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

Δελτίο 86
10 Αυγούστου 2007

What the U.S. Is Doing Wrong With E-Voting
eWeek (07/30/07), L. Vaas

On July 30, the office of California Secretary of State D. Bowen released the results of an investigation demonstrating that three major e-voting systems are vulnerable to exploitation, once again highlighting the shoddy state of e-voting in the United States. The urgency to address this situation is growing as the 2008 election season approaches, and other countries have tackled the problem with better results; Australia's e-voting effort is arguably the most successful, having embraced an open-source strategy in which e-voting systems are Linux-based and e-voting specifications are established by independent election officials and posted online for anyone to evaluate. The US e-voting infrastructure, in contrast, is a patchwork of disparate systems that use wireless communications and flawed off-the-shelf software that is not subject to testing. The US is rated by experts such as Australian National University's T. Worthington as having the developed world's most poorly designed e-voting systems, and the reasons for this are political and administrative in nature. E-voting systems must comply with a muddle of federal and state election laws, which "does present challenges to election technology providers because this is not a 'one-size-fits-all' marketplace where one machine or version of software can be used in any state," remarks Sequoia Voting Systems executive M. Shafer. She adds that the open-source disclosure of e-voting hardware/software code has the potential to put election-rigging tools in the hands of wrongdoers, while current legislative proposals that recommend the open-source approach see no difference between e-voting system manufacturers and third-party software producers. "Legally, manufacturers cannot provide source code for these third-party software programs or provide the names of the programmers involved in the creation of the third-party software," Shafer explains.

Florida Voting Chief Aims to Block Hackers
Miami Herald (08/01/07), M. Caputo

Florida secretary of state K. Browning on Monday announced that Diebold electronic voting machines used in 25 Florida counties are vulnerable to attack and vote manipulation and has given the manufacturer until Aug. 17 to fix the problem. A study by Florida State University found that a hacker could use a preprogrammed computer card on Diebold's optical-scan voting machines to switch votes or to create a "ballot-stuffing attack" that multiplies votes for a particular candidate or issue. Diebold says it will fix the problem. A new Florida state law requires all counties to use voting machines that leave a paper trail by next year, and all but bans ATM-style touch-screen voting machines. Diebold's M. Radke says the software upgrade is not a major enhancement and presents no risk to voters. However, Diebold made similar assurances in late 2005 after Leon Country election supervisor I. Sancho allowed Finnish computer scientists H. Hursti access to the voting system to see if it could be compromised. Hursti determined that someone could change the votes and leave a minimal trace. Hursti's findings were dismissed by then secretary of state D. Mann and Diebold because they said the study was not conducted in a real-world election environment. Browning, who was appointed this year by Gov. C. Crist, says that in addition to requiring a software upgrade, he will ask elections supervisors to develop a uniform security policy to ensure a chain of custody for election equipment to track who handled election systems.

Scan this Guy's E-Passport and Watch Your System Crash
Wired News (08/01/07), K. Zetter

RFID expert L. Grunwald, who has served as an e-passport consultant to the German parliament, says security flaws in the electronic passport system could allow someone to steal and copy the fingerprint image stored in the biometric e-passport, or create a specially coded chip that will cause the scanners to crash when they try to read the e-passport. Grunwald says he successfully sabotaged two passport readers from different vendors by copying a passport chip and modifying the JPEG2000 image file that contains the passport photo. The modified image, which contained a buffer-overrun exploit, caused the readers to crash, indicating that they could be vulnerable to manipulation, like injecting code that forces the readers to approve an expired or forged passport. "If you're able to crash something you are most likely able to exploit it," Grunwald says, adding that there is no reason to believe that any other e-passport scanners made by other vendors are any more secure. The International Civil Aviation Organization, the United Nations organization that created the standards for e-passports, suggests that issuing countries add an optional layer of security known as Extended Access Control, which makes readers obtain a digital certificate from the issuing country before the passport can be read by the scanners. However, Grunwald says that tactic is also flawed because the chip does not contain an onboard clock to monitor the digital certificate's expiration. "It's a basic mistake," Grunwald says. Grunwald will give a presentation on the e-passport vulnerabilities he discovered at the annual DefCon hacker conference in Las Vegas.

Securing Cell Phones
Technology Review (08/01/07), K. Greene

The recent hack of Apple's iPhone by researchers at a security company should serve as a warning to all mobile device manufacturers that there is a growing need for better mobile device security, experts say. Cell-phone viruses have existed for about a decade, buy many experts believe that threats to mobile devices could become far more significant and dangerous over the next few years because of mobile devices' growing computing power, popularity, and complexity. "I think a large part of this is that cell phones are becoming miniature computers," says University of California, Berkeley computer science professor D. Wagner, "and as a consequence, they are starting to inherit some of the same problems that we face with PCs." While using available security tools such as anitivirus software is an option, cell phones have their own unique problems. Some security companies have introduced products for mobile phones, but these solutions have limited functionality to avoid draining the battery too much, says NEC's A. Raghunathan. Problems associated with battery life and processing power can be avoided in some cases by running security software on the cell-phone carrier infrastructure, but Raghunathan believes the best solution for mobile device security is hardware-based security solutions, such as an extra processor and memory that are hardwired for specific tasks. Such a system would divide the phone into two environments, one the user has access to and includes the applications, while the other is designed to be impenetrable to viruses and malicious software that stores passwords and other critical information. If a virus were to be downloaded to a device with this system, it would be unable to access any information, and if the phone were lost or stolen the carrier could access the secure environment remotely and shut down the phone.

Senate to Hold Hearing on Security of Voting Machines
Wired News (07/31/07), K. Zetter

The Senate Rules and Administration Committee has scheduled a hearing for September to discuss findings from Red Team security researchers on voting machine security. The announcement by Sen. D. Feinstein (D-Calif.) comes a week after the security researchers reported that their efforts to hack into the voting machines of three top vendors were successful. The findings should not have been a surprise to Feinstein, who introduced a bill in 2007 that would require voting machines to produce a paper trail. Feinstein's bill has not had as much momentum as a measure from Rep. R. Holt (D-N.J.), although he had to reintroduce it this year. Holt's bill was going nowhere just two weeks ago, due to interest group differences over a paper trail mandate and voter accessibility, but a compromise appears to have been reached this week. Voting activists initially favored the use of touch-screen machines with add-on printers, as called for in Holt's bill, but they now say optical-scan machines that use a durable full-size paper ballot are needed.

Picture Your Password
Dark Reading (07/23/07), K. Higgins

A new study from researchers in Ottawa suggests that it would be easy for people to use graphical-based passwords in the real world. However, the research on "click-based" graphical passwords presented last week at a usability and security conference hosted by Carnegie Mellon University also indicates that there are some security concerns about the technique and that people prefer to use text-based passwords. S. Chiasson, a Ph.D. student in computer science at Carleton University in Ottawa, Ontario, says users often chose the same areas of the graphical representations for clicking on images, which would make it easier for attackers to guess their passwords. She believes users did not like graphical-based passwords simply because they are not used to them. What is more, the study suggests that graphical-based passwords are easy to remember, but adds they may be difficult to recall if users have several. The researchers will not allow users to select predictable click spots in the next phase of the research, as they study how to improve graphical-based passwords.

Security: A Business Enabler, Not Disabler
Baseline (07/07)No. 74, P. 41; McCormick, John

Purdue University professor E. Spafford, recipient of the ACM's President's Award for his "extensive and continuing record of service to the computing community, including major companies and government agencies," says one of the biggest weaknesses in corporate computer centers are business processes, operating systems, and applications that are developed and implemented with convenience or cost, rather than security, in mind. He says it is "just plain wrong" to assume that patches and add-ons will ensure the security of such products, when in fact security must be designed into the products from the outset. Spafford explains that part of this effort involves "having informed, empowered individuals who have the appropriate training and background to be making decisions about what goes in, and that those decisions are based on an adequate understanding of risk." A lack of knowledge about specific risks and the value of components constitutes a major failing, and Spafford says CIOs must obtain a comprehensive perspective of resources in need of protection and their associated risks. Spafford recommends that managers ask questions concerning whether the proper applications/operations/business processes are running, who ultimately decides new acquisitions and the architecture as project momentum builds, and whether risk is properly integrated in those decisions. He also suggests that people should get in a mindset that views security as a enabler rather than a disabler.

Scientists' Tests Hack Into Electronic Voting Machines in California and Elsewhere
New York Times (07/28/07) P. A11; C. Drew

A test of electronic voting machines used in California and other states has shown that the machines are easily hacked and there are several ways to alter the vote totals. The tests, conducted by computer scientists from several universities in California, focused on three of the four largest electronic voting machine vendors: Diebold Election Systems, Hart InterCivic, and Sequoia Voting Systems. A report issued by the state of California said that each of the systems had weaknesses that could be exploited to affect the correct recording and tallying of votes. University of California, Davis, computer science professor M. Bishop, who led one of the testing teams, says his team was surprised how easy it was to pick the physical lock and to bypass the software defenses. Bishop says that every machine had problems, particularly because security features seemed to be added after the basic design of the system was finished. Bishop says the best way to build a secure system is to build security into the system at the start of the design process. The drastic failure of the voting machines' security could cause California's secretary of state D. Bowen to ban the use of some machines in the 2008 election unless extra security precautions are established and election results are closely monitored. Electronic voting machine industry executives argue that the tests were not conducted in a realistic environment and that no machine has ever been known to have been hacked during an election. The report was released on the same day members of Congress reached an agreement on measures to add paper records to every voting machine so voters can verify that their ballots were correctly cast and to be used in case of a recount.

Q&A: Security Top Concern for New IETF Chair
Network World (07/26/07), C. Marsan

R. Housley, the new head of Internet standards body IETF, says he will maintain the objecttive he had when he was director of the IETF security area--to work for continuous, incremental improvement of the IETF standards process and the Internet as a whole. Housley, who runs consulting firm Vigil Security, says he took the volunteer position because he cares about the community and he believes that it is important to have a security expert in charge of the IETF because security is the biggest problem for the Internet right now. Housley says the deployment of IPv6 and DNS security are high priorities, while he also hopes the Secure Inter-Domain Routing working group will add new security improvements to Internet routing. Many of the problems the IETF must eventually fix, such as the lack of security in HTTP, are made more complex because there is little to no agreement on what is the most important security feature to add. Housley says more people think about security, but it is not the primary reason they look to the IETF. Housley says IPv6 will be deployed sooner rather than later, and suggests that people start working on IPv6 adoption now. The biggest challenge for the IETF, according to Housley, is establishing better working relationships through liaisons to other standards development organizations, particularly the International Telecommunication Union Telecommunications Standards Sector and the Third Generation Partnership Project.

E-Voting Systems Vulnerable to Viruses and Other Security Attacks, New Report Finds
UC Berkeley News (08/02/07), S. Yang

The source code in electronic voting machines contains security holes that leave them vulnerable to attack, conclude University of California, Berkeley researchers in a new report. The source code report was part of California Secretary of State D. Bowen's "top-to-bottom review" of electronic voting machines. The researchers, led by UC Berkeley associate professor of computer science D. Wagner, said that many of the security problems found were similar on each of the three systems examined, which includes machines by Diebold Elections Systems, Sequoia Voting Systems, and Hart InterCivic. "The most severe problem we found was the potential for viruses to be introduced into a machine and spread throughout the voting system," Wagner says. "In the worst-case scenario, these malicious codes could be used to compromise the votes recorded on the machines' memory cards or render the machines non-functional on election day." The vulnerabilities on the machines could allow a virus on one machine to infect an entire county's system when votes are uploaded to a central computer to be counted. Wagner says the flaws found would allow an attacker to defeat any technological countermeasures in the software. "Unfortunately, these vulnerabilities are not trivial implementation bugs that can be patched up," Wagner says. "The software just wasn't designed with fundamental safeguards in place to make them resilient to intrusion." The researchers also found flaws that could jeopardize voting anonymously in two of the systems. Bowen is expected to make decision regarding the certification of the machines on Aug. 3, six months before the state's primary election.

New Report Finds States Not Doing Enough to Ensure Accurate Count on Electronic Voting Machines, Brennan Center for Justice (NYU School of Law) (08/01/07), J. Rosen

The majority of states using electronic voting machines do not have adequate security measures and are not equipped to find sophisticated and targeted software-based attacks, non-systemic programming errors, or software bugs that could alter an election's results, concludes a report from the Brennan Center for Justice at NYU's School of Law and the Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley's Boalt Hall School of Law. The report, "Post Election Audits: Restoring Trust in Elections," says that more focused and rigorous audits of paper records can improve the integrity of election results. "No matter how long we study machines, we're never going to think of every attack or find every bug. We can try to close up every hole we find, but ultimately using paper records to check electronic tallies is the only way we can trust these machines," says lead author of the report L. Norden, who is also head of the Brennan Center's Voting Technology Assessment Project. To emphasize the importance of auditing, the Brennan Center released data compiled by Common Cause that highlighted instances of machine malfunctions altering vote tallies in 30 states. Common Cause director of Voting Integrity Programs Susannah Goodman says, "We need systemic, mandatory audits to insure that voters choose candidates not software bugs or programming errors." The report found that of the 38 states that require or use voter-verifiable paper records, 23 do not require audits after every election, and of the ones that do, none use audit methods that would maximize the chances of finding targeted software-based attacks, programming errors, or software bugs that would affect the outcome of the election.

Halt 'High Risk' E-Voting: British Watchdog
Reuters (08/02/07), P. Griffiths

Britain's election watchdog says Internet voting trials are too risky to continue, and that Britain was fortunate not to have had a security breach during a pilot in May. In a new report, the Electoral Commission calls for a halt to e-voting trials until the government comes up with a plan for testing, securing, and assuring the quality of the voting strategy. "We have learned a good deal from pilots over the past few years," says Peter Wardle, chief executive of the Electoral Commission. "But we do not see any merit in continuing with small-scale, piecemeal piloting where similar innovations are explored each year without sufficient planning and implementation time." In addition to concerns about fraud, transparency, and public trust, the watchdog also says e-voting is costly. The Electoral Commission cites a number of problems during the e-voting pilot in local elections earlier in the year, including people forgetting the Internet password needed to vote, and others believing they could vote over the telephone.

Clarke Wants to Know, Where Did We Go Wrong?
Government Computer News (08/01/07), W. Jackson

Former US counterterrorism czar R. Clarke says the United States lost its way sometime after the release of the National Strategy to Secure Cyberspace in 2003. "I'd like to know why it was that we lost momentum in solving the problem in more than a piecemeal manner," says Clarke, who gave the opening keynote speech at the Black Hat Briefings. "There is no leadership. There is no national plan implemented." Clarke says the nation's industry, commerce, health care, and national defense are growing increasingly dependent on an information infrastructure that cannot be defended. Clarke says there was once a high-level of awareness that there was a problem, but that since then little progress has been made and some has even been lost. Clarke believes the government has failed in its part as the role model it was supposed to be, and the situation will probably get worse before it gets better as federal funding for security R&D has been reduced. The problem is a lack of congressional and presidential leadership, Clarke says, compounded by a lack of executive initiative from the private sector. Clarke believes that without government leadership, corporations will not put forth the effort necessary for significant improvement unless threatened by some imminent catastrophe. Clarke says what is needed are more and better encryption practices, a secure Domain Name Service, service providers that filter out malware before it reaches the local-area network and the end user, and a parallel network to provide emergency services that uses IPv6 to prioritize traffic. Some progress has been made, including companies that have reduced the vulnerabilities in their software, and IPv6 has been slowly advancing.

Researchers Set to Spark Up New More Secure Network, Routers, Switches
Network World (07/31/07)

Stanford University researchers this summer are deploying and testing an updated version of Ethane, an architecture for corporate networks that provides a powerful and simple management model with strong security. Most current corporate networks allow for open communication automatically, which makes implementing effective security and privacy rules difficult. Ethane establishes a set of simple-to-define access polices, all maintained in one place, that are consistently applied across a network datapath and ensures users, switches, or end-hosts do not receive more information than needed. A preliminary version of Ethane was built and deployed in the fall of 2006. The new version of Ethane reportedly has better policy language support and a more feature-rich datapath that can support more diverse techniques such as NAC, MAC hiding, and end-to-end L2 isolation. Ethane works because all complex features, including routing, naming, policy declaration, and security checks, are performed by a central controller instead of in the switches as is the common practice. All movement on the network must first get permission from the controller, which verifies that the communication is allowed under network policy. If the flow is allowed, the controller determines a route for the flow, and adds an entry for that flow in each of the switches along the path. Stanford researchers say their Ethane project, which is funded by Stanford's Clean Slate Project, closely complements multiple projects at the National Science Foundation, including the Global Environment for Network Innovations project.

The New Face of Identity Protection: You
University of Houston News (07/30/07), A. Holdsworth

University of Houston professor I. Kakadiaris and researchers at the school's Computational Biomedicine Lab have developed facial recognition software that can be used for a variety of purposes, from securing government facilities to making credit card purchases. The software, called URxD, uses a three-dimensional image of a person's face to create a biometric identifier. The Face Recognition Vendor Test, conducted by the National Institute of Standards and Technology, found the URxD system to be the best 3D face recognition system for examining face shape. Kakadiaris says URxD's accuracy stems from the strength of the variables the system uses to examine and describe a person's face, and that it would make an excellent replacement for having to remember multiple passwords and PINs. "Remembering dozens of personal identification numbers and passwords is not the solution to identity theft," Kakadiaris says. "The solution is to be able to tie your private information to your person in a way that cannot be compromised." says Kakadiaris. Kakadiaris believes URxD will have a positive impact on several of today's biggest issues and that someday computers will be able to recognize the user sitting in front of them. "Everything will be both easier and more secure, from online purchases to parental control of what Web sites your children can visit," Kakadiaris says.

How Far Could Cyber War Go?
Network World (07/26/07), M. Kabay

The authors of NATO Review for Winter 2001/02, former CERT senior analyst T. Shimeall, former NATO fellow and University of Pittsburgh professor P. Williams, and former CERT intelligence analyst C. Dunleavy, establish three distinct levels of cyber war and argue that defence planning needs to account for the virtual world to minimize damage in the real world. The first level of cyber war, described as "cyber war as an adjunct to military operations," is intended to achieve information superiority or dominance in the battle space and would include physical or cyber attacks directed at military cyber targets with the objective of interfering with C41, or command, control, communication, computing, and intelligence. The second level, limited cyber war, would attack cybernetic targets with few real-world modalities but very real consequences by launching malware, denial-of-service, and data distortion attacks. The authors consider the third level, called unrestricted cyber war, to be the most serious and possibly the most likely type of cyber war to occur. Unrestricted cyber war attacks both military and civilian targets and deliberately tries to create mayhem and destruction. Targets may include any part of any critical infrastructure. The attacks could result in physical damage, including injuries and deaths among civilians. The authors suggest that improvements need to be made in anticipation and assessment abilities, preventative and deterrent measures, defensive capabilities, and damage mitigation and reconstruction measures.