



Technical Training and Consultancy to the NEW Communications Era

## VoIP and Security

### Introduction

Businesses & corporations that are implementing voice over IP (VOIP) technologies should *NOT* overlook the security risks that can crop up when the voice and data worlds converge.

Most users implementing VOIP these days are primarily concerned about voice quality, latency and interoperability. All are fundamental quality-of-service considerations that companies need to deal with before they can even begin justifying the move to VOIP. With most security organizations cautioning users about the dangers of unsecured VOIP services, many now believe VOIP will not make it into mainstream corporate use without it (at least realise the potential and opportunity).

### What are the VoIP security risks?

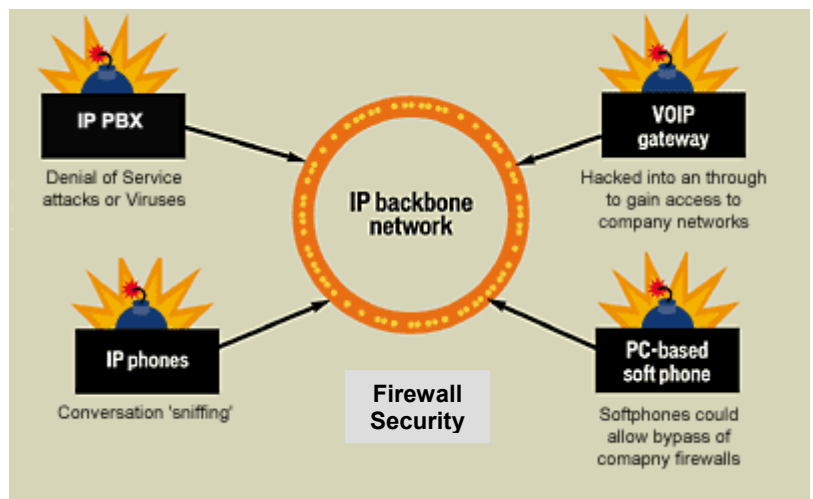
VOIP security needs to be handled in the overall context of data security, with the normal rules and issues being addressed. However, VoIP / IP Telephony has some security aspects that should not be overlooked. We take a look at these aspects below, with a summary of 'tips' and action points to minimize potential, security & risk.

Firstly, let's look at traditional telephony and the PBX. Most traditional PBX platforms run proprietary operating systems, telephony software and telephone firmware. Interfaces to the public domain (eg the PSTN) exist as a security risk, but really only for making 'free calls'. With an almost 100% voice only solution such as this, the most risk is to the conversation it 'self, and eavesdropping by inductive pick up.

By moving towards IP Telephony, we see vendors selecting standards based operating systems, control, signalling & codecs. Sitting alongside 'data' in a converged network, we now have a number of risk aspects and areas to consider, rectify or minimise.

The picture opposite shows aspects for risk consideration – we will follow this and discuss these risks as follows:

- **IP PBX** – Denial of Service, Viruses, DB access
- **VoIP Gateway** – Public / Private domain segmentation risks
- **IP Telephones** – Use and alias, Conversation 'sniffing'
- **Softphones** – applications used for access and bypass of company security policies / firewalls
- **Firewall Security** – Traversal and VoIP 'port' allocation



## ***Security and the IP PBX***

Whatever the name (IP PBX, Softswitch, Media Server.....), vendors are producing powerful, highly scalable and open standards based (software and hardware) telephony solutions. Making solutions in this way has great benefits for both the customers and the vendors, and is one of the key drivers for migrating towards VoIP. However, there are a number of security thoughts to be made.

- ***The Operating System (OS)*** – by making the OS open (such as UNIX / LINUX / WIN), this makes applications more readily interoperable – great. But as a consequence, it means that there are possibilities for access and corruption to the telephony application and information within. Create access permissions to the IP PBX, and limit availability by possibly segmenting from the rest of the network. Limit / do not allow customer access to base OS, restricting use and deposit of any conflicting / risk potential software to the IP PBX.
- ***Viruses*** – again limiting access and deposit to the IP PBX will minimize risk, keep isolated for other applications wherever possible.
- ***Denial of Service (DoS)*** – DoS attacks are where a hacker requests a connection or information from a server or application and then requests over again before acknowledgment is made. DDoS sees this on a larger scale with code typically placed on a server which repeatedly processes this action. As a result, the network is flooded and the performance of the server / application can be dramatically reduced. Limit access and look to segment the IP PBX server.

## ***Security and the VoIP Gateway***

The concern here is that gateways can be hacked into by malicious attackers in order to make free telephone calls. The trick to protecting against this lies in having strict access-control lists and making sure the gateway is configured in such a fashion that only the people on this list are permitted to make and receive VOIP calls.

Another security potential is where the gateway is used for access not only to the PSTN, but to allow for IP access to another domain, such as an IP VPN. In this case we should be looking towards secure and encrypted VPN links from enterprise to enterprise and site to site.

## ***Security and the IP Telephone***

An IP telephone 'connects' to an IP PBX or Server for service by registering and authenticating itself. The worry here is that by learning this process and gaining access to a users credentials (number and pin), any phone could register illegally (alias as someone else). Segment IP Telephones (different VLAN), but not too much worry here as most IP telephones run constantly, and the IP PBX would typically not allow a second illegal registration of the same number.

'Sniffing' or eavesdropping on a conversation is a potential security risk, but then so was it traditionally from copper and the PBX. The worry here is that the converged network could provide a huge available 'tap in' and eavesdrop access point, which is physically limited traditionally. Consider encrypting, at least one vendor has this available at this time – the problem it creates though is added time and latency. Watch out for some new / fast encryption algorithms to address this issue.

## Security and the IP Softphone

Like IP Telephones, the IP Softphone poses a security risk with aliasing (see above details). However, with softphones this risk is increased as they invariably register for service more often than IP telephones – effectively the start of each working day for most.

Another security aspect with softphones is the possible bypass of a companies security policies. As an application on a users PC (probably a laptop) there are a number of IP telephony application clients that enable services not available on an IP telephone. An example of this would be MS's Netmeeting or some Instant Messaging application. Both of these VoIP clients make it possible to 'send a file' to someone or server – potentially bypassing network security rules and firewalls.

## Security and Firewalls

Company or individual firewalls provide security protection, primarily from 'public' domains (such as the internet) to access 'private' customer domains. There are many types of firewalls, returning different methodology and degrees of protection, but the vast majority of them create a very large problem for VoIP.

- **The problem** – VoIP (SIP or H.323) uses 'dynamic port' selection of UDP streams for voice conversations. Most data communication and connections are made via well known and established ports (FTP, Telnet etc....) – however, the range of ports selected for VoIP is vast (1024 – 65535). Two of these are typically needed (for a 2 way conversation), but are dynamically selected by the endpoints. The problem for the firewall is which ports to open?
- **The answer** – numerous as follows:
  - Open up all ports – clearly not recommended
  - Open up a selection of ports and limit selection by endpoints – in use today, but again not recommended
  - Use a 'proxy' or 'applications' aware firewall which does one of two things:
    - Re-write the port numbers in application headers
    - Creates 2-calls for 1-call, scenario where the firewall handles the public side of the call as one conversation and creates another to the private – callers unaware

## VOiCOM VoIP Security Tips

VOIP security is a challenge that is "inextricably linked" with issues such as interoperability with data networks and quality of service. But ultimately, it's important to remember that securing a VOIP infrastructure involves nothing that is "drastically different" from the measures corporations have always taken to protect their data.

Security issues relating to VOIP have only begun to surface over the last year, but this has to be a major consideration. Chances are, you are unlikely to get hacked. But if you do, you'll never forget it.

### Tips for Securing VOIP Traffic

- Encrypt VOIP traffic and run it over a VPN.
- Make sure you've properly configured your firewalls. Check to see if your networking and security vendors have support for Session Initiation Protocol and the International Telecommunication Union's H.323 voice protocol.
- Consider segmenting voice and data traffic by using a virtual LAN. This will limit the threat posed by packet-sniffing tools and minimize disruption in the event of an attack.
- Think about using proxy servers in front of corporate firewalls to process incoming and outgoing voice data.
- Make sure that server-based IP PBXs are locked down and protected against viruses and denial-of-service attacks.