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

Δελτίο 40
16 Σεπτέμβρη 2006

How Much Can State Trust Electronic Voting?
Baltimore Sun (09/10/06) P. 1C; M. Harris

In response to the disastrous presidential election of 2000, an increasing number of states have been acquiring electronic voting machines, though their reliability and security have often been questioned by voting-rights advocates and computer scientists. While the machines have been blamed for isolated voting irregularities, analysts warn that even greater damage could be inflicted by a hacker tampering with the machine's code or a corrupt poll worker inserting a malicious memory card into the machine that could systematically alter the results. In Maryland, which adopted Diebold e-voting systems after the 2002 Help America Vote Act, the reliability of the systems has been hotly debated, with some experts claiming that the computer scientists' warnings are overblown. "Computer science guys are able to get away with what I consider to be shameless scare tactics that don't take into account everything else that goes on in an election," said D. Norris, director of the National Center for the Study of Elections at the University of Maryland, referring to accuracy tests for the machines, tamper tape, and the poll workers who monitor voters on Election Day. A. Rubin, an author who wrote one of the early texts on the flaws in Maryland's voting machines and a favorite target of Norris, was able in testing to find the machine's source code, and two vital passwords to protect the system. Six months later, a group of computer experts commissioned by the State of Maryland found that an attack on the state's machines might be difficult, but not impossible. The group found that someone looking to manipulate the results of an election would have to sleuth out the password to a legitimate voter's smart card--an ATM-sized card with a computer chip in the center that displays a voter's pre-programmed ballot on the screen. Reproducing the cards from scratch would cost around $750 each, the group found, noting that the cost could be well worth the value of fixing an election. In response to these concerns, many in Maryland have called for the state's voting machines to include a backup paper auditing mechanism that enables voters to verify their ballots after they are cast.

Voice and Signature for the Identification of Persons
Basque Research (09/07/06)

A number of universities in Spain are collaborating to design a database that would be linked to biometric systems used to identify individuals. Starting with voice, signature, and handwriting analysis, the database will play a key role in the comparison and contrasting of the algorithms of past and present samples, vital for biometrics to be accurate. The database will focus not only on spatial data but on dynamic data as well, that is the movement of a person while performing a certain action, which current systems often fail to differentiate accurately. Such actions could include a person's gait, or how they operate a mouse or keyboard. The Dept. of Electronics and Telecommunications at the School of Engineering in Bilbao, Spain, has been working in collaboration with Univ. of the Basque Country (UPV-EHU) researchers to automatically collect biometric signatures both offline and online. Online biometric verification is harder to forge, but has a higher margin of error, which is something the researchers hope to improve on.

IT Security Lags Five Years After Sept. 11
IDG News Service (09/07/06), G. Gross; B. Ames; R. McMillan

Cybersecurity leadership, airplane scanning, and interoperable communications networks have been neglected by the US government since the Sept. 11 attacks, say industry analysts. Progress has been slow in these particular areas and critics say there is too much emphasis being placed on the National Security Agency's (NSA) electronic-surveillance program, rather than on other forms of technology. NSA's program has been criticized for invading innocent people's privacy, but President Bush defends the program and insists it "helps protect Americans." "If an al Qaeda commander is calling the US, we need to know why they're calling," Bush says. IT security groups want the US government to focus more on cybersecurity. Meanwhile, unscanned cargo is coming into the United States every year on 11.2 million trucks, 2.2 million rail cars, and 51,000 cargo ships, according to the Dept. of Homeland Security. Beyond cargo, many say the government is not moving fast enough to help emergency responders get the spectrum they need. Emergency responders working during the Sept. 11 attacks discovered their communication systems were not interoperable. Congress has given TV stations a deadline to use digital broadcasts, and more radio spectrum is expected in February 2009. The Bush administration is adamant that it has made progress in the last five years, but others see differently. "There's no national strategy to coordinate all these efforts," says S. Jones at the First Response Coalition. "Nationally speaking, I don't know that we're better off than we were five years ago."

Modeling Terrorists
IEEE Spectrum (09/06) Vol. 43, No. 9, P. 26; H. Goldstein

The prediction and prevention of terrorist incidents could be aided by new simulators, such as first-person shooter-type games in which synthetic human agents improvise because they follow individualized sets of complicated rules instead of an inflexible script; such simulators model terrorists and their accomplices through profiling of terrorist backgrounds, value systems, and other variables. The development of such simulations is fueled by a belief that terrorists' mindset, motives, and organizational makeup--and thus their actions and plots--could be determined by computers equipped with the appropriate software. Outside observers are betting that software designed to identify key members of a terrorist organization will be used by intelligence analysts to compile a list of people to terminate or apprehend so as to cripple the organization most effectively; this possibility generates concern about the moral implications of relying on such models to make life-and-death decisions, and also raises questions as to whether analysts will even avail themselves of such technology, should it become widely available. Experts such as Ball State University anthropologist J. Nyce strongly doubt that these tools will be employed by the intelligence community, "because the cognitive, intellectual, and work requirements have not been taken into account in their design." Among the drawbacks of current intelligence analysis cited by experts is analysts' dependence on informal analytical methods, their tendency to make forecasts based on incorrect rules, and their responsibility after 9/11 to sift through even more data because of the elusive nature of terrorists and the conviction that the Internet is their primary means of communication. University of Pennsylvania professor B. Silverman thinks analysts' job could be greatly enhanced by having computers model an individual terrorist's desired vision for the world and what actions he is willing to take to realize that vision. Silverman's team has produced simulated terrorists complete with physiological traits, long-term memories, value systems, and reasoning skills extracted from over 100 models and theories drawn from political science, anthropology, and psychology, along with empirical data from medical and social science field research, polls, and experiments.

Stemming Spam: Internet Routing and Spam Data Reveal Trends to Help Researchers Build Better E-mail Filters, Georgia Institute of Technology (09/12/06)

Researchers at the Georgia Institute of Technology have found that addressing spam at the network level could be a more effective solution for Internet service providers than today's message content filters. They have also developed algorithms that can detect when a computer is a member of a botnet, as well as a technique for bolstering the security if the Internet's routing structure. "Content filters are fighting a losing battle because it's easier for spammers to simply change their content than for us to build spam filters," said N. Feamster, an assistant professor of computing. "We need another set of properties, not based on content. So what about network-level properties? It's harder for spammers to change network-level properties." The research will be presented at the ACM SIGCOMM conference on September 11-15 in Pisa, Italy. The researchers spent 18 months collecting Internet routing and spam data from one domain. They found that they can identify which Internet service providers are transmitting spam, as well as the numerous narrow ranges of IP address space that are only producing spam. Spammers exploit vulnerabilities in Internet routing protocols by broadcasting a route for that space to the routers on the Internet, enabling them to assign their machines any IP address within that space. They then send spam from those machines and promptly withdraw the route of transmission. The IP address is no longer reachable and the route disappears by the time the recipient can file a complaint. "Even if you're watching the hijack take place, it's difficult to tell where it's coming from," Feamster said. "We can make some good guesses. But Internet routing protocols are insecure, so it's relatively easy for spammers to steal them and hard for us to identify the perpetrators." Feamster hopes that his research will lead to more secure Internet routing protocols and improved spam filtering.

Sandia Fingerprinting Technique Demonstrates Wireless Device Driver Vulnerabilities Sandia National Laboratories (09/12/06)

Researchers at Sandia National Laboratories have demonstrated a wireless-networking vulnerability that could enable a hacker to identify an 802.11 wireless driver without modifying the device. By making the unique "fingerprinting" technique publicly known, the researchers hope to improve the security of wireless communications. Device drivers have become a principal vulnerability in today's operating systems, Sandia's J. van Randwyk says. Video and keyboard drivers are unlikely targets because it is difficult to gain physical access to them, but some types of drivers, such as wireless cards, Ethernet cards, and modems, can be compromised without physical access, Van Randwyk notes. "Wireless network drivers, in particular, are easy to interact with and potentially exploit if the attacker is within transmission range of the wireless device," he said. The research demonstrates that an attacker can monitor a victim's wireless traffic so long as he is within transmission range. Since the attacker is not sending data, he essentially operates invisibly, making the attack difficult to detect. Wireless configurations periodically send out probe request frames to scan for access points, but the requests are not governed by any standard 802.11 specifications. The fingerprint technique highlights the vulnerabilities that arise from different wireless device drivers performing the probe request function differently. The fingerprinting technique tested at accuracy rates between 77-96%, depending on the setting of the network.

Will Airport of the Future Fly?

CNet (09/13/06), S. Olsen

At the opening session of the FAA/NASA/Industry Airport Planning Workshop, Cisco Systems' Dave Evans articulated a bold vision of technological transformation for airports, where virtual intelligence agents could check in bags, new sensor networks could improve security, and pilots could even fly a plane from home using a remote brain-machine interface. Evans described RFID readers that could enable airlines to identify passengers by their cell phones and check them in remotely, while new display technologies could change the way that flight information is presented inside the airport terminal. Evans told the audience that he has developed software that could enable virtual intelligence agents to learn from their interactions with human airport workers. Executives in attendance from the airport industry reacted to Evans' predictions with a mixture of excitement and fear, as well as a healthy dose of skepticism, given that airports still lack some of the most basic technological needs, includeing devices to scan passengers and luggage for dangerous devices such as bombs. Government regulations also stall the adoption of new technologies. "I think it's a real challenge for government to react to technology changes whether it's security or flying," said Steve Martin, CFO of policy and planning for Airports Council International, North America. "I don't see government agencies being able to keep up with technology's exponential growth." Nevertheless, the participants expressed measured optimism that policymakers might cut through some of the red tape if they were shown simulations of how new technologies could improve the airport industry.

Personal Data Protection Vital to Future Civil Liberties
IST Results (09/13/06)

Researchers working under the SWAMI project set out to determine the privacy implications of the ongoing miniaturization of intelligent devices that can be embedded throughout the environment to capture and relay personal information. With microelectro-mechanical sensors the size of a grain of sand capable of detecting a whole spectrum of environmental conditions, from light to vibrations, the environment is becoming much more intelligent, but the era of continuous communication could have troubling implications for security, privacy, and civil liberties. Observers believe that ambient intelligence could be a major boon to Europe's economy, and the field has already received considerable research funding. But in order to deliver customized information and services to individual users, an inordinate amount of personal data must be stored, where it could be vulnerable to abuse. "Most people would be shocked to find out just how much information they consider private is already in the public domain," said David Wright, the project's information coordinator. The SWAMI researchers explored several everyday scenarios that demonstrated how information could be misused in a world of intelligent environments, such as a hacker accessing the control system of a traffic grid powered by ambient intelligence, or the theft of a large volume of personal data from a data-aggregation company whose main system is powered by ambient intelligence. Wright and his colleagues compiled a list of proposed measures for safeguarding personal data, including the privacy-enhancing technology that can be incorporated into fourth-generation mobile devices. They also call for legislation at both the national and European levels to meet the challenges of increasingly intrusive technologies.