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

Δελτίο 113
22 Απρίλη 2008

US Presidential Election Can Be Hacked
IDG News Service (04/10/08), R. McMillan

A recent audit of the three most widely used electronic voting systems has found that the machines can be hacked, says University of California, Berkeley professor D. Wagner. The audit, which was conducted as part of California's review of electronic voting, found that hackers could install a computer virus on three systems from Diebold Electronic Systems, Hart InterCivic and Sequoia Voting Systems. The virus could then spread to machines throughout the county and alter the vote count. "The three systems we looked at are three of the most widely used around the nation," Wagner said during an e-voting panel discussion at the RSA Conference on Thursday. "They're going to be using them in the 2008 elections; they are still going to have the same vulnerabilities we found. He says the problems uncovered in the audit affect not only California counties, but counties across the country. Yet despite the pervasiveness of the problem, academics such as Wagner will find it difficult to approach voting system vendors because of the deep mistrust that exists between the communities, says Florida State University professor A. Yasinsac. He says vendors feel that if they talk to security researchers, it could be tantamount to admitting that they have bugs.

US Cyber Readiness Lagging, Panel Says
Network World (04/09/08), N. Weinberg

Cybercriminals are becoming more sophisticated, more organized, and more dangerous while federal funding for cybersecurity is lagging, legislation intended to toughen laws against cybercrime has stalled, and cooperation between private and public sectors needs improvement, said cybersecurity experts during a panel at this week's RSA Conference. Business Software Alliance CEO R. Holleyman said an estimated 250,000 computers are compromised everyday by bot-herders, the number of exploits is seven times higher than it was a year ago, and the cyber threat is "growing exponentially." US Rep. J. Langevin (D-R.I.), chairman of the Homeland Security Subcommittee on Emerging Threats and Cybersecurity, said cybersecurity has largely been ignored by government until recently. However, he said meaningful legislation will probably not happen this year. Langevin said that two major priorities for federal government are securing its own networks and securing the nation's critical infrastructure. The Homeland Security Department's G. Garcia said the big challenge facing Homeland Security is strengthening federal networks. Garcia also said the department is working to build a worldwide network of protectors.

NIST Shows On-Card Fingerprint Match Is Secure, Speedy
NIST Tech Beat (04/01/08), E. Brown

Researchers at the National Institute of Standards and Technology say a new fingerprint identification technology for use in personal identification verification (PIV) cards is both fast and secure. As part of the authentication process for the technology, the cardholder enters a personal identification number to authorize the reading of fingerprint data from the card, and a card reader matches the stored data against the newly scanned image of the cardholder's

fingerprints. In one model, biometric data on the card would travel across a secure wireless interface, which would eliminate the need to insert the card into a reader. In a second model, biometric data from the fingerprint scanner would be sent to the PIV smart card for matching by a processor chip embedded in the card, and the stored data would never leave the card. "If your card is lost and then found in the street, your fingerprint template cannot be copied," says computer scientist P. Grother. Ten cards with a standard 128-byte-long key and seven cards that use a more secure 256-byte key passed the security and timing test using wireless, but only one of three teams met NIST's criteria for accuracy. A new round of tests on the technology, which offers an improvement in protection against identity theft, will begin shortly.

N.J. Voting Technology in Question After Discrepancies in February Vote
Daily Princetonian (04/14/08), J. Wolff

An investigation into discrepancies recorded by several of New Jersey's electronic voting machines shows that some of the tallies from February's primary elections may not add up. On April 8th, a court subpoenaed electronic voting machines used for the primary elections in six New Jersey counties, questioning the accuracy and security of the machines. Later that day, Sequoia Voting Systems, the manufacturer of the machines, filed a motion to suppress the subpoenas, arguing that the subpoenas sought to test their machines under "unknown circumstances and protocols," which could unfairly undermine the reputation of Sequoia's machines and the public's confidence in election results. The controversy surrounding the New Jersey primaries started in March, when a Union County clerk noticed that the number of Democratic and Republican voters recorded by the DRE paper reports generated after the election did not match the number of votes cast in each primary on those machines. For example, one machine recorded that 60 Republican and 362 Democrat ballots were activated, but 61 votes were cast for Republican candidates and only 361 were cast for Democrats. Princeton University professor E. Felten says it is not the size of discrepancy that is alarming, but that a single machine is disagreeing with itself on how many voters voted. Similar discrepancies have been discovered on at least eight other machines in Union County and several more throughout the state. Sequoia has issued a memo blaming the discrepancies on New Jersey poll workers.

Cryptographers Speak of Threats, Voting and Blu-Ray Rumors
CNet (04/08/08), R. Vamosi

The creators of the Diffie-Hellman key exchange and the EMC security division discussed the state of security over the past year and answered questions posed by a moderator during the annual cryptographers' panel at RSA 2008 in San Francisco. Sun Microsystems' W. Diffie said pure defense does not work on the Internet, and added that the government might consider going after opponents where they live and using different ways to shut them down. Stanford University professor M. Hellman said thinking something is 99.9% safe is the greatest risk, and he warned about becoming complacent. MIT professor R. Rivest, who is part of a group that has released a public proposal on voting system standards, said he favors software-independent voting systems, which do not entirely depend on software and use paper or another way to capture votes. Meanwhile, Weizmann Institute of Science professor A. Shamir said the rumor that Blu-Ray offers better overall security than HD DVD could be a sign that security is becoming a factor in consumer electronics.

Needed: A 'Turing Machine' for Security
Government Computer News (04/11/08), W. Jackson

The spread of wireless access, mobile computing, peer-to-peer communications, and Web-based applications has made the shortcomings of informational security all the more pronounced, while information management and security is being impeded by the massive amount of data IT systems are being flooded with. RSA CEO A. Coviello suggested at this year's RSA Security conference that the problem of informational security might be approached from the perspective of famed British mathematician Alan Turing, and he offered the concept of a Turing machine for security. The notion involves embedding within the enterprise infrastructure functionality that could assume the responsibility of intelligent risk management, which would give security managers more freedom to focus on promoting innovation. Though an intelligent security system would still depend on high-level policy produced by people, the system would be capable of comprehending and anticipating human behavior, and understanding what content is valuable to which people and achieving a familiarity with how it is accessed and employed. This knowledge could be utilized to identify patterns and anomalies that could constitute risks. Coviello said that security managers need to encourage more innovation based on a mindset that seeks ways to permit activities rather than deny them because they may be risky, comprehensive knowledge of an organization's mission and requirements so risk can be assessed, the construction of repeatable processes, and the establishment of relationships with other teams within the organization so needs can be predicted, among other things. Coviello also wants Congress to support greater investment in education to nurture a larger and better talent pool of security professionals and place a higher priority on research and development for cutting-edge security methods and technologies.

'Big Brother' Buildings Offer Less Invasive Security
New Scientist (04/09/08), M. Iman

Mitsubishi Electric Research Laboratories researchers say buildings filled with motion sensors capable of tracking people's movements are more effective and less invasive to privacy than closed-circuit TV systems. MERL researchers Y. Ivanov and C. Wren say in addition to privacy concerns, CCTV footage is difficult to search through or interpret quickly. To test their system, the researchers fitted their 3,000-square-metre office building with 215 detectors placed along hallways at 2-metre intervals. The detectors record when someone walks by but do not record specific actions. The system includes software capable of detecting unusual or interesting patterns in the data collected by the sensors and displaying the movements of people around the building on a map in real time. The system does includes a handful of cameras positions at specific spots in the building, and that footage can be used to identify people detected by the motion sensors. Certain paths on the map can be selected to call up the motion and video data from that path at a particular moment to reveal who used the route. The system can also improve safety procedures. For example, it discovered a traffic pattern during a fire drill that showed almost everyone in the building left through one exit while two other doors nearby were largely unused. The system could also lead to energy savings by monitoring how late people stay at work, helping management decide when to turn off heating or air conditioning.

Programmers, DIY Types Embrace Soft, Hackable Chumby
Wired News (04/15/08), B. Gardiner

The Chumby is a small, inexpensive, leather-clad Wi-Fi Internet appliance with a hackable operating system that has become a popular device with software and hardware hackers. "The

key part of the Chumby's appeal is that it's an embedded-hardware device that's open," says Linux programmer A. Walton, a Chumby software hacker who moderates his own Chumby-hacking forum. "Everyone's used to open source software, but with open source hardware it's a whole new game. When you combine them both, Chumby hackers can literally do anything they want." The Chumby can deliver whatever channels of Internet-based content a user wants, and also comes with Adobe's Flash, enabling developers to construct their own widgets. So far more than 600 developers have built Flash widgets for the Chumby, and about 200 developers have shared those widgets on the Chumby Network. The physical device is designed in such a way that its core electronics can be easily separated from its outer shell, allowing owners to make the device look anyway they want. Chumby Industries founder Duane Maxwell says the whole business model for the Chumby was developed around a device that was made to be hacked. "We found that if you open up your device, people will be in the business of enhancing it," Maxwell says.

UW to Lead $6.25 Million Project Creating Electronic Sherlock Holmes
UW News (04/16/08), H. Hickey

The University of Washington will lead the Multidisciplinary University Research Initiative, a seven-university research effort intended to improve computers' ability to interpret data and predict the behavior of complex systems. The Defense Department is backing the five-year initiative with a $6.25 million grant. "A complex monitoring system has far too many pieces of information for any one person to look at," says UW computer science professor and principal investigator P. Domingos. "This award lets us do the research to develop a system for the military to look at all the available information that might be valuable and use it to predict behavior." The new system will use the power of reasoning much like Sherlock Holmes. The military has millions of possible clues, including sensors on soldiers, satellite maps, road monitors, unmanned aerial drones, and reports from reconnaissance missions. The system will use this information to make decisions and predict an adversary's next move. Domingos says existing systems only look at a single type of sensor data, but more complex situations require going to a higher level and integrating different types of information. For example, a computer could combine X-rays, photographs, test results, and patient information to make a tentative diagnosis automatically. The diagnosis could also be based on information from sensors that track a patient's movements and heart rate for weeks at a time.

Security From Chaos
US Department of Homeland Security (04/16/08), G. Cleere

The Assistant for Randomized Monitoring Over Routes (ARMOR), a Dept. of Homeland Security-sponsored project at the University of Southern California, is improving security at LAX airport in Los Angeles by predicting risk. The USC researchers have developed a computer model that tells police where to go to conduct random checks based on calculated probabilities of a terrorist attack at specific locations. The software records the locations of routine, random vehicle checkpoints and canine searches at the airport. Police then provide data on possible terrorist targets, their relative importance, and any changing data such as security breaches or suspicious activity. The software then produces random decisions, creating security patterns that are difficult to predict. "What the airport was doing before was not truly statistically random; it was simply mixing things up," says computer science professor M. Tambe at the Center for Risk and Economic Analysis of Terrorism Events (CREATE), a DHS Center of Excellence at USC. "What they have now is systematized, true randomization." CREATE works with government agencies and researchers to evaluate the risk, cost, and

consequences of terrorism, helping policy makers set priorities to find the best ways to counter threats and prevent attacks. Tambe says humans cannot create purely random systems for an extended period of time, as they will eventually make decisions based on prior decisions and experiences. ARMOR recently completed a six-month trial, and airport officials have given the university approval to transfer the software to LAX on a more permanent basis.

Ensuring Security for Cognitive Radio Networks Goal of CAREER Award Research
EurekAlert (04/15/08), L. Crumbley

Virginia Tech researcher J.-M. Park has received a $430,000 National Science Foundation Faculty Early Career Development Program Award to investigate improving the security of cognitive radio technology. Park says that cognitive radio technology could one day be used for two-way communications between tactical military forces or emergency responders. However, the advantages gained by cognitive radio technology are countered by new security threats. "In a civilian cognitive radio network, the motive of a malicious user might be to simply cause mayhem to other users or to receive notoriety," Park says. In a military setting, hostile forces may try to disrupt or disable a network to interfere with communications and gain a tactical advantage. Park plans to conduct an in-depth investigation of critical security issues in cognitive radio systems and networks. The research will include investigations into cooperative spectrum sensing, which occurs when multiple cognitive radio devices collaborate to identify unused radio spectrum bands; on-demand spectrum contention, which are protocols that enable multiple devices to work together with minimum interference; and spectrum etiquette mechanisms, which would prevent the malicious use of cognitive radio devices. "We hope our findings will help service providers and manufacturers develop more secure technology, and also benefit regulators involved in the standardization of cognitive radio systems," Park says.

Cybersecurity Issues Misunderstood, Experts Tell Congress
Defense News (04/07/08) Vol. 23, No. 14, P. 53; W. Matthews

Since late 90s, some cybersecurity experts have been saying that the nation faces an impending all-out Internet attack on its critical infrastructure--one that shuts down the electricity grid and water systems and drains bank accounts. However, those threats remain largely hypothetical, said J. Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies, at a recent House Armed Services subcommittee hearing. Lewis said the US should worry about Internet-based crime and espionage instead, which are more serious threats. Lewis pointed to the fact that last year US government computers were repeatedly broken into during attacks that appear to have been carried out by the Chinese. In addition to collecting information from the computer systems, which belonged to the US Dept. of Defense, State, and Commerce, the attackers also likely planted malware in the computer systems, Lewis said. Meanwhile, Internet criminals have created a black market for buying malware, hiring hackers, and renting botnets. In order to protect US computer systems from these threats, the government should put existing security practices to better use, said cybersecurity expert S. Goodman, who also testified at the hearing.