




CyberPro

Volume 1, Edition 6
July 31, 2008

Keeping Cyberspace Professionals Informed

<p>Officers</p> <p>President Larry K. McKee, Jr.</p> <hr/> <p>CyberPro Research Analyst Kathryn Stephens</p>	<p><i>This newsletter is intended 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 shall not be used 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 other appropriate administrative, civil, and/or criminal action.</i></p> <p><i>The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. 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.</i></p>
<p>To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.</p>	



City of Hampton VA
 The City of Hampton has an advanced technology culture built on the foundation of personnel who live and work as an integral part of the community. Hampton and the surrounding region have an unmatched high technology defense industrial base and a skilled workforce with impressive education and security credentials. These critical capabilities combined with our world-class academic and government research centers, a strong pro-military culture, and superior lifestyle make Hampton the ideal choice for Cyberspace related activities. <http://hamptoncyberspace.net>

Table of Contents

** CYBER-RELATED CONFERENCES **	4
*** OPEN-SOURCE MATERIAL ***	5
Oracle issues warning over dangerous WebLogic flaw	5
Agencies encrypt less than third of laptops	5
Mid-year security report: Web sites, open source, social networking at risk.....	5
Botnets Behind One Fourth of Click Fraud	5
Marshalls Telecom Hit By Massive 'Zombie' Attack	5
Exiled Tibetans Wage Cyber Attack On China	6
Virtualization for your DMZ?	6
CIO Council to deal with Web 2.0 security	6
Study: Web 2.0 Poses Challenges for Banks	7
Top internal network threats in 2008 so far.....	7
Korea gets tough on web privacy	7
Analysis: Russia behind Georgia cyberwar?	7
Anonymity on the Web.....	7



Democrats ask DHS to halt work on network.....	8
The Pirate Bay Wants to Encrypt the Entire Internet.....	8
Clarifications sought on data mining	8
Security Policy Considerations for Virtual Worlds.....	9
Egypt's cyberactivism has limits	9
Malware prevalent on trusted Web pages.....	9
British ISP File Share Smackdown Targets Accounts, Not Users	9
U.S. Strategic Command chief closes cyber symposium	10
DNS attack code out in wild.....	10
Cyber Warfare: Strategy & Tactics.....	10
SMBs underestimate extent of cybercrime	10
Portrait of Hackers	11
Hackers snoop on mobile phones.....	11
Big Brother is Bluetoothing You.....	11
Regional push for Cyber Command	11
Hackers preparing to exploit DNS flaw	12
Top spammer sentenced to nearly four years.....	12
National security observers explain FISA ins and outs	12
Waging Communication War.....	12
NIST revises guidelines for IT security metrics	13
Q&A: Upcoming defense IT challenges.....	13
Details of major Internet flaw posted by accident	13
Cybersecurity Will Take A Big Bite of the Budget	13
DHS seeks cybersecurity capability info	13
Open source software a security risk, study claims.....	14
Secret Defense Data Lost on UK Government USBs.....	14
Elder, analyst keynote Air Force cyber symposium	14
Another ex-Soviet state under fire in web attack.....	14
Security analysts praise Obama's pledge for a cyber chief	15
Researchers trace structure of cybercrime gangs	15
Symposium gets to core of Air Force's role in cyberspace	15
Symantec products Common Criteria-certified	15
U.S. Air Force lets Web 2.0 flourish behind walls.....	16
'No decision' on giant database	16
Army Secretary: We're Falling Behind Online	16
Obama Wages Cyberwar	16



CyberPro

Volume 1, Edition 6
July 31, 2008

Keeping Cyberspace Professionals Informed

Schneier, Team Hack 'Invisibility Cloak' for Files 17

Major sites fall victim to Web hijack; check yours 17

Romanian authorities arrest cybercrime suspects 17

Bush leads biometric push 17

Government, health care Web sites attacked 18

Insider threat looms large as San Francisco's network crisis plays out..... 18

Vulnerabilities Could Expose Broad Range of Java Apps 18

Technology companies devise cyber security, defensive software, to combat the threat of information warfare..... 18

Analysts seek deterrence strategy for space and cyberspace..... 19

CyberPro Content/Distribution..... 19



**** CYBER-RELATED CONFERENCES ****

Note: Dates and events change often. Please visit web site for details.

Please provide additions/updates/suggestions for the CYBER calendar of events [here](#).

2 – 7 Aug 08	Black Hat USA 2008 Briefings & Training , Caesars Palace, Las Vegas, NV, http://www.blackhat.com/
19-21 Aug 2008	LandWarNet: Providing & Enabling Joint Generating/Operating Force Network Capabilities , Broward County Convention Center, Ft. Lauderdale, FL, http://events.jspargo.com/lwn08/public/enter.aspx
15-17 Sept 2008	24th Annual Air & Space Conference and Technology Exposition , Washington D.C., http://www.afa.org
18-19 Sept 2008	Current and Future Military Data Links , Washington D.C., http://www.asdevents.com/event.asp?ID=257
25-26 Sept 2008	Electronic Warfare Operations and Systems 2008 , London UK, http://www.asdevents.com/event.asp?ID=241
29-30 Sept 2008	Airbone Networks Conference , Washington D.C., http://www.asdevents.com/event.asp?ID=267
30 Sept – 2 Oct 2008	National Security 2008 , Brussels, Belgium, http://www.asdevents.com/event.asp?ID=265
6-8 Oct 2008	Strategic Space & Defense , Qwest Center Omaha Convention Center and Arena, Omaha, NE, http://www.stratspace.org/
7-9 Oct 2008	2008 Cyber Awareness Summit , Bossier City-Shreveport, LA, http://www.cyberinnovationcenter.org/
16-17 Oct 2008	8th Annual C4ISR Integration Conference , Defense News Media Group, Arlington, Virginia, http://www.dnmgconferences.com/07c4isr/index.php?content=home
3-5 Nov 2008	Global MilSatCom 2008 Conference & Exhibition , Millennium Conference Centre, London, UK, www.smi-online.co.uk/08globalmilsatcom20.asp



Intelligent Software Solutions
ISS is a leading edge software solution provider for enterprise and system data, services, and application challenges. We specialize in understanding user requirements and delivering software applications whose capabilities match real user needs. ISS has built hundreds of operationally deployed systems, in all domains – “From Space to Mud”™. Constant interaction with users in development, production, test, and implementation phases instills flexibility and rapid response in developing code that matches explicit, implicit, and implied user requirements. With solutions based upon modern, proven technology designed to capitalize on dynamic service-oriented constructs, ISS builds solutions that work today and are ready for the future. Visit us today at <http://www.issinc.com>.



*** OPEN-SOURCE MATERIAL ***

Oracle issues warning over dangerous WebLogic flaw

BY: JEREMY KIRK, NETWORK WORLD

07/29/2008

A severe vulnerability was found in Oracle's WebLogic Server, which prompted the company to issue a rare security alert. In the advisory, Oracle warned that the flaw can be exploited without a username or password. Oracle is developing an emergency patch for the flaw. The vulnerability scored a 10 on the Common Vulnerability Scoring System, which is the highest rating. Oracle said that they expect a fix to be ready soon, and they will release a Security Alert once it is ready.

<http://www.networkworld.com/news/2008/072908-oracle-issues-warning-over-dangerous.html>

Agencies encrypt less than third of laptops

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK

07/29/2008

The Government Accountability Office has released a report stating that federal agencies only encrypt 30% of their laptops and other devices, leaving other information vulnerable to data loss and unauthorized release. House Homeland Security Committee Chairman Bennie Thompson said that he was disappointed by the low rate, and emphasized the importance of encryption to information security.

<http://www.fcw.com/online/news/153305-1.html?CMP=OTC-RSS>

Mid-year security report: Web sites, open source, social networking at risk

BY: ELLEN MESSMER, NETWORK WORLD

07/29/2008

The IBM Midyear Trend Statistics report tracked software vulnerability for the first half of the year and found that companies like IBM, Microsoft, Apple, Sun and Cisco made the list of worst offenders. Of course, companies that make a large amount of software are subject to more disclosures. Other offenders were open source packages that are more vulnerable to infection attacks.

<http://www.networkworld.com/news/2008/072908-security-report.html>

Botnets Behind One Fourth of Click Fraud

DARK READING

07/28/2008

According to the Click Fraud Network, a group of 4000 online advertisers found that click fraud dropped just slightly from last quarter; however the methods for click fraud have changed. Botnets now generate fraud, which make the fraud more sophisticated and more difficult to detect.

http://www.darkreading.com/document.asp?doc_id=160195

Marshalls Telecom Hit By Massive 'Zombie' Attack

BY: GIFF JOHNSON, PACIFIC MAGAZINE

07/25/2008

The Marshall Islands' only Internet provider was attacked by "zombie" computers that flooded National Telecommunications Authority computers with emails. This attack strategy is known as



a “Distributed Denial of Service” attack. Technical teams added gateway resources to stop the zombie emails, although the system was not back to normal for 24 hours.

<http://www.pacificmagazine.net/news/2008/06/25/marshalls-telecom-hit-by-massive-zombie-attack>

Exiled Tibetans Wage Cyber Attack On China

INFORMATION WARFARE MONITOR

07/23/2008

Exiled Tibetans have been using the internet as a weapon to draw attention to the Free Tibet cause and to wage a virtual war against China. Tibetan websites only stay online for three or four days in China before they are taken down, but there are several websites that can connect users to sites related to the Tibetan cause, including www.tibetsites.com, and the exiled Tibetan administration has its own website at www.tibet.net, although these sites are sometimes hacked by Chinese hackers.

<http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1879>

Virtualization for your DMZ?

BY: JOAB JACKSON, GOVERNMENT COMPUTER NEWS

07/28/2008

Many agencies are looking for ways to consolidate servers and set up virtual switches between servers on one computer, hoping to save money on buying hardware for multiple security levels. Although the virtual separation of servers is technically possible, many critics are skeptical. Phil Cox, an engineer at System Experts claims there is no way to guarantee the isolation of each level, and although he offered multiple scenarios of how to bridge internal/external networks in one box, he states that he would not trust the separation.

http://www.gcn.com/print/27_18/46743-1.html?topic=defense-technology

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.

CIO Council to deal with Web 2.0 security

BY: MARY MOSQUERA, FEDERAL COMPUTER WEEK

07/28/2008

Dave Wennergren, deputy CIO at the Defense Department said the federal Chief Information Officers Council will create a security committee to provide information security in a Web 2.0 environment. Wennergren emphasizes the importance of balance between information sharing and strengthening security safeguards for businesses, and explained that the goal for the Council this year was to address Web 2.0 and the next-generation workforce.

<http://www.fcw.com/online/news/153299-1.html>



Study: Web 2.0 Poses Challenges for Banks

DARK READING

07/25/2008

Web 2.0 is expected to bring changes in online banking for small businesses. Although it will be 12-18 months before users see significant changes, Dark Reading believes most banks will change online banking procedures in the next three years. The delay is due to rigorous security evaluations that must be performed on new technologies, and IT budget constraints.

http://www.darkreading.com/document.asp?doc_id=160007

Top internal network threats in 2008 so far

HELP NET SECURITY

07/24/2008

Promisc released findings from security audits of more than 100,000 corporate endpoints that found that not one organization was completely clean of internal threats. Promisc found that unauthorized use of removable storage is increasing, endpoints are not properly updated, and unauthorized instant messaging is increasing. Promisc also found that infected computers had disabled anti-virus programs, used unauthorized personal storage, had unauthorized peer-to-peer applications installed or had unprotected shared folders and remote control software.

<http://www.net-security.org/secworld.php?id=6350>

Korea gets tough on web privacy

BY: SIMON BURNS, VNUNET.COM

07/24/2008

Korea has revised internet regulations, requiring major websites to change privacy policies and tighten copyright restrictions. Korean justice minister Kim Kyung-han has also announced a plan to combat internet libel. Kyung-han stated that Korea will be stricter with punishments for websites that spread false information, and will develop policies to identify online libel as a crime.

<http://www.vnunet.com/vnunet/news/2222478/korea-tightens-web-rules>

Analysis: Russia behind Georgia cyberwar?

BY: SHAUN WATERMAN, SPACEWAR

07/25/2008

Russia is suspected of hacking into the website of the President of Georgia, and has been blamed for cyber attacks on both Lithuania and Estonia as well. The attack was monitored in the United States by several Internet watch operations, although the centers are not involved in any response to the incident. According to one Internet security analyst, who was in Russia at the time, the attack came from the Ukraine and is being blamed on Russia. Cyber attacks are often hard to track, and it may be impossible to prove where the attack came from.

http://www.spacewar.com/reports/Analysis_Russia_behind_Georgia_cyberwar_999.html

Anonymity on the Web

PUBLIUS PROJECT

07/26/2008

Websites like JuicyCampus and rottenneighbor.com have received harsh criticism for allowing anonymous users to post information about people whether or not the entries are true.

According to the Communications Decency Act, websites cannot be considered publishers if



information comes from a separate information content provider, meaning the websites are not accountable for their content, even if the posts would be considered defamation if printed. The article notes that without some change in the law, the internet is free speech paradise, with no repercussions for false information.

<http://publius.cc/2008/07/25/anonymity-on-the-web/>

Democrats ask DHS to halt work on network

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
07/25/2008

The Homeland Security Department is currently working on a secure national information-sharing network that would provide terrorism alerts and other messages state/local governments and the private sector. After a briefing on the new network, Reps. Bennie Thompson and Jane Harman are asking that the program be stopped temporarily so that problems can be fixed. A report from the Government Accountability Office stated that DHS had rushed development of the network without consulting state, local and tribal users.

<http://www.fcw.com/online/news/153283-1.html>

The Pirate Bay Wants to Encrypt the Entire Internet

BY: JANKO ROETTIGERS, NEW TEEVEE
07/09/2008

The popular torrent site, The Pirate Bay, has begun work on a new technology that could provide encryption for all Internet traffic. The goal of the program is to encrypt all data exchanged on a user's PC, regardless of the information's nature. The encryption program would still not protect against all types of interference, and some transfers could be slowed down, but the program is currently only a concept.

<http://newteevee.com/2008/07/09/the-pirate-bay-wants-to-encrypt-the-entire-internet/>

BAE SYSTEMS

BAE SYSTEMS

BAE Systems is the premier global defense and aerospace company delivering a full range of products and services for air, land and naval forces, as well as advanced electronics, information technology solutions and customer support services.

Clarifications sought on data mining

BY: BEN BAIN, FEDERAL COMPUTER WEEK
07/24/2008

Several experts at a Homeland Security Department conference expressed concern over the misunderstandings surrounding the definition of data mining. Many agreed that there needed to be clarification on the definition of data mining and specific rules governing different types of data mining. Experts worry that the confusion increases the risk of privacy violations, and want clear rules about when data can be collected and how the data can be used.

<http://www.fcw.com/online/news/153267-1.html>



Security Policy Considerations for Virtual Worlds

BY: JEFF SURRATT, HELP NET SECURITY

07/24/2008

Online virtual worlds are now offering outreach and business development opportunities. As virtual worlds are basically public forums, all communication and data can be seen by anyone, and sensitive information should not be shared. Other rules for conduct in business oriented virtual worlds include: restricting client privileges, protecting proprietary information, protecting passwords and even following the company dress code. The article suggests that employees understand that all information is publicly visible, and may remain visible for long periods of time.

<http://www.net-security.org/article.php?id=1159>

Egypt's cyberactivism has limits

BY: DOMINIC MORAN, INTERNATIONAL RELATIONS AND SECURITY NETWORK

07/22/2008

A group of 400 cyberactivists called the "April 6 Youth" met in Cairo calling for civil and democratic reform in Egypt. The group began as an industrial strike, and gained members through Facebook.com. ISPs are asked to block IP addresses or domain information relating to the group, and internet cafes have been pressured by the police to provide personal information on surfers. The internet is increasingly being used to form activist groups and promote social activism.

<http://www.isn.ethz.ch/news/sw/details.cfm?ID=19219>

Malware prevalent on trusted Web pages

BY: JABULANI LEFFALL, GOVERNMENT COMPUTER NEWS

07/24/2008

A study released by UK-based IT security firm Sophos found that there are an average of 16,173 web pages that are infected with malware or malicious code daily. The report found that commonly visited sites such as Facebook and Blogspot.com are the most common sources of malware. Sophos claims that hackers have stopped focusing primarily on email and now infect computers through the Web browser.

http://www.gcn.com/online/vol1_no1/46707-1.html

British ISP File Share Smackdown Targets Accounts, Not Users

BY: ELIOT VAN BUSKIRK, WIRED BLOG NETWORK

07/24/2008

The British government has proposed a policy that would monitor internet accounts of users who share copyrighted material. Even if the material is shared by someone other than the account holder, the user's surfing habits would be under surveillance, and connection speeds would be limited. Six ISPs have agreed to the proposed policy so far, but participation is voluntary. Critics say that parents will end up taking the fall for their children's internet use, as well as neighbors who log on to unsecured wireless networks and share copyrighted material.

<http://blog.wired.com/music/2008/07/british-isps-wi.html>



U.S. Strategic Command chief closes cyber symposium

BY: SCOTT KNUTESON, AIR FORCE LINK

07/24/2008

Gen. Kevin Chilton, the U.S. Strategic Command commander, closed the Air Force's Cyber Symposium speaking about the importance of cyberspace and the joint effort that will be required to secure cyberspace. Chilton spoke about the roles that each service member has in defending cyberspace. Maj. Gen. Charles Dunlap, Jr. also gave a briefing, focusing on the legal dimensions of cyberspace. Attendees from all branches of the armed services attended the Symposium, although the major goal of the symposium was discussing the Air Force's involvement in guarding against threats.

<http://www.af.mil/news/story.asp?id=123108010>

DNS attack code out in wild

BY: ROBERT MCMILLAN, TECHWORLD

07/24/2008

Hackers released attack code which exploits a DNS flaw, which may give hackers the ability to launch undetectable phishing attacks. Users could also be redirected to fake software updates which would install malicious software onto their computers. The flaw was accidentally disclosed by IOActive researcher Dan Kaminsky and although a patch has been available for weeks, many service providers have yet to install patches.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=102222>

Cyber Warfare: Strategy & Tactics

BY: KENNETH GEERS, INTERNET EVOLUTION

06/19/2008

This article lists five strategic reasons why cyber warfare is on the rise. These are: the internet is vulnerable, the high return on investment, the inadequacy of cyber defense, plausible deniability and the participation of non-state parties. It also lists the five forms of cyber warfare tactics: espionage, propaganda, denial-of-service, data modification, and infrastructure manipulation. Understanding the motives behind cyber crimes and the tactics that hackers use are important in improving national security planning.

http://www.internetevolution.com/author.asp?doc_id=156849

SMBs underestimate extent of cybercrime

BY: JEREMY KIRK, TECHWORLD

07/23/2008

According to a recent survey by McAfee, small businesses believe they are not attractive to hackers and spend too little time on security. Many small businesses do not have the time or the resources to devote to security, and some feel that they do not have information valuable enough to steal. Small businesses, however, have employee information as well as client information which can be stolen. McAfee recommends patching software regularly, filtering email and using anti-virus software.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=102214>



Portrait of Hackers

INFORMATION SECURITY SHORT TAKES

07/23/2008

The article outlines four different types of hackers and includes information profiling each group including age, gender, expertise level, tools, organization and threat level. Hackers are divided into four categories: hacker wannabes, hackers, criminal hackers, and disgruntled IT personnel. “Hacker wannabes” are said to be the least dangerous, as wannabe hackers are usually young teenagers, with very little expertise besides bypassing parental controls. “Criminal hackers” and “disgruntled IT personnel” are said to be very dangerous, because they are usually older, have more developed skills, and usually have broad or unlimited system access.

<http://www.shortinfosec.net/2008/07/portrait-of-attacker-types.html>

Hackers snoop on mobile phones

BY: SUJATA DUTTA SACHDEVA, TNN

07/20/2008

According to TowerGroup, a U.S.-based research firm, “smart phones” including Blackberry, Windows Mobile, iPhone and Symbian phones are vulnerable to mobile viruses and hacking. Hackers can access user’s personal information, send text messages, activate camera features, and listen in on private conversations. TowerGroup reports 200 mobile viruses currently on the loose, and states that more are undoubtedly being developed. Recommendations for protecting user information include layering security features such as antivirus, firewalls, anti-SMS spam and data encryption technologies, as well as regular security updates.

http://timesofindia.indiatimes.com/Hackers_snoop_on_mobile_phones/rssarticleshow/3254547.cms

Big Brother is Bluetoothing You

BY: TECHRADAR.COM

07/21/2008

The UK is using Bluetooth technology to track citizens whereabouts by tracking signals from mobile phones, laptops and digital cameras. The Cityware study has come under harsh criticism, although the director of the study claims that the Bluetooth scanners are not used to track individuals, but to map the behavior of city dwellers as a whole. Critics feel that if a scanner is picking up a phone conversation, or signals from a laptop or camera, the person should be aware that they are under surveillance.

<http://www.techradar.com/news/portable-devices/big-brother-is-bluetoothing-you-428026>

Regional push for Cyber Command

BY: ANDREA KOSKEY, TMCnet

07/23/2008

In an effort to bring Cyber Command to Beale Air Force Base, Yuba County Board Chairman Dan Logue has suggested banding together a group of community organizers to connect the counties surrounding Yuba County. There are 15 other air bases still under consideration to be the headquarters for Cyber Command, which could provide economic boosts for the selected area. A final decision is expected in 2009.

<http://www.tmcnet.com/usubmit/-regional-push-cyber-command-/2008/07/23/3562965.htm>



Hackers preparing to exploit DNS flaw

BY: ROBERT MCMILLAN, TECHWORLD

07/23/2008

Security experts warn that a DNS attack is imminent, after the details of a DNS vulnerability were accidentally published. Dave Aitel, chief technology officer at security vendor Immunity, warns that hackers are almost certainly working on finding the flaw, and says that attacks will likely pop up in only a couple of days. A patch for the security flaw was made available weeks ago, but many companies have not resolved the security issue yet, making them vulnerable to attacks. The estimated size of damage has varied widely.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=102212>

Top spammer sentenced to nearly four years

BY: NANCY GOHRING, COMPUTER WORLD

07/23/2008

Robert Soloway, known as the “spam king” for sending massive amounts of junk e-mail, was sentenced to 47 months in prison for fraud, spamming and tax evasion. Soloway did not damage anyone’s computer, and never sent out malicious code. Despite this defense, the court used the opportunity to hopefully dissuade other criminals from cyber crimes. Microsoft attorney Aaron Komblum emphasized the importance of sending a strong message to cyber criminals.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110518>

National security observers explain FISA ins and outs

BY: SHANE HARRIS, GOVERNMENT EXECUTIVE

07/21/2008

Amendments to the Foreign Intelligence Surveillance Act have changed government policies for collecting and monitoring communications in the United States without court orders. The revised FISA pertains only to foreign intelligence, and is not focused on spying on domestic communications. Under the new regulations, the government does not need individual warrants to monitor international communications, but the targets of the surveillance are not Americans or legal U.S. residents. American citizens are not the targets of communication monitoring, although some communication will be intercepted. The article raises several other questions about the revised FISA regulations, specifically who is targeted and the legal implications of the changes.

http://www.govexec.com/story_page.cfm?articleid=40517

Waging Communication War

BY: KENNETH PAYNE, PARAMETERS

2008

Communication has become a vital part of the struggle in Iraq and Afghanistan. The evolution of “irregular warfare” and communications has changed the face of modern warfare, leaving the United States struggling to improve cybersecurity and defense methods. With the emergence of new technologies, the importance of effective communication has become more apparent, and sometimes means the difference between victory or defeat, as well as changing the way people perceive the military and the government.

<http://www.carlisle.army.mil/usawc/Parameters/08summer/payne.htm>



NIST revises guidelines for IT security metrics

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
07/22/2008

The National Institute of Standards and Technology has released "Performance Measurement Guide for Information Security", a revised version of guidelines to ensure agencies develop security measures to meet information technology security requirements. The guidelines focus on implementing measures that gauge security policies, assessing the results of security measures, tracking performance and allocating resources. The NIST security measures provide guidance to help businesses improve security and fulfill missions.

http://www.gcn.com/online/vol1_no1/46698-1.html

Q&A: Upcoming defense IT challenges

BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
07/21/2008

Jim Hendler, a computer science professor at Rensselaer Polytechnic Institute answers questions about the Navy's involvement in developing defense IT systems. Hendler emphasizes the importance of improving interoperability both within the Navy and between services. Hendler states that the military must utilize new technologies, as enemies of the United States are using new technology to plan attacks.

http://www.fcw.com/print/22_22/procurement/153174-1.html

Details of major Internet flaw posted by accident

BY: ROBERT MCMILLAN, COMPUTER WORLD
07/21/2008

A flaw in the Internet's Domain Name System was released accidentally weeks before details were due to be disclosed. IOActive researcher Dan Kaminsky discovered the flaw several months ago, and vendors including Microsoft, Cisco, and the Internet Systems Consortium released a fix for the flaw weeks ago. Details were to be disclosed at the Black Hat security conference on August 6.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110418>

Cybersecurity Will Take A Big Bite of the Budget

BY: WALTER PINCUS, WASHINGTON POST
07/21/2008

President Bush has singled out cyberspace as the most important initiative in the fiscal 2009 intelligence budget, making the largest request for funds for the Comprehensive National Cybersecurity Initiative. The Initiative is designed to secure government computer systems and will later be expanded to cover sensitive civilian systems. Mike McConnell, Director of National Intelligence, said that the government must move from discovering intrusions and cleaning up the damage to developing proactive measures to prevent intrusions.

<http://www.washingtonpost.com/wp-dyn/content/article/2008/07/20/AR2008072001641.html>

DHS seeks cybersecurity capability info

BY: BEN BAIN, FEDERAL COMPUTER WEEK
07/21/2008

The Homeland Security Department is looking to the private sector to help implement the Trusted Internet Connection Initiative, which aims to reduce the number of access points that



federal agents use to connect to the Internet. DHS is looking for interested companies with knowledge of EINSTEIN data analysis, the Trusted Internet Connection Initiative and compliance metrics.

<http://www.fcw.com/online/news/153190-1.html>

Open source software a security risk, study claims

BY: ELLEN MESSMER, NETWORK WORLD

07/21/2008

A study by Fortify Software evaluated 11 open source software packages, and found that most open source software does not adhere to even minimal security best practices. Jacob West, manager of the security research group, explained that there needs to be more confidentiality in reporting bugs, so that when the public is notified of vulnerabilities, attackers will not have early information to exploit. West also said that open source communities don't seem to be mindful about security practices like commercial companies who charge for software.

<http://www.networkworld.com/news/2008/072108-open-source-security-risk.html>

Secret Defense Data Lost on UK Government USBs

BY: JAMES ROGERS, DARK READING

07/18/2008

The United Kingdom's Ministry of Defence admitted that 121 USB sticks have been lost or stolen since 2004, including five that held secret information. The UK has lost an array of laptops, mobile phones and two disks containing welfare information. Japan had a USB drive stolen that contained sensitive information on military exercises with the U.S. Sweden had a USB drive containing military secrets found in a public library. Despite these events, surveys have found that almost three quarters of organizations still use removable media to hold sensitive information.

http://www.darkreading.com/document.asp?doc_id=159479

Elder, analyst keynote Air Force cyber symposium

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES

07/21/2008

The Air Force held a cyberspace symposium at the Air Force's Air University at Maxwell Air Force Base, Ala. Major presenters included Air Force cyber architect Lt. Gen. Robert J. Elder Jr. and analyst Rebecca Grant. The goal of the symposium was to bring together professionals from the cyberspace community to share ideas and discuss the implications of cyberspace. Elder's speech focused on defining cyberspace and its relationship to national security and the Air Force. Elder emphasized that cyberspace is not set up as a hierarchy, but as an interconnected network, and is a concern for every sector, not just the military.

<http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20080721/NEWS01/807210327>

Another ex-Soviet state under fire in web attack

BY: JEREMY KIRK, TECHWORLD

07/21/2008

The website for the president of Georgia was knocked offline by hackers for about a day by a botnet that is "frequently used by Russian bot herders" according to the Shadowserver Foundation. Lithuania, Estonia and now Georgia are all countries experiencing political friction with Russia, and have all been victims of cyberattacks. All three have taken steps to separate



themselves from Russia, and Georgia angered Russia specifically by pushing for entry into NATO.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=102194>

Security analysts praise Obama's pledge for a cyber chief

BY: JILL AITORO, NEXTGOV

07/18/2008

James Lewis, director of the technology and public policy program at the Center for Strategic and International Studies, praises Obama's promise to elect a national cyber advisor who would report directly to him. Obama spoke about making cyberspace a national priority at a summit on national security at Purdue University. Obama did not offer specific details on where a cybersecurity advisor would work. Bruce McConnell, who served three administrations on national information issues, emphasized the importance of giving the position more authority and some part in the decision structure. McConnell recommends that the cybersecurity advisor hold a senior-level position within the National Security Council, which is the president's primary forum for national security and foreign policy issues.

http://www.nextgov.com/nextgov/ng_20080718_2930.php

Researchers trace structure of cybercrime gangs

BY: JEREMY KIRK, TECHWORLD

07/16/2008

According to research by security company Finjan, the structure of a cybercrime gang is similar to the structure of the Mafia, organized as a pyramid of hackers, data sellers, managers and programmers. Data is supplied by affiliate networks, and then is marketed by salespeople, who report to a boss who handles distribution of crimeware. Finjan went to data selling websites, and established relationships with different groups to learn more about the hierarchy system.

<http://www.techworld.com/security/news/index.cfm?newsid=102157>

Symposium gets to core of Air Force's role in cyberspace

BY: SCOTT KNUTESON, AIR FORCE LINK

07/18/2008

Maxwell Air Force Base hosted a week-long cyberspace symposium which brought together 250 professional civilian and military information experts to discuss the implications of cyberspace with regard to the Air Force and national defense. 8th Air Force, which helped host the symposium, currently serves as the air component headquarters to the U.S. Strategic Command for cyberspace operations, although plans to select a permanent host base for Air Force Cyber Command are underway. Lt. Gen. Allen Peck explained that Maxwell Air Force Base was a fitting choice for the symposium as an intellectual and leadership center of the Air Force.

<http://www.af.mil/news/story.asp?id=123107290>

Symantec products Common Criteria-certified

BY: JOAB JACKSON, GOVERNMENT COMPUTER NEWS

07/18/2008

Symantec's Endpoint Protection and Network Access Control security packages achieved Common Criteria Evaluation Assurance Level 2 (EAL-2), which is an ISO-recognized set of security requirements. In order to have products certified, independent laboratories verify that



the products meet security requirements developed by government agencies and private companies. Criteria include functionality, development environment and product testing.
http://www.gcn.com/online/vol1_no1/46682-1.html

U.S. Air Force lets Web 2.0 flourish behind walls

BY: STEPHEN LAWSON, COMPUTER WORLD
07/18/2008

The Air Force is using Web 2.0 technologies including blogs, wikis and personal profiles, despite concerns about internet security. The Air Force Knowledge Now initiative hopes to help service members find information more quickly as well as share information with the Army, Navy and Marines. Response from service members has been positive, although personal blogs are becoming a problem for operational security, when military personnel and even spouses or friends of military personnel post sensitive information.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110300>

'No decision' on giant database

BBC NEWS
07/17/2008

Richard Thomas, the UK's Information Commissioner, had called for a full public debate regarding the proposed giant database. Thomas explains that the database, which is part of the new Communications Data Bill, would violate privacy by changing the policies for acquiring personal communications data, and explains that having a giant database could possibly make personal information more vulnerable to attackers.

http://news.bbc.co.uk/2/hi/uk_news/politics/7511671.stm

Army Secretary: We're Falling Behind Online

BY: DAVID AXE, WIRED BLOG NETWORK
07/17/2008

Army Secretary Pete Geren explains how Army leaders have fallen behind the development of digital communications. The Army is still ahead of the other military services regarding the Internet. For example, the U.S. Military Academy in West Point is creating Army-specific Web 2.0 tools, and the Army's graduate school in Kansas had added blogging to their curriculum. While the Army has embraced the Internet as a means of communication, other services, specifically the Air Force, still view the Internet as a battlefield to dominate.

<http://blog.wired.com/defense/2008/07/army-secretary.html>

Obama Wages Cyberwar

BY: NOAH SCHACHTMAN, WIRED BLOG NETWORK
07/16/2008

In a speech at Purdue University, Barack Obama stated that the United States is behind other countries, such as China, when it comes to cybercrime. Obama promised to "make cyber security the top priority that it should be in the 21st century." Obama also spoke about appointing a National Cyber Advisor and bringing together government, industry and academia to protect national security networks.

<http://blog.wired.com/defense/2008/07/obama-wages-cyb.html>



Schneier, Team Hack 'Invisibility Cloak' for Files

BY: KELLY JACKSON HIGGINS, DARK READING

07/16/2008

BT security expert Bruce Schneier and a group of researchers found that Microsoft Vista, Word, and Google Desktop were all able to find files that were “hidden” with a deniable file system (DFS) feature. DFS is supposed to mask the existence of files by first encrypting the file, and then hiding it within an encrypted area of the disk drive. TrueCrypt developers have just released a new version of the software which patches the leaks in the denial file system, however, Schneier claims DFS is easier to hack than encryption alone, and that its unlikely that all of the leakages could have been closed.

http://www.darkreading.com/document.asp?doc_id=159192

Major sites fall victim to Web hijack; check yours

BY: ERIK LARKIN, COMPUTER WORLD

07/17/2008

Security company Finjan released a list of over 1000 sites infected by the attack toolkit Asprox. This article explains how a company can check their own site for infection by running a Google search, although visiting any of the sites found could infect the visitor's computer. There are three searches to use, and HP also offers a free Scrawl tool which can search a company's site for vulnerabilities.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110240>

Romanian authorities arrest cybercrime suspects

BY: GRANT GROSS, COMPUTER WORLD

07/16/2008

Romanian authorities have arrested more than 20 people accused of stealing identities online on multiple websites, including some U.S. websites like eBay. \$640,000 from non-Romanians was stolen in the phishing scheme, which involves sending emails that look like official bank or credit card correspondence. Gary Warner, director of research in computer forensics at the University of Alabama at Birmingham, states the arrests are an example of the successes of international cooperation. The United States FBI and Romanian law enforcement have been working together to find the identities of the criminals in recent months.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110222>

Bush leads biometric push

BY: BEN BAIN, FEDERAL COMPUTER WEEK

07/16/2008

The new National Security Presidential Directive 59/Homeland Security Presidential Directive 24 requires agencies to share biometric information including methods for collecting and storing biometric information. The directive also explains how biometrics policy has not kept up with emerging technology, and encourages agencies to decide on similar and consistent practices in collecting and sharing biometric data. Rep. Mark Souder, a member of the House Homeland Security Committee's Border, Maritime and Global Counterterrorism Subcommittee, emphasizes the importance of open data sharing between government agencies, and states that the government enforced information sharing would increase interoperability.

http://www.fcw.com/print/22_17/policy/152825-1.html#



Government, health care Web sites attacked

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
07/16/2008

Internet security company Finjan Inc. found that more than 1000 websites have been compromised in recent weeks by an attack toolkit named Asprox, which searches Google for vulnerable web pages that have an .asp file extension. Finjan found that 13% of the infected websites belonged to the government, and 12% belonged to health care organizations. Finjan recommends using application firewalls and real-time content inspection tools to protect their browsers, and offers a free browser plug-in for content inspection.

http://www.gcn.com/online/vol1_no1/46651-1.html

Insider threat looms large as San Francisco's network crisis plays out

BY: ELLEN MESSMER, NETWORK WORLD
07/16/2008

Terry Childs, who has worked for the city of San Francisco for five years as a computer engineer, was arrested for refusing to relinquish control of the city's network. Childs was arrested for alleged computer tampering, and it is believed that he installed means to destroy sensitive electronic documents when he learned that he would be fired. The article also describes the concerns of some companies about threats from employees and insiders to computer security.

<http://www.networkworld.com/news/2008/071608-insider-threat.html>

Vulnerabilities Could Expose Broad Range of Java Apps

BY: TIM WILSON, DARK READING
07/16/2008

Two security vulnerabilities have been found in Spring Framework, an open-source environment for developing Java applications. The first vulnerability allows attackers to change user data and queries, and the second allows attackers to query the application for information, which could potentially expose sensitive information from the Java application. Ounce Labs, who exposed the vulnerabilities, have also published recommendations for how to fix the applications and improve future development processes.

http://www.darkreading.com/document.asp?doc_id=159170

Technology companies devise cyber security, defensive software, to combat the threat of information warfare

BY: COURTNEY E. HOWARD, MILITARY & AEROSPACE ELECTRONICS
7/17/2008

Information warfare is taking on more forms and becoming increasingly popular as the government and industry work to protect vulnerable critical infrastructures. Hacking tools have been found on the computers of terrorists, including known members of Al Qaeda. Richard Clarke, former presidential advisor for Cyberspace Security and chief terrorism advisor to the U.S. National Security Council explains the United States' critical infrastructures are built upon a fragile and penetrable network that must be secured and fortified. The article also emphasizes the importance of information sharing to protecting critical infrastructures.

http://mae.pennnet.com/display_article/334213/32/ARTCL/none/EXCON/1/Technology-companies-devise-cyber-security,-defensive-software,-to-combat-the-threat-of-information-warfare



CyberPro

Volume 1, Edition 6
July 31, 2008

Keeping Cyberspace Professionals Informed

Analysts seek deterrence strategy for space and cyberspace

BY: MICHAEL BRUNO, AEROSPACE DAILY & DEFENSE REPORT

07/17/2008

The United States Defense Department is analyzing ways to apply Cold War deterrence strategies to space and cyberspace. Suggestions included developing an international response to a cyber attacks and attacks on space assets. Both presidential candidates Sen. Barack Obama and Sen. John McCain have called for extending the United States defense capabilities beyond Iraq, specifically focusing on the conflict in Afghanistan.

CyberPro Content/Distribution

This newsletter is intended to serve as a snapshot of Cyber-related events and issues, and is distributed every two to three weeks. Feel free to forward this newsletter to other interested individuals. If you have information you think should be included, or if you would like to be added or removed from distribution, please e-mail [CyberPro News Subscription](#).

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or the [National Security Cyberspace Institute](#).