Government of Canada | Gouvernement du Canada

Office of Critical Infrastructure Protection and Emergency Preparedness

Bureau de la protection des infrastructures essentielles et de la protection civile

INFORMATION NOTE

Number: IN03-001
Date: 13 June 2003

SECURING VoIP

Purpose
This paper will focus on the emerging trend towards Voice over Internet Protocol (VoIP) telephony services and related security concerns.

Audience
This study is primarily intended for Canadian critical infrastructure owners and operators who make use of, or are considering the use of, VoIP technology to enhance their mission critical operations.

This paper may also aid small- and medium-sized private industries who are seeking to derive the benefits of VoIP technology, but are unaware of the potential security implications.

EXECUTIVE SUMMARY

- Voice over Internet Protocol (VoIP) telephony is an emerging technology, forecasted to become a ubiquitous technological tool for business.
- Properly securing emerging technologies is often initially overlooked in favour of efficiency and cost-effectiveness.
- VoIP technology is becoming increasingly used in the mission critical systems of Canadian critical infrastructure owners and operators.
- Multiple points of entry make VoIP networks susceptible to hackers.
- VoIP networks can be susceptible to denial of service attacks.
- VoIP networks can be “spoofed” in a variety of ways.
- Basic security measures and procedures provide a worthwhile baseline to securing networks; however, VoIP does present some unique challenges.

INTRODUCTION

Voice over Internet Protocol (VoIP) telephony or IP telephony is the transportation of voice traffic over a packet-switched data network via Internet protocol. VoIP networks treat voice as another form of data but use sophisticated voice-compression algorithms to ensure optimal bandwidth utilization.[1] VoIP promises lower operation and management costs than traditional circuit-switched telephone networks because it allows businesses to route compressed voice data over their existing data networks. This synergy is possible because the Internet is a relatively scalable interconnection between networks that use IP. VoIP eliminates the need for the purchase of new Private Branch Exchange (PBX) equipment and lowers the number of personnel required to monitor and maintain an organization's networks because only one network needs to be supported. In addition, long distance calls can be made over existing data network (Internet) connections instead of traditional telecommunications carriers. According to the market research firm Synergy Research Group, the worldwide market for VoIP, including IP telephones, experienced an annual growth of 21% for fiscal year 2001–2002.[2] Longer-range forecasts predict "worldwide revenue from (VoIP) will grow from US$74 million in 2000 to nearly US$40 billion in 2006."[3]

As with any emerging technology, those who employ VoIP technology for their mission critical operations should be aware of the potential security issues it presents.

This paper highlights a number of potential security vulnerabilities within VoIP systems. Many of the vulnerabilities appear to be related to the fact that users have, until recently, been more concerned with quality of reception and cost-efficiency than with synchronizing these aspects of VoIP technology with proper security measures and protocols. Potential concerns associated with VoIP technology include the usual security issues associated with Internet technologies and their ability to protect personal and corporate information, as well as some new concerns caused by creating dependencies between voice and data networks.

VOIP OVERVIEW

A generalized VoIP system (see Figure 1) consists of the following key elements: the participants to a call (the caller and the callee in the case of a two-person call); terminal devices (e.g. IP telephones, PCs) which are used to initiate and receive calls; servers which contain call information that may be needed during a phone call; and, communications routing devices. These routing devices can be either based on wires, or they can be wireless.[4] These elements within a VoIP network all present potential avenues for exploitation.

---

[1] Vijayan, Jaikumar. "VoIP: Don't Overlook Security." www.computerworld.com, 7 October 2002. http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html

[2] Vijayan, Jaikumar. "VoIP Security on the Back Burner." www.computerworld.com, 7 October 2002. http://www.computerworld.com/securitytopics/security/story/0,10801,74778,00.html

[3] Delaney, John and Hall, Peter. "Next Generation Services: Impacts on the Industry and Markets." June 2000. http://www.tdap.co.uk/uk/archive/internet/int(ovum_0006).html

[4] Marjalaakso, Mika. "Security Requirements and Constraints of VoIP." http://www.hut.fi/~mmarjala/voip

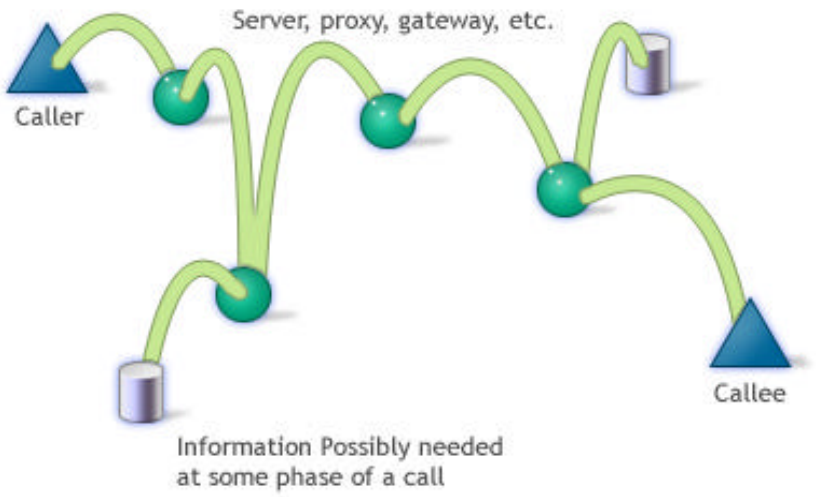
When a call is made using VoIP, the call participant's voice traffic is digitized and recorded as data. The voice data are then broken into packets that are sent over a local IP network or the Internet, and reassembled at the destination. Data to voice network gateways can be used to convert between VoIP and traditional voice networks ensuring compatibility with non-VoIP users.

Several additional protocols are used to handle the call initialization and other VoIP features:

- Session Initiation Protocol (SIP) – Used to create, modify, and terminate a session (i.e. a VoIP call). SIP handles the "phone numbers" for VoIP users.
- H.323 – A suite of protocols used for delivering multimedia conferencing applications that can be used to create VoIP calls.
- Megaco/H.248. – A suite of controlling protocols between the Media Gateway and the Media Gateway used for VoIP call control.

The SIP protocol is the most commonly used protocol for VoIP.

Figure 1 – Generalized VoIP System



SECURITY CONCERNS

VoIP inherits all of the generally accepted security concerns of traditional IP networks and the Internet. However, VoIP protocols allow new avenues of exploitation for known attacks (see OCIPEP Advisory *AV03-010*, "Numerous Vulnerabilities in the Session Initiation Protocol," released 21 February 2003) and provide access between voice and data networks where none previously existed.

Data Theft

VoIP can be exploited for the theft of information and data. Because the data packets are carried within network servers, they are inherently susceptible to hacking attempts. According to an August 2001 report released by the U.S.-based computer security organization, the SANS Institute, "Data sniffing tools are readily available and it will not be long before these tools are enhanced to become aware of the new VoIP protocols. Because VoIP traffic travels over a data network that is used by all of the regular users of the local area network (LAN), any or all of the conversations traversing the network could theoretically be compromised by anyone with a regular connection on the network. VoIP packets could be identified and stored for reassembly to be played back at a later time."[5]

VoIP gateway vulnerabilities

VoIP gateway technologies are also a potential vulnerability. When VoIP is used externally, gateway technologies convert data packets from the IP network into voice before sending them over a public-switched telephone network. When VoIP is used internally, the gateways basically route packetized voice data between the source and the destination. Such gateways can be hacked into by malicious attackers in order to make free telephone calls.[6]

Denial of Service attacks

Denial of service (DoS) poses a threat to any networked system. Properly configured security software, as well as redundant systems, will successfully mitigate against DoS attacks. These measures will secure the VoIP portion of the network as well.[7]

On 25 January 2003, as a result of the SQL Server 2000 worm (dubbed "Slammer") a 9-1-1 call centre outside Seattle, Washington, that services 14 fire departments, two police stations and a community of 164,000 people, was taken offline. Emergency responders were forced to handle requests manually. The 9-1-1 call centre was using VoIP for its phone system. The Slammer worm overloaded the network bandwidth causing a DoS incident. (For more information on the Slammer worm see the OCIPEP Incident Analysis *IA03-001*, released 14 March 2003)

IP Spoofing

An IP spoofing attack occurs when an attacker inside or outside a network impersonates the conversations of a trusted computer. This type of attack occurs when a hacker is able to trick a remote user into believing that they are talking to a trusted system when, in fact, they are really talking to the attacker. VoIP is subject to the same sort of attack by spoofing the caller ID and "phone number" information. Caller ID spoofing can take the form of placing a rogue IP phone in the network which then assumes the identity of a valid IP phone by modifying the "phone number" information stored in databases or through changing the routing information for the VoIP packets.

---

[5] Weiss, Eric. "Security Concerns with VoIP." www.sans.org, 20 August 2001. http://www.sans.org/rr/voip/sec_concerns.php

[6] Vijayan, Jaikumar. "VoIP: Don't Overlook Security."

[7] Taylor, Steven. "VoIP, Common Sense and Security." 15 July 2002. www.nwfusion.com http://www.nwfusion.com/columnists/2002/0715taylor.html

The personal privacy and integrity of information relayed over VoIP is effectively compromised when the network is vulnerable to IP spoofing.

PRIVACY CONCERNS

Privacy and security have always been a central concern with regards to emerging telecommunications technologies. Several current examples serve to illustrate this point. For instance, wiretapping has long been used by law enforcement, intelligence communities, as well as criminal elements in order to access information being carried across traditional telephone lines. In addition, recent wireless developments have led to an increase in "war driving." War driving entails persons patrolling streets with a laptop, wireless network adapter card and antenna, scanning for nearby networks in order to steal bandwidth, obtain sensitive information and gain unauthorized access to networks.

Privacy and security of information are serious concerns when using VoIP networks as well. Because voice travels in packets over the data network, hackers can use data-sniffing and other hacking tools to identify, modify, store and play back voice traffic traversing the network. Hacking into a VoIP data stream provides access to more calls than with traditional telephone tapping. As a result, a hacker has a much higher probability of getting "intelligent" or sensitive information by hacking into a VoIP data stream than by monitoring traditional phone systems.[8]

VoIP allows new levels of call logging and information capture. One of the features most sought after by managers employing VoIP is the technology's ability to log and track user information. This tracking can dramatically enhance an organization's ability to provide automated billing information to its customers. However, it also provides hackers with additional motive to attempt to breach the network to access that information.[9] This problem is exacerbated by the fact that the level of logging possible with VoIP goes beyond what is normally performed on traditional voice networks. Information relayed on a VoIP call, and even the entire call itself, can be easily recorded just like any other network data.

OCIPEP reminds CI owners and operators that an information security policy is an integral part of any critical infrastructure protection (CIP) strategy. Organizations should be very careful how they implement VoIP logging, and particularly what information is recorded. OCIPEP recommends that organizations consult with their legal counsel to draft policies and procedures that balance security, privacy, and legal requirements.

BEST PRACTICES FOR VOIP SECURITY

Although VoIP is an emerging technology, securing it requires adopting the same defensive posture that should be employed for all information technologies. The best practices currently being used to secure computers and network servers and landline

[8] "Internet Phone Calls Stymie FBI." www.wired,com, 4 April 2003. http://www.wired.com/news/privacy/0,1848,58350,00.html
[9] Ibid.

and wireless communications networks are generally transferable when adopting VoIP into the mission critical operations of critical infrastructure owners and operators. On 1 October 2001, OCIPEP released a full listing of computer and network security best practices entitled "Computer and Network Security Preparedness." This document included the standard best practices for regular Internet security, many of which also apply to VoIP systems. Such practices include, but are not limited to:

- Ensuring all networked systems are patched, and virus scanners are up to date. Many vendors maintain mailing lists to notify their customers of any product updates and fixes. Subscribing your administrators to these lists ensures prompt notification of patches which is crucial to timely response.

- Securing off-site backups and a developing disaster recovery plans. Well-maintained backups ensure business continuity in the event of a major equipment failure, natural disaster (fire, flood, earthquake, etc.) or cyber-related incident. Remember that backup media should be controlled with the same level of security that would be afforded the data that the media contains.

- Exercising diligence in analysing logs from intrusion detection systems, firewalls, routers, servers and other network devices. Extra care should be taken to investigate unusual or suspicious network activity.

- Implementing an appropriate layered security posture where the failure of any one security device can be mitigated. For example, blocking of specific types of file attachments in e-mails can prevent virus infections and support anti-virus software at the network gateway and desktops.

- Implementing egress and ingress filtering on all border routers. Egress and ingress filtering help stop IP address spoofing that is extensively utilised in denial of service attacks.

- Having a good working out-of-band communications procedure with your Internet Service Provider (ISP). A solid relationship with your ISP can be crucial in dealing with incidents such as Denial of Service attempts and other network based attacks.

- Reporting all suspicious activity on Government of Canada computer systems to OCIPEP. Mutual co-operation and communication are keys to identifying incidents which affect the government as a whole.

In addition to these general computer security precepts, VoIP does present some unique security considerations. In order to adequately protect VoIP from hackers, DoS attacks and IP spoofing, some additional security measures should be implemented.

1. **Avoid shared media devices.** Using a shared media device, such as hubs on the VoIP networks, could allow a potential hacker to have access to all conversations traversing the network.

2. **Encryption.** Currently, the driving force for vendors of VoIP equipment is quality of service. If, however, several instances of eavesdropping on confidential conversations occurred, users would lose confidence in the system. Encryption is an effective way to

achieve data security. In VoIP, end-to-end encryption, which requires a great deal of processing power, is not the only option. Encryption could also be done only at the link-level. Normally, gateway devices are designed to handle heavier processing loads and therefore encryption at this level may be more feasible than end-to-end encryption. As well, encryption could be limited to specific fields within the VoIP packets that contain sensitive information.

3. **Use IPSec protocols.** To properly secure VoIP networks, use of the IPSec protocol between the VoIP network elements should be considered. IPSec provides security functions, authentication and encryption, at the IP level. IPSec can provide a secure transport of control protocol messages between network elements such as Media Gateway Controller and Media Gateways. While encryption measures help prevent eavesdropping, use of IPSec measures will deter hackers from sniffing, spoofing, and taking control of the VoIP network.[10]

4. **Lock down VoIP servers.** VoIP systems have powerful management features that can tag logged calls in many ways to help in future retrieval. The added capabilities of storing user call data and reporting on this data easily requires an increased responsibility to protect this data. One solution is to place the VoIP servers on a separate segment protected by a VoIP-aware firewall.

5. **Redundancy.** It is vital to ensure that a back-up phone service system exists to ensure service delivery in the event of major network problems with VoIP. In addition, it is imperative that scheduled network downtimes are considered when drafting both business, and business continuity, plans.

CONCLUSION

VoIP telephony is becoming a widely-used communications tool in both the private and public sectors. The increased use of VoIP is predicated on the perceived benefits: efficiency, cost-effectiveness, and the ability to upgrade to enhanced telecommunications services such as unified communications.[11] However, as with many emerging technologies, security issues are often raised after the technology reaches widespread usage. Canadian critical infrastructure owners and operators should be made aware of the potential security implications related to VoIP. While VoIP presents some unique security challenges, network administrators who apply a combination of baseline network security procedures and the VoIP best practices included in this paper will ensure secure VoIP functionality.

NOTE TO READERS

OCIPEP's role is to provide national leadership on critical infrastructure protection and effective emergency management. To fulfill this role, OCIPEP collects information related to cyber and physical threats to, and incidents involving, Canadian critical

[10] "The IPsec protocols" http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/ipsec.html
[11] Vijayan. "VoIP: Don't Overlook Security."

infrastructure (CI). This information allows OCIPEP to monitor and analyse threats to our CI and to issue alerts advisories and other information products to our partners. To report **CI threats or incidents** to OCIPEP, please contact our operations coordination centre at (613) 991-7000 or at opscen@ocipep-bpiepc.gc.ca

Unauthorized use of computer systems and mischief in relation to data are serious Criminal Code offences in Canada. Upon conviction of an indictable offence, an individual is liable to imprisonment for a term not to exceed ten years. Any **suspected criminal activity** should be reported to local law enforcement organizations. The RCMP National Operations Centre (NOC) provides a 24/7 service to receive such reports or to redirect callers to local law enforcement organizations. The NOC can be reached at (613) 993-4460.

National security concerns should be reported to the Canadian Security Intelligence Service (CSIS).

For general information on OCIPEP, please contact our Communications division at:

Phone: (613) 991-7066 or 1-800-830-3118
Fax: (613) 998-9589
Email: communications@ocipep-bpiepc.gc.ca
Web Site: www.ocipep-bpiepc.gc.ca

Notice to readers

OCIPEP publications are based on information ob tained from a variety of sources. The organization makes every reasonable effort to ensure the accuracy, reliability, completeness and validity of the contents in its publications. However, it cannot guarantee the veracity of the information nor can it assume responsibility or liability for any consequences related to that information. It is recommended that OCIPEP publications be carefully considered within a proper context and in conjunction with information available from other sources, as appropriate.

BIBLIOGRAPHY

Carr, Kathleen and Duffy, Daintry. "The Pitfalls of VoIP." www.csoonline.com. http://www.csoonline.com/read/120902/briefing_voip.html

Delaney, John and Hall, Peter. "Next Generation Services: Impacts on the Industry and Markets." June 2000. http://www.tdap.co.uk/uk/archive/internet/int(ovum_0006).html

Hamblen, Matt. "SIP vulnerable to hacking, testing shows." www.computerworld.com, 26 February 2003. http://www.computerworld.com/printthis/2003/0,4814,78831,00.html

Hochmuth, Phil. "Costs, security vex VoIP users." www.nwfusion.com, 24 February 2003. http://www.nwfusion.com/news/2003/0224voicecon.html

"Internet Phone Calls Stymie FBI." www.wired,com, 4 April 2003.

http://www.wired.com/news/privacy/0,1848,58350,00.html

Marjalaakso, Mika. "Security Requirements of VoIP."
http://www.hut.fi/~mmarjala/voip

OCIPEP Advisory AV03-010: Numerous Vulnerabilities in the Session Initiation Protocol. 21 February 2003. http://www.ocipep.gc.ca/opsprods/advisories/AV03-010_e.asp

OCIPEP Incident Analysis IA03-001: Microsoft SQL Server 2000 "Slammer" Worm – Impact Paper. 14 March 2003.
http://www.ocipep.gc.ca/opsprods/other/IA03-001_e.asp

OCIPEP Information Note IN01-005: Computer and Network Security Preparedness. 1 October 2001.
http://www.ocipep.gc.ca/opsprods/info_notes/IN01_005_e.asp

Rash, Wayne. "Where computers and telephony meet." www.computerworld.com, 20 January 2003.
http://www.computerworld.com/printthis/2003/0,4814,77561,00.html

Stringfellow, Brian. "Secure Voice Over IP." www.sans.org, 15 August 2001.
http://www.sans.org/rr/voip/sec_voice.php

Taylor, Steven. "VoIP, Common Sense and Security." 15 July 2002.
www.nwfusion.com
http://www.nwfusion.com/columnists/2002/0715taylor.html

"The IPsec protocols" http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/ipsec.html

Weiss, Eric. "Security Concerns with VoIP." www.sans.org, 20 August 2001.
http://www.sans.org/rr/voip/sec_concerns.php

"VoIP under attack." www.asia.cnet.com, 22 December 2002.
http://www.asia.cnet.com/itmanager/specialreports/0,39006603,39101916,00.htm

Vijayan, Jaikumar. "VoIP: Don't Overlook Security." www.computerworld.com, 7 October 2002.
http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html

Vijayan, Jaikumar. "VoIP Security on the Back Burner." www.computerworld.com, 7 October 2002.
http://www.computerworld.com/securitytopics/security/story/0,10801,74778,00.html