Report Number: I332-016R-2005

Security Guidance for Deploying IP Telephony Systems

Systems and Network Attack Center (SNAC)

Released: 14 February 2006
Version 1.01

SNAC.Guides@nsa.gov

This Page Intentionally Left Blank

Warnings

- Do not attempt to implement any of the recommendations in this guide without first testing in a non-operational environment.
- This document is only a guide containing recommended security practices. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This is a living document and revisions will be constant; the change control area will state modifications.

This Page Intentionally Left Blank

Table of Contents

Executive Summary

This guide identifies the potential vulnerabilities and associated mitigation techniques with Internet Protocol Telephony (IPT) solutions. It is not specific to any IP telephony solution, but covers aspects of security that must be considered in the design or purchase of an IPT system. The vulnerabilities identified here in may not apply to all organizations. It is the responsibility of the organization to develop an information security policy, determine what vulnerabilities are applicable to the organization's environment, and determine the amount of acceptable risk.

The emphasis of this guide is on the importance of mitigating IP telephony vulnerabilities, so that organizations can embrace the benefits of IPT while assuming an acceptable risk of disclosure of sensitive information or loss of service. Migration to a new type of telephony system requires understanding the vulnerabilities and risk that accompany the new system. IPT systems have many characteristics that are not present in traditional telephony solutions and many of these characteristics pose risks to the IPT network. For example, attackers require less specialized knowledge in order to attack IPT systems because IP protocols, software, and attack implementations are readily available. In addition, IPT systems are more accessible to attackers because they use IP networks, and these network are often connected to public IP networks.

This paper's guidelines strongly follow a defense-in-depth approach to security. This is key to mitigating vulnerabilities in IPT systems. Mitigations must be implemented in the network, network perimeter, servers, and phones. Mitigations in the network aim to deny access to attackers through virtual separation of data and IPT networks using virtual LANs (VLANs), and perimeter security devices such as firewalls and filtering routers. Servers and phones must be security hardened. This involves disabling unnecessary features and regularly applying software security updates. Phones must require strong authentication and authorization of users to prevent identity spoofing. Phones may also encrypt voice streams in high risk environments. The network, servers, and phones must include high availability features to meet the service availability requirement of a telephony system. This includes redundant hardware, backup power supplies, and data backup mechanisms.

Vulnerabilities have multiple mitigations of various strengths. Since implementing the strongest mitigations is not always possible or necessary, mitigations are categorized by their strength or robustness. The minimum robustness should be implemented by all organizations. The middle level represents best practices. The highest level represents mitigations, which may be very difficult to implement, but necessary in mission critical settings. While an IPT solution designer could choose one desired robustness level and implement all mitigations for that level, no robustness level will exactly fit any environment. Instead, robustness levels should be used as a baseline and deviations made based on established security policies and accepted levels of risk.

Introduction

This guide identifies the potential vulnerabilities and associated mitigation techniques with Internet Protocol Telephony (IPT) solutions.

This guide is not specific to any IP telephony solution, but covers all aspects of security that must be considered in the design or purchase of an IP telephony system. As a result, it does not explain how to implement the vulnerability mitigation guidelines, as that information is specific to the solution chosen. Nor does this guide address individual voice over IP (VoIP) protocols. Further research is necessary to determine how the mitigation guidelines described should be applied to any specific IPT system. Readers should consult product documentation and vendors to determine how to implement the mitigation guidelines.

Not all identified vulnerabilities may be of concern to all organizations. This depends on the IPT system and installation environment. Readers must define what represents an acceptable level of risk to their organization in a security policy, and then apply these mitigations to meet that policy.

The emphasis of this guide is on the importance of mitigating IP telephony vulnerabilities, so that organizations can embrace the benefits of IPT while assuming an acceptable risk of disclosure of sensitive information or loss of service. This emphasis should not be taken as a recommendation against IPT, but as concerns that must be addressed to ensure reasonably secure use of IPT. Following all the mitigation guidelines does not guarantee that an IPT network is impervious to attack because not all vulnerabilities can be anticipated. However, applying the guidelines will provide reasonable security for most environments.

The mitigation guidelines strongly follow a defense-in-depth approach to IPT security. By planning multiple levels of defense, an organization can protect itself against unforeseen vulnerabilities in their IPT systems. This is especially important with a technology as new as IPT, in which many security features have not fully matured.

The guidelines presented within are not to be construed as NSA requirements for deploying IPT solutions. They are recommendations made in order to aid the IPT community to create and use IPT as securely as possible.

Audience

This guide is targeted at the managers, architects, and administrators of IPT networks. Managers can use this guide to learn about the vulnerabilities organizations face by implementing an IPT solution. Architects can use this guide as an aid when evaluating the security of various IPT solutions. Administrators can use this guide to improve the security of existing IPT networks.

The reader should be familiar with the concepts of VoIP and IP telephony, however, detailed knowledge of the VoIP protocols is not a prerequisite to understanding the guidelines. Application of the guidelines to an operational network requires an in-depth understanding of the IP telephony solution being deployed and the associated network infrastructure. This guide does not cover how to apply the guidelines.

Motivation

IPT is being adopted by many organizations. Organizations are either integrating IPT with their legacy telephony systems or completely replacing their legacy systems with

IPT. This is often due to expectations of lower total cost of ownership and benefits from numerous advanced IPT features.

Migration to a new type of telephony system requires understanding the security risks that accompany the new system. An IPT solution may provide the same ability to make and receive calls as a legacy telephony solution, but the underlying architectures are completely different. These differences affect the approach to securing the telephony system.

IPT systems have many features that are not present in legacy telephony solutions and many of these features pose risks to the IPT network. Features such as network services (HTTP, SNMP, telnet) on phones, wireless access built into phones, Internet access to telephony servers, network management of phones and servers, and software-only phones all create new avenues of attack that did not exist with traditional solutions. Employing more features generally increases exposure to vulnerabilities.

IPT solutions are no longer limited to proprietary software and protocols like many legacy telephony solutions, and therefore the barrier to entry for attackers in terms of knowledge and equipment is much lower. IPT solutions are primarily based upon open and standardized protocols, such as Session Initiation Protocol (SIP) and H.323. Software implementing these protocols is readily available. The equipment used by IPT solutions is based on readily available PC architectures. The underlying operating systems are general-purpose, widely used, and have numerous published vulnerabilities. Many legacy solutions required proprietary hardware and software, which was expensive and more difficult to obtain. These differences affect both the back-end infrastructure and phones.

Information carried by IPT solutions is more accessible to attackers if proper precautions are not taken. Whereas legacy telephony solutions had a dedicated wire between the switch and phone, IPT solutions share the wire and network infrastructure equipment with the existing data network. Accessing information carried by a dedicated wire requires physical access to the wire or switching equipment. On IP networks, by default, every device is accessible from other devices on the same network. Proper manipulation of the network could result in access to the information streams of other devices.

IPT solutions are likely to be connected to public IP networks such as the Internet. This is done to trunk calls over cheaper IP networks or to enable remote management of the system. Legacy solutions were not connected to public IP networks to the same degree. Calls were transferred in and out of an organization using networks controlled by the telephone company and remote management was usually performed over a dedicated analog modem connection.

IPT replaces the dedicated infrastructure of a legacy solution with an IP network. Commonly IPT is added to an existing data network. Changes to the existing network may be necessary if the security policy for the network does not meet the telephony requirements. Adding telephony to the data network may significantly increase the number of devices. Administrators must be prepared to manage the security of these devices.

Organization

The remainder of this guide is divided into two parts. The first part contains the bulk of the guide, and describes the vulnerabilities and vulnerability mitigations associated with IPT. It addresses the IPT network from the standpoint of an already existing data network. When implementing an IPT solution on a data network, a network

administrator must add the voice components to the existing data network, and in some cases change the existing hardware to be able to support the new requirements for the IPT network. The components that must be added or changed on the network include IP telephones, IPT servers, network infrastructure hardware, and network perimeter hardware. Each addition requires that the administrator secure the devices themselves, and in some cases the network surrounding the device, implementing defense-in-depth at each level as new devices are added to the network. Risks and mitigations will be approached from this perspective.

The second part is an appendix, which contains a chart of all the mitigation guidelines. Before consulting this chart readers should be familiar with the rest of the guide.

Definitions

Application-level firewall
Network border device that filters IP packets based on inspection of the application layer content.

Bluetooth
Short range personal area network wireless technology.

Convergence
The merging of traditionally separate voice and data networks and applications. The data network is offering traditional voice services and voice devices are offering traditional data services.

Data network
Network carrying traffic related to traditional TCP/IP services such as email, web, and file transfer. Excludes voice services.

Data synchronization
Making data, which is common to multiple devices consistent in the face of changes to the data on one or more devices. Example: Synchronizing a calendar on a handheld computer with the personal information manager on the desktop computer.

Defense-in-depth
Security protection based on multiple mechanisms deployed throughout an organization or layers of mechanisms at a single point, instead of a single mechanism deployed at a single point.

Embedded system
Dedicated special purpose computer used in a non-desktop computer form factor, such as in a VoIP telephone.

H.323
A set of International Telecommunication Union (ITU) standard protocols for VoIP. It includes, but is not limited to, H.245 and H.225. These protocols are binary encoded using the ASN.1 and BER standards. H.323 also utilizes the IETF Real Time Protocol (RTP).

IPT (Internet Protocol Telephony)
Includes the features commonly associated with a legacy PBX-based telephony network, such as phones, voice mail, conferencing, call transfer, and PSTN interconnections.

IPT system
References all devices needed to implement a complete IP telephony solution in an organization. Includes, but not limited to, phones, servers, and gateways.

IPT network
Network carrying traffic related to the IP telephony system. Primarily includes signaling, voice, and other multimedia traffic.

IPT device
Any computer or embedded system used as part of the IP telephony system.

IPT phone
Analogous to a traditional telephone handset, but contains an embedded system implementing VoIP.

IrDA (Infrared Data Association)
Short range point-to-point wireless link utilizing the infrared spectrum. Commonly implemented by handheld computers, printers, mobile phones, and IPT phones.

Local network segment
Portion of the network connected to the same Ethernet switch port or hub (collision domain).

Malicious code
Any computer program or portion of a computer program, which performs unauthorized or damaging operations, such as viruses, trojan horses, spyware, and worms.

Man-in-the-middle attack
Attacker uses any of a number of methods to route a victim's network traffic to the attacker's computer where the attacker can capture and/or manipulate the traffic before forwarding it to the intended destination.

Media stream
Portion of a VoIP session which carries encoded audio, encoded video, or other multimedia data. The Real Time Protocol (RTP) is most often used for carrying the media stream.

Packet filtering router
A network router, which can deny or accept packets based on fields in the network (layer 3) and transport (layer 4) layers.

PBX (Public Branch Exchange)
A private circuit switched telephone network traditionally used within an organization. PBXs have dedicated switching equipment and dedicated telephone lines. Newer PBXes include VoIP capabilities, but references to a PBX in this guide refer to a circuit-switched or legacy PBX.

Personal Area Network
The network used to interconnect portable devices carried on the person or connect such devices to larger networks. Personal area networks have limited range (less than 30 feet) and are most often wireless. Examples include Bluetooth and IrDA.

Real Time Protocol
Internet Engineering Task Force (IETF) standard for streaming of different types of media, such as audio and video, via an IP network. Defined in RFC 3550.

Secure channel
Network channel or tunnel through which all data is provided with confidentiality and integrity protections. Examples include IPSEC, TLS, and SSH.

Session Initiation Protocol (SIP)
VoIP protocol standardized by the Internet Engineering Task Force in RFC 3261. SIP is a text-based protocol similar to HTTP, which operates over TCP and UDP port 5060.

Signaling protocol
Protocol used for setting up and tearing down VoIP sessions. The signaling protocol is also responsible for enabling features such as hold, call forwarding, and call transfer. The Session Initiation Protocol (SIP) and H.323 are two common signaling protocols.

SNMP (Simple Network Management Protocol)
Protocol used to read and write device management settings to any supporting device connected to the network.

Softswitch
IP telephony device, which uses signaling protocols to manage IP phones, route calls, and implement call features such as hold, conferencing, and forwarding. Softswitches are often implemented on PC-based servers running commercial operating systems.

Softphone
IPT phone that runs as a software application on a desktop computer instead of using a dedicated hardware device.

TLS (Transport Layer Security)
Application-layer protocol, which provides confidentiality, integrity, and mutual authentication services. This is the IETF standardized version of Secure Sockets Layer (SSL) version 3.

VLAN (Virtual Local Area Network)
Network devices logically grouped together into the same subnet (broadcast domain) even though they are geographically distributed. This is achieved by configuring the network management software to tag packets as belonging to a certain VLAN instead of by physically reconfiguring the network.

Voice gateway
VoIP interface to a traditional telephony network such as the PSTN or a PBX. A voice gateway translates VoIP signaling protocols and media streams into a format understood by the traditional circuit switched networks.

VoIP (Voice over Internet Protocol)
The techniques and protocols for transmitting voice and other multimedia sessions over IP networks.

WiFi (Wireless Fidelity)
Wireless LAN technology with a medium range (300 feet). Also known by WLAN and its IEEE standard name, 802.11a/b/g.

IP Telephony Vulnerability Mitigation Guidelines

IP telephony solutions are usually deployed on existing data networks. Different devices, such as servers, IP phones, and gateways, must be added to the network to implement IPT. The devices themselves must be configured to mitigate a variety of security vulnerabilities. In addition, defense-in-depth necessitates modifying the existing network infrastructure to protect the IPT devices and the data network devices from each other. This dual layer, device and network, of protection is essential.

This part of the guide discusses the vulnerabilities and mitigations associated with adding IPT devices to the network in a step-by-step manner. The network infrastructure must be prepared, and the network perimeter (firewalls and gateways) secured before any IPT devices are deployed. Then, IPT servers can be added to the network. Finally, the IP phones are configured and deployed to users. Following this order ensures that no devices are left unprotected during deployment and that users have full functionality and call quality upon initial deployment. Figure 1 shows the completed IPT and data network, and will be used to illustrate each step of security deployment.

Each section first describes the vulnerabilities that must be addressed, and then presents possible ways to mitigate the vulnerabilities. In many instances, multiple mitigation strategies are given. The mitigation that should be used in an operational IPT network depends on many factors including established security policies, risk acceptance, the sensitivity of the information on that network, and the level of reliability needed. To aid in deciding what mitigations to implement, each section concludes with a chart that characterizes mitigations based on their robustness.

Security Robustness Levels

Security robustness describes the strength of mitigations that an architect can specify or an administrator can implement to protect the IPT system from attackers. A higher robustness level means an IPT system is better protected against attackers, but achieving that level is usually more difficult. The following definitions of robustness are applicable only to this guide. There are three levels:

- *Highest Robustness* – These mitigations represent the best way to protect an IPT system within the limits of current technology standards and can be implemented without sacrificing the basic features of a telephony solution, such as the ability to make and receive calls, call transfers, call holding, and voicemail. In many cases, these mitigations provide more protection against attack than a legacy PBX system. These mitigations may be difficult to implement because they do not scale or are not fully supported by existing products. However, in some environments the extra effort may be necessary.
- *Medium Robustness* – These mitigations represent the best practices for designing and administering an IP telephony solution that will provide a level of security as least as good as that of legacy PBX systems. All IP telephony systems should strive to implement all these mitigations.

- *Minimum Robustness* – These mitigations represent the bare minimum any IP telephony solution should follow in order to be considered acceptable for use. Not implementing these mitigations presents an unacceptable risk to any organization.

Choosing a robustness level for an IPT network is not a simple task. The robustness necessary for a specific environment depends on factors such as the value of the information being protected, motivation of attackers, resources available to attackers, accessibility (both physical and over the network) of the environment to attackers, trustworthiness of insiders, resiliency to denial of service. These factors all contribute to the likelihood and impact (risk) of a successful attack. The greater the risk, the more robust a security level is needed.

For example, an environment that contains high value information, but is on a physically isolated network and faces no insider threat could choose the minimum robustness level. If the same network was in a hostile area or offered services over the Internet, then the highest robustness level would be more appropriate.

In most cases, no network will fit into a single level. Mitigations from each level must be mixed and matched to meet the specific needs of a network. For example, an organization that suffers small damages due to compromised internal information may suffer large damages if access to that same information is lost. In this case, the organization should focus on the mitigations related to denial of service and backup rather than confidentiality.

Making these types of decisions require a security policy that identifies the value of information and the impact of loss or compromise of that information. Assessing this value is very important to effectively applying mitigations.

Network Guidelines

IPT security is dependent on defense-in-depth, and thus the network is a critical place to implement security. The convergence of data and IPT networks requires the network be modified to address threats related to IPT systems. Network infrastructure (Figure 1), in this context, refers to devices that handle data below the application layer such as switches, routers, and filtering firewalls.

First, IPT makes telephony infrastructure, such as phones and servers, more accessible to attackers. Attacks against the telephony network are performed using the same tools used to attack data networks, and attackers can connect to IPT infrastructure using the data network. Separating the telephony and data networks makes penetrating the IPT systems harder.

Second, because phone calls are now carried over more accessible data networks, eavesdropping is more of a risk. Network security can help make eavesdropping more difficult, but cannot eliminate the risk altogether.

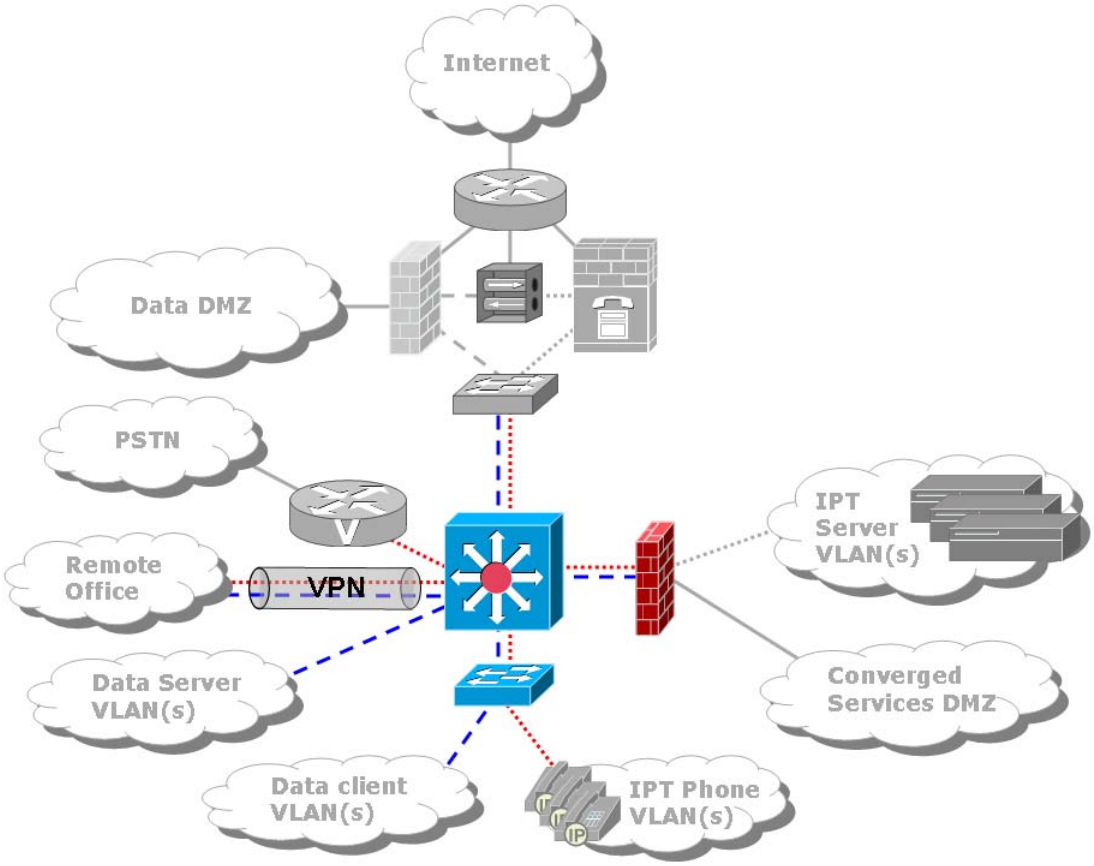

Figure 1 – Defense-in-depth requires implementing mitigations within the network infrastructure. Virtual separation of IPT and data networks using VLANs and filtering makes it easier to prevent problems on one network from affecting the other. Mitigations in the network also make eavesdropping more difficult. Administrative VLAN is not shown.

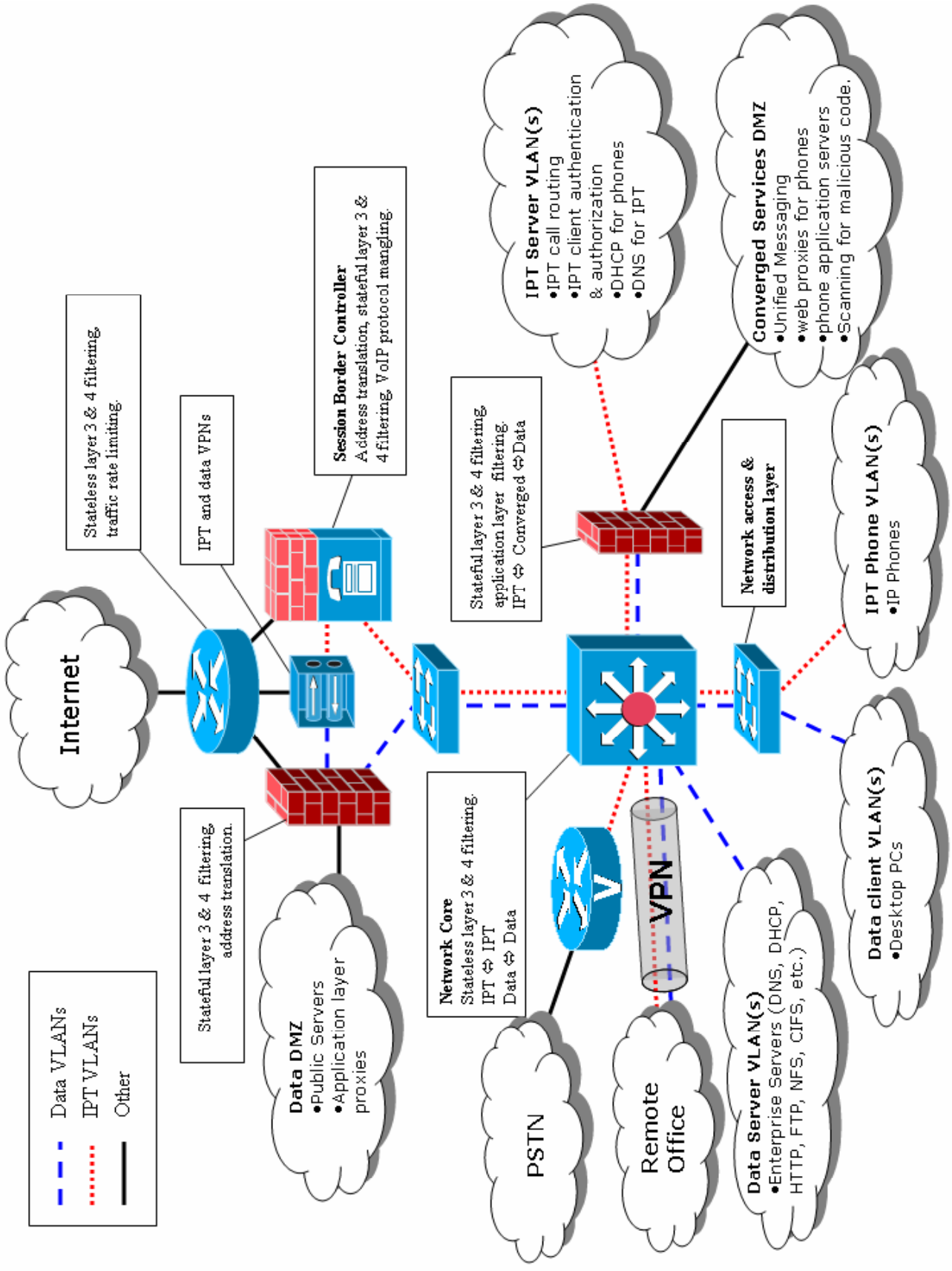

Figure 2 – Logical diagram of converged IPT and data network.

Finally, the data network must now meet the same reliability requirements as a traditional telephony network. This means implementing redundancy, physical protection of the network infrastructure, power backup, and data backup.

Figure 2 shows a logical diagram of a converged IPT and data network. Some functionality implemented using multiple devices in the diagram could be combined into a single device. For example, a HTTP proxy could be part of firewall rather than a separate server. The diagram also illustrates the separation of IPT and data networks using a different colored and dashed line for each VLAN. Additional VLANs could be used in the network design, but to keep the diagram simple all IPT-related VLANs are represented by a single line type, as are all data-related VLANs.

This network layout represents a medium robustness level. Layouts for the minimum and highest robustness levels differ primarily in the allowed connections between the IPT and data networks. In the highest robustness level, no interconnection is permitted. Thus, the converged services cloud and the attached firewall should be removed. At the minimum robustness level, an application-layer firewall is not used between the converged services, data, and IPT networks. Instead, traffic is routed directly between the networks with only stateful layer 3 & 4 traffic filtering, and the converged services DMZ is optional.

Accessibility and Network Separation

Physical convergence of voice and data networks is an advantage of IPT systems. However, placing both systems on the same network means both are now susceptible to the same attacks and the same attackers. Once an attacker has penetrated the network both data services and IPT will be vulnerable. This violates the basic defense-in-depth principle, because vulnerabilities in one part of the network make another part of the network, namely the telephony system, more vulnerable. The border between the voice and data networks should be treated no differently that the border between a private intranet and an untrusted network.

Virtual LANs

To reduce the probability of a successful network penetration also affecting the telephony network, the telephony and data networks must be logically separated using virtual LANs (VLANs). While VLANs were not designed as a security mechanism, they can be used to enable security features, such as by placing access controls on the type of traffic that is allowed on specific VLANs. VLANs allow telephony traffic to be isolated from data traffic and vice versa, while enabling any interactions between them to be tightly controlled. This limits the reconnaissance an attacker can perform against the telephony network from the data network, and limits the protocols an attacker can exploit.

For network separation to be effective, several different protected VLANs must be established. First, all network devices not specifically used to support IPT should be placed on data VLANs. These VLANs would support PCs, file servers, email servers, domain controllers, and the like. IPT devices should be placed on different VLANs depending on their role in the network. Limiting each VLAN to like devices and protocols makes the development, implementation, and management of security features much easier. All standalone IP phones should be placed in their own IPT phone VLAN(s). IPT servers should be placed in different VLANs depending on the VoIP protocol they implement. For instance, all H.323 servers should be on a H.323 only VLAN, and all SIP servers should be placed on a SIP VLAN. This may not be possible if a single server implements multiple protocols. Softphones should also be

placed on dedicated VLAN(s) (see *Softphones* on page 45). At minimum, IPT and data devices should be on separate VLANs.

The IPT and data VLANs must have their own servers for standard network services such as DNS, DHCP, and NTP. This is necessary because traffic from these services should not have to cross the perimeter between IPT and data VLANs.

Network separation does not prevent an attacker who has physical access to the network, as a malicious insider would, from bypassing any VLAN separation by simply unplugging the IP phone's network cable and attaching an attack computer. To prevent this, switch port level security must also be implemented. Layer 2 access switches should be configured to only accept traffic from known MAC addresses. A better solution is to use phones and switches which support 802.1x authentication. This will prevent unauthorized devices from connecting to the network at layer 2. When using 802.1x the IP phone users must not know or have access to the secrets used to authenticate the device to the switch, because that would negate any benefit of 802.1x access control. With access to these secrets, a user could connect an unapproved device to the network. Even with 802.1x enabled, an attacker can still

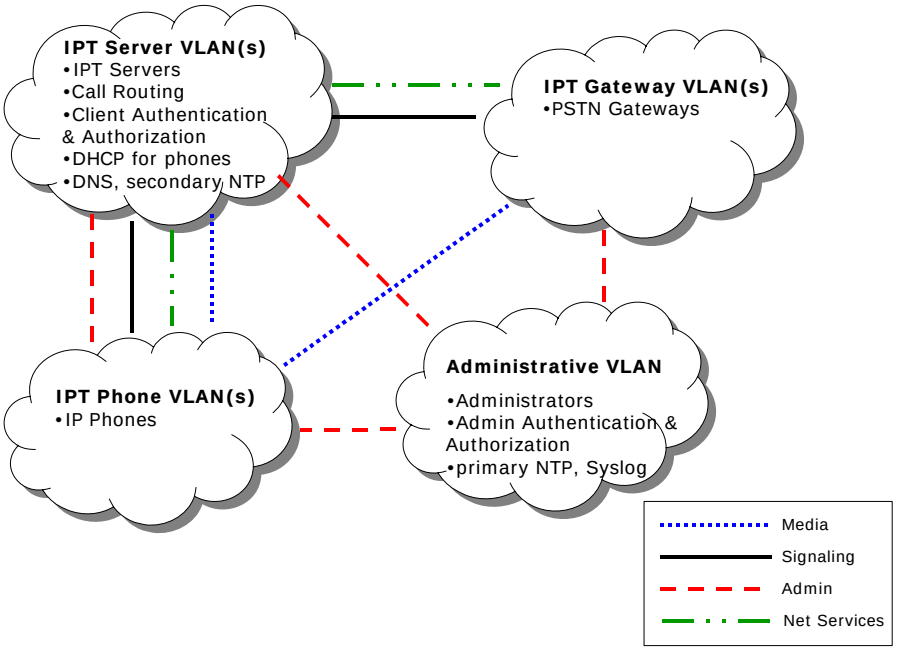

Figure 3 - IPT services grouped into four VLANs. The lines between VLAN clouds represent the network services that must be allowed between VLANs. The IPT server VLAN contains IPT servers implementing call routing, authentication, and authorization. The IPT phone VLAN contains IP phones. The IPT Gateway VLAN contains gateways to external network such as the PSTN. The administrative VLAN is used by administrators to manage and configure IPT devices, provide the primary time source to infrastructure devices and servers, and accept all logging information. The server VLAN must communicate with the phone and gateway VLANs using signaling protocols to setup and authorize calls. The IPT phone VLAN must exchange media traffic with the gateway VLAN and with the server VLAN if voicemail applications run on the servers. The IPT server and phone VLANs also share administrative protocols so that IPT servers can configure IP phones. These may be different protocols than those used by the administrative VLAN. The IPT server VLAN provides network services, such as DNS and NTP, which are used by most devices on the IPT network.

wait for an authorized device to authenticate, and then spoof that device's link layer address. The access switch should re-authenticate the device at short, regular intervals to make this more difficult.

Traffic Filtering and Firewalling

Dividing the network into multiple VLANs does not provide any benefit if the traffic between the VLANs is not restricted. Traffic between IPT VLANs must be controlled by packet filtering routers or layer three switches. The access control lists (ACLs) on these devices must be configured to only allow IP phones to connect to the IPT servers the phone needs to function and vise versa. For example, a SIP phone does not need to communicate with an H.323 gatekeeper. In many cases, this means that only VoIP signaling protocols need to be allowed between phones and IPT servers. Filtering should be done based on IP address, port number, and TCP/IP flags, not port number alone. Figure 3 illustrates the services that should be allowed between IPT related VLANs.

At minimum, the IPT and data VLANs should be separated by stateful layer 3 & 4 traffic filtering configured to block all protocols except those required for IPT features.

A more robust solution is to use an application-layer firewall to separate the IPT VLANs from the data VLANs. The application-layer firewall and associated DMZ will function as a checkpoint for all traffic between the IPT and data networks. No traffic should be allowed directly between the IPT VLANs and the data VLANs without being examined at the application layer by either the firewall or a proxy device in the DMZ. Despite this filtering, a minimal number of protocols should be allowed through the firewall or into the DMZ. If alternatives exist which eliminate the need for network traffic between the IPT and data networks, they should be used. For example, disable the web interface on the IP phone, and allow users to manage the phone on a central server that would securely push changes to the phone. See *Remote Management of VoIP Phones* on page 34 for further discussion.

Some devices, such as unified messaging servers, fulfill roles on both networks, and thus need access to both the data and IPT VLANs. These types of devices should be placed in the DMZ managed by the application-layer firewall separating the IPT and data networks.

Call Eavesdropping

Eavesdropping on unencrypted voice communication is more likely when conversations travel over a general use IP network. Media streams are easily reconstructed if packets can be captured. Security protections at the network layer can make call eavesdropping more difficult, but not prevent it.

A switched network means that network traffic is not broadcast to all devices connected to a switch, thus making packet capturing more difficult. However, there are methods to subvert the switch. One method is to flood the switch with traffic, which overfills the MAC address table causing the switch to broadcast traffic on all ports. The other method of subverting a switched network is to implement a man-in-the-middle attack. In this case, an attacker pretends to be the victim device by spoofing the victim's MAC address.

Mitigations

This can be dealt with by configuring the switch to alert an administrator or intrusion detection system when the switch is flooded with traffic. The switch could also be configured to cease sending any traffic if it is unable to properly switch traffic. However, this would create an easy denial of service attack.

Man-in-the-middle attacks can be mitigated by statically assigning MAC addresses to each switch port and allowing no other MAC address on that port. This could be difficult to manage on a large scale. Some switch vendors offer an alternative solution. The switch can detect a relationship between IP address, MAC address, and switch port by monitoring DHCP packets. The switch will only allow traffic on a port that matches the stored IP and MAC address pairs.

While the above techniques make eavesdropping more difficult, they are by no means robust. The best and only robust solution to eavesdropping is to encrypt all voice traffic on the network from end to end. *Eavesdropping and Impersonation* on page 40 discusses encrypting voice traffic in more detail.

Network Availability and Physical Access

Moving telephony to an IP network means that the IP network must meet the physical infrastructure requirements of a telephony network for reliability, availability, physical access control, power backup, and data backup.

Mitigations

Physical access to network hardware must be granted only to authorized personnel. With physical access to equipment an attacker can disable the network, eavesdrop, and otherwise attack the IPT system. All network hardware must be in restricted and controlled access areas. Video surveillance would be another good measure. Mitigations discussed in *Physical Security* on page 23 are applicable here also. The extent of the physical access control is dependent on the security policy governing the network.

Network hardware must also have power backup. Traditional phones receive their power over the phone line from the PBX switch. If building power fails and the PBX switch has power backup, then the telephony system continues to operate. The IP network must be configured to offer the same resilience. IP phones must receive power over the network cable using power-over-Ethernet technology. The network hardware must be provided with battery backups so that connectivity and phone operation is not lost when building power is lost.

Many network infrastructure devices are full-fledged computing devices and thus have sophisticated configurations. Firmware images and configuration files necessary for restoring a network device after a crash must be backed up regularly. A backup and recovery policy must be in place and processes must be tested. Backups must be stored in a secure location, such as an environmentally controlled and locked room. Backups that leave the physical control of the organization should be encrypted. This is all necessary to ensure the network is restored to operational status quickly after an attack or other events cause the network to fail.

Denial of Service

Denial of service (DoS) attacks take many forms and are difficult to prevent. DoS attacks can use software vulnerabilities to disable devices, consume resources on a device, or consume excessive amounts of network bandwidth. The first two are addressed by improving software security, and are discussed in *Software Security* on page 20. Over-consumption of network bandwidth can be addressed at the network level.

Mitigations

DoS attacks on network bandwidth can directly target IPT devices. Limiting the rate of traffic to IPT VLANs can reduce the effects of such an attack coming from outside

the IPT network. When designing the IPT network, determine the number of simultaneous incoming external calls that can be handled without detrimentally affecting the ability to place internal calls. Use network perimeter devices such as firewalls and filtering routers to limit the bandwidth allocated to incoming external calls. This should limit the amount of network traffic allowed into IPT VLANs. Also, configure IPT servers to accept a limited number of external calls. This will help protect the ability to place internal calls, however, attackers will still be able to disable external calling with a DoS attack.

Alternatively, DoS attacks can target other network services such as web and email servers. Most often, these types of attacks will be directed at publicly accessible services, and can consume all available Internet bandwidth. When such an attack occurs, external VoIP services are lost. Having a secondary Internet connection and/or a small pool of PSTN connections will help ensure limited continuity of external VoIP service if such an attack occurs.

Such an attack could occur internally if a fast spreading worm infects the network as occurred with the Code Red and Slammer worms. Separating data and IPT networks also helps in this instance since routers should be configured to prioritize IPT VLAN traffic over data VLAN traffic. Other router quality of service mechanisms can also be employed. Of course, the best defense is to not become infected with fast spreading worms in the first place by following data networking best practices like using anti-virus software on PCs and email servers and promptly applying software security updates.

Network Intrusion Detection

Detecting an intrusion into the data or IPT networks before the attacker has time to further attack internal systems limits the amount of damage done by the attacker. Selecting, and configuring network intrusion detection systems (IDS) is beyond the scope of this guide, however, IDSes should be placed at strategic points in both the data and IPT networks. Detecting an attacker in either network before they can penetrate the other network allows an administrator to protect the other network.

Mitigations Summary

Major sections conclude with a chart listing the mitigations discussed in that section. The mitigations are described briefly in the table. Read the section text to fully understand the vulnerability and associated mitigation.

A single mitigation may be appropriate at multiple robustness levels (minimum, medium, or highest). An ‘X’ in the column for a robustness level indicates that mitigation meets this level of robustness.

Mitigation	Minimum	Medium	Highest
Accessibility and Network Separation			
Place IPT phones, IPT servers, and data devices on separate VLANs.	X	X	X
Place IPT servers and gateways each on their own VLANs separate from IPT phones and data devices.		X	X
Place IPT servers implementing different protocols on separate VLANs. Example: a SIP VLAN and a H.323 VLAN.			X
Enable port level security on all switches.	X	X	X

Mitigation	Minimum	Medium	Highest
802.1x authentication is required of all devices connecting to the IPT network.			X
Traffic flow between IPT VLANs is controlled by packet filtering routers.	X	X	X
No network traffic is allowed between the IPT and data VLANs.			X
Traffic between the IPT and data VLANs is controlled by a layer 3 & 4 stateful firewall. Filtering traffic at the application layer is not required.	X		
Traffic between the IPT and data VLANs is controlled by an application-layer firewall.		X	
Servers needing access to devices in both the IPT and data network are kept in a DMZ connected to the firewall separating the IPT and data networks, e.g., unified message servers.	X	X	
The IPT network and the data network have separate servers for common network services such as DNS, DHCP, and NTP.	X	X	X
Call Eavesdropping			
Switched network.	X	X	X
Ethernet switch ports are configured to only allow known MAC addresses. **OR** Ethernet switches only allow traffic that matches the IP address and MAC address assigned to a port during a DHCP lease.		X	X
Configure switches to alert administrators when MAC address tables overflow.		X	X
Encrypt all IPT traffic end-to-end. See *Eavesdropping and Impersonation* on page 40.			X
Network Availability and Physical Access			
Network hardware is in a restricted access area. The section *Physical Security* on page 23 is also applicable here.	X	X	X
All network closets are monitored with video surveillance.			X
Network equipment has short-term power backup.	X	X	
Network equipment has long-term power backup.			X
IP phones obtain power from the network cable.	X	X	X
Network backup power is sufficient to supply power to IP phones.	X	X	X
All network equipment has configurations and software backed up regularly.	X	X	X
Backup and recovery policy is in place.	X	X	X
Backup and recovery processes are tested.	X	X	X
Backups are stored in an environmentally controlled and locked room.	X	X	X
Backups are encrypted when not under physical control of the organization.	X	X	X
Configuration and software backups are kept off site.			X
Denial of Service			

Mitigation	Minimum	Medium	Highest
Determine the number of incoming external calls the IPT network can handle and still adequately support internal calls. Use network perimeter devices to allocate bandwidth only sufficient for that number of external calls.		X	X
Limit the number of external calls accepted by the IPT servers.		X	X
Use routers to prioritize IPT VLAN traffic over data VLAN traffic.		X	X
Use anti-virus software and promptly apply software security updates.	X	X	X
Network Intrusion Detection			
Install network intrusion detection systems to monitor both IPT and data networks.		X	X

Perimeter Security Guidelines

The network perimeter (Figure 4) is where all communication external to the organization enters or leaves. Gateways are necessary if users are to communicate outside of the local IPT network. This should be done next to allow immediate communication with external entities following the replacement of the traditional telephones with IP telephones.

The perimeter, in this case, refers to the external method of communication for the IPT system only. This includes PSTN gateways (which bridge IPT communications with the external traditional telephony system), session border controllers (which are a technology that effectively acts as an application layer proxy for VoIP calls of other IPT systems), and virtual private networks (which create an encrypted tunnel for remote sites or users).

PSTN Gateways

PSTN gateways connect an IPT system to the traditional telephony network. The threat presented by gateway devices is that malicious users could connect directly to the gateway device and make unauthorized calls. Gateways operate using some of the same protocols as IP phones. A phone could be configured to directly connect to

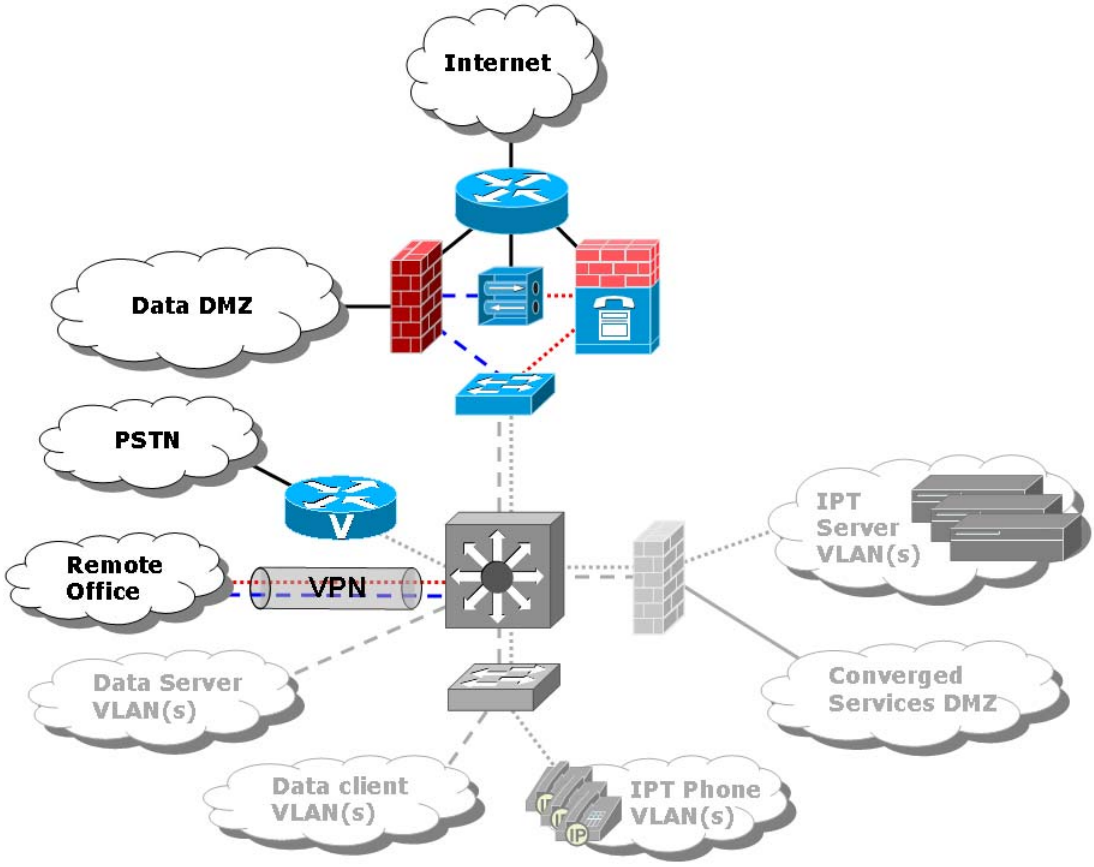

Figure 4 – The next part of the IPT system to deploy and secure is the network perimeter. This consists of the Internet firewalls and PSTN gateways. A VoIP application-level firewall, often called a session border controller, is necessary for IPT traffic over the Internet.

the gateway to place calls, and thus bypass the access control provided by an IPT server. Another problem with some PSTN gateways is they can directly pass PSTN signaling messages to internal IPT servers. This could allow a direct attack against the IPT servers.

Note that once calls are routed over the PSTN any encryption of the voice or signaling protocols done on the internal network is lost, because all calls over the PSTN are unencrypted.

Mitigations

The best way to prevent unauthorized calls is to require callers to authenticate to the gateway before the gateway will complete a call. Some gateways query a separate server to check if a call is authorized. In this case, a secure channel must be used between the gateway and the authorization server.

PSTN gateways should be placed on their own VLAN. Packet filtering should be used to allow signaling messages from authorized servers only. IP phones should not be able to send signaling messages directly to the gateway, and instead should use the IPT server as an intermediary.

Gateways must validate and terminate all PSTN signaling at the gateway. The gateway should convert PSTN signaling messages to VoIP signaling messages. This reduces the likelihood of a successful attack on the IPT servers through the gateway. An attacker could still directly attack the gateway and use it as a platform for attacking other IPT devices.

The software on gateways should have security updates applied regularly.

Public IP Networks as Voice Carriers

One of the cost benefits of VoIP is the ability to use private or public IP networks to carry voice traffic between physically separate offices or between organizations. This use of VoIP requires special security consideration, because the organization has little control over its voice traffic once it enters other networks.

Once on the public network, an organization's telephony traffic will traverse computers and networks owned by any number of third parties who could intercept and modify packets without the caller's knowledge. An organization's internal network policy may allow telephony traffic to be sent in the clear; however, the accessibility of telephony traffic on a public network necessitates the use of encryption and authentication to establish a secure channel between the calling parties. Interoffice communication can be established using VPNs. A VPN is likely already established between offices for data traffic. However, since IPT and data networks are kept on separate VLANs, a separate VPN must be established for IPT traffic or the VPN must respect and maintain VLAN separation.

VoIP is also used to establish calls between different organizations in order to avoid use of the PSTN. In this case, an organization should not trust traffic from other organizations and should hide its network topology from other organizations. These goals generally necessitate the use of a firewall and network address translation (NAT) on the network's border. The addition of a firewall using NAT presents several challenges. VoIP media streams use dynamic ports. Thus, the firewall must dynamically open "pinholes" in its protection to let through VoIP traffic. Most VoIP protocols include IP addresses in the bodies of their messages. The external and internal IP addresses are different when using NAT. Thus, the messages must be modified when they traverse the firewall. This presents a further challenge if VoIP sessions are encrypted or signed. The firewall must be able to decrypt and encrypt

the messages. Alternatively, a phone can use end-to-end call encryption. This requires the phone learn its external address and use the external address instead of the internal address when establishing the encrypted call. This way the firewall does not need to modify the messages.

Session Border Controllers

A class of products called session border controllers (SBC) addresses some of these problems. A SBC sits on the edge of the network next to a traditional network firewall or could be an integral component of the network firewall. VoIP sessions are routed through the SBC. The SBC takes care of rewriting signaling messages and opening holes in the firewall for media streams. The SBC replaces internal IP addresses found in the signaling messages with external IP addresses. This is needed when network address translation (NAT) is used between the internal and external networks. Some SBCs also provide services, such as STUN (Simple Traversal of UDP over NAT), that allow a phone to learn its external address. Note that an SBC cannot handle encrypted signaling messages. A SBC type device is necessary when using VoIP between organizations.

Wide Area Network (WAN) Links

Network connections to remote offices are considered part of the internal network and thus should follow the same data and IPT separation guidelines. In this context, remote office WAN links refers to dedicated leased lines connecting the remote and primary networks where the infrastructure and computers at both ends of the link are managed by the same organization.

Mitigations

The wide area network link must be protected by a VPN. The VPN must support the separation of IPT and data networks by either supporting VLANs or creating individual VPNs for each network.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
PSTN Gateways			
PSTN gateways require client authentication before completing calls.	X	X	X
PSTN gateways are placed on a separate VLAN and signaling (e.g., SIP, H.323) traffic is only accepted into the VLAN from authorized servers.		X	X
Validate and terminate all PSTN signaling messages at the gateway.	X	X	X
Public IP Networks as Voice Carriers			
All VoIP traffic over public IP networks (i.e., the Internet) is encrypted.	X	X	X
Interoffice VPNs respect and maintain the separation of IPT and data traffic.	X	X	X
Session border controllers are installed to supplement conventional firewalls when VoIP is used to complete external calls.	X	X	X

Mitigation	Minimum	Medium	Highest
Wide Area Network Links			
Tunnel all WAN traffic over a VPN. The VPN respects and maintains separation of IPT and data traffic.	X	X	X

Server Guidelines

IPT server deployment should follow network infrastructure and perimeter preparation. IPT servers (Figure 5) are analogous to the central switches in a legacy PBX system and are just as essential. They are necessary for establishing calls and using calling features such as call forwarding, voice mail, and conference calling. IPT servers are also used to manage IP phones.

Several aspects of the servers require security consideration in order to protect the IPT system from attack and misuse. The software installed on the IPT servers, such as operating systems, databases, and IPT applications, must be hardened against attacks. Most servers feature remote management capabilities that make the server more vulnerable if not configured with appropriate security mechanisms. The servers must meet the stringent reliability and availability requirements of traditional telephony systems.

IPT servers also perform the critical function of authenticating and authorizing phones and users. In addition to discussing how to protect servers themselves, this section addresses what authentication and authorization features on the server should be used to control access to the IPT network.

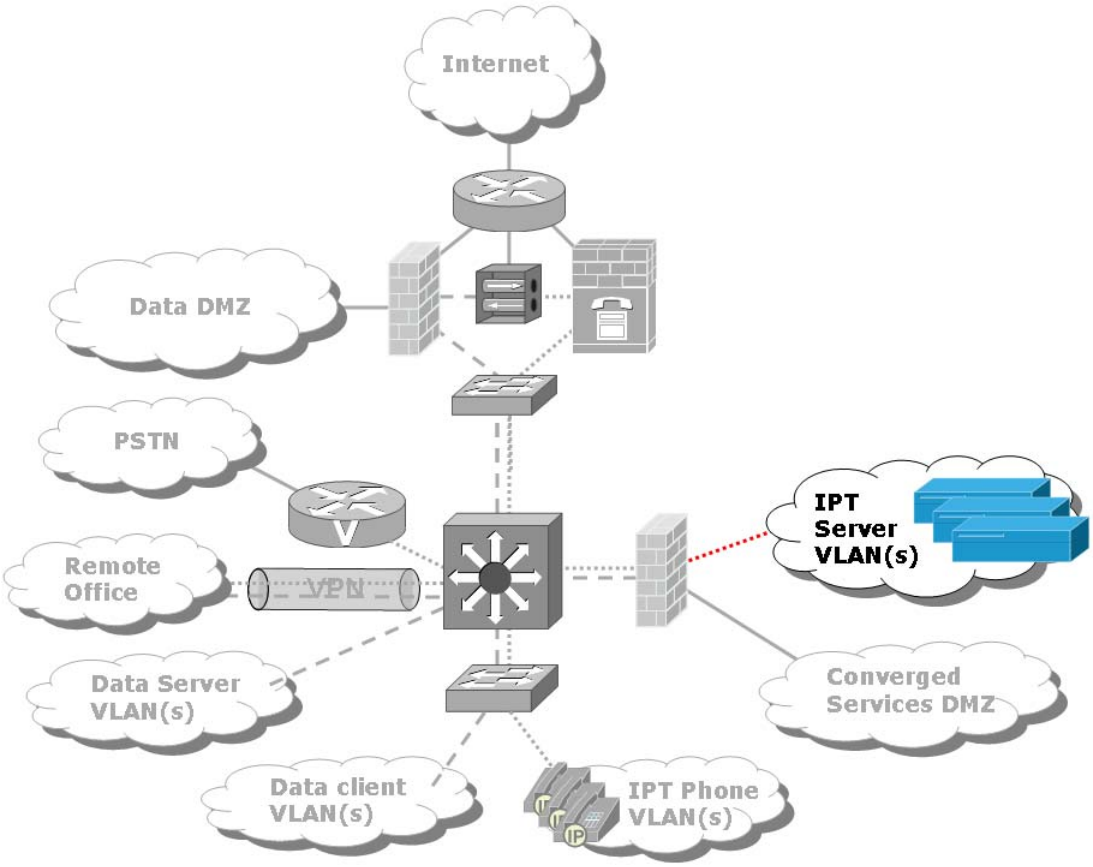

Figure 5 – IPT servers perform call routing and other essential IPT functions. They should be deployed and secured next. Important here are correct software configuration, applying security updates, redundancy, data backup, and power backup.

Software Security

IPT servers tend to use general-purpose server hardware running both general-purpose and IPT specific applications: many use operating systems such as Microsoft Windows, Sun Solaris, or Linux; data is stored in databases such as Oracle or Microsoft MSSQL; and vendors provide their own IPT software solutions. Despite the variety of software, they all have certain types of vulnerabilities and mitigations in common. All operating systems and applications deal with user accounts, insecure default configuration settings, auditing and logging, and software vulnerabilities. This section will address these problems as pertaining to all IPT server software.

However, software security is a large and complex topic and not every aspect of it can be covered here. As a result, security guides specific to the operating system and applications should be obtained and followed. [1], [2], and [3] provide many such documents. The recommendations provided in any security guidance document should be tested in a laboratory first, as some recommendations may adversely affect the functionality of the IPT server.

User Accounts

User accounts determine who may access the server and what they may do. It is vitally important that user accounts for all applications be tightly controlled. The more people who have access to a server, the higher possibility one of them may damage the server inadvertently or intentionally. If someone does not need access to the server or an application, then there should be no account for him or her.

Many operating systems and applications include a number of default user accounts with default passwords. These accounts provide easy entry for an attacker and are often overlooked during the installation process.

Mitigations

User accounts must only be given to those people who are responsible for managing the server or application. Those accounts should be given the minimum privileges needed for the person to complete his or her work (e.g., using role-based access control). If the IPT server is a member of a network-based directory, such as Microsoft Active Directory or Network Information Services (NIS), the operating system should be configured to limit the network identities that can login.

To prevent password guessing, complexity rules for user account passwords must be enforced, and the allowed number of failed login attempts must be limited.

At a minimum, all default passwords must be changed. Default user accounts should be renamed and their passwords must be changed before being exposed to the network.

Default Configuration Settings

The software on the IPT server is installed with default configuration settings. These settings may not provide adequate security. Instead, the server may be configured for maximum functionality. Unknown to the administrator, there could be features enabled that are not appropriate for the installation environment.

Mitigations

Configuration settings must be systemically checked to determine how the server is configured on delivery or after installation. Each setting should be evaluated for its affect on security. Documentation from the vendor should be used to help determine the security-related settings. Settings that enable extra features should be carefully considered and evaluated before enabling.

Auditing and Logging

Without auditing and logging, unauthorized access to or modification of the server will not be documented. Furthermore, an authorized change of the server's configuration might result in a server malfunction. Detecting and recovering from either event requires reconstructing the event from log messages. IPT systems also often require call logging for billing purposes. This is done using call detail records (CDRs). CDRs can also be used for detecting toll fraud and other unauthorized usage of the telephony system.

Mitigations

Auditing and logging (including CDRs) must be enabled on the server. These logs should be reviewed regularly for security and access violations. Should the need arise to investigate an intrusion or abuse, logs should be stored for a period of time in accordance with an organization's security policy. Logs should be saved on a hardened logging server and backed up regularly, because the integrity of the logs stored on the source server cannot be guaranteed if there is an intrusion. The log server should only accept log entries from authorized machines.

Software Vulnerabilities

Software vulnerabilities inevitably will arise in the server operating system and server applications. Software vulnerabilities can leave a server open to attacks such as denial of service and unauthorized remote access attacks.

Mitigations

Software security updates must be tested and then installed on production servers as soon as possible to limit the window during which the server is vulnerable. Software updates should be cryptographically signed by the software vendor to ensure authenticity. To reduce the chances of updates causing unforeseen problems on production servers, the updates must be tested on a test network that approximates the production network.

Malicious Software

Since many IPT servers run general-purpose operating systems, they are susceptible to the same computer viruses, trojan horses, worms, and other malicious software that affect these operating systems.

Mitigations

Anti-virus software must be installed on all IPT servers and virus definitions updated regularly from reliable sources. The IPT servers must not be used for general Internet activities, such as email and web browsing. Access to the Internet, if allowed, should only be used for administrative tasks.

Network Services

Network services running on production servers represent a threat, because unknown vulnerabilities could be exploited by an attacker. Unnecessary network services running on a server provide an additional avenue of attack and represent a drain on the resources needed to maintain these services. If administrators are unaware of the services running on their servers, attacks could go unnoticed, and security updates go unapplied.

Mitigations

All network services on the server that are not in use must be disabled. The IPT server vendor should be consulted to determine which services are required by the system. Carefully consider the security implications of maintaining a service against the features provided by the service.

Database Security

IPT systems may employ a separate database to store user and device information. Access to this database is typically managed via the remote management interface employed by the IPT server, such as a web interface or vendor software. However, the database server may be directly accessible by other means that need to be protected. Compromising the database server compromises the whole IPT network.

Mitigations

The database must be secured following all the guidelines for general software security outlined above.

The database server and IPT server should have a dedicated communication channel between them that is not accessible from the organization-wide network. This means either having both servers physically running on the same computer and using shared memory or the loopback network, or a dedicated network for traffic between the IPT and database servers. The later could be implemented using VLANs. The database server should still require authentication of all clients. If a dedicated network is not possible, connections to the database server should be restricted by IP address and protected using a secure channel. This could still leave the database server accessible to attackers when it need not be.

Cryptographic Key Material

Some servers store key material for encryption and authentication purposes. An attacker with access to these servers may be able to extract the key material from the server. If successful, they may be able to impersonate the server and more easily eavesdrop on calls, including some types of encrypted calls.

Mitigations

Different types of key material require different levels of protection. Private keys used to digitally sign configuration and firmware files, downloadable applications, and certificates must, at minimum, be encrypted with a complex password. Better yet, private keys should only be stored and used on a computer that is not connected to the network. Other key material should be encrypted with a password, unless use of the key material is required to boot the server. The safest solution is to use a cryptographic hardware token which stores keys and performs all cryptographic operations requiring access to the keys.

Mitigations Summary

Mitigation	**Minimum**	**Medium**	**Highest**
Secure servers following the appropriate NSA security guidance documents and industry best practices.	X	X	X
User Accounts			
Limit user accounts on servers to only the administrators of the server.	X	X	X
Assign to user accounts only the privileges necessary for the user to complete required tasks.		X	X
Remove or disable unused default accounts.	X	X	X
Require complex and hard to guess passwords for server user accounts, and audit passwords for compliance. Limit the number of failed login attempts.	X	X	X
Change all default passwords before connecting server to the network.	X	X	X
Default Configuration Settings			

Audit all default configuration settings before connecting the server to the network.	X	X	X
Auditing and Logging			
Enable system logging and logging of call detail records (CDRs).	X	X	X
Regularly review logs for discrepancies.		X	X
Send all logs to a hardened log server.		X	X
Log server should only accept log messages from authorized servers.		X	X
Software Vulnerabilities			
Promptly test and apply vendor security updates.	X	X	X
Require software updates be cryptographically signed by the software vendor.	X	X	X
Malicious Software			
Install anti-virus software on servers and update virus definitions regularly.	X	X	X
Do not use servers for general Internet access, such as email and web browsing.	X	X	X
Network Services			
Disable unnecessary network services on all servers.	X	X	X
Database Security			
Use a secure channel to connect the IPT and database servers, and limit access to database server to IP addresses of the IPT servers.	X		
Use a dedicated communication channel, such as a separate physical network, to connect IPT server and database servers.		X	X
Cryptographic Key Material			
Password protect cryptographic keys.	X	X	X
Store and use private keys for signing configuration files, firmware, downloadable applications, and certificates on a computer not connected to any network.		X	X
Use a hardware token to store keys and perform cryptographic operations using the keys.			X

Physical Security

The physical security of the IPT server should meet or exceed the minimum requirements set by security policy for the legacy PBX, because in most cases, if a server can be reached physically it can be compromised. An unauthorized person could easily disable the server by shutting it down or physically damaging it.

An unauthorized person could also use one of many common techniques to try to gain administrative access to the servers. BIOS passwords can be reset using jumpers on the motherboard, boot disks can be used to load alternate operating systems, passwords can be changed on servers, and many other things can be done to break into a server once physical access has been obtained.

Server hardware can be damaged in a number of other ways, including intentional and unintentional fires, flooding from broken water pipes, and natural disasters.

Mitigations

Physical security precautions must be taken to deny unauthorized access to the servers. This should include locking the IPT server room or cabinet, locking the server case, and placing alarms on all entry points to the server room. Cylinder locks provide basic access control to the server room, but better solutions include access cards or biometrics. These also enable logging of all people entering and exiting the room. Multiple types of locks can be combined for the strongest security. Surveillance cameras and human monitoring should be used in high value installations. Disable booting from removable media and enable BIOS passwords to prevent BIOS modification.

Fire suppression systems must be installed to protect the servers from fire damage. Use suppression systems safe for electronic equipment in high value installations.

To prevent accidental flooding, do not run water or sewage mains through the server room.

Ensure availability of services as discussed in later sections such that if a disaster destroys one data center the whole organization does not lose telephony services. For example, provide each location with its own IPT server and a backup connection to the PSTN.

Mitigations Summary

Mitigation	**Minimum**	**Medium**	**Highest**
Physical Security			
Servers are in a locked room or cabinet.	X	X	X
Control access to server room using cylinder locks and shared keys. (For highest robustness, use in combination with other access control mechanisms.)	X		
Control access to server room using access cards or biometrics. Maintain logs of people entering room.		X	
Control access to server room using both cylinder locks, and access cards or biometrics. Maintain logs of people entering room.			X
Install alarms on all entry points to the server room.			X
Disable booting from removable media.		X	X
Enable password protection of BIOS settings.		X	X
Monitor server rooms or cabinets with surveillance cameras.			X
Install fire suppression systems.	X	X	
Install fire suppression systems safe to electronic equipment.			X
Do not run water or sewage mains through server rooms.	X	X	X

Service Availability

Availability of telephony services is one of the most important considerations to be made, because telephony users are accustomed to 99.999% uptime. Telephony often is operational even when other communications services are down. To ensure IPT servers meet this level of availability, problems with power and hardware failures, data loss, and emergency services must be addressed.

Hardware and Power Failures

IPT server hardware failures must be expected and proactively protected against. Disk drives, power supplies, motherboards, memory, and other equipment will eventually fail. Power outages will occur.

Mitigations

At minimum, server hardware must have RAID (Redundant Arrays of Independent Disks) mirroring support to protect against disk drive failure. Better solutions would have servers with RAID 5 support, ECC memory, and redundant power supplies. To protect against total hardware failure, IPT servers must be configured with hot standbys that automatically take over the duties of the primary server should it fail. A spare duplicate server should be readily available to replace the failed server. All servers should have short-term power backup using uninterruptible power supplies. Where availability is very important, servers should have long-term backup power available.

Data Loss

High-availability hardware cannot protect against all hardware failures, software errors, or intrusions corrupting data on IPT servers. Such failures will require quick recovery of servers to a known good state in order to return to operational status. Recovery may need to take place at a remote location in very bad situations.

Mitigations

To ensure a quick system recovery, data from the VoIP systems must be backed up regularly so that restoration can occur quickly and efficiently. A backup and recovery policy must be in place, which describes the process necessary to achieve this. Backup and recovery processes must be tested.

At minimum, full backups should be done on a weekly basis. Additional daily incremental backups are best. Backups should be stored in a secure location that will ensure the backups are not corrupt or compromised, such as in an environmentally controlled and locked room. Backups that leave the physical control of the organization (i.e., for shipping) must be encrypted. Some backups should be archived in long-term storage to aid in future intrusion investigations.

Emergency Services

911 services have become a significant issue in the IPT industry. Traditional telephony systems can associate phone numbers with a dwelling or location, and thus, allow emergency services to pinpoint the location of the call.

IPT is not compatible with this aspect of 911 services. One of the advantages of IPT systems is number portability. This means that a person can pick up a phone, move to a different room, building, or even a different city, connect the phone to the network, and have exactly the same services and phone number. The IPT system has no way of knowing the exact location of a phone in such a flexible environment.

Mitigations

Each phone should be assigned to a fixed location until an acceptable 911 solution becomes available. The location should be saved on the phone or in the IPT server database. The phone should either send its location when it makes a call or the IPT server must be able to correlate the phone with its location in the database. Users may move their contact address to different phones as long as the server can identify the phone. Phones must not be moved without updating their location information. IPT systems must route 911 calls over a PSTN connection to ensure 911 operators receive correct location information.

Alternatively, a traditional PSTN phone can be installed in each office area specifically for use in emergencies.

The guidelines discussed here must be reviewed and revised in the light of the rapidly evolving E911 service for VoIP.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Hardware and Power Failures			
Servers use RAID disk mirroring.	X		
Servers use RAID 5 disk mirroring and striping.		X	X
Servers have redundant power supplies.		X	X
Servers have ECC memory.		X	X
Servers are configured with hot standbys.	X	X	X
A spare server is always available to replace a failed server.		X	X
Servers have short-term power backup.	X	X	
Servers have long-term power backup.			X
Data Loss			
Backup and recovery policy is in place.	X	X	X
Backup and recovery processes are tested.	X	X	X
Full backups are performed weekly.	X	X	X
Incremental backups are performed daily.		X	X
Backups stored in an environmentally controlled and locked room.		X	X
Backups stored at multiple geographically separated locations.		X	X
Archive backups periodically.		X	X
Backups are encrypted when not under physical control of the organization.	X	X	X
Emergency Services			
IPT servers maintain phone location information. Location needs to be updated manually, thus phone location must be static.		X	X
Provide each office area with an emergency phone connected to the PSTN.	X		

Access Control for IPT Clients

Automatic Registration of End Points

On many systems, phones first register with their IPT servers in order to receive service. This concept is similar to 802.1x data link layer authentication, in which PCs must authenticate to network switches before they will be allowed to transmit packets. Some systems allow IP phones to register automatically with the system. The problem with automatic registration is that the server cannot verify whether the end device that registered is an actual phone or an attacker masquerading as a phone. This could open the server up to attack. Combined with DHCP, an attacker could add an unauthorized device to the network and begin attacking the IPT server without an administrator's knowledge.

Mitigations

IPT systems should be configured to use two-way authentication. This means that the server should authenticate the identities of IPT clients, and the clients should similarly authenticate the identity of the server to which they register. However, some IPT systems attempt this by simply checking the IP address, which can be spoofed in many cases. Therefore, using strong cryptographic authentication, such as Transport Level Security (TLS), to verify the identities of both the phones and servers on the system is more secure and robust.

Limit the use of automatic registration and DHCP to periods of significant IP phone deployment and disable them once registration is complete. Automatic registration should never be left enabled. DHCP can be more safely enabled when protected by anti-spoofing features that keep associations of IP address, MAC address, and switch port in access and infrastructure devices (see *Call Eavesdropping* on page 10).

A valuable extension to this authentication security would be to have the phones and the phone users require separate authentications. This concept is similar to 802.1x authentication; the IP phone would authenticate to the IPT server as a PC would authenticate to a network switch. Then, to use that IP phone, a valid user must be able to authenticate to the device, just as a user would have to authenticate oneself to a PC before using the PC on the network.

Authentication and Authorization

The most important service IPT servers provide is the routing of calls between clients. In many systems the IPT server learns the network location of a user when the user's client registers with the server. The IPT server routes calls based on the information provided by the client. If the IPT server does not authenticate the source of the registration information, attackers can easily impersonate users and eavesdrop on calls using registration hijacking, in which the attacker sends a fake registration message to the server registering the victim at the attacker's network location. When someone attempts to call the victim the IPT server will route the call to the attacker.

Mitigations

The server must require IPT clients authenticate themselves. The server must also authenticate itself to the clients, otherwise an attacker could impersonate the server. This means the attacker could trick the client into revealing sensitive information, such as passwords, or route calls so it is possible to eavesdrop on them.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Access Control For IPT Clients			
Disable automatic registration capabilities after initial deployment of IP phones.	X	X	X
Disable DHCP after initial deployment of phones.			X
Enable DHCP, but only with anti-spoof protections.	X	X	
Enable two-way authentication between telephony end devices and servers.		X	X
Require users to authenticate themselves to the phone before making calls.			X

Remote Management

IPT servers offer a variety of methods of remote management, such as web-based interfaces, proprietary vendor software, and SNMP. The vendor may also remotely manage the IPT server as part of a service agreement. Remote management poses a security threat because unauthorized use can seriously damage IPT capabilities or security features. The timesaving benefits of remote management can be safely used if appropriate security precautions are taken.

Web-based Management Interfaces

Many systems offer web-based remote management interfaces because of its familiarity and ability to be used from any platform with a web browser. However, web servers and web applications commonly contain a variety of vulnerabilities such as buffer overflows, cross-site scripting, authentication bypass, and SQL injection.

Moreover, many web sessions are not encrypted, and thus, pass the IPT server administrator password in plaintext over the network allowing an attacker to obtain the password by capturing network traffic. Many browsers also cache user passwords for web pages. Unauthorized access to administrator workstations could potentially compromise the login for the IPT servers.

Mitigations

To mitigate web-based remote management problems, several actions can be taken. First, for any administrative interfaces, TLS should be enabled on the web server and non-TLS access disabled. This will encrypt the management sessions, including logins and passwords.

Second, the locations from which administrators can connect to web management interfaces should be limited. The web-based interfaces should be only accessible via an administrative network separate from the general-purpose network. Additionally, access to the web-based interface should be limited to IP addresses of administrative workstations. High value servers should be managed locally on the server itself and external access to the web interface disabled.

Third, on any computer from which web management can occur, the browsers must be configured not to cache usernames and passwords unless the passwords are protected with strong cryptography.

Finally, security updates must be applied to the web server in accordance with the guidelines in *Software Security* on page 20.

Proprietary Management Software

Web management is not the only method used to remotely manage IPT servers. Some vendors have written proprietary clients and servers to manage their IPT servers. The drawback to this is another potentially vulnerable network service running on the server. Furthermore, if the vendor software does not support encryption of network traffic it may be difficult for the end-user to add such support. In this case, TLS web-based management would be better.

Mitigations

To protect the use of proprietary management software, the precautions to take are similar to web-based interfaces. Network traffic should be encrypted. If the software does not support encryption then traffic should be routed through a secure tunnel using IPSEC, TLS, or SSH. Access to the management server should be limited to a separate administrative network and to specific IP addresses. Usernames and passwords must not be cached by the client software unless they are properly

encrypted. Finally, the security updates must be applied to the server in accordance with the guidelines in *Software Security* on page 20

Remote Management by the Vendor

Some IPT vendors remotely manage IPT systems as part of a service agreement with the customer. Vendors may require remote management of the IPT server in order to upgrade software, troubleshoot problems, or recover forgotten passwords. These setups require publicly available connections and special vendor accounts, both of which are vulnerabilities because they increase external access to the server. These services require that an organization have complete trust in the vendor's employees and networks. Vendor employees could be malicious and use their trusted status to compromise the IPT server, or attackers could penetrate the vendor's network and use it to compromise the IPT server.

Allowing vendor access to the IPT system opens several security vulnerabilities. First, the security of the IPT system is limited by the security of both the organization's network and the vendor's network. An attacker may be able to gain entry to the vendor network and extend his access from there. Second, this implies trust in the administrators at the vendor location. Third, this requires that a connection be created to allow the vendor remote access into the IPT servers, which creates a potential security hole in the perimeter network.

Mitigations

To prevent these problems, servers should be examined for vendor accounts and those accounts removed. Vendors should not have access to the systems. If an organization must allow a vendor to remotely access its IPT system then several precautions must be taken. First, a dedicated connection, such as a PSTN or ISDN phone line, must be used for all remote vendor management. The vendor must not connect over a public IP network such as the Internet, because this requires creating a hole in the perimeter firewall directly to the IPT servers. Second, when the connection is not in use, it must be disabled by physically disconnecting the line. Third, the vendor must contact the IPT administrator before performing any remote maintenance and the administrator must initiate the connection to the vendor. The remote connections should be done over a secure and authenticated channel such as a VPN, TLS, or SSH. Finally, all actions performed by the vendor must be monitored and logged.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Web-based Management Interfaces			
Limit access to web interfaces to the IP addresses of administrator workstations.	X		
Isolate web interfaces on a separate administrative network.		X	
Only allow access to the web interface from the server itself and disable remote access.			X
Enable TLS on the web server and disable non-TLS connections.	X	X	
Disable web browser password caching features unless the passwords are strongly encrypted.	X	X	X
Regularly apply security updates to the web server and web applications.	X	X	X

Mitigation	Minimum	Medium	Highest
Proprietary Management Software			
Limit access to the management server to the IP addresses of administrator workstations.	X	X	
Isolate management server on a separate administrative network.		X	
Only allow access to the management software from the server itself and disable external access.			X
Enable encryption features of the management software. If such features are not available, route all network connections through a secure tunnel, such as IPSEC, TLS, or SSH.	X	X	
Disable password caching features of vendor's client unless the passwords are strongly encrypted.	X	X	X
Regularly apply updates to the vendor's management software.	X	X	X
Remote Management by the Vendor			
Do not allow remote management of IPT servers by the vendor.			X
Use a dedicated connection, such as a PSTN or ISDN line, for vendor access to servers.	X	X	
Encrypt traffic over the dedicated connection.		X	
Physically disable the vendor's connection when not in use.	X	X	
Require that the administrator initiate the connection to the vendor.		X	
Require vendor to connect over a secure and authenticated channel (e.g. VPN, TLS, SSH).		X	
Monitor and log all actions performed by the vendor on the server.	X	X	

IP Phone Guidelines

With the data and telephony network infrastructures in place, IP telephones (Figure 6) can be added to the network and secured. When adding IP telephones to the network, several considerations must be made to properly secure both the phones and the network against attackers. Both the hardware and the software must be locked down and managed properly. Remote management of the phones must be done in a secure manner. The various methods that can be used to connect the phones to the network must be evaluated to determine which method would be the best to use. Convergence features, which allow IP telephones to interact with other devices, must be evaluated for security problems. Finally, the use of software telephones, also known as softphones, must be examined.

Software and Hardware Security

Traditional phones contain limited functionality in the actual phone hardware because telephony features are implemented in the central switch. However, IP phones are more autonomous because many do not require a central switch in order to take advantage of much of their functionality. This requires a more capable and complex phone. The additional functionality and complexity in IP phone software increases

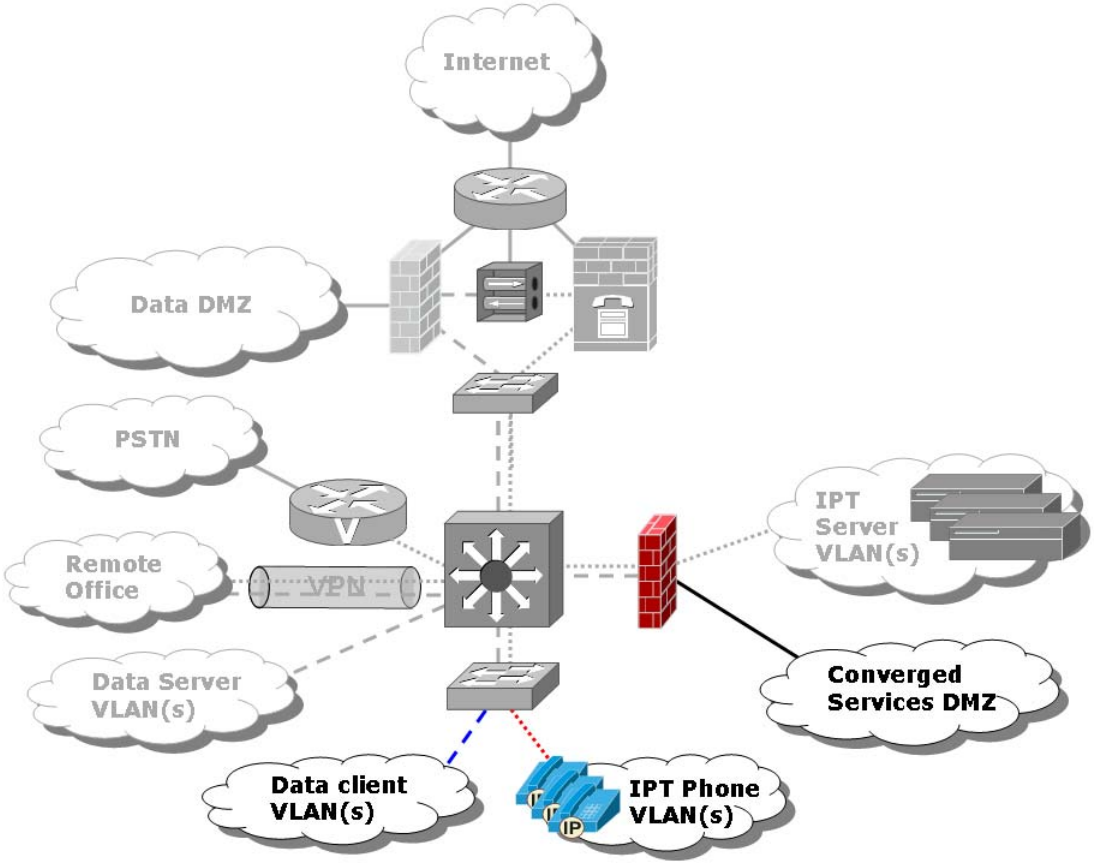

Figure 6 – Lastly, IPT client devices are added to the network. Converged services provide safe interfaces for the phones to access the data network and vice versa. Some important issues here are remote configuration of phones, applying security updates, protection of signaling and media streams, service availability, and adding softphones.

the chance of vulnerabilities. These vulnerabilities must be mitigated in a manner similar to any other computer on the network. Like desktop systems, some IP phones allow users to install third-party software. These applications could also add vulnerabilities if not properly controlled.

Software Vulnerabilities

IP phones run embedded operating systems that are often commercially available, though some phone operating systems are proprietary. Various applications run on top of the operating systems and provide VoIP and other necessary functionality. Examples include web and SNMP servers for phone management, address books, and web browsers. These applications could contain vulnerabilities that could allow denial of service attacks against the phone, disable remote management functionality, or allow an attacker to gain complete control of the phone.

Mitigations

Methods to mitigate the software vulnerabilities in phones are similar to methods used to protect other computer systems on the network. Unnecessary applications and services on the phones must be disabled, particularly if they provide remote access. See *Remote Management of VoIP Phones* on page 34. Any known vulnerabilities must be patched as soon as possible. This can be automated by having phones regularly and automatically download signed firmware files from a trusted central server. Finally, network access to the phones can be limited by placing phones on separate VLANs. This makes it more difficult, though not impossible, for an attacker who has access to a non-VoIP computer to attack vulnerabilities on a VoIP phone.

Third-party Software

Some phones have the capability to run third-party software downloaded from the network. For example, one Java-based phone allows the phone user to download Java applets from the vendor's Internet site. There are risks to allowing such behavior:

- The effects of third-party software on the phone are unknown.
- Downloaded software that appears legitimate may contain malicious functionality.
- The software may contain unknown vulnerabilities, which could be exploited to compromise the phone.

Mitigations

The policy for downloading external software onto phones should be at least as strict as that for downloading software to desktop computers. In many cases, the need for higher reliability for the telephony system will necessitate stricter policies. The way to mitigate the problem of external software is to disable the capability and only distribute necessary software with firmware upgrades. If there is a need to allow users to load applications on the phone then a server should be setup inside the organization to provide these applications and the applications should be cryptographically signed by the organization. Access to any vendor web sites offering application downloads for the phones should be blocked. Direct Internet access by the phones should be blocked in general, if possible. If that's not possible, use a DMZ proxy server for Internet web access.

Malicious Software

Viruses and worms could exploit software vulnerabilities in the phone. Though no IP phone-specific viruses or worms are yet known, there have been reports of viruses

for mobile phones. At some point, viruses and worms targeting IP phones will become a reality. The manifestations of virus or worm infection of an organization's telephone network are similar to those for the data network. Malicious software can install back doors into phones, gather sensitive information, or use phones to attack other systems. Many recent worms have caused debilitating network congestion. The spread of worms on IPT networks could disrupt or disable voice capability.

Mitigations

Antivirus solutions exist for some embedded platforms, but no known antivirus solutions target IP phones. Antivirus software by itself would not completely mitigate this problem. Virus scanners can only reliably detect viruses that the scanners know about. Therefore, the best defense against viruses or worms is to implement the mitigations in the previous sections entitled *Software Vulnerabilities* and *Third-party Software* (page 32), as well as monitor logs for suspicious activity.

Embedded Microphones

All phones contain at least a single microphone in the handset, and speakerphones contain additional microphones. Since phones are software-controlled devices, the microphones are also controlled by software. As such, a software vulnerability could enable an attacker to control the phone and thus the microphones.

Mitigations

If a phone is placed in a sensitive area, its speakerphone microphone should be removed. The original handsets should be replaced with push-to-talk handsets or headsets. This prevents the microphone from being activated except when a person is using the phone. Another possible mitigation is to use phones that physically disconnect the microphone when the handset is on hook.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Software Vulnerabilities			
Disable unnecessary features and applications.	X	X	X
Limit access to phones using VLANs, access control lists, and firewalls. See *Accessibility and Network Separation* on page 8.	X	X	X
Regularly test and apply security updates to phone firmware.	X	X	X
Separate IPT and data traffic using VLANs.	X	X	X
Third-party Software			
Allow only features that have been tested in laboratory environments.	X		
Limit applications on phones to those that have been tested in a laboratory environment, cryptographically signed by the organization, and made available through an internal server.		X	
Do not allow users to install software on their phones.			X
Block direct Internet access from phones.	X	X	X
Malicious Software			
Implement mitigations in the *Software Vulnerabilities* and *Third-party Software* sections (page 32) to prevent untrusted applications from being installed on phones.	X	X	X

Mitigation	Minimum	Medium	Highest
Embedded Microphones			
Physically disable speakerphone microphones.		X	X
Use dedicated phones, which physically disconnect the microphone when the handset is in the cradle.		X	
Use push-to-talk handsets or headsets.			X

Remote Management of VoIP Phones

The majority of IP phones can be classified as network-controlled devices. The sheer number of phones that an organization must deploy means that phones are more easily configured and managed using remote tools over the network. This capability means that each phone now represents another network end-point, and each must be secured. An exploit of this remote management functionality can have potentially serious consequences including denial of telephony services to an organization and leakage of information to unauthorized parties inside and outside the organization. The most common methods for remotely managing VoIP phones are: DHCP, firmware and configuration file downloads from a server, web-based management consoles, SNMP, and telnet. All of these methods have flaws that must be addressed during the design of an IP telephony network.

Dynamic Host Configuration Protocol (DHCP)

The DHCP is most often used to assign network settings such as IP addresses, name servers, and gateway routers on the startup of network end-points. DHCP is commonly used with desktop computers. Since phones are now just another network end-point, DHCP is a natural choice for assigning settings to phones. However, organizations may have higher standards for security and reliability for telephony, and as such, the use of DHCP with phones needs to be carefully considered.

DHCP has an inherent vulnerability in that it is not an authenticated protocol and thus it is open to spoofing. An attacker can provide incorrect network settings to a phone, which could result in a denial of service, redirection of calls to malicious servers, or man-in-the-middle attacks. Such attacks are possible if an attacker has access to the organization's network. Malicious DHCP clients can also cause a denial of service by continuously requesting IP addresses until none are left for legitimate devices. Without an IP address, phone service is unavailable.

Mitigations

Several mitigations are available to limit the threat posed by DHCP. The safest solution is to assign static IP addresses to IP telephony devices. At a minimum, static IP addresses must be given to IP telephony servers and phones that serve critical functions. Using DHCP for the initial deployment of IPT devices is acceptable if static IP addresses are assigned to critical devices after deployment. Second, access control lists on routers and firewalls should be configured to limit access to the DHCP client ports. Third, network devices can be required to use link layer authentication (such as 802.1x) before connecting to the network. This will prevent unauthorized users from stealing IP addresses. Finally, some network switches have the ability to associate Ethernet address, IP address, and switch port. When a packet is received on a port with an address that does not match, it is dropped. This makes spoofing DHCP-assigned addresses more difficult.

Downloading of Firmware and Configuration Files

Many IP phones are much like network-booted desktop computers. They connect to the network, obtain IP addresses using DHCP, and download operating system images and configuration files from a central server. This keeps the management of software and configuration versions centralized. It also allows for easy updates of the phone's firmware. However, for an attacker, it opens a pathway to complete control of an organization's phones. By modifying the firmware or configuration file, an attacker can insert malicious code into the phone's operating system, use the phone as a rogue agent, redirect calls to malicious servers, or disable the phone.

A phone's firmware or configuration file could be modified in one of two ways. First, an attacker could perform a man-in-the-middle attack to intercept and replace the files as they are downloaded from the server. This requires local network access or the ability to spoof DHCP messages. Second, an attacker could compromise the server storing the firmware and configuration files. This is a more serious problem because control of a download server enables an attacker to easily attack all phones in an organization.

Mitigations

The most effective way to mitigate these problems is to cryptographically sign all firmware and configuration files that must be downloaded over the network. Each phone must have the signature verification key loaded on the phone in a secure manner such as on an isolated network or over a direct serial connection. The phone must verify the signature on every file it downloads from the network and reject any files with invalid signatures. The signing key must be saved in a secure place and not be stored on the download server. The second mitigation is to harden the security of the download server and limit access to only necessary personnel. To ensure reliability, the download servers should be redundant and physically dispersed throughout the organization. Since updating IP phone software is critical, there should be redundancy in the download servers.

Web-based Management Interface

Many IP phones have embedded web servers, which publish web pages capable of modifying important settings on the phone. Many times the same settings downloaded in configuration files are modifiable in this manner.

Web servers on phones raise several concerns. First, access to the web interface must be limited to authorized people. This usually means username and password protection, which must be individually configured for each phone. Many phones are not capable of providing strong cryptographic methods to protect these passwords and this just gives users one more password they must remember. In addition, each phone is now also another web server that could contain vulnerabilities.

Mitigations

The web interface should be deactivated if users can access necessary phone features through the phone's display and administrators can configure phone settings using downloaded configuration files. If some essential features are only accessible through the web interface then access to the web interface should be limited to physical ports on the phone. That is, access to the web interface should only be available through a direct connection to the user's computer; for example, using a USB cable or the phone's dedicated Ethernet computer port. Alternatively, if the IP telephony system has the option for users to configure their phones on a central server and then have the phone automatically download a signed configuration file, this method should be used and web interfaces on phones should be deactivated. If none of these options are possible, then username and password authentication

must be used. At a minimum, the HTTP-Digest algorithm and complex passwords should be used for authentication. This is available on most phones with web consoles. If stronger cryptographic mechanisms such as TLS are available, they should be enabled.

Simple Network Management Protocol (SNMP)

The SNMP is used to read and write settings on many network devices, allowing them to be integrated into comprehensive network management tools. Some phones may also offer SNMP access to their settings. Compromising SNMP access to phones has consequences similar to compromise of configuration files or web interfaces.

Mitigations

If SNMP is used to manage phones, then SNMP version 3, with its authentication features, must be used. SNMP version 1 protects access to SNMP services using a community string, which is transmitted in cleartext over the network and must be shared with all persons who must access the phone. In addition, SNMPv1 did not use the passwords to protect the integrity of the messages. SNMPv3 allows per-user passwords and uses cryptographic functions to protect the password and message integrity. If SNMPv3 is not available, then the best option is to use signed configuration files that can be downloaded from the server rather than using SNMP to manage the phones.

Telnet

Another remote management solution common on phones is telnet. Telnet is a command line interface to the phone configuration. Telnet is an unsecured protocol, meaning that sensitive information, such as passwords, is transmitted in the clear over the network.

Mitigations

If telnet is not an absolute necessity, then it must be disabled on all phones. If other methods of remote management are available on the phones, they must be used instead. In general, if other more secure protocols meet the needs of the organization, then less secure protocols, such as telnet, must be disabled.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
DHCP			
DHCP enabled for most phones.	X		
DHCP enabled with link layer authentication for all phones.		X	
Static IP addresses assigned to all phones.			X
Access control lists on routers and firewalls configured to limit access to the DHCP client ports.		X	X
Static IP addresses assigned to critical servers and phones.	X	X	X
Network devices required to use link layer authentication (such as 802.1x) before connecting to the network			X
Implement DHCP anti-spoofing measures on network switches.		X	X

Mitigation	Minimum	Medium	Highest
Downloading Firmware and Configuration Files			
Cryptographically signed firmware and configuration files obtained from hardened servers.	X	X	X
Use redundant and physically dispersed servers for distributing firmware and configuration files.		X	X
Web-based Management Interface			
Use router or switch access control lists to limit access to the phone's web interface to authorized IP addresses only.	X		
Enable HTTP-Digest password authentication.	X		
Disable remote access to the phone's web interface and perform all phone configuration on a central server and have the phone automatically download new signed configurations. **OR** Enable TLS and use strong passwords on phone's web interface.		X	
Disable remote access to the phone's web interface and perform all phone configuration on a central server and have the phone automatically download new signed configurations. **OR** Allow access to the web interface to only those devices directly connected to the phone using the phone's PC port or USB.			X
Simple Network Management Protocol			
SNMP version 3 used to manage phone settings.	X	X	
Disable SNMP, or set to read-only if SNMP access is necessary.			X
Use router or switch access control lists to limit access to the phone's SNMP port to authorized IP addresses only.	X	X	X
Telnet			
Disable telnet on all phones	X	X	X

Network Connectivity

IP phones include a variety of network connectivity solutions such as Ethernet, IrDA, Bluetooth, and WiFi (802.11a/b/g) access. Some phones offer all of these connectivity solutions and thus act as a universal wireless access point. While some sort of network connectivity is required, too many connectivity options will make a phone more difficult to secure. Each connectivity solution adds configuration complexity and offers another potential path for an attacker to exploit.

Ethernet

Ethernet is a common means of connecting an IP phone to the IP network. To make deploying IP phones easier and to avoid adding additional Ethernet cabling for phones, many phones feature an integrated Ethernet switch. A PC can be plugged into the phone, and the phone can be connected to the network. This will enable both the PC and the IP phone to use the same network port. Thus, both the phone

and computer will be privy to network traffic meant for either device. An attacker who compromises the computer may have direct access to the phone and vice versa. An attacker can use this access to eavesdrop on calls and launch denial of service attacks against the phone.

Most deployments of IP telephony require telephony and data networks be kept separate using VLANs. If the phone does not support VLANs on the integrated Ethernet switch, then a computer connected to the phone's computer port has access to the IP telephony VLAN.

Mitigations

The most effective way to mitigate these problems is to not use the computer port on the phone and to disable it in the phone's configuration. This prevents a PC from connecting to the phone and prevents a PC from violating VLAN separation. If separation of telephony and data networks is needed and the computer port is used, then the phone's integrated Ethernet switch must support VLANs.

Infrared

Infrared data ports utilizing the IrDA protocol are used to transmit data between devices using invisible pulses of light. In addition to some IP phones, these ports are commonly found on PCs, handheld computers, laptop computers, and printers. Example uses of infrared ports include synchronization of data between handhelds and PCs, and printing from a handheld directly to a printer. Devices that communicate using infrared must be within sight of each other. While some phones presently have infrared ports, no phone is known to make use of this port. However, its existence suggests that features using the infrared port will be available in the future. For example, a person could synchronize his mobile phone address book with the address book on the IP phone.

Infrared ports on phones raise several security concerns. First, there is no built-in security mechanism other than range of transmission and the line-of-sight requirement. Each application must implement its own confidentiality and integrity mechanisms. Second, an attacker does not need to physically interact with the phone to access it. An attacker with line-of-sight could potentially attack the phone. Third, a compromised phone could use the infrared port to capture other infrared communications in the same room as the phone.

Mitigations

The most effective method of mitigating these vulnerabilities is to cover the infrared port with metallic tape. This prevents any use of the port, including by an attacker who has compromised a phone. Otherwise, the infrared port should be disabled if it is not required. If use of the infrared port is necessary, then each allowed application must be individually evaluated and configured for security.

Wireless Personal Area Networks

Bluetooth is a short-range wireless personal area network (PAN) technology that has applications similar to infrared ports. The primary differences between Bluetooth and infrared are that Bluetooth does not require line-of-sight for successful data transmission, and Bluetooth features some security mechanisms that provide confidentiality and integrity. Very few IP phones presently support Bluetooth; however, it or similar PAN technology is likely to start appearing in VoIP phones. The designers of IP telephony systems need to be aware of the security issues associated with PAN technologies.

Mitigations

The best solution is to use devices that do not support Bluetooth. Phones with Bluetooth functionality should have it disabled. If Bluetooth-enabled phones are used, then proper security measures must be taken. Addressing all the security issues related to Bluetooth is outside the scope of this document. An NSA information assurance advisory [6] discusses the details of Bluetooth security.

Wireless Local Area Networks

WLANs are increasingly common in organizations. This category of connectivity includes technologies referred to as WiFi or 802.11a/b/g. VoIP phones can use WLANs to either act as an access point to other devices, or as the primary source of connectivity instead of a wired link.

There are security concerns specific to VoIP phones containing WLAN access points. First, phones are more densely deployed throughout an organization than stand alone wireless access points would be. A large number of WLAN-enabled phones make wireless access more available to an attacker. Second, some networks may separate telephony and data network traffic using VLANs. A WLAN access point integrated into the phone is part of the telephony network and could violate this separation. Third, there may be confusion over the responsibility for managing the phone's security since WLANs and IP telephony are likely administered by different groups of people with different sets of skills.

Cordless IP phones can use WLANs to connect to the network. These phones must mitigate both WLAN and IPT vulnerabilities. They must address problems such as confidentiality, integrity, and reliability of the wireless link in addition to the IPT vulnerabilities discussed elsewhere in this guide. This makes deploying WLAN IP phones more complex.

Mitigations

WLAN access points and IP phones should not be combined into a single device. Phones with built-in WLAN access points should be avoided. If wireless access is needed then separate and dedicated WLAN hardware should be installed.

WLAN IP phones must meet the same security policy as other WLAN devices deployed by an organization. In addition, the WLAN phone and WLAN network must meet the requirements placed on all wired IPT infrastructure such as separation of data and IPT traffic.

There are many more security issues that must be addressed when deploying wireless LANs, and addressing all of them is outside the scope of this document. For more complete information on securing wireless LANs, reference the *DISA Wireless STIG* [7], *DoD Directive 8100.2* [8] and the *NSA Recommended 802.11 WLAN Architecture* [9].

Mitigations Summary

Of the various network connectivity solutions for VoIP phones, only Ethernet is really required. If telephony and data networks are separated onto different VLANs, the computer port on phones should not be used unless the phone supports VLANs.

The wireless network technologies discussed in this section all open significant vulnerabilities in the IP telephony network. If the organization needs wireless access, it should be implemented using a separate and dedicated wireless infrastructure, not as part of an IPT solution. If wireless access to the phone is mission critical, the infrared data port should be used due to its limited range, but with caution.

Mitigation	Minimum	Medium	Highest
Ethernet			
Enable VLAN separation on phone computer port.	X	X	
Disable computer port.			X
Infrared			
Enable security mechanisms in all IrDA applications.	X		
Disable IrDA port in phone's configuration.		X	X
Cover IrDA port on phones using metallic tape.			X
Wireless Personal Area Networks			
Disable wireless PAN connectivity to IP phones.		X	X
Wireless Local Area Networks			
Disable WLAN access points built into phones.		X	X
WLAN phones meet all security requirements specified in WLAN security policy.	X	X	X
WLAN phones and WLAN infrastructure meet all the same security requirements specified for IPT clients and infrastructure.	X	X	X

Eavesdropping and Impersonation

By eavesdropping on VoIP calls, attackers can obtain sensitive information such as passwords, usernames, caller location, proprietary information, and addresses of other IPT devices. They could also use traffic analysis to determine relationship patterns between members of the organization.

Eavesdropping on network traffic requires the attacker be connected to the same LAN segment as the target or have control of a network device along the traffic path, such as a router. Within an organization, access to routers and all devices except access switches may be limited enough that eavesdropping is difficult. On access switches, eavesdropping will be possible without specific mitigations. If VoIP traffic traverses public networks unencrypted, eavesdropping is a serious concern. An organization does not have firm control over where the traffic goes once it leaves the organization.

Impersonation of callers and servers is also a problem, and one that can be a more serious threat for some organizations. Impersonating a caller means an attacker can access services on IPT servers reserved for the legitimate user, spoof caller ID information, bypass filters based on caller name, and eavesdrop on calls. While people are use to using the caller's voice as a form of authentication, this only works after answering the phone and with IPT applications that are voice-based. If phones can be contacted from the Internet, this could lead to problems with SPAM over Internet Telephony (SPIT), because SPAMmers can cheaply automate sending messages or calling phones. In addition, by impersonating a user to the IPT server, an attacker can eavesdrop on calls from anywhere on the network using the registration hijacking attack. This attack allows an attacker to send spoofed messages to the IPT server and reroute a user's calls.

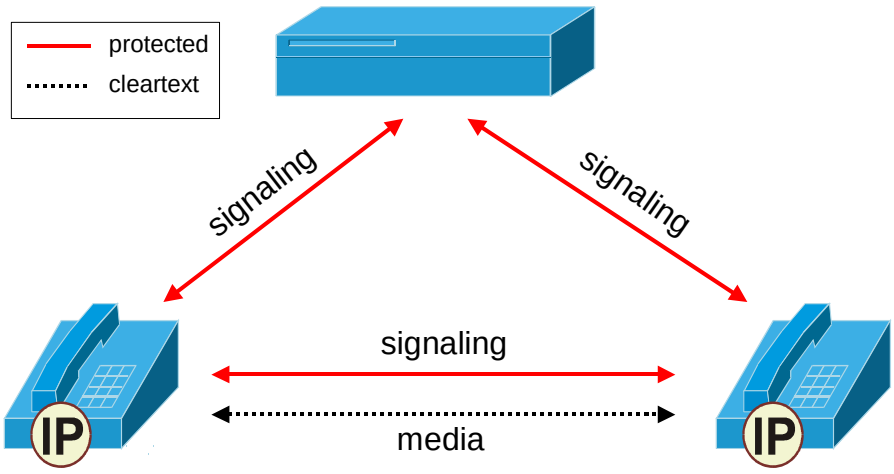

Figure 7 - Signaling messages are provided with confidentiality and integrity protection. Media streams are sent in the clear. Signaling protection prevents message spoofing and compromise of sensitive information in signaling messages. The unprotected media streams are susceptible to eavesdropping and spoofing.

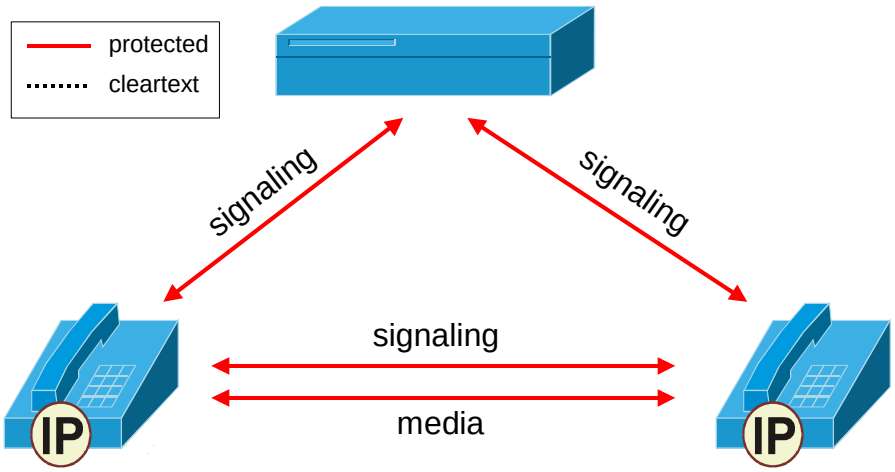

Figure 8 - Signaling messages and media streams are provided with confidentiality and integrity protection. This prevents eavesdropping on calls, spoofing of signaling messages, and hides any sensitive information contained in signaling messages.

Mitigations

Preventing eavesdropping and impersonation requires good network security, and enabling strong encryption and authentication on the phones and servers. Sections *Call Eavesdropping* (page 10) and *Public IP Networks as Voice Carriers* (page 16) discuss securing the network to prevent eavesdropping, while this section discusses VoIP specific methods. Authentication of phones to the IPT servers and other phones will make impersonation much more difficult. Encryption will prevent eavesdropping on call contents. Encryption refers to applying both confidentiality and integrity protections.

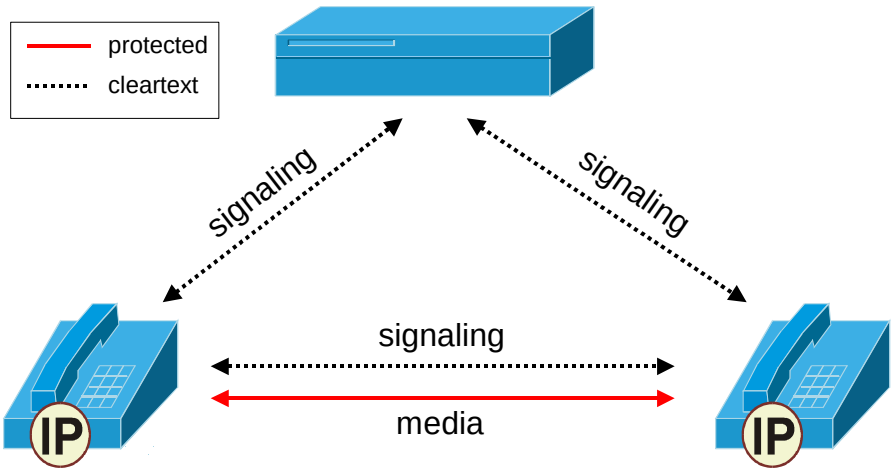

Figure 9 - Signaling messages are unprotected, but media streams are provided with confidentiality and integrity protections. While this prevents eavesdropping on conversations, it leaves the IPT system vulnerable to message spoofing and registration hijacking. It also requires a secure key exchange protocol, which does not depend on protection of the signaling messages. Such a solution is not widely available.

There are many choices on how to apply encryption and authentication to VoIP signaling and media traffic, and many different implementation technologies. Figures 7, 8, and 9 illustrate three of the choices. What an organization chooses to authenticate and encrypt depends on the importance of information as determined by the organization's security policy. At the very least, all phones must authenticate themselves to the IPT servers. There should be strong mutual authentication between phones and servers, and between phones. Media streams should be encrypted if call contents are sensitive and the network is accessible to attackers. Signaling protocols should be encrypted if signaling messages contain encryption keys, traffic analysis is a threat, or the identity of call participants is sensitive. However, using strong mutual authentication may require encryption of signaling protocols.

Technologies used to implement authentication and encryption vary with VoIP protocol, but there are several commonalities to briefly discuss. Most VoIP protocols support basic challenge-response password authentication from the phone to the IPT server. However, these are susceptible to offline dictionary attacks, and thus, require long and complex passwords. Authentication techniques using cleartext password are unacceptable. Many VoIP protocols also support using TLS to authenticate and encrypt signaling messages. Media encryption is often accomplished using the Secure Real Time Protocol (SRTP). Finally, some IPT systems may favor IPSEC or other secure VPN solutions.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Eavesdropping and Impersonation			
Phones authenticate to server using a challenge-response protocol (e.g., HTTP-Digest) with long and complex passwords.	X		
Mutual authentication between phones and IPT servers using strong cryptography (e.g., public keys).		X	X
Mutual authentication between phones.		X	X
Encryption of media streams.			X
Encryption of signaling protocols.		X	X

Convergence Features

A convergence feature allows the communication and synchronization of data between many different types of devices. Future IP phones may include features that allow them to interact with applications on other devices. For instance, an address book application on the PC instructs the phone to dial a number when the user clicks on an entry in the address book, or a PDA synchronizes its address book with the address book on the phone. Each of these features requires another service be available on the phone that could contain vulnerabilities. Each application requires an authentication and authorization mechanism to protect data stored on the phone and other convergence devices. The data must also be protected while it is in transit between devices. Each application will likely have its own mechanisms for implementing integrity and confidentiality since no standards exist. This makes consistently managing and protecting the use of these applications difficult.

A more serious problem is that synchronization with handhelds and mobile phones could result in the transfer of malicious code, such as viruses, from these devices to the IPT network. Many IP phones are embedded systems that run software similar to that used on handheld devices and cell phones. If these devices are infected with malicious code, that code could be transferred to the IP phone.

Voicemail services are another area where the IP telephony network interacts with the data network. Voicemail systems may make voice messages available to users in email. Users may be able to send email that can be accessed from the phone.

Mitigations

The common theme in the previous examples is data traffic between telephony and data networks. This further opens the telephony network to many of the same vulnerabilities that afflict the data network. The safest mitigation is to not allow traffic between networks. However, the advantages of convergence may outweigh the risk. At a minimum, any such service must have strong authentication and authorization controls in place to prevent attackers from abusing convergence solutions.

This in itself is not enough. Authorized users can still inadvertently spread malicious code. In this case, the points where data moves between networks should be tightly controlled. Data transfer should not occur directly between the IP phone and other devices. Instead, a firewall should be setup to act as a gateway between the telephony and data networks (Figure 10). At minimum, this should be a stateful layer 3 and 4 firewall. More appropriate is a stateful layer 3-5 and application-layer firewall that can check all data for malicious code. Any services that must be used on both networks should live in a DMZ between the networks. For example, consider synchronizing a PDA and phone with the same address book. The PDA should not synchronize directly with the phone. Instead, a messaging server would live in the DMZ between the telephony and data networks. The phone, PDA, and desktop PC would all access the address book from the messaging server. The messaging server could then act as a gateway between devices—providing authentication and authorization services and scanning data for malicious code.

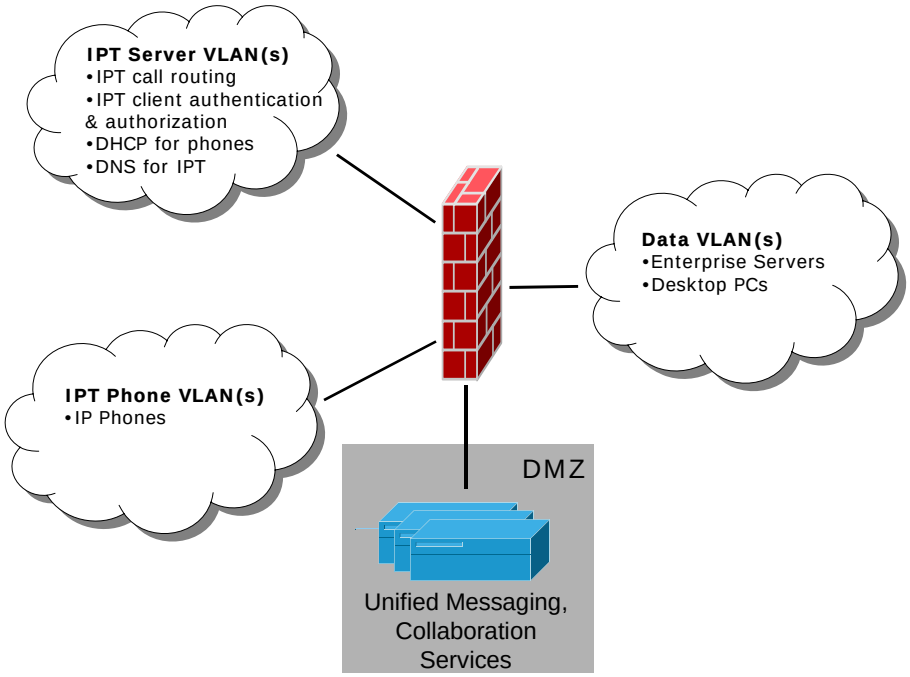

Figure 10 – Medium robustness level network layout for addition of unified messaging and other converged services. Both IPT devices (phones and servers) and data devices (PCs, data servers) require access to the unified messaging services. To preserve separation of IPT VLANs and data VLAN(s), such convergence services must be placed in a demilitarized zone (DMZ) between the VLANs. An application-layer firewall should limit the network services that are allowed between each network and the DMZ. No network services should directly cross the firewall between the IPT and data VLANs. All services must be passed through the DMZ. The minimum robustness layout would replace the application-layer firewall with a stateful layer 3 and 4 firewall.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Convergence Features			
Do not allow IP phone interaction with non-telephony devices.			X
Use strong authentication with all converged services.	X	X	
Place all converged services in a network demilitarized zone between the data and IPT networks.	X	X	
Install a stateful layer 3 and 4 firewall between the data, IPT, and converged services networks.	X		
Install a firewall between the data, IPT, and converged services networks. The firewall performs stateful layer 3 and 4, and application layer filtering.		X	
Scan for malicious code in the DMZ between voice and data networks and on the firewall between the networks.		X	

Softphones

A softphone is IP phone software that runs on a personal computer. The use of these phones poses several challenges when the telephony and data networks are logically separated using VLANs. The phones must operate on a computer that is connected to both the data and telephony networks. The PC violates the separation between the telephony and data networks, because it must directly access both networks. Thus, compromise of the PC would allow access to both networks.

Replacing desktop phones with softphones also creates a single point of failure for communications. A widespread problem, which affects many PCs or the network infrastructure, will disable all communications. Users will not even have a means to report the failure. A fast spreading worm or power outage could create such a situation.

Softphones make management of the IP phone network more difficult because the IPT server will not be able to reliably determine the type of device connecting to it. Untrusted softphones can be loaded on PCs by end users. Since the IPT server does not know about these phones, it will not be able to ensure they are configured securely.

Mitigations

If softphones are in use, then another VLAN should be created and all PCs with softphones should be placed on this VLAN. Traffic filtering rules should allow VoIP traffic between this VLAN and the IPT VLANs. VoIP traffic should not be allowed on the data VLAN. Similarly, general data traffic should not be allowed to the IPT server or IPT phone VLANs.

If softphones are densely deployed throughout the network, it is not practical to have a data VLAN and a softphone VLAN. Instead, all PCs, whether or not they have softphones installed, should be placed in a data VLANs. Traffic should be filtered as described for the softphone VLAN in the previous paragraph.

When softphones are used as the primary voice communication mechanism, then a backup communication method, which does not depend on the PC, must be available in every office area.

Mitigations Summary

Mitigation	Minimum	Medium	Highest
Softphones			
Do not use softphones.		X	X
Create a separate VLAN for PCs with softphones. Filter traffic from this network such that VoIP traffic is allowed to and from the IPT server and phone VLANs, and data traffic is allowed to and from the data VLAN.	X		

Conclusion

IPT systems are replacing legacy PBX systems due to expectations of cost and feature advantages. It is important to take advantage of these benefits without placing an organization's information and business continuity at risk. IPT systems can be secured, but not without cost. The reliability requirements and complexity of IPT systems can make implementing security protections a challenging task.

Determining a security policy that identifies information valuable to the organization and defines the value of that information is the first step in securing IPT systems. Though not discussed in great detail in this guide, writing a security policy is the most important step. Without knowing what information to protect, the value of that information, and from what attack vectors protection is required, effectively applying any security mechanism is difficult.

With a security policy in place, a robustness level that matches the organization's information assurance needs can be chosen. This can only serve as a baseline for the mitigations to implement, because no single robustness level will perfectly fit any organization. The security policy can help serve as a guide as to where to deviate to mitigations at higher or lower robustness levels.

The IPT system designer must then plan development of the IPT system. This involves choosing an IPT system vendor, determining what infrastructure improvements to make, and planning deployment of the IPT system. This guide can help with those steps by mapping the type of features the designer should look for in vendors' products. An IPT system should implement as many of the mitigations as possible and make it easy for an organization to manage those features. This guide describes the network security mechanisms that should be supported by the network infrastructure and provides a general order for implementing security mechanisms in a way that ensures no component of the IPT system is left vulnerable while waiting for other components to be deployed.

Defense-in-depth is essential to protecting an IPT system and ensuring availability of service. No single mechanism can ensure security, and thus, multiple layers of security are recommended in this guide. Network security mechanisms keep people off the network who do not belong and preserve availability of IP services, but cannot prevent malicious insider network use. Perimeter security and virtual separation of IPT and data services play key roles here. Virtual separation makes managing the security of the network easier and isolates different services into different network zones. Perimeter security techniques can then be used between those zones to filter traffic and prevent problems on the data network from affecting the IPT network and vice versa. Perimeter security also puts up a barrier to attacks against the IPT system from public networks such as the Internet or private VoIP carriers.

Security is also recommended at the application layer. Authentication and authorization of users is done using application layer security mechanisms. These are vitally important to securing IPT systems. Without strong authentication and authorization messaging, spoofing, impersonation, and eavesdropping are possible. Application layer security also provides end-to-end confidentiality and integrity protection.

The last layer is device security on servers and phones. IPT systems add a large number of new devices to the network and all these devices offer additional services, such as remote management and convergence features, beyond what is needed for

basic IPT service. Each device needs to have unnecessary services and features disabled. Those additional features, which are necessary, must be configured in a secure manner. This means regularly applying software security updates and enabling authentication and authorization of users of those features.

In order to make absorbing and reviewing the guidelines easier, all the mitigations summaries are combined into a single table and included in Appendix A. Since this table only includes mitigations, reading the text of the guide is still necessary in order to understand the vulnerabilities addressed by the mitigations in the table.

Following these guidelines will not only protect the IPT systems, but also protect data services. Many of the guidelines are not unique to IPT. Many are data and network security best practices that should be followed on all critical IP networks.

References

[1] National Security Agency Configuration Guides. *http://www.nsa.gov/snac*

[2] Defense Information Systems Agency (DISA) Security Technical Implementation Guides. *http://iase.disa.mil/stigs/stig/index.html*

[3] National Institute of Standards and Technology (NIST) Computer Security Special Publications. *http://csrc.nist.gov/publications/nistpubs/*

[4] "Security Considerations For Voice Over IP Systems," National Institute of Standards and Technology, Jan. 2005. *http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf*

[5] "Internet Protocol Telephony and Voice Over Internet Protocol Security Technical Implementation Guide Version 2, Release 1," Defense Information Systems Agency, Aug. 2005. *http://iase.disa.mil/stigs/stig/VoIP-STIG-V2R11.pdf*

[6] "Vulnerabilities and Countermeasures Associated with Integrated Bluetooth Capability," NSA Information Assurance Advisory IAA-004-2004, 2004. *See Appendix B.*

[7] "Wireless Security Technical Implementation Guide Version 4, Release 0.3," Defense Information Systems Agency, Aug. 2005. *http://iase.disa.mil/stigs/stig/draftwireless-stig-v4r0.3.pdf*

[8] "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," DoD Directive 8100.2, 2004. *http://www.dtic.mil/whs/directives/corres/html/81002.htm*

[9] "Recommended 802.11 Wireless Local Area Network Architecture," National Security Agency, 2005. *http://www.nsa.gov/snac*

Appendix A - Mitigations Summary

IPT Network Vulnerability Mitigation Guidelines

Mitigation	Minimum	Medium	Highest
Accessibility and Network Separation			
Place IPT phones, IPT servers, and data devices on separate VLANs.	X	X	X
Place IPT servers and gateways each on their own VLANs separate from IPT phones and data devices.		X	X
Place IPT servers implementing different protocols on separate VLANs. Example: a SIP VLAN and a H.323 VLAN.			X
Enable port level security on all switches.	X	X	X
802.1x authentication is required of all devices connecting to the IPT network.			X
Traffic flow between IPT VLANs is controlled by packet filtering routers.	X	X	X
No network traffic is allowed between the IPT and data VLANs.			X
Traffic between the IPT and data VLANs is controlled by a layer 3 & 4 stateful firewall. Filtering traffic at the application layer is not required.	X		
Traffic between the IPT and data VLANs is controlled by an application-layer firewall.		X	
Servers needing access to devices in both the IPT and data network are kept in a DMZ connected to the firewall separating the IPT and data networks, e.g., unified message servers.	X	X	
The IPT network and the data network have separate servers for common network services such as DNS, DHCP, and NTP.	X	X	X
Call Eavesdropping			
Switched network.	X	X	X
Ethernet switch ports are configured to only allow known MAC addresses. **OR** Ethernet switches only allow traffic that matches the IP address and MAC address assigned to a port during a DHCP lease.		X	X
Configure switches to alert administrators when MAC address tables overflow.		X	X
Encrypt all IPT traffic end-to-end. See *Eavesdropping and Impersonation* on page 40.			X
Network Availability and Physical Access			
Network hardware is in a restricted access area. Physical security mitigations for servers are applicable here also.	X	X	X
All network closets are monitored with video surveillance.			X

Mitigation	Minimum	Medium	Highest
Network equipment has short-term power backup	X	X	
Network equipment has long-term power backup.			X
IP phones obtain power from the network cable.	X	X	X
Network backup power is sufficient to supply power to IP phones.	X	X	X
All network equipment has configurations and software backed up regularly.	X	X	X
Backup and recovery policy is in place.	X	X	X
Backup and recovery processes are tested.	X	X	X
Backups are stored in an environmentally controlled and locked room.	X	X	X
Backups are encrypted when not under physical control of the organization.	X	X	X
Configuration and software backups are kept off site.			X
Denial of Service			
Determine the number of incoming external calls the IPT network can handle and still adequately support internal calls. Use network perimeter devices to allocate bandwidth only sufficient for that number of external calls.		X	X
Limit the number of external calls accepted by the IPT servers.		X	X
Use routers to prioritize IPT VLAN traffic over data VLAN traffic.		X	X
Use anti-virus software and promptly apply software security updates.	X	X	X
Network Intrusion Detection			
Install network intrusion detection systems to monitor both IPT and data networks.		X	X
PSTN Gateways			
PSTN gateways require client authentication before completing calls.	X	X	X
PSTN gateways are placed on a separate VLAN and signaling (e.g., SIP, H.323) traffic is only accepted into the VLAN from authorized servers.		X	X
Validate and terminate all PSTN signaling messages at the gateway.	X	X	X
Public IP Networks as Voice Carriers			
All VoIP traffic over public IP networks (i.e., the Internet) is encrypted.	X	X	X
Interoffice VPNs respect and maintain the separation of IPT and data traffic.	X	X	X
Session border controllers are installed to supplement conventional firewalls when VoIP is used to complete external calls.	X	X	X
Wide Area Network Links			
Tunnel all WAN traffic over a VPN. The VPN respects and maintains separation of IPT and data traffic.	X	X	X

IPT Server Vulnerability Mitigation Guidelines

Mitigation	Minimum	Medium	Highest
Secure servers following the appropriate NSA security guidance documents and industry best practices.	X	X	X
User Accounts			
Limit user accounts on servers to only the administrators of the server.	X	X	X
Assign to user accounts only the privileges necessary for the user to complete required tasks.		X	X
Remove or disable unused default accounts.	X	X	X
Require complex and hard to guess passwords for server user accounts, and audit passwords for compliance. Limit the number of failed login attempts.	X	X	X
Change all default passwords before connecting server to the network.	X	X	X
Default Configuration Settings			
Audit all default configuration settings before connecting the server to the network.	X	X	X
Auditing and Logging			
Enable system logging and logging of call detail records (CDRs).	X	X	X
Regularly review logs for discrepancies.		X	X
Send all logs to a hardened log server.		X	X
Log server should only accept log messages from authorized servers.		X	X
Software Vulnerabilities			
Promptly test and apply vendor security updates.	X	X	X
Require software updates be cryptographically signed by the software vendor.	X	X	X
Malicious Software			
Install anti-virus software on servers and update virus definitions regularly.	X	X	X
Do not use servers for general Internet access, such as email and web browsing.	X	X	X
Network Services			
Disable unnecessary network services on all servers.	X	X	X
Database Security			
Use a secure channel to connect the IPT and database servers, and limit access to database server to IP addresses of the IPT servers.	X		
Use a dedicated communication channel, such as a separate physical network, to connect IPT server and database servers.		X	X
Cryptographic Key Material			
Password protect cryptographic keys.	X	X	X

Store and use private keys for signing configuration files, firmware, downloadable applications, and certificates on a computer not connected to any network.		X	X
Use a hardware token to store keys and perform cryptographic operations using the keys.			X
Physical Security			
Servers are in a locked room or cabinet.	X	X	X
Control access to server room using cylinder locks and shared keys. (For highest robustness, use in combination with other access control mechanisms.)	X		
Control access to server room using access cards or biometrics. Maintain logs of people entering room.		X	
Control access to server room using both cylinder locks, and access cards or biometrics. Maintain logs of people entering room.			X
Install alarms on all entry points to the server room.			X
Disable booting from removable media.		X	X
Enable password protection of BIOS settings.		X	X
Monitor server rooms or cabinets with surveillance cameras.			X
Install fire suppression systems.	X	X	
Install fire suppression systems safe to electronic equipment.			X
Do not run water or sewage mains through server rooms.	X	X	X
Hardware and Power Failures			
Servers use RAID disk mirroring.	X		
Servers use RAID 5 disk mirroring and striping.		X	X
Servers have redundant power supplies.		X	X
Servers have ECC memory.		X	X
Servers are configured with hot standbys.	X	X	X
A spare server is always available to replace a failed server.		X	X
Servers have short-term power backup.	X	X	
Servers have long-term power backup.			X
Data Loss			
Backup and recovery policy is in place.	X	X	X
Backup and recovery processes are tested.	X	X	X
Full backups are performed weekly.	X	X	X
Incremental backups are performed daily.		X	X
Backups stored in an environmentally controlled and locked room.		X	X
Backups stored at multiple geographically separated locations.		X	X
Archive backups periodically.		X	X
Backups are encrypted when not under physical control of the organization.	X	X	X
Emergency Services			
IPT servers maintain phone location information. Location needs to be updated manually, thus phone location must be static.		X	X

Provide each office area with an emergency phone connected to the PSTN.	X		
Access Control For IPT Clients			
Disable automatic registration capabilities	X	X	X
Disable DHCP after initial deployment of phones.			X
Enable DHCP, but only with anti-spoof protections.	X	X	
Enable two-way authentication between telephony end devices and servers		X	X
Require users to authenticate themselves to the phone before making calls.			X
Web-based Management Interfaces			
Limit access to web interfaces to the IP addresses of administrator workstations.	X		
Isolate web interfaces on a separate administrative network.		X	
Only allow access to the web interface from the server itself and disable remote access.			X
Enable TLS on the web server and disable non-TLS connections.	X	X	
Disable web browser password caching features unless the passwords are strongly encrypted.	X	X	X
Regularly apply security updates to the web server and web applications.	X	X	X
Proprietary Management Software			
Limit access to the management server to the IP addresses of administrator workstations.	X	X	
Isolate management server on a separate administrative network.		X	
Only allow access to the management software from the server itself and disable external access.			X
Enable encryption features of the management software. If such features are not available, route all network connections through a secure tunnel, such as IPSEC, TLS, or SSH.	X	X	
Disable password caching features of vendor's client unless the passwords are strongly encrypted.	X	X	X
Regularly apply updates to the vendor's management software.	X	X	X
Remote Management by the Vendor			
Do not allow remote management of IPT servers by the vendor.			X
Use a dedicated connection, such as a PSTN or ISDN line, for vendor access to servers.	X	X	
Encrypt traffic over the dedicated connection.		X	
Physically disable the vendor's connection when not in use.	X	X	
Require that the administrator initiate the connection to the vendor.		X	
Require vendor to connect over a secure and authenticated channel (e.g. VPN, TLS, SSH).		X	
Monitor and log all actions performed by the vendor on the server.	X	X	

IPT Phone Vulnerability Mitigation Guidelines

Mitigation	Minimum	Medium	Highest
Software Vulnerabilities			
Disable unnecessary features and applications.	X	X	X
Limit access to phones using VLANs, access control lists, and firewalls. See *Accessibility and Network Separation* on page 8.	X	X	X
Regularly test and apply security updates.	X	X	X
Separate IPT and data traffic using VLANs.	X	X	X
Third-party Software			
Allow only features that have been tested in laboratory environments.	X		
Limit applications on phones to those that have been tested in a laboratory environment, cryptographically signed by the organization, and made available through an internal server.		X	
Do not allow users to install software on their phones.			X
Block direct Internet access from phones.	X	X	X
Malicious Software			
Implement mitigations in the *Software Vulnerabilities* and *Third-party Software* sections (page 32) to prevent untrusted applications from being installed on phones.	X	X	X
Embedded Microphones			
Physically disable speakerphone microphones.		X	X
Use dedicated phones, which physically disconnect the microphone when the handset is in the cradle.		X	
Use push-to-talk handsets or headsets.			X
DHCP			
DHCP enabled for most phones.	X		
DHCP enabled with link layer authentication for all phones.		X	
Static IP addresses assigned to all phones.			X
Access control lists on routers and firewalls configured to limit access to the DHCP client ports.		X	X
Static IP addresses assigned to critical servers and phones.	X	X	X
Network devices required to use link layer authentication (such as 802.1x) before connecting to the network			X
Implement DHCP anti-spoofing measures on network switches.		X	X
Downloading Firmware and Configuration Files			
Cryptographically signed firmware and configuration files obtained from hardened servers.	X	X	X
Use redundant and physically dispersed servers for distributing firmware and configuration files.		X	X

Mitigation	Minimum	Medium	Highest
Web-based Management Interface			
Use router or switch access control lists to limit access to the phone's web interface to authorized IP addresses only.	X		
Enable HTTP-Digest password authentication.	X		
Disable remote access to the phone's web interface and perform all phone configuration on a central server and have the phone automatically download new signed configurations. **OR** Enable TLS and use strong passwords on phone's web interface.		X	
Disable remote access to the phone's web interface and perform all phone configuration on a central server and have the phone automatically download new signed configurations. **OR** Allow access to the web interface to only those devices directly connected to the phone using the phone's PC port or USB.			X
Simple Network Management Protocol			
SNMP version 3 used to manage phone settings.	X	X	
Disable SNMP, or set to read-only if SNMP access is necessary.			X
Use router or switch access control lists to limit access to the phone's SNMP port to authorized IP addresses only.	X	X	X
Telnet			
Disable telnet on all phones	X	X	X
Ethernet			
Enable VLAN separation on phone computer port.	X	X	
Disable computer port.			X
Infrared			
Enable security mechanisms in all IrDA applications.	X		
Disable IrDA port in phone's configuration.		X	X
Cover IrDA port on phones using metallic tape.			X
Wireless Personal Area Networks			
Disable wireless PAN connectivity to IP phones.		X	X
Wireless Local Area Networks			
Disable WLAN access points built into phones.		X	X
WLAN phones meet all security requirements specified in WLAN security policy.	X	X	X
WLAN phones and WLAN infrastructure meet all the same security requirements specified for IPT clients and infrastructure.	X	X	X

Mitigation	Minimum	Medium	Highest
Eavesdropping and Impersonation			
Phones authenticate to server using a challenge-response protocol (e.g., HTTP-Digest) with long and complex passwords.	X		
Mutual authentication between phones and IPT servers using strong cryptography (e.g., public keys).		X	X
Mutual authentication between phones.		X	X
Encryption of media streams.			X
Encryption of signaling protocols.		X	X
Convergence Features			
Do not allow IP phone interaction with non-telephony devices.			X
Use strong authentication with all converged services.	X	X	
Place all converged services in a network demilitarized zone between the data and IPT networks.	X	X	
Install a stateful layer 3 and 4 firewall between the data, IPT, and converged services networks.	X		
Install a firewall between the data, IPT, and converged services networks. The firewall performs stateful layer 3 and 4, and application layer filtering.		X	
Scan for malicious code in the DMZ between voice and data networks and the firewall between the networks.		X	
Softphones			
Do not use softphones.		X	X
Create a separate VLAN for PCs with softphones. Filter traffic from this network such that VoIP traffic is allowed to and from the IPT server and phone VLANs, and data traffic is allowed to and from the data VLAN.	X		

Changes

Version 1.00, 18 Nov 2005

- Initial release.

Version 1.01, 03 Jan 2006

- Removed leftover firewall from figures 2, 4, 5, & 6.