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

Δελτίο 68
4 Απρίλη 2007

Security That Nets Malicious Websites
Queensland University of Technology (03/23/07)

An IT researcher at Queensland University of Technology wants search engines to use reputation systems to warn users against visiting dangerous sites. "Just because a Web site ranks highly on a search engine doesn't mean it's a good Web site, in fact highly ranked Web sites can be malicious Web sites," says QUT professor A. Josang, referring to various practices that can elevate a Web site's rank. Most people can identify a dangerous site, but those who cannot need to be informed about such sites. Josang envisions browsers equipped with an Internet security system that allows users to rate Web sites as dangerous. A page that received low rankings would be made "invisible to unsuspecting users," he says. "Social control methods, also known as soft security, adhere to common ethical norms by parties in a community," explains Josang. "They make it possible to identify and sanction those participants who breach the norms and to recognize and reward members who adhere to them." Security systems such as the one Josang envisions could become crucial for maintaining the legitimacy of the Internet. "There is a deception waiting for you around every corner on the Internet and the technology we develop will protect people from that," Josang says.

UCF Researchers Work on Spy Drones
Orlando Sentinel (FL) (03/22/07), C. Cobbs

Two University of Central Florida researchers are developing drones of unmanned aerial vehicles (UAVs) that can provide the military with more comprehensive views of enemy locations than the single UAVs currently in use. The researchers will use a Defense University Research Instrumentation Program grant to buy three unmanned planes with six-foot wingspans and three helicopters in 48-inch bodies, plus cameras, communications equipment, and computers to control the UAVs. The single UAV systems currently in use in Iraq and Afghanistan make it difficult for operators to piece together separate images, but the UCF work aims to allow flocks of 10 or more UAVs to efficiently combine and analyze the images their cameras capture. What the UCF researchers are doing is the next step to make spy planes more proficient," says aircraft manufacturer S. Morris. "The idea is to have a bunch of them working together like an ant colony. A single ant is not a threat, but a swarm can strip a cow to the bone." Months could pass before the new aircraft is purchased, but the researchers hope to see results within the year. UAV swarm technology could be also used in law enforcement or search-and-rescue operations.

Tougher Standards Could End E-Voting
Inside Bay Area (CA) (03/28/07), I. Hoffman

California Secretary of State D. Bowen has announced new voting standards that could result in the end of e-voting in the state. The state will now demand the ability to use "red teams" of computer experts to try hacking into every voting machine and scrutinize every line of the machines' software code. Election officials say that with the primary election set for February 2008, it is unlikely the machines could be repaired in time if they fail these reviews. Bowen's

decision was praised by several e-voting experts. Johns Hopkins' A. Rubin says, "D. Bowen is holding up voting machines to the standards they deserve," and VerifiedVoting.org founder D. Dill says, "It's much to be preferred over our current see-no-evil approach. In every other case of red team attacks on voting machines and examination of their software code, experts have found major security problems." For three years California has had, but not enforced, laws requiring paper ballots that the blind can verify using audio playback, and that voting machines be "reasonably secured against untraceable vote tampering" and DoS attacks. "The criteria are clearly designed to eliminate DRE voting in California," said Carnegie Mellon University computer scientist M. Shamos. "An army of computer scientists will come forward to testify that computer programs cannot be verified to be secure against undetectable vote tampering and therefore they all will have to be decertified." Bowen's plans include decertification or withdrawal of state approval if the systems do not meet the standards. Florida and New Mexico have already gone back to paper ballots for elections.

World Scholar to Run New UTSA Cyber-Security Institute
University of Texas at San Antonio (03/27/07), D. Gabler

The University of Texas at San Antonio is creating a cyber security research institute, and information assurance and security expert R. Sandhu will serve as its founding executive director and chief scientist. Sandhu, chief scientist and co-founder of security solutions provider TriCipher, will leave George Mason University in Fairfax, Va., and join UTSA as the Lutcher Brown Chair in Computer Science June 1. The UTSA Institute for Cyber Security Research (ICSR) will look to commercialize its research into solutions that will help protect the key cyber infrastructure of the nation. Sandhu is an ACM fellow, and was the founding editor-in-chief of the ACM Transactions on Information and System Security. An author of more than 160 research papers on information security, Sandhu has contributed tremendously in the area of role-based access control and his work is found in the standards of the National Institute of Standards and Technology-American National Standards Institute and the upcoming International Organization for Standardization model. UTSA is using a $3.5 million grant from the Texas Emerging Technology Fund to help create ICSR and hire Sandhu.

Researchers Talk Cyber Security at Conference
Dartmouth News (03/27/07), M. Coburn

Dartmouth hosted a conference last week of more than 60 researchers from 12 different countries, who discussed the necessity of protecting the world's computer systems from cyber-terrorism. Given the growing interconnectivity of the computers that support transporttation, banking, and other systems, cyber-terrorism could have a tremendous impact on security and the global economy. Oil and gas infrastructure was a major topic of discussion at the conference. "The way it works is the oil and gas are controlled through process control systems," said I3P research director E. Goetz. "They would reduce temperature and flow of the pipeline and could open and close valves. What's happened in the last five to 10 years is that these systems are run off of Windows system and are connected to the Internet. The connectivity creates real vulnerability." Potentially exploitable gaps in infrastructure security must be identified, according to keynote speaker and I3P research director C. Palmer, but researchers must also develop solutions that can be realistically executed. "We can provide technology but the failure of the industry and research is that what we offer people is so complicated to get secure it's impossible to use," Palmer said. "People are the critical infrastructure we need to protect. We need to build systems that are secure and usable for what my sister calls 'normal people' or we're just doomed."

Despite Upgrades, Security Experts Fear $100 Laptops
InfoWorld (03/25/07), M. Hines

At this year's SchmooCon show, computer experts discussed the possible impact of the One Laptop Per Child Program, specifically regarding its security capabilities. The XO-1 laptop, the latest model to be created, includes security features such as embedded technology that allows improved encryption and a Linux-based operating system that cannot be changed. Users are able to download any application they want, but the system will not run those that exhibit virus-like behavior. The security architecture, known as BitFrost, runs each program in a semi-virtual environment, so as to keep applications from interacting with each other maliciously. "Security vendors would say don't let the kids run anything you haven't signed, but that says nothing about the corrupting of approved applications or attacking the rest of the system; and since we want kids to have complete control of the computers, that's not an option," explains OLPC security director I. Krstic. "Instead of protecting from executing untrusted code, we protect while running unwanted code, and keep it from doing bad things to the system." However, efforts to let users access the laptop's foundational operations, such as a button that shows a program's source code, could allow the machines to be made into a 10-million-node botnet operation, warns Booz Allen Hamilton consultant S. Coyne. "Through changing it, people can nullify all the security concerns that have been taken, and throw away the good work that's been done," he says. Foreign governments could use the laptops to distribute propaganda or track people's movements. Many are concerned that the project was too quick in assuming the educational effect of handing laptops to children, and has ignored important security concerns.

U.S.-Based Servers Host Majority of Malicious Code, Study Finds
Computerworld (03/26/07), J. Vijayan

The majority of malicious code is hosted on US-based servers, according to an analysis of more than 10 million URLs collected from live end-user traffic in Britain, using security vendor Finjan's content inspection engines. Finjan CTO Y. Ben-Itzhak said about 80% of malicious code comes from servers hosted in the United States. The other countries hosting the most significant amount of malicious code are the United Kingdom, with 10%, followed by Canada, Germany, and Italy. Ben-Itzhak said the findings dispel the myth that the majority of malicious code is hosted in countries with underdeveloped e-crime laws. The reason for this malware hosting trend may be that free Web hosting servers are more readily available in North America and Europe, making it more cost-effective for cybercriminals to host malicious code on servers in those countries. In many cases, malicious code appears to have been hosted on servers with legitimate content that was compromised by hackers. Malicious code is also more commonly found on sites visited by business users and consumers, such as travel and financial sites, whereas previously malicious code was most commonly found on sites with questionable content, such as pornographic sites. Botnets and Trojans are the most widely distributed programs, according to the Finjan report.

Hackers, Designers Talk Tech's Future at eTech
CNet (03/26/07), S. Olsen

The O'Reilly ETech Conference will bring together more than 1,000 technologists to discuss emerging technology, and will focus on how new applications and gadgets change the world. "We're featuring individuals who are innovating in slight changes in the use of technology," said program chair R. Dornfest. "A lot of what we will see in the next year or two are these

ongoing plate tectonics, rather than massive sea change in technology. Therein lies the magic." One such example was AttenTV, an application that provides Internet users with a streaming record of another users' clicks, which is currently available for Mac users only. "As you spend more time online, your clickstream increasingly represents who you are and what you are interested in," says the AttenTV Web site. "AttenTV turns one person's clickstream data into another person's entertainment." ETech is also focusing on the perspective shifts resulting from the new use of old technology. "Little innovations that make a big difference are more interesting than some of the big product announcements," said Dornfest. Topics of discussion at this year's conference will include how to develop Web 2.0 applications that ensure individuals' privacy, how collaborative, reality-based games take on social issues, and how high-end computer graphics will increasingly play into our lives.

Far Infrared Can Be Used for Anti-Terror Devices, Faster Wireless
University of Utah News (03/28/07)

University of Utah research have shown how far-infrared light can be used to create much faster short-range wireless communications between computers and other devices. The researchers found that shining far-infrared radiation, also known as terahertz radiation, through thin steel foil or film with holes punched in a semi-regular pattern known as "quasicrystal" allows nearly all of the radiation to pass through. When this method of transmission has been used in the past, unwanted frequencies were also transmitted, but the new study displayed the ability to choose which wavelength of far-infrared and visible light passed through the holes, and that by tilting the film, the researchers could switch the transmission on and off. Such results show that high-frequency terahertz signals can be used to carry information in the digital code of ones and zeros, and that superfast switches could potentially be constructed to move data at terahertz speeds. Fiber-optic phone and data lines currently use some near-infrared and some visible light, but far-infrared radiation is not used at all. The rest of the spectrum is full of communication signals, and "industry is starving for more electromagnetic frequencies," says principal study author Z. Valy Vardeny. Many obstacles face the creation, manipulation, and detection of far-infrared radiation, since today's optical and electronic switches are unable to turn the signal on and off fast enough to create binary code fast enough. No terahertz switch has ever been built, but the researchers believe that their findings show that such switches are possible and could be used for superfast communication over a short distance. The study also showed that far-infrared radiation could be used to detect chemical or biological weapons.

Wright State Researchers Pioneer New Ground in Web Technology Affecting Health Care, Terrorism, Defense, Financial Services, Wright State University (03/28/07)

Wright State University's Kno.e.sis Center is working to make it easier for computers to understand data. "We live in a society where we are deluged with data, and a key goal in our work is to organize and analyze this data through computer applications and software development," explains the center's A. Sheth. "We want to collect the dots and then connect the dots." Kno.e.sis focuses on establishing new techniques and technologies for the understanding and implementation of data and for the control and oversight of processes. Sheth dedicates a good deal of his efforts to the Semantic Web, the vision of expressing Web content in a way that computers can understand and analyze. The applications developed by Kno.e.sis could effect many different fields. Researchers at the center educate and train graduate students and develop technology that leads to software products. Better electronic records could improve health care by understanding the relationships and rules of different drug inter-

actions, treatment, and diagnosis. Life sciences could benefit from enhanced automation of experiments and analysis of data. Financial services could more accurately identify patterns and trends using the Semantic Web. Kno.e.sis could allow security to improve thanks to the ability to coordinate data from many different sources. Finally, integrating sensor data from many sources with known databases could provide military troops and officials with improved situational awareness. Kno.e.sis receives funding from the NSF, NIH, and DoD.

Q&A: New IAB Chair Mulls DNS Security, Unwanted Internet Traffic
Network World (03/28/07), C. D. Marsan

New chairman of the Internet Architecture Board (IAB) O. Kolkman explains in an interview that the narrow adoption of the DNSSEC DNS traffic authentication approach is not a sign of failure, but rather a sign of the slow deployment of the DNSSEC protocol. "For most application developers, DNSSEC is not on the radar because of the lack of infrastructure, while for the providers of infrastructure there are not sufficient users to justify their expense," he points out. Luckily, some top-level domains have stepped up to the plate to hasten DNSSEC implementation, although Kolkman notes that "more DNS infrastructure will need to be signed" while applications will have to start making use of the data. He says ascertaining the importance of the DNS' authority and integrity to a service is key to understanding the relevance of DNSSEC. Kolkman's investment in the IAB is borne out of his hope to maintain the consistency of the core principles for Internet usage for a time when his children use the Internet as young adults. Among the issues he expects the board will address over the next few years is unwanted Internet traffic. "In order to connect to those billion of devices mentioned above, we will need to have a network that will be able to deal with the dynamics of the interconnections, as well as the sheer number of possible interconnections," Kolkman comments. "Within the IETF there is, partly as of a result of an IAB sponsored workshop on the topic, a fair amount of energy to define an approach to deal with the strain put on the network."

Are Your Software Programmers Coding Securely?
Computerworld (03/26/07), J. Vijayan

A group of organizations led by the SANS Institute has launched the National Secure Programming Skills Assessment program, a series of tests designed to give companies with internal software development employees a way to test their coding skills so any flaws can be caught and corrected. Initially, four examinations will be offered, with each one testing a different type of programming language. The four areas covered are C/C++, Java/J2EE, Perl/-PHP, and .Net/ASP. The exams will first be available in Washington, DC, in August, and be made available worldwide later in the year. The necessity for a security assessment test comes from the growing need to improve programming skills while cybercriminals are becoming increasingly better at exploiting application-level vulnerabilities, many of which are the result of common coding errors such as input validation, buffer overflows, and integer errors. The program involved more than 360 organizations from the private sector, government agencies and universities. The exams are being designed to test knowledge of basic security problems that may arise during programming, not to test advanced security knowledge. The objective is to test an individual's ability to spot coding errors and apply fundamental best practices while coding software.