Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 142
5 Μάρτη 2009

Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts
Computerworld (02/09/09), J. Vijayan

President Barack Obama has tapped Bush administration official M. Hathaway, architect of a multi-billion dollar project aimed at better securing federal infrastructure against network threats, to head a 60-day audit of the government's cybersecurity initiatives. As the Homeland Security Council and the National Security Council's acting senior director for cyberspace, Hathaway will be in charge of leading a systemwide review of the government's cybersecurity programs and drafting recommendations to ensure they are meeting their objectives in the public and private sectors. Sources say Hathaway also is the top choice to become the White House cybersecurity secretary once the review is finished. Hathaway chaired the National Cyber Study Group, a multi-agency group that spearheaded the development of the Comprehensive National Cybersecurity Initiative (CNCI), which was approved by former President G Bush last year. "She has been really charging and moving forward with CNCI for the past 24 months," says former US cybersecurity director A. Yoran, who says Hathaway is well known within the federal cybersecurity community. Gartner analyst J. Pescatore praises Hathaway's appointment, but says the CNCI is behind the private sector in dealing with intrusion prevention and detection. "I don't think it's a very good model for how the government should move forward," he says.

P2P Networks Rife With Sensitive Health Care Data, Researcher Warns
Computerworld (01/30/09), J. Vijayan

Sensitive medical data is easily available through peer-to-peer (P2P) file-sharing networks, reveals a study by researchers at Dartmouth College. During the study, the researchers used search terms related to the top 10 publicly traded US healthcare organizations to see if they could find medical data on P2P networks such as Gnutella, FastTrack, Aries, and e-Donkey. Dartmouth professor Eric Johnson says the searches yielded a plethora of information from healthcare companies, suppliers, and patients. For example, Johnson says he was able to find a 1,718-page document containing Social Security numbers, dates of birth, insurance information, treatment codes, and other sensitive data belonging to roughly 9,000 patients at a medical testing laboratory. Johnson and the other researchers were able to obtain the information because employees at healthcare providers installed P2P networks on their computers, which allow users to download and share music and videos from shared folders but also can allow users to obtain other types of files if care is not taken to control which folders users have access to. Johnson says the study underscores the need for hospitals and other healthcare providers to be aware of the dangers of inadvertent data leakage as well as the need to put improved controls in place to monitor, detect, and stop them.

Sensors Help Keep the Elderly Safe, and at Home
New York Times (02/13/09) P. A1; J. Leland

Sensors and other monitoring technologies offer senior citizens more freedom to live independently and at less risk within the home. Motion sensors, medication reminder systems linked to mobile phones, pill compliance detectors, and wireless devices that transmit data on blood pressure and other physiological indicators are just some of the tools being used. These systems can be less costly than assisted living and nursing home care. One objective of personal health monitoring is to spur people to enhance their health by changing their behavior with the knowledge that they are being observed. However, the technologies are largely untested and are not usually covered by the government or private insurance plans. Moreover, there is the danger that the technologies could substitute for one-on-one interaction between seniors and their physicians, nurses, and relatives. "It's not that we need new technologies," says Dr. J. Kaye with the Oregon Health and Science University. "We need to use what we have more creatively." Monitoring technologies can gather terabytes of data, and researchers are working on ways of analyzing that information to help the well-being of users. For example, Kaye is working with Intel on a program that analyzes the motion data of seniors for patterns that would point to the onset of dementia well before it could be diagnosed with cognitive tests.

Microsoft Announces $250,000 Conficker Worm Bounty
Network World (02/12/09), H. Messmer

In an effort to stop the spread of the Conficker/Downadup worm, which is believed to have infected at least 10 million PCs around the world since November, Microsoft is offering a $250,000 reward for anyone who has information that leads to the arrest and conviction of those responsible for spreading the malicious code. In addition to offering the reward, Microsoft has partnered with security vendors, Internet registries and DNS providers such as ICANN, ORG, and NeuStar, to stop the Conficker worm from spreading further. Despite the efforts by Microsoft and others, the Conficker worm is set to wreak greater havoc on the world's PCs, security experts say. Experts say the worm connects to more than 250 command-and-control servers around the world every day as it awaits instructions on future downloads or actions. But the coalition formed by Microsoft is planning to take action to target the worm's update mechanism, including taking out the unique domain names for servers used for Conficker control, says Symantec's G. Egan. Microsoft says the coalition has already disabled a significant number of domains targeted by Conficker in an effort to disrupt the use of the worm and prevent attacks.

Sniffing Out Illicit BitTorrent Files
Technology Review (02/12/09), D. Graham-Rowe

Illegal content transferred using the BitTorrent file-trading protocol can be detected and tracked though a new method that monitors networks without disrupting the data stream, according to its creators. When the tool spots an illicit file, it retains a record of the network addresses involved for analysis, says the Air Force Institute of Technology's K. Schrader. Peer-to-peer transfers now account for the majority of Web traffic for many Internet service providers, which are generally only interested in this kind of traffic for the purpose of controlling or "throttling" it to liberate bandwidth for other uses. Schrader says this method does not reveal anything about the contents of each transfer, and while a small number of network-monitoring tools can identify specific BitTorrent files, it is generally a slow process. "Our system differs in that it is completely passive, meaning that it does not change any information entering or leaving a network," he says. The system first detects files that exhibit the signs of the BitTorrent protocol by analyzing the first 32 bits of the files' header data, and then examines the files' hash. If a hash matches any stored in a database of banned hashes, then the system will record the transfer and store the network addresses involved. The speediness of the method is partly explained by the presence of a specially configured field programmable gate array chip and a flash-memory card that stores a log of the illegal activity, allowing file contents to be scanned directly by tapping into an Ethernet controller buffer without interfering with network traffic. Schrader says the network monitoring cannot be detected by users.

Proposed Law Might Make Wi-Fi Users Help Cops
IDG News Service (02/20/09), S. Lawson

Congressional Republicans have introduced the Internet Security Act, legislation in the US House and Senate that would require Internet service providers (ISPs) and possibly Wi-Fi router owners to store and retain information on their users for at least two years to aid police investigations. The law would require Internet and email service providers to retain "all records or other information" about anyone using a network address temporarily assigned by the service. The retention requirements would apply to any provider of "an electronic communication service or remote computing service," and anyone who receives the content and recipient list of email messages that it "transmits, receives, or stores." The law would require ISPs to retain subscriber records similar to the records retained by telecommunications carriers, though civil liberties advocates point out that phone records are not kept for use in investigations. Carriers and ISPs are already required to retain information related to specific communications on their networks that are involved in a criminal investigation, notes Electronic Frontier Foundation attorney K. Bankston. Center for Democracy and Technology president L. Harris says the Internet Safety Act would amount to ISPs storing personal information on their customers just in case they are later accused of a crime. Bankston says the law could impose a heavy burden on private citizens and enterprises that operate wireless networks, and that it could mean Wi-Fi routers would need hard drives to store data on every user on the network.

Does Better Security Depend on a Better Internet?
Computing Community Consortium (02/21/09), P. Lee

The New York Times' recent article, "Do We Need a New Internet?," by J. Markoff, has sparked debate in the research community over whether creating a secure Internet will require creating a new Internet. In the article, Stanford University's N. McKeown says that unless today's Internet is changed, a public catastrophe is likely. In a blog post, E. Spafford, executive director of Purdue University's Center for Education and Research in Information Assurance and Security, writes "the Internet itself is not the biggest problem. Rather, it is the endpoints, the policies, the economics, and the legal environment that make things so difficult." University of California, San Deigo's S. Savage agrees. He says the network is the smalllest part of the security problem, and that on a technical level the security problem is an end-host problem in combination with an interface issue. "At a social level it's a human factors issue," Savage says. The Washington Advisory Group's P. Freeman says although technical improvements are needed, a major part of the security issue comes from people, not technology. However, Freeman says that reinventing some networking aspects is still an important research goal. As director of the National Science Foundation's computer science division, Freeman helped launch the GENI Project in 2004 with the goal of developing an experimental platform for exploring reliable and high-capacity networks. The GENI Project has made significant progress, and a version of the testbed will be available for early testing in a few months, which will enable researchers to investigate core networking research questions.

For a Poisoned Internet, No Quick Fix

Forbes (02/19/09), A. Greenberg

A large number of Domain Name System (DNS) servers have still not been patched to prevent hackers from exploiting that vulnerability security researcher D. Kaminsky found last summer. According to an analysis of roughly 200,000 DNS servers by researchers at the Georgia Institute of Technology, between one-fifth and one-third of those servers have not been patched for the vulnerability, which can be used by hackers to launch DNS cache poisoning attacks. In those attacks, users looking for legitimate Web sites are redirected to fraudulent sites without their knowledge. The analysis also found that roughly 2% of those servers had been attacked by cybercriminals trying to take advantage of the vulnerability. In the wake of the release of the analysis, Kaminsky is urging IT administrators to patch their DNS servers to correct the flaw. However, he notes that the Internet will not be completely safe from DNS cache poisoning until DNSsec is more widely used. That technology authenticates the destination to which Internet traffic is being sent instead of simply redirecting it. The researchers, led by Georgia Tech professor D. Dagon, presented their findings at the recent Black Hat security conference. Dagon says every server must be patched to stop the attacks. "In most cases when a fix goes out, 90% of the Internet is patched within a year. So we're still ahead of schedule," he says. "But given the size of the risk here, the rate of patching is still discouraging."

Improved Sensor Technology Could Someday Keep Tabs on Terrorists by Remote Control, Rochester Institute of Technology (02/12/09), S. Gawlowicz

Rochester Institute of Technology (RIT) scientists are developing new optical sensors for use in unmanned air vehicles and surveillance drones that could track suspects that have been identified as a threat. RIT professor J. Kerekes was awarded a $1 million Discovery Challenge Thrust grant by the Air Force Office of Scientific Research to design sensors that use multiple techniques to track an individual or vehicle. The sensor will collect necessary data, assess the situation and choose the best sensing mode. The sensor creates two strands of information, one of the target and one of the background environment, to maintain a connection and negate any camouflage effects. The sensor collects a black-and-white image of a target to record the shape and uses hyperspectral imaging to plot the object's color as it appears in multiple wavelengths. The hyperspectral mode can lock onto the unique material properties of a target object. "These are all complementary pieces of information and the idea is that if the object you are tracking goes into an area where you lose one piece of information, the other information might help," Kerekes says. Other members of Kerekes' team are working on a variety of projects, including modifying astronomical optical sensors, designing tunable microelectronics devices to collect specific wavelengths, and developing algorithms to track a target and pick the right imaging mode based on the scenario. The researchers are testing preliminary models using generic scenarios in a simulated world similar to Second Life.

Researchers Say Gazelle Browser Offers Better Security
Campus Technology (02/26/09), K. Mackie

Researchers at various universities are working with Microsoft Research to develop a more secure Web browser code-named Gazelle. The researchers recently demonstrated Gazelle on Windows Vista and with Internet Explorer's Trident renderer, and have also published a paper describing the project. Gazelle uses a browser-based operating system, a browser kernel that consists of approximately 5,000 lines of C# code and can withstand memory attacks. "No existing browsers, including new architectures like IE 8, Google Chrome, and OP [another experimental browser], have a multi-principal OS construction that gives a browser-based

OS, typically called browser kernel, the exclusive control to manage the protection and fair-sharing of all system resources among browser principals," the authors write. The principals, or Web sites, communicate with each other by passing messages through the browser kernel, which manages security and the sharing of system resources. The browser uses separate processes to run a Web page and its embedded principals. Still in the prototype stage, Gazelle is slow because of its level of overhead, and the team also will have to address the browser plug-in issue.

Report From Dartmouth's Institute for Information Infrastructure Protection (I3P) Makes Cyber Security Research Recommendations, Dartmouth News (02/19/09), S. Knapp

Dartmouth College's Institute for Information Infrastructure Protection (I3P) has given the US Senate Committee on Homeland Security and Governmental Affairs chairman Sen. J. Lieberman (I-Conn.) and committee member Sen. Susan Collins (R-Maine) a report on the research and development challenges in cybersecurity. The report, "National Cyber Security Research and Development Challenge: an Industry, Academic and Government Perspective," contains the opinions of the executives, government officials, and researchers who took part in the series of I3P forums Sens. Lieberman and Collins co-chaired last fall. The report includes a set of recommendations from the I3P participants on how to advance research in cybersecurity over the next 5-10 years. The report also discusses several needs that became apparent during the I3P forums last year, including the need to develop a coordinated and collaborative approach to cybersecurity, the need to develop metrics and assessment tools, and the need to create an effective legal and policy framework for security. In addition, the report discusses the need to address the human aspects of cybersecurity. The report concludes that the federal government will manage and oversee many of these recommendations, though it also will have to work with the private sector to implement the suggestions.

US Spy Agency May Get More Cybersecurity Duties
Reuters (02/26/09), R. Mikkelsen

During his testimony before the House Intelligence Committee on Feb. 25, Director of National Intelligence D. Blair told lawmakers that the National Security Agency (NSA) should be given more responsibility for securing the nation's IT networks. According to Blair, the NSA is best suited to handle the job of securing the nation's cyberinfrastructure because of its technology and its ability to detect attacks. Members of the House Intelligence Committee appear to be receptive to Blair's proposal, since some have said that they believe the Dept. of Homeland Security (DHS) is not capable of continuing to play a leading role in US computer security. However, Blair's proposal to give DHS' cybersecurity responsibilities to the NSA would probably not go over well with many of the lawmakers' constituents, due to the deep distrust many have for the NSA in the wake of its participation in former President G.W. Bush's warrantless wiretapping program.

Aussie Govt Considers Quantum Leap in Secure Comms
Computerworld Australia (03/03/09), D. Pauli

The Australian government is building a secure data communication system using quantum key distribution (QKD) technology, which uses lasers to detect any attempt to eavesdrop. The QKD system uses one-time keys to encode and decode data, but the random key is encoded at the quantum level in the sidebeam in the phase and amplitude, or brightness and color, of a highly tuned laser. QuintessenceLabs founder V. Sharma, one of the system's designers, says field trials with government agencies will be conducted over a fiber-optic network starting in the second half of this year. Sharma says the QKD network can be used for sensitive data, critical infrastructure, and secret commercial IP and financial information that requires ongoing protection. He says the QKD system uses as much off-the-shelf and open standard networking technology as possible to keep costs down and to make the system more robust. "The 21st century will see a number of advancements in quantum technologies, which will improve our lives in the much the same way that electricity and magnetism did in the previous century," Sharma says. "We are likely to see more quantum technology work its way into a number of practical applications over the next few years." Sharma designed the system with colleagues P.K. Lam, T. Symul and A. Lance at the Australian National University.

Report: Diebold Voting System Has 'Delete' Button for Erasing Audit Logs Wired News (03/03/09), K. Zetter

An investigation by California's secretary of state into why a product made by e-voting system vendor Premier Election Solutions (formerly Diebold Election Systems) lost about 200 ballots in Humboldt County during the US presidential election revealed the presence of a "clear" button in some versions of the machine's Global Election Management System (GEMS) software that allows someone to permanently erase audit logs from the system. The secretary of state's report says the logs "contain--or should contain--records that would be essential to reconstruct operator actions during the vote tallying process." The proximity of the clear button to the "print" and "save as" buttons raises the risk of the logs being erased accidentally, and the system provides no warning to operators of the danger of clicking on the button. Premier/Diebold retained the button despite an apparent warning from a system developper, and though the button was removed from subsequent iterations of the software, the version with the button is still used in three California counties and other US states. The report says that under the voting system standards "each of the errors and deficiencies in the GEMS version 1.18.19 software...standing alone would warrant a finding by an Independent Testing Authority (ITA) of 'Total Failure' (indicated by a score of 1.0) had the flaw been detected." The California report's findings bring up issues about the auditing logs on voting systems made by other vendors, and about what course of action states that use the Premier system will follow now that they are aware that their voting software fails to produce a sufficient audit trail to guarantee the integrity of an election.

Cards on the Table: Low-Cost Tool Spots Software Security Flaws During Development Process, NCSU News (02/25/09), M. Shipman

North Carolina State University (NCSU) computer security experts have developed Protection Poker, a new risk management tool that helps software developers find security vulnerabilities in their programs early in the development process. Protection Poker asks software development managers to present ideas for new software features or applications to their team of programmers. Members of the software development team are then asked to vote on two questions: how valuable is the data that the feature will be using, and how easy will it be to attack the new feature? The development team uses a special deck of cards to vote, which allows them to rank the value and vulnerability of the new feature on a scale of one to 100. Everyone on the team reveals their cards simultaneously, and the members who voted the highest and lowest are asked to explain their votes. If one team member has voted significantly higher or lower than the rest of the team they may know something the others do not, or they may be missing a vital piece of information. The process is particularly effective during the planning stage, so potential problems can be identified before any coding takes place. Lead researcher and NCSU professor L. Williams says Protection Poker also is an effective training tool that helps team members share their security knowledge and development process. The research was presented at the recent Engineering Secure Software and Systems Conference in Leuven, Belgium.

This Internet Fix Is No Pipe Dream
InfoWorld (02/27/09), R. Grimes

The Internet's security problems could be corrected by exploiting existing standards and protocols for Web services, security, identity, and authentication, writes R. Grimes. Such protocols include Web Services specifications and extensions, Security Assertion Markup Language, Simple Object Access Protocol, WS-Security, WS-Federation, WS-Trust, OpenID, and Security Token Service. "Essentially all these open standard protocols and specifications will allow huge, interconnected identity and authentication systems to be created between multiple, disparate parties," Grimes writes. "In relation to cloud services, these standards are often the way you will connect to them." In other words, "the specifications...allow the identity and authentication services necessary to connect to cloud services to be 'clouded' themselves," he says. Users will be able to receive one or more security tokens from one or more authentication providers and employ them as they desire, while each token can have one or more claims, which is any information characteristic associated with a specific identity. Grimes says these new specs and standards will facilitate the construction of massive identity metasystems in which large circles of trust can be organized through the linkage of many disparate identity/-authentication systems. This would eliminate the boundaries created by every commercial Internet service's own isolated authentication system, he concludes.