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

Δελτίο 156
17 Αυγούστου 2009

Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk
The New York Times (08/01/09), J. Markoff; T. Shanker

At the core of the US Obama Administration and its Pentagon leadership's efforts to develop rules governing cyberwarfare is the question of whether offensive measures could result in unintended damage to civilians and civilian infrastructure. Two traditional military limitations are currently being applied to cyberwar--proportionality and collateral damage, which requires militaries to minimize civilian casualties. "We are deeply concerned about the second- and third-order effects of certain types of computer network operations, as well as about laws of war that require attacks be proportional to the threat," says a senior military officer. For example, in 2003 the Pentagon and US intelligence agencies planned a cyberattack designed to freeze billions of dollars in the bank accounts of Saddam Hussein and hamstring his government’s financial system before the US invasion of Iraq. However, the plan was abandoned out of concern that it could unintentionally generate worldwide financial chaos. "If you don't know the consequences of a counterstrike against innocent third parties, it makes it very difficult to authorize one," says J. Lewis with the Center for Strategic and International Studies. The Naval Postgraduate School's J. Arquilla says that "extremely restrictive rules of engagement" are holding back the use of cyberweapons, which he insists are "disruptive and not destructive." Cyberattacks may not be as physically destructive as bombs, but they could cripple vital civilian infrastructure such as power grids or water treatment plants, which can be life-threatening.

A Police Woman Fights Quantum Hacking and Cracking
American Friends of Tel Aviv University (07/30/09)

Quantum computing will give people and institutions an enormous amount of computing power, but it will also make their data vulnerable to attack. For J. Kempe of Tel Aviv University's Blavatnik School of Computer Science, now is the time to think about building systems that could withstand a quantum attack. She says it is only a matter of time before quantum computers become as powerful as expected by physicists and mathematicians, which means they would be able to break current encryption standards. "If a very rich person worked secretly to fund the building of a quantum computer, there is no reason in principle that it couldn't be used for malevolent power within the next decade," Kempe says. "Governments, large corporations, entrepreneurs, and common everyday people will have no ability to protect themselves." Kempe is designing algorithms for quantum computers in an effort to learn about their limitations, as well as future programs that would protect their data.

Top Cybersecurity Aide at White House Resigns
The Washington Post (08/04/09) P. A3; E. Nakashima

M. Hathaway, the Obama administration's senior aide on cybersecurity, is stepping down from her role due to delays in the choosing of an administrator to lead the government's initiative to fortify the US's cyberinfrastructure. Hathaway, who was appointed by the Bush administration, had been a top choice for the cybersecurity coordinator job. But in a statement she said she was no longer applying for the job. "I wasn't willing to continue to wait any longer, because I'm not empowered right now to continue to drive the change," Hathaway said. "I've concluded that I can do more now from a different role," possibly working for a private company. Hathaway called President Obama out on his statement two months ago that he would hand pick a cybersecurity coordinator to spearhead the initiative. "We've made a lot of progress in the last 30 months that I've been in government, and now it's time to move on," Hathaway said. "It's up to the administration to take the next step." A former government official says the administration has interviewed 30 people for the job, and others have expressed frustration with the appointment's delays. The new cybersecurity coordinator will be responsible for developing a national cybersecurity strategy involving military, civilian and intelligence agencies.

New Epidemic Fears: Hackers
The Wall Street Journal (08/04/09) P. A6; B. Worthen

Under the economic stimulus bill and other US federal government proposals, hospitals and doctors' offices that invest in electronic records systems may receive compensation from part of a $29 billion fund. However, such systems can be vulnerable to security breaches. Last year health organizations publicly disclosed 97 data breaches, up from 64 in 2007, including lost laptops with patient data on them, misconfigured Web sites that accidentally disclosed confidential information, insider theft, and outside hackers breaking into a network. Because most healthcare organizations keep patients' names, Social Security numbers, dates of birth, and payment information such as insurance and credit cards, criminals often target these places for identity theft. "Healthcare is a treasure trove of personally identifiable information," says Secure Works researcher D. Jackson. The US Federal Trade Commission says medical fraud is involved in about 5% of all identity theft. Smaller practices can become easier targets, as they rarely have a technology professional or security specialists, and often lack a security plan or proper tools. The government plans to release guidelines over the next year, as part of the stimulus bill, to illustrate a secure information system, but critics warn that data encryption and other security functions are worthless if they are not correctly used. "If you take a digital system and implement it in a sloppy way, it doesn't matter how good the system is," says World Privacy Forum executive director P. Dixon. "You're going to introduce risk."

Warning Issued on Web Programming Interfaces
Technology Review (08/05/09), E. Naone

Application programming interfaces (API), software specifications that allow Web sites and services to interact with each other, have been a major factor in the rapid growth of Web applications, but security experts at the DEFCON hacking conference revealed ways of exploiting APIs to attack different sites and services. API have been key to the success of many social sites. J. Musser, founder of Programmable Web, a Web site for users of mashups and API, says that the traffic driven to Twitter through APIs, like from desktop clients, is 4-8 times greater than the traffic that comes through Twitter's Web site. However, N. Hamiel from Hexagon Security Group and S. Moyer from Agura Digital Security say that API could be exploited by hackers. The security researchers note that several APIs are often stacked on top of each other. Hamiel says this kind of stacking could led to security problems on several layers, and that APIs can open sites to new kinds of threats. In the presentation, Hamiel demonstrated that an attack might be able to use an API in unintended ways to gain access to parts of a Web site that should not be visible to the public. Hamiel says whenever a site adds functionality it increases its attack surface, and the same thing that makes API powerful often makes them vulnerable. Musser says any site that builds an API on top of another site's API is relying on someone else's security, and it is difficult to determine what has been built to see how well it is handled. WhiteHat Security founder and chief technology officer J. Grossman says sites that publish API can find it difficult to discover security flaws in their own API, and it is often hard to tell how a third-party site is using an API and if that site has been compromised by an attacker.

US Web-Tracking Plan Stirs Privacy Fears
Washington Post (08/11/09) P. A2; S. Hsu; C. Kang

The White House is proposing to soften a long-existing prohibition on tracking how users peruse US government Web sites with cookies and other methods, inciting suspicion among privacy advocates. The US Office of Management and Budget (OMB) has proposed replacing a ban on using cookies and other technologies on government sites and replacing it with new standards. Supporters of the proposal say social networking and other services have transformed the way users share knowledge, and White House officials say those services can be used to enhance transparency and public participation in the government. Some privacy advocates say the change represents a fundamental and inexplicable shift in federal policy. The American Civil Liberties Union's M. Macleod-Ball says the proposal could "allow the mass collection of personal information of every user of a federal government Web site." Even those in favor of revising the policy question whether the Obama administration is pursuing these changes at the behest of private companies, as the sector's clout in Washington has expanded significantly. The Electronic Frontier Foundation and the Electronic Privacy Information Center cite the language of a February contract with Google, in which a government agency specifically exempted the company so that it could access Google's YouTube site. E-lectronic Frontier Foundation legal advocate C. Cohn calls the agreement troubleing. "It appears that these companies are forcing the government to lower the privacy protections that the government had promised the American people," Cohn says. "The government should be requiring companies to raise the level of privacy protection if they want government contracts."

Napolitano: Cybersecurity Issues Remain Unresolved
CongressDaily (08/04/09), C. Strohm

US Department of Homeland Security secretary Janet Napolitano recently affirmed that her staff is still weighing options about how best to assimilate the public and private sectors in responding to security threats, saying a number of decisive factors remain foggy. "We need to be thinking outside our traditional boxes. We need to be thinking ahead," she says, adding that her staff was not sufficiently prepared to handle cybersecurity when she took over the department earlier this year. "We need to be recruiting and training investigators who only do this kind of work. That is where we are headed within the Dept. of Homeland Security and, indeed, within the United States Secret Service." Napolitano says she is open to new ways of cultivating interaction between the White House and the Pentagon's new cybercommand, preferably through a joint committee or middlemen. But she immediately voiced privacy concerns generated by having the armed forces involved in securing US civilian infrastructure. "That's why I haven't really come to a conclusion about how do we share without raising the specter that the Dept. of Defense is somehow going to be spying on civilian computers in the United States," Napolitano says.

Microsoft Team Traces Malicious Users
Technology Review (08/13/09), R. Lemos

In a paper that will be presented at ACM SIGCOMM 2009, which takes place Aug. 17-21 in Barcelona, Spain, Microsoft researchers will demonstrate HostTracker, software that removes the anonymity from malicious Internet activity. The researchers were able to identify the machines responsible for anonymous attacks, even when the host's IP address rapidly changed. The researchers say HostTracker could lead to better defenses against online attacks and spam campaigns. For example, security firms could create a clearer picture of which Internet hosts should be blocked from sending traffic to their clients, and cybercriminals would have a more difficult time disguising their activities as legitimate communications. The researchers analyzed a month's worth of data collected from a large email service provider to attempt to determine users responsible for sending spam. Tracking the origins of a message involved reconstructing relationships between account IDs and the hosts used to connect to the email service. The researchers grouped all the IDs accessed from different hosts over a certain time period, and the HostTracker software searched through this data to resolve any conflicts. The researchers also developed a way to automatically blacklist traffic from an IP address if HostTracker determines that the host at that address has been compromised. HostTracker was able to block malicious traffic with an error rate of 5%, and using additional information to identify good-user behavior reduced the error rate to less than 1%.