



White Paper

metagroup.com



800-945-META [6382]

January 2005

IP Telephony Security:

Deploying Secure IP Telephony in the Enterprise Network

A META Group White Paper

“The objective is to integrate IP telephony and traditional data services onto a shared network infrastructure — without compromising the security of either service. Protective mechanisms against all types of attacks must be applied in a holistic manner throughout the enterprise network.”



METAGROUP

Contents

Introduction	2
Identifying and Understanding the Risks	2
<i>Evaluating Risks</i>	4
Degraded Data Network Security Due to Degraded Firewall Security	4
Increased Capital Expenditures Due to Degraded Firewall Performance	4
Loss of Revenue Due to Loss of Communication	4
Excessive Operational Costs Due to Fraudulent Usage	5
The Compromising of Business or Personnel Information Stored on Servers in the Data Network	5
Violation of Confidentiality by Interception of Communication	5
Designing Secure IP Telephony Solutions	5
<i>Defining a Security Framework</i>	6
End-User Devices	6
IPT Media-Related Servers	6
<i>Network Security Features</i>	8
LAN Impacts	8
WAN Impacts	8
<i>Security Across the Domain Boundary</i>	9
<i>IP Telephony-Specific Security Features</i>	10
The Call Control Server	10
The Voice Gateway	11
The IP Phone	11
Bottom Line	12

Introduction

As voice over IP (VoIP) installations increasingly evolve from PBX trunking over private data networks to IP telephony (IPT)-based solutions — and, in some cases, incorporating public networks — it becomes increasingly important to recognize and address associated security issues. The risk and threat to enterprises deploying IP telephony are very real, and although few incidents have been reported in public, these are expected to increase in number as IP telephony deployments increase in number and size. Unless protective security measures are taken, the enterprise will be left open to privacy violation, fraud, and malicious attacks.

To mitigate these threats appropriately, the actual risks must be identified and mapped to a security framework. This framework can then be used to establish security requirements for the products used to obtain an appropriate level of security for the IPT solution. However, since IP telephony is a service that enables direct communication between end-user IP phones throughout an enterprise, it is critical that security measures allow this type of peer-to-peer traffic flow while protecting the telephony service. The telephony service is a convergence of the enterprise voice and data infrastructure, so it is critical that a security strategy be implemented on an enterprisewide level within the enterprisewide security framework. These measures must be taken as VoIP projects are planned and executed, and if properly implemented, most risks can be adequately mitigated.

Identifying and Understanding the Risks

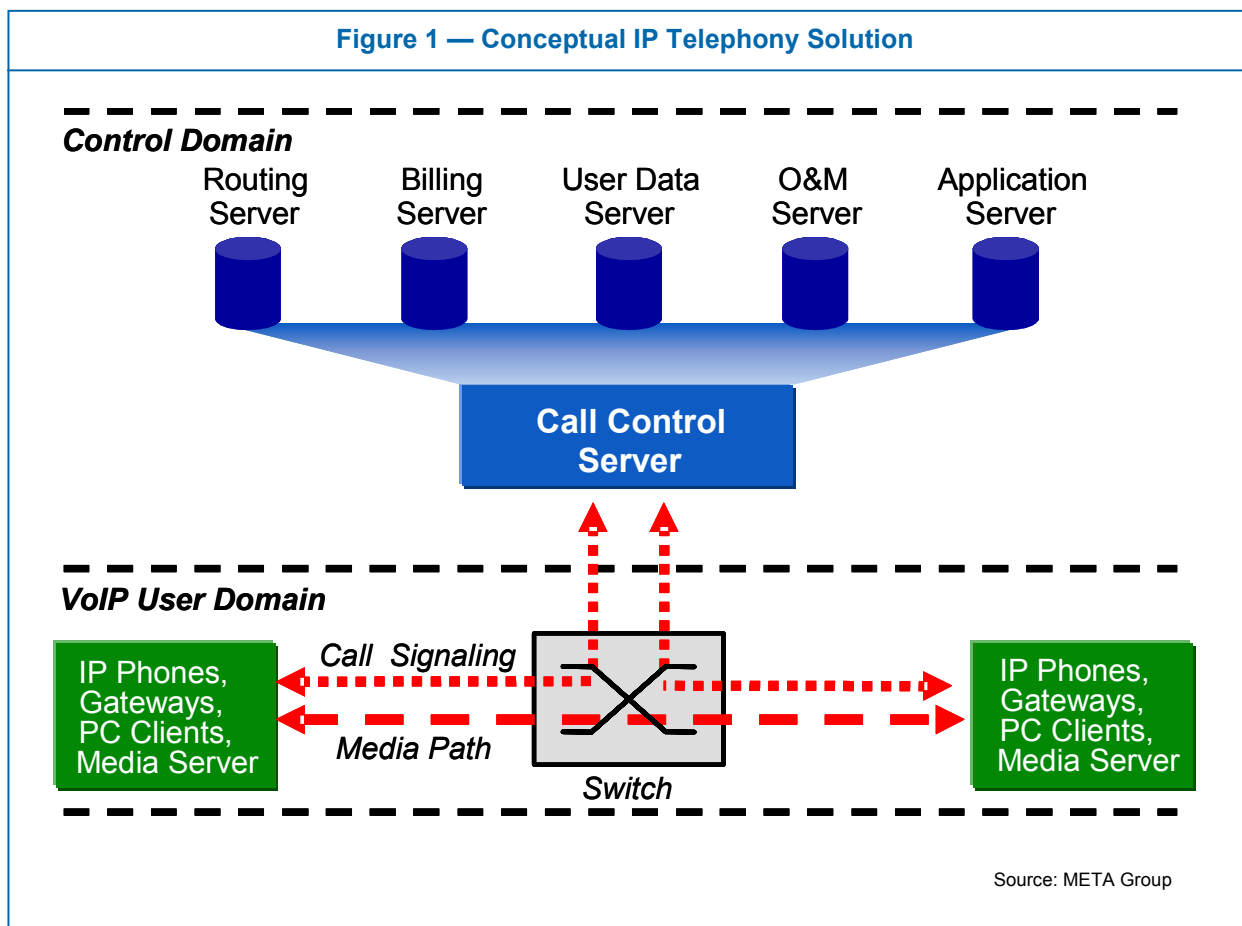
IP telephony is still a young technology with rapidly evolving products, and the initial focus typically is on issues other than security, such as telephony-grade reliability, voice quality, and telephony features. As a result, various solutions have been implemented in enterprise networks with only a limited degree of focus on security issues. Therefore, a significant number of existing telephony deployments have been left unsecured, leaving both the telephony service and the enterprise IP network open to attack. This is often due to lack of understanding of the actual risk level, and even lack of recognition that security is a potential issue.

The first step toward securing an IP telephony solution is to gain understanding of the risks involved. General security risks can be grouped into the following four areas:

1. Interception and impersonation of IPT sessions invading privacy or tampering with information
2. Intrusion of other network services facilitated by the IPT implementation
3. Non-authorized or fraudulent use of IPT equipment
4. Malicious degradation of voice service (denial-of-service [DOS], virus, and hacker attacks)

IP Telephony Security: Deploying Secure IP Telephony in the Enterprise Network

An IPT application typically consists of proprietary software hosted on open or commercially available hardware and operating systems (e.g., Windows, Linux, Unix). The number of servers depends on vendor implementation as well as the actual deployment. A telephony solution will typically consist of IP phones or softphones, call control servers performing telephony call routing as well as other control functions, and other devices such as voice gateways, mail servers, and conference servers. These components will typically communicate via IP over Ethernet and may be interconnected via switches or routers.



Therefore, the main areas of risk can be associated with IP-based attacks on vulnerabilities in the following areas:

- Vendor-specific software
- The hardware or OS platform hosting the software
- Communication between the components in the solution

- Other network-based devices and applications being enabled or facilitated by vulnerabilities in the design or implementation of the IP telephony solution

Evaluating Risks

The following are some of the risks that may exist in an IPT deployment.

Degraded Data Network Security Due to Degraded Firewall Security

An IPT session will have numerous protocols and port numbers associated with it. H.323 uses numerous protocols for signaling, and both H.323 and SIP use the real-time transport protocol (RTP) for media. The result is that an H.323 session may use seven to 11 port numbers — only two are static; SIP uses at least three, with only one being static. An IPT session uses both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and these may be initiated from both inside and outside the firewall. The standard firewall configuration is to open all potential application ports that may be used. For the IPT application, this can mean a large number of ports, creating unacceptable vulnerabilities.

Increased Capital Expenditures Due to Degraded Firewall Performance

Often, an enterprise network will use a private IP address space partly for address conservation and partly to hide the internal network structure from a security point of view. Thus, the firewall will implement a network address translation (NAT) function. In the case of IPT, the application protocol (H.323 or SIP) will have an IP address embedded as well as the IP address used in the IP header. The NAT function must translate both IP addresses. The resulting increased processing load may lead to reduced firewall throughput.

Loss of Revenue Due to Loss of Communication

As a distributed system, IPT has many individual components that must be protected. Attacks at any point can render the system unusable for one or more users:

- Endpoints and servers (including voice gateways, IP phones, and call control servers) may be targets of DOS attacks initiated from the IP network.
- Endpoints and servers may be infected with viruses that can degrade the IPT service or even propagate themselves to servers in the data network, leading to damaged data storage.
- Malicious attacks may lead to significant changes in routing protocols and other configuration information.

Excessive Operational Costs Due to Fraudulent Usage

Hackers in the IP network may gain unauthorized access to the IPT service via spoofing, replay attacks, or connection hijacking — or simply due to lack of proper access control. Once hackers have gained access, the system can be hijacked for unauthorized uses, and very high usage bills can ensue.

The Compromising of Business or Personnel Information Stored on Servers in the Data Network

- A compromised IP telephony server may serve as a launching point for malicious attacks on other servers in the network. Other networks can also be compromised, which can potentially lead to legal retribution.
- Hackers in the IP network may gain access to call log files or voice messages and thereby obtain information about call and business activities (e.g., who the CEO is calling or who marketing and salespeople are calling, deducing business-critical insight).

Violation of Confidentiality by Interception of Communication

Because voice is transported over a shared IP network, an attack such as man-in-the-middle is possible within the enterprise network by employees and others within a facility as well as in a public shared network. Although this risk is present in traditional systems, it may be slightly elevated due to the shared nature of IP and Ethernet.

These risks may not all be applicable in all different types of IP telephony implementations, and it is important to establish an overall security policy in which all assets, potential risks, rules, mitigation methods, and products are listed. It is advisable to perform a risk assessment on existing IP telephony implementation, especially if these are older implementations based on older and less-advanced products. For new implementations, it is equally important to perform an initial cross-disciplined risk assessment, including a review of the impact on the data network.

Designing Secure IP Telephony Solutions

The objective is to integrate IP telephony and traditional data services onto a shared network infrastructure without compromising the security of either the voice or the IP network. A layered defense is essential: The IP telephony system by itself should not be assumed to mitigate all security risks. Neither should traditional network security measures be assumed to be enough on their own. Instead, a comprehensive risk mitigation strategy must be implemented in combination with IP telephony native features and standard network security measures.

These protective mechanisms must be applied in a holistic manner throughout the enterprise LAN as well as any potential WAN connections. IT organizations should create and implement an IP telephony security framework, using it to mitigate risks as well as to define security requirements for vendors. Failure to implement an IP telephony security framework is likely to expose company security breaches and service disruptions, leading to expensive reactive measures.

Defining a Security Framework

Two main principles of a security framework are the *simplification of design and configuration*, and the *limitation of exposure*. A useful strategy is to divide the actual solution into domains and to limit access rights to each domain depending on functions and associated trust levels within each domain. This will assist in containing potential sources of risks and thereby facilitate simple and cost-effective risk mitigation.

The IPT domain model defines four domains based on the different types of generic functions involved in an IP telephony solution and the generic types of risk mitigation measures needed within each domain: 1) end-user devices; 2) IPT media-related servers; 3) IPT call control-related servers; and 4) IPT operational and management access.

The model is focused not only on enhancing security by simplifying design, but also on the need to be practical and avoid unnecessary inconvenience. For this reason, the model differentiates between all user-dedicated devices (IP phones, PCs, and PC-based IPT client software) and IPT servers (call control server, conferencing server, voice mail server) and is divided into two trust levels, depending on user access needs and level of critical information.

End-User Devices

The domain where end-user PCs is placed is generally considered a high risk domain due to the potential for virus infection, and the risks of end users themselves engaging in undesirable activities. Therefore, this level should be described as the lowest trust level from an IPT service point of view, and only IPT assets without influence on the overall IPT service (e.g., IP phones, IPT PC clients) should be placed in this level. Devices associated with call control or systems administration should not be placed at this layer.

IPT Media-Related Servers

All IPT media-related servers such as gateways and message and conference servers are placed in a medium trust level. Access is voice traffic from voice devices (IP phones), except for operations and maintenance (O&M). No user-

sensitive or service-critical data should be accessible at this layer, but the layer must be widely accessible for all telephony traffic.

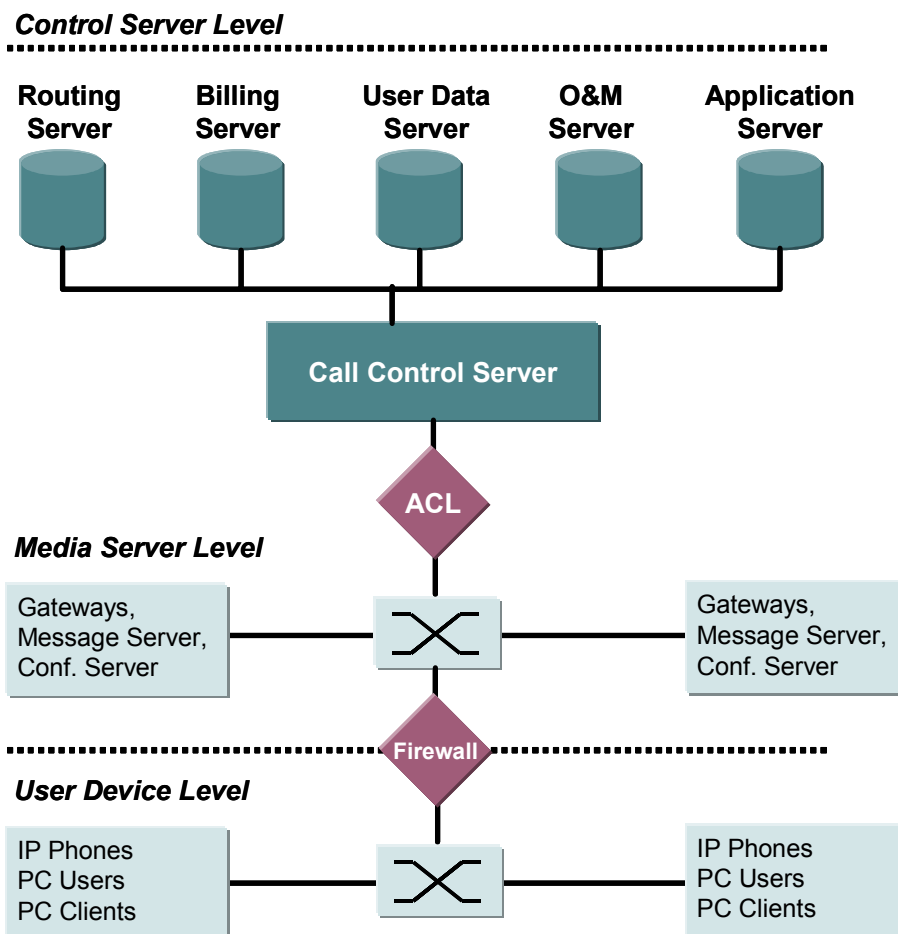
IPT Call Control-Related Servers

All IPT call handling-related servers (e.g., call control server, routing server, user database) are placed in a high trust level. These contain service-critical or potentially sensitive data and are the most critical element to protect against DOS attacks.

IPT Operational and Management Access

All IPT operational and management access must be restricted and accessed only via strong authentication control.

Figure 2 — Conceptual IP Telephony Security Model



Source: META Group

Various types of IPT traffic (call signaling, media, O&M, call statistics, etc.) will flow between the various IPT components and must pass between the domains. This must be allowed while preventing all other types of data traffic from entering the trusted domains containing critical IPT servers and devices.

The risk of service intrusion and service interruption is thus best reduced by controlling traffic between the security levels in a layered approach:

- Traffic from the user level should be considered untrusted and should be controlled by an IPT application-aware firewall.
- Traffic from the media server level can be considered trusted, because the server equipment has been pre-authenticated. However, we recommend implementing access control to the control layer via access control lists (ACLs) to lower the risk level further.
- Use virtual LANs (VLANs) to enhance access control to both the media server level and the control level.

Although the model is illustrated as an all-IP solution based on an IP-PBX, the key principles apply to other solutions such as hybrid PBX, hosted IP-PBX, or IP Centrex-based solutions.

Network Security Features

Although the key objective of the network is to enable full connectivity between all the IP telephony components, basic network traffic separation techniques should be used where possible to enhance the level of security.

LAN Impacts

A key issue in the local-area network is to lower the risk of privacy violation by voice interception and to prevent unsolicited traffic from entering secure domains. Reduction of the risk of privacy violation from internal personnel intercepting voice packets can be implemented by using a fully switched network infrastructure. Domain segmentation can be implemented by using VLANs for enhanced traffic control between different security domains.

WAN Impacts

A key issue in the wide-area network is to lower the risk of privacy violation from external people intercepting voice packets by using traditional Layer 2 and 3 switching (FR, ATM, or MPLS) over outsourced carrier infrastructure, and by using encrypted IP VPN (virtual private network) protocols over public shared

infrastructure such as the Internet. Although encryption secures the traffic, the potential performance issues must be considered (e.g., encryption overhead, public network exposures, poor public service-level agreements [SLAs]).

Security Across the Domain Boundary

The firewall is a main component in both perimeter security and internal domain isolation, but to perform this task in IP telephony deployments, the firewall must be IP telephony application aware. Using application-aware firewalls offers a significantly enhanced level of perimeter security, and it is recommended with any VoIP implementation going across domain boundaries.

Traditionally, firewalls function by inspecting packets based on IP addresses and the transport layer protocol port numbers, applying any predefined policies and rule sets to those packets. This creates three significant problems related to a VoIP or IP telephony solution:

1. Various protocols are involved in a VoIP call session, and for both H.323 and SIP, the initial call setup is performed via static well-known ports, while media and media control occur via ports allocated dynamically during call setup. H.323 is especially problematic, since ports are selected randomly in the range of 1024-65535, which prevents stringent static policy rules, specifically for these protocols in traditional firewalls. Opening up large numbers of ports compromises overall network security and is not an acceptable solution.
2. An IP telephony call can be initiated from both outside and inside the firewall, but the standard firewall configuration will not allow such “unsolicited” call requests from outside the firewall.
3. NAT is another particularly difficult issue for VoIP. IP phones communicating with each other embed the IP address within the VoIP protocol (H.323 or SIP) and in the IP header. Traditional NAT functionality checks only the IP header.

These problems are overcome by making the firewall application aware on an individual session basis. This means that the firewall must scan VoIP protocol setup messages (H.323, SIP, proprietary, etc.) and open and close ports dynamically only for calls approved by the call control server. At call disconnection, the firewall must close the session as well as any open ports. The firewall must be:

- Monitoring call setup signaling, allowing only voice traffic that has been authorized

- Opening dynamically allocated ports only for authorized calls
- Closing used ports at call disconnection
- Ensuring traffic is accepted only from allowed origin/destination addresses, at least in a closed enterprise IPT network
- Offering call audit log support

VoIP-based screening significantly enhances the level of perimeter security and should be deployed in all implementations of VoIP, especially those going across the Internet. However, clients should thoroughly check their firewall capabilities and ensure that the firewall has been interoperability tested with the VoIP products being used. VoIP firewalls are part, but not all, of a converged security architecture.

IP Telephony-Specific Security Features

IP telephony products have evolved dramatically since the conception of commercial voice over IP in 1996. Although dedicated security features have been limited to simple registration access control of users, with limited usage control and rudimentary fraud protection, more comprehensive security features are rapidly being adopted. The types of security features and capabilities needed depend on the actual components within the IP telephony solution, which can be grouped into the following areas.

The Call Control Server

The call control server is a critical network entity in the IP telephony solution. It contains all routing, service, and user information, and it can control access to servers containing this information.

The call control server:

1. Is a software entity typically implemented on commercially available operating systems. All standard security precautions should be taken — turning off all unused services, keeping patching of OS and services up-to-date, and using only the operating system for the call control server.
2. Is implemented on secure operating systems (e.g., Linux, Unix, embedded RTOS) by leading vendors. We expect this trend to continue through 2004/05, with Linux or Unix being the dominant platform.

3. Should have all user or device access to servers authenticated and authorized. This will not only reduce fraud, but also enable user-defined service privileges (e.g., VPN, CUG, OCB/ICB).
4. Must support strong authentication for any configuration or software upgrades.
5. Should support application-level, hop-by-hop signaling message authentication on a per-packet basis.
6. Should support encryption of call setup information.

The Voice Gateway

The voice gateway is a network entity that provides media conversion (and in some cases, signaling conversion) between the IP network and the public switched telephone network.

The voice gateway:

1. Must support strong authentication for any configuration or software upgrades.
2. Provides denial-of-service protection on the IP interface.
3. Should be configured to route calls only via the call control server.
4. Has a server component that should be configured with both virus protection and host-based intrusion detection.
5. Should support encryption of both call setup information and media. (An additional end-to-end delay on each media packet of approximately 5ms should be expected.)
6. Should support a media protocol authentication on a per-packet basis.

The IP Phone

The IP phone is an end-user device that provides voice and call signaling connections, and in some cases, advanced feature support, Web browsing, wireless connectivity, etc. These devices will typically have numerous parameters that need configuration, as well as software that must be maintained.

The IP phone:

1. Must authenticate itself to the call control server or a proxy server upon initial registration.
2. Must support strong authentication for any remote configuration or software upgrade.
3. Should support a configurable access control list to control any incoming traffic (e.g., H.323/SIP, RTP, HTTP, FTP, DHCP).
4. When supporting an additional Ethernet port for PC connectivity, should have this implemented via a switching function combined with VLAN functionality.
5. Should support encryption of both call setup information and media as needed. Using encryption can add an additional end-to-end delay on each media packet.

Bottom Line

IP telephony deployments expose the enterprise to new and potentially serious threats. Fortunately, these risks can be adequately mitigated. Best-practice organizations properly understand the risks and manage them via a holistic enterprisewide security architecture, using a combination of IPT system-specific and network-specific security features.

Secure IP telephony requires:

- A risk domain model where IP telephony system critical servers are placed in highly secured domains. IP Telephony endpoints are regarded as system non-critical entities that must maintain a high level of integration flexibility with other end-user devices and services.
- That such domain separation be implemented with IPT-aware firewalls implemented in combination with switched Ethernet, VLAN, and access control list mechanisms.
- That IPT system access control be implemented, and that all IPT system entities be implemented on hardened servers.

Bjarne Munch is a Senior Research Analyst with Infrastructure Strategies, a META Group advisory service. For additional information on this topic or other META Group offerings, contact info@metagroup.com.



About META Group

Return On IntelligenceSM

META Group is a leading provider of information technology research, advisory services, and strategic consulting. Delivering objective and actionable guidance, META Group's experienced analysts and consultants are trusted advisors to IT and business executives around the world. Our unique collaborative models and dedicated customer service help clients be more efficient, effective, and timely in their use of IT to achieve their business goals. Visit metagroup.com for more details on our high-value approach.

