempt to dial-thru to their chosen number.

  As with traditional dial-thru the goal is to get the PBX to generate an outbound call, which the customer is liable to pay for, in response to the inbound call.

SIP registration (or Registration hijacking)

- Registration hijacking occurs when an attacker is able to obtain valid username/s and password/s for SIP based extensions on an unsecure PBX.

How is it achieved?

Again port 5060 is targeted, but this time the attacker scans this port looking for valid extensions on the PBX. If the attacker is able to find a valid extension they will generally then launch a brute force attack hoping to crack the registration password for that extension.

If the attacker is able to obtain the SIP registration username and password for an extension they have a couple of options open to them:

Register their own SIP phone against the PBX and make calls for their own use (low-level) or use these registration details in a software package and launch a high volume of calls to a premium rate number for premium rate/revenue sharing fraud.

Figure 1 shows a very basic converged network for voice and data with a couple of home workers for good measure. The customer has a DSL circuit for data internet connectivity, a DSL circuit dedicated for voice only and traditional TDM lines as backup for the PBX.

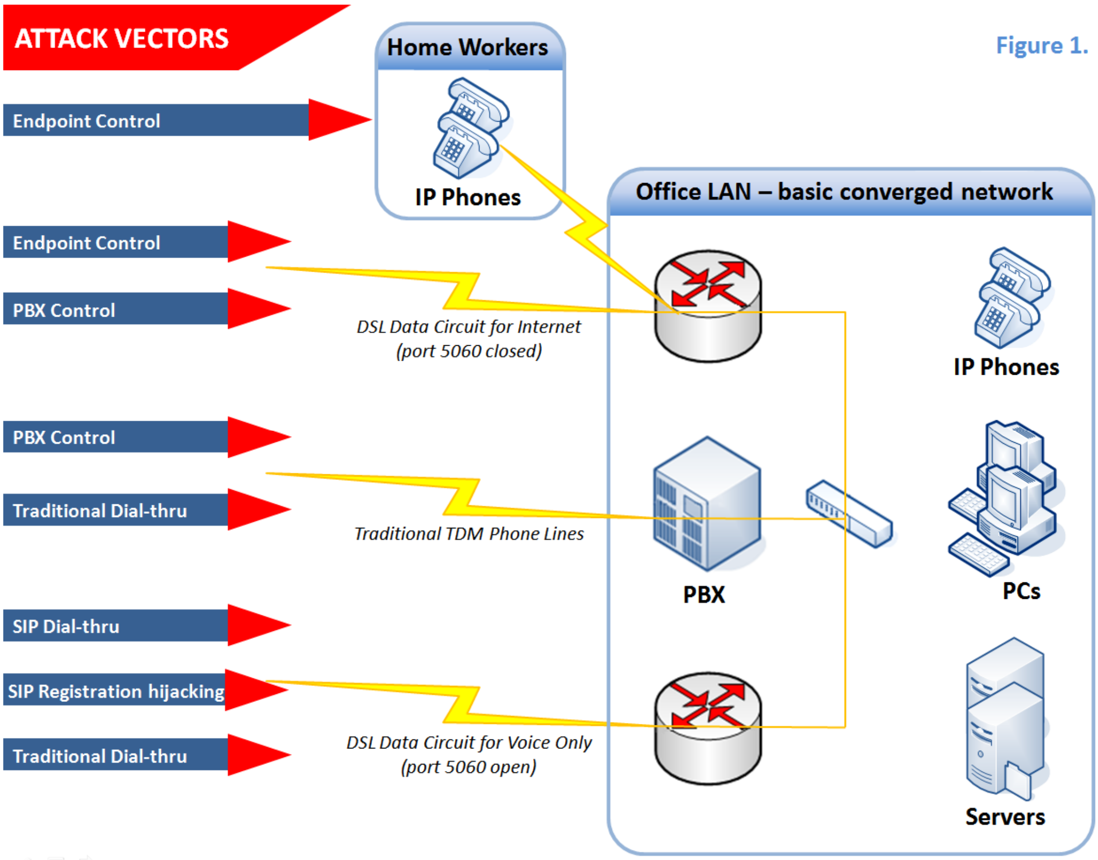

Figure 1.

As you can see, depending on the attack vector there are multiple paths to the target. It is also worthwhile noting that the same attack vector can use multiple paths i.e. traditional dial-thru can be delivered over the traditional TDM lines or the Voice only data circuit where the SIP trunks terminate.

Tips for Security

As the good doctor says prevention is better than the cure so in the first instance stopping the attacker from actually reaching your PBX or network is the ultimate solution. Unfortunately a PBX that is completely unreachable from the outside world is pretty much useless so securing any potential vulnerability becomes a very important second consideration in your overall security.

On occasions you will need to implement features that could become vulnerabilities – particularly those under end user control i.e. mailbox passwords. Although you cannot close them down completely many PBX's have anti-hacking, logging and alert features that can help you spot unusual or suspicious activity. This can give you a chance of stopping the fraud in its tracks, or even preventing it entirely.

Your lines provider, whether traditional or IP based, may also have security features that can help ranging from fraud detection to premium rate number barring. What features are available is dependent on your provider but checking their website or a simple phone call should give you all the information you need.

Prevention

Securing port 5060

If you have port 5060 open for remote SIP endpoints the use of firewalls, SBC's or router ACL's is strongly recommended. Even better is to close 5060 and use a VPN to carry traffic between the remote endpoint and the PBX.

Establish with your ITSP which IP addresses need to be configured to access port 5060 and only allow those. If your ITSP supports NAT traversal this is preferable to assigning a public IP address to a PBX.

It is worth noting that all the successful SIP registration attacks noted by Spitfire so far have taken place through routers with the SIP port forwarded to the PBX when it was not required.

Network Security/Access

If there is no requirement to access the PBX from outside your network, don’t allow it. Otherwise block access to the PBX from all IP addresses except those that have a legitimate need for access. If you do need access to the PBX, consider the use of VPN’s, ACL rules, firewalls etc to secure yourself as much as possible. Scan the network for any potential vulnerability or advise the customer to run a similar scan.

Physical security

Consider the physical security of your internal voice LAN. Try and locate the PBX and switches in a secure area and think about preventing access to this network by anything other than recognised endpoints. VLANS are another good way to prevent casual access to your voice LAN.

Inbound Rules:

You have provisioned all your DDI’s onto the PBX, but are only using half of them. Instead of routing the unused DDI’s to an Auto Attendant (where they may be able to access voicemail) why not simply end the call thus reducing the number of routes into your PBX?

Securing Vulnerabilities

Passwords – Administrator & Provisioning:

Ensure that you change the default administrator password to something secure. It is all very well to use admin/admin in a closed lab environment but using it in a production system is asking for trouble.

When provisioning a SIP phone against an IP PBX ensure that you use a strong password. If extension 101 has password 101 this will not take long to break.

Don’t forget that there are passwords for system extensions i.e. Fax Server, conference rooms etc. As hackers are often aware of these numbers (or can easily Google them) it is extremely important to ensure they have strong passwords.

Make sure you understand from the vendor's documentation what the default passwords are.

Voicemail

Ensure that any voicemail passwords are secure. It is almost always going to be a 4 digit number but there is no need for it to be 1234.

Allowing end users to access their voicemail from outside the office is a very common feature; unfortunately it is also a very common "phreaking" attack vector. Only enable this feature if the end user is fully aware of the potential implications. If you absolutely must enable this feature consider using your Outgoing Rules/Call barring to limit the exposure to expensive numbers.

Many PBX's have a user web portal or application that uses the mailbox password and from here you (or the attacker) can often divert your incoming number to an external destination.

Restrict the ability of an attacker to dial expensive numbers:

Think about your dial plans and call barring. Many TDM based systems have fine grained COS/TRS (Class of Service/Toll Restriction) capability that allows you to restrict dialling certain numbers. This is not always available on IP based PBX's but you might be able to create something similar using dial plans.

Rather than just create a default route break down the dial plan. Does the user have a requirement to call 09 numbers? No, then create an Outbound Rule allows 01, 02 etc but not 09

If there is a requirement to dial 09 it would be worth considering only allowing access to that rule to extensions that require it.

Office Hours

If the PBX has the ability to disable, or restrict outbound calls to expensive numbers outside of office hours it would be worth considering. Many frauds are committed outside of office hours this can be a very effective way of combating most types of fraud during the quiet hours.

In fact one of the few attacks that will overcome this security is PBX control as outgoing calls are barred from dialling expensive numbers.

System/default extensions

System extensions are created when the PBX is installed and usually have a standard number. Hackers are often aware of these system extension numbers and target them first. We have seen a number of SIP registration attacks recently and they have all started (for example) with the well known system extensions. Ensure you have a strong password for these extensions, or do as some engineers do and change the extension number.

Anti-Hacking, logging & alert features

Anti-Hacking features on the PBX

Many modern PBX's have anti hacking features built in. These can range from the simple i.e. disallowing the use of extension outside the LAN to advanced features such as failed authentication protection, where an attacker attempting registration hijacking only gets 10 attempts to register before the account is locked, IP blacklisting, the ability to lock extensions to MAC addresses, ACL rules etc

What is available and how it operates is specific to each PBX but if it is available I strongly recommend that you get to know the capabilities of you systems and make use of it accordingly.

We have seen recent attacks that could have been avoided by making use of anti-hacking features. In one case the engineer simply disabled his anti-hacking security altogether. In another the engineer was struggling to register his handsets so allowed registration from outside the LAN and used a simple password. Both paid a rather heavy price.

Logging & Alerts

Modern PBX's often have logging which can be used to track unusual or suspicious activity. As well as generating logs when the anti-hacking features are triggered, call logs and server activity logs may also be a good place to spot unusual activity – calls placed outside normal working hours and calls to un-recognised destinations.

Often a hacker will make one or two test calls from a PBX before committing a full scale attack overnight or over a weekend, so even spotting a single odd call may be an early warning sign.

Often there is also the ability to e-mail notification for events. You can configure it to e-mail you when (among others) an IP address has been blacklisted or the number of registration attempts has breached a threshold. Not everyone wants their weekend spoiled with a barrage of warning e-mails but it at least gives you the option of an alert when the office is unmanned.

Do I need it?

Question your setup

Ask yourself or your customer one of the most important questions when provisioning or reconfiguring the PBX or voice network – Do I or you need it?

If there is no requirement for dialling out of voicemail for example, don't enable it. It may sound like a nice feature, but all you have done by enabling it when not required is give a potential fraudster another vulnerability to exploit.

Lines provider features

Number Barring on the trunk or lines

The options available are dependent on your provider but many will give you the option (normally for a small fee) to have premium rate number barring on you trunks or lines. If the your own security is breached then this can be a very good way of limiting the damage as your provider will block calls to these premium rate numbers.

Fraud detection

Fraud detection on your trunks or lines is often another option available from your provider. Basically call spend on your trunk or line is monitored and when it breaches a certain threshold the provider will contact you to ascertain whether or not the calls are legitimate. Calls may then be barred by yourself or the provider. Some offer automatic barring but you need to speak to the provider to determine their exact capabilities. These are provided on a "best effort" basis and may be up to 48 hours behind.

Checklist

- Passwords □
- Voicemail □
- Inbound Rules □
- Outbound Dial Rules □
- Office Hours □
- Anti-Hacking & IP Blacklist □
- Logging & Alerts □
- External Phones □
- Network & Physical security □
- IP Access to management interface □
- IP Access to port 5060 □

About the author

Terry Regan is a SIP trunk engineer with Spitfire Network Services Ltd. He has over 20 years experience of working with telephone systems and he regularly deals with cases of PBX fraud and attempts to attack customers PBXs.

He advises staff, vendors and Spitfire partners on dealing with fraud and securing their systems.