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

Δελτίο 94
26 Οκτώβρη 2007

Hackers Could Skew US Elections
New Scientist (10/09/07), J. Marshall

Security experts at the recent APWG eCrime Researchers Summit at Carnegie Mellon University warned that hackers are likely to use the Internet to deceive US voters in an attempt to affect the outcome of elections. Although election deception is nothing new, security experts say it could be much more difficult to uncover the perpetrator as the Internet creates far greater anonymity. The Internet could be used to spread misinformation such as the location of voting sites, voting times, and candidates' positions on issues through spam, botnets, and Internet phone calls. Internet-based telephone attacks are more difficult to trace than those using landlines, notes R. Dhamija of the Harvard Center for Research on Computation and Society. Such attacks could employ botnets, which would make them even harder to trace and potentially much larger. Candidates may also be attacked, either directly through their Web site, as J. McCain was when a picture on his Web site was changed stating he had altered his position on an issue, or through typo domains such as hillaryclingon.com or muttromney. com, which could be used to collect fraudulent donations or spread malware. In 2004, a fake J. Kerry web site stole campaign contributions and users' debit-card numbers. Fraudulent campaign sites can also be used to expose users to phishing and malware attacks as it is difficult to know what the official site of a candidate is. "The fact is that all of the technology for all of these things to happen is already in place," says Indiana University's C. Soghoian. "I'm not sure this will happen in 2008, but it will happen."

Quantum Cryptography to Secure Ballots in Swiss Election
Network World (10/11/07), E. Messmer

Swiss officials plan to use quantum cryptography technology to protect ballot information in an election in the Geneva region of Switzerland on Oct. 21, the first time such advanced encryption will be used for an election. "We would like to provide optimal security conditions for the work of counting the ballots," says Geneva state chancellor R. Hensler. "In this context, the value added by quantum cryptography concerns not so much protection from outside attempts to interfere as the ability to verify that the data have not been corrupted in transit between entry and storage." A quantum encryption system will be used for the point-to-point encryption of ballot information sent over a telecommunications line from the central ballot-counting station to the government data center. "Protection of the federal elections is of historical importance in the sense that, after several years of development and experimentation, this will be the first use of the 1 GHz quantum encrypter, which is transparent for the user, and an ordinary fiber-optic line to send data endowed with relevance and purpose," says University of Geneva professor and quantum cryptography researcher N. Gisin. He says "this occasion marks quantum technology's real debut." The use of quantum cryptography in the election marks the start of the SwissQuanum, a project managed by Gisin that aims to set up a pilot communications network throughout Geneva that supporters compare to the first Internet links in the United States in the 1970s.

Panelists Cite Threats to US Computer Networks
CongressDaily (10/10/07), O. Kreisher

The United States' ability to protect its electronic networks from cyberattacks is hampered by "policy restraints" and a dearth of coordination, a panel of experts said Tuesday. "Cyberspace has become a really big deal," says Lt. Gen. R. Elder, commander of the Air Force's Cyberspace, Global Strike and Network Operations command. "We do our banking, our commercial activities over the Internet." However, the country's interconnected electronic networks are under constant attack, analysts say. The military Web and computer networks are attacked thousands of times each year, reports military analyst R. Grant. In June 2007, one such attack brought some of the Pentagon's unclassified computer systems to a halt and interrupted the Defense Secretary's office email system. The major denial-of-service attack that paralyzed Estonia's government and commercial communications for weeks further revealed the capacity of a cyberassault. Because the US Air Force uses cyberspace to transmit satellite and aircraft data and convey global communications, the Air Force has designated cyberspace as one of its "warfighting domains." Elder plans to use Air National Guard staff to develop a force of "cyberwarriors" who can safeguard America's networks and, if needed, bring down an enemy's systems. Elder plans to establish a cyber security unit in every US state within one year. In addition, Elder and other Air Force officials believe the country needs to adopt a comprehensive policy on cyberwarfare operations.

Technology Would Help Detect Terrorists Before They Strike
University at Buffalo News (10/05/07), E. Goldbaum

University at Buffalo computer and behavioral scientists are developing automated tracking systems that monitor people's faces, voices, body movement, and biometrics and automatically compare it to tested behavioral indicators to provide a quantitative score on the likelihood of the subject being a terrorist. "We are developing a prototype that examines a video in a number of different security settings, automatically producing a single, integrated score of malfeasance likelihood," says UB professor of computer science and engineering V. Govindaraju. The project will focus on developing an accurate baseline of indicators to an individual during extensive interrogations as well as clues during faster, routine security scans. The system will also be able to learn from subjects during the course of a 20-minute interview, an important feature according to Govindaraju, because many behavioral clues to deceit are unique to each individual person. "As soon as a new person comes in for an interrogation, our program will start tracking his or her behaviors, and start computing a baseline for that individual 'on the fly,'" Govindaraju says. The UB researchers expect to have a working prototype ready in a few years.

ORNL's SensorPedia Targets National Security Mission
Oak Ridge National Laboratory (10/04/07)

The Oak Ridge National Laboratory is developing a writeable Web site that will enable emergency responders and decision-makers to share data from different kinds of sensor networks in near-real time. Current sensor systems that detect radiation, chemicals, and biological agents are unable to offer such access because there is not a single standard for making interoperable sensor networks. ORNL calls its system SensorPedia because it is based on the underlying technology of Wikipedia, but it differs from the online encyclopedia in that it links to near-real-time data for streaming data, supports interactive "mashups" of information, and limits written contributions to approved personnel. The federal government will initially use SensorPedia, which is being built with existing tools and resources. SensorPedia will be hosted on a Wiki-enabled ORNL server that controls credentials and authentication. "Our system simplifies sensor information sharing while preserving the integrity, security, and authenticity of sensor information," says B. Gorman of ORNL's Computational Sciences and Engineering Division. Interoperability is the key to effective sensor networks, adds Gorman.

'Dark Web' Project Takes on Cyber-Terrorism
Fox News (10/11/07), S. Kotler

Dark Web is an extensive, searchable database on extremists and terrorist-generated content. Developed by H. Chen, director of the University of Arizona's Artificial Intelligence Lab, Dark Web uses advanced technology to cross-reference, catalog, and analyze terrorist Web sites, message boards, and any other online information. Chen says the amount of information is massive, posted in dozens of languages, and is often hidden behind ordinary-looking pages. "Since the events of 9/11, terrorist presence online has multiplied tenfold," says Chen. "Around the year 2000, there were 70-80 core terrorist sites online; now there are at least 7,000-8,000." Chen says the Internet is arguably the most powerful tool for spreading extremist violence because Web pages can be used for activities such as spreading propaganda and offering advice on how to plot a series of attacks. To process the massive amount of information gathered, Dark Web uses a variety of analytical tools, including statistical, cluster, content, link, and sentiment analysis, a new analytical tool capable of determining the emotional content of a site, so the system can differentiate between social activists and hateful extremists. Dark Web also uses social-network analysis to map extremist networks and determine the importance of each member. Chen's team recently studied online training manuals and methods on how to build and use improvised explosive devices, including where such content was downloaded, which has led to countermeasures that are keeping soldiers and civilians safer. However, critics see a number of similarities between Dark Web and the DARPA's controversial Total Information Awareness initiative, while Electronic Privacy Information Center executive director M. Rotenberg notes that "the very same tools that can be used to track terrorists can also be used to track political opponents."

Data Sharing Threatens Privacy
Nature (10/11/07) Vol. 449, No. 7163, p. 644

The field of computational social science relies heavily on access to electronic datasets such as email records, Web-search histories, and mobile-phone call logs, and such data sharing offers "enormous potential… for lines of research that shed new light on basic social-science questions," says Cornell University network analysis specialist J. Kleinberg. But concerns about how such data sharing might threaten privacy could create a major public backlash, says Consortium for Political and Social Research director M. Gutmann. Kleinberg agrees that "as the number of these types of study increases, the community is clearly going to need to engage in deeper discussions about the right way to safeguard privacy in working with these kinds of data." Software tools for protecting privacy while sharing data are often developed by social scientists with heavy computer science backgrounds, but as these tools are mainstreamed they are adopted by less experienced academics. The need for an institutional and systematic strategy for strengthening the privacy rights of those whose data is used thus becomes obvious, says Boston University researcher M. van Alstyne. A recent study by the US National Academies reached a similar conclusion, in that individual researchers cannot be given sole responsibility for protecting privacy. However, social scientists are quick to point out that private firms, unlike academics, operate with few restrictions on retaining and exploiting personal data.

Ohio Brings in Experts to Review Troubled E-Voting Systems
Computerworld (10/16/07), T. Weiss

The state of Ohio has hired computer security researchers from three universities-Pennsylvania State University, University of Pennsylvania, and the University of California, Santa Barbara--as well as e-voting testing lab SysTest Labs to conduct independent tests on the state's e-voting machines in an effort to find and fix any potential problems before the 2008 presidential election. Ohio assistant secretary of state C. Nance says the review will test a representative sample of 40,000 e-voting machines from Ohio's 88 counties. Ohio's e-voting hardware is primarily from Election Systems & Software and Premier Election Solutions, formerly known as Diebold Election Systems. SysTest Labs President Brian Phillips says the testing process began on Sept. 24 and will be finished by Nov. 30. The testing will examine hardware, election management software, polling place devices, and the central counting applications that tally the votes. SysTest will also conduct configuration management testing to ensure that the e-voting system hardware and software match the specifications of the certified systems allowed in Ohio. Final reports from the testing will be delivered to Ohio Secretary of State J. Brunner on Dec. 14.

Carnegie Mellon's A. Perrig Leads Research Team Dedicated to Analyzing and Disrupting Internet Attackers' Black Markets, Carnegie Mellon News (10/15/07), C. Swaney

Carnegie Mellon University professor A. Perrig, along with researchers from the International Computer Science Institute and the University of California, San Diego, have developed new computer tools to better understand and possibly stop the growth of Internet black markets for malware. "These troublesome entrepreneurs even offer tech support and free updates for their malicious creations that run the gamut from denial-of-service attacks designed to overwhelm Web sites and servers to data stealing Trojan viruses," Perrig says. Project researcher J. Franklin says the team found more than 80,000 potential credit card numbers available on illicit underground Web markets. Transactions on the markets are difficult to track because buyers usually contact the seller through private email or instant messaging and payments are made through non-bank payment services. The Carnegie Mellon researchers proposed two technical approaches to reduce the number of transactions by destabilizing the market. The first approach is a slander attack that would eliminate the verified status of a buyer or seller. "By eliminating the verified status of the honest individuals, an attacker establishes a lemon market where buyers are unable to distinguish the quality of the goods or services," Franklin says. The researchers also developed a technique to establish fake verifyed-status identities so buyers cannot tell the difference between real sellers and fake sellers. "So, when the unwary buyer tries to collect the goods and services promised, the seller fails to provide the goods and services. Such behavior is known as 'ripping,'" Franklin says. "And it is the goal of all black market site's verification systems to minimize such behavior."

Univ. of Virginia Computer Security Video Wins Award
University of Virginia (10/16/07)

The University of Virginia's Office of Information Technology and Communications won the first-place award from ACM's Special Internet Group for University and College Computing Services for a video on how excessive, inappropriate personal information on the Web can be damaging. The 70-second video shows a job applicant trying to explain the contents of his personal blog and a picture of himself on a photo sharing site to a hiring committee. The applicant is unable to come up with an appropriate answer and is embarrassed by the situation.

The video ends with the warning, "What happens on the Web, Stays on the Web," with an emphasis that it will be there permanently for all to see. The video was one of the university's contributions to the "Who's Watching Charlottesville?," a cross-sector community initiative campaign to create greater cyber awareness in the Charlottesville-Albemarle area and help residents learn to protect themselves online. "We created this video to get our message across to students in a humorous to-the-point way," says S. Crittenden, a systems analyst in the Information Technology and Communications office and director of the video. "It's a gratifying culmination of our efforts to be recognized by SIGUCCS for a national award."

Rebinding Attacks Unbound
Security Focus (10/17/07), F. Biancuzzi

Stanford University PhD student A. Barth participated in a study that determined that Web browsers are still vulnerable to DNS rebinding. He says in an interview that rebinding attacks are successful because browsers and plug-ins employ DNS host names to distinguish between different origins, but browsers do not really communicate with the hosts by name--they must first use DNS to align the host name with an IP address and then communicate with the host through its IP address. DNS rebinding can be used to bypass firewalls or to temporarily commandeer a client's IP address to issue spam email or defraud pay-per-click advertisers. Barth says the solution used to fix the classic DNS rebinding vulnerability--DNS pinning--no longer effectively defends against the vulnerability because today's browsers contain many different technologies that allow network access, such as Java and Flash. These technologies support separate pin databases, but are allowed to communicate within the browser. Barth says an effective defense against firewall circumvention is the configuration of DNS resolvers not to bind host names to internal IP addresses, while host name authorization can prevent DNS rebinding vulnerabilities in the longer term. "I'm hopeful the vendors will reach a consensus to fix these issues using host name authorization, but this requires the vendors to cooperate with each other," he notes. Barth says DNSSEC offers no protection against DNS rebinding attacks because it is designed to prevent pharming not rebinding.

Threats to Power Facilities on the Rise
Associated Press (10/17/07), J. Hebert

Cybersecurity threats to the nation's power plants, electricity grid, and refineries are increaseing and a successful attack could cause economic chaos, say congressional investigators. Control systems are more vulnerable to hackers and terrorists today than they have been in the past, says the Government Accountability Office, who along with other security groups is working to close loopholes that might allow hackers to disrupt the US's energy infrastructure. G. Wilshusen, the agency's director of information security issues, told the House Homeland Security subcommittee that power lines, nuclear plants, refineries, and power stations are more secure but admitted that there is "no overall strategy to coordinate the various activities across federal agencies and the private sector." G. Garcia, assistant secretary for cybersecurity, recently spoke to legislators about efforts involving the Dept. of Homeland Security and other groups to raise standards and tighten security on crucial control systems. "The cyber-risk to these systems is increasing," says Rep. J. Langevin (D-R.I.), chairman of the subcommittee on emerging threats, cybersecurity and science and technology. "If this administration doesn't recognize and prioritize these problems soon, the future isn't going to be pretty."

Cyber Wars
Government Executive (10/01/07) Vol. 39, No. 17, P. 16; B. Brewin

Alleged attacks against Pentagon computer systems by Chinese hackers, and subsequent accusations by the Chinese of Western state-organized cyber intrusions, are symptoms of what SANS Institute director A. Paller terms "cyber espionage," or probes to rate the security of networks. He says government policies "keep attacks so secret that top government executives do not know how bad the problem really is." Director of the Federation of American Scientists' Project on Government Secrecy S. Aftergood reports that the cyberattacks, regardless of who orchestrated them, should function as a warning that there is a heavy price to be paid for shoddy computer security. Over the past year the Dept. of Defense has mounted an effort to develop offensive information warfare capabilities, and Strategic Command commander Marine Gen. J. Cartwright informed the House Armed Services Committee in March that if "we apply the principle of warfare to the cyber domain, as we do to sea, air, and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary, to deter actions detrimental to our interests." The Air Force and Army began moving toward the acquisition of cyber warfare technology this year, but Center for Defense Information adviser P. Coyle argues that countries should instead devise a code of "best behavior" for the Internet. "It wouldn't be any easier to negotiate such arms control than it has been where nuclear weapons are concerned," he notes. "But it may become necessary just the same."