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

Δελτίο 116
12 Μάη 2008

White House Plans Proactive Cyber-Security Role for Spy Agencies
Washington Post (05/02/08), B. Krebs

The White House could soon announce a policy in which US spy agencies would play a role in collecting intelligence on cyber-security threats, said an anonymous administration official. The official noted that the intelligence community is uniquely poised to counter cyber-attackers who are continuously developing new intrusion strategies and taking advantage of unknown security holes in software and hardware to expose government networks. President Bush signed a directive in January that empowered the intelligence agencies to monitor all federal network traffic to prevent intruders from stealing sensitive data or disrupting vital systems, and the official said the directive will enable cyber-threat intelligence sharing between the government and the private sector. "We want a broader information flow to the private sector of the threats we're seeing, so that they can increase their security posture as well," the official stated. The majority of the 18 strategic objectives outlined in the cyber initiative are classified, but the official said the administration plans to issue additional details on at least a dozen of those goals, as soon as the Office of Management and Budget releases rules for assigning classification levels for data collected and shared under the new program. The SANS Institute's A. Paller says intelligence agencies often face a dilemma in sharing new threat information with allies and the private sector because spy agencies frequently obtain intelligence by leveraging the same security holes in software and hardware used by America's enemies. The Center for Democracy & Technology's J. Dempsey says the Bush administration has a tendency to tag even the most innocuous information as classified, which means the intelligence community may share less information with the private sector rather than more. "The more information that gets classified, the less likely the initiative will succeed," he says.

Electronic 'Pet' Could Replace Passwords and PIN
New Scientist (05/02/08), C. Barras

Northumbria University psychologist and computer scientist P. Briggs and Newcastle University computer scientist P. Olivier say portable electronic pets capable of recognizing their owner's voice and walking style could replace passwords and PIN to secure personal information. Instead of storing a person's biometric signature in a database, that information would be kept in a small electronic pet or "biometric daemon" the owner carries around. The daemon would learn to imprint itself on its owner, after which it would use biometric signals such as a voiceprint, fingerprint, or walking pattern to identify its owner. The connection between the owner and pet would be strengthened by games and interactions between the two. When near its owner, the daemon would receive "nourishment," and act happy as a confirmation of the owner's identity, but a daemon separated from its owner would no longer receive this nourishment and die to protect the owner's information. Olivier says the elements needed to make a prototype daemon already exist, although adequate battery power is still problematic. Briggs says the daemon does not have to be an animal, but it should be something people relate to best.

Ballot Box Blues
Government Computer News (04/28/08) Vol. 27, No. 9, Dizard III, P. Wilson

Voting process experts generally concur that states that have already deployed direct-recording electronic (DRE) systems have little choice at this point but to stick with the machines through the current election cycle. "The problem with the upcoming [general] election is that any county that doesn't have its election system locked in by now is in real trouble," says Fortify Software chief scientist B. Chess. Supporters of DRE cite the systems' improved accessibility, among other things, while the voting equipment industry's trade association argues that the security questions raised by state studies do not take real-world conditions or the complete spectrum of anti-fraud safeguards embedded in voting policies and procedures into account. However, in December 2006 the NIST issued a draft report noting that software-dependent systems such as DRE machines cannot be audited against any proof of the voter's intent, which adds fuel to "continued questions about voting system security and diminished public confidence in elections." The organization urged the employment of software-independent systems with a paper trail, pointing out that most states have some type of voter-verified paper records that are either used across the state or on a county-by-county basis. A bill was brought before the House earlier in April that sought to encourage states to discard DRE machines in favor of paper ballots, but the measure failed due to White House opposition based on budget considerations, says Rep. R. Holt (D-NJ).

USACM Urges Congress to Build in Safeguards for Automated Employment Checks
AScribe Newswire (05/06/08)

ACM US Public Policy Committee Chairman E. Spafford's testimony at a Congressional hearing on employment verification systems and their impact on the Social Security Administration on Tuesday highlighted several potential problems in a pilot system operated by the US Dept. of Homeland Security intended to allow employers to electronically check employee work eligibility. Spafford urged Congress to include sufficient safeguards to ensure that employers and employees are adequately protected from technical failure and system abuse. Congress is considering several proposals to expand the DHS E-Verify automated employment verification system, including requiring employers to verify all new hires and existing employees using an expanded version. Verification is now optional for employers. "As technologists, we are acutely aware of the limitations and failure modes of current information technology," Spafford said. "Any system must take the extreme failure modes into account and provide appropriate safeguards to avoid injury to the blameless seeking gainful employment to better themselves." Spafford said the three biggest concerns are the accuracy and timeliness of system results, the security and privacy protection afforded to information kept in the system, and the technical feasibility of multiple approaches to creating such a system. He said those same concerns apply to the REAL ID Act, US-VISIT, and a US immigration and border management system.

Pentagon Wants Cyberwar Range to 'Replicate Human Behavior and Frailties'
Wired News (05/05/08), N. Shachtman

Congress has told the Defense Advanced Research Projects Agency (DARPA) to create a National Cyber Range as part of a $30 billion governmentwide effort to prepare for digital warfare. To make the facility as realistic as possible, DARPA has released a request for proposals that requires contractors to provide robust technologies that emulate human behavior on all nodes for testing all aspects of behavior. The range should produce realistic chains of events between multiple users without scripting behavior, implement multiple user roles similar to roles found on operational networks, and change replicant behavior as the network environment changes. Replicants also must simulate physical interactions with peripherals such as keyboards and mice, drive all common applications on a desktop environment, and interact with authenticate systems, including Defense Department authentication systems. The digital people have to demonstrate human behavior 80 percent of the time. The facility should also include realistic offensive and defensive opposition forces capable of fighting military cyber-warriors in simulated combat. Contractors must create 10,000-node tests using government-provided configuration files and network diagrams in under two hours, and the nodes must be more than computers connected to a faux Internet.

Huge Databases Offer a Research Gold Mine--and Privacy Worries
Chronicle of Higher Education (05/09/08) Vol. 54, No. 35, P. A10; D. Glenn

Congress's rejection of the notion of a national "unit-record tracking" system for student data has provoked speculation that states will bolster their own education-data centers, which many researchers say would be valuable resources for evaluating schools and colleges and helping them to improve. However, there is a darker aspect to this possibility in the form of potential privacy violations, and this is one reason why many states' efforts to build such data clearinghouses have been sluggish. The development of additional state data centers was advocated by a group of scholars attending a recent conference organized by the National Academies and the American Educational Research Association, who nevertheless acknowledged that the trustworthiness of the systems would be undone by a single serious breach of anonymity. Pending changes in Family Educational Rights and Privacy Act (FERPA) regulations incorporate several clarifications about how states, school districts, and colleges should safeguard student confidentiality when working with databases, such as requiring educational agencies to sign written agreements when they provide data to outside researchers and mandating that the researchers return or destroy the data when they are finished using it. The commentary accompanying the draft regulations notes that privacy issues can remain even with the total removal of names, Social Security numbers, and birth dates from the data, so the regulations instruct each state to identify a number below which data may not be disclosed for a specific "cell" of students. "Even if FERPA did not exist, many of these challenges would still be with us," says T. Bailey with Columbia University Teachers College's Community College Research Center. "Colleges' IT systems aren't set up to analyze this stuff. The data generally aren't stored in a way that's ideal for research, because that's not the purpose for which the system was designed."

Botnet Beaten, But Now What?
eWeek (05/05/08) Vol. 25, No. 14, P. 13; R. Naraine

TippingPoint Digital Vaccine Laboratories software security researchers C. Pierce and P. Amini have devised a way to crack into the Kraken botnet by reverse-engineering the encryption routines and working out the communication structure between the botnet owner and the commandeered computers. "We basically have the ability to create a fake Kraken server capable of overtaking a redirected zombie," Pierce says. However, this breakthrough places TippingPoint in the middle of an ethical dilemma concerning whether compromised computers employed in denial-of-service attacks and spam runs should be purged without the permission of the systems' owners. Amini advocates this practice as a tool for impeding the botnet epidemic, arguing that "we never hear from the infected system again and neither can the actual botnet owner's command-and-control servers." Pierce agrees with Amini's argument, and supports an industry-wide dialogue on more proactive, vigilante-style anti-botnet tactics. Opposed is TippingPoint director of security research D. Endler, who entertains the possibility that system cleansing without consent could endanger the operations of end-user systems with critical functions, such as life support. He notes that the issue of liability is one reason why TippingPoint decided not to modify an infected computer within the botnet.

Careful With That Call
Government Computer News (05/05/08) Vol. 27, No. 10, W. Jackson

With more attention being focused on stopping hackers from using email and security vulnerabilities in Web applications as an avenue for breaching IT systems and stealing data, hackers could begin to see Voice over Internet protocol (VoIP) systems as the path of least resistance, security experts say. The experts add that now is the time to begin defending VoIP systems before hackers begin exploiting the vulnerabilities in those systems. Those vulnerabilities are similar to the vulnerabilities that exist in other types of applications. For example, the vulnerabilities in VoIP systems can allow arbitrary code to be executed on an endpoint, such as a telephone handset or a laptop PC running a soft phone client. In addition, hackers can use vulnerabilities in VoIP systems to access an organization's data if its voice services and data are carried on the same network. As a result, researchers are beginning to heed security experts' call to begin developing defenses for VoIP systems. For example, Georgia Tech researchers are working on so-called soft credentials that assign a level of trust to voice calls based on social-networking techniques and circles of trust. With this system, levels of trust are assigned by studying who talks to whom, under what circumstances, and for how long. Although such a solution would require a learning period in which the system studies the user's calls, it would be a very effective defense mechanism once the learning period was over, says professor M. Ahamad, director of Georgia Tech's Information Security Center.