CYBER SECURITY
INDUSTRY ALLIANCE

Cyber Security for IP Telephony

FINDINGS AND RECOMMENDATIONS BY THE
CYBER SECURITY INDUSTRY ALLIANCE

MAY 2005

www.csialliance.org

Issues for Telecommunications Reform in 2005

How Vulnerabilities in Voice-over-IP May Affect National Security / Emergency Preparedness Programs and the IT-Based Economy

As Congress considers updates to national telecommunications policy, it is useful to review cyber security implications of a popular trend called IP telephony. The landmark Telecommunications Act of 1996 passed when nascent technology called "voice-over-Internet protocol," or VoIP, was a back-room experiment. The purpose of VoIP is to allow phone calls to move in packets over the public Internet rather than traditional private telephony circuits. VoIP is still an emerging technology, but it is swiftly being adopted by organizations and consumers. The VoIP acronym is synonymous with IP telephony.

Experts believe VoIP will transform the telecommunications industry. Commercial use is rising because IP telephony is typically more economical than traditional telephone service. Competition is forcing carriers to consider VoIP because cable companies and other providers are luring voice customers with this cheaper Internet-based service. IP telephony usage will soar when consumers adopt WiFi cell phones, and promises to become ubiquitous when wide-area wireless technologies, such as WiMax are commonplace.

Security Holes in VoIP

- **Ease knocking out IP telephony service**
- **Threaten NS/EP services**
- **May harm critical infrastructure and IT-dependent economy**

But there is an Achilles heel to IP telephony: the issue of cyber security. IP telephony is inherently insecure, and since its operations depend on the Internet, all cyber vulnerabilities on the Internet also threaten to knock out telephone systems that use VoIP. As more Americans come to rely on IP telephony, there are serious implications for critical government services operated by national security and emergence preparedness (NS/EP) providers. Repercussions also affect information technology underpinning critical infrastructure and the economy.

The Cyber Security Industry Alliance (CSIA) presents this briefing for public consideration as Congress contemplates revision of the '96 Telecommunications Act. The briefing surveys how cyber security affects IP telephony, NS/EP programs, and information technology used for critical infrastructure and business. The briefing concludes with recommendations for new policy.

CYBER SECURITY IS A BIG PROBLEM FOR VOIP

IP telephony presents big cyber security challenges because it moves voice communications onto the Internet – the biggest party line in the world. The exposure demands strong security for IP telephony and is subject to the same Internet vulnerability exploits we read about in the papers. A typical example is a denial of service attack, which congests a network with illegitimate traffic. This prevents network access for email, web services, and other business processes, including voice calls with IP telephony. Network congestion easily degrades the quality of voice calls over the Internet.

VoIP multiplies the impact of Internet-borne attacks because the architecture for an IP telephony system offers many points of vulnerability. Potential targets include IP phones, broadband modems, gateways for signaling and media, soft switches, and servers for IP telephony and security applications. Ensuring cyber security is a challenging process. If an organization's cyber security policy is inadequate, adding IP telephony is like a skipper piercing holes in an already-leaky boat.

A more insidious issue is cyber-savvy organizations being lulled into a false sense of security when adding IP telephony. Standard cyber security equipment and applications often do not protect IP telephony because VoIP security demands an extra measure of processing capability. Those demands can overwhelm standard security devices and delay transmission of packets, which can trigger poor quality of Internet-based voice service. Adding an extra layer of security infrastructure for VoIP can help, but performance is not the only issue.

Consider the following points:

- Caller ID services, including those used by first-responder organizations, have been demonstrated to be easily bypassed or subverted by IP Telephony.
- IP Telephony hubs, the equivalent of Key Systems or PBX's, can be hacked, and information stored on there (to/from and routing information for billing purposes) can be exposed.
- Automated tools can easily drop SPIT, the IP Telephony version of spam, to any and all voice mail boxes in a given range of the provider, address space or area codes.
- Voice mail boxes can be broken into by Internet users. Voice mail messages, essentially each a computer file, can be hijacked, utilized or played back to an unlimited audience.
- Conversations over IP, many in the same file format, can be recorded, duplicated and quickly distributed to anyone beyond the original audience.
- Wireless devices will further complicate the issue of IP Telephony security, much in the same way that old, analog cell phones could have been "tapped" by anyone with a radio scanner.
- Finally, the FCC regulates IP Telephony differently than traditional phone services.

Some cyber security applications are unaware of specific requirements for VoIP and inadvertently expose new weaknesses in the infrastructure. Older firewalls are one example. Their purpose is to block packets bearing inappropriate traffic by regulating passage through digital communications ports. VoIP requires opening many communications ports on the firewall to place and route phone calls – more than a dozen for each IP telephony session. Older firewalls may lack dynamic interaction with VoIP so they simply leave a range of ports continually open for call activity. Ironically, in these cases, firewalls multiply entry points vulnerable to attacks by hackers instead of closing unused ports to protect the IP telephony application.

The radio spectrum is divided into many parts for use by the military, public safety and consumers. The current wireless network is divided into licensed and unlicensed halves. Licensed services include cellular phone service, while wireless fidelity, or WiFi, is an example of unlicensed radio spectrum. New mobile devices are being introduced that are capable of communicating on both halves of the consumer radio spectrum. Phone calls will automatically be switched from cellular to WiFi networks using VoIP. The associated security issues with these new mobile devices include roaming and handing-off of identities needs to be addressed.

VoIP challenges traditional security solutions because of quality of service issues such as latency, jitter and packet loss. Firewalls can delay or block call set ups and encryption can cause unacceptable latency and jitter. Traditional phone companies have built in quality of service features that businesses and consumers rely on because they are mandated by regulatory authorities. Since VoIP is lightly regulated as an information service, it does not have the same reliability and outage reporting requirements.

There are unresolved issues to securing VoIP because it is an emerging technology with competing standards still under development. The two big contenders are protocols called SIP and H.323. SIP is favored by many academics but H.323 is more widely deployed. Cyber security for VoIP must support both protocols to ensure a stable and robust network. There is also debate about whether to use end-to-end virtual private networks (VPNs) or firewall-based VPNs to secure call traffic. These, and other technical issues associated with cyber security for VoIP are discussed in a recent comprehensive analysis by the National Institute of Standards and Technology.[1]

Finally, IP telephony brings several privacy and legal issues pertaining to storage of call detail records (CDR). VoIP systems may produce different types and higher volumes of CDR data than conventional phone systems, so organizations must also determine retention requirements.

[1] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology," Special Publication 800-58 (Jan. 2005). View online at http:/csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf.

SOLUTIONS FOR CYBER SECURITY

Experts recommend a “multi-layer” policy for VoIP cyber security, just as they do for the rest of the IP network. Strong cyber security requires use of a variety of solutions and processes for particular security issues such as:

Anti-Virus Software automatically checks new files entering a PC for infection.

Asset Management Used to match inventory against scans for known vulnerabilities; helps pinpoint and fix specific security holes.

Authentication A critical step to ensure appropriate users access reliable data using two factor authentication and digital certificates.

Education Teaches users why and how to practice security-wise behavior.

Intrusion Detection / Prevention Technologies that monitor content of network traffic for infections and block traffic carrying infected files or programs.

Encryption Transforms data into password (key)-protected packets that prevent reading by unauthorized users.

Firewall Blocks unauthorized traffic from entering PCs and servers from the Internet.

Patch Fixes vulnerability in software by replacing a portion of faulty code.

Policy Management Enforces security rules and regulations of IT systems.

Vulnerability Management Remediate vulnerabilities through scanning devices that identify and patch vulnerabilities, as well mitigate misconfigurations, unnecessary services, unsecured accounts, and malware.

CRITICAL GOVERNMENT SERVICES MAY SUFFER

Exploitation of vulnerabilities in IP telephony is more than a mere nuisance, such as when a virus knocks a PC out of use for a few hours. Voice communications are the key enabler of critical government services operated by national security and emergence preparedness providers. If VoIP service is knocked out by a cyber attack, people lose their lifeline to critical NS/EP services. There are other urgent operational issues related to VoIP and NS/EP, summarized in the following program profiles.

NS/EP Program	Urgent Issues
GETS – Government Emergency Telecommunications Service. The program provides emergency phone access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). Use is for emergency or crisis situations when the PSTN is congested, and the probability of completing a call over normal or other	***IP telephony users cannot currently access GETS. Engineering efforts are in process and a solution is expected sometime in 2006.***

alternate telecommunications means is significantly decreased. GETS is accessed via a universal access number using common telephone equipment, and authorized with a Personal Identification Number. Directed by the White House and implemented by the National Communications System (NCS) under the Information Analysis and Infrastructure Protection Division, Department of Homeland Security. http://gets.ncs.gov	
911 Services. The official national emergency number in the United States and Canada. Dialing 911 quickly connects callers with a Public Safety Answering Point dispatcher trained to route calls to local emergency medical, fire and law enforcement agencies. Directed by the White House and implemented by the Federal Communications Commission. www.fcc.gov/911	***Some IP telephony services do not work during power outages. Some do not allow seamless connection with 911 or identify the location of VoIP 911 callers and some 911 systems are using VoIP solutions as well.***
CALEA – Communications Assistance for Law Enforcement Act. This program preserves the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology. CALEA is technology neutral so it applies to packet-mode communications such as IP telephony. Program directed by the White House and implemented by the Federal Bureau of Investigation. www.askcalea.net	***Electronic wiretaps including IP telephony constituted just 4% of all intercepts during 2003. FBI is concerned about falling behind the continual and rapid changes in technology.***

VoIP Exposes Vulnerabilities to Critical Infrastructure and the IT-Based Economy

Direct fallout from attacks on a VoIP service can include eavesdropping on voice conversations and interference with audio streams. Attackers could disconnect or reroute calls – or answer someone else’s phone. Opportunities for illegal mischief are endless, such as phishing schemes by criminals leaving voicemails masquerading as a bank, credit card company, merchant, or government agency. And there will be other intrusions without adequate protection for VoIP. Email “spam” currently plagues millions of people, and a growing number experience “spim” (spam over instant messaging). The next bother will be “spit” (spam over IP telephony), telemarketing voice mail messages automatically blanketed to millions of users that could potentially throttle operations of IP telephony.

VoIP vulnerabilities also act as entry points for attacks on the rest of the network, including non-VoIP applications, systems and infrastructure. Potential fallout as it impacts business continuity includes:

- Crippling impacts on the operations of critical infrastructures which are dependent on IT, including banking and finance; chemical; defense industrial base; electric power generation and distribution, and oil and gas production and storage; emergency services, including law enforcement; information technology; postal and shipping; public health services; telecommunications; transportation systems; water supply; agriculture, meat, poultry and egg products.
- Potential for weakening the national response capability as part of a blended cyber and physical attack.
- Loss of revenue for operations stoppages such as call centers, order processing, and shipping.
- Theft, erasure, or alteration of business and personal information.
- Violations of privacy and confidentiality regulations, possibly resulting in civil and/or criminal penalties depending on the particular violations.

Cyber security for VoIP is essential for protection of the entire information technology ecosphere.

ISSUES TO BE CONSIDERED

In general, CSIA recommends Congress consider the impending cyber security issues facing next generation communication and information applications such as VoIP. Basic research and development can contribute new ideas on how to improve security and reliability of VoIP. Given the rapid advancements being made in VoIP and growing dependence on information technology, government regulatory roles and responsibilities need to be defined for agencies such as the Department of Homeland Security, the Federal Communications Commission and Department of Defense.

To facilitate constructive discussion on new policy for VoIP security, the Cyber Security Industry Alliance invites appropriate scientists, technologists, policy makers, and domain experts to convene and discuss the issues outlined in this white paper and elsewhere. In conjunction with the University of North Texas, University of Tulsa and George Mason University, CSIA will co-host the 2nd Workshop on Securing Voice over IP: "Harmonizing Technology and Policy" on June 1-2, 2005 in Washington, D.C. Current workshop information can be found at: http://pfidc.com/voip/

ABOUT THE CYBER SECURITY INDUSTRY ALLIANCE

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc., Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., iPass, Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Symantec Corporation, and TechGuard Security.

Cyber Security Industry Alliance
2020 North 14th Street
Suite 750
Arlington, VA 22201
703-894-2742
www.csialliance.org