Asia-Pacific
Economic Cooperation

VoIP Security

Not feeling safe in the online world?

Use this guide to understand Voice over Internet Protocol (VoIP)

Telecommunications and Information Working Group (TEL)

AUGUST 2008

VoIP Security

Introduction

About this Booklet
This booklet is intended primarily to assist Small and Medium Enterprises (SMEs) in understanding the issues around VoIP security and to aid in safely using VoIP. This booklet also provides awareness information on the various types of VoIP implementations that are available, differences between traditional telephony and VoIP solutions, the different risks and threats introduced by a VoIP system, and how to protect against these threats.

A Background on VoIP
Traditional landline telephony has been the mainstay of both household and business communication in the last century. With the introduction of fast broadband Internet connections available at low-cost, a new technology has emerged in the voice communication space. Voice over Internet Protocol (VoIP) can offer significant cost savings over traditional landline services for local or long distance calls, and for calls to both international locations and mobile devices. In view of this, market research companies and analysts project that VoIP uptake is rapidly increasing and the future of voice communication is closely tied to IP technologies.

Why was VoIP developed?
VoIP was developed primarily as a technology to compete with traditional telephony, and as such, the priorities during its development were focused on quality of voice calls and the reliability of the service. The ability to utilise VoIP telephony with existing telephone switchboard technology and computer systems have also become pivotal considerations in VoIP development and adoption. This focus has allowed VoIP to rapidly become a feasible alternative to traditional telephony, however has also introduced a number of security considerations to be addressed prior to achieving the same degree of 'trust' that is now placed in the traditional landline telephone system.

The out of the box security of certain VoIP and Internet Telephony solutions is considered inadequate for some uses, unless properly considered and accounted for. An insecure VoIP system may expose organisations and individual users to potential eavesdropping on conversations, theft of services, interruption of service and other impacts.

Target audience of the booklet
This booklet is aimed at all users, regardless of skill level. The content is written for SMEs, but is also applicable to consumer level users.

Contents

A glossary of terms is usually found at the back of a book and referred to only as required. However, you will find it much easier to understand this booklet if you take a few minutes now to familiarise yourself with the vocabulary of VoIP technologies.

What you need to know to read this book

POTS (Plain old telephone service)	Plain old telephone service (POTS) is a term which describes the telephone service that remains the basic form of residential and small business service connection to the telephone network in most parts of the world.
PSTN (Public switched telephone network)	The public switched telephone network (PSTN) is the infrastructure for the world's public circuit-switched telephone networks. This network is now almost entirely digital and includes fixed (land line) telephones. The PSTN is able to deliver quality of service (QoS) guarantees meaning that downtime of the network is limited.
IP (Internet Protocol)	The internet protocol (IP) is a data-oriented protocol for transmitting data across computer networks. IP is one of the fundamental technologies on which the Internet is built. IP provides a best effort delivery strategy which means that there are no guarantees about packet delivery, however reliability and delivery can be enhanced with a number of solutions.
IP Packets	IP packets are small blocks of data which are used to send information across an IP network. A packet is a container of both the configuration and transport information required to deliver the packet to the correct destination, and the actual information that the system / user / device is trying to communicate, i.e. the payload.
Confidentiality, Integrity and Availability	Confidentiality, integrity and availability (often referred to as CIA) are three principal properties that information security aims to protect. To maintain confidentiality is to ensure that data remains private – only the intended and authorised recipients, individuals, processes or devices, may read the data. To maintain integrity is to ensure that data has not been altered during transmission from origin to reception. Availability is the assurance of timely and reliable access to data services.
PBX (Private Branch eXchange)	The private automatic branch exchange (PABX) or private branch exchange (PBX) is a connection between a private business and the PSTN. The PBX handles calls between your organisation's extensions as well as connections to the PSTN.
DSL (Digital Subscriber Line)	Digital subscriber line (DSL) is a technology which allows for digital data transmission over the wires of a local telephone network – enabling broadband Internet access. A particular form, called ADSL (asymmetric digital subscriber line) enables faster data transmission over copper lines than conventional modem based technology. The distinguishing characteristic of ADSL compared with other forms of DSL is that the volume of data flow is greater in one direction than the other – thus it is called asymmetric. Generally download bandwidth is greater than upload bandwidth.
Cable Internet	Cable Internet is a form of broadband Internet access which uses cable television infrastructure to transmit data. Cable Internet cabling does not require traditional telephone line connections, but does require cable television connections and wiring to be in place.
Softphone	A softphone is a software program that enables IP telephony calls on a computer device or workstation. A softphone can be used with a microphone and speakers, or with a softphone capable handset (such as a USB IP telephone). An example softphone is Skype.
Convergence	Convergence is the merging of separate networks, technologies, and environments into one collaborative multi-media network. A converged network is theoretically capable of handling the different elements and functionalities associated with each separate network, and enables a higher level of interactivity between them. This booklet will be dealing with the convergence of voice data and regular data on the same network.
Denial of Service (DoS)	A denial of service (DoS) attack is an attempt at limiting or stopping legitimate users from accessing a specific computer system or resource. In the context of this booklet, DoS attacks will mainly be referring to the disruption of VoIP telephony.
Protocol	A protocol is a standard method for implementing communication between two computer entities. Different protocols can exist to tackle the same basic issue however their success may be highly varied. In many cases, the protocols must be the same at each end of a connection for computers to communicate.
Hardened System	A hardened system is a computer server / terminal which has been configured in such a way that it is highly resilient to security risks. A hardened system would likely have a well configured and up-to-date version of operating system, be well patched and have appropriate security software installed. The way the system communicates with other systems would be configured with security and protection in mind.
Interoperability	Interoperability is the ability of different systems and technologies to communicate and share information with one another.
SIP and H.323	The Session Initiation Protocol (SIP) and H.323 are the two standard protocols that enable voice communication connections to occur. SIP is the newer of the two and was created specifically for IP multimedia technologies. H.323 is an earlier protocol and was conceptualised initially for PBX technologies.

Find Answers to Your Questions

When using VoIP compare to traditional telephony services, questions you might ask:	Page Reference:
Will VoIP offer any significant benefits over my landline PSTN network?	There are many benefits to VoIP networks, though there are also some tradeoffs. Some potential benefits include higher scalability, mobility and being future ready. To learn more about the differences between VoIP systems and PSTN networks including both positives and negatives, see the section: Differences between VoIP and traditional telephony services, Page 8.
What's the difference between software-based VoIP solutions (e.g. Skype) and other VoIP solutions?	VoIP solutions are widely varied. For the home user, software-based VoIP or use of a Voice Box solution may be adequate for their needs. Most businesses will opt for a complete vendor VoIP telephony deployment as they offer the most functionality and scalability. Make the right decision by learning what the differences are between available VoIP solutions. See the section: Selecting your VoIP Solution, Page 10.
Can VoIP be used to replace my cell / mobile telephone?	Mobile VoIP does exist, however in 2008 it is still in its infancy, and offered by a limited number of service providers. Currently, most users would find the service inadequate to completely replace their cell / mobile telephone. Learn more about VoIP mobility in the section: Differences between VoIP and traditional telephony services, Page 8, and the section: Selecting your VoIP Solution, Page 10.
Is VoIP secure?	The protection that VoIP offers for the privacy of calls varies depending on how the VoIP system is implemented and on the environment that the system is integrated into. VoIP can be secured to similar or stronger levels of security than PSTN networks. For further background on VoIP and the security offered of the service, see the section: VoIP Security Primer, Page 14.
How strong is the privacy in VoIP?	VoIP privacy can be close to or equivalent to that of PSTN networks, though requires some additional security measures to bring it to this level. For further background on some of the privacy and confidentiality issues in VoIP, see the section: VoIP Threats: Confidentiality, Page 16.

Page Reference:	When using VoIP compare to traditional telephony services, questions you might ask:
Fraud and theft risks do exist in VoIP, as with any communication protocol or network. However controls can be implemented to minimise this security risk. See the section: VoIP Threats: Integrity, Page 18.	Are there any fraud or theft risks with VoIP?
VoIP operates via a significantly different transport method to that of traditional telephony, and is a relatively young technology (circa 20 years) when compared to traditional telephony (over 100 years). As a result of these two factors, VoIP suffers from a number of availability issues. These include issues from network congestion, power availability and malicious disruption of services. To learn more about these, see the section: VoIP Threats: Availability, Page 20.	Does VoIP have any reliability issues compared to traditional telephony?
There are many security attacks which can potentially jeapordise the confidentiality, integrity or availability of VoIP services. Some of these include eavesdropping, message alteration and theft of service. For more information on the technical aspects of security risks in VoIP threats sections beginning from Page 16.	At a technical level, what are the security risks involved with a VoIP implementation?
Securing a VoIP implementation requires careful consideration and customisation to ensure that the controls put in place best cater for each organisation's infrastructure, policies and risk tolerance. Some of the available security measures include implementing a VPN, firewall and encrypting traffic. For more information on security measures, see the section: Protecting your VoIP System, Page 23.	How can I secure my VoIP implementation?
There are a number of standard practices that should be followed when connecting to the Internet, regardless of use of VoIP or not. For information and basic recommendations on these standard practices, see the section: Computer Security Essentials, Page 30.	How can I secure my workstation, and what are some general security measures I should be aware of?

Functionally, both VoIP and traditional telephony offer the same basic set of capabilities, however through distinctly different core infrastructure. Both technologies have their own sets of advantages and disadvantages which this section will highlight alongside the main differences that a basic VoIP solution offers in comparison to the traditional landline.

Differences between VoIP and Traditional Telephony Services

Connection differences

Traditional telephones transmit voice communications over electronic signals through centralised public telephone exchanges. The call connection is generally dedicated for the duration of the call. With VoIP, the fundamental difference is that the connection resides over a packet-switched network (such as the Internet or a private LAN), as opposed to a circuit-switched network (such as PSTN).

While Internet connections generally utilise the telephone network, there exist a multitude of other available connection means, such as cable and wireless Internet. Software based VoIP and some hardware VoIP solutions use typical Internet infrastructure as a transport layer. Managed VoIP services offered by companies such as Cisco may utilise an IP infrastructure separate to the Internet which offer higher quality of service and security than other Internet-based VoIP services, for additional costs. With VoIP, voice communications are transmitted in the same way as data communications, such as when you send an email or view a web page.

In traditional telephony, phone calls may be shared with other telephone line based services (e.g. DSL Internet), however these phone calls will have dedicated frequencies which guarantee phone call accessibility. VoIP phone calls also share a connection (an IP connection) however VoIP calls may not have guaranteed connection use. At a technical level, VoIP conversations are broken down into "IP packets" (small blocks of data) and these packets are sent separately via potentially different journeys across the network, which may include the Internet. This approach is noticeably different to the single continuous transmission circuit provided by traditional telephones.

ADVANTAGES	DISADVANTAGES
VoIP security — Correctly implemented, the security, particularly the confidentiality of phone calls made, can be better secured than in PSTN systems.	**VoIP security** — There is added complexity in securing a VoIP system when compared to securing a PSTN system. Because VoIP utilises data networks, these can be used as additional methods of attack into and on the VoIP system. Where VoIP traffic travels over public IP networks such as the Internet, the traffic is susceptible to attacks from a significantly larger number of malicious users.
Lower cost of call connection and call rates — Call rates are usually cheaper over VoIP services. This includes calls to locations overseas or interstate, as well as calls to mobile telephones. In some cases, calls to other VoIP phones operating from the same VoIP provider will be free of time based charge.	**VoIP services may not work during power outages** — Many countries keep traditional telephone line connections running even when electrical power outlets are unavailable, in which case a VoIP handset would not function.
Future ready — Many VoIP solutions offer a level of integration with other IP technologies such as Fax over IP, Video, IPv6 and other rich functionality whereas the PSTN (currently) does not.	**Unavailable call services** — Certain premium rate call services and free call services may not be available. For example, service providers may not be able to provide call services to premium rate numbers such as those utilised in competitions, voting numbers, weather forecasts and other services., Free call numbersmay also be non contactable.
Scalability — Additional handsets can be added and configured into existing VoIP implementations relatively easily, provided that the network has the required bandwidth available to tackle the extra load.	**May lack directory listing** — VoIP services may not offer a listing in your city's primary phone number directory.
Higher mobility — Some providers allow VoIP to be used wherever you have an available broadband connection. This offers benefits such as an employee working from home could utilise an organisation dedicated number.	**VoIP services may lack some of the features and capabilities of current PSTN and POTS networks** — VoIP services may not be able to work correctly with disability access protocols (such as TTY), may not be able to send alarm signals to a monitored security service, or may not be able to make calls to certain telephone numbers.
Additional telephone services – VoIP offers potentially convenient advances to telephony and integrated technologies.	Emergency services – In some VoIP service cases it may not be possible to utilise emergency services to their full extent. It may be possible for customers to sign up for E911 however, in which a local land address is taken by the service provider, which can be sent to emergency services should an emergency call ever be made.

A number of different VoIP solutions are available which are tailored to suit the specific needs of different groups of users. Each solution varies in its functionality, underlying technology and approach to implementation, which in turn impacts on cost, scalability, performance and complexity.

The more common VoIP implementations include the following:

Selecting Your Voice over IP Solution

Software based VoIP (Softphone)

- Requires a computer workstation / laptop and a broadband Internet connection
- Often able to send and receive free calls to other users of the same softphone network
- May utilise a 'username' instead of a phone number. Regular phone numbers are also available for some services
- May lack the functionality and reliability of other solutions
- Softphones are emerging in the mobile device market eg. PDAs and 3G mobile telephones
- Some commercial softphones have had security weaknesses identified in the past, however these are usually fixed in future releases / patches of the softphones

Business-grade VoIP telephony deployments

- Requires a number of infrastructure upgrades and placements
- Designed specifically for business grade usage
- Costs significantly more than software-based VoIP solutions
- High functionality, reliability, quality of service, can offer strong security, scalable
- Best suited for deployments with a requirement of more than 10 separate endpoint handsets
- Usually requires an IT specialist – either internal or via a service provider – to analyse the business needs and tailor an appropriate solution

VoIP handsets / adapters

- Requires a VoIP handset or adaptor package from the service provider, alongside broadband Internet connection and router
- These offer call functionality and services similar to that of typical PSTN services (eg call forwarding, voicemail, caller ID, time screening etc.)

Instant Messaging voice services

- Requires a computer workstation / laptop a broadband Internet connection and the instant messaging software
- Services such as AIM, MSN and QQ may offer 'voice chat' functionality
- Allows free voice chat with other users on your contact list
- Very limited call functionality, not suitable for most businesses

Mobile VoIP

- Requires mobile telephone with 3G connectivity or wireless connectivity
- Using a mobile version of a softphone mobile devices and telephones are capable of offering VoIP services
- The technology may require additional connection and ongoing costs
- The full functionality of these services is limited to areas which have 3G coverage

To help determine which solution is best suited to your business, the following section categorises typical business types or usage types, and identifies possible systems for each type.

RECOMMENDED VoIP SETUP:	WHY THIS SOLUTION?
I only use my phone to contact family, friends and maybe a few clients	
Softphone	Softphones may be the most applicable VoIP service for you. Calls are generally cheap and setup is usually quite simple. It should be noted that softphones may not offer call functionality such as emergency services, call forwarding, voice mail and others. Softphones will generally only be contactable if the computer / device that it is installed on is switched on.
VoIP adapter / handset	VoIP adapters / handsets may be utilised as your telephony solution due to their generally feature rich nature and similar usage style to traditional telephones. Many VoIP adapters / handsets only require a broadband Internet connection and router to operate.
I use my phone primarily to contact clients/customers from my small business (< 5 people)	
Softphone	Softphones may be useful as an additional service alongside another primary telephony connection. This broadens accessibility for some of your clients / customers, and is generally low cost to maintain. A softphone service may not be functional enough to serve as your sole telephony system however, due to its lack of call features discussed above.
VoIP adapter / handset	VoIP adapters / handsets may be utilised as your telephony solution due to their generally feature rich nature and similar usage style to traditional telephones. Many VoIP adapters / handsets only require a broadband Internet connection and router to operate.
I use my phone primarily to contact clients / customers from my small business (between 5 – 10 employees)	
VoIP adapter / handset	VoIP adapters / handsets may be utilised as your telephony solution due to their generally feature rich nature and similar usage style to traditional telephones. It is also possible to set up separate VoIP connections for multiple contact points if each user requires their own desk phone.
Business-grade VoIP Telephony deployment	Business-grade VoIP can be implemented to have significantly better security than other VoIP solutions, and can be more secure than PSTN telephony solutions. If your organisation deals with confidential or highly sensitive information (for example financial information, or private client data), business-grade VoIP is the best equipped VoIP solution for maintaining privacy and integrity.
The company phones are used primarily to contact clients / customers (> 10 employees)	
Business-grade VoIP Telephony deployment	Business-grade VoIP can be implemented to have significantly better security than other VoIP solutions, and can be more secure than PSTN telephony solutions. If your organisation deals with confidential or highly sensitive information (for example financial information, or private client data), business-grade VoIP is the best equipped VoIP solution for maintaining privacy and integrity. Furthermore, business-grade VoIP is highly scalable, configurable and can be tailored to suit specific businesses telephony needs with the help of service provider.

Short guideline on VoIP call costs

These are estimated call rates for the various VoIP types, however rates will vary from network to network. When considering the costs of a VoIP solution, organisations should also factor in initial setup costs, Internet or other connection costs, infrastructure costs, and any necessary support costs.

- Some VoIP services offer monthly packages where subscribers pay from $5 to $50 in monthly fees and receive unlimited free / untimed calls or significantly reduced call rates
- Softphone costs calls to other same-network softphones are usually free of charge
- Softphone local and international calls are often priced at lower per minute rates than other VoIP solutions. International rates typically cost from US$0.05 to US$1.80 depending on the location of the caller and the location of the receiver.
- VoIP adapter / handset providers often provide free calls to other numbers subscribed to their services
- VoIP adapter / handset local per minute call costs are priced from US$0.05 to US$0.20. International calls are priced higher than most softphone international rates, typically by US$0.10 to US$0.50 **extra**
- Business-grade VoIP solutions offer similar per minute call rate costs to VoIP adapter / handset provider rates. Business-grade VoIP solutions also provide free calls within the organisation's internal phone networks

VoIP Security Primer

VoIP was designed with the core priorities of reliability, interoperability and quality of service and as such, concern for security has generally been secondary to these in early VoIP implementations. Unfortunately VoIP suffers from a number of overarching security issues, including:

- Transmission over IP / Internet – Since VoIP utilises the same infrastructure as that utilised by data services, VoIP suffers from the underlying data security problems as well as problems unique to VoIP.
- VoIP does not have a standardised protocol for sending & receiving information. Different protocols exist (e.g. SIP and H.323), though many devices support more than one. This increases the chance of poorly written applications / implementations to be exploited maliciously.
- Security may reduce Quality of Service (QoS)– Security measures may add to the data being transmitted in a VoIP session thus increasing the risk of lower quality of service due to network congestion.

While a VoIP compromise may result in significant loss, to date there have been few significant - and disclosed - real world VoIP security breaches.

Despite the fact that only a few security incidents that relate directly to VoIP systems have been publicly reported, securing a VoIP solution is an important task for all organisations deploying such technology to mitigate VoIP related risks and threats highlighted in the Threats section of this booklet. Security is an essential consideration when looking into VoIP as a new technology investment, and should be a fundamental requirement for an SME who has already implemented a VoIP solution (or is in the process of doing so).

The scope of information security used in this booklet is based on the "CIA" acronym, covering:

- Confidentiality – ensuring that sensitive data is safeguarded from prying ears, and ensuring the privacy of conversations.
- Integrity – detecting whether information has been altered (maliciously or accidentally), and assessing whether the voice message data can be trusted and relied upon as authentic.
- Availability – ensuring that reliability and timely access exists to voice data and resources.

One of the challenges highlighted by the addition of a VoIP system into an SME's technology environment is the dependency on a single communication network. If VoIP becomes the sole land based telephony solution, the uptime of Internet / Broadband may become critical to the organisation, as it then carries the majority of communication links for a business (email, web and telephone). This may drive the need for a higher-grade Internet / Broadband service and such changes will need to be factored into any cost savings associated with the move.

Most organisations will elect to have (non VoIP) mobile telephone services and a PSTN phone available in the event of Internet access failing.

VoIP Threats — Confidentiality

A key expectation for both our daily business and personal telephone calls is confidence in the privacy of these conversations. Whether we are discussing a sensitive business transaction, our own health or finances, or just matters private to our families, we rely on the confidentiality of the telephone system to ensure this information does not leak into the public domain or fall into the hands of malicious individuals.

With traditional telephone networks someone wishing to listen or seriously breach the confidentiality of the network usually requires physical access to transmission lines or network systems. In contrast, on the Internet, the idea of a connection is markedly different. As the Internet is a truly global network, an individual may be able to listen to or copy the communications of a poorly secured VoIP system without the need for physical access.

EAVESDROPPING

In VoIP architecture, voice communications are passed around the Internet as 'packets' of data. Attackers may be able to gain access to this transmitted data and make sense of its contents if they are unencrypted.

COLLECTING OF USER AND USE INFORMATION

It is possible for network structure information and call patterns to be traced via traffic analysis. As VoIP devices need to be in a position to accept connections (i.e. telephone calls) attackers may be able to identify these devices on your network and monitor the calls via software built to tap into VoIP calls (e.g. SIPtap). By doing so, attackers can gain valuable information about your organisation's physical setup, work processes, client and supplier contact information.

UNAUTHORISED VOICEMAIL ACCESS

Many VoIP systems now provide a voicemail function similar to that available with standard telephony services. This voicemail function may be subject to confidentiality attacks where the contents of the system are accessible through unauthorised methods. However, VoIP Voicemail can be made more secure than traditional telephony voicemail systems with the aid of encryption and access controls.

Recommendations

- Ensure that VoIP communications are secured effectively using encryption – for example via a Virtual Private Network (VPN) or other encrypted link
- If this is not possible, it may be sufficient to minimise the use of VoIP for confidential phone calls
- Implement network security and personal firewall systems to ensure unauthorised network traffic does not enter the environment
- Ensure that any network firewall is capable of handling encrypted VoIP data
- Apply the latest security patches recommended by the product vendors
- Where possible use VoIP on DSL connections. VoIP over cable Internet which has not been adequately protected can be easily 'sniffed' by other users who share the cable line

CASE STUDY

SCENARIO

Sandra is the director of a medical centre which currently has a residency of 6 doctors and an administration team of 4 including Sandra. The medical centre is located in a local shopping complex and caters for general medical consultations for all residents.

The use of telephones is highly important to the business. Administrative staff are required to create and follow up on bookings and appointments, doctors need to speak to the administrative staff when assistance is required, and doctors also may need to initiate direct contact to patients via telephone. To maintain compliance to health information privacy acts, calls involving patient health details must be kept confidential. The centre utilises an ADSL2 Internet connection.

VoIP OPPORTUNITY

Given the volume of outgoing calls made by the medical centre and the low number of telephones, Sandra wants to consider replacing the existing telephone system with VoIP. Sandra also realises that maintaining confidentiality and privacy will be required by any VoIP system she chooses.

SOLUTION

Given this scenario, Sandra elected to install a business-grade VoIP telephony deployment[1] for the medical centre for both inbound and outbound calls. The PSTN system is retained alongside the VoIP deployment in emergency areas for backup communication should the VoIP system fail. Sandra was aware that the expertise required to secure the new VoIP deployment was far beyond her skills or those of any of her staff. Sandra was also aware that protecting this system would require secured switches, phone devices and a well configured firewall.

Sandra had the vendors install the VoIP infrastructure (VoIP handsets, VoIP gateway switches, VoIP call manager) into the centre's existing computer network which incorporates the ADSL2 line for internet connectivity. Sandra hired external security specialists to assess and harden the centre's computer network. The specialists configured the VoIP switches to encrypt call data from the VoIP networks, to keep data confidential, but minimise any latency introduced. The specialists also configured the centre's firewalls to allow the encrypted VoIP traffic to traverse the network efficiently, to further reduce latency. The devices were also adjusted to work with the securely configured network.

To maintain the security of the system, the specialists advised Sandra that she should maintain the VoIP infrastructure by installing patches and updates as they are made available.

Despite the initialisation costs, the VoIP system was expected to lower overall call costs to the centre over time, while still maintaining high level of service. Sandra decided that the retained PSTN system would be kept as an emergency backup system for a period of time, or phased out in future as deemed unnecessary.

[1] *See the 'Selecting your VoIP solution' section for clarification on this VoIP system.*

VoIP Threats – Integrity

The reliability and trustworthiness of message content are fundamental assumptions for users of telephone systems today. VoIP uses technologies that traverse infrastructure used by many other users – in the case of the Internet, many millions of other users – this trustworthiness of content is in some cases subject to question.

MESSAGE ALTERATION

The process of interception, alteration and resending of messages within a trusted conversation is known as "man-in-the-middle" attack. In some VoIP systems, data is transmitted as packets through shared computer networks – often including the Internet – where its path is shared with other types of traffic and is more widely accessible. Without proper protection, attackers may be able to alter or scramble the content of messages such that they are non usable or recognisable. Message alteration can also include changing voice mail, fax and other messaging services via VoIP, as well as video reconstruction.

IDENTITY FRAUD

Unauthorised individuals may be able to assume another user's identity through the rerouting of telephone calls. If an unauthorised person is able to gain access to the necessary users' Internet connections, they can redirect their VoIP calls from any geographic location in the world to any other geographic location in the world.

SCENARIO - HARDWARE STORE

The local hardware store uses VoIP for both incoming and outgoing calls. A client seeks to lodge an order with the store and calls the store's number as appears on their website. If the hardware store's VoIP call server were to be compromised (for example via exploits which attacked a vulnerable unpatched operating system), this call could be directed to a fraudulent receptionist without the hardware store ever knowing that the call had come through. The fraudulent recipient of the call could then impersonate a hardware store employee to collect the necessary payment card details and personal information for use in other fraudulent activities.

In this scenario, the integrity of the call has been lost due to weaknesses in the underlying infrastructure used by the VoIP service – in this case, an unpatched operating system. Protecting VoIP requires securing or 'hardening' all layers of the system, including the devices & infrastructure (network and otherwise), operating systems and protocols. Patching the operating system to its latest update helps prevent a compromise, and consequent fraudulent activity.

FALSE CALLER-ID

Another potential threat to integrity may arise from users being able to change their caller ID to a fraudulent value (commonly referred to as caller ID spoofing). Similar to altering the message content, identity fraud can also include utilising false caller IDs to allow fraudsters to be proactive in engaging contact with a VoIP user while pretending to be someone else. Through using a caller ID phone number known to be associated with a given organisation, a fraudster can gain further credibility in their claim to be someone else.

ROGUE IP PHONE

A malicious user may connect an unauthorised IP phone to the network. A rogue phone poses threats such as identity fraud and can be utilised to start unauthorised services or launch attacks against other devices in the network.

VISHING (OR VoIP PHISHING)

Vishing is similar to an email-based phishing. A victim will receive an email or be contacted with a phone call that directs him or her to a customer service number where they go through a number of voice prompted menus, in an attempt to steal account numbers, credit card numbers, PINs, and other critical information.

Recommendations

- Always make sure the person you are speaking to is who they claim. This may require the development of a standard set of authentication questions for existing customers and suppliers.
- Do not simply rely on caller ID to accurately identify who the caller is.
- Always use an additional method (ie voice call, SMS or email) to confirm with customers and users of key decisions made during a telephone conversation or if you are unsure about thae validity of phone call requesting critical information such as account numbers or PINs

CASE STUDY

SCENARIO

Jason owns and runs a small convenience store which frequently requires inventory cleansing and reordering. Jason places his orders with stockists via telephone, and currently uses a softphone both at home and at the shop to place the shop orders and uses an ADSL2 connection for both. The stockists utilise a PSTN.

Jason has been noticing that there have been discrepancies in some of the orders made, where a number of orders he had stated were never invoiced nor delivered. Unsure of what was going on, Jason asked stockists why certain orders were missing. The stockists claimed that the orders had never been placed during the phone calls, but that there had been a number of silent gaps in the calls.

VoIP COMPROMISE

Jason contacted the support team for the softphones that he uses for investigation of likely problems. Support stated that either Jason's connection was dropping out (but this was unlikely as the call did not end until Jason hung up the phone), or that Jason was experiencing a man-in-the-middle attack on some of his phone calls – someone was tapping into his conversations and introducing silence into the conversation before it reached the stockists.

SOLUTION

Disturbed by the thought of someone having such access to his calls, Jason looked around the Internet for ways to secure his softphone from man-in-the-middle attacks. He found that the easiest solution for his purposes and limited technical background was to install a 3rd party VoIP security solution which would maintain the integrity (and confidentiality) of his calls.

The solution utilised protocols which offered end-to-end security, and would protect Jason's calls during transmission while travelling over Internet infrastructure.

VoIP Threats — Availability

An important aspect of the traditional telephone system is its consistent availability over time. Through decades of development, most APEC region PSTN networks yield an uptime of 99.999% - or less than six minutes of downtime a year[2].

Currently, VoIP technologies do not guarantee a similar level of availability. Common threats to VoIP availability may be the result of any number of physical or electronic occurrences, which may be either malicious or accidental in nature. The following items detail some of these potential threats:

NETWORK CONGESTION

One of the primary reasons why VoIP does not perform as well as traditional telephone systems in availability is because it depends on computer networks and the Internet to work. The limitations of current communications technology mean that these computer network connections can only handle a certain level of data transfer – known as 'bandwidth' – at any given point in time. All Internet connectivity suppliers and broadband users are subject to bandwidth limitations. By adding VoIP to home or business networks, the bandwidth may be insufficient such that performance of both voice and data transmission suffers.

NETWORK DENIAL OF SERVICE

For calls within a single physical location, the VoIP call may not leave the internal network, however for calls to people outside the office or home, most VoIP systems travel over public computer networks. As a result, these systems may be susceptible to the full spectrum of computer network denial of service (DoS) risks. A large number of these DoS risks relate to the network or devices being 'flooded' with an unmanageable amount of traffic, such that the devices are unable to function normally. Other such attacks utilise weaknesses in the software or hardware components to exploit the devices and reconfigure them so they can no longer be accessed or used.

DEPENDENCE ON ELECTRICITY

Traditional telephone lines have electricity provided from the telephone exchange. This means in the event of a power failure at an individual's home or place of work, traditional telephone systems will often still be available for use. As most VoIP systems require electrical equipment (including modems, VoIP telephone systems, and personal computers) to be available in addition to the Internet connection, such telephone systems may not be available in the event of an electrical outage.

INABILITY TO ACCESS TO EMERGENCY SERVICES

Emergency telephone numbers (000, 911 etc depending on your location) are not always available with VoIP services. It is up to the VoIP provider to ensure the access is provisioned. In cases where downloadable software is used to set up VoIP via an Internet connection, emergency services are quite often not available. In addition to this, the location information associated with your VoIP call may not be reliable enough for emergency services staff to locate you as quickly and easily as traditional telephone services, especially if an emergency call is made from a VoIP solution currently not at its 'home' location (e.g. a VoIP adapter / phone utilised interstate or overseas).

Other location based telephony services may be similarly not available, such as service directories, monitoring security services and others. Certain premium rate call services and free call services may also not be available. For example, in Australia, 190X numbers (competitions, voting numbers, weather forecasts etc.), 1800 (free call numbers) or 13 (premium rate number) numbers are not able to be called from some VoIP services.

VOICE SPAM

Voice spam refers to the sending of unwanted or illegitimate calls on a VoIP network. Voice spam may also be referred to as Spam over Internet Telephony (SPIT). The key concern of spam in VoIP is the congestion it could cause to voicemail boxes, which unlike people, cannot identify and reject spam calls. Electronic stores where voice mail is kept could undergo significant load, and organisations may lose genuine voice mail messages. Fortunately voice spam is currently not a common occurrence but is forecast to grow in the future.

Another potential issue of voice spam is the impact it could have on the QoS of other legitimate calls. In extreme volumes, voice spam may congest bandwidth and reduce throughput for both data and voice services in an organisation.

Recommendations

- Regularly assess your business availability requirements keeping in mind existing network traffic and emergency situations
- Ensure that your VoIP service provider has an agreed level of service and technical support which is acceptable to your business requirement
- Check whether your VoIP service provider supports emergency services
- Ensure basic computer security essentials are adhered to if your VoIP solution utilises your computer systems
- Consider backup and recovery options for VoIP systems, including VoIP service and Internet provider fail-safe capabilities, backup alternatives such as secondary links, secondary telephony options (PSTN, cellular networks etc)

Ways to maintain availability in your VoIP system will be discussed in the "Protecting your VoIP solution" section of this booklet. Links to where you can find further details are also available on the APEC VoIP security website.

CASE STUDY

SCENARIO

Stuart is the owner of a fine dining restaurant located in the heart of the city. The restaurant's prestige and exclusiveness have meant that the restaurant need only rely on pre booked dinners, and that drop-ins were no longer required. Stuart's confidence in his restaurant has fuelled his decision to make the restaurant available solely by pre booking.

[2] *Sources of Failure in the Public Switched Telephone Network, IEEE Computer, Vol. 30, No. 4, Richard Kuhn, April, 1997.*

Stuart's booking system requires diners to book over the phone, and should the line happen to be busy, leave a voice message. The telephone system is also frequently used to order stock, confirm bookings, book taxis and for other general services.

Stuart realises that the telephone connection must be constantly working for his plans to work, and that the voice mail must be readily available. He currently has a PSTN telephone for the restaurant.

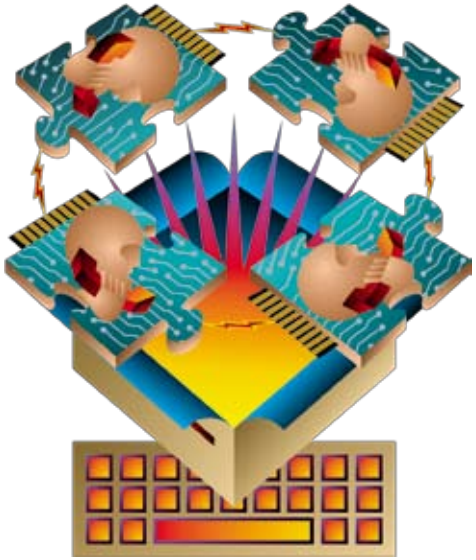
VoIP OPPORTUNITY

Stuart would like to trial a VoIP solution, as he is aware that it could be used to minimise call costs, and work as a parallel secondary phone to his current PSTN telephone. The VoIP phone would need the same capabilities as his current PSTN phone which is extremely reliable and has voicemail built in.

SOLUTION

Stuart elected to install a hardware based VoIP box in his restaurant. The VoIP service allows staff to handle multiple bookings at once while delivering cheaper outbound calls. The service he adopted also included free voice messages.

To maintain availability, Stuart has put in place surge protection and an uninterruptable power supply (UPS). Should a power failure occur for longer than his UPS can supply, Stuart still has his PSTN line available for either incoming or outgoing calls. This backup facility allows him to call his VoIP vendor in the event of an outage. The vendor would then forward any VoIP incoming calls to the PSTN phone. Stuart also made sure that his VoIP provider allowed QoS options to be utilised on his phone, and that the phone recognised and made use of these QoS features.



As an added bonus, Stuart found that his voice messages could be checked when he was away from the restaurant phone system, either by dialing into the voice message bank, or via his email account.

Note: Each business will have their own set of availability needs and tolerance, and the case study reflects only a certain sample of availability needs. A business must consider its own availability requirements and value these against what VoIP is capable of sustaining.

Ensuring that a VoIP solution performs as securely as possible may require additional consideration and configuration by SMEs. In some cases configuring the VoIP solution may require expertise or specialised knowledge in computer networking, so additional costs may be involved in acquiring personnel or consultants capable of implementing and maintaining high levels of VoIP security.

The following section breaks down protection of VoIP into the specific VoIP solution types identified in the "Choosing your VoIP Solution" section. It then details more generic measures that can be applied to most or all of the different VoIP solutions.

Protecting Your VoIP System

PROTECTING YOUR SOFTPHONE

Softphones required the use of a workstation in order to operate. The core attack vectors on this platform would be through vulnerabilities in the softphone application, operating system, network and attacks on your service provider.

Softphone configuration / protocols

Softphones can be tricky to protect, as often the user has little control over configuring how the application works. As this is the case, users should put careful consideration into which softphone they select, particularly what protocols are enabled on the program. For workstation softphones, it is recommended that the phone utilises SIP and SRTP protocols (most vendors will state if their softphone supports these, or can be asked for such information). Both these protocols (if well implemented by the vendor) will boost the security of the VoIP service significantly.

Note: Some softphones utilise their own proprietary protocols so the security strength of these programs is not well known.

SRTP is the Secure Real Time Protocol. SRTP improves the encryption, authentication and integrity of VoIP calls (and other communications not relevant to this booklet)

End-to-end security solutions

A recent development in softphone protection is in third party end-to-end VoIP security solutions. End-to-end solutions offer protected channels during the entire transmission of a connection from

the caller to the receiver and vice versa. Installation of these applications is recommended, as they can offer far higher assurances of confidentiality and integrity than softphones without these installed. It is often a requirement of end-to-end solutions for both endpoints to have the security solution installed. This may make such products less practical for businesses with large volumes of outgoing calls which require high security.

Improving Insecure Networks

If you are using your softphone through public insecure networks (eg. using it from Internet cafes, open/free wireless networks) there may be additional security issues. Using a VoIP softphone on a workstation which has not been adequately hardened, or which is not owned by the VoIP enabled SME could jeopardise the privacy of calls made. If utilising VoIP from a public network, utilisation of a VPN or other end-to-end VoIP solution is recommended.

If the VoIP solution is going to be used outside of the organisation's network, ensure that the connection from the handset or softphone to the organisation's internal VoIP server is established over a secure and encrypted connection. The use of a well configured VPN is highly recommended to achieve this. It should be noted that a VPN may add extra data overhead to the VoIP connection and could introduce some lag.

If a VPN is utilised, alongside QoS options, the QoS flags in the voice stream may be obfuscated, so QoS will no longer be in effect – that is, VoIP traffic will not necessarily be given high delivery priority, so calls may become lagged.

PROTECTING YOUR VoIP ADAPTERS AND VoIP ENABLED ROUTERS / MODEMS

End user options for protecting VoIP adapters and routers / modems is often limited to only the security features that the VoIP vendor supplies or updates in their product. Despite this, it is possible to select a VoIP product which has good VoIP security built in. For these devices, it is recommended that the phone utilises SIP and SRTP protocols (most vendors will state if their softphone supports these, or can be asked for such information). Both these protocols (if well implemented by the vendor) will boost the security of the VoIP service significantly.

PROTECTING YOUR VoIP ON YOUR MOBILE / WIRELESS DEVICE

Mobile devices with VoIP rely on a portable backend softphone to operate. Therefore protecting a mobile device with VoIP shares many commonalities with the protection recommendations used for softphones, with a few additional considerations.

These devices will likely utilise some form of wireless connection to either connect directly to an Internet service, or to connect to a network which has Internet accessibility.

When wirelessly connecting directly to an Internet service

If a mobile device connects directly to an Internet service (eg. Mobile telephones which utilise 3G networks), there are few security configuration options available to users. Instead, users should ensure that the VoIP software on devices are up to date revisions of the software, and that the software supports and utilises secure protocols such as SIP and H.323 and if available, SRTP.

When wirelessly connecting to a network with Internet accessibility

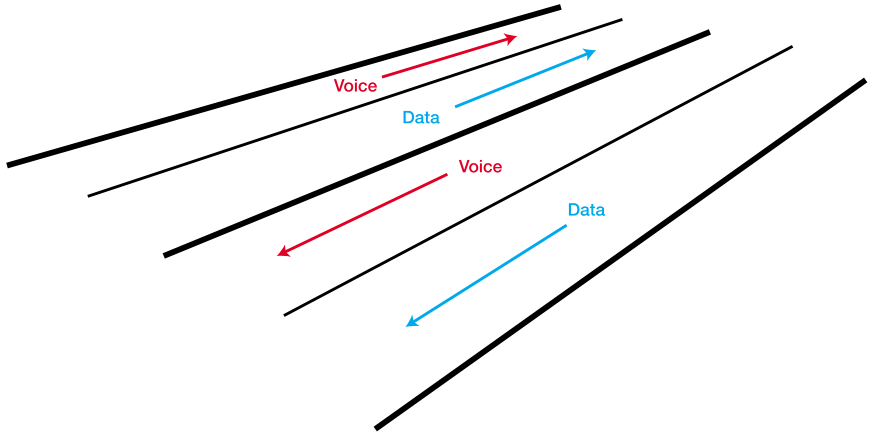
These connections will usually be made using a wireless protocol known as WiFi. WiFi technology offers a variety of potential security configurations, the main ones being WEP, WPA and WPA2. Where possible, users should ensure that the connection is made with WPA or WPA2 wireless protection (contact your mobile device vendor to see if your device supports this). If the mobile device only offers WEP protection, or no protection at all, utilising a VPN to protect the voice stream is recommended. If this is also not possible, users should be aware that their conversations are highly susceptible to confidentiality and availability attacks.

WEP, WPA and WPA2 are security protocols utilised in wireless connections. WEP offers the weakest protection of the three, and WPA2 offers the strongest.

PROTECTING YOUR COMPLETE VoIP DEPLOYMENT

Generally the security of these deployments is relatively higher than other VoIP solutions, and can be equivalent to the security offered by PSTN telephony.

- For both inbound and outbound IP connectivity, separating the Voice data from other data (e.g. web surfing, email, file sharing traffic) via a VLAN will allow better bandwidth management, and will generally improve voice quality. Some phones can automatically perform VLAN segmentation.



Separating voice streams and data streams in VLANs

- Firewalls are used to inspect packets and either allow them into your network, or reject them. If your firewall is configured incorrectly, VoIP traffic may not be able to pass into or out of your network, rendering the VoIP system inoperable. Ensure that your corporate firewall can handle the VoIP communication protocols that your VoIP solution is using (for example SIP or H.323, TLS etc.). New generations of network firewalls are often designed with VoIP security in mind and offer many voice security features.

- Protection of gateways, gateway controllers and transmission lines in between these is essential. The underlying system should be hardened (patched to the most recent release / patch), and turning off any unneeded services. Hardening can be completed with the help of operating system benchmark utilities such as the Center for Internet Security benchmark tools http://www.cisecurity.org/
- A vulnerability assessment (VA) for VoIP applications, systems and networks can help identify weaknesses in VoIP implementations if the security of the system is critical to the organisation. If such a VA is conducted, it is important to clearly define the scope and intent and allocate sufficient timing and funding to ensure the test is worthwhile.
- Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) triggers alarms if suspicious activities or events take place. VoIP specific IDS / IPS are expected to be created in future. An IPS or IDS could potentially introduce network overhead and may deteriorate the VoIP service.
- Network structure planning of VoIP infrastructure can significantly reduce the attack vectors available to malicious users. VoIP servers and infrastructure are best placed in a restricted zone on the network, which have been configured to allow only authorised users in.

PROTECTING INSTANT MESSAGING VOIP SERVICES

End user options for protecting instant messaging VoIP services (such as voice chat on MSN Messenger and QQ) is currently very limited. Use of these services should be restricted to non business related conversations, which do not require assurance of privacy or security.

GENERAL PROTECTION MEASURES

- Timely and consistent patching of applications, operating systems and device firmware is critical to managing external threats to a business' IT infrastructure. Patches are updates released by software vendors which rectify flaws which may have been found after product release. Unpatched systems may give attackers a way to break in to your systems and access data without authorisation.

  Businesses should develop a routine of periodically searching for and applying regular patches to VoIP system components and all other devices in the VoIP setup to ensure that systems are as up to date as possible. Check for
- Operating systems
- VoIP endpoints (softphones, adapters, VoIP enabled handsets)
- Any network infrastructure in the VoIP system (routers, switches, gateways etc.)
- Security applications (eg. anti-virus software)
- An uninterruptible power supply (UPS) will ensure that during an internal power outage the VoIP system can still be available for as long as the UPS can provide sufficient battery power. UPS must be available for all VoIP related power requiring infrastructure for effective backup power (handsets, workstations, servers, routers, switches and other gateway devices). For fallback service, organisations can either resort to mobile telephone capabilities, or maintain at least one traditional telephony line running on site.
- Backup planning for VoIP systems is essential in an organisation where call functionality is considered critical. To ensure the availability of telephony services, organisations can opt for backup PSTN phones, utilise QoS capabilities or run secondary backup Internet links.
- The ability to control physical access to VoIP infrastructure is an important consideration for SMEs implementing VoIP. As with any IT system, physical access to core servers would allow a malicious person to cause significant outages to the related service. For a VoIP solution, adequate physical protection is necessary for all VoIP related components.
- Monitoring access and usage is another useful way to ensure the system is used for authorised business purposes only. While monitoring of call patterns is generally easier to undertake with a VoIP system when compared to traditional telephones, the importance of effectively managing the monitoring system and ensuring the integrity of data analysis is increased.
- Ensure staff are trained in the usage of the VoIP solution. This training should include specific reference to safe use of the technology.
- Utilise strong passwords for any password fields (e.g. for logging into your softphone account or administration consoles on other solutions).

Note: Network based security controls can slow down the speed at which voice data is sent (latency), and may negatively affect the VoIP service's voice quality, as a result of inspecting traffic. The latency introduced is usually small however, and a well managed and configured VoIP system should avoid any potential availability issues caused by network security controls.

Using VoIP with Other Technologies

Perhaps one of the more interesting features of VoIP is its portable nature when compared to traditional landline telephony. Several VoIP solutions allow users to utilise their VoIP telephony solution away from base locations, via wireless technologies, publicly available network connections, and mobile capable devices, while still utilising the same telephone number or username.

While this is often a very desirable feature, using these technologies can undermine the security capabilities of a VoIP solution, as the point of connection into the network is no longer controlled by the user and can therefore introduce vulnerabilities into a VoIP system. Most of these publicly available connections will not be able to be configured by VoIP end users to improve security, or will be too complex for most such users to configure, however upcoming 'end-to-end' VoIP encryption solutions may cover these issues. If not utilising an end-to-end security solution, it would be best to avoid using VoIP over these mediums, particularly for confidential or calls which may disclose sensitive information (e.g. where credit card details must be supplied to an operator).

Using VoIP with wireless connections

VoIP can be used over wireless broadband connections, and via wireless LAN networking technologies. These wireless connections offer significantly improved mobility when compared to other networking options (such as wired solutions), and are highly valuable if considering VoIP capabilities on the go.

However, there are some disadvantages to using VoIP over wireless regarding performance and security issues. Regarding performance, wireless services may introduce heavy latency which affects the quality of the voice connection, particularly the flow of speech. In terms of security, wireless connections are susceptible to extra attack vectors beyond wired network options, so require additional security controls to properly protect. These controls may also have an adverse effect on the performance of VoIP over a wireless network.

Using VoIP with Mobile Devices

Use of VoIP over mobile devices such as 3G telephones and PDAs can offer even greater mobility. These technologies will usually utilise a specific version of a softphone solution to enable VoIP.

Use of VoIP on mobile devices may expose the VoIP calls to additional attack vectors due to these device's generally less secure operating systems and the vulnerabilities found in the wireless protocols they employ. The limited bandwidth to such devices means that introducing the required security controls to protect the calls may render the performance of the VoIP system unusable.

To better protect the privacy of calls made through networks other than those at your home or office, it is recommended to use a VPN (explained further in Section 9: Protecting your VoIP Infrastructure) to encrypt voice data if the technology supports this.

Using VoIP with other applications

Another feature increasingly seen in VoIP solutions is the integration of VoIP services with common desktop applications.

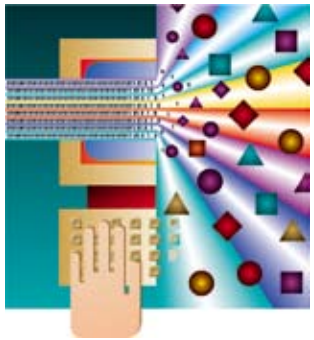
VoIP converged applications and services

- Messaging and collaboration tools – e.g. Microsoft Unified Communications, Zimbra, Cisco Unified Communications
- Conferencing software
- Customer Relationship Management (CRM) software
- Extension into web browsers, email etc.
- And many more

It is important for organisations to carefully consider all the implications involved in integrating VoIP with other applications. Security considerations are of particular concern, as the vulnerabilities from either the VoIP system or the application may carry over into the other, doubling the potential for a security weakness to arise.

Recommendations

- Minimise sensitive conversations via VoIP when using any public Internet hotspots (eg. Internet cafés, Wireless enabled cafés etc.) unless a VPN is implemented
- Contact service providers and software support regarding potential security issues of incorporating VoIP functionality into existing applications. For a comprehensive list of VoIP service providers please visit http://www.marketclarity.com.au/voip/. For further information on some of the convergence risks please visit http://www.covergence.com/content50.html.
- Ensure that all relevant applications and systems are patched with the latest security patches.
- To protect the privacy of calls, utilise a VPN to encrypt voice data.



Many VoIP systems use personal computer systems as key parts of the infrastructure. Given this, a number of activities should be followed to help secure these systems and protect the confidentiality, integrity and availability of the entire VoIP system. The following section runs through some common and key items to address to ensure the underlying computer system is secure:

Computer Security Essentials

Utilise a supported version of your operating system

For security reasons, it is extremely important to use a supported operating system and to update this with the most recent updates and patches. All users of Windows, Mac OS X and Linux should check the appropriate websites regularly for software upgrades. By using a supported version, "patches" become accessible for known security problems, protecting both the computer and contained data from becoming a target.

Prior to upgrading to the latest version of an operating system, ensure that:

* the computer is sufficiently powerful to run the new operating system;
* the application programs are compatible with the new platform; and
* data is backed up prior to the upgrade.

Create strong passwords

Follow best practice recommendations when creating passwords. Many tools exist that can rapidly 'guess' passwords. These tools can discover a simple password in a matter of minutes. However, a strong password that follows best practice "dos and don'ts" will need much longer to 'crack':

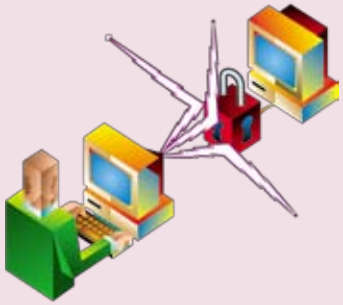
- Do change all vendor-supplied default passwords before any equipment and / or software is put into operation.
- Don't use any word that can be found in your local language.
- Don't use any word in reverse that can be found in your local language.
- Don't use any word that can be associated with the user, i.e. the user's address, phone number, birth date, pet's name, nicknames, favourite sports activity or hobby.
- Don't use consecutive letters or numbers like "abcdefg" or "234567".
- Minimise repetition of characters eg "zzzzzzzzzzzz"
- Don't use adjacent keys on the keyboard like "qwerty".
- Do make it simple enough that passwords can be remembered without being written down.
- If you have to write a password down, ensure that it is kept secure and private.
- Do use a combination of letters (upper and lower case), numbers and special characters in random order.
- Do use at least 6 characters – and using 8 or more is recommended.
- Don't give personal passwords out for any reason.
- Don't select the "remember my password" feature associated with some websites and disable this feature in Internet browsing software.
- Don't use the same password for everything - have one for non-critical activities and another for sensitive or critical activities.
- Do change passwords regularly

With these constraints in mind, it is still possible to make a strong password which is easily remembered. For example taking the lyrics "Row Row Row your boat, gently down the stream" could become: "Row3gdts".

Install a 'personal firewall' on your computer

Through the use of personal firewall software, a user can protect their computer from hackers and prevent unwanted programs from accessing their system. Although many users believe that they have nothing on their computer worth looking at or stealing, there are many other reasons why hackers may want to break into your computer.

As a result, all computers accessing the Internet should use a firewall. The occasional user is just as vulnerable as the full-time user in terms of random scanning by hackers. There are several firewalls available at no cost from major vendors.



From time to time, personal firewalls will pop up windows containing warnings which require a response to a question about access. Be sure to take the time to understand the nature of the question so the appropriate response can be given.

Install anti-virus software

Anti-virus software stops unwanted and dangerous viruses from entering computers and other devices such as PDAs and mobile phones. Viruses are software programs, and the actual effect of any particular virus depends on how it was programmed and for what purpose. Some viruses are deliberately designed to damage files on a system or in some way interfere with the computer's operation. All viruses can potentially damage or destroy files stored on a computer's hard disk. In addition to real-time protection, be sure to perform regular full virus scans of computer systems. These scans can be automated to occur at convenient times.

It is imperative that users install anti-virus software on their computers. A recent version of the software should be used, and should implement the "automatic update" option offered by most such programs to maintain up-to-date virus definitions. Unanticipated files from anyone should not be opened unless the user can positively verify what the file is, who sent it, and why it was sent to them. For email attachment virus checking, anti-virus software that is integrated into email is recommended. If this is not possible, use anti-virus software to check any suspicious email file attachment prior to opening.

Most users understand the need for anti-virus software and have installed it on their computer. However, many forget to keep the virus definitions up to date and this can actually render the software useless. The best defence is to select the "automatic update" option - this facility automatically checks for new virus definitions each time a user logs onto the Internet.

Install an anti-spyware program on your computer

Spyware is a software program used for advertising, collecting personal information for marketing purposes, or changing a computer's configuration, all without the user's consent.

Typical signs of spyware having been installed on a computer include the following:

- Pop-up advertisements even when the computer is not connected to the Internet.
- The page a browser first opens to has changed without the user's knowledge.
- A web browser has a new toolbar or other component that the user doesn't remember installing.
- The computer seems generally sluggish or takes longer than usual to complete certain tasks.
- Some settings have changed and the user can't change them back to what they were.
- For no apparent reason the user experiences a rise in computer crashes.

Users can perform regular spyware checks on systems to guard against malicious applications. Weekly scans are recommended.

IMPORTANT NOTE: Each anti-spyware program is designed to look for different types of problems. Check with different manufacturers and decide which will best meet your needs. If necessary, multiple anti-spyware programs can be installed.

Backup important data

Developing and adhering to a backup strategy is important for protecting data. There are many reasons why data is lost and they are not all related to security issues. Power blackouts, hardware failures and human errors can all cause data to be lost. The best protection is to regularly backup files. An organisation will need to decide on a backup schedule, the type of storage device and the approach to backup (eg the use of a remote backup service, or manually backing up to a portable hard drive).

Whether performed internally or through a hired service, organisations will need to determine a backup schedule, with the following backup techniques in mind:

- Full backup: a backup of the complete set of all data and system files. This generally doesn't need to be performed daily, as most files don't change every day.
- Differential backups: a backup of the set of files that have changed since the last full backup.
- Incremental backups: a backup of the set of files that have changed since the previous backup (whether it is a differential, incremental, or full backup). This takes the least time and space, but in the event of data loss, data will have to be restored from several backups and restored in the correct order.

Backup can be carried out onto tape, CD, DVD or auxiliary hard disk. There are services available today that allow users to backup with an online service, providing off-site storage that further protects data from physical disaster (e.g. fires, floods, theft, accidental erasure)

IMPORTANT NOTE: It is important to perform periodic tests of backups. What good is a backup if it can't be used to restore the system? Current best practice for SMEs is to store backups with a secure, on-line storage facility. This protects data from physical damage (e.g. fire, flood) as well as unauthorized access.

Update software regularly

Better yet, take advantage of the "automatic update" option whenever available. The software running on a computer can be a source of security problems if it is not kept up to date. After a program has been in use for a while, small problems are discovered and the manufacturer will need to create "updates" or "patches" to fix them. Additionally, with each new version of a software program, new security measures will likely be introduced, as reputable software manufacturers are working hard to make the online environment safer for users with each new release.

IMPORTANT NOTE: The "automatic update" option is the best way to keep your software up to date. These updates may be quite large however, so for organisations that utilise a volume-based Internet access plan, they may have to monitor program updates to avoid exceeding imposed download limits.

Don't open email attachments

Email attachments should NEVER be opened unless a user is certain of the source and is sure that the attachment was sent by that user intentionally. For example, email addresses can be forged to look like the sender is a person that is known and trusted to the recipient. Since most viruses, worms and Trojans are disseminated by email attachments, if in doubt, the best defence is to check with the sender before opening the file. Anti-virus software can also be used to perform a manual scan of the attachment to determine if it is safe to open.

VoIP Security Checklist

VoIP type / Security type	Security question	Check
Softphones	Does the softphone utilise secure protocols?	☐
	Do I utilise an end-to-end security solution?	☐
VoIP adapters / routers / modems	Does the adapter / router / modem utilise secure protocols?	☐
VoIP over wireless / mobile VoIP	Can the softphone utilise secure protocols? Is it configured to do so?	☐
	Is my wireless connection protected with strong encryption?	☐
Complete VoIP deployment	Are Firewalls VoIP capable?	☐
	Is voice data separated from other network data?	☐
	Are gateways and gateway controllers / call manager servers hardened?	☐
	Has a VoIP vulnerability assessment been conducted?	☐
	Are intrusion detection systems utilised?	☐
	Is VoIP access restricted to authorised users only?	☐
	Do we protect against rogue VoIP phones?	☐
General VoIP security controls	Is patching applied consistently and timely for all VoIP related technologies?	☐
	Is the power supply of VoIP technologies protected?	☐
	Do we have backup or recovery plans in case of VoIP failure?	☐
	Is the physical access of VoIP infrastructure protected?	☐
	Is call usage monitored?	☐
	Are staff aware of the implications of poor VoIP security? Do they use the technology safely?	☐

LINKS AND ACKNOWLEDGEMENTS

VOIPSA – VoIP Security Alliance

http://www.voipsa.org/

VoIPSA provides a VoIP Threat Taxonomy, which describes security threats to VoIP deployments, services and end users. VoIPSA is also working on their 'Best Practices project' and 'Security Requirements' project.

SANS Information Security Reading Room – VoIP Issues

http://www.sans.org/reading_room/whitepapers/voip/

The SANS reading room offers a selection of research papers from SANS Institute students on various aspects of VoIP security, including network threats and mitigating controls, and latency and QoS considerations and controls.

NIST Security Considerations for Voice Over IP Systems SP800-58

http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

The NIST Security Considerations for Voice Over IP Systems document offers key security controls and recommendations on how to secure an enterprise sized VoIP system. Many of the security checklist items were sourced from this document.

DISA VoIP Security Technical Implementation Guide

http://iase.disa.mil/stigs/stig/VoIP-STIG-V2R2.pdf

Developed for the Department of Defense, this paper provides suggested security controls for securing the VoIP environment. The controls are listed at a high level, and do not specifically go into a technical listing of applicable controls / tools / techniques.

Security Guidance for Deploying IP Telephony systems

http://www.nsa.gov/snac/voip/I332-016R-2005.pdf

Developed by the NSA, this guide identifies the potential vulnerabilities and associated mitigation techniques with Internet Protocol Telephony (IPT) solutions.

Market Clarity - Aussie VoIP List

http://www.marketclarity.com.au/voip/

For Australian organisations and users, this site includes a comprehensive list of many of the Australian VoIP service providers currently available.

Stay Smart Online

http://www.staysmartonline.gov.au/

An Australian Government Initiative site designed to help home users and small businesses use the Internet in a safe manner.

VoIP Security

What you need to know to read this book

Find the answers to your questions

Selecting Your Voice over IP Solution

Using Your VoIP System

Using VoIP with Other Technologies

VoIP Security Checklist

Prepared By:
SIFT Security Consultants (www.sift.com.au)
WINIT Inc (www.winitinc.com)

Proposed by Australia and Korea.

Co-sponsored by Malaysia and USA.

Produced By:
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace, Singapore 119616
Tel: (65) 68 919 600 Fax: (65) 68 919 690
Email: info@apec.org Website: www.apec.org

APEC: 208-TC-03.3 ISBN: 978-981-08-1393-2

www.apecsecurity.com