



CyberPro

Volume 2, Edition 1
January 15, 2009

Keeping Cyberspace Professionals Informed

<p>Officers</p> <p>President Larry K. McKee, Jr.</p> <p>Chief Operations Officer Jim Ed Crouch</p> <p>----- ----</p> <p>CyberPro Editor in Chief Lindsay Trimble</p> <p>CyberPro Research Analyst Kathryn Stephens</p> <p>CyberPro Archive</p>	<p>The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest and to keep subscribers who are involved in the development of Cyber-related concepts and initiatives informed on items of common interest. The newsletter and the information contained therein are not intended to provide a competitive advantage for any commercial firm. Any misuse or unauthorized use of the newsletter and its contents will result in removal from the distribution list and/or possible administrative, civil, and/or criminal action.</p> <p>The views, opinions, and/or findings and recommendations contained in this summary are those of the authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or National Security Cyberspace Institute.</p>
<p>To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.</p> <p>Please contact Lindsay Trimble regarding CyberPro subscription, sponsorship, and/or advertisement.</p>	

All rights reserved. CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.

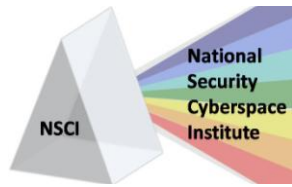


TABLE OF CONTENTS

Table of Contents.....	2
This Week in CyberPro	7
Senior Leader Perspective	8
Cyberspace – Big Picture	11
U.S. Not Ready for Cyber Attack.....	11
Cyberattack Simulation Highlights Security Challenges.....	11
Cyberspace Security Can Be Gone in a Flash	11
U.S. Agencies Seek More Proactive Approach to Cyber Defense	12
FBI Warns of Cyber Attack Threat.....	12
Nuclear Regulatory Commission Expands Cybersecurity Requirements for Nuke Power Plants	12
Despite Economy, Security Spending To Increase In 2009	13
Critical Security Projects Escape Budget Ax	13
Ankit Fadia Speaks on Cyber Terror Attack	13
Congress’ Computers Still Vulnerable, Cries Wolf	13
Hacked Lawmaker Calls for Cyber Briefings	14
Auditor: IRS Doesn’t Check Cyberaudit Logs.....	14
Ethical hacking course launched	15
Undersea Robot Searches for Severed Cables	15
Hash contest moves on to mass free-for-all.....	15
NERC Releases Phase I Cyber Security Standards For Review.....	15
New Open Standard Arrives For Gauging Security of Web Apps, Services	16
Revised Phase I Cyber Security Standards Under Review by NERC.....	16
Commission to fund research on China’s cyberwarfare capabilities	16
Thompson Files: Internet Threats – Part 1	16
Unleashing Hurricanes In Cyberspace: Part Five.....	17
Cyber Progress Often Lost in Translation	17
Meyerrose to Head Cybersecurity at Harris	18
U.S. Defense Contractors Look to Cyber Security Contracts.....	18
Lockheed, Boeing Tap \$11 Billion Cybersecurity Market.....	18
Cyberspace – President-Elect Obama.....	18
Seeking Obama’s Cyber Czar	18
IAC to Obama: Federal IT needs overhaul.....	19



Cyberspace – Department of Defense (DoD)	19
Pentagon Pushes Defense Companies to Strengthen Cyber Security	19
Gen. Lorenz on Leadership: At War in Cyberspace	19
Air Force Embraces Web 2.0.....	19
Classified Spillage	20
Army Approves Cisco Wireless Package	20
Cyberspace – Department of Homeland Security (DHS)	21
Chertoff calls for less secrecy in cybersecurity.....	21
After Six Years, Homeland Security Still Without ‘Cybercrisis’ Plan	21
DHS and cybersecurity: Yes, no, maybe so?	21
For your eyes only	21
DHS Privacy Office: Fusion Centers Endanger Privacy	22
Cyberspace – International	22
Israeli-Palestinian Conflict Could Result In Increased Internet Hacking Attacks	22
Is Someone In China Reading Your Emails?	23
Ministries in Bulgaria and New Zealand Fight Computer Viruses	23
Waging a War With Bits and Bytes.....	23
Iranian Hackers ‘Bring Down Mossad Web Site’	24
India’s Cyber Warriors Are Volunteers	24
World Bank Admits Top Tech Vendor Debarred for 8 Years	24
Uproar in Australia over plan to block Web sites.....	24
The Big War You Never Hear Much About.....	25
Undersea Cable Cuts Disrupt Internet Access	25
Chinese spy scare sours Australia’s plans for nationwide broadband	25
Israel Hacks Arab TV Station.....	25
Commonly Used Tools of the Chinese Hacker.....	26
Pak Now Planning Attack on Indian Cyber Networks.....	26
Pakistani Hackers Target Kalam’s Group.....	27
Thousands of legitimate sites SQL injected to serve IE exploit.....	27
Pro-Palestine Vandals Deface Army, NATO Sites	27
Korea Plans Hacking Competition	27
Hackers Take Battle with Hamas to Cyberspace	27
DECT Phones and POS Terminals Are Vulnerable	28
Iranian Hackers Attack Israeli Web sites	28
Hundreds of Israeli Web sites Hacked in ‘Propaganda War’	28



With Gaza Conflict, Cyberattacks Come Too 29

Government to allow private firms to monitor every move we make. I'm moving to China..... 29

Cyberspace Research 29

NSA Patents A Way to Spot Network Snoops..... 29

Network Security Against Today's Threats..... 29

Mobile Operators Anticipate Increased Spam Attacks But Are Slow to Protect..... 30

Researchers Point Out XSS Flaws On American Express Site 30

Researchers seek advanced network prioritization, security technology 30

DARPA Unveils Cyber Warfare Range 31

DARPA Leads Game-Changing Cyber Innovation..... 31

Rolls-Royce To Work On Electric Cyber Raygun Aero-Tech..... 31

SANS Releases List of Top 25 Most Dangerous Programming Errors in Software 31

Many RFID Cards Poorly Encrypted 32

Microsoft: MD5 hack Poses No Major Threats to Users..... 32

Internet Needs Global Regulation, Says Researcher..... 32

Software [In]security: Software Security Top 10 Surprises 33

IT Operations, Security Pros at Odds Over Virtualization Risks 34

44 Percent of SMBs Have Been Attacked by Cyber Criminals 34

Cyberspace 2009 Predictions 34

Four Threats for '09 That You've Probably Never Heard Of (Or Thought About) 34

Securing IT Networks Cheaply in the New Year 35

2009 Security Predictions: Déjà vu All Over Again..... 35

On botnets, encryption and mega-worms: Security predictions for 2009..... 35

Encryption Top IT Security Initiative in 2009 36

Cyber Attacks on Infrastructure Systems to Escalate: VeriSign..... 36

Cyberspace 2008 in Review 36

The Five Coolest Hacks of 2008..... 36

PC Tools: Top Internet Blunders of '08..... 36

Cyberspace Hacks and Attacks..... 37

Hacker's Choice: Top Six Database Attacks 37

Reply-all E-mail Storm Hits State Department 37

American Express Web Bug Exposes Card Holders..... 37

Researcher Releases Free DoS Hacking Tool..... 38

Major Bug Opens All Browsers to Phishing Attack..... 38

'Huge Increase' In Worm Attacks Plague Unpatched Windows PCs 38



Congress Hacked Again	39
Researchers Hack VeriSign's SSL Scheme for Securing Web Sites	39
Hacker Leaves Message For Microsoft in Trojan Code	39
Storm Worm Botnet Cracked Wide Open.....	39
Slow and Silent Targeted Attacks On The Rise	40
Fake CNN Malware Attack Spins Gaza Angle	40
Hack Simplifies Attacks on Cisco Routers.....	40
Researchers Hack Intel vPro Security	41
'Curse of Silence' Hack Kills SMS Text Message Delivery	41
'Undetectable' phishing attack identified by research team.....	41
New SSL Hack Imperils Secure Web sites.....	41
Friendster Social Networking Users Attacked by Malicious Spam	42
Microsoft warns of SQL attack.....	42
Hacked Phone System Leaves Company with \$50,000 Bill.....	42
Scareware Mongers Hitch Free Ride on Microsoft.com and Others	42
Online Jihadists Plan for 'Invading Facebook'	43
Hackers Bypassing IE Patch with Word Bugs	43
CheckFree.com Hijack May Have Affected 160,000 Users	43
Twitter Gets Hacked, Badly	43
You Could Be Flushed Into A Con.....	44
Cyberspace Tactics and Defense	44
FBI's IC3 Issues Tips For Preventing Website Attacks	44
Social networking malware: Protect yourself.....	44
Security on Social Networks Takes Efforts by All Sides.....	45
FTC: Reduce Data Theft by Regulating Social Security Numbers.....	45
Anatomy of an XSS Attack	45
Tech Insight: Finding Common Ground for Security, IT Teams	46
SanDisk Puts 'One-Touch' Backup On Flash Drive	46
As Phishing Evolves, Criminals Switch to Malware.....	46
VeriSign Remedies Massive SSL Blunder (Kinda, Sorta)	47
Self destruct technology for lost and stolen mobile phones	47
Cyberspace - Legal	47
Rep. Jackson Lee Proposes Cybersecurity Bill.....	47
U.S. Must Update Laws Defending Against Foreign Hackers.....	47
First 'Pretexting' Charges Filed Under Law Passed After HP Spy Scandal	48

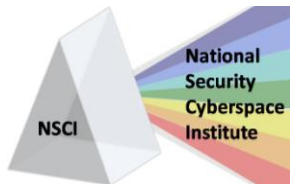


CyberPro

Volume 2, Edition 1
January 15, 2009

Keeping Cyberspace Professionals Informed

British Police Granted Hacking Rights.....	48
TJX Hacker Sentenced To 30 Years In Turkish Prison.....	49
Hacking Godfather 'Maksik' Sentenced to 30 Years by Turkish Court.....	49
New GA Law Forces Sex Offenders to Hand Over Their Internet Passwords.....	49
US district court orders CyberSpy to stop selling its RemoteSpy keylogging spyware program	49
Accused Hacker Facing Felony Charges	50
Software executive sentenced for hacking.....	50
Cyberspace-Related Conferences.....	51
Employment Opportunities with NSCI	52
CyberPro Content/Distribution.....	52



THIS WEEK IN CYBERPRO

BY JIM ED CROUCH, NATIONAL SECURITY CYBERSPACE INSTITUTE, INC.

A combination of factors has contributed to the “robust” nature of this first-of-the-year edition of *CyberPro*: an extra week since our last publication, more news surrounding the presidential transition, and an increase in both the frequency and significance of recent cyber attacks.

With the presidential inauguration scheduled for next Tuesday, we include a few stories related to the incoming administration and cyberspace. One such item is a *Forbes* report ([page 18](#)) on the candidates most likely to be appointed by President-Elect Obama to the newly-created position of National Cyber Advisor, reporting directly to the White House.

Also featured in this edition ([page 19](#)) is a report on recommendations made by the Industry Advisory Council to the Obama transition team, calling for an “overhaul of the government’s policies and practices regarding IT...”

The Commission on Cyber Security for the 44th Presidency recently recommended that the new administration transfer responsibility for cybersecurity from the Department of Homeland Security, saying that DHS “isn’t equipped to protect the federal government against cyber attacks.” Bill Brenner, writing in *Network World*, offers his views on the subject on [page 21](#).

In this edition’s Senior Leader Perspective ([page 8](#)), Maj. Gen. Kevin Kennedy, director, Joint Capability Development, U.S. Joint Forces Command, discusses JFCOM’s cyber-specific role as the Department of Defense lead for joint experimentation and training.

Also included in this week’s *CyberPro* is a story concerning an end-of-year release of the Top 5 Internet Blunders of 2008 ([page 36](#)), along with a list of the types of Internet threats expected to play a role in the Blunders of 2009 ([page 34](#)).

Enjoy these and the other stories contained in this issue of *CyberPro*. As always, we welcome your [feedback](#).



Alion is a progressive employee-owned research, management and technology company with worldwide government and commercial capabilities supporting complex programs including network and information security, M&S, experimentation, testing and Risk / Vulnerability tools.



SENIOR LEADER PERSPECTIVE

NSCI's Larry McKee recently had the opportunity to interview Maj. Gen. Kevin Kennedy, director of the U.S. Air Force Joint Capability Development, U.S. Joint Forces Command, regarding the organization's cyberspace capabilities and efforts.

NSCI: As the lead for the Department of Defense Joint Experimentation, what concepts, organizational structures, and/or emerging technologies is JFCOM looking at to improve the department's cyberspace capabilities?



MAJ. GEN. KEVIN KENNEDY: As the DoD lead for Joint Experimentation, we base our experimentation campaign on support to warfighters. Before we look at concepts, organizational structures, or emerging technologies, we must define what military problem we are trying to solve. That means we must do the necessary research to ask the right questions, or risk getting the wrong answers. Joint Operating Environment 2008, a JFCOM report, outlines a strategic framework and forecasts possible threats that will challenge the future joint force. The exponential growth of cyber and information technologies is one of several trends we've identified and we're addressing that in several ways.

Right now, we have a two-year Joint Concept Development & Experimentation (JCD&E) project to address challenges in cyberspace operations. We want to achieve two things through these efforts: improved integration and synchronization of computer network attack, defense; and exploitation as well as improved integration and synchronization of cyberspace and information operations. We're also working with our partners to provide foundational concepts for joint cyberspace operations.

In examining the cyberspace domain, we must remind ourselves that war is a human endeavor. Adversaries will challenge us in multiple ways; first, by constructing opposing "strategic narratives" distributed throughout multiple networks to change beliefs, perceptions, attitudes, and behaviors in their favor. Additionally, we must assume our networks will be attacked. No matter what technology emerges, it will not be a panacea. We cannot be lured by promises of decision-making machines and perfectly protected networks; instead we must be ready and able to continue operations even with degraded supporting networks.

NSCI: Can you tell us a little bit about how JFCOM's Global Force Management efforts are, or will be, helping commanders request and receive cyberspace forces?

KENNEDY: Adversaries do not wage discrete land, sea, air, space or cyberspace wars – instead they use all elements of power to wage war. As a global force provider, we need to address each situation on its own terms.



The Global Force Management construct has improved both the efficiency and effectiveness of Combatant Commanders' force requirements identification, submission, validation, force provider assignment and force sourcing processes. Most recently, the implementation of the Joint Capabilities Requirements Manager (JCRM) tool enabled the GFM community to consolidate all force requirements (including Cyber-Space force requirements) into a single Web-based management tool. This facilitated more informed and efficient force sourcing. We will continue to refine these processes and tools. We must improve our ability to provide forces – cyber or otherwise – in a careful and considered manner.

NSCI: According to JFCOM's Web site, one of the command's goals is to "Design Integrated, Properly Structured Command and Control." Can you tell us about any initiatives JFCOM has underway to integrate the command and control of cyberspace with other domains (e.g. maritime, ground, air and space)?

KENNEDY: One of our areas of emphasis at USJFCOM is to design integrated, properly structured joint command and control. Command and control is not synonymous with network operations or advanced technology. We need to enable joint interoperability from the beginning by sharing information, training, planning and technology. As the Department of Defense portfolio manager for Joint Command and Control, we work closely and transparently with the services and Combatant Commanders to provide needed capabilities.

One initiative JFCOM has underway is a Cyberspace C2 Assessment Team. We formed this team, in support of the National Military Strategy for Cyberspace Operations, to analyze existing command and control processes for their adequacy in conducting operations in the cyberspace domain. The JFCOM-led team then conducted numerous workshops and data calls with Combatant Commands, services and agencies to develop recommendations for improving and integrating command and control of the cyberspace domain with the other domains. Our goal is to integrate cyberspace into joint doctrine, joint training and joint experimentation. Our focus is on empowering commanders at all levels.

NSCI: The Services appear to be leaning forward to ensure they are positioned to train and equip "cyber warriors" in support of Combatant Commanders. What is JFCOM's role when it comes to training cyberspace professionals?

KENNEDY: The future landscape requires unprecedented levels of flexibility and adaptability. Adversaries will work to blur the line between political conflict and open war. We must build a force that is adaptable, agile and resilient. Joint warfighters demand and deserve improved training/education and integration, as well as robust and agile equipment. Realistic, timely and responsive joint training, along with agile and robust command and control network design, can underpin warfighter success.

At USJFCOM, we provide Combatant Commanders exercise design support to ensure the exercise environments replicate the operational environment (to include supporting command and control networks). Subject matter experts from the information operations and cyberspace operations communities assist in the planning and execution of joint exercises. Cyberspace activities in our training



evolutions include an accurate portrayal of current policies, authorities, threats, capabilities and challenges across all aspects of cyberspace operations.

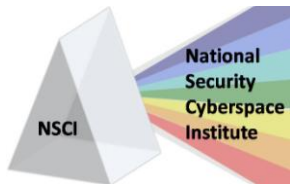
We will continue to work closely with the Joint Staff, USSTRATCOM, other Combatant Commands and the services to ensure U.S. forces are trained to conduct operations effectively in and through cyberspace.

NSCI: The Tidewater area of Virginia has long been a DoD leader in areas such as Modeling & Simulation, Command & Control, and Experimentation. Do you have any thoughts on how industry and academia expertise in these areas may be able to help the department with improving cyberspace capabilities?

KENNEDY: We are continually investigating, reviewing and applying the best of current business practices to our DoD processes to ensure the intellectual capital of the business community is leveraged to save U.S. taxpayer dollars. Effective cyberspace capabilities will require the combined efforts of industry, academia and DoD. Industry and academia offer a comprehensive suite of security tools for cyber warfare and can provide solutions for cyber defense and attack by using state-of-the-art technologies that include encryption of data at rest, secure wireless networks, rapid internet protocol traceback and Web-based forensic databases for automatic verification of hardware/software integrity. We want to enable joint interoperability from the beginning through our efforts in establishing standards, sharing information, training, planning and technology.

NSCI: Given the ongoing cyberspace attacks on DoD and industry networks, what is JFCOM's Joint Center for Operational Analysis (JCOA) doing to collect and analyze cyberspace lessons learned?

KENNEDY: We must capture enduring battlefield innovation and lessons and apply them after rigorous testing and evaluation. The Joint Center for Operational Analysis (JCOA) conducts studies at the request of the Secretary of Defense, the Joint Staff or a supported Combatant Command. To date, JCOA has not been asked to conduct a systematic study of lessons learned for defending against such attacks. One thing that is very clear is the enemy has decided to take us on in the cyber domain, and we will not let him steal a march.



CYBERSPACE – BIG PICTURE

U.S. Not Ready for Cyber Attack

BY: RANDALL MIKKELSEN, REUTERS UK
12/19/2008

230 representatives from government defense and security agencies, private companies and civil groups recently participated in a two-day cyberwar simulation, which exposed issues with leadership, planning and communications. Mark Gerencser of Booz Allen Hamilton, which hosted the simulation, said that there is currently no response plan, and that “there isn’t really anybody in charge.” U.S. Rep. James Langevin (D-RI), who participated in the simulation, explains that a successful attack could possibly cause a failure of the banking or national electrical systems. U.S. Rep. Dutch Ruppersberger of Maryland also commented, saying that billions of dollars are needed to improve security for both government and industry. Homeland Security Secretary Michael Chertoff, who spoke at the end of the exercise, said that cyberattacks may become a “routine warfare tactic,” accompanying more traditional attacks, and also emphasized the importance of updating international law and military doctrines.

<http://uk.reuters.com/article/idUKTRE4BI00520081219>

Cyberattack Simulation Highlights Security Challenges

BY: BEN BAIN, FEDERAL COMPUTER WEEK
12/18/2008

Government and industry officials participated in the Cyber Strategy Inquiry, a two-day simulation exercise that focused on “the importance of a cross-sector, integrated approach to cybersecurity.” Participants represented sectors including homeland security defense, transportation,

telecommunications and intelligence. The game included teams from government, industry and one from civil society that had to use a “control team” representative of Congress and the White House for communication. Mark Gerencser, a senior vice president at Booz Allen Hamilton, explained that the groups were required to consider multiple perspectives and focus on interdependencies. The article also discusses some of the challenges presented during the games and the main issues that faced each team, including: privacy versus attribution; regulation versus incentives; disclosure versus classification; and risk management versus resilience.

<http://fcw.com/Articles/2008/12/18/Cyberattack-simulation-highlights-security-challenges.aspx>

Cyberspace Security Can Be Gone in a Flash

SIGNAL ONLINE
12/2008

There is an unending struggle in cyberspace that will require constant attention. Solid defenses against cyber attacks exist and many of these defenses rely on strong and constantly-adapting computer safety technologies. Unfortunately, the weakness in this defensive perimeter is usually human. At times, for example, the protections available on government-issued drives are bypassed to save a few seconds of effort and the use of personal drives in government computers contributed to opening the door for the introduction of potentially dangerous code.

http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1798&zoneid=245



U.S. Agencies Seek More Proactive Approach to Cyber Defense

BY: JANET SASSI, FORDHAM UNIVERSITY
01/2009

The 2008 Comprehensive National Cyber Security Initiative (CNCSI) was created by President Bush to unify governmental agencies in the war on cyber crime and terrorism. The United States must adopt a proactive approach to protecting its newest national security asset – its cyber infrastructure. The CNCSI brings together 22 federal departments and agencies to create an integrated response to cyber intrusions that threaten national security and to develop a front line of defense to prevent intrusions, defend the nation against a full spectrum of threats and to shape the nation's cyber environment to ensure a U.S. advantage in cyberspace. Sandra Stanar-Johnson, deputy special assistant to the director of NSA/Central Security Service, stressed the CNCSI's commitment to protecting the privacy and civil liberties of all Americans. "This effort is not about sitting on the Internet like in some other countries and controlling what people see," she said. "All federal agencies would work together to maintain legal forms of protection."

Nuclear Regulatory Commission Expands Cybersecurity Requirements for Nuke Power Plants

BY: NUCLEAR REGULATORY COMMISSION, DARK READING
12/18/2008

The Nuclear Regulatory Commission recently approved regulations that upgrade security requirements for nuclear power reactors. The new rule includes updates to the regulatory framework to prepare for the licensing of new nuclear power plants. The new rules also include a "safety/security interface section,"

http://www.fordham.edu/Campus_Resources/eNewsroom/topstories_1442.asp

FBI Warns of Cyber Attack Threat

BY: SEBASTIAN SMITH, THE SYDNEY MORNING HERALD
01/07/2009

At a security conference in New York, Shawn Henry, the assistant director of the FBI's cyber division, said that cyber attack is the biggest risk to national security "other than a weapon of mass destruction or a bomb in one of our major cities." Henry cites the potential threat to our infrastructure, intelligence and computer networks from cyber attacks. He warns that cyber terrorists are working towards an "online 9/11" and hope to inflict the same kind of damage online as they did in New York in 2001. While an attack of that size has not happened yet, we can see the evolution of cyberspace as a weapon of war, especially in the Russian cyber attacks against Estonia and Georgia, and recent Palestinian attacks against Israeli Web sites. Attacks from financially-motivated cyber criminals who use the Internet to steal identities and billions of dollars are also becoming increasingly sophisticated.

<http://news.smh.com.au/world/fbi-warns-of-cyber-attack-threat-20090107-7bot.html>

which will require plants to take measures to avoid adverse interactions between security and other plant activities, as well as requiring plants to implement comprehensive cyber security programs. Plants will also be required to develop strategies and response procedures to address risks, and implement training and qualification requirements for security personnel.

<http://www.darkreading.com/security/cybercrime/showArticle.jhtml?articleID=212501188>



Despite Economy, Security Spending To Increase In 2009

BY: TIM WILSON, DARK READING
01/05/2009

New reports released by Forrester Research examined security trends in large enterprises and small and midsize businesses and found that security spending will continue to increase despite pressure to cut IT spending. Forrester analyst Jonathan Penn says that enterprises are allocating 11.7 percent of their IT operating budget to IT security in 2008, compared to only 7.2 percent in 2007. The report predicts that on

Critical Security Projects Escape Budget Ax

BY: STACY COLLETT, COMPUTERWORLD
12/30/2008

Vice president and chief information security officer at Sun Microsystems, Inc., Leslie Lambert, says that projects like server security, application security and Web security will take a back seat to deeper enhancement of user-access and identity management systems. Lambert explains that all projects are important, and should continue, but that economic conditions are forcing organizations to prioritize their security programs. John Pescatore of Garnet Inc. says that spending on projects that “keep the bad guys out” are usually recession-proof, although projects that “let the good guys in” are usually closely tied to business cycles. In 2009, many companies will focus on compliance with legal and regulatory mandates that aim to protect private and sensitive information.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=17&articleId=329993>

average, IT security budgets will increase to 12.6 percent of the IT operating budget in 2009. The research also found that SMBs will increase IT security budgets from 9.1 percent of the IT operating budget in 2008 to 10.1 percent in 2009. The reports predict that enterprises will invest in IAM technologies over the next year, while SMBs will focus on implementing personal firewalls and host intrusion prevention systems. <http://www.darkreading.com/security/management/showArticle.jhtml?articleID=212700661>

Ankit Fadia Speaks on Cyber Terror Attack

CXOTODAY
12/17/2008

According to Ankit Fadia, a widely respected security and cyber terrorism expert, countries currently rely too heavily on technology and computers to carry out daily activities while cyber terrorists can make computers inaccessible for weeks or steal sensitive personal information such as bank accounts. Fadia discussed the cyber attacks in Estonia, saying that if the attacks there had taken place in India, the situation would be “unimaginable.” Fadia also said that police departments are not knowledgeable of cyber security basics.

http://www.cxotoday.com/India/News/Ankit_Fadia_Speaks_on_Cyber_Terror_Attack/551-96665-912.html

Congress' Computers Still Vulnerable, Cries Wolf

BY: TIM WILSON, DARK READING
01/07/2009

Rep. Frank Wolf (R-Va.) wrote that only a few Congressional members have attended the classified briefings that resulted, in part, from last year's attacks on his computers, supposedly originating in China. The computers of Wolf and seven other representatives were infected with a virus that removed files and monitored the



Keeping Cyberspace Professionals Informed

victim's e-mails and text messages. Wolf wrote to House Speaker Nancy Pelosi requesting that the briefings be made mandatory for all Congressional members. Wolf wrote, "I fear that members are no better informed than they were before."

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212701181>

Hacked Lawmaker Calls for Cyber Briefings

BY: SHANE HARRIS, NATIONAL JOURNAL
01/06/2009

Rep. Frank Wolf (R-VA.) told House leaders that only a few Congressional members had attended secret briefings that were meant to

educate members about cyber threats. Wolf wrote to House Speaker Nancy Pelosi, requesting that the briefings be made mandatory. Wolf also recommends that the meetings should address cyber threats to House information security, threats to members who are traveling abroad and measures that are being taken to improve security on House computer networks and devices. Wolf's chief of staff, Daniel Scandling, said that cybersecurity is "a serious issue, and we have got to have bipartisan participation."

<http://techdailydose.nationaljournal.com/2009/01/hacked-lawmaker-calls-for.php#more>

NORTHROP GRUMMAN
DEFINING THE FUTURE™

World-Class Cyber Solutions

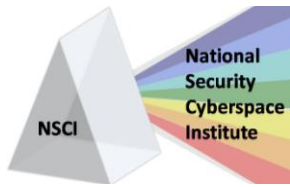
- Proven, complete understanding of the entire cyber environment
- Combined experience and value of classified & unclassified domains
- Accessible, distributed world-class cyber integration capabilities
- High-performance computing centers, labs, test ranges, and R&D facilities
- Measurable, repeatable cost-effective application of technology

Auditor: IRS Doesn't Check Cyberaudit Logs

BY: GRANT GROSS, PC WORLD (AU)
12/17/2008

The U.S. Internal Revenue Service's inspector general's office released a report which said that although the IRS has implemented intrusion detection systems and uses access controls for firewalls and routers, the agency

does not always review the system audit logs and that settings on some firewalls and routers do not comply with IRS rules. The report said that Internet intruders could potentially access sensitive taxpayer data on the IRS network. The report recommends that the IRS allow independent reviews of audit logs, implement procedures for saving audit logs, and regularly



test Internet gateways for compliance. According to IRS CIO, Arthur Gonzalez, the IRS has taken steps to correct the problems found in the report and is “aggressively implementing additional changes” to protect Internet gateways.

<http://www.pcworld.idg.com.au/article/271093>

Ethical hacking course launched

BY: BOBBIE JOHNSON, THE GUARDIAN

12/17/2008

The International Correspondence School is offering a distance-learning course in ethical hacking, which is often used by Internet security companies to combat computer crime. Ethical hackers focus on methods used by criminals and learn how to test computer systems for weaknesses that could lead to attacks. Ethical hackers can even perform fake attacks and penetration tests to evaluate the security of a client’s system. The course will teach students how to run denial-of-service attacks and social engineering tactics.

<http://www.guardian.co.uk/technology/2008/dec/17/internet>

Undersea Robot Searches for Severed Cables

BY: JAMES NICCOLAI, COMPUTERWORLD

12/22/2008

A robot submarine was used to search the Mediterranean Sea in hopes of locating the undersea cables that were accidentally cut Dec. 19, interrupting voice and Internet traffic. Jean-Bernard Orsoni, a spokesman for France Telecom, explained that the robot would find the ends of the cables and pull them to the surface for repairs. Voice and IP traffic was rerouted, but some communications were still affected due to network congestion. According to Keynote Systems, network availability dropped at one point to 72 percent, and network response times between India and the

rest of the world increased three or four times normal levels.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=16&articleId=9124163&intsrc=hm_topic

Hash contest moves on to mass free-for-all

SECURITYFOCUS

12/22/2008

The National Institute of Standards and Technology recently released 51 submissions that made the first cut in the competition for the next United States secure hashing standard. The current family of hash functions is cryptographically weak, leading the NIST to find a stronger replacement for the hash functions. The federal agency will host a conference based on the proposals in February, and the NIST will choose approximately 12 final contenders.

<http://www.securityfocus.com/brief/874>

NERC Releases Phase I Cyber Security Standards For Review

BY: PHIL LEGGIERE, HOMELAND SECURITY TODAY

12/30/2008

The North American Electric Reliability Corporation’s Cyber Security Standard Drafting Team recently released phase one of revisions to eight Critical Infrastructure Protection reliability standards for industry review. The standards aim to ensure that appropriate procedures are in place to protect critical infrastructure from cyber attacks. The revisions include wording changes to the standards outlined in the Federal Energy Regulatory Commission’s Order 706, which was originally released in January 2008. Other changes include removing “references to reasonable business judgment” from the standards.

<http://www.hstoday.us/content/view/6637/187>



New Open Standard Arrives For Gauging Security of Web Apps, Services

BY: KELLY JACKSON HIGGINS, DARK READING
12/29/2008

The Open Web Application Security Project has released an open industry standard for Web application and Web service security. Named "The Application Security Verification Standard (ASVS)", the standard is intended to assist users with a tool to assess the degree of security of their applications and to help security pros determine what security features need to be built in to the applications. The ASVS includes four levels of security verification and will help differentiate between those running tools and those doing detailed design-based analysis in their Web applications.

<http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=212700095>

Revised Phase I Cyber Security Standards Under Review by NERC

BY: THE NORTH AMERICAN ELECTRIC RELIABILITY CORP., TRANSMISSION AND DISTRIBUTION WORLD
12/16/2008

The North American Electric Reliability Corp.'s Cyber Security Standard Drafting Team recently released its proposed revisions to eight Critical Infrastructure Protection reliability standards for review and industry comments. The standards hope to ensure that utilities and other owners and operators of the bulk power system implement appropriate procedures to protect critical infrastructure from cyber attack. Phase I revisions include a specific compliance schedule for newly-identified critical assets; Phase II revisions are expected to include more thorough evaluations of the National Institute of Standards and Technology standards and risk management framework.

http://tdworld.com/customer_service/nerc-cyber-security-under-review-1208/

Commission to fund research on China's cyberwarfare capabilities

BY: BEN BAIN, FEDERAL COMPUTER WEEK
12/29/2008

Congress has established the U.S.-China Economic and Security Review Commission that will help analyze the capabilities of the Chinese government to conduct cyberwarfare. The Commission has released a request for proposals for a contract for an unclassified report which would identify the major players in China; identify different organizations and how they may be linked; evaluate the development of China's cyberwarfare doctrine; provide a timeline of Chinese-based hacking and intrusion incidents; and analyze the vulnerability of U.S. government computer systems and policy recommendations. Submissions are due by Jan. 21.

<http://fcw.com/Articles/2008/12/29/Commission-to-fund-research-on-Chinas-cyberwarfare-capabilities.aspx>

Thompson Files: Internet Threats – Part 1

BY: LOREN B. THOMPSON, UPI
12/24/2008

The article discusses the reliance of modern civilization on digital networks and the necessity of Internet-style communication in the global economy. The article points out that the Internet empowers everyone equally, including criminals and enemy foreign governments. The article also asserts that while the U.S. government has taken some steps towards combating digital threats, the current federal framework is flawed and will not be able to keep up with emerging technologies and threats. The Obama administration will have to examine current cybersecurity efforts closely to determine if additional resources should be allocated to addressing cyber threats.



http://www.upi.com/Emerging_Threats/2008/12/24/Thompson_Files_Internet_threats_-_Part_1/UPI-39201230128902/

Unleashing Hurricanes In Cyberspace: Part Five

BY: LOREN B. THOMPSON, SPACEWAR
01/02/2009

Experiments conducted by the Department of Homeland Security demonstrated some ways that hackers could penetrate utilities, however, no one really knows how much damage potential enemies are already capable of doing. The article also identifies attribution as a key challenge to addressing cybersecurity issues. In light of these challenges, experts fear that it is only a matter of time before hackers seriously damage the national economy. Security experts also warn that malicious software is generated

and launched on such a large scale that there is no immediate solution for the problem, even when a virus is detected. The article warns that while cyberspace makes complete regulation almost impossible, the federal government must find a way to combat cyber threats or risk losing a military and economic edge in the future. The article concludes with two "basic principles" of effective defense: First, users must be educated on risks and avoid creating vulnerabilities. Finally, access to sensitive networks must be restricted through limited entry points, traffic filtering and rigid authentication procedures.

http://www.spacewar.com/reports/Unleashing_Hurricanes_In_Cyberspace_Part_Five_999.htm
!

Intelligent Software Solutions



ISS is a leading edge software solution provider for enterprise and system data, services, and application challenges. ISS has built hundreds of operationally deployed systems, in all domains – "From Space to Mud"™. With solutions based upon modern, proven technology designed to capitalize on dynamic service-oriented constructs, ISS delivers innovative C2, ISR, Intelligence, and cyber solutions that work today and in the future. <http://www.issinc.com>.

Cyber Progress Often Lost in Translation

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES (LA.)
12/18/2008

The Cyber Innovation Center, operating temporarily at Bossier Parish Community College in Bossier City, is facing criticism from skeptics, partly due to the secrecy surrounding the center. State Rep. Jane Smith explains that it is hard to define what the center will do and how its customer base extends beyond the Air Force while respecting the classified nature of government and military business. Although the secrecy can be frustrating, CIC Executive Director Craig Spohn emphasizes that the center is having a positive impact on the local economy of Bossier City, citing the \$13 million

in outside federal spending in the region from the center. Spohn also believes that the return on investment in the center will continue through growth in the National Cyber Research Park. Spohn states that there are many interested tenants, although leasing in the new building will not begin until early 2009. Les Guice, Louisiana Tech's vice president for research and development, explains that the center is bringing together the military and academia which will lead to new collaborative opportunities and revenue.

<http://www.shreveporttimes.com/article/20081218/NEWS01/812180313>



Meyerrose to Head Cybersecurity at Harris

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
01/12/2009

Dale Meyerrose, former federal chief information officer, is joining Harris Corp. as vice president and general manager for cyber and information assurance and will oversee development of the contractor's new cybersecurity and information assurance business unit. Meyerrose will head strategy, business development and program execution for the new unit and will also be in charge of the new Harris Center for Information Assurance at the Florida Institute of Technology in Melbourne, Fla.

<http://fcw.com/articles/2009/01/12/meyerrose-to-head-cybersecurity-at-harris.aspx>

Lockheed, Boeing Tap \$11 Billion Cybersecurity Market

BY: GOPAL RATNAM, BLOOMBERG
12/30/2008

Military contractors and the world's largest defense companies, Lockheed Martin Corp. and Boeing Co., have dedicated new business units to defending U.S. government computers from cyber attacks. Boeing created its Cyber Solutions division in August, while Lockheed launched its cyber-defense operation in

U.S. Defense Contractors Look to Cyber Security Contracts

BY: NICK FARRELL, IT EXAMINER
01/02/2009

U.S. Defense contractors including Boeing, Lockheed, L-3 Communications and SAIC are setting up cyberdefense units in anticipation of budget increases for cybersecurity. It has been estimated that \$11 billion could be dedicated to cybersecurity projects by 2013. The article also claims that smaller computer security firms could benefit from budget increases because the big name defense contractors lack expertise in cyber defense.

<http://www.itexaminer.com/us-defence-contractors-look-to-cyber-security-cont>

October. Linda Gooden, executive vice president of Lockheed's Information Systems & Global Services unit, said that cyber is one of the federal budget's fastest growing areas, and that she expects cybersecurity to be a significant focus of the Obama administration. U.S. Rep. James Langevin (D-RI) said that developing cybersecurity mechanisms will be "a multiyear, multibillion-dollar project".

http://www.bloomberg.com/apps/news?pid=20601103&sid=an2_Z6u1JPGw

CYBERSPACE – PRESIDENT-ELECT OBAMA

Seeking Obama's Cyber Czar

BY: ANDY GREENBERG, FORBES
12/18/2008

The person who is appointed as Obama's National Cyber Advisor will have more authority to implement changes by working from the White House and reporting directly to Obama. The Cyber Advisor will continue work started by Bush's Cyber Initiative and work to stop intrusions of networks by foreign hackers. Some

believe that the position has already been informally offered to Paul Kurtz, a security consultant with Good Harbor Consulting.

http://www.forbes.com/technology/2008/12/18/cybersecurity-czar-obama-tech-security-cx_ag_1219cyberczar.html



IAC to Obama: Federal IT needs overhaul

BY: MATTHEW WEIGELT,
WASHINGTON TECHNOLOGY
12/17/2008

The Industry Advisory Council recently released several reports which said that the Obama administration must work to modernize the government which is traditionally “resistant to change, taking risks and innovation.” The IAC’s Transition Study Group met early in December with Obama’s transition team. Obama’s team

has begun reaching out to IT groups and is accepting papers on various IT topics from the IAC study group. The papers urge the new administration to take advantage of the \$100 billion annual federal IT investment to overhaul government policies and practices. The group recommends that the administration appoint a senior IT leader in the Executive Office.
<http://washingtontechnology.com/Articles/2008/12/17/IAC-to-Obama-Federal-IT-needs-overhaul.aspx>

CYBERSPACE – DEPARTMENT OF DEFENSE (DoD)

Pentagon Pushes Defense Companies to Strengthen Cyber Security

BY: GOPAL RATNAM, BLOOMBERG
01/09/2009

The pentagon is pushing U.S. defense companies to boost the security of their computer systems in order to better protect sensitive military information. The effort is part of the Pentagon's Defense Industrial Base Cyber Security Initiative and serves to advise contractors about emerging threats and suggest ways to tighten their security. Security breaches on U.S. and private-computer networks reported to the Department of Homeland Security doubled to almost 72,000 last year. The program will be a cooperative effort with all defense contractors involved.

relentless intrusions into government networks and widespread vulnerabilities.” General Raduege identified four stages in securing cyberspace, and said that we are past the first stage – ignorance of cyber attacks. According to Raduege, the second stage is awareness of attacks. The third stage, actualization, includes education and training, and cooperation to reduce network vulnerabilities. Raduege explains that the fourth stage, the “cyber mindset,” is when we think and act as warriors in cyberspace as we do in more traditional warfare domains.

<http://www.af.mil/news/story.asp?id=123129337>

Air Force Embraces Web 2.0

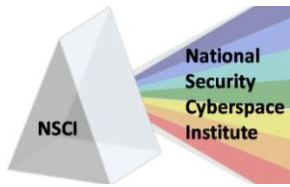
BY: SAM LAGRONE, AIR FORCE TIMES
01/11/2009

The Air Force is embracing Web 2.0 features like YouTube, Facebook and Twitter to improve its public reputation and fight enemy propaganda. Capt. David Faggard, chief of Emerging Technology, explains that using new media outlets allows the Army to instantly communicate its message publicly. Air Force airmen are now available on Facebook and the

Gen. Lorenz on Leadership: At War in Cyberspace

AIR FORCE LINK
12/23/2008

Retired Air Force Lieutenant General Harry Raduege Jr. said that the list of cyberspace challenges is “growing and endless” and includes “cybercrime, increasing identify theft, sophisticated social engineering techniques,



Keeping Cyberspace Professionals Informed

Air Force blog provides readers with free downloads. The Defense Department originally called for all services to expand their online presence in the 2004 Quadrennial Defense Review, and the AF Emerging Technology Office is developing an online policy that will provide airmen with blogging guidelines.

http://www.airforcetimes.com/news/2009/01/airforce_blog_rules_010909/

Classified Spillage

BY: BILL GERTZ, THE WASHINGTON TIMES
01/08/2009

According to a Navy report, the service branch is currently paying technology company EDS \$5 million each year to clean up "electronic spills" that occur when classified electronic

information is transferred to unclassified laptops and other machines. The report states that the Navy is experiencing an average of 36 electronic compromises per month, and that incident numbers are increasing. The report included details of an incident in October in which a Navy official scanned a classified document onto an unclassified network and then e-mailed the document to others. With an average price tag of \$11,800 for each electronic spillage, many question why the Navy is paying EDS almost ten times the cost of destroying and replacing every affected machine.

<http://www.washingtontimes.com/news/2009/jan/08/classified-spillage/>



CISCO

Cisco (NASDAQ: CSCO) enables people to make powerful connections-whether in business, education, philanthropy, or creativity. Cisco hardware, software, and service offerings are used to create the Internet solutions that make networks possible-providing easy access to information anywhere, at any time. Cisco was founded in 1984 by a small group of computer scientists from Stanford University. Since the company's inception, Cisco engineers have been leaders in the development of Internet Protocol (IP)-based networking technologies.

Today, with more than 65,225 employees worldwide, this tradition of innovation continues with industry-leading products and solutions in the company's core development areas of routing and switching, as well as in advanced technologies such as: Application Networking, Data Center, Digital Media, Radio over IP, Mobility, Security, Storage Networking, TelePresence, Unified Communications, Video and Virtualization. For additional information: www.cisco.com

Army Approves Cisco Wireless Package

BY: JOAB JACKSON, GOVT. COMPUTER NEWS
12/18/2008

The Army recently added the Cisco Unified Wireless Network package to its Information Assurance Approved Products List, following an

evaluation by the Army Information Systems Engineering Command. The package includes wireless network controllers, access devices and software for WLAN management. The Army requires its organizations to buy only products that appear on the approved list.

110 Royal Aberdeen • Smithfield, VA 23430 • ph. (757) 871-3578



<http://gcn.com/Articles/2008/12/18/Army-gives-green-light-to-Cisco-wireless->

[package.aspx](#)

CYBERSPACE – DEPARTMENT OF HOMELAND SECURITY (DHS)

Chertoff calls for less secrecy in cybersecurity

BY: ANDREW NOYES, CONGRESSDAILY
12/18/2008

Homeland Security Secretary Michael Chertoff said that the Defense Department and intelligence agencies should determine whether work with President Bush's national cybersecurity initiative can be declassified. Chertoff said that the American public needs to be engaged in cybersecurity efforts, and that Internet security thrives by collaboration and cooperation. Chertoff also said that the Obama administration will need to make public engagement a "core component of its cybersecurity plan."

http://www.nextgov.com/nextgov/ng_20081218_5010.php

After Six Years, Homeland Security Still Without 'Cybercrisis' Plan

BY: DECLAN MCCULLAGH, CNET NEWS
12/19/2008

Although cybersecurity was a primary focus of the U.S. Department of Homeland Security when it was created in 2002, the article claims that after six years and more than \$400 million in cybersecurity spending, DHS has still not been able to "gather and focus" cybersecurity efforts. DHS Secretary Michael Chertoff recently spoke at a conference in Washington, D.C., and said that DHS must develop a plan for responding to a cybercrisis. Many feel that there has been a lack of clear leadership in cyber efforts and a cybersecurity commission recommended that cybersecurity efforts be moved from DHS to the White House.

http://news.cnet.com/8301-13578_3-10127134-38.html

DHS and cybersecurity: Yes, no, maybe so?

BY: BILL BRENNER, NETWORK WORLD
12/17/2008

Cyber experts have recommended that cybersecurity be moved from the Department of Homeland Security to an office within the Obama White House. Members of the Commission on Cyber Security for the 44th Presidency said that leaving a cyber function with the DHS would "doom that function to failure." The commission also calls for government regulations to protect computer networks. Author Bill Brenner writes that it may be best to leave cybersecurity with the DHS. Brenner writes that DHS problems may be improved by a change in leadership and maturation of the agency. Brenner also says that the White House may not do a better job than the DHS of overseeing cybersecurity efforts.

<http://www.networkworld.com/news/2008/12/1708-dhs-and-cybersecurity-yes-no.html?hpg1=bn>

For your eyes only

BY: KATHLEEN HICKEY, GOVERNMENT COMPUTER NEWS
12/24/2008

The Department of Homeland Security has developed new privacy guidelines for its Science and Technology Directorate. Named "Principles for Implementing Privacy Protections in Science and Technology Research," the guidelines



Keeping Cyberspace Professionals Informed

incorporate privacy protections into sensitive research conducted by the directorate, while allowing it to provide advanced tools, technologies and systems related to homeland security. Data quality and integrity will ensure only accurate and appropriate data for the project is researched and data minimization will ensure that the least amount of information consistent with the purposes of the project is exposed.

<http://gcn.com/Articles/2008/12/24/DHS-develops-privacy-guidelines-for-Science-and-Technology-Directorate.aspx>

DHS Privacy Office: Fusion Centers Endanger Privacy

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK 12/23/2008

A report recently released by the Homeland Security Department's chief privacy officer claims that intelligence fusion centers that are

run by state and local law enforcement agencies could jeopardize privacy. The fusion center program was created by the DHS to improve information sharing between the department and state and local police. DHS' Privacy Office identified a number of problems including distrust from the public because law enforcement agencies share personal information with each other and federal officials. The report also found that the fusion centers do not have clear regulations for storing and sharing personal information, and recommends implementing consistent policies and training. The report also cited excessive secrecy, inaccurate information, data mining, and private-sector involvement as privacy concerns.

<http://fcw.com/Articles/2008/12/22/Fusion-centers-endanger-privacy.aspx>



High Tech Problem Solvers

www.gtri.gatech.edu

From accredited DoD enterprise systems to exploits for heterogeneous networks, GTRI is on the cutting edge of cyberspace technology. Transferring knowledge from research activities with the Georgia Tech Information Security Center, GTRI is able to bring together the best technologies, finding real-world solutions for complex problems facing government and industry.

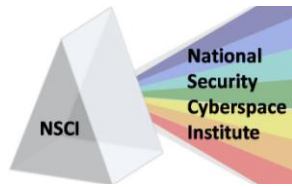
CYBERSPACE – INTERNATIONAL

Israeli-Palestinian Conflict Could Result In Increased Internet Hacking Attacks

SECURITY PARK
01/09/2009

Companies with any connections to the Middle East are being warned to be on guard against a malware or similar cyber attack resulting from

the conflict between Israel and the Palestine. Security expert Bruce Jenkins said attacks are no longer focused only on the Department of Defense or government organizations as hackers are moving to less suspecting targets. Jenkins warns that any company with an Internet connection and even vague ties to



either country involved could be attacked. Jenkins recommends taking extra precautions, including ensuring software patches are up-to-date and monitoring network traffic for unusual activity.

http://www.securitypark.co.uk/security_article_262478.html

Is Someone In China Reading Your Emails?

BY: MAURA MOYNIHAN, ALTERNET

01/12/2009

The article discusses the post-Olympic Chinese cyber-espionage campaign that has targeted government, military and civilian computer networks. According to 2008 press statements, the Pentagon reports a dramatic increase in Chinese cyber espionage before and after the Olympics. A report from the bipartisan U.S. China Economic and Security Review Commission, released in November 2008, concluded that "China is targeting U.S. government and commercial computers for espionage (and) is stealing vast amounts of sensitive information from U.S. computer networks." The article also includes examples of numerous attacks from China on classified U.S. networks in the past few years, including an attack on Congressional members' computers as recently as last summer. Finally, the article warns that Chinese military academies are rigorously training young workers in computer hacking. Larry M. Wortzel, the author of a 2007 U.S. Army War College report on Chinese cyber campaigns, provides the most frightening findings, stating: "The thing that should give us pause is that in many Chinese military manuals they identify the U.S. as the country they are most likely to go to war with. They are moving very rapidly to master this new form of warfare."

http://www.alternet.org/audits/119064/is_someone_in_china_reading_your_emails/

Ministries in Bulgaria and New Zealand Fight Computer Viruses

BY: LUCIAN CONSTANTIN, SOFTPEDIA NEWS

01/12/2009

The Bulgarian Interior Ministry and the New Zealand Health Ministry are experiencing an outbreak of viruses on their computer networks. The attacks started in the network of Sofia's Direction of Interior Affairs, and some parts of the infrastructure have had to be isolated while the Ministry cleans the virus from the network. Alan Hesketh, deputy director general of New Zealand's health information directorate, reported that the e-mail system was shut down to contain a virus outbreak in the Ministry's network. Security vendor Symantec is working with the Ministry to help contain the virus.

<http://news.softpedia.com/news/Ministries-in-Bulgaria-and-New-Zealand-Fight-Computer-Viruses-101676.shtml>

Waging a War With Bits and Bytes

BY: MAYANK TEWARI, DNA INDIA

01/11/2009

The article discusses the cyber war between India and Pakistan that started in May 1998, and is still occurring more than a decade later. The article also says that Indian authorities discovered cyber attacks from China two years ago, which India officially acknowledged as cyber warfare only in July 2008. According to officials at the Ministry of Information Technology, about 300 Indian Web sites are defaced on average each month. The article claims that most hackers involved are ordinary citizens, known as patriotic hackers, who take up hacking without any direct government go-ahead. Patriotic hackers primarily target government-run Web sites, usually only defacing the Web sites without actually gaining access to secure and crucial networks. India has,



however, also been the victim of more sophisticated threats. For example, the Ministry of External Affairs' networks were compromised by suspected Chinese hackers. These "serious network-related attacks" can cause significant damage to the infrastructure of the targeted nation and are usually carried out by groups that are either directly or discreetly funded by their government.

<http://www.dnaindia.com/report.asp?newsid=1220525>

Iranian Hackers 'Bring Down Mossad Web Site'

PRESS TV
01/07/2009

The Israeli secret service's Web site, used to voice solidarity with Gazans, has been brought down by a group of Iranian hackers. The group, known as Ashiyaneh, announced that they had carried out the attack against Mossad's Web site in protest of the ongoing Israeli assault on the Gaza Strip. The head of the Iranian group stated that the fact that the Web site could be hacked despite high security measures makes a mockery of the Israeli secret service agency.

<http://www.presstv.ir/detail.aspx?id=81123§ionid=351021701>

India's Cyber Warriors Are Volunteers

BY: NICK FARRELL, IT EXAMINER
01/07/2009

According to an article by DNA India, the cyber war between India and Pakistan is fought primarily by patriotic hackers – citizens who want to do something for their country, although they do not have direct government support. The article includes a discussion with a 26-year-old Indian software engineer who said that he puts in three hours of attacking sites and defending India online each night. The teams of hackers monitor vulnerabilities and publish confirmed worms and viruses for other hackers to use.

<http://www.itexaminer.com/indias-cyber-warriors-are-volunteers.aspx>

World Bank Admits Top Tech Vendor Debarred for 8 Years

BY: RICHARD BEHAR, FOX NEWS
12/22/2008

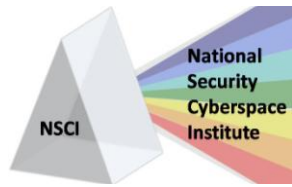
An official from the World Bank recently admitted that India-based information technology vendor Satyam Computer Services was barred from all business at the bank for eight years beginning in September of 2008. The debarment was reportedly imposed for "improper benefits to bank staff" and "lack of documentation on invoices." India's securities commission announced that it would investigate Satyam, and the case was turned over to the Justice Department and U.S. Treasury Department, although it is not known if a case against either Satyam or World Bank officials is being pursued by either agency. According to Fox News sources, investigators discovered spy software that had been installed on the bank's Washington headquarters by contractors from Satyam, but the bank denies that any breaches of its treasury unit have taken place.

<http://www.foxnews.com/story/0,2933,470964,00.html>

Uproar in Australia over plan to block Web sites

BY: TANALEE SMITH, THE ASSOCIATED PRESS
12/26/2008

Hundreds protested in state capitals earlier this month in opposition to a proposed Internet filter dubbed the "Great Aussie Firewall." The proposal would make Australia one of the strictest Internet regulators among democratic countries. Communications Minister Stephen Conroy proposed the filter earlier this year, following up on a promise of the year-old Labor Party government to make the Internet cleaner



and safer. The plan, which would have to be approved by Parliament, has two tiers. A mandatory filter would block sites on an existing blacklist determined by the Australian Communications Media Authority and an optional filter would block adult content.

http://news.wired.com/dynamic/stories/T/TEC_AUSTRALIA_INTERNET_FILTER?SITE=WIRE&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2008-12-26-11-40-17

The Big War You Never Hear Much About

STRATEGY PAGE

12/21/2008

According to the article, Shia and Sunni radicals have been launching cyber attacks on each other's Web sites for the past three months, starting with a Shia attack on two main Web sites for Sunni radical religious propaganda Sept. 11, 2008. The cyber war has drawn Arab and Iranian hackers that would not normally be involved in Islamic radicalism, and attacks are fueled by animosity between the Shia and Sunni sects that goes back almost a thousand years. Iran has also been working to unite Moslem hackers against Israel. The Hamas office in the capital of Iran has sponsored a hacking contest for two years now that awards the hacker who makes the "most spectacular attack" on important Israeli Web sites.

<http://www.strategypage.com/htmw/htwin/articles/20081221.aspx>

Undersea Cable Cuts Disrupt Internet Access

BY: ROBERT MCMILLAN, COMPUTERWORLD

12/19/2008

Telecommunications company, France Telecom, announced that Internet and telephone traffic between Europe, the Middle East and Asia was interrupted after underwater data lines were cut in December. An unnamed spokeswoman for France Telecom said that it would take two weeks to fix the cut lines, which she explained

may have been damaged by an earthquake or ship. Affected countries included India, Saudi Arabia, Egypt and Malaysia. Danny McPherson, chief security officer at Arbor Networks, said that his company's sensors found that between 3,000 and 5,000 Internet routes were offline because of the incident.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124093&intsrc=hm_list

Chinese spy scare sours Australia's plans for nationwide broadband

BY: AUSTIN MODINE, THE REGISTER

12/18/2008

The Australian recently reported that a frontrunner bid for building Australia's national broadband network from telecom provider Singtel Optus would be examined closely because of Singtel Optus's connections with Chinese networking firm Huawei Technologies. Optus confirmed that they have worked with Huawei in network tests. Security agencies fear that Huawei's government contract work outside of China could lead to cyber-espionage concerns.

http://www.theregister.co.uk/2008/12/18/huawei_optus_ties_nbn_security_concerns/

Israel Hacks Arab TV Station

BY: JOHN LEYDEN, THE REGISTER

01/06/2009

The latest phase in a war in cyberspace earlier this week involved Israeli military forces reportedly hacking into a Hamas-run TV station and substituting regularly-scheduled broadcasts with propaganda. Audiences have been treated to propaganda clips featuring the gunning down of Hamas leadership accompanied by a message in Arabic that said: "Time is running out." Former cyber attacks featured anti-Semitic children's cartoons and the bombing of Al-Aqsa's main studio by IDF planes. As part of the



huge upswing in attacks since the conflict began, radio has also been interrupted by such broadcasts.

http://www.theregister.co.uk/2009/01/06/idf_al_aqsa_hack/

Commonly Used Tools of the Chinese Hacker

BY: HEIKE, THE DARK VISITOR
01/11/2009

The article contains a short list of security software products produced in China that are commonly used by Chinese hackers. The tools include: Snow Trace, a password decoder; Chaotic Knife, a UNIX password analyzer; Sky Net, a firewall approved by the Ministry of Public Security; Glacier, a Trojan; Little Analyst, a monitoring software sniffer comparable to NetXray; and Fast Search, a port scanner that offers multiple thread search.

<http://www.thedarkvisitor.com/2009/01/commonly-used-tools-of-the-chinese-hacker/>

Pak Now Planning Attack on Indian Cyber Networks

SAMAY LIVE
01/06/2009

The article claims that Pakistani hackers are currently planning an attack on Indian computer networks in response to the Mumbai terror strikes. Pakistani hackers have created Web sites such as www.Songs.Pk that are infected with software that can be used to steal information from targeted computers. An expert in the Indian Home Ministry says that more than 12 lakh Indian users download software from the Web site daily, which puts those machines at risk of becoming Zombies controlled by the hackers. Experts speculate that these small virus downloads may be part of a "dry run" in preparation for a bigger attack. Government Web sites have also been heavily targeted by the Pakistani hackers, who use new variants of viruses that cannot be identified by most anti-virus software programs.

<http://www.samaylive.com/news/pak-now-planning-attack-on-indian-cyber-networks/603514.html>

design
develop
evolve
transition

ITT CORPORATION
Cyber Assurance Department
ADVANCED ENGINEERING & SCIENCES

Our goal is to design, develop, evolve and transition information technology solutions and provide engineering services in response to cross-domain information sharing, information assurance and cyber security requirements.

474 Pheonix Dr.
Rome, NY 13441
315 838 7000
aes.itt.com

 ITT



Pakistani Hackers Target Kalam's Group

BY: NICK FARRELL, IT EXAMINER

01/08/2009

A group of Pakistani hackers have targeted former president Abdul Kalam's Orkut community group Web site, and reportedly were able to obtain moderators' rights to the site. The hackers are known for defacing Indian Web sites, giving them a "Pakistani theme." The hackers posted a message on the main profile page which reads, "We, the people of India, apologizes to out Pakistani brothers and ISI for barbaric acts of terrorism like Mumbai and Gujrat which were originated and carried out by few citizens of India and supported by government of India." Vikas Sankrityayan, the owner of the RSS Rashtriya Swayamsevak Sangh community, claims that the hackers are being supported by the Pakistani government.

<http://www.itexaminer.com/pakistani-hackers-target-kalams-group.aspx>

Thousands of legitimate sites SQL injected to serve IE exploit

BY: DANCHO DANCHEV, ZDNET

12/17/2008

Chinese hackers recently launched massive SQL injection attacks that have affected more than 100,000 Web sites primarily targeting Asian countries with password-stealing malware. Statistics from Symantec found that China has been the most actively-targeted country by the IE exploit, although the attacks have been traced to Chinese hacking groups. The article claims that most Internet users have a false sense of security, and continue browsing the Internet with insecure browsers and ignoring the rest of the software on their computers as potential security risks.

<http://blogs.zdnet.com/security/?p=2328>

Pro-Palestine Vandals Deface Army, NATO Sites

BY: DAN GOODIN, THE REGISTER

01/10/2009

Hackers who oppose Israel's military action in Gaza have attacked and defaced thousands of Web sites, including the U.S. Army and the North Atlantic Treaty Organization Web sites. A group, which calls itself Agd_Scopr/Peace Crew, is claiming responsibility for the attacks and defacing the sites with anti-U.S. and anti-Israel slogans and pictures. According to researcher Gary Warner, the group has also attacked sites belonging to Microsoft, Shell, Harvard and Mercedes Benz under the name Terrorist Crew. The recent surge in cyber attacks has coincided with Israel's two week "assault on Gaza."

http://www.theregister.co.uk/2009/01/10/army_nato_sites_defaced/

Korea Plans Hacking Competition

BY: KIM TONG-HYUNG, THE KOREA TIMES

12/15/2008

The Korean Ministry of Knowledge and Economy recently announced a plan to invest 230 billion won (about \$168 million) through 2013 for research and development in network security and convergence technologies and training for about 3,000 security experts. The government will invest in three key areas: network security; physical security systems; and convergence technologies. Korea will also host an international hacking competition as a part of the training process for 1,000 ethical hackers in Korea.

http://www.koreatimes.co.kr/www/news/biz/2008/12/123_36163.html

Hackers Take Battle with Hamas to Cyberspace

BY: NOA PARAG, GLOBES [ONLINE]

01/05/2009

Help Israel Win, an Israeli Internet initiative, is looking for recruits to participate in crashing



hostile Web sites by downloading a file that overloads and crashes Hamas servers. About 5,000 people have joined the initiative so far. Another site, Winnet, is offering a similar campaign that provides links to Hamas Web sites and asks surfers to enter the sites and post messages in Hebrew, English and Arabic that read, "We won't surrender to terrorism." Pro-Palestinian hackers have continued to attack Israeli Web sites, including recent attacks on the site of Israel Discount Bank and the English edition of the daily "Yediot Ahronot."

<http://www.globes.co.il/serveen/globes/DocView.asp?did=1000413534&fid=1725>

DECT Phones and POS Terminals Are Vulnerable

BY: PETER JUDGE, TECHWORLD
01/05/2009

German security experts have developed new technology that can break into wireless phones, debit card terminals and security door mechanisms. The attack, which will be effective against even the next generation version of DECT, called CAT-iq, allows hackers to bypass encryption to intercept phone calls and information which is then digitally recorded. Andreas Schuler, of the Dedected group, said that phone manufacturers often prioritize interoperability over security, which leaves mobile devices vulnerable to attacks. The Dedected group is currently working to reverse-engineer the DECT encryption system, which many experts feel should be replaced with GSM and 3G encryption.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=108996>

Iranian Hackers Attack Israeli Web sites

BY: AHARON ETENGOFF, IT EXAMINER
01/02/2009

According to Applicure Technologies, the number of hacking attempts against Israeli Web

sites has significantly increased with the continuation of the Israel Defense Forces' Operation Cast Lead in the Gaza Strip. Applicure founder and CTO David Allouch said that the attacks are coming from Iranian organizations and some organizations associated with Syria and Hizbullah. Allouch said that the hackers are trying to crash as many Web sites as possible "irrespective of their strategic importance." The attacks pose a threat to many countries, including the United States. Russian hackers were recently blamed for a malware attack against CENTCOM (U.S. Central Command), which is responsible for coordinating U.S. operations in Iraq and Afghanistan. The attack, which came from a malware application identified as Agent.bz, reportedly affected computers in combat zones and forward operating bases and brought down a highly protected classified network.

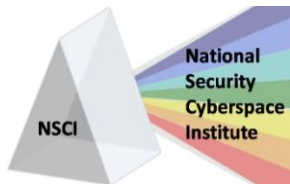
<http://www.itexaminer.com/iranian-hackers-attack-israeli-websites.aspx>

Hundreds of Israeli Web sites Hacked in 'Propaganda War'

BY: KELLY JACKSON HIGGINS, DARK READING
12/31/2008

According to Gary Warner, director of research in computer forensics at the University of Alabama at Birmingham, hundreds of Israeli Web sites have been attacked and defaced with anti-Israeli and anti-U.S. messages since Israel's bombing of Gaza. Warner warns that U.S. Web sites could also suffer from similar attacks. In his blog, Warner explains that these types of attacks, which are part of a propaganda campaign, focus on a site's location rather than size or prominence. Warner recommends that webmasters check their site contents each day for tampering and regularly install security patches.

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212700313>



With Gaza Conflict, Cyberattacks Come Too

BY: ROBERT MCMILLAN, COMPUTERWORLD
12/31/2008

Thousands of Web sites were defaced by hacking groups from Morocco, Lebanon, Turkey and Iran, coinciding with the recent conflict in Gaza between Israel and Palestine. Victims were primarily small businesses and pages hosted on Israel's Internet domain space. Some defaced sites include messages condemning the U.S. and Israel and graphic pictures of the violence. Gary Warner, director of research in computer forensics with the University of Alabama at Birmingham, said that Israeli government sites have been targeted, but were not successfully attacked. Warner explained that the online attacks began soon after Israel launched air strikes into Gaza in response to rocket attacks, and estimates that about 10,000 Web pages have been hacked.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124658>

Government to allow private firms to monitor every move we make. I'm moving to China.

BY: MIKE BUTCHER, TECH CRUNCH
12/31/2008

Proposed regulation in the UK would implement a communications database that would track every move a user makes on the Internet, every call, text message and every transaction. While the government claims that it will not look at the content of the transactions, simple daily routines of checking e-mails, visiting Web sites and making purchases online will build up a pattern of recognition about our Internet movements. The regulation would utilize private firms to maintain the data.

<http://uk.techcrunch.com/2008/12/31/government-to-allow-private-firms-to-monitor-every-move-we-make-im-moving-to-china/>

CYBERSPACE RESEARCH

NSA Patents A Way to Spot Network Snoops

BY: ROBERT MCMILLAN, NETWORKWORLD
12/20/2008

The U.S. National Security Agency has patented software which measures the time the network takes to send different types of data, and then provides an alert if something is taking longer than expected. Tadayoshi Kohno, assistant professor of computer science at the University of Washington, explains that the NSA patent is unique because it takes into account differences between the network layers. The software could, for example, detect a fake phishing Web site that intercepts data between a user and the legitimate site. Critics, like security researcher Dan Kaminsky, are

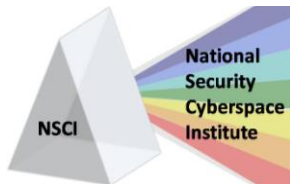
concerned that the software could raise a red flag even if the user just happens to route through a slower network path.

<http://www.networkworld.com/news/2008/12/2008-nsa-patents-a-way-to.html?fsrc=rss-security>

Network Security Against Today's Threats

BY: SAMARA LYNN, CHANNELWEB
01/09/2009

Over the past several months, the CRN Test Center has performed analysis of routine network threats through a honeynet. The Center found that there was a surge of attacks against the SQL database toward the end of 2008, and that at times there was almost



continuous port scanning by hackers hoping to find an entry to the data center. The article asserts that the most secure infrastructures do not rely on a single network security technology, but rather utilize a multilayered comprehensive strategy. The article discusses key network vulnerabilities based on the analyzed threats and also looks at key products that can help protect networks from malicious attacks. The featured security products focus on one or more of the key areas of a typical corporate network that the Center identified: database security; intrusion detection/protection; end-point control; and malware and Web content management.
<http://www.crn.com/security/212701657;jsessionid=MG2BLP0L3ISR4QSNLPCCKHSCJUNN2JVN>

Mobile Operators Anticipate Increased Spam Attacks But Are Slow to Protect

SECURITY PARK
01/04/2009

A recent survey from Cloudmark found that the top 12 European mobile operators expect an increase in spam as mobile social networking and e-mail use increases. Although 100 percent of the operators anticipate the increase, only 16 percent are evaluating ways to best guard against spam attacks. The mobile operators reported that up to 20 percent of their users experience mobile SMS spam and 83 percent of the operators have no filtering system currently in place. Neil Cook, head of technology services EMEA, Cloudmark, emphasized the importance of operators implementing security solutions to prevent losing customers because of spam messages. Cook also warned that operators should make messaging security a top priority now, before the spam attacks lead to identity theft, fraud and phishing attacks.
http://www.securitypark.co.uk/security_article_262416.html

Researchers Point Out XSS Flaws On American Express Site

BY: TIM WILSON, DARK READING
12/22/2008

Researchers recently found new XSS vulnerabilities on the American Express Web site which could compromise personal information of American Express customers. The vulnerability is caused by an input validation deficiency and can be used to harvest session cookies and inject iFrames which exposes Amex site users to attacks including identity theft. Security researcher Russell McRee said that the vulnerability violates the PCI Data Systems Security guidelines that American Express helped to create, and claims that American Express did not respond to his warnings about the flaw. An Amex spokesperson told The Register that the company is looking into the vulnerability reports.
<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212501694>

Researchers seek advanced network prioritization, security technology

BY: LAYER 8, NETWORK WORLD
12/23/2008

The Defense Advanced Research Projects Agency (DARPA) wants to develop a "self-configuring network technology" that would allow administrators to identify traffic, reallocate bandwidth between users, and automatically make quality of service decisions. The system would have 32 levels of prioritization that would be changeable at the system level. The system is part of DARPA's Military Networking Protocol program, which aims to develop an identification system for military and government data networks. The article includes a more detailed description of the technology from DARPA.



<http://www.networkworld.com/community/node/36633>

DARPA Unveils Cyber Warfare Range

BY: DAVID A. FULGHAM, AVIATIONWEEK.COM
12/30/2008

The Defense Advanced Research Projects Agency has approved funding for a new program called the National Cyber Range. Rance Walleston, director of BAE Systems' Information Operations Initiative said that the program will provide an environment to simulate anticipated cyber challenges and experiment with new tools and techniques. Walleston explained that the range will provide isolation and an infrastructure that can be attacked for analysis. Walleston says that the range's ability to upgrade and change with emerging threats will be a prominent challenge for contractors.

http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/DARPA12308.xml&headline=DARPA%20Unveils%20Cyber%20Warfare%20Range

DARPA Leads Game-Changing Cyber Innovation

GOVTECH.COM
01/12/2009

The Comprehensive National Cybersecurity Initiative is "beginning full execution" starting with the contracts awarded under the Defense Advanced Research Projects Agency National Cyber Range program. The National Cyber Range program will include collaboration with private-sector partners to develop "real-world simulation environments" where organizations can develop and test new technology concepts and capabilities. The total value of all awarded contracts is about \$30 million, which was awarded to BAE Systems, General Dynamics, John Hopkins University, Lockheed Martin, Northrop Grumman, Science Applications

International Corp. and SPARTA. Each contractor will oversee a team of businesses, universities and federal laboratories. DARPA Director Dr. Tony Tether said that the program is a "crucial component of the CNCI" and demonstrates the government's focus on technological innovation.

http://www.govtech.com/gt/print_article.php?id=583579

Rolls-Royce To Work On Electric Cyber Raygun Aero-Tech

BY: LEWIS PAGE, THE REGISTER
01/08/2009

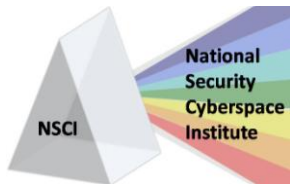
According to reports from Flight International, the U.S. Air Force Research Laboratory has awarded a \$690,000 contract to Rolls-Royce's North American Technologies unit as part of the Integrated Vehicle Energy Technology (INVENT) program. The Air Force is evaluating subsystem technologies to make future aircraft more electric in nature. Specifically, the USAF wants to find ways to generate larger amounts of electricity from jet-engine prime movers, improve electrical actuator system performance, and transfer to electric power rather than hydraulics for operating plane control surfaces. Combat planes are expected to eventually feature high-power radars and jammers which could reach out electronically, making the planes more advanced "cyber weapons."

http://www.theregister.co.uk/2009/01/08/rolls_juice_jet_tech/

SANS Releases List of Top 25 Most Dangerous Programming Errors in Software

BY: KELLY JACKSON HIGGINS, DARK READING
01/12/2009

A number of global security organizations including Apple, Microsoft, Symantec, RSA, CERT, Mitre, Oracle, DHS and the NSA have created a list of the 25 most dangerous



programming errors in software, and recommendations for how to mitigate the coding errors. Steve Christley, who leads the Common Weakness Enumeration (CWE) project for Mitre, explains that the Top 25 list is meant to help customers evaluate their security software programs and identify the most important weaknesses to address. The project also aims to provide developers with a set of guidelines for writing more secure code by avoiding common errors. Flaws that made the list are separated into three categories: insecure interaction between components; risky resource management; and porous defenses. <http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=21280020>
[2](#)

Many RFID Cards Poorly Encrypted

HEISE SECURITY UK

01/01/2009

According to security investigator Karsten Nohl, many RFID smartcards are vulnerable to attacks because of weak encryption systems. RFID cards that are used to control access to buildings, cars and electronic devices, use mifare chips that are also widely used in payment systems. Nohl explains that the manufacturers of the chips often neglect encryption standards. Nohl used the Mifare Classic card to demonstrate how the chips' encryption could be easily bypassed with simple proxy or relay attacks. Nohl also said that the RFID chips are practically defenseless against more sophisticated cryptographic attacks. Nohl recommends that the manufacturers of RFID solutions implement standardized encryption algorithms and protocols, and develop tested norms for secure RFID.

<http://www.heise-online.co.uk/security/25C3-Many-RFID-cards-poorly-encrypted--/news/112336>

Microsoft: MD5 hack Poses No Major Threats to Users

BY: GREGG KEIZER, COMPUTERWORLD

12/30/2008

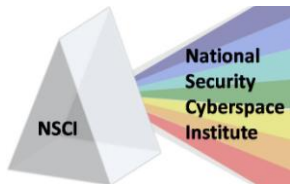
In a security advisory, Microsoft Corp. responded to the recent disclosure of an exploit in the MD5 hashing algorithm, saying that the flaw does not significantly increase risk to customers because the details of the attack are not published and no actual attacks using the techniques have been discovered. Microsoft also said that most certificate authority vendors no longer use MD5 but have upgraded to the more secure SHA-1 algorithm. Microsoft did recommend that users keep Windows updated with regular software patches. Jonathan Nightingale, a security issues spokesman for Mozilla, said that Mozilla has not seen any actual attacks exploiting the flaw, but recommends that users exercise caution when visiting sites that require personal information. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124564>

Internet Needs Global Regulation, Says Researcher

BY: JOHN E. DUNN, TECHWORLD

12/22/2008

Mary Landesman of ScanSafe says that the Internet needs global regulation to stop scams such as security 'scareware.' Landesman says that addressing scams as they arise makes it simple for criminals to keep up with security developments. Landesman emphasizes the effectiveness of 'scareware' scams as hackers are using increasingly sophisticated attacks to lure victims into downloading malicious software. Because there is no individual body responsible for investigating rogue ISPs, it may take months for the ISPs to be de-peered. Landesman acknowledges that the FTC has



been making progress recently, but says that there is still much to be done in the regulation of bogus scams.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=108714>

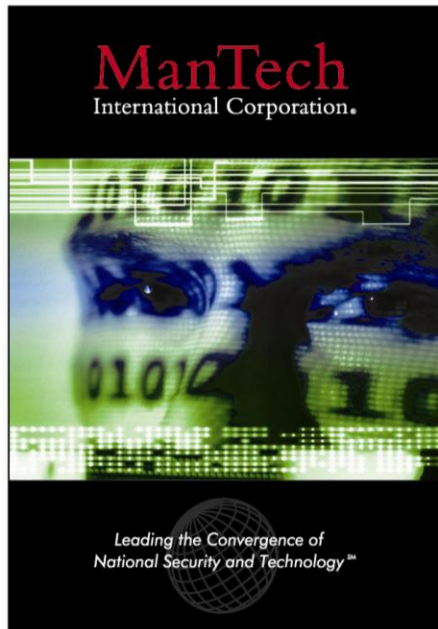
Software [In]security: Software Security Top 10 Surprises

BY: GARY MCGRAW, BRIAN CHESS AND SAMMY MIGUES, INFORMIT
12/15/2008

InformIT interviewed nine executives from financial services, independent software vendors, and technology firms that currently run top software security programs to gather information on the programs. InformIT is still in

the process of analyzing the data they gathered, and will release a maturity model based on the analysis. The article discusses the top 10 most surprising findings from the interviews including: the lack of widespread use of web application firewalls; the harmful effects of bad software security metrics; the lack of understanding of how attacks actually work and who hackers are; and the decreasing role of penetration testing in all nine practices. The article discusses these findings and the other top 10 surprising finds in detail.

<http://www.informit.com/articles/printerfriendly.aspx?p=1315431>



ManTech's Cyber Solution Center Helps Combat Threats to our National Infrastructure

ManTech International Corporation is a leading provider of innovative technologies and solutions for mission-critical national security programs for the Intelligence Community; the departments of Defense, State, Homeland Security and Justice; the Space Community and other U.S. federal government customers. It has recently established a Cyber Solution Center that marshals expertise from across the company to help the U.S. government and private industry fight the increasing threats to our IT and communications infrastructure. ManTech has been providing cyber operations services to the U.S. government and private industry for 11 years and its cyber security professionals have authored books and articles on honeypots (catching hackers), service oriented architecture security and network security monitoring. They have also taught for leading cyber security education providers such as SANS, Foundstone, USENIX, HTCIA and Black Hat. For additional information on ManTech's Cyber Solutions contact Mark Root at: mark.root@ManTech.com



IT Operations, Security Pros at Odds Over Virtualization Risks

BY: ELLEN MESSMER, NETWORK WORLD
12/18/2008

Research firm Ponemon Institute recently released the 2009 Security Mega Trends Survey, which found that about two-thirds of IT staff members felt that the virtualization of computer resources did not increase information security risks, although two-thirds of information security professionals felt that virtualization did increase risk. Nelson Martinez, systems support manager for the City of Miami Beach, says that the security for virtualization is “way, way behind” and believes that there are both performance and maintenance issues that need to be worked out. The 825 respondents to the survey in IT operations, and the 577 information security professionals who responded agree that the “inability to properly identify and authenticate users to multiple systems” is the most prominent risk associated with virtualization.

<http://www.networkworld.com/news/2008/12/1808-security-survey.html>

44 Percent of SMBs Have Been Attacked by Cyber Criminals

BY: GREG DAY, SECURITY PARK
12/19/2008

A recent survey by the GetSafeOnline initiative found that 44 percent of Europe’s small and medium-sized businesses (SMBs) have been attacked due to the businesses’ increasing dependence on technology. Small and medium-sized businesses suffer greatly from viruses, hackers, spyware and spam because of more restrictive security budgets and fewer back-up support options than larger businesses. The survey also found that 56 percent of SMBs feel that they would not be targeted by cyber criminals, and 90 percent believe that they are adequately protected from cyber threats. McAfee also recently conducted a research report, called ‘Does Size Matter?’ to identify the risks facing small businesses and found that average SMBs dedicate only an hour a week to IT security. The article provides some general security tips for SMBs which include: never opening email attachments and downloads; exercising caution with emails from unknown sources; deleting chain and junk emails; continually updating anti-virus software; backing up company files; and protecting credit card and password information.

http://www.securitypark.co.uk/security_article_262430.html

CYBERSPACE 2009 PREDICTIONS

Four Threats for '09 That You've Probably Never Heard Of (Or Thought About)

BY: KELLY JACKSON HIGGINS, DARK READING
12/31/2008

The article discusses large-scale Internet threats including Internet infrastructure attacks, radical extremist hackers, attacks that affect online ad

revenue and the possibility for human casualties resulting from cyberattacks that could trickle down to affect organizations in 2009. The article explains that organizations are more likely to experience hacks from insider threats, Web 2.0, and targeted attacks, but says that organizations should be aware of the larger

110 Royal Aberdeen • Smithfield, VA 23430 • ph. (757) 871-3578



possible security risks. The article discusses the four examples of large-scale Internet threats in detail, including what effect these events could have on individual organizations.

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212700328>

Securing IT Networks Cheaply in the New Year

BY: FORTINET, DIRECTOR OF FINANCE ONLINE
12/22/2008

Fortinet predicts the economy will have a significant effect on IT security trends in 2009. Although corporate network security will still be a high priority, companies will need to make purchasing decisions “on a need-to-have vs. nice-to-have basis.” The article also includes Fortinet’s “Top 9 in ‘09” security trend predictions which are: an increase in integrated security appliances; a greater emphasis on database security and compliance; an increase in Web 2.0 vulnerabilities; an increase in high speed security protocols; more opportunity for attacks against mobile devices; changes in programs and incentives for security professionals; an increase in targeted attacks using custom malware; and unification of law enforcement agencies.

<http://www.dofonline.co.uk/management/securing-it-networks-cheaply-in-the-new-year-120822.html>

2009 Security Predictions: Déjà vu All Over Again

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD
12/18/2008

Most security vendors’ predictions for 2009 include spikes in spam, phishing, botnet and malware volumes and an increase in attacks against mobile applications. The article discusses some of the predictions that were most common from security vendor predictions. According to Web app security vendor Websense, more than 80 percent of all

malware in 2009 will be hosted on legitimate sites and hackers will increasingly use a distributed model for botnets which makes the malicious Web sites easier to move and harder to shut down. MessageLabs, a Symantec company, predicts that phishing attacks against social networking site users and smart phone users will become more sophisticated, especially in attacks that utilize free application downloads and games. The article discusses common predictions, including the growth of distributed Denial of Service attacks and the increase of attacks on SCADA systems.

<http://www.networkworld.com/news/2008/12/1808-2009-security-predictions-deja-vu.html?hpg1=bn>

On botnets, encryption and mega-worms: Security predictions for 2009

BY: ANDREAS ANTONOPOULOS, NETWORK WORLD
12/30/2008

Andreas Antonopoulos predicts what will be the security trends for 2009. Antonopoulos believes that host-based security will become the focus in 2009 with the release of Windows 7 and continued interest in Mac OS which both focus on operation-system and endpoint security. He also predicts that mobile security concerns will continue to increase, and encryption requirements and solutions to mobile security concerns will be developed. Antonopoulos believes that there will be an increase in the spread of “super-stealthy” malware and the development of new, larger and more dangerous botnets. Finally, he predicts regulatory compliance will be a focus and security projects will struggle for funding.

<http://www.networkworld.com/columnists/2008/123008antonopoulos.html>



Encryption Top IT Security Initiative in 2009

BY: ELLEN MESSMER, NETWORK WORLD
01/05/2009

According to a recent Forrester Research survey of North American and European IT and security managers, security budgets will increase to 12.6 percent of the entire IT operating budget in 2009, up from 11.7 percent in 2008. Forrester's report, "The State of Enterprise IT Security: 2008 to 2009" also found that 20 percent of IT security funding will go to security outsourcing, consultants and services. Another 18.5 percent will go towards new security initiatives. The report said that full-disk encryption and file-level encryption were identified as the top security technologies that organizations will be piloting or adopting this year. Respondents identified "cost and business justification" and "complexity of architectural efforts needed" as the biggest challenges for data security.

<http://www.networkworld.com/news/2009/01/0509-forrester-it-security.html>

Cyber Attacks on Infrastructure Systems to Escalate: VeriSign

RESELLER NEWS
01/07/2009

The recently-released 2009 Cyber Threats and Trends report from infrastructure provider VeriSign claims that critical systems will become a primary target of cyber attacks, and that hackers will exploit the global financial crisis in their attacks. Jason Greenwood, VeriSign vice president and general manager, said that the rise of professional cyber criminals using sophisticated online fraud for financial gain is a sign of a new era of online security threats. The report also predicts an increase in attacks on critical infrastructure systems in 2009, and warns that Middle Eastern cyber criminals may increase fraud operations online to raise money to support their political agendas. Intelligence Director Rick Howard says that the increasing use of mobile phones, virtual worlds and interconnection of devices will provide hackers with new attack opportunities.

<http://reseller.co.nz/reseller.nsf/news/B1B397867DC0E00ACC2575360074E941>

CYBERSPACE 2008 IN REVIEW

PC Tools: Top Internet Blunders of '08

BY: PC TOOLS, DARK READING
12/29/2008

Security software vendor, PC Tools, recently released a list of the Top 5 Internet Blunders of 2008, and also predicted the types of Internet threats and trends that are expected in 2009. The article discusses in detail each of the top five blunders including the breach of the Epilepsy Foundation's Web site, the infection of NASA laptops and the discovery of a flaw in the Internet's core infrastructure. The article predicts that hackers will target Internet users

most affected by the economic crisis in 2009, and PC Tools also says that clickjacking and social engineering threats will be big trends in 2009.

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212700075>

The Five Coolest Hacks of 2008

BY: KELLY JACKSON HIGGINS, DARK READING
12/17/2008

Dark Reading chose five of the most unusual or bizarre hacks from 2008 which were all carried out by security researchers. The first hack is



from researcher Nate Lawson, who cloned the FasTrak toll tags used for pre-paying highway tolls in the San Francisco Bay Area. Lawson found that the tags did not use encryption at all, and said that he was surprised that they had not been cloned and sold already. Researchers Nitesh Dhanjani and Akshay Aggarwal researched how online activity can be used for intelligence gathering and influencing a user's behavior. Another pair of researchers used an iPhone to collect security information on a WiFi network. Researcher Rich Smith discovered and

demonstrated a "permanent denial-of-service" attack that requires a system to be completely reinstalled or replaced. Finally, a U.K. researcher built the Gecko device, which intercepts a user's authentication entry data and gives the attacker the user's entry credentials. The article discusses each attack further and details the lessons that we can learn from each.

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212500902>

CYBERSPACE HACKS AND ATTACKS

Hacker's Choice: Top Six Database Attacks

BY: KELLY JACKSON HIGGINS, DARK READING
05/08/2008

According to many experts, many enterprise databases are still not properly secured, allowing hackers to use "shockingly simple" attacks such as password exploitation to break into databases. Noel Yuhanna, principal analyst with The Forrester Group, explains that typical databases have thousands of connections per second, which makes it difficult to detect database attacks. Slavik Markovich, CTO of database security vendor Sentrigo, says that database configuration is usually so weak,

hackers do not even need to use buffer overflow or SQL injection attacks to break into databases. The article examines six popular database hacks which often exploit simple weaknesses in database organization. Each of the six hacks is discussed in detail and include: brute-force password cracking; privilege escalation; exploitation of unnecessary database services; targeting unpatched vulnerabilities; SQL injection; and stolen backup tapes.

<http://www.darkreading.com/security/encrypton/showArticle.jhtml?articleID=211201064>

Reply-all E-mail Storm Hits State Department

BY: MATTHEW LEE, ASSOCIATED PRESS
01/11/2009

An unclassified cable sent last week by Under Secretary of State for Management, Patrick Kennedy, warned State Department employees of "disciplinary actions" for using the "reply to all" function to reply to e-mails with large distribution lists. The cable explained that employees hitting "reply to all" on e-mails with several thousand recipients had caused an e-mail storm on the department's e-mail system.

Department e-mail had been interrupted because of the large volume of e-mails.

http://hosted.ap.org/dynamic/stories/S/STATE_DEPARTMENT_E_MAIL?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT

American Express Web Bug Exposes Card Holders

BY: DAN GOODIN, THE REGISTER
12/16/2008

Security researcher Russell McRee recently exposed a vulnerability on the American Express Web site that puts site users at risk and



violates industry regulations after receiving no response from American Express regarding the flaw. The vulnerability, a cross-site scripting (XSS) error, allows hackers to steal authentication cookies from users, granting the hackers access to customer accounts. XSS vulnerabilities allow hackers to inject malicious code into legitimate Web sites and steal cookies and passwords through spoof sites. The article claims that the American Express vulnerability resulted from a lack of input validation. Since the publication of this article, American Express patched the flaw.

http://www.theregister.co.uk/2008/12/16/american_express_website_bug/

Major Bug Opens All Browsers to Phishing Attack

BY: ROBERT MCMILLAN, TECHWORLD
01/13/2009

Researchers at Trusteer report that a bug in major browsers could help criminals obtain online banking credentials through a new attack called 'in-session phishing.' In-session phishing replaces traditional phishing e-mails with pop-up browser windows in legitimate Web sites that ask victims to enter password and login information. Amit Klein, Trusteer's chief technology officer, said that a bug in the JavaScript engines of many widely-used browsers help to make the attack seem more believable. Klein also explains that hackers launch the pop-up windows while the victim is logged into a financial institution Web site, which makes the message seem more legitimate.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=109445>

Researcher Releases Free DoS Hacking Tool

BY: KELLY JACKSON HIGGINS, DARKREADING
12/16/2008

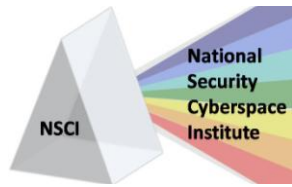
Italian researcher Aciri Emanuele recently released a package of tools that include a free denial-of-service (DoS) hacking tool for flooding TCP sessions. Emanuele said that he had some doubts about releasing the penetration testing tool to the public, because the tool allows users to crash a server with slow connections without using botnets. Other tools in the Complemento package include a domain scanner and an HTTP server scanner, banner grabber and data retriever.

<http://www.darkreading.com/security/attacks/showArticle.jhtml;jsessionid=XAP3DSE4VNFYSQ.SNDLPSKHSCJUNN2JVN?articleID=212500752>

'Huge Increase' In Worm Attacks Plague Unpatched Windows PCs

BY: GREGG KEIZER, COMPUTERWORLD
01/12/2009

Ryan Sherstobitoff, chief corporate evangelist at Panda Security, said that there has been an increase in malware samples and infections from the "Conficker.c" worm, leading Panda to increase its Global Threatwatch to "orange" status, meaning the company believes that users face "an important danger." The worm exploits a flaw in the Windows Server service that is included as part of all versions of Microsoft's operating system. According to Sherstobitoff, the worm looks for PCs that have not been patched, but can also be spread through brute-force attacks, and by passing from infected PCs to USB-based devices. Once on a PC, the worm replicates and downloads new versions of itself from malicious Web sites. Security firm Symantec Corp. estimates that about 3 million PCs have been infected by the worm.



<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125737>

Congress Hacked Again

STRATEGY PAGE
12/28/2008

Congress members recently found that their office PCs and networks had been infected with software that was monitoring PC use and reporting back to the hackers. The White House computer networks were under “constant attack” in November 2008, but no details of those attacks have been released. Still, many experts believe that the attacks on the White House networks originated in China. The article explains that government officials usually do not release details of attacks on government networks, presumably so that hackers will not know they are being monitored.

<http://www.strategypage.com/htmw/htiw/articles/20081228.aspx>

Researchers Hack VeriSign’s SSL Scheme for Securing Web Sites

BY: ROBERT MCMILLAN, COMPUTERWORLD
12/30/2008

An international team of security researchers discovered a way to undermine algorithms that protect secure Web sites, which could allow hackers to launch undetectable phishing attacks. The researchers exploited a flaw in the MD5 hashing algorithm that is used to create digital certificates for secure Web sites, and were able to hack VeriSign Inc.’s RapidSSL.com certificate site, allowing the researchers to create fake digital certificates for any Web site on the Internet. The researchers presented their findings at the Berlin hacking conference, Chaos Communication Congress, in December. Cryptography expert Bruce Schneier said that with the amount of research into MD5, upgrades to more secure algorithms should

have been made years ago. Tim Callan, vice president of product marketing for VeriSign, said that RapidSSL.com will no longer issue MD5-based digital certificates starting at the end of January and will encourage its customers to move to new certificates.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124558>

Hacker Leaves Message For Microsoft in Trojan Code

BY: ROBERT MCMILLAN, COMPUTERWORLD
01/12/2009

A French security researcher discovered a message from a Russian hacker to Microsoft on a variation of a Trojan program that victims are tricked into installing. The message reads, “Just want to say ‘Hello’ from Russia. You are really good guys. It was a surprise for me that Microsoft can respond to threats so fast.” The Trojan was a variation of the Win32/Zlob virus – one of the most common types of Trojan programs used to attack Microsoft. The hacker had also sent a note to Microsoft’s security group last year, saying, “I want to see your eyes the man from Windows Defender’s team.”

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125745>

Storm Worm Botnet Cracked Wide Open

HEISE SECURITY
01/09/2009

The Storm Worm botnet infected more than 1 million computers over the last two years through peer-to-peer techniques for finding new servers. Even after a clean-up attempt with Microsoft’s Malicious Software Removal Tool, experts believe that around 100,000 drones still remain. A team of researchers from Bonn University and RWTH Aachen University dissected the Storm Worm botnet, and found



that it was not as invulnerable as it once seemed. The article also explains how botnets are the main tool used by hackers to collect millions each year through fraud and extortion. The article also points out that there are currently no legal preconditions or even discussion regarding creating preconditions to combat botnets.

<http://www.heise-online.co.uk/security/Storm-Worm-botnet-cracked-wide-open--/news/112385>

Slow and Silent Targeted Attacks On The Rise

BY: KELLY JACKSON HIGGINS, DARK READING
01/08/2009

Security experts warn that the most dangerous attacks are "low and slow" targeted attacks, where hackers infiltrate a network silently and undetected. Hackers will even stop attacks for days at a time to avoid raising suspicion. Mike Rothman, senior vice president of strategy at eIQnetworks, explains that attacks used to be "smash and grab" where criminals tried to see what they could get as quickly as possible. Rothman says that hackers are starting to be careful about leaving tracks or attracting attention. Rothman also warns that the path of least resistance when breaching a system is through applications. Experts recommend using whitelisting to monitor unusual application activity and securing user credentials to combat spear-phishing attacks.

<http://www.darkreading.com/security/attacks/showArticle.jhtml;CIMRIOFBWT1H2QSNLRSKH0CJUNN2JVN?articleID=212701434>

Fake CNN Malware Attack Spins Gaza Angle

BY: GREGG KEIZER, COMPUTERWORLD
01/08/2009

Sam Curry, vice president of product management at RSA, explains how hackers are using fake CNN.com news notifications that promise graphic images of the Israeli invasion of

Gaza to launch spam attacks. Curry says that victims receive a phishing e-mail that appears to be from CNN, and lures the target to a Web site that requires an update to Adobe Acrobat 10. The download infects the victim's computer with an SSL stealer Trojan horse, which looks for traffic from financial services. The hackers have been preparing for the attacks for weeks, originally planning on featuring news about the upcoming inauguration. Some subject lines from the bogus messages read " Hamas launching rocket war after Gaza evacuation" and " Hamas Goads Israel into War."

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9125422>

Hack Simplifies Attacks on Cisco Routers

BY: KELLY JACKSON HIGGINS, DARK READING
01/06/2009

Felix "FX" Lindner, a researcher with Security Labs, demonstrated last week at a conference in Berlin a technique that allows an attacker to execute code remotely on Cisco routers with only basic knowledge of the targeted device and without knowledge of the specific version of IOS. During the demonstration, he was able to execute memory writes and disable CPU caches. Security researcher Dan Kaminsky says the hack disproves conventional wisdom in enterprises that routers are at low risk of attack, and that patching them is riskier than an attack due to the potential network outages that patching can cause. Lindner's demonstration proved that however much changes from one version to another, there's a little piece of every Cisco router that's the same, and attackers can use that piece to attack most of the hardware out there.

<http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=212700896>



Researchers Hack Intel vPro Security

BY: ROBERT MCMILLAN, TECHWORLD
01/06/2009

Invisible Things Labs researchers Rafal Wojtczuk and Joanna Rutkowska recently announced new software which could “compromise the integrity” of software that is loaded using the Trusted Execution Technology (TXT) – part of Intel’s vPro processor platform. TXT is supposed to protect software from being seen or tampered with by other programs on a machine. Wojtczuk and Rutkowska created a two-stage attack that exploits both a vulnerability in Intel’s system software as well as a design flaw in the TXT technology. Intel spokesman George Alfs said that Intel is working with the Invisible Things team, who plan on presenting their work at the Black Hat Washington security conference next month.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=109058>

‘Curse of Silence’ Hack Kills SMS Text Message Delivery

BY: KELLY JACKSON HIGGINS, DARK READING
01/02/2009

Researcher Tobias Engel recently presented the “Curse of Silence” attack at the Chaos Communication Congress in Berlin, which uses a formatted SMS message to launch a denial-of-service attack on a victim’s phone. The attack, which targets Nokia mobile phones, causes the messaging features on the phones to shut down although the phone itself remains operational. The attack messages are invisible and cannot be deleted from the phone. Engel says that the attacks are more annoying than dangerous, and will probably not be widely used. Still, Engel says that the attacks show that mobile phones are connected and vulnerable just like computers, and that manufacturers should have a way to quickly deploy security fixes to phones.

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212700442>

'Undetectable' phishing attack identified by research team

BY: ROBERT MCMILLAN, TECHWORLD
12/31/2008

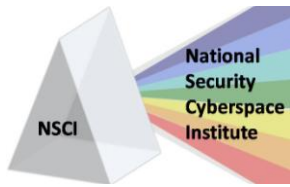
A team of security researchers was able to exploit a bug in the digital certificates of Web sites that allowed the researchers to launch an almost undetectable phishing attack. The hackers were able to break into Verisign’s RapidSSL.com certificate authority which allows them to create fake digital certificates for any Web site on the Internet. The international team of researchers will present their findings at the Chaos Communication Congress hacker conference in Berlin. The hackers also said that an attack using their techniques is unlikely although they do recommend that the MD5 hashing algorithm no longer be used by companies that issue digital certificates.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=108907>

New SSL Hack Imperils Secure Web sites

BY: KELLY JACKSON HIGGINS, DARK READING
12/30/2008

Researchers revealed the use of a cluster of more than 200 PlayStations 3s to crack a weakness in the Internet’s digital certificate infrastructure to impersonate secure Web sites. They determined that one major problem is that some certification authorities (CAs) still use outdated MD5 encryption technology rather than the newer and stronger SHA-1 cryptographic algorithm. To prove the theory, they obtained a certificate from RapidSSL for their rogue Web site and then lifted RapidSSL’s signing authority in order to sign and verify other certificates. The researchers were able to impersonate a legitimate Web site, complete



with the padlock icon that accompanies actual secured sites.

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212700234>

Friendster Social Networking Users Attacked by Malicious Spam

CYBERINSECURE.COM
12/29/2008

TrendLabs Malware blog recently announced that a ZLOB variant is being used by hackers to target social networking sites. Users of the Friendster, a social networking site most popular in Asia, may have received messages from the site with videos that link to an external site. The fake video site asks the user to download an updated version of what appears to be Adobe Flash Player that actually installs malware on the victim's computer. The article urges social networking site users to use caution when opening unsolicited messages and recommends that users only download software or updates from the vendor's site or through automatic update features rather than through pop-ups.

<http://cyberinsecure.com/friendster-social-networking-users-attacked-by-malicious-spam/>

Microsoft warns of SQL attack

BY: ROBERT MCMILLAN, NETWORK WORLD
12/23/2008

Microsoft released a security advisory late last month warning users of a bug in its SQL Server database software which could be exploited to run unauthorized software on systems using versions of Microsoft SQL Server 2000 and SQL Server 2005. Marc Maiffret with the security consulting firm, DigiTrust Group, said that the bug is low risk and is unlikely to be used in widespread attacks. Microsoft has released an emergency patch for the bug.

<http://www.networkworld.com/news/2008/12/2308-microsoft-warns-of-sql.html>

Hacked Phone System Leaves Company with \$50,000 Bill

BY: KIM ZETTER, WIRED BLOG NETWORK
12/23/2008

After discovering a strange code on a phone display, HUB Computer Solutions owner Alan Davison spoke with his phone company, Manitoba Telecom Services, and found that a hacker had made \$52,360 worth of calls to Bulgaria through the company's system. Davison said that the phone company should have a fraud alert system that can notify customers of fraudulent activity, although MTS claims that HUB is responsible for securing their own phone equipment. Hackers dialed in to the company's voicemail, and used the outbound call transfer feature to make the calls remotely. The article recommends that companies block overseas calling and prohibit outbound call-transfer features on their phone systems.

<http://blog.wired.com/27bstroke6/2008/12/hacked-phone-sy.html>

Scareware Mongers Hitch Free Ride on Microsoft.com and Others

BY: DAN GOODIN, THE REGISTER
12/23/2008

According to the article, hackers are currently exploiting flaws in more than 1 million Web sites operated by the federal government, media companies and Microsoft to get visitors to install harmful software onto their computers. These "open-redirect" exploits trick victims into clicking on links that appear to lead to trusted domains, but actually redirects target users to malicious Web sites. Some infected sites ask users to install updates to programs like Internet Explorer, and other exploited pages offer video streaming. Microsoft has since disabled the infected links on their company site.



http://www.theregister.co.uk/2008/12/23/open_redirect/

Online Jihadists Plan for 'Invading Facebook'

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
12/18/2008

Extremist jihadists, who already use social media outlets to spread radical propaganda, are now planning to invade social networking site Facebook. Recent posts on the extremist al-Faloja forum talk about using Facebook to "fight the media." Groups like al-Qaida already use the Internet to train and organize followers, although the groups have been reluctant to use Web 2.0 tools like Facebook. The extremists now hope to exploit the existing networks of people on social networking sites by distributing videos and writings of "martyrs" in both Arabic and English.

<http://blog.wired.com/defense/2008/12/online-jihadist.html>

Hackers Bypassing IE Patch with Word Bugs

BY: GREGG KEIZER, COMPUTERWORLD
12/19/2008

Security researchers recently announced that attackers are hiding malicious ActiveX controls in Microsoft Word documents, utilizing a recently patched vulnerability in Internet Explorer. David Marcus, director of security research and communications at McAfee's Avert Labs, explains that the infected documents include an ActiveX control that accesses the malware hosting site. The documents are being spread as attachments to spam and on hacked Web sites. Microsoft recently released a patch for the flaw, although researchers believe that thousands of legitimate Web sites have already been compromised. Other researchers report that the exploit is part of multiple hacker toolkits, and recommend that users exercise caution when opening Word documents.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=108625>

CheckFree.com Hijack May Have Affected 160,000 Users

BY: BRIAN KREBS, WASHINGTON POST
12/17/2008

CheckFree.com recently reported that its Web site was hijacked, affecting almost 160,000 people. Hackers redirected Web site traffic to a site in the Ukraine that tried to install a version of the Gozi Trojan to steal user passwords. CheckFree allows users to pay many kinds of bills, including credit accounts, utilities and insurance payments, and the company currently controls between 70 to 80 percent of the U.S. online bill pay market. CheckFree has alerted its users of the attack, although the company has not said if their e-mail systems were also compromised.

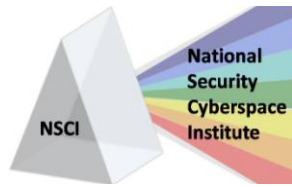
http://voices.washingtonpost.com/securityfix/2008/12/checkfreecom_hijack_may_have_a.html?nav=rss_blog

Twitter Gets Hacked, Badly

BY: MICHAEL ARRINGTON, TECH CRUNCH
01/05/2009

In addition to phishing attacks early in January, Twitter recently announced that 33 accounts had been compromised, including the high-profile accounts of Rick Sanchez and Barack Obama. Twitter explained that the attacker was able to hack into the site's admin tools that are used by the site's support team, allowing them access to the users' accounts. Twitter also announced that they have taken the support tools offline and will make sure that the tools are secure before they are put back.

<http://www.techcrunch.com/2009/01/05/twitter-gets-hacked-badly/>



You Could Be Flushed Into A Con

BY: MAYANK TEWARI, DNA INDIA
01/02/2009

According to Gulshan Rai, head of Cert, exploitations of the domain name system (DNS) servers of Internet service providers are having an especially significant impact in India, where many ISPs have not implemented up-to-date security patches. The DNS flaw was originally discovered last February by Net security expert Dan Kaminsky, and allows hackers to redirect traffic to fraudulent Web sites that gather personal information. Flush.M, one variant of

the bug, is unknowingly downloaded to a victim's computer when the user visits a malicious Web site. The Flush.M variant uses infected machines to redirect other computers on a local area network to fraudulent sites. Samir Kelekar of the Bangalore security consulting firm Tekno Trends, said that India needs compliance laws that require ISPs to implement security patches, and said that his ISP has been unable to fix the patch.

<http://www.dnaindia.com/report.asp?newsid=1218204>

CYBERSPACE TACTICS AND DEFENSE

FBI's IC3 Issues Tips For Preventing Website Attacks

BY: KELLY JACKSON HIGGINS, DARKREADING
12/16/2008

The FBI's Internet Crime Complaint Center (IC3) recently released a list of preventative measures for organizations to take to prevent Web site attacks. Recommendations include denying extended URLs; implementing a specific approach to secure dynamic Web content; applying the "least privilege" principle on SQL machine accounts; requiring passwords on Microsoft administrator, user and machine accounts; and implementing firewall rules. The article includes additional recommendations for organizations aiming to increase security.

<http://www.darkreading.com/security/attacks/showArticle.jhtml;jsessionid=0EFIAUKJRNVIUQSNDLOSKH0CJUNN2JVN?articleID=212500683>

Social networking malware: Protect yourself

BY: C.G. LYNCH, NETWORK WORLD
12/16/2008

Matt Sergeant, senior anti-spam technologist at MessageLabs, believes that spammers are increasingly using social networking sites instead of traditional e-mail spamming. Sergeant offers some tips for staying safe on social networking sites which include: choosing a new, more secure password; using caution when filling out applications for third party features including apps or games; and not clicking on links provided by other users.

<http://www.networkworld.com/news/2008/121608-social-networking-malware-protect.html?hpg1=bn>



Security on Social Networks Takes Efforts by All Sides

BY: BRIAN PRINCE, EWEK
12/17/2008

Security vendors expect the trend of increasing attacks on social networking sites to continue into 2009, and predict that social engineering will play a large role in attacking users of sites such as MySpace and Facebook. Mary Landesman, senior security researcher at ScanSafe, recommends that users of these sites take caution when accepting new virtual friends and emphasizes the importance of never clicking on links received unexpectedly. Social networking sites are vulnerable to attacks because of their use of third-party applications. One site, Facebook.com, is now requiring developers to comply with certain regulations before building on the site's platforms and is also implementing automated statistical analysis of site activity. Experts agree that increasing security on social networking sites will require cooperation from both the site users and administrators.

<http://www.eweek.com/c/a/Security/Security-on-Social-Networks-Takes-Efforts-By-All-Sides/?kc=rss>

FTC: Reduce Data Theft by Regulating Social Security Numbers

BY: CHUCK MILLER, SC MAGAZINE
12/18/2008

The Federal Trade Commission recently released a report that found that using Social Security numbers to authenticate users leads to increased identity theft. The report said that there are millions of victims of identity theft each year, resulting in billions of dollars in financial losses, primarily to businesses. The report recommends the development of nationwide regulations for how businesses verify their customers' identities. The report also recommends that the display and transmission of SSNs should be restricted, and that organizations "enhance coordination and information-sharing" among other businesses that use SSNs.

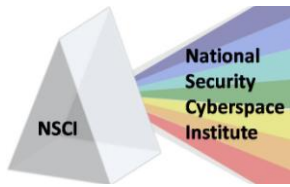
<http://www.scmagazineus.com/FTC-Reduce-data-theft-by-regulating-Social-Security-numbers/article/123116>

Anatomy of an XSS Attack

BY: RUSS MCREE, DARK READING
01/09/2009

Russ McRee writes "Point blank: XSS exploits consumers. The gullible and the innocent fall prey, and their financial well-being is often left to the greedy and malicious." McRee recommends that users validate their inputs, follow a secure development life cycle, scan their Web sites for vulnerabilities on a regular basis, and do not assume you are safe. He says it is also important to utilize a web application firewall in addition to good code and monitoring. Finally, he suggests that you conduct Web application vulnerability scans on a regular basis and fix findings immediately. He reports: "According to the Internet Security Threat Report from Symantec, 'during the last six months of 2007, 11,253 site-specific, cross-site scripting vulnerabilities were documented, compared to 6,961 between February and June.' That's a 62% increase in six months."

<http://www.darkreading.com/bestofweb/>



Tech Insight: Finding Common Ground for Security, IT Teams

BY: JOHN SAWYER, DARK READING

12/19/2008

The article discusses how security teams and IT groups often have different opinions and practices on incident response in key areas including password policies, patch management and network security. Developing better password policies requires compromise from users and security groups, and the article recommends educating users on the importance of passwords and utilizing technologies like self-service portals for password resets and multifactor authentication to improve password security. Patch management, which can fall under both systems administration and security teams, requires constant monitoring and updates. The article claims that risk assessment is crucial to developing policies for patch management. Security teams should take time to explain security measures to promote “better interaction and cooperation with IT.”

<http://www.darkreading.com/security/management/showArticle.jhtml?articleID=212501481>

SanDisk Puts ‘One-Touch’ Backup On Flash Drive

BY: JOHN E. DUNN, TECHWORLD

01/09/2009

SanDisk's announcement of a new and improved flash back-up product promises the ability to back up chosen data directories and data types at the touch of a button, but in a much smaller device than the widely-used USB flash drive. The new Ultra Backup comes with built-in encryption for a basic level of security, and capacities from 8GB to 64GB, putting it in direct competition with lower-cost hard drives. Earlier this week, SanDisk announced a version of the product that will automatically and securely back up data to an online service every time it is near an Internet connection.

<http://www.techworld.com/security/news/index.cfm?RSS&NewsID=109322>

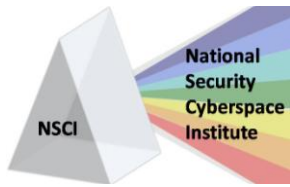
As Phishing Evolves, Criminals Switch to Malware

BY: ROBERT MCMILLAN, COMPUTERWORLD

12/18/2008

Security researchers have been able to improve security against “phishing” attacks by blocking many fraudulent e-mail messages. In response to increased security, phishing gangs began tricking victims into installing malicious software that steals banking information from the hacked computers. Mickey Boodaei, CEO of Trusteer, explains that attacks that install malicious software are easy to launch and are increasing as attacks shift from traditional phishing attacks. Trusteer recently released a search tool that allows banks and Web site operators to see if their domains have been targeted in attacks. Experts also said that hackers are increasingly targeting smaller financial institutions and European banks, which may be less prepared for fake e-mail campaigns. Sean Brady, a senior manager at RSA Security, explains that phishing scams will continue to increase because of high profits and the ability to hit victims worldwide.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124079&source=rss_topic82



VeriSign Remedies Massive SSL Blunder (Kinda, Sorta)

BY: DAN GOODIN, THE REGISTER
01/09/2009

An international team of researchers recently discovered a flaw in VeriSign's RapidSSL product, which allows hackers to spoof encryption certificates of any Web site on the Internet. According to Tim Callan, vice president of VeriSign's product marketing, the company has made changes to ensure its SSL products are now immune to the attacks, although the article explains that only VeriSign SSL products that are issued on or after Dec. 30 are immune to the attack. Callan says that it is highly unlikely that anyone besides the researchers were able to figure out how to execute the attack, which was the result of a year of research into MD5 vulnerabilities and "intense computational processing."

http://www.theregister.co.uk/2009/01/09/verisign_ssl_remedy/

Self destruct technology for lost and stolen mobile phones

SECURITY PARK
12/23/2008

Virtuity recently released BackStoff Mobile, which is able to completely delete the contents of lost or stolen mobile phones and handheld devices. BackStoff Mobile can track down a device almost anywhere in the world and delete all information from the device. It is used to create a report detailing what was deleted, when it was deleted and the location of the stolen or lost device. Virtuity also recently announced a significant upgrade to its core laptop location tracking and data protection applications which will now include encryption integration, Wireless and RFID integration, HR system integration, user controlled device downtime and O/S destruction.

http://www.securitypark.co.uk/security_article262376.html

CYBERSPACE - LEGAL

Rep. Jackson Lee Proposes Cybersecurity Bill

BY: BEN BAIN, FEDERAL COMPUTER WEEK
01/09/2009

Rep. Sheila Jackson Lee (D-Texas) introduced a bill Jan. 7 that would require the Homeland Security Department (DHS) and the National Science Foundation (NSF) to create a grant program that would help schools improve cybersecurity education. Funding is also available for professional development or associate degree programs, as well as for purchasing training equipment. The bill would also establish an E-Security Fellows program that would award fellowships to state, local, tribal and private sector officials who are

interested in participating in the work of the DHS' National Cybersecurity Division.

<http://fcw.com/articles/2009/01/09/rep-jackson-lee-proposes-cybersecurity-bill.aspx>

U.S. Must Update Laws Defending Against Foreign Hackers

BY: JIM LANGEVIN AND MICHAEL MCCAUL, THE HOUSTON CHRONICLE
12/20/2008

The article claims that modern hackers are part of organized crime groups and national militaries that are constantly infiltrating sensitive U.S. computer networks to steal military technologies and trade secrets from American companies. The article also asserts



that American cyberspace laws are outdated, and must be updated to meet 21st century threats. Defense and intelligence officials briefing the incoming Obama administration place cybersecurity at the forefront of the national security agenda. The article recommends the development of a national cyber doctrine that would make U.S. cyber infrastructure a “national security and economic asset that requires protection from all instruments of national power.” The authors also recommend that one person or agency be responsible for the overall cybersecurity vision, specifically a National Office for Cyberspace within the White House. The article calls for a comprehensive approach towards securing cyberspace on the federal level, and federal support for research and development.

<http://www.chron.com/disp/story.mpl/editorial/outlook/6174987.html>

First ‘Pretexting’ Charges Filed Under Law Passed After HP Spy Scandal

BY: KIM ZETTER, WIRED BLOG NETWORK
01/09/2009

Pretexting is a method where a criminal pretends to be a phone-company customer or

other person to request a customer’s phone records. Twenty-eight-year-old Vaden Anderson of Ohio was charged with using pretexting to obtain confidential phone records from Sprint/Nextel. Anderson reportedly provided the phone company with a phony U.S. District Court civil subpoena to get the records.

Anderson faces a maximum prison sentence of 10 years and a \$250,000 fine if convicted.

Nicholas Shaun Bunch of Alabama was charged with using a victim’s name and social security number to obtain confidential records from T-Mobile. Because Bunch used the victim’s SSN, he is also charged with aggravated identity theft. Although pretexting has been used for years by private investigators and data brokers, the tactic received national attention in 2006 when investigators working for Hewlett-Packard used pretexting to spy on company board members and reporters. The Telephone Records and Privacy Act that made pretexting illegal went into effect in January 2007.

<http://blog.wired.com/27bstroke6/2009/01/first-pretextin.html>

Raytheon

Raytheon

Aspiring to be the most admired defense and aerospace systems supplier through world-class people and technology Raytheon is a technology leader specializing in defense, homeland security, and other government markets throughout the world. With a history of innovation spanning more than 80 years, Raytheon provides state-of-the-art electronics, mission systems integration, and other capabilities in the areas of sensing; effects; command, control, communications and intelligence systems, as well as a broad range of mission support services.

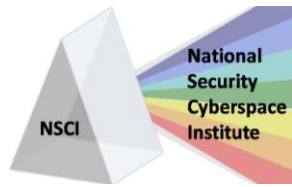
British Police Granted Hacking Rights

BY: AHARON ETENGOFF, IT EXAMINER
01/05/2009

British police have been given authority to hack into personal computers without a warrant,

although officers must have the permission of a local chief constable before accessing a suspect’s computer. Officers execute the searches by installing stealth malware onto a suspect’s machine that supplies a surveillance

110 Royal Aberdeen • Smithfield, VA 23430 • ph. (757) 871-3578



team with the suspect's e-mails and browsing habits. Law enforcement officials said that the policy is critical to combating cyber-crime, however home secretary Dominic Grieve has demanded the government explain what safeguards would be established. Critics, such

TJX Hacker Sentenced To 30 Years In Turkish Prison

BY: KELLY JACKSON HIGGINS, DARK READING
01/08/2009

Maksym "Maksik" Yastremskiy, from Ukraine, was one of 11 men charged with stealing more than 40 million credit and debit card numbers as part of a campaign of WiFi hacks on major retailers including OfficeMax, Barnes & Noble, DSW and TJX. A Turkish court sentenced Yastremskiy to 30 years in prison for his role in the hacks. The group of hackers, which included members from the United States, Ukraine, China and Estonia, installed malware on vulnerable WiFi networks that stole customers' credit card numbers and personal information.
<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212701407>

Hacking Godfather 'Maksik' Sentenced to 30 Years by Turkish Court

BY: KEVIN POULSEN, BLOG WIRED NETWORK
01/08/2009

Ukrainian hacker Maksym Yastremski, who was responsible for countless major breaches of U.S. retail networks over the past four years, was sentenced to 30 years in prison by a Turkish court, although Yastremski was convicted on unrelated charges of hacking into computer systems of 12 Turkish banks. Yastremski, who is called "Maksik", was well-known for selling stolen credit and debit card information underground. U.S. prosecutors claim that Yastremski made more than \$11 million from selling the stolen credit and debit card information between 2004 and 2006 alone.

as Shami Chakrabarti, director of human rights campaign group Liberty, argue that the warrantless searches violate privacy rights.
<http://www.itexaminer.com/british-police-granted-hacking-rights>.

<http://blog.wired.com/27bstroke6/2009/01/hacking-godfath.html>

New GA Law Forces Sex Offenders to Hand Over Their Internet Passwords

BY: KELLY JACKSON HIGGINS, DARK READING
01/02/2009

A new state law in Georgia that requires sex offenders to provide law enforcement authorities with their Internet passwords, screen names and e-mail addresses is facing criticism from privacy advocates. State Sen. Cecil Staton acknowledges that the law may infringe on the privacy of sex offenders, but says that the safety of children online must be the top priority, justifying the infringement. Most states provide physical addresses of sex offenders online, and 15 states require offenders to provide information of their online presence, but only Georgia and Utah currently require the offenders to provide their passwords. Sara Totonchi, with the Southern Center for Human Rights, argues that law enforcement authorities should not be allowed to access personal e-mails between family members or employers.

<http://www.darkreading.com/security/privacy/showArticle.jhtml?articleID=212700431>

US district court orders CyberSpy to stop selling its RemoteSpy keylogging spyware program

SECURITY PARK
12/30/2008

According to the FTC, CyberSpy released to its customers detailed instructions on disguising



spying programs as innocuous files through a password-protected Web site. A U.S. district court has ordered CyberSpy Software to stop selling its RemoteSpy keylogging spyware program, and both the RemoteSpy and CyberSpy Web sites have been taken offline. The article explains that many companies offer products that are promoted as a way for wives to spy on their husbands or babysitters, but security experts warn that the software can be used with a wide variety of motives, including identity theft.

http://www.securitypark.co.uk/security_article262403.html

Accused Hacker Facing Felony Charges

FOXRENO.COM
12/24/2008

Terry Childs, 44, of Pittsburg was arrested and charged in July with four counts of computer network tampering, as well as one count of causing losses of more than \$200,000 for allegedly tampering with the city's main computer network. He will stand trial on felony charges but a trial date has not yet been scheduled. Prosecutors have alleged that Childs

rigged the city's FiberWAN network with his own passwords and had installed traps on the system that would have caused a full system failure if power were to be shut down.

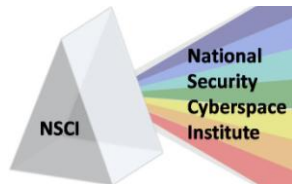
<http://www.foxreno.com/news/18356693/detail.html>

Software executive sentenced for hacking

BY: ROBERT MCMILLAN, COMPUTERWORLD
12/22/2008

Jay E. Leonard, owner of Platte River Associates Inc., was recently sentenced to 12 months of supervised probation and fines after pleading guilty to stealing passwords from a competitor. Leonard's company, Platte River Associates Inc., builds software that is used in petroleum exploration. Leonard reportedly gained access to a password-protected area of the Web site of competitor, Zetaware, Inc. The plea agreement also said that Leonard discussed a plan to exploit and utilize the downloaded Zetaware files for economic gain.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124238>



CYBERSPACE-RELATED CONFERENCES

Note: Dates and events change often. Please visit web site for details. Please provide additions, updates, and/or suggestions for the CYBER calendar of events [here](#).

19-21 Jan 2009	International Workshop on e-Forensics Law , Adelaide Australia, http://www.e-forensics.eu/
19-21 Jan 2009	Gulf C4ISR , Abu Dhabi, United Arab Emirates, http://www.asdevents.com/event.asp?ID=324
25-28 Jan 2009	NANOG45 , Santo Domingo, Dominican Republic, http://www.nanog.org/meetings/nanog45/index.php
26-29 Jan 2009	U.S. Department of Defense Cyber Crime Conference , St Louis MO, http://www.dodcybercrime.com/9CC/
27-29 Jan 2009	Network Centric Warfare USA , Washington, DC, http://www.asdevents.com/event.asp?ID=339
28-29 Jan 2009	CyberWarfare 2009 , London, UK, http://www.cyberwarfare-event.com/
2-6 Feb 2009	United States Army Global Information Operations Conference , Peterson AFB, Colorado Springs, CO, http://portal.smdc.army.smil.mil/C19/CVTI/default.aspx?Mode=Edit&PageView=Shared
16-19 Feb 2009	Black Hat DC 2009 , Washington DC, http://www.blackhat.com/
9-11 Mar 2009	INFOSEC World Conference & Expo , Orlando FL, http://www.misti.com/default.asp?page=65&Return=70&ProductID=5539
13-15 Mar 2009	Cybercultures: Exploring Critical Issues , Salzburg Austria, http://www.inter-disciplinary.net/ci/Cyber/cybercultures/c4/fd.html
30 Mar – 2 Apr 2009	Computational Intelligence in Cyber Security , Nashville TN, http://www.ieee-ssci.org/index.php?q=node/21
6-8 Apr 2009	Cyber Security and Information Intelligence Workshop , Oak Ridge National Laboratory, http://www.ioc.ornl.gov/csiirw07/
14-17 Apr 2009	Black Hat Europe , Amsterdam The Netherlands, http://www.blackhat.com/
20-24 Apr 2009	RSA Conference , San Francisco CA, http://www.rsaconference.com/2009/US/Home.aspx
13-14 May 2009	Cyber Defence , Stockholm, Sweden, http://www.smi-online.co.uk/events/overview.asp?is=1&ref=3080
24 – 28 May 2009	Internet Monitoring and Protection , Venice Italy, http://www.iaria.org/conferences2009/SECURWARE09.html
26-29 May 2009	Network Centric Warfare Europe , Cologne, Germany, http://www.asdevents.com/event.asp?ID=358
14 – 19 Jun 2009	International Conference on Emerging Security Information, Systems and Technologies ; Athens Greece, http://www.iaria.org/conferences2009/SECURWARE09.html
15-19 Jun 2009	Air Force Cyberspace Symposium 2009 , Bossier City, Shreveport, LA, http://www.cyberinnovationcenter.org
25-30 July	Black Hat USA 2009 , Las Vegas NV, http://www.blackhat.com/
7-10 Jul 2009	Conference on Ubiquitous Intelligence and Computing , Brisbane, Australia, http://www.itee.uq.edu.au/~uic09/
17-19 Aug 2009	DFRWS (Digital Forensics Research) 2009 Annual Conference , Montreal, Canada, http://www.dfrws.org/2009/



EMPLOYMENT OPPORTUNITIES WITH NSCI

<u>Job Title</u>	<u>Location</u>
Operational Deterrence Analyst	NE, VA
Defensive Cyber Ops Analyst	NE, VA, CO
Cyber SME	NE, VA, TX, CO
Geospatial Analyst	NE
Logistics All-Source Intelligence Analyst	NE
SIGINT Analyst	NE, CO
Cyber Operations SME	NE
Website Maintainer	NE
Cyberspace Specialists	NE
Cyberspace Manning IPT	NE

CYBERPRO CONTENT / DISTRIBUTION

<p>Officers</p> <p>President Larry K. McKee, Jr.</p> <p>Senior Analyst Jim Ed Crouch</p> <p>-----</p> <p>CyberPro Editor-in-Chief Lindsay Trimble</p> <p>CyberPro Research Analyst Kathryn Stephens</p> <p>CyberPro Archive</p>	<p>The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest and to keep subscribers who are involved in the development of Cyber-related concepts and initiatives informed on items of common interest. The newsletter and the information contained therein are not intended to provide a competitive advantage for any commercial firm. Any misuse or unauthorized use of the newsletter and its contents will result in removal from the distribution list and/or possible administrative, civil, and/or criminal action.</p> <p>The views, opinions, and/or findings and recommendations contained in this summary are those of the authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or National Security Cyberspace Institute.</p>
<p>To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.</p> <p>Please contact Lindsay Trimble regarding CyberPro subscription, sponsorship, and/or advertisement.</p>	

All rights reserved. CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.