CyberPro

Volume 1, Edition 10
September 25, 2008

Keeping Cyberspace Professionals Informed

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.

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.

To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.

Please contact Larry McKee , ph. (757) 871-3578, regarding CyberPro subscription, sponsorship, and/or advertisement.

CyberPro

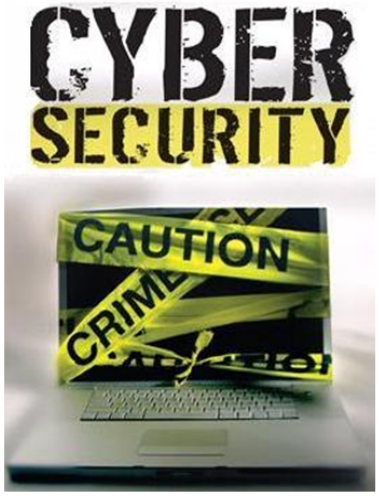
Volume 1, Edition 10
September 25, 2008

Keeping Cyberspace Professionals Informed

Conference Co-hosts:

Keeping Cyberspace Professionals Informed

2008 Hampton Roads Cyber Security Awareness Conference



Date: October 21, 2008

Time: 8:00 am - 4:30 pm

Hampton Roads Convention Center
1610 Coliseum Drive
Hampton, VA 23430

Contact person:
Larry McKee
Larry.McKee@nsci-va.org
Ph. (757) 871-3578

Conference Sponsors

The City of Hampton and National Security Cyberspace Institute are pleased to announce the 2008 Hampton Roads Cyber Security Awareness Conference (HRCSAC) to be held on October 21 at the Hampton Roads Convention Center.

Cyber Security is a fundamental building block for facilitating commerce and securing the homeland. Over the next few years we will see tremendous growth and innovation in cyber security.

This one-day event brings together professionals for thought-provoking presentations on current cyberspace issues and best-practices to facilitate improved cyber security.

Highlights

- The core mission of the conference is to inform the community about cyberspace security challenges and opportunities.
- Attendees will gain knowledge from local government, industry, and Department of Defense experts on existing and emerging cyberspace organizations, concepts, challenges, and activities.
- Attendee Profile: A mix of academia, military, industry experts and government officials, including decision-makers from numerous local, state, and federal agencies.

- Attendee check-in and continental breakfast will begin at 7:00 am.
- Speakers will include state and local government officials, industry, and military experts.
- Registration fee of $75 includes one-day event, continental breakfast, and lunch

REGISTER EARLY TO RESERVE YOUR SEAT: https://www.regonline.com/hrcsac

More information is available at: http://nsci-va.org/hrcsac

CyberPro

Volume 1, Edition 10
September 25, 2008

Keeping Cyberspace Professionals Informed

TABLE OF CONTENTS

CyberPro

Volume 1, Edition 10
September 25, 2008

Keeping Cyberspace Professionals Informed

CYBERSPACE BIG PICTURE

The Winner Is . . .

BY: BOB BREWIN, GOVERNMENT EXECUTIVE
09/22/2008

Pentagon leadership has determined that the U.S. Strategic Command in Omaha, Neb. will lead a joint cyber command, taking some Cyber control form the Air Force. STRATCOM will reportedly announce formation of the organization in October. STRATCOM currently has the Joint Task Force-Global Network Operations handling defense of the military's Global Information Grid, and the new joint command will be responsible for network attack and defense.
http://www.govexec.com/story_page.cfm?filepath=/dailyfed/0908/092208wb.htm

Draft Cybersecurity Review Has Department On Defensive

BY: CHRIS STROHM, NATIONALJOURNAL.COM
09/22/2008

A commission of cybersecurity experts established by the Center for Strategic and International Studies believes that the Homeland Security Department should not be in charge of securing federal computer networks. Homeland Security was originally given the task of securing federal and key private sector networks under the Bush administration's cybersecurity initiative, but the commission feels that it is difficult to determine who is in charge and not much is being done. Robert Jamison, undersecretary for Homeland Security's national protection and programs directorate argues that they have developed a comprehensive strategy as evidenced by the decrease of government Internet access points from 4000 to fewer than 1000. Jamison also states that there are devices that will be installed in federal civilian networks by the middle of next year which will provide real time detection of intrusions.
http://www.nationaljournal.com/congressdaily/cdp_20080922_3512.php

Upcoming transition creates uncertainty

BY: BRIAN ROBINSON, FEDERAL COMPUTER WEEK
09/22/2008

James Lewis, a senior fellow at the Center for Strategic and International Studies explains that the upcoming transition to a new administration will be a critical time for the Comprehensive National Cybersecurity Initiative (CNCI). Both the McCain and Obama presidential campaigns have shown support for increased cybersecurity initiatives, and both will receive independent recommendations on cybersecurity including analysis of the CNCI. Mark Gerencser, a senior partner at Booz Allen

Hamilton states that he sees signs of CNCI being taken more seriously including efforts from the Office of the Director of National Intelligence and increasing Congressional involvement.
http://www.fcw.com/print/22_31/features/153840-1.html?CMP=OTC-RSS

Unlocking the national cybersecurity initiative

BY: BRIAN ROBINSON, FEDERAL COMPUTER WEEK
09/22/2008

The Bush Administration's cybersecurity initiative, launched earlier this year, is still mostly secret, but Amit Yoran, a former director of DHS National Cyber Security Division explains that all cybersecurity initiatives have been organized under the Homeland Security Department. This is the first time a single office is in charge of coordinating the work of many different federal cybersecurity organizations. The classified cybersecurity initiative, included in the Homeland Security Presidential Directive 23 was issued on January 8. The article lists the few details that are currently publicly known, and comments on the future of the cybersecurity efforts.
http://www.fcw.com/print/22_31/features/153818-1.html

Today's Airborne Military Communications Market - It's More than Radios

FORECAST INTERNATIONAL, INC.
09/22/2008

Military communications systems currently consist of voice, data, video and imagery communications including encryption protection. These advanced systems have created an estimated $3 billion market for the development of airborne defense communications systems over the next decade. Forecast International has released "The Market for U.S. Military Airborne Communications Systems" which analyzes current and future military communications systems, including an analysis of the leading program, Northrop Grumman's Integrated Communications, Navigation and Identification Avionics System which is estimated to account for 30% of total market sales in the next ten years.
http://www.asd-network.com/press_detail_B.asp?ID=17756&NID=71163

U.S. Cybersecurity Is Weak, GAO Says

BY: KEITH EPSTEIN, BUSINESS WEEK
09/15/2008

According to Government Accountability Office reports, the U.S. Computer Emergency Readiness Team (US-CERT) is experiencing problems due to management changes, lack of timely security alerts and a lack of access to networks. The Department of Homeland Security had lead cybersecurity efforts for five years, and still has not produced "a truly national capability" according to one GAO report. The article explains in detail the lack of a system for releasing warning and notifications in the event of a cybersecurity threat. The GAO also emphasizes the importance of advising the next administration to develop a "coherent national strategy" for approaching security threats.
http://www.businessweek.com/technology/content/sep2008/tc20080915_347282.htm?chan=top+news_top+news+index+-+temp_news+%2B+analysis

CIO Council creates security committee

BY: MICHAEL HARDY, FEDERAL COMPUTER WEEK
09/12/2008

The Security and Identity Management Committee, which was created by the Chief Information Officers Council, will work to address security and identity management problems. The panel will also work to improve and coordinate a "secure, well-protected national cyber infrastructure". Co-chairs of the

committee are Navy CIO Robert Carey and Justice Department CIO Vance Hitch.
http://www.fcw.com/online/news/153767-1.html

US Focusing Cybersecurity on Backdoors in Tech Products

BY: GRANT GROSS, PCWORLD
09/15/2008

According to the Department of Homeland Security, the National Cybersecurity Initiative, announced in January, will take the place of previous government defense systems and will include improving protection against malicious code installed during electronic device manufacturing processes. Paul Schneider, deputy secretary at DHS explained that the government will work with private vendors to address "supply-chain concerns" and will develop stricter rules for acquiring tech products. The initiative also focuses on other issues including information sharing between the government and the private sector, recruiting more cybersecurity experts for U.S. agencies and educating Internet users.
http://www.pcworld.com/businesscenter/article/151075/us_focusing_cybersecurity_on_backdoors_in_tech_products.html

Homeland Security: Don't take away our cybersecurity responsibility

CNET.COM
09/22/2008

In response to critics arguing that the U.S. Department of Homeland Security should no longer be in charge of the nation's cybersecurity efforts, DHS Undersecretary Robert Jamison wrote that we must "stay the course". Members of the CSIS cybersecurity commission told Congress that the DHS has proved incapable of handling cybersecurity and that responsibility should be moved to the White House. James Lewis of the CSIS claims that there is no clear leadership from the DHS and that only the White House has the authority and oversight to provide the interagency coordination and focus required for cybersecurity.
http://news.cnet.com/8301-13578_3-10048063-38.html

Should NSA take over federal cybersecurity efforts?

CNET.COM
09/19/2008

The Center for Strategic and International Studies' Commission on Cybersecurity for the 44th President have made recommendations to take the lead role over cybersecurity away from the U.S. Department of Homeland Security. The commission states that a new White House program on cybersecurity should have authority over all agencies and departments that secure the country's networks. Some believe that the lead should be transferred to intelligence agencies such as the CIA or the National Security Agency which already have critical expertise in cybersecurity.
http://news.cnet.com/8301-13578_3-10045980-

38.html?part=rss&subj=news&tag=2547-1_3-0-20

New Al Qaeda Tape Surfaces Despite US Efforts to Block It

BY: BRIAN ROSS, ABC NEWS
09/19/2008

Al Qaeda's annual September 11 video surfaced, delayed by eight days due to U.S. efforts to block it. There were no pictures or videos from Osama bin Laden, but there was a video that Al Qaeda claims they captured from U.S. bounty hunter Keith "Jack" Idema. Former CIA intelligence officer John Kiriakou explained that intelligence operations have tried to block videos in the past, and this was the first year the video was delayed past September 11, although U.S. officials did not expect to block the video altogether. Intelligence sources claim the United States has improved infiltration into the al Qaeda internet distribution network.
http://abcnews.go.com/Blotter/story?id=5841873&page=1

Cybersecurity is crucial to protecting nation's water supply, official says

BY: GAUTHAM NAGESH, GOVERNMENT EXECUTIVE
09/15/2008

During a U.S. Chamber of Commerce event, Bruce Larson, the security director for American Water, stated increasing technology and use of computer systems has increased the need for advanced cybersecurity measures. Many utility companies use industrial control systems that run on platforms such as Microsoft Windows, which leaves the companies vulnerable to hackers or enemy states. Larson claims security should be built into new control systems which would require collaboration between the private sector and the Homeland Security Department. Larson also recommends having backup servers and IT infrastructures to avoid disruption of service, and stated the oil, gas and electrical industries are also facing similar security issues.
http://www.govexec.com/story_page.cfm?articleid=40971&dcn=todaysnews

Commission to recommend DHS loses cybersecurity oversight role

BY: JASON MILLER, FEDERAL NEWS RADIO
09/17/2008

The Government Accountability Office issued three reports on the Homeland Security Department's efforts to secure federal computer networks, and all three found "significant shortcomings" especially in making warnings to agencies and industry, and updating the cyber exercise, Cyber Storm. Jim Lewis, director of the Center for Strategic and International Studies' technology and public policy program, believes that cybersecurity is a problem of "international proportions" and may be too large for the DHS alone. Lewis also states that only the White House has the authority and influence necessary to effectively oversee cybersecurity, and moving responsibility to the White House will be recommended by the Commission on Cyber Security for the 44th Presidency.
http://www.federalnewsradio.com/?nid=169&sid=1479802

Panel says DHS botching cyber security

BY: SHAUN WATERMAN, UNITED PRESS INTERNATIONAL
09/17/2008

David Powner of the Government Accountability Office testified before the House Homeland Security Committee, stating the DHS is not effectively defending federal computer networks and lacks coordination with the private sector. Spokeswoman for the DHS, Laura Keehner, calls the accusations "political posturing" and claims the DHS has made significant improvements in cyber security since receiving the lead role in 2003. The DHS also acknowledges that there is room for

improvement, but requests more time to prove that they are making advances in protecting federal networks.
http://www.washtimes.com/news/2008/sep/17/panel-says-dhs-botching-cyber-security/

Critics: Homeland Security unprepared for cyberthreats

CNET.COM
09/17/2008

The Department of Homeland security is facing serious criticism of its ability to lead cybersecurity efforts, including recommendations that the responsibility be moved to another federal agency or the White House. Both the Commission on Cybersecurity for the 44th Presidency, which is expected to release a formal report in November, and two reports from the Government Accountability Office point out shortcomings from the DHS. James Lewis, a director at the Center for Strategic and International Studies, emphasizes the importance of a strong cybersecurity strategy from the new administration, and both Obama and McCain have representatives on the CSIS commission.
http://news.cnet.com/8301-13578_3-10043665-38.html

Panel says DHS should not oversee cybersecurity

BY: JILL R. AITORO, NEXTGOV
09/16/2008

Nextgov.com interviewed Jim Lewis, program manager of the Commission on Cybersecurity for the 44th Presidency, in response to the Commission's recommendations to move cybersecurity from the Department of Homeland Security to the White House. Lewis states the DHS lacks authority and interagency oversight that is necessary to oversee cybersecurity strategy. The commission points to lack of focus, overlapping missions and poor coordination and collaboration among agencies as primary concerns facing the DHS. Lewis also details capabilities that he feels must be improved before the United States can influence global cybersecurity efforts.
http://www.nextgov.com/nextgov/ng_20080916_4289.php?zone=ngtoday

Telecoms body slammed for endangering Net anonymity

BY: PETER SAYER, IDG NEWS SERVICE
09/15/2008

The International Telecommunications Union produced a draft recommendation which would make it possible to trace the origin of Internet traffic to its source IP address. Privacy advocates oppose the IP tracing as it would remove some anonymity on the Internet. The International Telecommunication Union met in Geneva to discuss traceback use and requirements and different ways to identify the source of information sent across IP networks
http://www.techworld.com/security/news/index.cfm?newsid=104394&pagtype=all

Officials talk cyber initiative with industry

BY: BEN BAIN, FEDERAL COMPUTER WEEK
09/15/2008

Officials from the Homeland Security Department, the Office of the Director of National Intelligence, the White House and other agencies spoke with an industry group about details included in the Bush administration's new cyber initiative including areas of counterintelligence, supply chain security and research and development. The DHS' deputy secretary, Paul Schneider, explained that three focus areas of the initiative are establishing defense against attacks and current vulnerabilities, utilizing intelligence to counter threats, and investing in research and technology. Officials are emphasizing the importance of collaboration between federal agencies and the private sector in order to address security threats.

http://www.fcw.com/online/news/153789-1.html

Homeland Security to direct cybersecurity initiative

BY: JILL R. AITORO, NEXTGOV
09/15/2008

Paul Schneider, deputy secretary of the Department of Homeland Security announced that the Department would lead President Bush's new cybersecurity initiative under the direction of Robert Jamison, undersecretary for national protection and programs at DHS. The Defense Department and intelligence agencies will also work with the DHS. The DHS will focus on protecting civilian federal computer networks by reducing network access points and will also implement improvements to Einstein, which monitors and analyzes online activity information. The National Cybersecurity Center will use that information to establish common security procedures across civilian, defense and intelligence agencies.
http://www.nextgov.com/nextgov/ng_20080915_3583.php

Council points to security challenges

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
09/15/2008

A report from the Homeland Security Advisory Council found that the new presidential administration will face challenges in homeland security including border security, information sharing and disaster response. The report recommends advancing homeland security, examining current programs and developing a better oversight system, improving intelligence and information sharing through education and training, improving security research and development, and improving disaster response in critical infrastructures.
http://www.fcw.com/online/news/153785-1.html

DHS rejects criticism of agency as Beltway politics

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD
09/17/2008

The Department of Homeland Security has dismissed recent claims by the Commission on Cyber Security for the 44th Presidency that the DHS should relinquish control of the nation's cybersecurity initiatives to the White House. The commission states the DHS lacks the leadership, implementation capabilities and influence both at the federal level and among the private sector to enforce security improvements. Laura Keehner, a DHS spokeswoman, states the criticism is a "political gambit" and feels that progress made so far by the DHS is being overlooked. The article also explains advanced details of the recommendations that were made.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9114938&taxonomyId=17&pageNumber=1

Juniper cranks up security gateways for 10G Ethernet

BY: TIM GREENE, NETWORK WORLD
09/15/2008

Juniper has introduced new security gateways that are able to handle massive traffic streams in corporate networks. The new SRX Dynamic Service Gateways provide various security services, designed to provide better protection than traditional firewalls. In addition to firewalls, "the devices support network address translation, intrusion prevention, denial-of-service protection, quality of service and dynamic routing". Software can also be used to add new services to the processing cards and additional capabilities will be added over time.
http://www.networkworld.com/news/2008/091508-juniper-security-gateways.html?fsrc=netflash-rss

Google search finds seafaring solution

BY: MURAD AHMED, TECHNOLOGY TIMES
09/15/2008

Google is considering placing computers necessary for operation of its search engines on barges anchored offshore. These data centers would use wave energy to both power and cool computers in an effort to reduce costs, avoid paying property taxes on data centers and increase energy efficiency. Other companies are considering radical approaches to energy efficiency including Microsoft, who has investigated placing data centers in the cold climate of Siberia. The major concern for the offshore data centers is protection from natural events such as hurricanes.
http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4753389.ece

MySpace At War

STRATEGY PAGE
09/11/2008

The U.S. government has utilized software from companies including Google and Wikipedia for use in internal networks, and is currently installing a classified version of MySpace. The CIA, NSA, and Department of Defense all use these internal networks to find and share information in formats that are basically identical to what Internet users use. The intelligence community has found that the Google and Wikipedia formats are popular with staff and the familiar formats allow the intelligence agencies to implement the tools without much additional training. The internal MySpace, called "A Space" will be available September 22 to all sixteen U.S. intelligence agencies.
http://www.strategypage.com/htmw/htintel/articles/20080911.aspx

50-State Cyber Strategy

BY: BOB BREWIN, GOVERNMENT EXECUTIVE
06/16/2008

In an attempt to secure government backing and money, the Air Force Cyber Command planned to form a cyber unit in every state. These network operations sites are located in all 50 states although eight bases are considered centers of power. These include bases in Washington, Virginia, New York, Louisiana, Texas, Colorado, Nebraska and Illinois. The list of these eight bases is included in the article. 18 states also entered the competition for the command's new headquarters which was planned to be announced in September 2009. The article also includes a brief summary of goals of the new cyber command, new jobs, and possible slogans and badges.
http://www.govexec.com/dailyfed/0608/061608wb.htm

CYBERSPACE RESEARCH

'Profiler' Hacks Global Hacker Culture

BY: KELLY JACKSON HIGGINS, DARK READING
09/23/2008

Raoul Chiesa, a reformed hacker and the director of communications for the Institute for Security and Open Methodologies (ISECOM), is leading the Hackers Profiling Project together which involves building a database of different types of hackers based on surveys of over 1000 hackers worldwide. Chiesa hopes to prevent cyber crime and learn about different types of criminal hackers, different types of attacks and possible ties to organized crime and cyber terrorism. Although the project is only halfway complete, many organizations are already taking advantage of early data. One company, for example, contacted ISECOM for information

about hacking in Romania when considering moving its IT headquarters. The project's early findings will be published in the book *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* in November.
http://www.darkreading.com/document.asp?doc_id=164364&WT.svl=news1_1

NIST needs a few good ideas

BY: KEVIN MCCANEY, GOVERNMENT COMPUTER NEWS
09/16/2008

The National Institute of Standards and Technology has issued a request for suggestions of national needs that could be improved by new technologies. These suggestions would qualify for competitions for research and development funding under NIST's Technology Initiative Program. The program aims to conduct research that addresses areas of critical national need and funds projects from small/midsize businesses and academia, nonprofit organizations and national laboratories. The complete guide for submitting white papers is available on the NIST Web site.
http://www.gcn.com/online/vol1_no1/47165-1.html?topic=&CMP=OTC-RSS

Juniper invests in Packet Design

BY: JIM DUFFY, NETWORK WORLD
09/15/2008

Juniper Networks has provided a $2 million investment to Packet Design, which develops routing analysis and optimization software. The funding will go towards the development of network management products and improving Packet Design's international sales force. Former Cisco CTO and former Cisco Chief Scientist Van Jacobson founded Packet Design in 2003. Juniper issued a statement calling Packet Design "an innovator in both routing and traffic analysis".
http://www.networkworld.com/news/2008/091508-juniper-packet-design.html?fsrc=netflash-rss

Hackers prevent research on malicious code

BY: DAN RAYWOOD, SC MAGAZINE
09/17/2008

Websense Security Labs claims that malware tracking is becoming more difficult because cybercriminals are randomizing content on malicious web pages, which prevents security researchers from being able to analyze the malware. Carl Leonard, security research manager at Websense explains that authors of malware are able to see the person attempting to access the malware and then decide whether or not to present it. The company investigated a spam email by following a link should have led them to malware, but were instead given a "403 forbidden" response.
http://www.scmagazineus.com/Hackers-prevent-research-on-malicious-code/article/118099/

Disclosure of Major New Web 'Clickjacking' Threat Gets Deferred

BY: KELLY JACKSON HIGGINS, DARK READING
09/16/2008

Web security researchers Robert Hansen and Jeremiah Grossman have delayed presenting

details of a new Web attack at the request of Adobe until the company could develop a patch. The researchers had planned to release their proof-of-concept code at the OWASP USA security conference in New York. The researchers found a vulnerability that allowed "clickjacking" attacks in browsers including Microsoft's and Mozilla's that affects Adobe's application that could allow other attacks like cross-site scripting, SQL injection and cross-site request forgery. Although details have not been released, it is known that the attack could originate from a victim clicking a malicious link or through a Website infected with malicious code. Grossman explains that he is surprised that Adobe took responsibility for the vulnerability that should have been the browser vendors, and claims that a patch from Adobe will fix only 90% of the problem.
http://www.darkreading.com/document.asp?doc_id=163928&WT.svl=news1_1

CISO Perspectives: The Einstein Program

GOVERNMENT COMPUTER NEWS
09/12/2008

In response to increasing cyberattacks against United States network infrastructures, President Bush's Cyber Initiative order allowed the National Security Agency to monitor federal computer networks. The initiative also authorized Einstein sensors on government Internet access points, which capture federal network traffic for analysis. The article gives a detailed outline of the kind of data that is collected by the Einstein Program. The article also discusses in detail the challenges facing the Einstein Program, including assumptions that the targeted agencies have trained and capable personnel for incident response and the wide variances between federal department and agencies regarding incident response. Response to these challenges is necessary to improve the program's effectiveness and improve cybersecurity warnings and indicators.
http://www.gcn.com/online/vol1_no1/47139-1.html?topic=&CMP=OTC-RSS

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

CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

CISO Perspectives: Deep packet inspection

GOVERNMENT COMPUTER NEWS
09/12/2008

Deep packet inspection (DPI), which merges Intrusion Detection Systems and firewalls, examines network traffic and is essential for identifying viruses, spam, rootkits, and malware. Despite the overwhelming security advantages, federal chief information security officers have been slow to adopt DPI technology. The article examines the reasons for this delay which include enterprise enumeration, a lack of centralized control and management, compliance issues, and the lack of budgetary resources. The article explains each challenge for DPI implementation in detail.
http://www.gcn.com/online/vol1_no1/47132-1.html?page=1

Waking Up to the Clouds

BY KENNETH CORBIN, INTERNETNEWS.COM
09/15/2008

A study release by the Pew Internet and American Life Project found that 69% of Internet users who access "cloud-based applications" such as Webmail and YouTube do not have a clear understanding of how the applications are being provided. John Horrigan, associate director of the Pew Internet Project, presented the research at a policy talk in Google's Washington D.C. headquarters and said that users appreciate the convenience of these applications, but are concerned about how their data is used. The Pew study examined six common cloud computing activities including Webmail, photo storage, online applications, video storage, online file storage, and online hard drive backup. 68% of participants said they would oppose companies analyzing personal data for advertising, 80% opposed their information showing up in marketing campaigns and 90% showed concern about companies selling the contents of their personal files.
http://www.internetnews.com/webcontent/article.php/3771406/Waking+Up+to+the+Clouds.htm

Cybercrime 'Major Business Risk'

BY: ELLEN MESSMER, NETWORK WORLD
09/14/2008

Security firm Finjan surveyed 1,387 IT professionals and found that 91% of those who responded thought that cybercrime was a "major business risk". 73% said that they were more concerned about data theft than damage from malware, and 25% said that they had experienced data breaches. TigerDirect, which has 30 retail stores and an online store, explained the majority of identity theft occurs in online purchases. TigerDirect has developed a system which gives an alert if a credit card payment comes from an IP address in Eastern Europe or if the credit card number has been through an "anonymizer site" which attempts to hide the originating IP address.
http://www.pcworld.com/businesscenter/article/151051/cybercrime_major_business_risk.html

Analysis: New measure for cybersecurity

BY: SHAUN WATERMAN, SPACE DAILY
09/11/2008

A group of 80 experts from academia, private sector and government, which was formed by the Center for Internet Security, are attempting to develop standards that will measure the cost effectiveness of cybersecurity efforts. Bert Miuccio, the Center's CEO, explains that the standards must be specific and provide methods for measuring an organization's information security status. Standards will measure the time between security incidents and recovery time to determine the success of security initiatives. The standards are expected to be developed by the end of the year.
http://www.spacedaily.com/reports/Analysis_New_measure_for_cybersecurity_999.html

Japan, U.S., China are leading sources of Web attack traffic

BY: DAN CAMPBELL, GOVERNMENT COMPUTER NEWS
09/10/2008

A study by Akamai Technologies, Inc. found that Japan, the United States and China were responsible for more than 60% of attack-oriented Internet traffic. Japan took the top spot on the list, and the study found that the United States had a 50% increase in attack traffic since the first quarter and China's rate dropped by 50%. Akamai Technologies manages a global content delivery network that includes a set of servers that monitor Internet traffic. http://www.gcn.com/online/vol1_no1/47109-1.html

CYBERSPACE HACKS, TACTICS AND DEFENSE

All webmail could be easy prey to tyro hackers

BY: GREGG KEIZER, COMPUTERWORLD
09/22/2008

Tests run by Computerworld indicate that Google's Gmail, Microsoft's Windows Live Hotmail, and Yahoo's Mail all rely on automated password reset mechanisms which can be hacked into easily, which is believed to be how Alaska Gov. Sarah Palin's email was accessed. A hacker called "rubico" researched answers to Palin's security questions which are required to reset e-mail passwords to access Palin's account. All of the e-mail services examined reset passwords online, and none required the new password to be sent to an alternate e-mail. Adam O'Donnell, director of emerging technologies at security vendor Cloudmark, explained that this automated password reset is standard in web-based mail. http://www.techworld.com/news/index.cfm?RSS&NewsID=104680

Cybereye | IT security in the executive suite

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
09/22/2008

Some claim that the recent hack into Alaska Gov. Sarah Palin's Yahoo e-mail account is an example of how security is often weak at the executive level, after official information was found in the unsecured private account. The incident is being investigated by both the FBI and the Secret Service. The article claims that increasing technologies and how easy these technologies are to use have allowed executives who are nearly computer illiterate to expose sensitive or dangerous information. The article also states that security must be uniform and enforced at all levels to be most effective. http://www.gcn.com/online/vol1_no1/47187-1.html

The Winds of Cyber War

BY: JACK M. GERMAIN, TECHNEWSWORLD
09/16/2008

The article explains that the recent cyberattacks on Georgian Web sites is significant both because it was coordinated with a conventional attack and because the cyber attacks were completed and successfully reinforced the conventional attacks. The article also points out that there were similarities between the Georgia and Estonia incidents including their distribution, coordination, use of a common toolset and origins in Russia. Both incidents represent a new age in warfare, in which attacks are waged by governments for military purposes in addition to high-tech criminals

seeking financial gain. The United States also has experience with cyberwarfare. The article states that the DHS reports 37,000 attempted government and computer system breaches in fiscal 2007 alone.
http://www.technewsworld.com/edpick/64494.html?wlc=1222319473

Al-Qaida's Propaganda Sites, Smacked Down

BY: NOAH SCHACHTMAN, WIRED BLOG NETWORK
09/17/2008

Al-Qaida's propaganda network, al-Ekhlaas.net was re-registered, all content was deleted and related pages including al-Ekhlaas' YouTube account were suspended. Hosting companies have dropped al-Ekhlaas sites before due to Western pressures, but this attack is unique because of its scope which indicates an attack on a major nerve center of al-Qaida's information warfare effort. Due in part to this attack, release of the annual 9/11 propaganda video was delayed by nearly a week. Internet jihadists point to American intelligence agencies as the source of attacks.
http://blog.wired.com/defense/2008/09/al-qaedas-once.html

Keyloggers beaten by new crypto utility

BY JOHN E. DUNN, TECHWORLD
09/15/2008

PMC Ciphers, a German company, has introduced a new program that reportedly addresses the key weakness in encryption systems which is when passphrases are recorded as they are being entered. The new program which is built into the TurboCrypt encryption utility encrypts characters instantaneously, before keylogging or screen capture can record the information. The program is slow and difficult to use, but is revolutionary in the level of security it provides.
http://www.networkworld.com/news/2008/091508-keyloggers-beaten-by-new-crypto.html?fsrc=rss-security

Wiring Up Warfighters

BY: BOB BREWIN, GOVERNMENT EXECUTIVE
09/15/2008

Defense Department officials are examining acquisition and management of computer networking and communications services in an attempt to save money while improving communications between warfighters and civilian employees worldwide. The Army is working on a new IT infrastructure for its LandWarNet network and developing universal e-mail addresses, telephone numbers and a file storage system to connect soldiers. The Defense Information Systems Agency is using the same approach in an effort to connect users form the military services and Defense agencies, in hopes of improving information delivery and cutting costs.
http://www.govexec.com/features/0908-15/0908-15s4.htm

BusinessWeek turned into malware playground

BY: JOHN E. DUNN, TECHWORLD
09/15/2008

The BusinessWeek magazine website was the victim of an SQL injection attack that left malware on hundreds of pages. Visitors to an infected page would be hit by the malware without any interaction, although the code appears to be currently non-functioning. The section of the BusinessWeek website that posts job opportunities to MBA graduates was infected. Graham Cluley of Sophos said that BusinessWeek needs to work quickly to remove the malicious script, and emphasizes the importance of ensuring that they do not get infected again after the database has been cleaned up.
http://www.techworld.com/news/index.cfm?RSS&NewsID=104414

Romanian Phishing Busts Were Years in the Making

BY: ROBERT MCMILLAN, IDG NEWS SERVICE
09/14/2008

The FBI arrested dozens of people who were behind phishing scams operated in Romania and the United States. Shawn Henry, assistant director of the FBI's Cyber Division said that he has been meeting with Romanian police and lawmakers since 2003 in order to improve the country's cybersecurity. Romania has since added new hacking laws and worked on fighting cybercrime. The Cyber Division sent six FBI agents to Romania in 2006 to assist Romanian National Police on an effort called Operation Cardkeeper, which eventually led to 13 arrests for phishing scams. The FBI also formed a task force last year and has worked with Romanian police in investigations that have led to 60 arrests in Romania and the United States.
http://www.csoonline.com/article/449226/Romanian_Phishing_Busts_Were_Years_in_the_Making

Hackers hit Large Hadron Collider Web site

BY: GREGG KEIZER, COMPUTERWORLD
09/12/2008

Web sites of the Large Hadron Collider were defaced by hackers under the name Greek Security Team. James Gillies, a spokesman for the European Organization for Nuclear Research, states there was no damage to the computer network besides the defacement. The site is back up, but is not accessible to the public. Zone-H.org, a company that collects evidence of cyberattacks, logs hundreds of Web site defacements each day, but attacks against sites that have internationally known domains are rare.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114590

Turkish Police Arrest Alleged ATM Hacker-Kidnapper

BY: RYAN SINGEL, WIRED BLOG NETWORK
09/12/2008

Turkish officials arrested notorious hacker Chao, who was also accused of abducting and beating a police informant. Chao, whose real name is Cagatay Evyapan, was wanted for marketing a skimmer that records magstripe data from debit and credit cards that are inserted into ATMs. The magstripe data was transferred to blank cards and used to make ATM withdrawals. Miami Beach police also arrested multiple Bulgarian nationals who had been planting the ATM skimmers for two years, stealing more than $160,000 from bank accounts in just two weeks.
http://blog.wired.com/27bstroke6/2008/09/turkish-police.html

US-Based Malware Network Shuts Down

BY: TIM WILSON, DARK READING
09/22/2008

Atrivo, a U.S. based Internet service provider (ISP) that was used by hackers and criminals is no longer in operation, and attempts to contact Atrivo operators have received no reply. The ISP and others, such as the Russian Business Networks, do not filter malware and malicious traffic, which allows for the exchange of data and malware by hackers. Robert Graham, CEO and founder of Errata Security, explains that users of Atrivo will just move to another network to host and exchange malware.
http://www.darkreading.com/document.asp?doc_id=164306&print=true

Network Forensics

BY: JOHN H. SAWYER, DARK READING
09/22/2008

There are many products currently available in the area of network forensics, although they provide many services such as network analysis, file recovery and user tracking. One of those products, NetworkMiner, is a free product that works on live network data to provide fingerprinting of operating systems, extract media files from FTP, HTTP and SMB, and display user credentials and search keywords. Unlike other network forensics products, NetworkMiner will not reconstruct full Web pages, find downloaded files or upload instant messaging conversations.
http://www.darkreading.com/blog.asp?blog_sectionid=447&doc_id=164343&WT.svl=blogger1_1

CYBERSPACE – LEGAL

Justice Department Moving to Immunize Snooping Telcos

BY: DAVID KRAVETS, WIRED BLOG NETWORK
09/12/2008

U.S. telecommunication companies were granted immunity from lawsuits that accused the companies of funneling American's electronic communications to the National Security Agent without warrants. The companies will still face lawsuits for breaching customer's Fourth Amendment right to privacy, although Justice Department special counsel Anthony Coppolino said that the government would seek full immunity for the companies. The article details five reasons that the EFF believes that the immunity is unconstitutional. The article also provides access to the latest court document.
http://blog.wired.com/27bstroke6/2008/09/justice-departm.html

DOJ's e-mail privacy stance might hamper prosecution in Palin case, EFF claims

BY JAIKUMAR VIJAYAN, COMPUTERWORLD
09/23/2008

According to the Electronic Frontier Foundation (EFF), the U.S. Department of Justice's position on a law regarding electronic storage could determine how the hacker who accessed Sarah Palin's Yahoo e-mail account is prosecuted. The Department of Justice reportedly disagreed with a decision issued in 2003 by the U.S. Ninth Circuit Court of Appeals that claimed that e-mails that were previously opened by the recipient were considered to be in electronic storage, and therefore under the protection of the federal Stored Communications Act (SCA). The DOJ's disagreement with this ruling means that it would harder to prosecute the hacker, because he could not be charged with violating the SCA. The DOJ's interpretation will be critical

in this case because it's likely that a legal case related to the Palin hacking incident would go through the Ninth Circuit Court because Yahoo is located in California, and Palin is the governor of Alaska.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115371

U.N. agency eyes curbs on Internet anonymity

CNET.COM
09/12/2008

An IP Traceback drafting group, named Q6/17 is drafting a set of technical standards which will aid in tracing the source of Internet communications in an effort to curb the ability of Internet users to remain anonymous. Many technologists and privacy advocates oppose the standards, claiming they violate privacy laws in the United States and the Council of Europe. The U.N. currently has no power to impose universal Internet standards, but officials have been trying to get more influence over Internet management. The United States also faces legal issues considering a legal requirement to adopt IP traceback would violate first amendment rights.
http://news.cnet.com/8301-13578_3-10040152-38.html

Bill Would Give Federal Power Regulator a Tool to Counter Cyber-Attacks

BY: ADRIANNE KROEPSCH, CONGRESSIONAL QUARTERLY
09/22/2008

The Federal Energy Regulatory Commission (FERC) which regulates the nation's power system currently has no legal power to respond to threats against the power grid. Proposed legislation from the House Energy and Commerce Committee would allow FERC to issue emergency orders to act against imminent threats after receiving a presidential directive. The legislation comes after a simulated cyber attack in March 2007 that remotely destroyed a $1 million diesel-electric generator. Many industry groups oppose the legislation and feel that it would inappropriately increase federal power.
http://www.cq.com/document/display.do;jsessionid=5755CF13D21FD78539233BDCF737ED2D.monhegan?matchId=65702566

DOJ Issues Cyber Report On Heels Of Hill Action

CONGRESS DAILY
09/18/2008

Congress has proposed a major identity theft bill to President Bush which would give ID theft victims the right to seek restitution for time and money that are lost restoring credit and would allow criminals impersonating businesses to steal personal information to be prosecuted under federal ID theft laws. The Justice Department also conducted a survey of 7,818 U.S. businesses and found that over half of the responding businesses have experienced one or more cyberattacks. 90% of those businesses suffered monetary loss, and cyber theft was blamed for more than half of the total monetary loss and one-third of the attacks. Some claim that the statistics may still be conservative, as many businesses are reluctant to provide information about attacks.
http://techdailydose.nationaljournal.com/2008/09/doj_issues_cyber_report_on_hee.php#more

Cyberattack threat spurs US rethink on power grids

CNET.COM
09/15/2008

U.S. Congress has been looking into legislation which would increase federal authority over electric companies, in response to increasing threats for attacks against U.S. power grids. The proposed legislation would expand the

authority of the Federal Energy Regulatory Commission and would require owners and operators of power systems to follow specific measures when addressing security threats. Some oppose the legislation, claiming the federal government would be given too much power over the electric industry.
http://news.zdnet.co.uk/security/0,1000000189,39488214,00.htm?r=5

Senators propose bills to boost IT security

BY: MATTHEW WEIGELT, FEDERAL COMPUTER WEEK
09/12/2008

Sen. Tom Carper (D-Del.) introduced the Federal Information Security Management Act of 2008 which proposes requiring agencies to prove their ability to secure sensitive or personal data. The bill would also appoint a chief information security officer in an attempt to strengthen the role of the CISO in the agencies. The bill was developed due to concerns about the Federal Information Security Management Act. The Senate Armed Services Committee proposed the fiscal 2009 National Defense Authorization Act which would create a 1% tax on the Defense Department's security programs in an effort to have money set aside for anticipated developments. Sen. Norm Coleman introduced the State Cyber Security Protection Act, which would create a program within the Homeland Security Department to provide money for improving cybersecurity among state governments.
http://www.fcw.com/online/news/153773-1.html

Bill would give FERC authority on cyber threats

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
09/12/2008

Joseph Kelliher, the Federal Energy Regulatory Commission's chairman, called the commission's legal authority "inadequate" in light of increasingly complex challenges of cybersecurity. Kelliher spoke to the House Energy and Commerce Committee's Energy and Air Quality Subcommittee, who is considering the Bulk Power System Protection Act of 2008 which would address cybersecurity threats to the bulk power system by increasing the commission's emergency powers. Many industry executives support this increase of power, although they recommend that the authority not interfere with the reliability regime that Congress requires.
http://www.fcw.com/online/news/153769-1.html

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.

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
16-17 Oct 2008	**Cyber Security Conference,** Caesars Palace Hotel and Casino, Las Vegas, NV, **http://www.asdevents.com/event.asp?ID=319**
21 Oct 2008	**Hampton Roads Cyber Security Awareness Conference,** Hampton Virginia, http://www.nsci-va.org/hrcsac
3-5 Nov 2008	**Global MilSatCom 2008 Conference & Exhibition,** Millennium Conference Centre, London, UK, www.smi-online.co.uk/08globalmilsatcom20.asp

CyberPro

Volume 1, Edition 10
September 25, 2008

Keeping Cyberspace Professionals Informed

CYBERPRO CONTENT / DISTRIBUTION

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.

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.

To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.

Please contact Larry McKee , ph. (757) 871-3578, regarding CyberPro subscription, sponsorship, and/or advertisement.