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

Δελτίο 105
6 Φλεβάρη 2008

Digital Identification Plan Still Facing Many Hurdles
Investor's Business Daily (01/29/08) P. A5; D. Howell

Although implementing Real ID standards for driver's licenses is not required until 2014, some experts are worried that problems could arise as early as this spring, specifically at airport security lines. By law, Real ID-compliant driver's licenses will eventually be required to board commercial flights or to enter federal facilities, but 17 states have passed legislation against the Real ID act amid concerns over costs and privacy fears. States can apply for extensions to complying with Read ID, but those that do not by early May could find their licenses invalid for boarding commercial aircraft or for entering federal facilities. The Dept. of Homeland Security "has been aware of problems with the way the Real ID Act was written since May 11th, 2005," says the American Civil Liberties Union's T. Sparapani. "They failed to go back to Congress to ask for modifications or repeal." Homeland Security Secretary M. Chertoff says Real ID will give law enforcement a powerful advantage against falsified documents and will bring piece of mind to citizens concerned over identity theft. The purpose is not to establish a national ID card, but to create common standards for licenses, DHS says. To comply with the Real ID Act, states will have to collect significantly more information to issue a license than they currently do. "As a result of Real ID requirements, more information might be stored in a (new) set of databases that are going to be accessed by thousands of people around the country, along with some existing databases," says E. Spafford, chairman of ACM's US policy committee. "The combination of that information will make it easier to commit identity theft and fraud."

Voting With (Little) Confidence
Technology Review (01/29/08), E. Naone

The Emergency Assistance for Secure Elections Act of 2008, recently introduced by Rep. R. Holt (D-N.J.), proposes government funding for jurisdictions that use electronic voting machines to help switch to systems that produce a paper trail, but many experts believe that a paper trail alone is not sufficient. University of Maryland professor B. Bederson, who was part of a team that conducted a five-year study on voting machine technology, says that machines need to be evaluated on more than security, with a stronger focus on usability, reliability, accessibility, and ease of maintenance. "Security, while important, happens to be one of those places where voting machines actually have not proven to fail," Bederson says. "However, in many other ways, they have failed dramatically, especially [regarding] usability." In a usability study run by the University of Maryland, the University of Rochester, and the University of Michigan, researchers evaluated electronic voting systems built by Diebold, Elections Systems and Software, Avante Voting Systems, Hart InterCivic, and Nedap Election Systems, as well as a prototype built by Bederson. Participants were told to vote for specific candidates in mock elections. The researchers compared the results against how the voters were told to vote and found that even in simple elections--a single race present on one screen--there was an error rate of about 3%. As the task became more complicated, such as having a voter change their selection, the error rate increased to between 7-15%. In one test, errors caused different candidates to win based on which machine was used. Bederson's machine had the lowest error rate for the simple task, which Bederson says is a strong indication that voting machine vendors need to improve their systems.

Face Recognition Made Possible
AlphaGalileo (01/25/2008)

Hung-Son Le of Umea University in Sweden has developed algorithms that enable a computer to recognize a face, even if it accesses a database that has only one picture of the individual. The algorithms are capable of improving contrast in both under-exposed and over-exposed pictures, and the system does not need to be retrained, like existing Hidden Markov Model (HMM)-based competitors, to "know" new pictures with different expressions taken under different illumination conditions. In experiments and tests, the system performed better than the leading competitors. Face-recognition systems are usually trained using a database of face images that have different illumination and poses, which can be costly and difficult to collect. With Le's algorithms, users would not have to worry about the quality of pictures, facial expressions, different angles, and illumination. Banks could potentially use Le's research to roll out ATMs that are capable of recognizing the face of customers as they look into a camera.

Cyberadvice Awaits the Next President
Government Computer News (01/21/08) Vol. 27, No. 2, W. Jackson

The Center for Strategic and International Studies, a security and policy think tank, is organizing a list of recommended security initiatives for the next president to follow. The Commission on Cyber Security, formed by the CSIS, will brainstorm practical policy changes and will address issues of infrastructure protection, software assurance, and inter-agency cybersecurity before submitting an agenda by the end of this year. Senior fellow J. Lewis, also the director of CSIS' Technology and Public Policy Program, says the group is comprised of 35 reputable experts who are likely to get the next president's attention with their views on security. "We want to focus on what can be implemented, not what would be nice to have," he says. The group expects to recommend up to six new initiatives to the incoming president. "Despite the good work of a lot of people, the problem has gotten worse," Lewis says. "With a new administration coming in, this was an opportunity to step back and look for new ideas. It seemed like a good time to do it."

University of Virginia Engineering School Student Probes Facebook's Vulnerabilities
University of Virginia (01/30/08)

University of Virginia computer science major A. Felt is leading a research project focusing on privacy issues surrounding the Facebook social networking site, and is investtigating the information sharing that takes place when users download a Facebook application. Although the applications add variety to a Facebook user's profile page, they also increase the user's vulnerability. Anyone with a Facebook account can create and distribute an application. While the applications appear to be part of Facebook's platform, they are actually running on the developer's server. When a user installs an application, the developer is capable of seeing everything the user can see, including names, addresses, friends' profiles, and photos. "Since all applications receive access to private information," Felt says, "this means that 90.7% of Facebook's most popular applications unnecessarily have access to private data." There are currently no restrictions on what applications, and their developers, can do with user information, and while Facebook's "Terms of Use" warn developers not to abuse the data they have access to, there is no way for Facebook to enforce this rule, Felt says. "An application developer could easily acquire personal information for millions of users," says U.Va. computer science professor D. Evans. Felt's goal is to close this privacy loophole with a privacy-by-proxy system she developed that will allow Facebook to hide user information while still maintaining the applications' functionality.

Getting CERIAS About Security
Network World (01/31/08), M. Kabay

At Norwich University, a meeting of ACM's Special Interest Group on Security, Audit and Control (SIGSAC) student chapter has been a weekly lunchtime ritual for several years. M.E. Kabay writes that the vast collection of research and educational letters, documents, and links available from the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University is an excellent resource for meeting material. CERIAS developed out of the Computer Operations, Audit, and Security Technology (COAST) project in the Computer Sciences Department at Purdue in 1991, under the direction of professors E. Spafford and S. Wagstaff Jr. In 1999, COAST became part of CERIAS, considered one of the world's leading centers for research and education in information security critical to the protection of vital computing and communication infrastructure.

Paper Outlines Methods for Beating Anonymity Technology
Dark Reading (01/30/08), T. Wilson

S. Murdoch, a doctoral candidate at the University of Cambridge's Computer Laboratory, has published a dissertation that shows that observing the behavior of users of "covert channels," especially anonymity systems, may be enough to discover their intentions, or even their identity. In the 140-page paper, Murdoch says the approach is similar to how card players in a game of bridge are able to determine cards by observing the behavior of other players, and adds that collusion between two partners can make the process easier. The strategy can be applied to TCP/IP environments and the simple traffic analysis of an "anonymous" network such as Tor. His findings are not very different from those presented by a group of researchers at the Black Hat conference last August. Murdoch says that anonymizing technologies might offer protection from casual scans or monitoring, but they are unlikely to withstand the intense and careful scrutiny of truly dedicated attackers, researchers, or law enforcement officials. "[There is] a wealth of practical experience in covert channel discovery that can be applied to find and exploit weaknesses in real-world anonymity systems," the paper says.

Prof. Aims to Improve Internet Security
Wisconsin State Journal (01/26/08), H. LaRoi

University of Wisconsin-Madison computer scientist P. Barford and his colleagues have developed a new approach to detecting network intrusions by focusing on a slight vulnerability in malicious traffic. When installed by network service providers, Barford's technology is able to be specific and more general at the same time when detecting and identifying malicious signatures, which will prevent benign traffic from being labeled as malicious, reducing the false positives that can cripple security systems. The technology can also use a single signature to detect classes of attacks, a feature other systems do not offer, Barford says. "If an attack is similar to something we've already seen, we're going to catch it," he says. "That's our mechanism for staying ahead." UW-Madison's Office of Campus Information Security's J. Savoy says the key to Barford's technology is its ability to reduce false positives. "Sometimes false positives can lead you to a better understanding of your network," Savoy says. "The problem is if you have hundreds of false positives and you have to weed through every one, the chance of you missing a real one is greatly increased." Barford says countering botnets is mostly a matter of damage control. "The attackers only have to find one means of attack," he says. "The defenders have to defend against all means of attack."

Q&A: For E-Voting, Holt Looks to Undo HAVA's Havoc
Computerworld (02/04/08), D. Radcliff

In an interview, US Rep. R. Holt (D-N.J.) says the Help Americans Vote Act of 2002 (HAVA) has forced the nation to accept insecure, electronic-voting systems that undermine confidence in the election process. Aside from security, Holt says the biggest problem with e-voting is there is no way to verify the validity of a voter record. For the past six years Holt has been championing the voter Confidence and Increased Accessibility Act, which would require voter-verifiable paper ballots and random, mandatory audits of votes cast over e-voting systems in every county in every state. Holt is also pushing to approve emergency funds to help election officials add paper systems to their e-voting machines by the general election in November. "If you're going to be able to verify, there has to be an independent path accessible only to the person able to verify that the voter's intentions are reflected in the vote," Holt says. Beyond shoring up existing e-voting systems, Holt says future e-voting legislation should include "chain-of-custody requirements and transparency of software so that the software would be available for independent people to check." He says that "an audit will be the most direct, simplest way of uncovering problems even if there is a software error, be it innocent or malicious."