

WHITE PAPER

Intrusion Prevention: The Future of VoIP Security

TippingPoint
The Leader in Intrusion Prevention

Introduction	2
VoIP Building Blocks	3
VoIP Security Threat Scenarios	7
Attacks against the underlying VoIP devices' OS	7
Configuration Weaknesses in VoIP devices	8
IP Infrastructure Attacks	9
VoIP Protocol Implementation Vulnerabilities	9
VoIP Application Level Attacks	9
The Future of VoIP Security	10
VoIP and TippingPoint.....	11

Summary

Voice-over-IP (VoIP) technology has come of age and is quickly gaining momentum on Broadband networks. VoIP packetizes phone calls through the same routes used by network and Internet traffic and is consequently prone to the same cyber threats that plague data networks today. These include denial-of-service attacks, worms, viruses, and hacker exploitation. In addition to these traditional network security and availability concerns, there are also a plethora of new VoIP protocols that have yet to undergo detailed security analysis and scrutiny. The challenge of VoIP security is not new. History has shown that many other advances and trends in information technology (e.g. TCP/IP, Wireless 802.11, Web Services, etc.) typically outpace the corresponding realistic security requirements that are often tackled only after these technologies have been widely adopted and deployed.

Introduction

VoIP technology in general refers to the set of software, hardware and industry standards that enable “voice” to be transported using the Internet Protocol (IP). The technology has been initially welcomed by many broadband service providers who plan on offering telephony services to their customers. According to some analyst estimates, VoIP will account for 75 percent of the world voice services by 2007 and the IP-based PBX market is estimated to grow to \$16 billion worldwide by 2006¹. The technology is compelling to a wide audience for several reasons:

- VoIP phone bills are typically cheaper than traditional phone bills to the consumer.
- VoIP networks offers providers easier IT management and reduction in operating cost for a combined network for voice and data.
- VoIP technology is feature rich to support next generation multimedia applications.

However, despite the seemingly overwhelming advantages of VoIP to Public Switched Telephone Networks, there are stringent and mandatory requirements that VoIP providers and the technology itself must live up to:

- For service providers, a VoIP network must provide emergency services like 911 at all times, and have a similar uptime (99.995%) as the traditional phone network.
- To make the end-user experience of a phone call over the IP network comparable to the traditional phone call, VoIP networks must guarantee a Quality-of-Service similar to the traditional phone systems. This implies that the VoIP implementations must effectively deal with lost voice packets and voice packets arriving out-of-order, which are a common occurrence in a typical IP network.
- The VoIP network must also guarantee that any communication between the end parties in a call cannot be intercepted or modified by a malicious third party. It should be difficult for a hacker to conduct a man-in-the-middle attack between the end parties.
- The VoIP implementation should enforce user authentication and not allow any unauthorized party to make free phone calls.

Along with the aforementioned requirements, the convergence of voice and data networks only serves to exacerbate and magnify the security risks of today's prevalent cyber attacks. Successful attacks against a combined voice and data network can totally cripple the functioning of an enterprise, halt all communications required for productivity, or result in irate customers and lost revenue.

Part of the inherent problem in protecting VoIP data networks is simply keeping the infrastructure completely up-to-date with patches for the latest vulnerabilities. The trend of shrinking vulnerability-to-exploit windows presents a daunting challenge for administrators trying to patch hundreds of servers and desktops. Because of availability concerns in a VoIP network, maintenance windows for normal upgrades and patching may be few and far between.

Defense-in-depth strategies that include "virtual patching" are a necessity in defending an organization's VoIP data network.

VoIP Building Blocks

There are a variety of devices, protocols and configurations seen in typical VoIP deployments today. VoIP technology can be used to make calls between: a PC and a traditional phone, a PC and another PC, a traditional phone and another traditional phone (voice is packetized and travels over the IP network), a VoIP phone and another PC, and a traditional phone or VoIP phone.

The physical elements that are present in a typical VoIP deployment include:

- **VoIP Telephone:** The VoIP phone used by an end-user to make a telephone call. The phone is capable of converting voice into media data packets. The phone may also have advanced features like Web browsing, instant messaging and multi-media conferencing.
- **Call Server:** Software that runs on a dedicated server platform and offers the functionality of call control and call signaling. This is essentially porting the conventional functions of Private Branch Exchange (PBX) to a dedicated server.
- **Gateway:** The network device that connects the IP network and the carrier network such as ISDN or PSTN.
- **Optional Elements:** MultiPoint Control Units for conferencing, backend services for data tracking of call endpoints, authentication servers etc.

There are currently three protocols widely used in VoIP implementations – the H.323 family of protocols, the Session Initiation Protocol (SIP) and the Media Gateway Controller Protocol (MGCP). VoIP vendors are current selling solutions that can work with either of these families of protocols.

H.323 Family of Protocols

H.323 is a set of recommendations from the International Telecommunication Union (ITU) and consists of family of protocols that are used for call set-up, call termination, registration, authentication and other functions. These protocols are transported over TCP or UDP protocols. The following diagram shows the various H.323 protocols with their transport mechanisms:

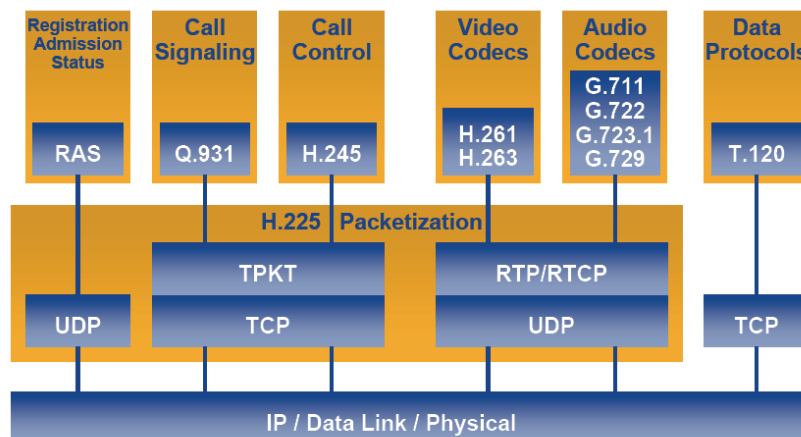


Figure 1: H.323 Protocol Familyⁱⁱ

These protocols can be further sub-divided into two classes – protocols used for call signaling (Q.931, H.225, H.245, H.235, RTCP) and the protocol that carry the compressed voice traffic (RTP). The following figure illustrates the typical set-up and voice data transfer using H.323 family of protocols.

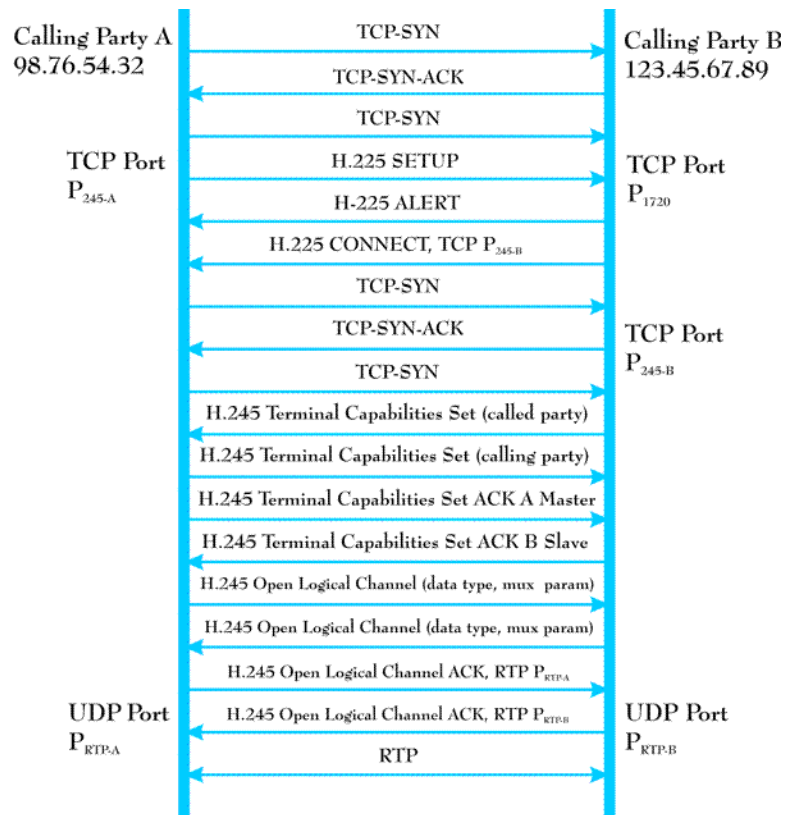


Figure 2: H.323 Call Set-Up and Voice data Transferⁱⁱⁱ

SIP

The Session Initiation Protocol (SIP) was defined by the Internet Engineering Task Force (IETF) for creating, modifying and terminating sessions between two or more participants. These sessions are not limited to VoIP calls. The SIP protocol is a text-based protocol similar to HTTP, and offers an alternative to the complex H.323 protocols. Due to its simpler nature, the protocol is becoming more popular than the H.323 family of protocols and will likely emerge as the dominant standard in coming years.

A SIP deployment typically uses a proxy server to initiate calls on behalf of the endpoint (a user or VoIP phone), and a location server to track an end point's location. These figures illustrate a typical SIP-based call:

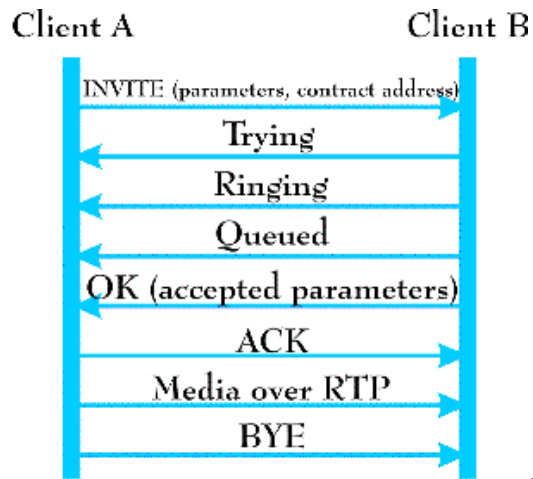


Figure 3 SIP Call Setup and Data Transfer ^{iv}

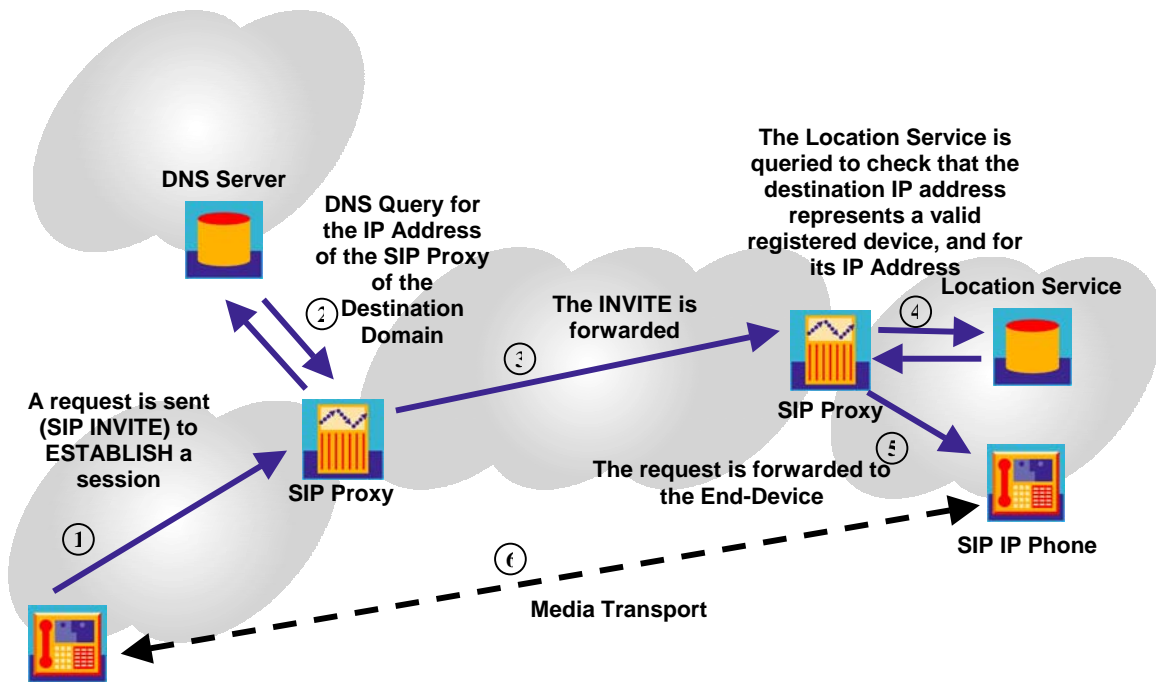


Figure 4: SIP Call in Progress

MGCP and MeGaCo/H.248

MGCP and Megaco/H.248 are control protocols designed to centrally manage Media Gateways deployed across a VoIP infrastructure. A Media Gateway executes commands sent by the centralized Media Gateway Controller (MGC) and is designed to convert data between PSTN to IP, PSTN to ATM, ATM to IP, and also IP to IP.

MGCP and Megaco/H.248 provide mechanisms to interconnect with other VoIP networks, and also facilitate large-scale deployments of VoIP. MGCP and Megaco/H.248 can be used to set up, maintain and terminate calls between multiple endpoints, while monitoring all of the events and connections associated with those endpoints from the MGC.

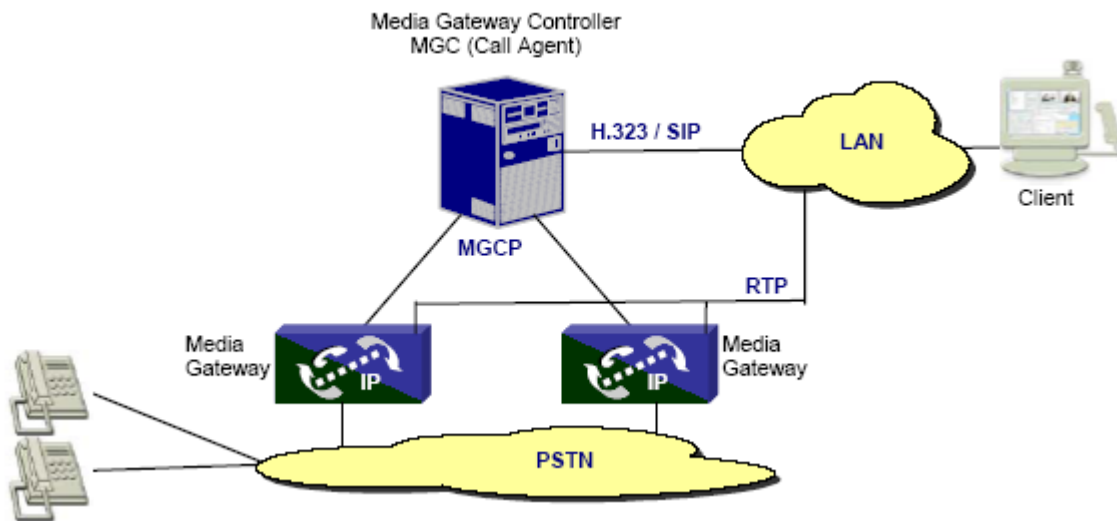


Figure 5: Media Gateway and Media Gateway Controller^v

VoIP Security Threat Scenarios

A VoIP deployment faces a variety of threats from different networking layers, as well as from different areas of trust from within the network. For instance, an attacker can try to compromise a VoIP gateway, cause a denial-of-service attack to the Call Manager, exploit a vulnerability in a vendor's SIP protocol implementation or try to hijack VoIP calls through traditional TCP hijacking, UDP spoofing, or application manipulation. The attacks against a VoIP network can be best categorized as follows:

Attacks against the underlying VoIP devices' Operating System

VoIP devices such as IP phones, Call Manager, Gateways, and Proxy servers inherit the same vulnerabilities of the operating system or firmware they run on top of. For instance, the Cisco Call Manager is typically installed on Windows 2000 and the Avaya Call Manager on Linux. There are hundreds of remotely

exploitable vulnerabilities in flavors of Windows and Linux operating systems for which there are numerous “point-and-shoot” exploits freely available for download on the Internet. No matter how secure an actual VoIP application happens to be, this becomes moot if the underlying operating system is compromised. The following are merely a few examples of historical issues with popular VoIP devices:

- The Cisco Call Manager is vulnerable to the same Windows buffer overflows that have emerged over the last few years (LSASS, Messenger, ASN.1, etc.) [2]. An attacker gaining control of a Call Manager or an IP phone may provide the necessary access to launch more sophisticated attacks against the entire VoIP network.
- Similarly, any denial of service vulnerability in the underlying Cisco IOS running on a Gateway device could potentially be exploited to disrupt the VoIP network. There is a variety of known denial of service vulnerabilities and corresponding public exploits for Cisco IOS.
- In a recent security study, an Avaya IP phone was rendered unusable by bombarding it with specific IP traffic [3].
- Alcatel, Avaya and Cisco phones are reportedly vulnerable to a DoS that can be triggered by sending fragmented UDP packets, and TCP ACK flood [5].

Configuration Weaknesses in VoIP devices

Many of the VoIP devices in their default configuration may have a variety of exposed TCP and UDP ports. The default services running on the open ports may be vulnerable to DoS, buffer overflows or weak passwords, which may result in compromising the VoIP devices.

- Many VoIP devices run Web servers for remote management purposes, which may be vulnerable to attacks ranging from information disclosure to buffer overflows. Multiple installations of the Cisco Call Manager that runs an IIS server were reportedly compromised by the Nimda and the Code Red worms [4].
- If any of the open services are not configured with a password or a weak password, an attacker may acquire an unauthorized access to that device. This is a known vulnerability against the Cisco SIP-based phones’ telnet service [6].
- The SNMP services offered by the devices may be vulnerable to reconnaissance attacks or buffer overflows. In a recent testing, valuable information was gathered from an Avaya IP phone by using SNMP queries with the “public” community name [3].
- Many VoIP devices are configured to periodically download a configuration file from a server through TFTP or other mechanisms. An attacker could potentially divert or spoof this connection and trick the device into downloading a malicious configuration file instead.

IP Infrastructure Attacks

The availability of VoIP services directly depends on the availability of the IP infrastructure it rides upon. Any DDoS attacks such as SYN floods or other traffic surge attacks that exhaust network resources (e.g. bandwidth, router connection table, etc.) could severely impact all VoIP communications. Even worms or zombie hosts scanning for other vulnerable servers could cause unintentional traffic surges and crater availability of these VoIP services.

VoIP protocols all rely on TCP and UDP as transport mediums and hence also vulnerable to any low level attacks on these protocols such as session hijacking (TCP), malicious IP Fragmentation, spoofing (UDP), TCP RST window brute forcing, or a variety of IP protocol anomalies which may cause unpredictable behavior in some VoIP services.

VoIP Protocol Implementation Vulnerabilities

Functional protocol testing (also called “fuzzing”) is a method of finding bugs and vulnerabilities by creating different types of packets for that protocol which contain data that pushes the protocol's specifications to the point of breaking them. These specially crafted anomalous packets are consequently sent to an application, operating system, or hardware device capable of processing that protocol, and the results are then monitored for any abnormal behavior (crash, resource consumption, etc.).

Functional protocol testing has already led to a wide variety of Denial of Service and Buffer Overflow vulnerability discoveries in vendor implementations of VoIP products that use H.323 and SIP. Many of these vulnerabilities have been the direct result of focused VoIP research conducted by the University of Finland's PROTOS group [7], which specializes in the security testing of protocol implementations. The PROTOS group typically makes their tools available to the public, which means any script kiddie can download and run the tools necessary to crash vulnerable implementations.

VoIP Application Level Attacks

At the application level, there are a variety of VoIP specific attacks that can be performed to disrupt or manipulate service. Some of them include:

- **Denial of Service:** By spoofing his identity, an attacker may cause a denial-of-service in SIP-based VoIP networks by sending a “CANCEL” or “BYE” message to either of the communicating parties and end the call. Since SIP is UDP based, sending a spoofed ICMP “port unreachable” message to the calling party could also result in a DoS [8].

- **Call Hijacking:** An attacker can also spoof a SIP response, indicating to the caller that the called party has moved to a rogue SIP address, and hijack the call [8].
- **Resource Exhaustion:** A potential DoS attack could starve the network of IP addresses by exhausting the IP addresses of a DHCP server in a VoIP network.
- **Eavesdropping:** An attacker with local access to the VoIP LAN may sniff the network traffic and decipher the voice conversations. A tool named VOMIT (voice over misconfigured internet telephones) can be downloaded to easily perform this attack.
- **Message Integrity:** The attacker may be able to conduct a man-in-the-middle attack and alter the original communication between two parties.
- **Toll Fraud:** An attacker can impersonate a valid user/IP phone and use the VoIP network for making free long distance calls.

The Future of VoIP Security

VoIP technology is still at the early stage of adoption, and attacks against deployments have been largely unheard of or undetected. As VoIP increases in popularity and numbers of consumers, so does the potential for harm from a cyber attack.

The 2004 CSI/FBI computer crime and security survey states that Denial-of-Service attacks are now the most expensive problem for organizations, with insider network abuse ranked third. This does not bode well for ensuring availability of VoIP networks without a proactive way to detect and block these attacks. It will become easier for attackers to infect and control a large number of zombie “bots” by continuing to exploit the vulnerabilities in the widely deployed Windows and Linux platforms. It has been reported that the wildly successful strain of Agobot worms at one time had infected hundred of thousands of Windows systems, allowing groups of hackers to launch distributed attacks. A recent DDoS attack on Akamai’s DNS infrastructure is estimated to have involved over 15,000 compromised zombie hosts worldwide [12].

Undoubtedly there are an abundance of vulnerabilities yet to be discovered in the implementations of other VoIP protocols such as H.245, H.235, H.248 through similar functional fuzzing techniques employed by the PROTOS group. It will be important to prevent these as-yet-undiscovered vulnerabilities from being exploited by enforcing selective conformance of VoIP protocols to their specifications and provide proactive zero-day protection.

We can expect to see more VoIP application-level attacks occur as attackers become savvier to the technology and gain easier access to test the VoIP infrastructure as it becomes more prevalent across residential areas. It will be important to keep track of calls, devices, users, and sessions to enforce security policy and prevent abuse of the VoIP network.

VoIP and TippingPoint

Much like firewalls in any IT infrastructure today, Intrusion Prevention technology will become a required component in any VoIP deployment. TippingPoint's UnityOne Intrusion Prevention System (IPS) offers a unique, total security and high performance solution for protecting VoIP deployments. The UnityOne IPS prevents DDoS floods, viruses, worms, buffer overflows and many other malicious attacks against the IP infrastructure and the VoIP devices. The IPS also examines the VoIP protocols at wire speed, and blocks any anomalies and application-level attacks.

TippingPoint has established the VoIP Security Research Lab as a nerve center for breakthrough VoIP security testing. TippingPoint's industry-recognized security researchers work alongside VoIP vendors and customers in analyzing weaknesses in VoIP architectures, discovering new vulnerabilities through functional protocol testing, educating and training, as well as presenting research in trade magazines, security journals and conferences. The by-product of these research efforts ensures UnityOne IPS is able to protect against the latest VoIP vulnerabilities and attack techniques.

To learn more about how TippingPoint can help prevent the onslaught of VoIP cyber threats mentioned in this paper, e-mail voip@tippingpoint.com or call 1-888-648-9663.

References

[1] Recent ASN.1 Vulnerabilities

<http://icat.nist.gov/icat.cfm?cvename=CAN-2004-0123>

<http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0818>

[2] Cisco Call Manager Windows 2000 Workstation Service Buffer Overflow

<http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml>

[3] Breaking Through IP Telephony

<http://www.nwfusion.com/reviews/2004/0524voipsecurity.html>

[4] Cleaning Nimda Virus from Cisco Call Manager

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00800941e4.shtml

[5] Miercom VoIP Security Assessment

<http://www.miercom.com/?url=products/spreports>

[6] Cisco IP Phones Compromise

http://www.sys-security.com/archive/papers/The_Trivial_Cisco_IP_Phones_Compromise.pdf

[7] Security Testing of Protocol Implementations at the University of Finland

<http://www.ee.oulu.fi/research/ouspg/protos/>

[8] Security Risk Factors in IP Telephony Based Networks

http://www.sys-security.com/archive/papers/Security_Risk_Factors_with_IP_Telephony_based_Networks.pdf

[9] Vulnerabilities in Pingtel VoIP Phone

<http://icat.nist.gov/icat.cfm?cvename=CAN-2002-0668> (Call Hijack)

<http://icat.nist.gov/icat.cfm?cvename=CAN-2002-0667> (Null Password)

[10] VocalTec DoS

<http://www.securityfocus.com/bid/10411>

[11] CSI/FBI Computer Crime Survey

<http://www.gocsi.com/>

[12] 'Zombie' PCs caused Web outage, Akamai says

<http://zdnet.com.com/2100-1105-5236403.html>

[13] RFC 3435 - Media Gateway Control Protocol (MGCP)

<http://www.ietf.org/rfc/rfc2705.txt?number=2705>

[14] Voice over IP

<http://www.utdallas.edu/~vxa024100/docs/acn/VoIPRep.pdf>

ⁱ <http://www.cconvergence.com/shared/article/showArticle.jhtml?articleId=8707174>

ⁱⁱ http://www.switch.ch/vconf/ws2003/h323_basics_handout.pdf

ⁱⁱⁱ http://www.its.bldrdoc.gov/tpr/2001/its_p/voice_ip/voice_ip.html

^{iv} http://www.its.bldrdoc.gov/tpr/2001/its_p/voice_ip/voice_ip.html

^v http://csrc.nist.gov/publications/drafts/NIST_SP800-58-040502.pdf