

# **VOIP SECURITY REVIEW**

---

## *INSURANCE*

**Internet-based telephony: an anticipated producer of major losses in cyberspace, a new frontier for Insurance carriers.**

**Emerson Development LLC**

**By Harry E. Emerson, III**

[www.IronPipe.net](http://www.IronPipe.net)

May, 2010

**With**

Paul Henry  
Kevin Nixon  
Glenn Tippy  
R. Scott Wolff

**CONTACT INFORMATION:** For general information and inquiries regarding this report, please contact Jacqueline Herships, Jacqueline Herships & Associates Communications, at 973-763-7555, or email [Jacqueline@jacquelineherships.com](mailto:Jacqueline@jacquelineherships.com).

---

**I**nternet phone service, commonly called VoIP (for Voice over Internet Protocol), is a low-cost, discounted service that is rapidly being adopted in the U.S. and throughout the world.

In this process, organizations are also unwittingly shifting from our reliable and secure traditional telephone network to an Internet environment of extreme risk. As it becomes more prevalent, we anticipate that VoIP will be increasingly vulnerable to hostile acts.

The VoIP industry is attempting to manage the risks generated by VoIP; however, their approach is inadequate and short-sighted because it does not solve the fundamental structural vulnerabilities of the Internet. For this reason, as it develops market share, Internet phone service will suffer the same critical cyber-security risks as every other Internet system, and therefore will become a likely attack vector for hackers, cyber-criminals, foreign governments, and terrorists. As demonstration, the VoIP Industry Security Alliance publishes a listing of almost 100 downloadable software tools for hacking and spying on VoIP calls and systems (see Appendix B, and [voipsa.org](http://voipsa.org)).

This is significant to the Insurance Industry because a growing range of insured user sectors depend upon VoIP online telephone service. These sectors include, but are not limited to governments, the military, manufacturers, the banking industry, the legal profession, hospitals, pharmaceutical companies and medical practices, the not-for-profit sector, and private individuals in greater and greater numbers.

This review has been compiled to direct the attention of members of the insurance industry to VoIP vulnerabilities which we anticipate will adversely affect their clients, to provide examples of such vulnerabilities which have already been exploited and which continue to be exploited with rising frequency, and finally to suggest a singular solution which marries the existing secure telephony infrastructure now in place worldwide, with the fabulous but highly vulnerable broadband capabilities of the Internet.

---



“We anticipate that insurance carriers will increasingly price for Internet / VoIP telephone exposure.

“Cyber insurance products will be created for users of VoIP, as well as for VoIP providers and vendors.

“The effects upon our economy will be profound.”

**Glenn Tippy**, President and Managing Partner of [Gerrity, Baker, Williams Inc.](http://Gerrity, Baker, Williams Inc.), and board member of the Professional Insurance Agents of New Jersey Inc. [www.gbwinsurance.com](http://www.gbwinsurance.com)



“As the economy worsens, more and more companies are adopting VoIP, but there’s no allowance for security there....Dropping VoIP in on top of network infrastructure is suicide today.”

**Paul Henry**, Lead Forensic Analyst, Forensics & Recovery LLC  
[www.forensicsandrecovery.com](http://www.forensicsandrecovery.com)



“The FBI considers the cyber threat against our nation to be one of the greatest concerns of the 21st century...Protecting the United States against cyber crimes is one of the FBI’s highest priorities and, in fact, is the FBI's highest criminal priority.”

**Director Robert Mueller**, Press Release: April 23, 2010  
[www.fbi.gov/pressrel/pressrel10/snow042310.htm](http://www.fbi.gov/pressrel/pressrel10/snow042310.htm)

**Comments from Intellectual Property/Litigation Attorney Ronald Abramson on Potential Legal Ramifications**

*From a legal and liability standpoint, we have taken telecommunications security for granted. But, as the potential abuses outlined herein begin to take place, telecommunications weaknesses could open up potential lawsuits against VoIP hardware and software vendors, against VoIP carriers, against carriers that interconnect to VoIP carriers, against corporations that chose VoIP, against compromised law enforcement providers, against local e-commerce providers who recommended VoIP, and so on.*

Ronald Abramson, Esq.  
Partner  
Hughes Hubbard & Reed LLP



“Because of the Internet’s inherent architecture, every person and every system has direct access to one another; therefore, we all implicitly have a trusted relationship with every hacker and terrorist in the world. It is vitally important to understand that these exposures and risks are due to the fundamental architecture of the Internet itself, which cannot be fixed.”

“We are recognizing that VoIP shares all the risks of the Internet, exposing all the features of voice communications to hacking and exploitation with the potential for disastrous results.

“And when hackers, terrorists, and foreign governments succeed in taking down our voice communications at a perilous time, when they eavesdrop and spy on critical communications, and steal identities, corporate secrets, Intellectual Property, and government and military secrets, then we will see a parade of VoIP industry executives and the CEO’s of organizations that purchased VoIP testifying before Congress to explain why they thought the dollars saved in the short term were worth taking such a hazardous and potentially catastrophic risk.”

**Harry Emerson, III** founder of [Emerson Development](#), creator of IronPipe™, an armored technology plan for enhancing the worldwide public telephone network to enable multimedia capabilities of the Internet while protecting information and eliminating the risks of VoIP.

[www.IronPipe.net](http://www.IronPipe.net)



Find 100 software tools for  
hacking VoIP in Appendix B

**Table of Contents**

FOREWORD:..... 1

GLENN TIPPY, INSURANCE EXPERT, ON INSURANCE RISKS ..... 2

PAUL HENRY, SECURITY EXPERT, ON SECURITY RISKS ..... 2

FBI DIRECTOR, ROBERT MUELLER, ON NATIONAL CYBERSECURITY RISKS ..... 2

ATTORNEY RONALD ABRAMSON ON POTENTIAL LEGAL RAMIFICATIONS..... 3

HARRY EMERSON, SUMMARY STATEMENT ..... 3

VoIP – UNREGULATED, UNPROTECTED ..... 5

RISK MANAGEMENT SPECIALIST SCOTT WOLFF ON RISK IMPLICATIONS ..... 7

HOW 130 YEARS OF SECURITY AND RELIABILITY WILL END..... 9

VoIP SECURITY RISKS ARE WELL KNOWN TO INSIDERS ..... 11

INSURANCE INDUSTRY QUESTIONS TO PONDER..... 12

VoIP KEY AREAS OF RISK..... 13

THE EASE OF ATTACKING VoIP – A HACKERS’ DREAM ..... 13

VoIP RISKS: PERSONAL ..... 14

VoIP RISKS: ORGANIZATIONAL, CORPORATE, and ENTERPRISE ..... 15

NEW SNIFFER CAN ATTACK VoIP USERS..... 15

VoIP RISKS: NATIONAL SECURITY ..... 17

A BRIEF, UGLY HISTORY OF NON-VoIP CYBER-SECURITY FACTS & FIGURES ..... 21

WHO ARE THE ATTACKERS? ..... 23

REVIEWING VoIP-RELATED CYBER-SECURITY BREACHES ..... 24

HOW VoIP WORKS – BACKGROUND FACTS RELATING VoIP SECURITY ISSUES TO  
INTERNET SECURITY ISSUES ..... 25

MODES OF ATTACK..... 27

THE FREE-WHEELING, UNREGULATED INTERNET DEMOCRACY ..... 28

CYBER SECURITY EXPERT KEVIN NIXON ON ENCRYPTION AND VoIP WEAKNESSES .... 29

HOW DOES THE HEAD OF YOUR IT DEPT. STACK UP AGAINST THE FBI? ..... 30

SUMMARY OF VoIP EXPOSURES, RISKS, AND LIABILITIES ..... 31

THE SOLUTION: THE FUTURE WE WANT vs. THE FEATURE DEFICIT OF VoIP ..... 32

FURTHER TECHNICAL INFORMATION AND RESOURCES..... 34

CONCLUSION ..... 35

ABOUT THE AUTHORS ..... 36

APPENDIX A, “TOP VOIP THREATS DETAILED BY SECURITY FIRM” ..... 38

APPENDIX B, 100 SOFTWARE TOOLS FOR HACKING/SPYING VOIP ..... 41

**VoIP - UNREGULATED, UNPROTECTED**

Being server-based, Internet telephony is susceptible to espionage, hacking, intrusion, interruption, identity theft, denial-of-service attacks, and other forms of malicious and criminal interference via any and all the techniques that hackers employ. The role of hackers is to devise schemes to break into Internet servers. Therefore, no one should be surprised that with the accelerating trend towards widespread use of VoIP technology, they will turn their attention to VoIP servers. **ALL INTERNET SERVERS ARE SUSCEPTIBLE TO HACKING.** The fact that VoIP depends upon servers accessible on the Internet endangers personal, corporate, and national security, which will have a direct and increasing impact upon the insurance industry and those it serves. "VoIP is making it easier to wage cyberwar..." an analyst reported as far back as 2004, "just as flaws that make some VoIP products vulnerable were revealed." Network World 1/19/2004. The growth in malware and cyber attacks is exponential. According to F-Secure Corporation, malicious software attacks tripled in 2008<sup>1</sup>. Midway through 2009 McAfee's Avert Labs reported that attacks have tripled since 2008<sup>2</sup>.

The Obama administration is rightfully zeroing in on cyber security, cyber crime and cyber warfare as a major part of its homeland security priorities. Businesses and government are spending vast amounts of money to protect themselves against what begins to feel like an army of shadowy terrorists invading the technology we all depend upon. And the situation is getting worse, not better, which is why it has now been elevated to the level of a national security concern. Should we be worried about phone service too? Unfortunately, the answer is "Yes."

With the rise of phone services utilizing the Internet it is incumbent upon the insurance industry to examine the probability of cyber-insurance issues for users of VoIP, as well as for VoIP providers and vendors.

Given our growing awareness of the perils of VoIP telephone service, as revealed herein, why do businesses continue to move communications online? The answer is simple but extremely short-sighted. Internet Telephony is very inexpensive. The lure of easy money has caused nontraditional carriers to

---

<sup>1</sup> [http://www.f-secure.com/en\\_US/security/security-lab/latest-threats/security-threat-summaries/2008-4.html](http://www.f-secure.com/en_US/security/security-lab/latest-threats/security-threat-summaries/2008-4.html)

<sup>2</sup> <http://www.avertlabs.com/research/blog/index.php/category/Malware%20Research/>  
(This is a very lengthy blog, but scanning through it will give insight into the many modes of attack used by hackers, terrorists, and criminals.)

provide customers with VoIP services which in many cases are nearly free. In addition, VoIP companies such as [Skype \(NASDAQ: EBAY\)](#), [Vonage \(NYSE: VG\)](#) and the various Cable carriers ([Comcast NASDAQ: CMCSA](#), [Time Warner: NYSE TMC](#), and [Cablevision: NYSE CVC](#)), which have ventured into Internet Telephony, did so not only to provide cheaper communications, but to avoid regulatory scrutiny. Not having to deal with the regulations creates an even less costly, more profitable environment. But these profits come at a price. As we know, there is no free lunch, and while they are cheap, it is becoming increasingly clear that VoIP services carry risks and potential consequences.

In short, the integrity of our telecommunications system has been compromised because of short term thinking geared towards reducing short term costs. There appears to have been little practical thought given to the enormous and inevitable costs of developing, securing, purchasing and installing backend security protections, to the extent it is even possible, once the commitment to VoIP telephony has been made.

**Insurance and risk management specialist, R. Scott Wolff comments:**

*"Unfortunately, in today's world, even the most fundamental daily activities, such as talking on the telephone, open up complex issues of risk. Cyber liability and business exposures to it are real and seemingly inescapable. But, the issues related to the developing field of online telephony are a separate challenge due to inherent differences in technology and therefore plans for a solution must be investigated separately and addressed from a risk management perspective.*

*"The internet is wide open to risk. As such any business utilizing internet/web based programs is at risk. This includes telecommunications systems. Some of the risks/exposures when using VoIP telephony include unauthorized access, spying, theft of trade secrets, intellectual property theft, identity theft, interruption of commerce both on-line and off-line, diversion of delivery, extortion, invasion of privacy, sabotage and associated third party liability just to name a few.*

*"Imagine you are on the telephone with a business confidant discussing new product planning information that when implemented will give your company a significant advantage in your specific marketplace and tremendous market share. Two months later a competitor unveils the same product with the exact same detail you were planning. How could this be?"*

*"Or, you are having conversations concerning a very private matter that if disclosed could have a serious negative impact. A few weeks later you learn that your conversations are known to others. You know that these "very private" discussions were made only using the phone in your office, off-hours when no one else was in the office. How did these people gain access to your conversations?"*

*"The growing connectivity between information systems, the internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks and other critical infrastructures". 72% of businesses express concern about information and/or physical security of company assets. – from a report conducted by Runzheimer International in 2006. The GAO (Government Accountability Office) has reported that the number of incidents of attempted and successful security breaches has increased threefold since 2006. In its report dated May 5, 2009 they state that critical federal information systems are "not sufficiently protected to consistently thwart cyber threats," which are "evolving and growing." These risks hold true for businesses as well. Therefore it is incumbent upon every organization to examine its telephone-based communications and to then make an assessment of exposures related to telephony which can be done by addressing the following fundamental questions:*

- What are our risks?
- What are the threats?
- Where are we exposed?
- Ask - if this happened... how would it affect our flow of business?
- What would the financial impact be on our business if this happened?
- Do we have contingency plans in place?
- How will our insurance policies respond? Are there gaps?
- What would be the cost to remediate the system/security?
- Can we implement a disaster recovery program in case an event occurs?
- What can we implement to prevent an occurrence from happening?

*"While this line of questioning is not comprehensive it does provide good direction to begin an assessment. And each question is likely to develop into several additional considerations."*

**HOW 130 YEARS OF SECURITY AND RELIABILITY WILL END**

We have grown comfortable over the years with the reliability and security of the telephone system. We don't even think about the possibility of someone hacking into our phone system, intercepting our calls, or stealing our identities through the telephone. Other than a scenario straight from the movies of a determined spy climbing a pole or sneaking into our homes to plant a bug in a phone, we can't even imagine this happening.

Most people don't think about or understand that there is a difference between voice transmission over our traditional phone system and voice transmission over the Internet. To the end user it all seems the same. However, it is not the same. As voice transmission migrates to the Internet, all of the concerns relevant to the security of our networked computers become relevant to phone service as well.

While the talk we hear about the national importance of cyber terrorism may seem borderline hysterical, there now is sound evidence that cyber security attacks are being managed by organized groups with substantial resources and zeal, which in addition to hackers, include criminal consortiums, international terrorists, and even nations.

These are the fundamental principles behind this risk:

Each change in technology brings benefits, but also unanticipated risks. In this case, Internet telephone service uses the Internet, and so is exposed to every risk of the Internet.

The architecture of the Internet is inherently flawed. It presumes a trusted relationship between every person and every system, which was appropriate 40 years ago when the Internet was designed by scholars and inventors for their own use. But now, when every person and every system has direct access to one another it means that, implicitly, each of us has a trusted relationship with every hacker and terrorist in the world.

The core of the cyber security problem relating to VoIP lies within the structure of VoIP technology itself. Simply stated, all aspects of VoIP, including the calling and called systems, the call setup mechanism, and the digital transfer of voice information and associated visual and video material, are "in the wild" on the Internet – unsecured, exposed to unprecedented risk and therefore to unprecedented potential liabilities.

Last but not least, the FCC has chosen not to recognize VoIP as "telecommunications" (viz. classifying VoIP under Title II of the

Communications Act of 1934). In the absence of that classification, VoIP instead defaults to being classed as an “information service”, and therefore not subject to any of the nation’s telecommunications regulations. The FCC has attempted to regulate some limited aspects of VoIP as if it VoIP operators were Title II common carriers, but without making that formal classification, and instead using the “ancillary jurisdiction” provision of the Act. However, in a major case ruled on by the U.S. Court of Appeals for the DC Circuit ([Comcast v. FCC](#)), in April, 2010, the court undermined even the ancillary jurisdiction authority upon which the FCC relied (see [CommonLaw Blog](#) for an abbreviated explanation). The FCC is desirous of having an Internet free from stifling regulation, and in that VoIP is essentially a software application running on the Internet, the FCC is reluctant to impose regulations on VoIP by classifying it under Title II. There still are five aspects of VoIP that are regulated by the FCC under the ancillary jurisdiction clause, but since the Comcast ruling undermines the ancillary jurisdiction authority, all of those provisions are subject to being overturned if challenged. This will essentially leave VoIP unregulated unless and until the FCC (or Congress) classifies VoIP under Title II.

## **VoIP SECURITY RISKS ARE WELL KNOWN TO INSIDERS**

Don't think that cyber security concerns are news to the VoIP industry. The following announcement records the formation of a VoIP Industry Alliance (called VoIPSA, for VoIP Security Alliance) to address VoIP security concerns as far back as 2005:

*In Feb. 07, 2005 the following report noted, "Industry Alliance Formed To Fight VoIP Cyber Attacks."*

*VoIP Security Alliance focuses on VoIP security risks; members include Avaya, Symantec, SANS Institute, and 3COM's TippingPoint, among others.*

*Major VoIP and security vendors, including 3Com (NSDQ:COMS)'s TippingPoint, Avaya (NYSE:AV), Symantec (NSDQ:SYMC), and the SANS Institute among others, have formed the VoIP Security Alliance (VOIPSA) to discover and fight VoIP security risks.*

*The alliance is the first group to focus on security risks posed by increasingly popular VoIP technology. It is backed by a wide spectrum of organizations, including universities, security researchers, VoIP vendors, and VoIP providers. TippingPoint, a division of 3COM, has been instrumental in forming the group, and through it, hopes to use and improve a VoIP security testing tool it developed to find and research VoIP vulnerabilities.*

*The group warns that the growing convergence of voice and data networks magnifies the security risks posed by cyber attacks. Successful attacks against a combined voice and data network can cripple an enterprise, halt communications required for productivity, and result in unhappy customers and lost revenue, it claims. The group also warns that as VoIP deployments become more widespread, the technology becomes a more attractive target for hackers. And it believes that VoIP application-level attacks will likely occur as attackers become more familiar with the technology.*

*Among the charter members of the group are 3Com, Alcatel, Avaya, Codenomicon, Columbia University, Ernst & Young's Guiliani Advanced Security Center, Insightix, NetCentrex, Qualys, SecureLogix, Siemens, Sourcefire, Southern Methodist University, Spirent, Symantec, the SANS Institute and Tenable Network Security. A complete list of members can be accessed at <http://www.voipsa.org/>*

*By Networking Pipeline Staff, ChannelWeb  
11:08 AM EST Mon. Feb. 07, 2005*

*<http://www.crn.com/it-channel/59301529;jsessionid=4RVEHR0LINAOPQE1GHPCKHWATMY32JVN>*

**INSURANCE INDUSTRY QUESTIONS TO PONDER:**

Cyber liability is an evolving coverage. Is the coverage for network breaches only? If so, what networks?

Is there a first-party business interruption coverage for network security breaches and does it extend to VoIP?

What about first party cyber extortion? Does a third party coverage for network security and data privacy, and the professional coverage, apply to VoIP?

Is there enterprise-wide privacy breach coverage?

What are client demands for coverage, in contract or demands for certificate of insurance wording?

Are the insurance carriers pricing for the telephone exposure?

While these are open questions, there certainly is the likelihood that as VoIP systems are breached and damage incurred, legal liabilities will be exposed, including possibilities of mass tort.

### **VoIP KEY AREAS OF RISK**

Here is a brief summary of the types of risk exposure caused by VoIP. Detailed explanations of these types of risk are explored throughout the rest of this report.

- Denial of Service (phones become useless -- cannot even call for help during emergencies.)
- Other Interruptions of Service (e.g. by disabled servers)
- Hacking/Intrusion
- Identity Theft
- Eavesdropping
- Impersonation
- Redirection of Calls
- Discovery of Unlisted Numbers, Geographic Location of Callers
- Theft of Secrets/ Intellectual Property
- Espionage

### **THE EASE OF ATTACKING VoIP - A HACKER'S DREAM**

Readers may be astonished to learn that there are almost 100 ways to sniff and hack VoIP systems and calls. It's a wide open castle, no guards, no parapets, the drawbridge is down, and the moat is empty.

To see how bad it really is, review Appendix B which provides a listing from a VoIP Security organization, VoIPSA, of almost 100 software tools to sniff, hack, attack, record, manipulate, spy upon, and interfere with or block VoIP systems and calls. These are all readily available. You can download and install them, and try them out for yourself. And, while these may be new to you, you know that hackers are well acquainted with these tools and techniques.

**VoIP RISKS: PERSONAL**

As earlier noted VoIP is unregulated and unprotected. But there are fundamental requirements of Privacy, Secrecy, and Security that we have taken for granted in traditional telecommunications, which are seldom discussed openly with regard to VoIP. These have now become serious issues which need to be fully considered by users such as corporations, telecommunications carriers, VoIP carriers, law enforcement agencies, and federal and state governments.

Therefore, let us examine the situation by first taking a look at the problem — and then at what the insurance industry can do to mitigate the effects of an anticipated tide of criminal damage as technology adjusts to the new world order.

For example, in traditional telephony an unlisted number provides privacy and security. The called party has no access to the caller's number. But with VoIP, if the called party can access the IP address of the caller, which can be done in some cases with alarming ease, the called party will then have information about the geographic location of the caller.

There are endless scenarios in which privacy could be compromised. What if that caller is a scientist in a research laboratory? Or a counselor in a safe house for victims of abuse? If phone message content can be trapped or diverted, what happens to a law firm discussing client information and case strategies? What happens to the company that sold them VoIP?

From a law enforcement perspective, all phone service, including VoIP, must provide for legal wiretap, legal call trace, and the ability to identify and block abusive, harassing, or threatening callers, either as a police action in defense of victims or in pursuit of villains, or in response to a court order. Since VoIP is being implemented by an estimated hundreds of independent vendors around the globe, VoIP services are so diffuse that there is no assurance that these fundamental requirements will be met. The FCC's decision to interpret VoIP as "data communications", and therefore not subject to telecommunications regulations has left law enforcement and government entities impotent against VoIP threats.

## **VoIP RISKS: ORGANIZATIONAL, CORPORATE, and ENTERPRISE**

VoIP communications within an enterprise (a corporation, a law firm, a government agency, an insurance company) are especially vulnerable. Here is an announcement of a software application, purportedly for risk assessment, but this software and others like it are available to friend and foe alike:

### **New Sniffer Can Attack VoIP Users**

*Next-generation VoIP sniffer was released on Saturday at Toorcon in San Diego by Jason Ostrom of VoIP Hopper. The tool, that might be used for attacks, should help raise awareness of the type of vulnerabilities businesses face as they adopt unified communications (UC) technology.*

*According to Jason, the tool, UCSniff, has two settings. One is a learning mode, sniffing all the IP traffic then mapping telephone extensions to specific addresses. By default, it is capturing all the calls and saving them to wave files.*

*The other setting is targeting conversations. After learning the IP addresses of the phone system, someone using UCSniff can listen to all the VoIP, or Voice over Internet Protocol, conversations made by a specific user, say the CEO. That's user mode. A second mode, conversation mode, allows someone to monitor calls made exclusively between two extensions, say only when the CEO calls the CFO.*

*"So it's like dynamic ARP poisoning," Ostrom explained, referring to Address Resolution Protocol spoofing. "The tool, on the fly, figures out how to do the ARP poisoning for you so you're not intercepting the traffic of phones that you do not want to intercept."*

*The flaw, if any, is within the structure of the system and not specific to any platform, such as that of Cisco Systems. There are two other tools and combined, the tools can allow one to create a man-in-the-middle attack on VoIP networks in an enterprise.*

*Some of the pieces are already available on the Internet. However, UCSniff "brings together what is lacking, what is needed to be the most effective and secure VoIP security assessment tool available."*

CyberInsecure.com    September 29th, 2008  
<http://cyberinsecure.com/category/voip/>

The existence of spy software packages as described above means that even the most private, important, and privileged conversations can be monitored and recorded by a malicious insider. But, even worse, standard hacker and virus techniques might be used to plant a spy package on one or more user computers

or servers within an enterprise to operate autonomously and remotely, and send the recorded conversations to competitors, or industrial spies, or your opponents, or to Russia, North Korea, Iran, or China. And you might never know.

## **VoIP RISKS: NATIONAL SECURITY**

The *Virtual Criminology Report* Nov. 2007 by McAfee, NATO, the FBI, and United Kingdom's Serious Organized Crime Agency indicates that it is believed that 120 countries are launching web espionage operations to spy on and attack financial markets, government computer systems, Air Traffic Control, electrical generation systems and networks among other critical infrastructures. In particular, it is believed that China has invaded and attacked computer systems, not just against the U.S., but also against India, Germany, and Australia.

### **Analysis: One Step Behind**

*“Several miles from Tiananmen Square in Beijing a slight young man with long hair and dressed in a black T-shirt sits in a smoky cyber cafe staring at the screen of his laptop computer. He doesn't look like a soldier, but he is conducting offensive combat operations as a first lieutenant in the People's Liberation Army. He is a graduate of an elite academy where he learned to master the weapons and techniques of warfare: botnets, spoofing, phishing and polymorphous worms to name just a few. He is engaged every day in attacking numerous U.S. computer systems to gain access to sensitive and classified government data. He is quiet, he is patient, he is skilled, and he is winning.*

*“Every day thousands of people like him around the globe tap into government systems. The vast amounts of data they extract range from veterans' medical records to the refueling protocols for Navy ships at sea to the systems responsible for diagnosing maintenance problems for the F-35 Lightning II fighter and even the unclassified e-mails of Secretary of Defense Robert Gates. According to media reports, the Homeland Security Department estimates more than 60,000 cybersecurity breaches targeting government, industry and individuals in 2008 -- more than 18,000 for the federal government alone.*

*“The damage does not end there. While massive amounts of official data are being exfiltrated from federal computers, other attackers are probing emergency response systems in hundreds of cities and municipalities, mapping electrical power grids and tapping into communications nodes. Still others are stealing the personal and financial information of hundreds of thousands citizens and causing the loss of hundreds of millions of dollars to businesses whose systems have been invaded and compromised.*

*“Cyberwarfare could soon become the No. 1 threat to national security. Think about it, how much of our daily lives is controlled in cyberspace? The gas we buy at the pump, the ATMs we use to get some quick cash, the air traffic control system that directs 6,000 to 8,000 planes aloft at any given time, all these and many more actions are governed by computers. Imagine the havoc that would result if these systems suddenly were offline due to a massive denial-of-service*

*attack. Life would grind to a halt. Traffic lights would go dark, elevators would stop, life-support systems in hospitals would blink out."*

By Jack Thomas Tomarchio 06/19/2009  
NEXTGOV - Technology and the Business of Government  
[http://www.nextgov.com/nextgov/ng\\_20090619\\_6396.php](http://www.nextgov.com/nextgov/ng_20090619_6396.php)

It should be apparent that VoIP systems will not escape the interest or attention of the malevolent side of these 120 countries. If they can exploit weaknesses in VoIP, they will.

An article from Canada.com reveals the advantages and sophistication of the attackers in comparison to that of the defenders.

### **Cyber attacks 'grossly underestimated'**

***Industries lack technology and skill to counter dangerous hackers, security expert says***

*By Jordana Huber, Canwest News Service June 25, 2009*

*Cyber attacks have become increasingly sophisticated and targeted, and their threat is underestimated, according to a former top U. S. cybersecurity official.*

*"These are not hypothetical teenage hackers from New Hampshire," said Amit Yoran, former director of the U. S. Department of Homeland Security's national cyber-security division. "This is a very real threat environment, where nation-state actors are actively engaged, where non-nation-state actors and where organized crime is actively engaged."*

*Speaking at the World Conference on Disaster Management, Yoran, CEO of NetWitness Corp., a cybersecurity consulting firm, said government and industry systems are being compromised daily by cyber threats that are far more focused and specific than in the past.*

*Yoran said cyber espionage favours the attacker, and can be very difficult to defend against.*

*Most industries' understanding of the threat is "very poor and grossly underestimated," he said, noting there is also frequently a lack of technical knowledge or skill to respond to an attack.*

*"The most advanced technologies that we use to defend ourselves are basically preparing us for the types of threats we saw in 1995, not for the types of advanced-threat methods and techniques that we are seeing from any sophisticated adversary," he said.*

*"The terrorists, the nation states, the criminals are using only those techniques which have not yet been identified," Yoran said.*

<http://www.canada.com/technology/Cyber+attacks+grossly+underestimated/1731010/story.html>

The Georgia Tech Information Security Center hosted its annual summit on emerging security threats Oct. 15, 2008 and published its annual attack forecast, *Emerging Cyber Threats Report for 2009*. According to the research, the electronic domain will see greater amounts of malware, botnets, attacks on VOIP systems, and cyber-warfare in the coming year.

### **VOIP attacks:**

*The experts contended that attackers will increasingly flock to the world of VOIP technologies to "engage in voice fraud, data theft and other scams -- similar to the problems e-mail has experienced."*

*DoS (denial of service), remote code execution and botnet threats will also apply to VOIP networks in the coming year, and will become more problematic for mobile devices as well, the report said.*

*"Criminals know that VOIP can be used in scams to steal personal and financial data, so voice spam and voice phishing are not going away," said Tom Cross, an X-Force researcher with IBM Internet Security Systems. "Most people have been trained to enter Social Security numbers, credit card numbers, bank account numbers, etc. over the phone while interacting with voice response systems; criminals will exploit this social conditioning to perpetrate voice phishing and identity theft."*

### **Cyber-warfare:**

*Security experts contributing to the report contended that cyber-warfare "will accompany traditional military interaction more often in the years ahead."*

*The experts said e-war tactics will also "play a more shadowy role in attempts by antagonist nations to subvert the U.S. economy and infrastructure."*

*To get a firmer grasp on what is likely to come, the GTISC researchers said observers should look no further than the targeted cyber-attacks that occurred between Russia and Georgia earlier in 2008.*

*George Heron, founder of BlueFin Security and a former chief scientist for McAfee, submits that cyber-warfare will play a significant role between China and the United States.*

*"Cyber-threats originating from China are very real and growing," Heron said. "Other evidence supports this, such as the majority of bot masters being traced back to China, along with malware and other disruptive threats."*

[http://securitywatch.eweek.com/exploits\\_and\\_attacks/2009\\_outlook\\_more\\_malware\\_botnets\\_voip\\_attacks\\_and\\_cyberwar.html](http://securitywatch.eweek.com/exploits_and_attacks/2009_outlook_more_malware_botnets_voip_attacks_and_cyberwar.html)

**A BRIEF, UGLY HISTORY of NON- VoIP CYBER SECURITY FACTS**

- Malicious software attacks have tripled in 2008, much higher in 2009, according to F-Secure Corporation and McAfee.
- Theft of intellectual property, fraud and damage of corporate networks cost corporations over a \$1 trillion globally in 2008, according to a recent report by the security firm McAfee and Purdue University.
- Russia began Aug. 2008 Georgia war with cyber-attack, not jets knocking out Georgian radar installations. Russian hackers literally brought Georgia to a standstill by interrupting services to Banking, ATMs, transportation systems, power-generation systems. Attacks were carried out by Russian civilians and sympathizers but were coordinated with the invasion of the former Soviet state and had the cooperation of both the Russian military and organized crime, according to a report released Aug. 17, 2009 to U.S. government officials.
- Similar attack by Russia against Estonia in 2007.
- According to public reports, Russian, Chinese hackers cracked Obama and McCain networks.
- According to public reports, Cyber-Hackers broke into International Monetary Fund computer system in 2008.
- According to public reports, in November, 1998, Computer hackers suspected of working from Russia successfully penetrated Pentagon computer systems including computers for the US Central Command, which oversees Iraq and Afghanistan, in one of the most severe cyber attacks on US military.
- According to public reports, Hackers infiltrated and defaced U.S. Senate website, May 2009.
- According to public reports, in July 2009, a powerful attack overwhelmed computers at U.S. and South Korean government agencies for days, also targeted the White House, the Pentagon and the New York Stock Exchange. Other targets of the attack included the National Security Agency, Homeland Security Department, State Department, the NASDAQ stock market and The Washington Post. Some government Web sites – such as the Treasury Department, Federal Trade Commission and Secret Service – were still reporting problems days after the attack started during the July 4 holiday.
- The Wall Street Journal reported April 21, 2009 that unknown cyber-intruders had over the past two years hacked into defense-contractor servers housing information about the \$500 billion F-35 Joint Strike Fighter (Lockheed Martin's [NYSE: [LMT](#)] Lightning II), the next-generation fighter/bomber for the U.S., Britain and seven other close allies. The hackers, whom all signs indicated were based in China, copied "several terabytes" – several thousand gigabytes – of data about the F-35's systems, internal maintenance and electronics.

- The Wall Street Journal also reported in front page news in April 2009 that Russian and Chinese hackers penetrated the U.S. electricity grid.
- The Pentagon reports that its systems are "probed daily." Throughout the federal government, more than 18,000 cybersecurity breaches were reported last year, including more than 3,200 known cases of unauthorized access and nearly 2,300 known cases of malicious code being inserted into federal IT systems, according to [Motley Fool's](#) Rick Smith, April 22, 2009.
- SecureWorks, a leading security provider, reports huge increase in hacker attacks against its 36 major retail chain customers in 2<sup>nd</sup> half 2008, up from 34,000 to 137,000 per customer per month, totaling 5 million attacks per month.
- Even space isn't safe. The BBC reported August 28, 2008 that NASA has confirmed that laptops carried to the International Space Station in July were infected with a virus known as Gammima.AG. NASA said it was not the first time computer viruses had traveled into space.

### **WHO ARE THE ATTACKERS?**

From an examination of information such as is stated above, U.S. government experts believe that the majority of serious attacks are organized efforts put together by groups such as these:

- Independent Hackers working in leagues, especially in cooperation with and sponsorship from government entities.
- Organized Crime Syndicates (notably the Russian Mafia)
- Industrial Spies (especially, those acting on behalf of governments)
- Foreign Governments (Intelligence Organizations, Military)
  - 120 Countries have Cyber Espionage units
  - Russia, China, North Korea extremely active
  - Operations are well funded
  - Government agencies provide advanced training in cyber espionage techniques
  - Government agencies pay for theft of secrets & damage
  - Government agencies coordinate activities of independent hackers and organized crime syndicates

## **REVIEWING VoIP-RELATED CYBER SECURITY BREACHES**

- The entire worldwide DNS<sup>3</sup> system was brought to its knees by hackers multiple times in recent years<sup>4</sup>.
- Every Scheme that hackers use against Internet servers will be used against all the types of Servers deployed in VoIP.
- Localized DNS attacks occur regularly.
- VoIP security concerns include reports that German authorities have tapped conversations, while the Chinese authorities. openly monitor and record messages and personal information
- If DNS is brought down, VoIP users can't even make emergency calls.
- All of the VoIP Internet services are uncontrolled, in the wild, with no way for users to tell if their systems or calls are safe.
- You are at risk even if the other party uses VoIP and you don't
- VoIP Risks Are Internet Risks. Internet Risks Are VoIP Risks.

---

<sup>3</sup> The Domain Name System is like the phone book for the Internet. DNS maps the IP addresses (e.g., 207.241.148.80) to human readable hostnames (e.g., www.about.com). So DNS determines which physical server handles a domain's website traffic or email delivery. <http://onlinebusiness.about.com/od/onlinebusinessglossary/g/dns-domain-name.htm> About.com

<sup>4</sup> "Massive DDoS Attack Hit DNS Root Servers  
During the course of the ping-flood pounding, only four of 13 root servers remained up and running while seven were completely crippled..... Tuesday evening's distributed denial of service (DDoS) attack on the 13 copies of the U.S. root server should serve as a warning to every company employing DNS, said the inventor of the technology Wednesday." InternetNews.Com Oct. 23, 2002.

A similar attack June 15, 2004 brought down Google, Yahoo, Microsoft, FedEx, Apple, Akamai, and many others.

And more recently: "ICANN says that starting at 4 a.m. PST (12:00 UTC) on February 6, 2007, a massive distributed denial-of-service attack hit six of the root servers like a brick wall, with a wave of bogus queries hitting the root servers at the rate of 1GB per second. Two of the root servers were immediately and severely compromised; four fared well under the strain. According to ICANN, the amount of data sent to the DNS root servers during the attack was roughly equivalent to receiving 13,000 e-mails every second, or 1.5 million every two minutes." CNet.com March 23, 2007

**HOW VoIP WORKS - BACKGROUND FACTS RELATING VoIP SECURITY ISSUES TO INTERNET SECURITY ISSUES**

The types of threats that arise from VoIP are similar to those of the Internet as a whole, but more extensive.

In the VoIP model, all call setup signaling data, as well as the conversation data, traverses the Internet and thus is susceptible to all the known threats of snooping, eavesdropping, and intercepting or replacing one communication with another. This essential fact is what endangers the privacy and secrecy of personal and corporate communications, which, by extension, represents a national security risk.

**Background:** Internet Telephony is commonly referred to as **VoIP** (Voice over IP, where the “IP” refers to the Internet Protocol), but is alternately referred to simply as **Internet Telephony** or Internet phone service. The major protocols and services used by VoIP include **DNS** (Domain Name Service), **SIP** (for Session Initiation Protocol - the basic VoIP call processing mechanism), and **ENUM** (Electronic Number).

Additionally, VoIP systems run on servers, including **gateway servers** (for access on/off a corporate LAN [Local Area Network], and connecting to/from the Public Switched Telephone Network), **SIP proxy servers**, **location servers** (for locating users), and **registrar servers** (for registering location information). The registrar and location server may be integrated in the proxy server. These are servers on the Internet which store account information and control the placement and receiving of calls. More advanced VoIP systems store personal information in SIP, location, and registration servers.

**DNS** (Domain Name Service) is the Internet phone book that associates a domain name like Google.com to a numerical IP address. Every time you click on a link in a browser, a series of **DNS** queries are made to obtain that numerical IP address - once it is obtained, the browser connects using the numerical IP address. Routers know the numeric mapping of the Internet, and are able to route data packets from one place to another using the numerical IP addresses. The **DNS** system, numerical IP addresses, and routers are the essential elements of the Internet.

Just as every access to a web page requires a series of **DNS** queries, every VoIP call depends on a series of **DNS** queries. **SIP** and **ENUM**, and VoIP in general, depend upon the basic Internet infrastructure consisting of millions of routers and **DNS** servers. **DNS** is notoriously trouble-prone, slow, and susceptible to errors, and, as mentioned previously, a target for Denial of Service attacks (DoS, or DDoS for “Distributed DoS”). There isn’t anything a DoS target can do - the enemy turns on a fire hose and you flounder and drown until they turn it off.

Also, **DNS** servers have been hacked into and records changed so you thought you were going to one place but you go to somewhere else put up by the hackers. In terms of VoIP, who knows where your call might go? Most likely, though, the hacker will initiate the call to the proper party, but will remain in the middle with access to all information (the “man in the middle” exploit).

**SIP** is a protocol for storing and communicating call setup signaling information across the Internet, and runs on **SIP** servers. The standard industry concept of implementing multimedia telephony is to deploy VoIP using **SIP** and **ENUM**. There is some practical experience with **SIP**, but **ENUM**, in general, is an unknown.

**ENUM** is an arrangement using **DNS** to cross-referencing phone numbers to IP addresses. It is important to understand that, in order to achieve universality and the simplicity of just dialing a phone number to make a multimedia call (see below: *The Future We Want vs. the Feature Deficit of VoIP*), **ENUM** must be universally deployed. (And that would mean that every phone number in the world must be stored in **DNS** systems.) Otherwise, the caller must use a computer-style interface and type an “address” similar for to an email address: “sip:joe.rizzo@generalmotors.com”. This requirement is certainly beyond the realm of the non-computer literate. Furthermore, taking one moment to realize the implications of this in some non-English languages that require hieroglyph keyboards (Chinese, for example), one can readily anticipate that this approach for will never see universal deployment. Anyone can dial a number, many won’t be able to “type” an “address” (at least, not conveniently, and not for the illiterate who might know their numbers but not their letters). Therefore, in the VoIP scheme, universality demands **ENUM**.

## **MODES OF ATTACK**

There are many advocates of Internet telephony, but we believe that **VoIP**, **SIP**, and **ENUM** are fundamentally flawed, because, among other things, they are dependent upon **DNS**, which is, itself, fundamentally flawed. In essence, there is zero assurance that the particular systems which will handle your call are trustworthy, competent and reliable. With more and more frequency, they are not. These telephony solutions expose the industry and the nation to serious and unnecessary risks, while compromising the quality of our nation's phone service.

In addition to the more common attack modalities such as viruses and spyware, these and other systems are susceptible to more sophisticated methods such as phishing<sup>5</sup>, vishing<sup>6</sup>, pharming<sup>7</sup>, and Denial of Service (DoS) attacks. Using these methods, it may well be possible for a hacker or terrorist to divert phone calls by replacing one phone number with another. An unsuspecting caller might find him or herself not talking to the help desk of a reputable company, but talking directly to the hacker or terrorist ("I'm sure I can help you. Just let me remote into your computer and I'll take a look.")

We can expect that as VoIP becomes more widely utilized, hackers and cyber-terrorists will develop all the types of exploits currently being used on the Internet to target VoIP, in addition to utilizing the new voice communications types of threats such as logging all the calls someone might make, and blocking, intercepting, or redirecting calls.

---

<sup>5</sup> In the field of computer security, **phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. <http://en.wikipedia.org/wiki/Phishing>

<sup>6</sup> **Vishing** (Voice phISHING), also called "VoIP phishing," is the voice counterpart to phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's credit card number. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number. In either case, because people are used to entering credit card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed, and the entire operation can be brought up and taken down in a short time, compared to a real telephone line. [http://www.pcmag.com/encyclopedia\\_term/0,2542,t=vishing&i=57067,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=vishing&i=57067,00.asp)

<sup>7</sup> **Pharming** refers to setting up a fraudulent Web site that contains copies of pages from a legitimate Web site in order to capture confidential information from users. By hacking into DNS servers and changing IP addresses (see DNS hijacking), users are automatically redirected to the bogus site, at least for some period of time until the DNS records can be restored. [http://www.pcmag.com/encyclopedia\\_term/0,2542,t=pharming&i=49165,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=pharming&i=49165,00.asp)

**THE FREE-WHEELING, UNREGULATED INTERNET DEMOCRACY**

**DNS** is completely decentralized (there are 12 million DNS servers), and is operated by millions of businesses, organizations, ISP's, and anyone else who wishes to do so. Anyone can put up a **DNS** server. You don't need a license, you don't have to pass a test, you don't need to be bonded and insured, you just do it, and no one can tell you that you can't. From a practical perspective, we depend on the good faith, integrity, and reliability of the **DNS** operators for successful operation of the Internet. However, allowing the national and worldwide telephone system to depend on **DNS** exposes the United States to a similar dependency, which is hardly prudent.

Similarly, anyone can operate a VoIP telephone company - and there are thousands of them around the world. You and I and that shady character downtown can set up a business, promote ourselves as a quality and reliable service, and operate it with whatever level of competence and integrity suits us. We can set up a **DNS** server, run **ENUM** on it, and set up a **SIP** server using whose ever **SIP** software we choose (might be the free kind). The same rules apply here that apply to running your own **DNS** server - there aren't any. You did not take a test, your chief technologist isn't certified in anything, you didn't apply to the State, or the FCC, or to anyone else to get a license, and you don't have to report anything to anybody (other than for taxes, of course). And who's to know that the shady guy is really a (pick one) member of organized crime, religious fundamentalist terrorist, drug user who needs money, industrial spy, undercover operative for a foreign country, or \_\_\_\_\_ (fill in the blank).

**Comments from Cyber Security Expert Kevin Nixon on Encryption and VoIP Weaknesses**

*“VoIP has some specific weaknesses from a cyber security perspective. First, VoIP uses the protocol combination of RTP over UDP, and that combination cannot readily be protected. There are already seven or eight hacker software packages that can get to the data, which means that if someone can intercept your call, they can capture the audio in digital form.*

*“Various schemes of encryption are possible, but generally only implemented within an enterprise where the IT managers have the ability to fully specify the particulars of deployment so that all the elements are properly configured and compatible. In such an arrangement, a VoIP phone in an office in Boston may be able to communicate securely with a peer VoIP phone in the organization’s Atlanta office.*

*“However, there generally is no mechanism to encrypt a VoIP call that leaves the protected boundaries of the enterprise since there is no way to assure, or even identify, that the remote device has the same capabilities. As a blatant example, you may be calling a VoIP phone in China where the Chinese government has not only disabled encryption by matter of law, but has also inserted a monitoring system into the middle of every call.*

*“In another scenario, you may be a subscriber to a VoIP service, and as such, have no control whatsoever over the provisioning of that service. They may not even provide encryption among phones belonging to the same subscriber or group.”*

Kevin M Nixon, CISSP® CISM® CGEIT®  
Professional Governance, Risk,  
Compliance & Privacy Strategist

<http://www.information-security-resources.com>

<http://www.linkedin.com/in/kevinnixon>

**HOW DOES THE HEAD OF YOUR IT DEPARTMENT STACK UP AGAINST THE FBI?**

The FBI's unclassified email system was hacked into and shut down for almost the entire last week of May, 2009. The FBI did not provide details on the security incident, but it looks as though hackers may have used malicious file attachments to hack into the network.

So ask yourself, "Is my IT department more capable than the FBI?" Because if the FBI can't protect itself from hacking and malicious attacks, what is the chance that your IT organization (or your clients') will be able to do so? Translating this discussion into the perils of VoIP, the indications are that everyone using VoIP will be walking unarmed into the lion's den. As confident as your IT department might be, the reality is that VoIP communications arrangements are unavoidably hazardous, and the might of almost any IT department will wither under the onslaught of determined, expert, well-funded, well-trained hackers, terrorists, organized crime syndicates, and foreign governments.

We believe that those promoting VoIP are naïvely overconfident.

## **SUMMARY OF VoIP EXPOSURES, RISKS, AND LIABILITIES**

There are innumerable ways to go wrong with VOIP. Unlike traditional telephone service in which the operational systems are connected together by a private network and are not exposed to the Internet, every system involved in Internet telephony is susceptible to espionage, hacking, intrusion, interruption, and identity theft. And while the goals of VoIP planners might have been laudable, they are now exposing us to tremendous risk.

*Do you know the type of phone system or service used by the people you call? Traditional telecommunications? or VoIP? Quality service vendor? Up-to-date on all their patches? Fanatical diligence, or just normal (or worse)? And even if you knew all that, it simply doesn't matter – how are they going to protect against every vulnerability known and future? It's an impossible task, and some challenges such as Denial of Service attacks can't be protected against. You are at risk even if only the other party is using VoIP, and you are not.*

Some of our concerns may seem more appropriate to Hollywood than to information-technology departments and law-enforcement agencies, just as cyber-security and cyber-warfare were simply fanciful topics of movies just a few years ago. But they are illustrative of the sorts of issues which are now surfacing, and which will almost certainly erupt. Two extreme examples cited earlier are very telling: In 2007 Russia utilized cyber-warfare against Estonia and in 2008 against Georgia, to completely shut down the infrastructure of those countries. As corporations and individuals in the United States adopt VoIP more widely, risks from cyber terrorism and cyber warfare will include shutting down substantial portions of our communications infrastructure.

The risks and exposures of the Internet and VoIP are beginning to be described and documented. But, since they cannot be fixed, the insurance and legal communities will be left to deal with the consequences.

**THE SOLUTION: The Future We Want vs. the Feature Deficit of VoIP**

All of the preceding discussion focuses on the risk aspects of VoIP, without the consideration of any redeeming qualities of VoIP, which begs the issue of “Why even bother?” There are some important factors to discover within this topic.

First, as has been stated previously, VoIP, as it is currently being implemented by almost all vendors, is a minimalist technology aimed at shaving pennies off the cost of a call. With the exception of a couple of minor features offered by a few vendors, VoIP just lowers cost. The originators of VoIP and the VoIP standards had better things in mind, including the ability for multimedia phone calls, but those visions have all been lost in the rush to market where the sales pitch is really simple – you can save a little money over what you now pay the phone company.

Well, here is where we are. The telephone was invented 130 years ago – it was voice-only then, and it is still voice-only. Despite the tremendously rich experience offered by multimedia on the Internet, phone service, even phone service from a cell phone with images on it, is still audio-only. This is a glaring gap in technology in comparison to the rich media capabilities of the Internet – telephone service is 15 years behind the times. But at the same time, it presents an enormous opportunity to modernize a multi-trillion dollar industry. And it promises a bigger, faster revolution than the development of the PC or the cell phone. Bigger and faster because the public is already sensitized to the value of multimedia – there won’t be any selling required – and because, for the most part, the infrastructure already exists, so technology development and rollout can be quick with only modest capital outlays.

Now we can take a clean piece of paper, and write down what we want from the next generation of telecommunications. **Here are some key aspects of Next Generation telephony:**

- ✓ Technology that seamlessly merges the best of the Internet with the best of the telephone network
- ✓ Internet-style graphics & visual communications, including videophone, on screen-based phones
- ✓ Requires no knowledge or training for users – Simply dial a phone number like you always have
- ✓ Audio/visual calls will become standard for routine, daily communications
- ✓ Traditional “phone company” security, quality, and reliability

And, what do we mean by MultiMedia? Well, in today’s jargon, it enables us to make Web 2.0 Internet-style rich media visual telephone calls on broadband Internet connections, using wire-line or wireless touch-screen phones such as the

Apple ([NASDAQ: AAPL](#)) iPhone, simply by dialing a phone number, and still enjoy the privacy, security and reliability of traditional telephone calls.

The experience will be similar to accessing a web page with a browser, but would be done by dialing a phone number. In this new environment, every phone will be a website; every phone number will be a domain name.

For example, rather than having to wait through a tedious series of audible call prompts from a call answering system, the call answering system will send you a screen with the prompts on touch buttons, enabling you to navigate quickly and effortlessly to the person or system that you want. You might call a store to learn their hours or location, or check stock, or speak to someone, and all those options would be presented on your screen phone – if you just wanted a map, or to know the hours, you get that information instantly, but if you want more, just click a button or hang on for a moment and the call will complete.

This new technology will define the next generation of telecommunications, and will offer features that will enrich telecommunications and enable vendors to charge significant premiums for the new services that result. Many more exciting features are possible. We suggest you visit the [IronPipe.net](#) website to learn more if you are interested in the future of telecommunications. There, you can read or download a white paper, view a self-paced presentation, or watch a 30-minute webinar.

**FURTHER TECHNICAL INFORMATION AND RESOURCES**

A number of firms have sprung up specializing in VoIP security threats. Please refer to Appendix A for excerpts from a report prepared by one such firm identifying seven specific threats in an [InternetNews.com article](#) entitled, "TOP VOIP THREATS DETAILED BY SECURITY FIRM".

Also, here is a good technical reference article reviewing the major security threats, weaknesses and attack targets of VoIP, "[Voice over IP Security - A layered approach](#)", from the security consulting firm of XMCO Partners.

**Most importantly, review Appendix B for a listing of almost 100 software tools to sniff, hack, attack, record, manipulate, and spy upon VoIP Systems and calls.**

## **CONCLUSION**

In short, as VoIP becomes more widespread because of the appeal of low cost of entry, we can anticipate great difficulty in maintaining privacy, secrecy, and security across the spectrum of private, commercial and government communications. And, we can expect hackers and cyber-terrorists to develop all kinds of methods to exploit the system, at an incalculable cost to society.

In short, as VoIP becomes more widespread because of the appeal of low cost of entry, we can anticipate great difficulty in maintaining privacy, secrecy, and security across the spectrum of private, commercial and government communications. And, we can expect hackers and cyber-terrorists to develop all kinds of methods to exploit the system, at an incalculable cost to society.

An entire VoIP industry is currently developing comprised of hundreds of companies, including many specializing in VoIP security, and tens of thousands of personnel whose futures and livelihoods depend on the success of VoIP. We expect there will be acrimonious response to this report from the VoIP sector, diminishing and trivializing the risks while trumpeting security enhancements proposed for adoption, as if they are a systemic, holistic solution. The reader can evaluate these responses independently: If the VoIP industry can confidently and honestly assert that the risks of the Internet have been solved, that hacking and intrusion have been conquered, that there no longer are threats from viruses and Trojan horses, then it will be fair to consider VoIP as a reliable and secure alternative to the traditional telephone network. But until that time, every person considering VoIP or hearing a VoIP promotion should clearly understand that it means moving from a reliable and secure service to one that will expose themselves, and those they communicate with, to extreme risk.

Emerging armored technologies for Internet telephony, like IronPipe™, will have a role in mitigating these exposures. However, until such changes are implemented and security restored, insurance counselors should be developing and recommending a full range of available extensions of coverage for cyber liability. And, they will have to be monitoring carrier changes to those coverages if Internet telephony exposures become major loss producers, as we predict they will.

*A portion of this material appeared in the September 2009 and March 2010 issues of PIA magazine, an award-winning industry publication dedicated to the professional insurance agent and the American agency system.*

## **ABOUT THE AUTHORS**

**Harry Emerson** is a principal in NJ-based Emerson Development LLC, and the creator of the patented IronPipe™ plan to integrate the Public Switched Telephone Network (PSTN) with the Internet, overcoming risks to VoIP from spying / espionage, hacking, intrusion, and interruption, while enabling numerous MultiMedia features that take advantage of the broadband capabilities of the Internet. A white paper and audio-visual presentation material describing Mr. Emerson's IronPipe security system is available at [IronPipe.net](http://IronPipe.net).

**Paul Henry** is one of the world's foremost global information security and computer forensic experts, with more than 20 years' experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. He is currently the lead forensic investigator and president of Forensics & Recovery LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security and as a retained consultant at the VoIP security company Siperia. Mr. Henry also serves as the board vice president of the Florida Association of Computer Crime Investigators (FACCI) and is the USA board vice president of the International Information Systems Forensics Association (IISFA). Throughout his career, Mr. Henry has played a key strategic role in launching new network security initiatives to meet our ever-changing threat landscape. Mr. Henry also advises and consults on some of the world's most challenging and high-risk information security projects, including the National Banking System in Saudi Arabia, the Reserve Bank of Australia, the Department of Defense's Satellite Data Project, and both government as well as telecommunications projects throughout Southeast Asia. Mr. Henry is frequently cited by major and trade print publications as an expert in computer forensics, technical security topics, and general security trends and serves as an expert commentator for network broadcast outlets, such as FOX, NBC, CNN, and CNBC. Mr. Henry serves as a featured and keynote speaker at seminars and conferences worldwide. In addition, he regularly authors thought leadership articles on technical security issues, and his expertise and insight help shape the editorial direction of key security publications, such as the Information Security Management Handbook, where he is a consistent contributor.

**Kevin Nixon** is a Master Security Architect (MSA); Certified Information Systems Security Professional (CISSP); Certified Information Security Manager (CISM); Certified US Domestic and International Regulatory Professional; Certified in the Governance of Enterprise IT (CGEIT) designation; and is a Licensed Private Security Consultant.

Mr. Nixon has over 25 years of experience in MIS design and development, Information Security, Business Continuity and Disaster Recovery, and US and European Regulatory Compliance.

Mr. Nixon has testified as an expert witness before the Congressional High Tech Task Force, the Chairman of the Senate Armed Services Committee, and the Chairman of the House Ways and Means Committee. He served on infrastructure security boards and committees including the Disaster Recovery Workgroup for the Office of Homeland Security (which developed the National Strategy to Secure Cyberspace), and is a U.S. Voting Delegate to the International Standards Organization (ISO), Financial Data Protection, Privacy and Security Standards TC68-SC2 & US TC68-SC6.

**Glenn Tippy** is the president and managing partner of Gerrity, Baker, Williams Inc. GBW provides risk-management and insurance-coverage services to small and mid-size businesses and their owners. Mr. Tippy has served on the Boards of the New Jersey Insurance Underwriting Association and the Insurance Council of New Jersey. He currently serves on the New Jersey Insurance Commissioner's Territorial Rate Equalization Exchange Committee. He is a board member of the Professional Insurance Agents of New Jersey Inc. and is the chair of its Legislative and Regulatory Affairs Committee. Mr. Tippy holds the CPCU and CLU professional designations. He can be reached at 1-800-548-2329.

**R. Scott Wolff, CIC, CRIS**, is a partner in Premier Risk Management, LLC., where he provides insurance and risk management consulting services to public, private and not-for-profit organizations throughout the U.S. Mr. Wolff provides clients with an independent and unbiased viewpoint on overall effectiveness of their insurance and risk management programs, saving his clients significant time and money while obtaining better overall coverage. Over the years he has saved his clients in excess of \$60 million dollars on premium.

Mr. Wolff has published articles on insurance tips and strategies in a variety of media. Recently, he has authored a book titled "Executive's Guide to Risk Management and Insurance - Reduce the Risk Boost Your Bottom Line", written for the astute executive, CEO, CFO, Controller, COO, VP, Board Member or Business Owner, who appreciates the complexity and importance of insurance issues and who wants to realize all the profit-boosting potential the right decisions afford the company. He has been a keynote speaker and involved in numerous panel discussions regarding insurance related topics.

## APPENDIX A

A number of firms have sprung up specializing in VoIP security threats. Here are excerpts of a report from one such firm identifying seven specific threats in an [InternetNews.com article](#).

### **Top VoIP Threats Detailed by Security Firm**

*By David Needle*

*April 16, 2009*

*IT professional can add VoIP to the growing list of security threats they need to monitor. Security firm WatchGuard Technologies detailed seven leading threats to Voice over IP services in a release this week. While they aren't all new, they stand to become higher profile as the bad guys seek to exploit VoIP's increased popularity.*

*"Some of these are tested and true blue data hacks that have been around for a while, and now there's a lucrative new field for hackers and criminals to go after on the VoIP side," WatchGuard spokesman Chris McKie told InternetNews.com. "The bad guys are going to go where the money is."*

*WatchGuard says recent reports predict as much as 75 percent of corporate phone lines will be using VoIP in the next two years. By the end of this year, the total number of VoIP subscribers worldwide (residential and commercial) is expected to reach nearly 100 million.*

*Heading WatchGuard's list are Denial of Service (DoS) attacks, similar to those made to data networks. VoIP DoS attacks leverage the same tactic of running multiple packet streams, such as call requests and registrations, to the point where VoIP services fail.*

*These types of attack often target SIP (Session Initiation Protocol) extensions, according to WatchGuard, that ultimately exhaust VoIP server resources, which cause busy signals or disconnects.*

*Another is Spam over Internet Telephony (SPIT). Like unwanted e-mail, SPIT can be generated in a similar way with botnets that target millions of VoIP users from compromised systems. Like junk mail, SPIT messages can slow system performance, clog voicemail boxes and inhibit user productivity.*

*VoIP is also potentially vulnerable to Directory Harvesting attacks. These occur when attackers attempt to find valid VoIP addresses by conducting "brute force" attacks on a network.*

*When a hacker sends thousands of VoIP addresses to a particular VoIP domain, most of the VoIP addresses will "bounce back" as invalid, says WatchGuard. But from those that are not returned, the hacker can identify valid VoIP addresses.*

*By harvesting the VoIP user directory, the hacker now gains a new list of VoIP subscribers that can be new targets to other VoIP threats, such as SPIT or vishing attacks.*

*Vishing, or Voice Phishing, attempts to get users to divulge personal and sensitive information, such as user names, account numbers and passwords.*

*The trick works by spamming users and luring them to call their bank or service provider to verify account information. Once valid user information is given, criminals are free to sell this data to others, or in many cases, directly siphon funds from credit cards or bank accounts.*

*Analyst Michael Dortch agreed the threat to VoIP services should be a key IT concern.*

*"Users and network operators need to begin taking steps to protect their VoIP deployments and resources, such as directory databases, now, so they can try to get a jump on the bad guys when they start trying to figure out how to steal and automatically process actual VoIP conversation streams," said Dortch, principal analyst at DortchOnIT, said in an e-mail to InternetNews.com.*

*"As voice and data streams increasingly converge, and businesses increasingly rely on IT to do business, the business criticality of digital voice and data grows significantly," continued Dortch. "When building and implementing their data security architectures, users and network operators alike must ensure that no data is left behind to minimize operational and reputational risks."*

*Another threat on WatchGuard's list relates to Dortch's comments on conversation stealing. Like data packets, voice packets are subject to man-in-the-middle attacks where a hacker spoofs the MAC address of two parties, and forces VoIP packets to flow through the hacker's system.*

*By doing so, the hacker can then reassemble voice packets and literally listen in to real-time conversations. From this type of attack, which WatchGuard calls eavesdropping, hackers can also grab all sorts of sensitive data and information, such as user names, passwords, and VoIP system information.*

*Rounding out WatchGuard's threat list are Voice Service Theft and Registration Hijacking.*

*VoIP service theft can happen when an unauthorized user gains access to a VoIP network, usually by way of a valid user name and password, or gains physical access to a VoIP device, and initiates outbound calls. Often, these are international phone calls to take advantage of VoIP's toll by-pass capabilities.*

*A SIP registration hijack works by a hacker disabling a valid user's SIP registration, and replacing it with the hacker's IP address instead. This allows the hacker to then intercept incoming calls and reroute, replay or terminate calls as they wish.*

<http://www.internetnews.com/security/article.php/3815611>

## APPENDIX B

### *VoIP SECURITY ALLIANCE REVEALS THAT ALMOST 100 SOFTWARE TOOLS EXIST TO SNIFF, HACK, AND ATTACK VoIP CALLS AND SYSTEMS.*

---

The following list of attack tools is from the industry association VoIPSA ("The *Voice over IP Security Alliance* aims to fill the void of VoIP security related resources through a unique collaboration of VoIP and Information Security vendors, providers, and thought leaders.", from <http://www.voipsa.org>).

VoIPSA is interested in identifying and studying the security issues of VoIP, in the hope that those risks can be resolved. We believe the reader will be better served by understanding that, if there now are 100 ways to crack and attack VoIP, soon there will be 200. These are all readily available - you can easily download and install them, and try them out for yourself. And, while these may be new to you, hackers are well acquainted with these tools and techniques.

For details on all of the following, please go to <http://www.voipsa.org/Resources/tools.php>, and follow the individual links.

### VoIP Sniffing Tools

- [AuthTool](#) - Tool that attempts to determine the password of a user by analyzing SIP traffic.
- [Cain & Abel](#) - Multi-purpose tool with the capability to reconstruct RTP media calls.
- [CommView VoIP Analyzer](#) 💰 - VoIP analysis module for CommView that is suited for real-time capturing and analyzing Internet telephony (VoIP) events, such as call flow, signaling sessions, registrations, media streams, errors, etc.
- [Etherpeek](#) 💰 - general purpose VoIP and general Ethernet sniffer.
- [ILTY \("I'm Listening To You"\)](#) - Open-source, multi-channel SKINNY sniffer.
- [NetDude](#) - A framework for inspection, analysis and manipulation of tcpdump trace files.
- [Oreka](#) - Oreka is a modular and cross-platform system for recording and retrieval of audio streams.
- [PSIPDump](#) - psipdump is a tool for dumping SIP sessions (+RTP traffic, if available) from pcap to disk in a fashion similar to "tcpdump -w".
- [rtpBreak](#) - rtpBreak detects, reconstructs and analyzes any RTP session through heuristics over the UDP network traffic. It works well with SIP, H.323, SCCP and any other signaling protocol. In particular, it doesn't require the presence of RTCP packets.

- [SIPomatic](#) - SIP listener that's part of LinPhone
- [SIPv6 Analyzer](#) - An Analyzer for SIP and IPv6.
- [UCSniff](#) - UCSniff is an assessment tool that allows users to rapidly test for the threat of unauthorized VoIP eavesdropping. UCSniff supports SIP and Skinny signaling, G.711-ulaw and G.722 codecs, and a MITM ARP Poisoning mode.
- [VoiPong](#) - VoiPong is a utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to separate wave files. It supports SIP, H323, Cisco's Skinny Client Protocol, RTP and RTCP.
- [VoIPong ISO Bootable](#) - Bootable "Live-CD" disc version of VoIPong.
- [VOMIT](#) - The vomit utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players.
- [Wireshark](#) - Formerly Ethereal, the premier multi-platform network traffic analyzer.
- [WIST](#) - Web Interface for SIP Trace - a PHP Web Interface that permits you to connect on a remote host/port and capture/filter a SIP dialog

### VoIP Scanning and Enumeration Tools

- [EnableSecurity VoIPPack](#) for CANVAS 💰 - VoIPPack is a set of tools that are designed to work with Immunity CANVAS. The tools perform scans, enumeration, and password attacks.
- [enumIAX](#) - An IAX2 (Asterisk) login enumerator using REGREQ messages.
- [iaxscan](#) - iaxscan is a Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts.
- [iWar](#) - IAX2 protocol Wardialer
- [Nessus](#) - The premier free network vulnerability scanner.
- [nmap](#) - the premier open source network port scanner.
- [Passive Vulnerability Scanner](#) 💰 - The Tenable Passive Vulnerability Scanner (PVS) can find out what is happening on your network without actively scanning it. PVS detects the actual protocol, various administrative interfaces, and VoIP scanner(s). Currently includes over 40 VoIP checks.
- [SCTPScan](#) - This tool enumerates open SCTP ports without establishing a full SCTP association with the remote host. You can also scan whole networks to find SCTP-speaking machines.
- [SIP Forum Test Framework \(SFTF\)](#) - The SIP Forum Test Framework (SFTF) was created to allow SIP device vendors to test their devices for common errors.
- [SIP-Scan](#) - A fast SIP network scanner
- [SIPcrack](#) - SIPcrack is a SIP protocol login cracker. It contains 2 programs, SIPdump to sniff SIP logins over the network and SIPcrack to bruteforce

- the passwords of the sniffed login.
- [Sipflanker](#) - Sipflanker will help you find SIP devices with potentially vulnerable Web GUIs in your network.
- [SIPSCAN](#) - SIPSCAN is a SIP username enumerator that uses INVITE, REGISTER, and OPTIONS methods.
- [SIPVicious Tool Suite](#) - svmap, svwar, svcrack - svmap is a sip scanner. It lists SIP devices found on an IP range. svwar identifies active extensions on a PBX. svcrack is an online password cracker for SIP PBX
- [SiVuS](#) - A SIP Vulnerability Scanner.
- [SMAP](#) - SIP Stack Fingerprinting Scanner
- [VLANping](#) - VLANPing is a network pinging utility that can work with a VLAN tag.
- [VoIPAudit](#) 💰 - VoIP specific scanning and vulnerability scanner.

### VoIP Packet Creation and Flooding Tools

- [IAXFlooder](#) - A packet flooder that creates IAX packets.
- [INVITE Flooder](#) - Send a flurry of SIP INVITE messages to a phone or proxy.
- [iThinkTest FlowCoder](#): SiPBlast 💰 - SIP Flood/Capacity testing of infrastructure by emulating mass CPE call traffic
- [kphone-ddos](#) - Using KPhone for flooding attacks with spoofed SIP packets
- [NSAUDITOR](#) - SIP UDP Traffic Generator - Flooder 💰 - SIP UDP traffic generator / flooder generates SIP traffic to stress test voice over IP systems, SIP programs and implementations under heavy network load. It is a very simple and fast program which can simulate SIP client and call activity.
- [RTP Flooder](#) - Creates "well formed" RTP Packets that can flood a phone or proxy.
- [Scapy](#) - Scapy is a powerful interactive packet manipulation program. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery.
- [Seagull](#) - a multi-protocol traffic generator especially targeted towards IMS.
- [SIPBomber](#) - SIPBomber is sip-protocol testing tool for Linux.
- [SIPNess](#) - SIPness Messenger is a SIP testing tool which is used for testing SIP applications.
- [SIPp](#) - SIPp is a free Open Source test tool / traffic generator for the SIP protocol.
- [SIPsak](#) - SIP swiss army knife.

## VoIP Fuzzing Tools

- [Asteroid](#) - this is a set of malformed SIP methods (INVITE, CANCEL, BYE, etc.) that can be crafted to send to any phone or proxy.
- [Codenomicon VoIP Fuzzers](#) 💰 - Commercial versions of the free PROTOS toolset
- [Fuzzy Packet](#) - Fuzzy packet is a tool to manipulate messages through the injection, capturing, receiving or sending of packets generated over a network. Can fuzz RTP and includes built-in ARP poisoner.
- [Interstate Fuzzer](#) - VoIP Fuzzer
- [Mu Dynamics VoIP, IPTV, IMS Fuzzing Platform](#) 💰 - Fuzzing appliance for SIP, Diameter, H.323 and MGCP protocols.
- [ohrwurm](#) - ohrwurm is a small and simple RTP fuzzer.
- [PROTOS H.323 Fuzzer](#) - a java tool that sends a set of malformed H.323 messages designed by the University of OULU in Finland.
- [PROTOS SIP Fuzzer](#) - a java tool that sends a set of malformed SIP messages designed by the University of OULU in Finland.
- [SIP Forum Test Framework \(SFTF\)](#) - SFTF was created to allow SIP device vendors to test their devices for common errors. And as a result of these tests improve the interoperability of the devices on the market in general.
- [Sip-Proxy](#) - Acts as a proxy between a VoIP UserAgent and a VoIP PBX. Exchanged SIP messages pass through the application and can be recorded, manipulated, or fuzzed.
- [Spirent ThreatEx](#) 💰 - a commercial protocol fuzzer and robustness tester.
- [VoIPER](#) - VoIPER is a security toolkit that aims to allow developers and security researchers to easily, extensively and automatically test VoIP devices for security vulnerabilities.

## VoIP Signaling Manipulation Tools

- [BYE Teardown](#) - This tool attempts to disconnect an active VoIP conversation by spoofing the SIP BYE message from the receiving party.
- [Check Sync Phone Rebooter](#) - Transmits a special NOTIFY SIP message which will reboot certain phones.
- [H225regreject](#) - H225regreject is a tool is used to disconnect H.323 calls. It first monitors the network in order to determine if a call is taking place. Once a call has been identified, it then injects a Registration Reject packet into the call.
- [IAXAuthJack](#) - IAXAuthJack is a tool used to actively perform an authentication downgrade attack and force an endpoint to reveal its password in plaintext over the network.
- [IAXHangup](#) - The IAXHangup is a tool is used to disconnect IAX calls. It first monitors the network in order to determine if a call is taking place. Once a call has been identified, it then injects a HANGUP control frame into the call.
- [iThinkTest FlowCoder](#): SiPCPE 💰 - Evaluate SIP infrastructure protocol compliance using inserted SIP messages.

- [RedirectPoison](#) - this tool works in a SIP signaling environment, to monitor for an INVITE request and respond with a SIP redirect response, causing the issuing system to direct a new INVITE to another location.
- [Registration Adder](#) - this tool attempts to bind another SIP address to the target, effectively making a phone call ring in two places (the legitimate user's desk and the attacker's)
- [Registration Eraser](#) - this tool will effectively cause a denial of service by sending a spoofed SIP REGISTER message to convince the proxy that a phone/user is unavailable.
- [Registration Hijacker](#) - this tool tries to spoof SIP REGISTER messages in order to cause all incoming calls to be rerouted to the attacker.
- [SIP-Kill](#) - Sniff for SIP-INVITEs and tear down the call.
- [SIP-Proxy-Kill](#) - Tears down a SIP-Session at the last proxy before the opposite endpoint in the signaling path.
- [SIP-RedirectRTP](#) - Manipulate SDP headers so that RTP packets are redirected to an RTP-proxy.
- [SipRogue](#) - a multifunctional SIP proxy that can be inserted between two talking parties
- [vnak](#) - VoIP Network Attack Toolkit - vnak combines a number of attacks against multiple protocols in to one easy to use tool. Its aim is to be the one tool a user needs to attack multiple VoIP protocols.
- [VoIPHopper](#) - VoIP Hopper is a security validation tool that tests to see if a PC can mimic the behavior of an IP Phone. It rapidly automates a VLAN Hop into the Voice VLAN.

### VoIP Media Manipulation Tools

- [RTP InsertSound](#) - this tool takes the contents of a .wav or tcpdump format file and inserts the sound into an active conversation.
- [RTP MixSound](#) - this tool takes the contents of a .wav or tcpdump format file and mixes the sound into an active conversation.
- [RTPInject](#) - RTPInject is a minimal-setup prerequisites attack tool that injects arbitrary audio into established RTP connections. The tool identifies active conversations, enumerates the media codec in use, and allows for the injection of an arbitrary audio file.
- [RTPProxy](#) - Wait for incoming RTP packets and send them to wanted (signaled by a tiny protocol) destination.
- [SteganRTP](#) - SteganRTP is a steganography tool which establishes a full-duplex steganographic data transfer protocol utilizing Real-time Transfer Protocol (RTP) packet payloads as the cover medium. The tool provides interactive chat, file transfer, and remote shell.
- [Vo<sup>2</sup>IP](#) - With Vo<sup>2</sup>IP, you can establish a hidden conversation by embedding further compressed voice data into regular PCM-based voice traffic (i.e. G.711 codec).

## Miscellaneous Tools

- [IAX.Brute](#) - IAX.Brute is a passive dictionary attack tool on IAX's challenge/response authentication method. This attack allows malicious users to steal passwords and hijack endpoint identities.
- [SIP-Send-Fun](#) - Sip Send Fun is a tiny command-line based Script, which exploits specific vulnerabilities.
- [SIP.Tastic](#) - SIP.Tastic is a passive dictionary attack tool on SIP's digest authentication method. This attack allows malicious users to steal passwords and hijack endpoint identities.
- [Spitter](#) - A set of tools for Asterisk to perform VoIP spam testing.
- [VoIP Security Audit Program \(VSAP\)](#) - VSAP is an automated question/answer tool to audit the security of VoIP networks (SIP/H.323/RTP). It provides security topics and audit questions for the end user to complete. Once all the questions are answered, VSAP will provide a final score.
- [XTest](#) - A simple, practical, and free, wired 802.1x supplicant security tool implementing the RFC 3847 EAP-MD5 Authentication method.

## Tool Tutorials and Presentations

- [An Analysis of Security Threats and Tools in SIP-Based VoIP Systems](#) - Shawn McGann and Douglas C. Sicker (University of Colorado at Boulder)
- [An Analysis of VoIP Security Threats and Tools](#) - Shawn McGann at 2nd VoIP Security Workshop June 2005
- [Hacking VoIP Exposed](#) - David Endler and Mark Collier for BlackHat 2006
- [Hacking VoIP Wired and Wireless Phones](#) - Shawn Merdinger for NoConName 2006
- [Real-time Steganography with RTP](#) - DEFCON 15 presentation by I)ruid on using steganography with RTP and the SteganRTP tool.
- [Security testing of SIP implementations](#) - Christian Wieser, Mark Laakso, and Henning Schulzrinne (Columbia University)
- [SIP Stack Fingerprinting and Stack Difference Attacks](#) - Hendrik Scholz, BlackHat USA 2006
- [Two attacks against VoIP](#) - by Peter Thermos - The purpose of this article is to discuss two of the most well known attacks that can be carried out in current VoIP deployments using SiVuS.
- [VoIP Attacks!](#) - Dustin Trammell for ToorCon 2006