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

Δελτίο 11
20 Φλεβάρη 2006

Panel Sees Progress Made in Cybersecurity
CNet (02/14/06), J. Evers

In the three years since President Bush approved the National Strategy to Secure Cyberspace, the country's vulnerability to cyber attacks has been reduced, a panel of experts at the RSA Conference agreed, though more work needs to be done to keep pace with the increasing sophistication of cyberattacks. "Are we making progress? Yes. Do we have to hit some afterburners? I think that answer is yes also," said panelist Daniel Mehan, the former CIO at the Federal Aviation Administration. Mehan gives the state of government cybersecurity a rating between a D and a C+, noting the 500 percent increase in the number of incidents that CERT tracked from 2000 to 2003. The government has significantly improved its coordination with industry in responding to threats, as the recent Cyber Storm mock attack showed a high level of information being shared between agencies and companies. Andy Purdy, the acting director of the National Cyber Security Division, noted that the government could still simplify security for consumers, step up its efforts to protect children on the Internet, and raise awareness about the hazards of filesharing. Independent security consultant Howard Schmidt agreed with Purdy that software must become more secure, noting also that small and midsize businesses must bolster their protections against phishing attacks and other threats that compromises users' personal information. Increased regulation patterned after Europe's cybercrime draft treaty could also help, as well as an effort to strengthen the telecommunications infrastructure.

Flawed Election Machines Leave Maryland Voters Guessing
Baltimore Sun (02/15/06), P. 13A; A. Rubin

Maryland's direct recording electronic (DRE) voting machines are the least transparent voting system available, argues Avi Rubin, computer science professor at Johns Hopkins University. Rubin claims that without an auditing capability, voters must take on faith that the machines recorded their ballots accurately, and that they have not been tampered with by malicious programmers or election insiders. Installing malicious code in DREs is far easier than detecting it, and absent an auditing mechanism, verifying election accuracy is impossible. The most easily verified auditing mechanism is a paper trail. A recent University of Maryland study examined the Diebold machines currently in use in Baltimore County, finding that none contained sufficient verification technologies. The study failed to examine alternatives to the Diebold machines, however. Several states have scrapped the Diebold machines in favor of more transparent alternatives, and 26 states now require their systems to produce a voter-verified paper trail. Legislation has recently been introduced in Maryland to mandate paper records, as well as periodic spot checks of the machines and complete public disclosure in the event that voting discrepancies occur. Optical scan machines would satisfy these requirements, and are among the least expensive systems available. While optical scan machines might complicate the job of election coordinators and poll workers, the resulting transparency and accuracy would far outweigh such a minor inconvenience, Rubin says.

Internet Firms to Defend Policies
Washington Post (02/15/06), P. D1; Y. Noguchi

Yahoo!, Microsoft, and Google will claim to have struck a balance between business interests and human-rights concerns when they go before Congress today to defend their corporate policies toward China. Yahoo! will testify before the House subcommittee on Africa, Global Human Rights, and International Operations and the subcommittee on Asia and the Pacific that the Internet's presence has a beneficial effect on closed societies even when it is subject to censorship. Yet some human rights proponents plan to argue that American corporations are waiving their ethical duties by complying with Chinese law, which often comes down hard on free speech. Google announced last month that it would expurgate certain results on the Chinese version of its search engine; in December, Microsoft's MSN shuttered a dissident reporter's blog; and in 2005, Yahoo! supplied the Chinese government with email data resulting in the imprisonment of another dissident journalist. "If you're on the ground in China, you have to comply with the [local] law," reported Yahoo! general counsel M. Callahan, who is slated to testify today. "Fundamentally, being there transforms lives, society and economies." Callahan's argument--one echoed by Google and Microsoft--is that when any government requests information, the company is frequently in the dark about how that information will be employed. Reporters Without Borders' L. Morillon said the prevention of future crackdowns on dissident reporters should be facilitated by a combination of corporate self-regulation and government oversight. The State Department announced on Tuesday the establishment of a Global Internet Freedom Task Force that will monitor the censorship policies and information access restrictions of other governments, and make policy recommendations to keep Internet access to a maximum while keeping government attempts to suppress information to a minimum.

Virtual Reality Prepares Soldiers for Real War
Washington Post (02/14/06), P. A1; J. A. Vargas

For a generation of soldiers raised on video games, real-life combat can seem more like an outsized simulation of "Halo" or "Full Spectrum Warrior" than a physical reality. The Army acknowledges that Ctl+Alt+Del is as ingrained as the alphabet in today's soldier and it has capitalized on that fact in its training. While they cannot replace field experience, simulations have become an integral part of today's military training, and have indeed changed warfare itself. "The technology of games has facilitated a revolution in the art of warfare," said D. Bartlett, who heads the Pentagon's computer-related training, pointing to an increase in battle preparedness that comes from playing first-person shooter games. Objective comparisons between soldiers of one generation and another are typically anecdotal and inherently problematic, though military experts agree that modern soldiers do have a more thorough knowledge of weapons than previous generations. Video games are a favorite pastime for many soldiers in Iraq and Afghanistan on their off hours. "Over there in Iraq, I think playing those games helped," said Sgt. S. Crippen. "It kept me on my toes. It taught me what to do and what not to do." Other observers point to the reality gap between video games and real combat, claiming that many soldiers weaned on first-person shooting scenarios find the genuine article to be much more wrenching. Some battle-hardened soldiers abandon shooting games when they return home, claiming that the games only bring them back to a level of violence they had hoped to forget. By contrast, others play them as avidly as they did before the war, admiring features such as the realistic simulation of a soldier's heartbeat as the enemy approaches.

Denial-of-Service Attack-Detection Techniques
Internet Computing (02/06), Vol. 10, No. 1, P. 82; G. Carl; G. Kesidis; R. Brooks

A survey of methods for detecting denial-of-service (DoS) attacks points to the need to distinguish between network-based flooding attacks and abrupt increases in flash events or legitimate activity. In a flooding attack scenario, the attacker sends the victim a large amount of network traffic workload, causing bottlenecks that can severely hamper legitimate workloads, and no software vulnerability or specific conditions are needed to execute such an attack. Locally installed DoS attack-detection strategies can shield potential victims, while remotely installed approaches can be used to spot propagating attacks; most IT departments opt for local detection in which detectors are located at the potential victim resource or at a router or firewall inside the victim's sub-network. A variety of detectors distributed across three attack-detection method categories--activity profiling, change-point detection, and wavelet analysis--were analyzed, and several core problems were outlined. Rigorous testing of the surveyed detectors was impossible partly because comprehensive test data, testing environments, and standards are unavailable, although the authors hope efforts such as the Cyber Defense Technology Experimental Research Project will solve this problem. Also, none of the detector schemes have nominal-traffic measures covering the whole of potential network conditions, while researchers for the most part offer no guidance on how much each detector's multiple operating parameters can vary and thus impact performance. Real-world implementation issues were also omitted in the studies. The authors conclude that though all the surveyed detectors yield promising results in limited testing, none can completely address the detection challenge; they reason that the optimum solution is to combine various strategies and supplement them with the participation of seasoned network operators.

Voter Databases Must Be Secured, Report Says
CNet (02/17/06), D. McCullagh

States are scrambling to comply with federal requirements that voter records be stored in central databases, but a 60-page report ACM released on Thursday warns that the databases could be vulnerable to fraud, and that states must do more to shore up security, reliability, and privacy. "Nobody's done this kind of analysis," says former ACM President B. Simons. "We're not out to criticize anyone. We're out to try to provide information." Simons, co-chair of the ACM Committee on Guidelines for Implementation of Voter Registration Databases, notes the committee's report highlights numerous security applications familiar to computer scientists, but likely unknown to many election officials. In accordance with the Help America Vote Act, which requires election officials to create state-wide voter registration databases, 28 states have hired outside contractors to provide their election databases, and 21 have opted to develop their own. While requiring "adequate technological security," the legislation does not require encryption or any other specific method. Without sufficient security provisions, hackers could remove eligible voters or insert fraudulent names into the database. ACM is also concerned about privacy, noting that many states allow the sale of voter registration databases for both political and commercial purposes. The National Association of Secretaries of State reports that just 24 states had been expected to comply with the federal deadline of Jan. 1, 2006, though most of the rest will likely have created their databases by the fall elections. The complete ACM report, entitled Statewide Databases of Registered Voters:

Calling Cryptographers
Technology Review (02/16/06), K. Greene

In his keynote address at this week's RSA Conference in San Jose, Microsoft Chairman Bill Gates outlined a holistic vision of information security, comprising a "true ecosystem" where all members of the computing industry work together to combat cyberattacks. Gates and other conference speakers argued for a multilayered security approach that, while not foolproof, would shore up hardware, software, and networks. Claiming that password protections can be easily compromised by phishing and other rudimentary schemes, Gates plugged Microsoft's InfoCard digital identity system as a worthy replacement, though Gates admitted that the move away from passwords would take at least four years to complete due to the multitude of vendors that would have to collaborate. RSA Security CEO Art Coviello outlined his company's community policing program, which would address security on a global scale. RSA's system could instantly flag an IP address associated with a fraudulent transaction and notify banks and other relevant institutions. Sun CEO Scott McNealy spoke about the steps that his company has made to improve security in server hardware and data centers, describing the elliptical curve cryptography (ECC) built into Sun's processors. The security standard, approved by the National Security Agency, employs a smaller key than conventional cryptography applications, making it suitable for smaller devices such as cell phones and censors. A panel of distinguished cryptographers reiterated the call for the creation and dissemination of new methods, as, aside from Sun's development of ECC, the industry currently uses only the RSA, and Diffie-Hellman standards of cryptography, leaving scant recourse in the event that one technique fails.

UC Santa Cruz Computer Scientist Fights Spam on Two Fronts
AScribe Newswire (02/15/06)

In an effort to protect minors from email with offensive or adult content, Utah and Michigan have implemented a "do-not-spam" registry that began as a student project at the University of California, Santa Cruz, where researchers have also developed a technique to combat harvesters who scour the Internet collecting email addresses to expand their spam lists. Emailers will be fined $1,000 in Utah and $5,000 in Michigan for each message with adult content that they send to minors with registered email addresses. The UCSC registry, developed under the guidance of technology and information management research associate Arthur Keller, was licensed to Unspam in 2003 for commercial development. Unspam collects less than one cent per address from companies cross-referencing their mailing lists with the registry, and splits the proceeds with the State of California. While registry is a significant step toward online child protection, the Free Speech Coalition has challenged the constitutionality of the Utah law in a federal court. Despite the security concerns voiced in a Federal Trade Commission report, Keller maintains that the registry is impervious to hackers. Meanwhile, Keller has also helped launch Project Honey Pot, the initiative targeting email harvesters, providing the first meaningful enforcement of the CAN-SPAM Act of 2003. Robotic harvesting programs continuously crawl the Internet, mining for email addresses. Project Honey Pot distributed more than 250,000 Web sites with spam traps, containing a disclaimer prohibiting the harvesting of the address, and capturing information about the robot, enabling subsequent identification in the event that the email address later receives a spam message. Keller reports that 30 percent of the messages that Honey Pot receives involve some type of phishing scam, while the remainder are trying to sell a product.

Cellphone Could Crack RFID Tags, Says Cryptographer
EE Times (02/14/06), R. Merritt

Weizmann Institute computer science professor Adi Shamir says a cell phone could be used to compromise the most popular brand of RFID tags. The cryptography expert recently monitored how RFID tags used power as they were being read using a directional antenna and digital oscilloscope. Speaking during a panel discussion at the RSA conference in San Jose, Shamir added that one could determine whether the tag received password bits that were correct or not. "We can see the point where the chip is unhappy if a wrong bit is sent and consumes more power from the environment?to write a note to RAM that it has received a bad bit and to ignore the rest of the string," noted Shamir. The test was done on the biggest brand of RFID tags, and it showed that the tags were not protected. "A cell phone has all the ingredients you need to conduct an attack and compromise all the RFID tags in the vicinity," said Shamir. He noted that designers have cut back on security features because of the need to lower the cost of tags to five cents each, but warned that next-generation tags will have to shore up the security issue.