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

Δελτίο 56
12 Γενάρη 2007

Citing Problems, US Bars Lab From Testing Electronic Voting
New York Times (01/04/07) P. A1; C. Drew; I. Urbina

Inadequate inspections of voting machines were highlighted by the Election Assistance Commission's (EAC) temporary ban on Ciber's testing of electronic voting systems following the discovery that the Colorado lab was not complying with quality-control procedures and was unable to document that it was performing all the necessary tests, which are considered imperative to bolstering confidence in the results. Criticism was also leveled against Ciber concerning its plan to test new voting machines for New York State by Nystec analysts, who determined that Ciber failed to specify any procedures or testing methods for the bulk of the requirements, and also did not elaborate on how Ciber would seek bugs in the computer code or test defenses against hacking. "What's scary is that we've been using systems in elections that Ciber had certified, and this calls into question those systems that they tested," noted Johns Hopkins University computer science professor A. Rubin. Ciber is the leading tester of US voting machine software, and the company insisted that it is correcting its problems and will soon obtain EAC certification. It is only recently that the labs testing voting hardware and software became subject to federal oversight. The EAC has lacked a significant budget and it only completed creating the oversight program in December. There will be 3 EAC staffers and 8 part-time technicians tasked with passing test plans for each system and checking the results, but Rubin feels it would be better if the labs were required to employ teams of hackers to find software vulnerabilities.

Watch & Learn
Baltimore Sun (01/05/07) P. 1D; F. Roylance

The University of Maryland's James Clark School of Engineering and others are developing behavior recognition software that's being used to apprehend criminals and look for terrorist activity. R. Chellappa, a University of Maryland professor of electrical and computer engineering and director of UM's Center for Automation Research, developed computer programs using algorithms that transform digital video into mathematical patterns; these patterns can then be analyzed by software that looks for suspicious activity. The software can determine whether or not an individual is carrying anything, for example. Data from dozens of cameras can be analyzed by the software; 18 behaviors can trigger the software's attention, such as people moving very fast or standing around, cars that abruptly stop or speed up, crowds that form or break up, objects left unattended, and people who fall down. When an individual is identified as a threat, a yellow box appears around him on the computer screen. Chellappa has also created systems that can recognize an individual's gait as a means of identifying and remembering them, as well as noting changes in their gait. Gait recognition could also be used to help surgery patients in rehab, or people with disabilities, but recent pressure and funding from DARPA has caused the research to focus on security. The challenge facing behavior recognition software is how to track a person as they move between non-overlapping cameras, but Honeywell's Automation and Control Solutions chief technical officer D. Sheflin says, "I think we're only a year or two away from having it figured out." Chellappa explains

that discerning normal actions from the abnormal could lead to many innocent people being stopped, and that for the system to interest the public, false positives must be cut down on.

Open-Source Personal Tracking System Gets First Test
IDG News Service (01/02/07), N. Gohring

The developers of OpenBeacon say the open-source wireless tracking system is an attempt to address some of the limitations of existing commercial tracking technology. The OpenBeacon team had a crowd-control solution for millions of Muslim pilgrims to Mecca in mind in developing the technology, which was on display at last week's Chaos Communications Congress in Berlin. Though radio-frequency identification technology requires tags to pass through a specific spot, Wi-Fi systems present cost and power consumption issues. The tracking devices that OpenBeacon relies on are designed to transmit and then sleep, to ease demands on battery life, which is expected to last for several months. Meanwhile, OpenBeacon co-creator M. Meriac says mesh protocols will allow the devices to communicate with each other, rather than just a central base station. At the four-day event, attendees who bought 900 tags were able to use touch-screen monitors to see the whereabouts of other participating volunteers, view their profiles, and even update them. "We wanted to make this analysis transparent so that people are more aware of what data they're willing to give away," says Meriac.

Predicting the Top Security Threats for 2007
TechNewsWorld (12/30/06), J. LeClaire

McAfee Avert Labs expects identity theft and other efforts by malicious programmers to be on the rise in 2007. McAfee says that of the 217,000 known security threats, the leading security concerns for this year will be password-stealing sites with fake sign-in pages resembling well known services, adware, mobile phone attacks, and the use of video files to infect users with malware. Due to the computer's increasing role in everyday life, "there is a huge potential for monetary gains by malware writers," said J. Green of McAfee Avert Labs. He adds that increasingly sophisticated malicious methods make it more difficult for the average user to evaluate threats. IM attacks, in the form of spam over IM (SPIM), are predicted to rise, as are instances of hackers posing as familiar IM identities. Meanwhile, botnets will benefit from peer to peer architecture, encryption, and custom packing, and although botnets will be used to attack more common multimedia programs, the central control points of botnets will be far more difficult to find. "Money mules" are expected to play a large role in the year's botnet scams by physically transporting stolen goods, allowing cyberthieves to get around shipping regulations. The openness being driven by "Web 2.0" puts security at risk, as unfiltered user input and "client/server communication that takes place behind the scenes without end user interaction" can create vulnerabilities, says security expert Michael Sutton. He adds that programmers often ignore threats because no interaction is needed by the end user, but "attackers can ... intercept this communication and use it to attack the server." Phishing attacks have also been on the rise lately, and are expected to exploit Web programs.

Changes in e-Voting Likely Coming, Experts Say
IDG News Service (01/05/07), G. Gross

Several advocacy groups, including Common Cause and the Electronic Frontier Foundation, hosted a panel of election experts, who agreed that something must be done about the state of the nation's e-voting systems, but admitted that no widely accepted solution currently exists. Kentucky Secretary of State T. Grayson said, "We're at this point ... where I believe there's a

consensus that we need to do something. However, the consensus is ahead of the solution." Grayson added that since Kentucky has used e-voting machines without incident since the 1980s, many districts would be reluctant to change. Transparency is a widely accepted goal for e-voting, but experts disagree whether audits of both machines and ballots, or attaching printers to voting machines, can achieve transparency. Twenty-seven states currently require paper-trail systems to accompany e-voting, but only 11 of them require officials to conduct audits to assure the electronic votes match the paper ones. US House of Representatives Administration Committee staffer T. Hicks says it would be very difficult to complete wide-ranging changes to e-voting systems before the 2008 elections; 2010 or 2011 is a more realistic goal, he says. Hicks predicts that paper-trail audit legislation will be introduced in the next two years, and that another bill could allow independent researchers to see the source code used by e-voting machines.

Attack of the Zombie Computers Is a Growing Threat, Experts Say
New York Times (01/07/07) P. 1; J. Markoff

In light of the current trend of increasing botnet-enabled Internet crime, computer security experts are admitting that the Internet is becoming more at the mercy of cybercriminals, and that a new approach must be adopted. G. Evron, a computer security researcher for Beyond Security, says, "It's the perfect crime, both low-risk and high-profit. The war to make the Internet safe was lost long ago, and we need to figure out what to do now." Georgia Institute of Technology researcher D. Dagon, who co-founded a startup that concentrates on botnets, estimates that botnet programs exist on 11% of the over 650 million computers connected to the Internet. Internet pioneer and Carnegie Mellon computer scientist D. Farber laments, "It's an insidious threat, and what worries me is that the scope of the problem is still not clear to most people. The popular [Windows-based] machines are so easy to penetrate, and that's scary." A voluntary organization known as ShadowServer is observing botnet activity on about 400,000 infected machines. Computer security firm Message Labs estimates that over 80% of spam currently being sent comes from botnets. A program known as "rustock" recently gained attention for its ability to secretly add machines to a botnet, and use them for "pump and dump" schemes, yet it could also be used for a wide array of Internet crimes. Rustock is able to conceal infecting agents so that no digital fingerprints can be detected. Despite their best efforts, computer scientists cannot keep up with the improvements being made to botnet programs and are even beginning to fear for the commercial viability of the Internet; most ISPs are only making the situation worse, they say, by either ignoring or downplaying the problem. San Diego Supercomputer Center Internet researcher K. Claffy says, "It's a huge scientific, policy, and ultimately social crisis, and no one is taking any responsibility for addressing it."

The Logic of Privacy
Economist (01/04/07)

Stanford University computer scientists J. Mitchell, A. Barth and A. Datta are using the theory of contextual integrity to address the tension between the wide availability of personal data and the demand for privacy. The theory notes that total privacy is not required by people; information sharing can proceed provided certain social norms are adhered to. Mitchell and colleagues believe contextual integrity can be used to represent the codes of privacy in the formal phraseology of a computer language. Contextual integrity is dependent on four classes of variable: An information flow's context, the acting capacities of the individuals sending and receiving information, the types of information involved, and the transmission principles

that serve as the foundation of the information flow. Barth is using linear temporal logic, a mathematical logic system that expresses elaborate constraints on the past and future, to transform the descriptions of contextual integrity variables into formal expressions that can be employed in computer programs, in cooperation with New York University's H. Nissenbaum, the developer of contextual integrity. Linear temporal logic-based computer programs, unlike those written in other programming languages, describe the desired vision of the world. Mitchell's team has crafted logical formulas to represent American privacy laws, including those that encompass children's activities online, financial institutions, and health care; transmission principles can be communicated in logical terms by employing concepts such as "previously" and "eventually" as mathematical operators such as "plus," "minus," "multiply," and "divide" signs. Questions of privacy can be handled better through the application of contextual integrity, while the reasons why new information gathering techniques arouse anger can be better determined, according to Nissenbaum.

CMU Professor Investigates Vote
Pittsburgh Tribune-Review (01/09/07), R. Amen

The design of Florida's electronic ballot may have led 18,000 people to not vote for a candidate in the 13th Congressional District during last fall's general election, although seven leading computer scientists continue to study the software used in the touch-screen voting machines. A study from M. Herron, an associate professor in the Department of Government at Dartmouth College, cites poor ballot design as the likely problem. The 25-page e-ballot had the race between Republican V. Buchanan and Democrat C. Jennings atop the second page, and it was in between two races that had a large number of candidates. Some voters may not have realized the Buchanan-Jennings race was a separate contest, says Carnegie Mellon University computer scientist M. Shamos, who added that "the banner for the [US House of Representatives] race was very subdued." After testing the software of the iVotronic machines of Election Systems & Software, the Florida Department of State uncovered no flaws and believes ballot design and voter intent were behind the lack of votes. Like the state, the research team has not found any problems with the software so far. "[The work] is not complete, and we might yet find something," says Shamos, who expects the team to report its findings in January.

Spafford Leads as Computer Advisor, Scholar
Purdue Exponent (01/10/07), A. Thomas

E. Spafford is internationally known for his work in information security and ethics, but has always been respected for his dedication and positive attitude toward his field, his ability to work with people, and his sense of humor. Despite once quipping that trying to get useful information from the Internet is like trying to take a sip from a fire hose, he has not abandoned his own efforts to improve Internet functionality. "I'm intrigued by the problem," says the ACM US Public Policy Committee Chairman and Purdue University professor of computer science and electrical and computer engineering. "I think there is an incredible potential there; it's an interesting challenge." He still runs the Center for Education and Research in Information Assurance and Security, which was the first of its kind when he developed it. Spafford works a great deal at bringing talented individuals into computing, but devotes an equal amount of energy to making sure that those already in computing are paying attention to more than just the computers. He says, "It's important to think about people and communication. There are issues that don't get solved with programs or mathematics; the field is beginning to change to recognize that, but it's got a ways to go." Over his career, Spafford claims to have

learned three valuable lessons: That "Individuals can make a difference;" that trying new things is very beneficial, as "Some people seem very daring and some people seem very lucky, but you can make a lot of luck by actually thinking a little bit and then trying things;" and that promoting students and colleagues is the most rewarding thing he does, even though this is not a commonly held idea "in business or personal relationships."

Researchers: Hack Will Help Kill HD DVD Copy Protection
IDG News Service (01/08/07), R. McMillan

A hacker has recently published software, known as BackupHDDVD, that could facilitate the cracking of the Advanced Access Content System (AACS) copy protection encryption used on HD DVD and Blu-Ray disks. The software itself did not crack the encryption, but if the right title keys, numeric codes used to unlock digital content, are found, BackupHDDVD could allow users to unscramble the content of a disk. Princeton computer science student A. Halderman and researcher Ed Felten say the software is "the first step in the meltdown of AACS." Content Scrambling Software (CSS), the system used to protect DVD, was hacked by three individuals only a few years after it release. While AACS allows Hollywood to revoke a key, meaning changing a new movie so its keys cannot be read by a HD DVD or Blu-Ray player that has been cracked, this system only works if hackers publish their findings, and even if a key is revoked, disks that have already been published cannot be changed. Halderman says, "What the future looks like to us is that some individuals will have cracks that they don't publish and which Hollywood is unable to revoke. Other people will have cracks that they do publish, and which will work for all old disks." He says it is just a matter of time until title keys are available, but Gartner analyst Mike McGuire says Hollywood will not suffer too much as long as they keep movies from being illegally cracked and traded while they are still in theatres.