White Paper

Enterprise VoIP Security

Best Practices

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale CA, 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number 200179-001 Apr 2006

TABLE OF CONTENTS

Executive Summary

The opportunity to migrate telephony and voice applications from TDM circuit-switched networks to IP packet-switched networks offers many advantages for enterprise network managers. The current state of Voice over IP (VoIP) technologies allows companies with dedicated WAN resources to leverage their infrastructures for voice and data applications, and realize cost savings in the process. With a single, integrated network in place of two disparate networks, enterprises can consolidate staffing and streamline operations. In addition, the integration of voice and data content onto a single technology platform creates the potential for the development of new, interactive applications that may increase productivity or streamline operations.

In migrating voice applications to IP, however, enterprises now must cope with the security risks inherent in all data applications. While consolidating voice and data traffic can add infrastructure and operational efficiencies, voice networks are now subject to viruses, worms, Denial of Service (DoS) attacks, and other well-known threats to network integrity. Indeed, many of these threats may even be more acute in VoIP networks. For one thing, VoIP architectures tend to be complex and hierarchical, incorporating many networked components, including IP PBXs, application servers, media gateways, and IP phones, in addition to the more ubiquitous routers, switches and firewalls. In addition, VoIP networking relies upon numerous protocols, some of which remain poorly defined, and all of which introduce their own security risks. And finally, the advent of VoIP introduces such well-known risks as toll fraud and telephony hacking (so-called “phreaking”) into the IP world, where shared network resources are now vulnerable.

Fortunately, with proper planning and foresight, network managers can integrate VoIP capabilities into an enterprise network without compromising security, performance, or manageability. That is because, despite their complexity, the risks associated with the protocols and architectures used in VoIP networking are well understood. Not only can enterprises take concrete measures to secure enterprise applications from VoIP network operations – and vice-versa – they can do so while supporting high-quality voice communications.

The purpose of this white paper is as follows:

- to enumerate the risks inherent in enterprise VoIP networking
- to describe and quantify them, and
- to prescribe approaches for minimizing these risks in accordance with the highest standards now available to the industry.

Common VoIP Security Threats

According to a recent IBM Global Business Security Index, the first half of 2005 saw more than 237 million security attacks worldwide.[i] Such attacks can be extremely costly to companies financially and decrease productivity due to downtime. Network attacks cost U.S. companies an average of over $200,000 in 2004, much of this through the theft of proprietary information.[ii] By their very nature, all data networks face some risk of attack from malicious individuals or groups, both within an enterprise environment and outside it. The very advantage of IP networking – the ability to distribute corporate applications and processes across multiple physical locations and geographic boundaries – makes corporate networks attractive targets for opportunistic cybercriminals, disgruntled employees, and other rogue elements.

Security threats of concern to VoIP network managers fall into five categories:

- Distributed DoS (DDoS) Attacks
- Unauthorized Access
- Toll Fraud
- Eavesdropping
- Application-Level Attacks

DDoS or DoS Attacks

DoS attacks are malicious attempts to seriously degrade or crash system operations by sending packets carefully crafted to exploit software weaknesses. Even more malicious are DDoS attacks, which are DoS attacks from multiple systems, all coordinated to flood a particular network system. Enterprise VoIP systems are particularly vulnerable to DDoS attacks for two reasons. First, VoIP systems involve many devices with very specific functionality; a failure in one of these devices could bring the entire voice network to a halt. Second, VoIP devices use multiple protocols, each of which brings its own risk profile. **Exhibit 1** summarizes the protocols most commonly used by voice networking devices, their functions in the network, and their risk profiles.

Unauthorized Access

VoIP systems – and IP PBX systems in particular – involve multiple systems for call control, administration, billing, and other voice telephony functions. Each of these systems may contain data that, if compromised, could enable rampant fraud. The cost incurred by such fraudulent use of enterprise VoIP data, in terms of direct losses, compensatory payments to external parties affected, and damaged goodwill, could be devastating. Access to call data can be the golden ticket a malicious user seeks to perpetrate toll fraud. Repositories in these systems may contain even more damaging data, such as billing or accounting records, which can then be applied more broadly to fraudulent ends, such as credit card fraud or identity theft.

Toll Fraud

During the 1980s, when carriers began to migrate their systems from analog to digital switching technologies, perpetrating toll fraud became something of a dark art among a growing community of telephone system hackers, or "phreakers." The advent of Internet-based telephony only adds to the already-expansive list of methods by which attackers can penetrate call control systems to fraudulent ends.

As with TDM-based PBXs, phreakers can gain unauthorized access to PBX lines to make long-distance or international phone calls. As mentioned above, they may sometimes accomplish this by gaining unauthorized access to accounting records. In another form of toll fraud, phreakers orchestrate a Man In The Middle (MITM) attack that redirects an inbound call to a media gateway, thereby gaining unauthorized use of the VoIP network. Finally, attackers can sometimes exploit networks whose poor authentication systems allow calls from unauthorized IP phones.

Eavesdropping

Without proper precautions, VoIP systems may also be vulnerable to eavesdropping, the interception of voice conversations by unauthorized agents. Eavesdropping can result from intercepting packets or by connecting unauthorized IP phones to VoIP systems.

Application-Level Attacks
As VoIP architectures and products have come into the mainstream, attacks on specific devices and functional components have become a growing threat. Attacks targeted specifically toward VoIP applications include registration hijacking, illegal teardowns, register floods, call floods, malformed packets, harassing calls and spam over Internet telephony (SPIT). By this definition, toll fraud also constitutes an application-level attack.

Of particular concern for VoIP network managers are (Session Initiation Protocol) SIP attacks. SIP is a session and call control protocol, components of which are used by standards-based IP PBX and IP telephone systems. In addition to the standard IP vulnerabilities, SIP brings other risks. While the Internet Engineering Task Force (IETF) has made great strides over the past few years in developing the protocol, a great deal more definition remains before SIP can be considered mature. SIP also ranks high among IP protocols in complexity and extensibility. Finally, like HTTP and SMTP, SIP is text-based. While these characteristics may bestow various advantages to SIP in terms of elegance, durability and utility, they also render the protocol vulnerable to application-level attacks. SIP sessions use at least three port numbers, only one of which is static which makes it a little more challenging from a security perspective.

H.323 is another staple of VoIP that causes some concern for network managers. Technically not a single protocol, but an umbrella recommendation, H.323 originally emerged as a means of transporting multimedia applications over LANs, but later found a place in VoIP networking. As an ITU-T recommendation, H.323 is complex, specifying the application of numerous ITU-T protocols for such functions as call signaling, control message formatting, and stream packetization, all critical to IP-based telephony. An H.323 session may use from 7 to 11 port numbers, only two of which are static. H.323 also selects ports randomly in the range of 1024 through 65535, making it almost impossible to enforce strict firewall policies.

Exhibit 1: Protocols Commonly Used in VoIP

Protocol	Application	Maturity	Risk Level
H.323	Call Signaling, Control Message Formatting, Stream Packetization	Medium-High; high multi-vendor interoperability, but proprietary extensions still used by most vendors.	High; uses up to 11 port numbers per session; standard firewall configurations open all potential application ports, rendering networks extremely vulnerable.
Internet Protocol (IP)	The network layer protocol in the Internet Protocol suite, used to communicate data across a packet-switched network.	Relatively high; IPv6 improves upon IPv4, the most prevalent version of IP in use worldwide, primarily in the use of 128-bit addresses, rather than 32-bit addresses.	High; due to its nature, IP provides only best-effort delivery, and upper-layer protocols must address reliability issues.
Media Gateway Control Protocol (MGCP)	Control and call state communications between Softswitch/Media Gateway Controller and Media Gateway.	Relatively low; the industry *de facto* standard is the informational RFC 2705, maintained by PacketCable and the Softswitch Consortium; implementation of subsequent standard MEGACO/H.248 remains sparse.	Medium; MGCP supports IPSec for message protection, and allows call agents to provide gateways with session keys for encrypting audio messages, to protect against eavesdropping.
Real-time Transport Protocol (RTP)	Streaming Media (e.g., tones, announcements, voice messages)	Medium-High; first defined by ITU-T, later "adopted" by IETF, and now encompasses specific profile for audio and video conferencing and optional Secure RTP.	Medium: encryption supported, but typically with compromised performance.
Session Initiation Protocol (SIP)	Initiation, Modification, and Termination of interactive multimedia user sessions.	Medium; proprietary extensions still used by key system vendors to enable nonstandard features.	Medium; SIP supports point-to-point encryption, but management and technical drawbacks persist, and definition is lacking for SIP requests sent to multiple endpoints.

Best Practices Security Measures

The bottom line: the introduction of voice onto corporate networks increases security risks twofold. First, due to their complexity and immaturity, VoIP technologies introduce a host of new threats to existing IP networks. Second, because voice and data applications now share a common, extensive infrastructure, these new threats make the entire corporate network vulnerable in new ways.

The good news is that there are a number of best-practice security measures that network managers can take to minimize the risk of attack on VoIP systems. These measures include the installation of various devices at key interfaces in the network, the implementation of strategic security provisions on vulnerable VoIP devices, and the deliberate formulation and enforcement of standard procedures to limit exposure of the network to attacks from both within and outside the organization.

The following provides a list of cardinal rules to be applied to any enterprise Best Practices approach to VoIP security.

1. *Maintain Current Patch Levels*

This first rule is rather elementary. Inadequate software patching exposes networks – VoIP or otherwise – to unnecessary risk. Network attacks have grown in sophistication, targeting software vulnerabilities to achieve very specific aims, rather than merely to cause broad, indiscriminate disruption, so a programmatic approach to monitoring and installing patch releases can form an important bulwark for your network, your applications, and your investments.

2. *Install a Good Anti-Virus System and Update it Regularly.*

A Best-Practices item that almost goes without mentioning. With the current proliferation of worms and viruses of increasing sophistication, no computer or network device should go without anti-virus protection; VoIP merely adds another reason to install it. From a VoIP perspective, anti-virus systems tend to protect voice components from infections borne of computers and data systems that are much more vulnerable to attack. Certain firewall products (e.g., Juniper Networks NetScreen firewalls) integrate anti-virus functionality, along with other attributes of particular utility in VoIP implementations and management.

3. *Apply State-of-the-Art Intrusion Detection and Prevention Systems.*

Intrusion Detection and Prevention (IDP) systems use stateful detection and prevention techniques to protect against both current and emerging threats at both the application and network layers. State-of-the-art IDP systems guard against attacks by conducting deep examinations of all packets that comprise communications traffic, thereby exposing a wide variety of suspicious activities and legitimate threats, including those operating at the application layer.

Sophisticated IDP systems, such as Juniper Networks' NetScreen IDP 10, 100, 500 and 1000 products, incorporate such *active* techniques as protocol anomaly detection, recognition of attack signatures, backdoor detection, and regular expression pattern matching. This affords significant advantages over more conventional firewalls that use passive Network Intrusion Detection Systems (NIDS), and which are therefore prone to false alarms, low manageability, high maintenance, and an inability to prevent attacks,

Integrated prevention capabilities can then be exercised to automatically eliminate the certain threats, and flag suspicious items for later review. Armed with these attributes IDP systems pick up where conventional

firewalls leave off, monitoring both internal and cross-boundary traffic, and providing zero day protection against worms, Trojans, spyware, keyloggers, and other malware. As an additional benefit, the Juniper Networks IDP systems use a centralized, rules-based management system, which allows for high levels of control and flexible deployment.

Best-practice VoIP security measures include deploying IDP in conjunction with high-criticality, high-vulnerability, multi-protocol VoIP systems, such as IP PBXs, media servers, and call accounting systems.

4. Install Application-Layer Gateways between Trusted and Untrusted Zones.

Application-Layer Gateways (ALGs) are back-to-back user agents that can perform the function of dynamically opening and closing firewall pinholes to maintain security. ALGs designed specifically to handle demanding applications such as VoIP can prevent against malicious attacks on either VoIP or other systems, as well as against severe system outages due to malfunctioning VoIP devices. Certain ALGs can also read and interpret signaling information in message headers and act upon it as appropriate. Armed with this capability, ALGs can monitor call setup messages to determine whether they appear to be legitimate or bogus (e.g., end devices crash, malicious user manipulation, etc.).

True to their name, ALGs are highly specialized components, and must accommodate the demands of specific protocols and operations by design. ALGs are usually embedded into firewalls and other security devices as a means of enhancing their effectiveness and performance for specific applications. As part of a Best Practices approach to network security, network managers therefore need to consider their ALG needs and deployment strategies protocol by protocol; for VoIP, these protocols are H.323, SIP and MGCP.

The strategic installation of H.323 ALGs will secure communications between VoIP terminal hosts, including IP phones and multimedia devices. Deployed in this way, H.323 ALGs manage call registration, admission, and call status, all critical tasks in call setup and administration, and all vulnerable to attack. H.323 ALGs should be deployed between devices in trusted zones and untrusted zones, and policies should be set accordingly. Some H.323 ALGs (e.g., Juniper Networks NetScreen Enterprise Security Platform products) can also be configured to accept or allow calls that traverse Network Address Translation (NAT) boundaries, a capability that affords even greater security, while maintaining high-quality voice communications across trusted and untrusted zones.

SIP ALGs—ALGs that support SIP as a service and that can screen SIP traffic—are also critical for secure VoIP networking. SIP is used to distribute call session description information, negotiate and modify session parameters during the calls, and to terminate multimedia sessions. There are two types of SIP traffic: signaling and media stream. SIP signaling messages require only a single designated port, and require the creation of a relatively straightforward policy to permit SIP service. The media stream, however, presents challenges for ordinary security devices, in that it uses dynamically assigned port numbers that can change several times during the course of a call. For this purpose, static policies are useless. This characteristic alone makes SIP ALGs indispensable, for the only way to control media traffic is to read SIP messages in order to extract the port number information needed to dynamically open or close pinholes as needed to allow media streams traversal.

MGCP ALGs perform a similar payload inspection task that the aforementioned H.323 and SIP ALGs perform, albeit with MGCP, a text-based Application Layer protocol used for call setup and control. MGCP is based on a master-slave call control architecture in which the media gateway controller maintains call control intelligence via a call agent, while media gateways carry out the instructions of the call agent. As part of a comprehensive security strategy, an MGCP ALG must have the capability to: conduct VoIP signaling payload inspection, to prevent malformed packet attacks, among other threats; conduct MGCP signaling payload inspection, again, to safeguard against malformed packets; provide stateful processing at the UDP packet level, to prevent DoS attacks; perform NAT; and manage pinholes dynamically for media and signaling associated with VoIP traffic.

5. Enforce SIP security by means of Authentication, Authorization and IPSec.

SIP was developed in large part to endow VoIP networks with a superset of the call processing features and functions broadly enjoyed via circuit-switched voice networks. Central among these are device registration, call setup, call termination, and advanced features (e.g., call waiting, call transfer, caller ID, etc.). Unfortunately, the very attributes of SIP that enable this functionality also introduce unique vulnerabilities of concern to VoIP network managers. For starters, like two other protocols in widespread use today, Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP), SIP is text-based. This lends SIP to easy monitoring and spoofing; VoIP network managers face growing threats such as Spam over Internet Telephony (SPIT), essentially unsolicited calls and voice messages; registration hijacking, the malicious impersonation of a valid User Agent (UA) to a registrar; unauthorized call transfers; and unauthorized access to directory information.

The key to securing SIP transactions is strong authentication, authorization and IPSec. As specified in RFC 3261, SIP provides a stateless, challenge-based mechanism for authentication that is based on authentication in HTTP. Whenever a proxy server or UA receives a request, it *may* challenge the initiator of the request to provide assurance of its identity. Once the originator has been identified, the recipient of the request *should* ascertain whether or not this user is authorized to make the request in question. A Best-Practices approach to VoIP security dictates that network managers configure proxy servers and user agents to require identification and perform authorization for every request, in order to avoid proxy impersonation, session teardown and DoS attacks. IPSec provides an additional layer of security at the network layer, by encrypting and authenticating all SIP packets.

All of which boil SIP security to incorporating adequate (and adequately specialized) firewall protection. Juniper Networks NetScreen Integrated Firewall / VPN products provides an ideal platform for the stringent authentication, authorization and IPSec encryption required to secure corporate voice communications. In addition, with their deep inspection capabilities, the products allow SIP source IP limitation, allowing SIP traffic from specific sources to be limited or even blocked. This capability allows VoIP network managers to fend off a variety of network threats, from attacks by unauthorized SIP phones to SPIT and DDoS attacks.

6. Establish Policy-Based Security Zones to Isolate VoIP Segments.

Juniper's products take the concept of security zones beyond the level provided by other products and solutions, by allowing greater flexibility in defining, creating, and parameterize virtual zones. No longer limited to rudimentary Untrust, Trust and DMZ zones, VoIP network managers can leverage the ability of Juniper Networks' security zones to isolate voice network devices, and even virtually segregate voice networking segments, such as by defining intra-office, local and long-distance/international zones, or H.323, SIP and MGCP zones. Defining security zones in this way provides an additional layer of security for critical voice components, limits the impact of attacks and breaches to specific zones, and thus enables faster identification of, and corrective action against, the root problems.

7. Run VoIP Traffic on VPNs to Minimize Eavesdropping Risk on Critical Segments.

Running enterprise VoIP traffic on VPNs can prevent eavesdropping, although encryption/decryption processing can also decrease bandwidth and increase latency. For this reason, a Best-Practices approach might involve VPN encryption selectively, such as only over untrusted network zones. Applied in this way, the VoIP VPN can transparently encrypt a call made to a destination with decryption capability, and proceed without encryption for calls to destinations without decryption.

Most enterprise VoIP deployments are internal or campus-level, where all external calls are converted by a media gateway to travel over the circuit-switched Public Switched Telephone Network (PSTN). An attack must therefore originate from the internal IP network. An enterprise may also use VoIP between distributed

sites or for remote workers. In this case, a Virtual Private Network (VPN) is normally used to connect the sites and provide protection of the data traveling over the untrusted network. In this scenario, VoIP is still only being used internally, because the sites are considered part of the internal, trusted network. Note, however, that a remote worker may be more likely to contract a virus/worm, which could be a threat to the VoIP system.

If session synchronization is not maintained and a tunnel failure occurs, the Security Association (SA) is lost and must be reestablished. Generating, negotiating, and exchanging encryption keys are computationally intensive and overall downtime can increase with a high number of VPN connections. To provide voice-grade resiliency and the lowest possible latency during switchover, each SA must be mirrored and automatically associated with the active connection. Advanced VPN systems, such as Juniper's integrated firewall/IPSec VPN appliances, mirror all VPN security associations, including the timers, keys and certificates. In the event of a failure, VPN tunnels (and the sessions that run through them) can be re-associated immediately with their interfaces and routes.

8. Use VLANs to Prioritize and Protect Voice Traffic from Data Network Attacks.

Virtual LANs (VLANs) help prioritize voice traffic by segmenting voice and data traffic, resulting in low latency and better voice quality. VLAN separation also helps to prevent data network attacks from affecting voice traffic. However, VLANs lack user authentication and can accept packets from other networks, which could result in information from one VLAN jumping over to another VLAN. In addition, tools such as dSniff can create VLAN tags and turn the switched system into a shared medium.

In situations where security is deemed critical, data and voice traffic can be segregated completely through VLANs. To achieve a full isolation of voice from data traffic, IP telephones sharing a physical cable connection with PCs must support the IEEE 802.1Q standard for trunking between VLANs. Where IP phones and PCs coexist on separate subnetworks, isolation may be achieved through the use of a voice-aware firewall, such as Juniper Networks' NetScreen products.

9. Apply Encryption Selectively.

As part of a Best-Practice approach to enterprise VoIP security, VoIP network managers should evaluate the use of encryption to VoIP signaling, media streams, or both. Where the risk of eavesdropping exists, network managers should consider the use of encrypting phones. Because of potential performance issues, however, network managers should approach encryption with surgical discretion, rather than as a security panacea. The full benefit of IPSec, for example, cannot be realized if a NAT device is in the media path. IPSec or simple media encryption will also affect transcoding, which may occur for calls traveling over the WAN. Encrypted calls converted to TDM by a media gateway may fail because the PSTN can lose bits on non-clear channel circuits. Finally, end-to-end encryption over long haul networks generally requires many devices to be encryption-aware. The potential for performance issues to compromise the overall value and utility of a VoIP network must be weighed against the heightened security encryption enables; voice quality guarantees stipulated in service-level agreements, for example, may render encryption unacceptable as a security approach.

10. Protect Against UDP Flooding.

UDP Flooding is a specialized attack on networks that occurs when UDP packets are sent with the intention of slowing down the system to the point where it can no longer handle valid connections. The best way to prevent this type of attack is to install specialized firewall products that enable UDP flood protection, such as Juniper Networks' integrated firewall/VPN solutions. UDP flood protection involves setting a threshold to limit the rate at which UDP packets are transmitted from one or more sources to a single destination.

Should this limit be exceeded, Juniper Networks' solution ignores further UDP packets to that destination for the remainder of that second, as well as the subsequent second.

11. Develop a Holistic Security Program.

As firewalls, VPNs, and other vital systems are installed, security zones are established, and configurations are set to optimize VoIP performance and protection, a Best Practices approach warrants the methodical documentation of security policies and procedures. VoIP network managers should monitor resources constantly in an effort to track known vulnerabilities. To properly secure the network, telnet and other non-secure forms of remote access must be disabled, even at the cost of alienating entire departments who rely on telnet to get their work done; make a companywide pitch for SSH and other secure interfaces to address dissenters' concerns. Disable any unneeded services on all VoIP components, and maintain patches to ensure these components' efficient and safe operation.

Finally, make certain all of this hard work is not undone by a "phishing" attack, involving the manipulation of an unsuspecting insider into disclosing secured information (e.g., username-passcode combination) or granting somebody inappropriate network access. Establish policies and procedures for all personal interactions, from telephone calls to service and maintenance visits, and always demand positive identification. Create and disseminate standard escalation procedures for disputes over such access.

Conclusion

The era of enterprise VoIP has arrived. VoIP technologies have reached a level of maturity where the business case for migrating from more traditional circuit-switched voice is compelling for many companies. But while the integration of voice and data resources promises greater efficiencies and lower cost, it also introduces numerous risks for the security and integrity of the enterprise network.

The good news is that, with proper planning, maintenance and administration, VoIP need not strike fear and loathing into the hearts of MIS professionals. True, the addition of VoIP systems add to existing network security risks, but these risks can be managed by applying common sense, installing the appropriate types of security devices into the networks, configuring them according to the enterprise's needs, and developing a comprehensive policy for maintaining secure networks. **Exhibit 2** lists the Best-Practice approaches for managing different enterprise VoIP networking security risks.

The complexity of VoIP networking demands extraordinary performance on the part of firewalls and other security appliances. In order to protect confidential data and other network resources, as well as to ensure the performance necessary to support high-quality voice communications, network security devices must be protocol-aware, and even application-aware.

Juniper Networks NetScreen products offer protocol-aware and application-aware operation, as well as deep packet analysis, affording networks a combination of high security and high performance unparalleled in the industry. Armed with these advanced capabilities, NetScreen products offer uncompromising performance, making them a strategic cornerstone of any Best-Practice enterprise VoIP network.

Exhibit 2: Best-Practice Approaches for Minimizing Common VoIP Network Risks

Risk	Best-Practice Approaches
Application-level attack	• Use application-aware IDP systems • Use ALGs
DDoS	• Maintain current patch levels • Install and maintain antivirus system • Use application-aware IDP systems • Establish policy-based security zones

	• Use VLANs to protect voice traffic from data network attacks
Eavesdropping	• Isolate critical VoIP traffic on VPNs • Apply encryption selectively
Protocol-targeted attack	• Use ALGs and IDP
SPIT	• User strong authentication, authorization and IPSec
Unauthorized SIP monitoring, spoofing	• Use strong authentication, authorization and IPSec
Virus, Worm	• Maintain current patch levels • Install and maintain antivirus system • Use application-aware IDP systems • Establish policy-based security zones • Use VLANs to protect voice traffic from data network attacks

Glossary

ALG – Application-Layer Gateway, a user agent with the ability to open and close pinholes dynamically in firewalls, as a means of maintaining security even during demanding transactions associated with complex protocols.

DDoS – Distributed Denial of Service attack, an attack on a computer or a network through the use of multiple hosts, which causes a loss of service to users.
.

DoS – Denial of Service attack, which is an attack on a computer or a network that causes a loss of service to users.

dSniff – a packet sniffer and set of traffic analysis tools.

H.323 – An umbrella recommendation for protocols to be used for multimedia sessions published by the International Telecommunication Union's ITU-T body.

HTTP – Hypertext Transfer Protocol, the protocol used to transfer information on the World Wide Web.

IETF – Internet Engineering Task Force, the standards body charged with developing and promoting Internet standards, particularly the TCP/IP protocol suite.

IDP – Intrusion Detection and Prevention system (e.g. Juniper Networks IDP products), which has the ability to inspect packets at high speed in order to identify and block non-compliant data traffic.

IP – Internet Protocol, which refers both to the data-oriented protocol used to send data across a packet-switched network and to the suite of communications protocols on which the Internet runs.

IPSec – A standard for securing IP communications by encrypting and/or authenticating all packets.

MGCP – Media Gateway Control Protocol, which defines the means by which softwitches communicate with media gateways.

MITM – Man In The Middle attack, in which a VoIP call is fraudulently redirected as a means of gaining unauthorized access to the network.

NAT – Network Address Translation, a process by which source and/or destination addressing is redefined as packets traverse a router or firewall.

PBX – Private Branch Exchange, a premises-based telephone switching system.

Phishing – A type of attack that involves deception as a means of gaining unauthorized entry or access to network resources.

Phreaker – An individual or organization who engages in unauthorized intrusion to, and manipulation of, voice networking systems.

PSTN – Public Switched Telephone Network, the legacy voice network, characterized by circuit-switched, dedicated-facility service.

SIP – Session Initiation Protocol, an IETF standard for initiating, modifying and terminating an interactive user session involving voice, video or other multimedia components.

SMTP – Simple Mail Transfer Protocol.

SPIT – SPAM over Internet Telephony, a form of harassment that occurs when unwelcome calls, typically with the intent to advertise, are targeted toward a VoIP system.

SSH – Secure Shell, both a computer program and a network protocol for secured, encrypted login and command execution on a networked computer.

TDM – Time-Division Multiplexing, the conventional paradigm for transporting voice calls via a dedicated circuit-switched network.

UDP – User Datagram Protocol, which defines how networked computers can communicate with each other via short messages, or *datagrams*.

VLAN – Virtual Local Area Network, a network that is logically independent, even though several VLANs can physically coexist on a single switch.

VoIP – Voice over Internet Protocol, generally, the routing of voice communications over the Internet or any IP-based network.

VPN – Virtual Private Network, a private network created via the use of standard or nonstandard protocols over a public network.

WAN – Wide-Area Network, a computer network covering a wide geographical network (e.g., the Internet).

Notes

[i] Internet attacks increase in number, severity, Elizabeth Millard, CIO Today (www.cio-today.com), August 2, 2005.
[ii] Beyond viruses. Sebastian Rupley. PC Magazine 24.15 (Sept 6, 2005): p26(1).

