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

Δελτίο 137
15 Δεκέμβρη 2008

Saying 'Cheese' for More Effective Border Security
National Institute of Standards and Technology (11/25/08), B. Stein

Facial recognition systems can be extremely useful in situations that require comparing a photograph to images of known or suspected criminals, but creating a match can be almost impossible when using low-quality images. National Institute of Standards and Technology (NIST) researchers have discovered that several simple steps can significantly improve the quality of facial images collected at border points like airports and seaports. The NIST recommendations for improving facial images can be implemented relatively easily using existing facial recognition technology. The Dept. of Homeland Security's US-VISIT program digitally collects picture and fingerprints from travelers entering the United States, and the NIST has been working with US-VISIT to improve the processes and technologies. Following the observation of the entry-point at Dulles Airport in Washington, the NIST researchers identified and shared several steps for acquiring better facial images. For example, a report from NIST recommends that operators should adjust camera settings to ensure subjects are properly in focus, as well as using a traditional-looking camera in facial-recognition systems so individuals clearly recognize the camera and look directly into it when having their picture taken. In tests that followed the NIST's suggestions, 100% of images from the improved systems were able to capture participants' faces, with all of the participants facing the camera; the researchers also found additional improvements could be made using a graphical overlay on the camera display to better position the camera. The researchers believe such changes will improve the performance of facial recognition systems in real-world settings using existing technology.

Paper Ballots Touted as Most Secure
The Denver Post (12/02/08), J. Ingold

Colorado's Election Reform Commission discussed the reliability of electronic-voting machines during a recent meeting. Voting-machine expert and Rice University professor D. Wallach addressed the state officials, county clerks, and elections experts charged with improving the state's elections policies and said e-voting machines are vulnerable to tampering. "In terms of the systems that are available today, hand-marked paper ballots counted by scanners are the best technology," Wallach said. Some of the largest counties in the state are using e-voting machines, but many counties still rely primarily on paper-ballot voting. More county clerks have begun to make security an issue, said Paul Craft, an expert in voting-machine certification. "You simply cannot continue to operate systems out there that cannot be secured," Craft said. US Election Assistance Commission Chairwoman R. Rodriguez said her agency is in the process of creating stronger voting-machine security standards.

You're Leaving a Digital Trail. What About Privacy?
The New York Times (11/30/08), J. Markoff

About 100 Massachusetts Institute of Technology (MIT) students have accepted free smartphones that track their every move as part of a research project, and these and other technolo-

gies are enabling collective intelligence, which promises to open up new social services and benefits. But collective intelligence also has the potential for misuse, such as allowing the government to identify members of a protest group by tracking social networks. "Some have argued that with new technology there is a diminished expectation of privacy," says Electronic Privacy Information Center executive director M. Rotenberg. "But the opposite may also be true. New techniques may require us to expand our understanding of privacy and to address the impact that data collection has on groups of individuals and not simply a single person." Cornell University sociologist M. Macy observes that people and organizations are increasingly electing to interact with one another via digital technologies that record traces of those interactions, which enables scientists to analyze those interactions in ways that were deemed impossible five years ago. The MIT Media Lab's A. Pentland says the surveillance-society traps that lurk in collective intelligence technologies can be evaded, and he has proposed precepts to ensure that people have ownership rights to their behavioral data. The principles dictate that people are entitled to possess their own data, that they control the data that is collected about them, and that they may redeploy, remove, or destroy their data as they see fit.

U.S. Is Losing Global Cyberwar, Commission Says
BusinessWeek (12/07/08), K. Epstein

The United States is woefully unprepared for the challenges of 21st century cybersecurity, concludes a new report from the US Commission on Cybersecurity, which calls for the establishment of a Center for Cybersecurity Operations to be supervised by a special White House advisor. The center would function as a new regulator of computer security in both the public and private sector, while active policing of government and corporate networks would incorporate new rules and a "red team" to test computers for flaws currently being exploited by cybercriminals. The report notes break-ins at the US Depts. of Defense, State, Homeland Security and Commerce, and at NASA and the National Defense University in 2007. For example, both military and corporate networks have been hit by the malicious agent.btz program, and the attacks have become more sophisticated and tougher to track down. The US military has uncovered approximately 7 million unprotected electronic devices. Cybersecurity commission member T. Kellermann says Homeland Security Department-led initiatives to bolster cybersecurity have been impeded by bureaucratic confusion and agencies and corporations' refusal to share information about data breaches. He adds that several members of the commission are working to persuade President-elect B. Obama to take appropriate action. Obama's July 16 pledge to "declare our cyberinfrastructure a strategic asset" and to "bring together government, industry, and academia to determine the best ways to guard the infrastructure that supports our power," has given members hope, as has his promise to appoint a national cyber advisor who would report directly to the president.

Thieves Winning Online War, Maybe Even in Your Computer
New York Times (12/06/08) P. A1; Y. Markoff

Malware continues to overcome security professionals' efforts to defend against it. "Right now the bad guys are improving more quickly than the good guys," says SRI International's P. Lincoln. As businesses and individuals become increasingly involved in online communities, cybercriminals are given more opportunities to infect machines and commit crimes. The Organization for Security and Cooperation in Europe estimates that credit card thefts, bank fraud, and other online scams rob computer users of $100 billion annually. In late October, the RSA FraudAction Research Lab discovered a cache of 500,000 credit-card numbers and bank account log-ins that were stolen by a network of zombie computers run by an online

gang. "Modern worms are stealthier and they are professionally written," says British Telecom chief security technology officer B. Schneier. "The criminals have gone upmarket, and they're organized and international because there is real money to be made." Meanwhile, malicious programs are becoming increasingly sophisticated, with some programs searching for the most recent documents on the assumption that they are the most valuable and others stealing log-in and password information for consumer finances. Microsoft researchers recently discovered malware that runs Windows Update after it infects a machine to ensure the machine is protected from other pieces of malware. Purdue University computer scientist E. Spafford is concerned that companies will cut back on computer security to save money. "In many respects, we are probably worse off than we were 20 years ago," he says, "because all of the money has been devoted to patching the current problem rather than investing in the redesign of our infrastructure."

New Tool to Audit the Use of Private Data
University of Southampton (ECS) (12/05/08), J. Lewis

University of Southampton computer scientists have developed a method for analyzing personal and confidential information to determine where it has come from, how it is being used, and how it can be made secure. L. Moreau and R. Aldeco-Perez in the School of Electronics and Computer Science have developed a case study based on private data in a university and the requirements of the Data Protection Act. As a result of the tool, called Provenance, systems could be redesigned to include secure auditing strategies, which ultimately would make them more robust and trusted. "At the moment when data is leaked, there is no systematic way to analyze the scenario," Moreau says. "We are now working towards the first prototype capable of auditing this data." A Provenance prototype should be available in six months.

Safer, Better, Faster: Addressing Cryptography's Big Challenges
ICT Results (12/04/08)

The European Union-funded ENCRYPT network of excellence united 32 research institutions, universities, and companies in a four-year cryptography research effort. International Association for Cryptologic Research president and ENCRYPT leader B. Preneel, a professor at Katholieke Universiteit Leuven in Belgium, says the three major issues facing cryptographers are cost, speed, and long-term security. Cost and speed are closely connected as a result of the trend of storing increasing amounts of information in distributed systems. Cost refers to both the cost of hardware systems capable of managing complex encryption and the energy used to run cryptographic processes on increasingly small, low-power devices. "In a few years we will have devices in our pockets with 10 terabytes of storage capacity--current methods are far too slow to encrypt that amount of data practically," Preneel says. Another major problem is that much of the data currently being generated will need to be kept secure for decades, or even centuries, but cryptography becomes increasingly easy to crack as it ages. The ENCRYPT project was structured into five core research areas, in which the researchers developed improved cryptographic algorithms, ciphers, and hash functions. A major achievement of the project is eight new algorithms with the ability to outperform the Advanced Encryption Standard. The project also developed a new method for creating cryptographic protocols based on game theory, and created lighter cryptographic algorithms for use in small, low-power devices such as smart cards and RFID tags.

DHS Creates Privacy Principles for Scientific Research

CNet (12/09/08), S. Condon

The US Department of Homeland Security (DHS) has developed privacy principles for science and technology-related research and development projects that involve data mining. The DHS privacy office worked with the agency's directorate of science and technology to create the "transparency principle," which would have the directorate conduct privacy impact assessments for all research projects using personally identifiable information. By creating privacy impact statements from the inception of a project, the department would be able to clearly articulate and document the purpose of its research initiatives, as stated in the "purpose specification principle." The DHS also would publish the assessments for any non-classified projects. The principles are meant to assure the public that DHS will only use data that it needs and keeps secure. They also address privacy training for personnel involved in projects, audits, and a redress program for handling complaints and questions. DHS sent the privacy policies to Congress on Dec. 8.

Hackers, Others Seek DMCA Exemptions
Wired News (12/03/08), D. Kravets

The US Copyright Office has received 19 comments as part of 9 requests for exemptions to anti-circumvention provisions to the Digital Millennium Copyright Act (DMCA). Enacted 10 years ago, DMCA requires that the Copyright Office and the Librarian of Congress request proposals for changes every 3 years. More than a dozen DMCA exemptions have been granted, and public hearings on the most recent requests will be held in early 2009. Several groups have proposed a variety of exemptions. The American Foundation for the Blind has asked to renew an exemption allowing the hacking of an e-book's shuttered read-aloud function. Film studies professors are currently allowed to copy clips from copyrighted and encrypted DVDs for educational purposes, and several petitions have asked that the right be extended to documentary filmmakers and US teachers of all subjects at all levels. University of Michigan computer scientist J. Halderman has submitted petitions to hack copy-control measures on sound recordings, videos, and audiovisual works for good-faith testing, investigating, or correcting security flaws or vulnerabilities. The Electronic Frontier Foundation is asking for an exemption to circumvent DVD encryption to obtain clips for use in noncommercial videos that do not infringe copyright.

'Privacy Will End in 2013'
Financial Times - Digital Business (12/03/08) P. 6; J. Shillingford

CSC Digital Disruptions report lead researcher A. Fuss says that information will become increasingly transparent in the future, and social networks will enable businesses to solve problems far faster and more effectively. Fuss envisions a future in which RFID-like tags enable the world to track every detail of the financial markets, similar to how department stores can track products. By 2013, technology will be widely used to monitor people's lives, but Fuss believes if this information is made available to everyone the Big Brother element would be negated. "You'll still be able to have secrets, but only if you can keep them off the Net," he says. "Privacy will be available, but only to those who can afford to pay for it. For most people, privacy will end in 2013, or a little beyond that." Multitasking will increase, so attention metrics will re-emerge to measure the success of TV programs, advertisements, and other initiatives, Fuss says. Quantum computing will make modern encryption obsolete, jeopardizing any transaction that relies on encryption. People also will be able to print toys, parts, furniture, and other products using three-dimensional printers. From 2025 to 2050, and beyond, na-

notechnology will provide the ability to create anything, molecule by molecule, Fuss predicts. "The technology is at very early stages, but it is definitely going to happen," he says.

Carnegie Mellon CyLab Survey Unveils Major Gap in the Way U.S. Boards and CEOs Manage Cyber Risks, Carnegie Mellon News (12/02/08), C. Swaney

Carnegie Mellon University's CyLab has surveyed 703 corporate board directors and found that only 36% of the respondents said their board was directly involved in overseeing the management of information security. The boards were involved about 31% of the time in assessing risk related to IT or personal data. Only 8% said their boards had a risk committee that is separate from the audit committee, and 12% have established functional separation of privacy and security. Cybersecurity should be viewed as an enterprise risk management issue rather than an IT problem, say Carnegie Mellon researchers. "There is a clear duty to protect the assets of a company, and today, most corporate assets are digital," says CyLab's J. Westby, lead author of the survey. The researchers offer recommendations for improving the corporate governance of privacy and security, such as establishing a board risk committee that is separate from the audit committee, reviewing existing top-level policies, and embracing security and privacy issues. "Without the right organizational structure and interest from top officials, enterprise security can't be effective no matter how much money an organization throws at it," says report co-author Richard Power.