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

Δελτίο 69
11 Απρίλη 2007

Association for Computing Machinery President's Award Honors Leading Proponent of Computer Security, Ethics, Safety, AScribe Newswire (04/03/07)

ACM Fellow Eugene H. Spafford will be given the rarely bestowed ACM President's Award at the ACM Annual Awards Banquet on June 9, in San Diego, for his enduring and impressive leadership in computer security, policy, professional responsibility, and the Internet. In a career that has included writing, research, teaching, and addressing Congress, Spafford has worked in software debugging, intrusion detection, digital crime forensics, firewalls, security management, and secure architectures. Among his accomplishments is the development of TripWire, the first free intrusion detection system distributed on the Internet. Spafford currently enjoys a joint professorship in Computer Science and Electrical and Computer Engineering at Purdue University, where he founded and currently serves as the executive director of the Purdue Center for Education Research and Research in Information Assurance and Security (CERIAS). Spafford also chairs the ACM US Public Policy Committee and has received honors including the 2006 Outstanding Contribution Award from ACM SIGSAC, the 2004 Making a Difference Award from the ACM SIGCAS, and the 2006 IEEE Computer Society Technical Achievement Award. In addition, Spafford has served as a member of the President's Information Technology Advisory Committee (PITAC) from 2003 through 2005 and senior advisor to the NSF's Assistant Director of the Computer Information Sciences and Engineering (CISE) Directorate, the Government Accountability Office, the US Air Force, the National Security Agency, the FBI and the Department of Energy.

Opposition to Electronic Voting System Grows in France
New York Times (04/03/07) P. A3

France's presidential election is less than three weeks away, but many are concerned about the reliability of e-voting machines, which will be used for the first time in a French presidential election. More than 80 municipalities plan to use the machines. Some fears have been spurred because a small portion of the machines to be used are manufactured by the company whose machines were at the center of the recent Florida congressional election controversy, where 18,000 votes allegedly went unrecorded. "The fear shown by numerous voters faced with a system they don't know runs the risk of keeping them away from the polls," said a Socialist party release, adding that the threats of fraud and "massive and undetectable errors" are quite realistic. The party also noted that machines made by Nedap, a Dutch company, had been "sharply disputed in countries in which they've been used." Nedap machines are scheduled for use in 80% of French municipalities. Ireland abandoned Nedap machines in 2004 and 2006, after their reliability came into question. The manufacturer has denied any factual basis for these claims, stating the machines meet French regulations. The Union for French Democracy candidate for president, F. Bayrou, has said the nation must "stop this evolution and suspend all use" of electronic voting, since its reliability cannot be ensured. However, the Constitutional Council, the country's highest constitutional body, said the machines "have been declared in conformity with the Constitution." France has used e-voting in regional and European elections since 2004 and has not experienced problems.

Congress Finally Considers Aggressive E-Voting Overhaul
Ars Technica (04/01/07), T. Lee

The Voter Confidence and Increased Accessibility Act is gaining support for its proposed reform of America's e-voting systems. Included in the bill is a ban of e-voting machines that do not have a paper trail; a requirement that prominently displayed notices remind voters to check the print-outs; a requirement for at least 3% of all votes to be audited to check for discrepancies between the paper and electronic records; a ban on voting machines that use wireless networking or connect to the Internet; and a requirement that machine source code be made publicly available. In hearings held by the House Administration Committee's Subcommittee, public interest groups and security experts expressed their approval of the bill. Some state officials complained that implementing the bill would be costly and difficult and would cause election results to be delayed. University of Maryland public policy professor D. Norris made the claim that paper-based voting systems are inherently flawed and that computerized machines are more secure. He cited a Las Vegas survey showing that only 40% of respondents checked the print-out of their votes. Troubles stemming from the use of paper trails in Georgia and North Carolina were also brought up. Some pointed out the toll the bill would take on states that had already implemented a rigorous e-voting measures. However, the bill states that auditing procedures other than those specifically mentioned would be allowed, so long as they are approved by the NIST. States would also have the option of abandoning e-voting altogether.

Don't Use WEP, Say German Security Researchers
IDG News Service (04/04/07) Sayer, Peter

German security researchers have found a way to crack Wired Equivalency Privacy that is much faster than previously discovered methods. They recommend that those relying on the protocol to protect sensitive information find a stronger means of protection. Earlier efforts showed that WEP could be cracked in a matter of minutes, although this method could be foiled by systems that change their security key every five minutes, but the new research carried out at Darmstadt University of Technology proves that it takes only 3 sec to obtain a 104-bit WEP key from intercepted data using a 1.7GHz Pentium M processor. The required data can be accessed in less than a minute, and the attack itself requires less computing power than previously thought, allowing it to be done in real time as a person walks through an office, potentially using a mobile device. Forty thousand packets captured means a 50% chance of a successful attack, and 85,000 packets mean a 95% chance, according to the researchers. WEP is still widely used for security in Germany, often without encryption. However, this type of attack can be detected by an intrusion detection system or by hiding the security key among numerous dummy keys.

That Face! Those Eyes! How Recognizable?
Government Computer News (04/03/07) Dizard III, Wilson P.

The National Institute of Standards and Technology (NIST) recently announced that facial recognition technology has improved by a factor of 10 in the past four years. The institute recently held tests called the Face Recognition Vendor Test (FRVT) 2006 and the Iris Challenge Evaluation (ICE) 2006, which compared the ability of vendor systems to recognize high-resolution still images, 3D facial images, and single iris images, in both controlled and uncontrolled lighting. Recognition performance was found to be the same for the still 3D facial images and single iris images. "In an experiment comparing human and algorithm [system]

performance, the best-performing face recognition algorithms were more accurate than humans," according to the institute. Error rates for facial recognition in a partially automated 1993 evaluation were found to be around 0.73% evaluation and were found to be around 0.01 in the fully automated FRVT 2006 evaluation. The time required for algorithms to process iris images ranged from 6 to 300 hours. The study tested performance under a variety of lighting conditions and took into account the resolution of different images used.

Professor Lectures at U. Massachusetts on Electronic Voting
Massachusetts Daily Collegian (04/06/07) Trull, Andrew

MIT electrical engineering and computer science professor Ron Rivest last week spoke to a University of Massachusetts audience about the challenges facing electronic voting. Voting system security can be split into two sectors, according to Rivest, ensuring that votes are "cast as intended" and that they are "counted as cast." The biggest challenge to the creation of a secure system is voter anonymity, since "privacy is the most important part of any voting system," but developing a system that runs on "hundreds of thousands of lines of programming" and ensuring that all votes are counted accurately without keeping any record of how specific people voted is extremely daunting, Rivest said. Although several solutions were brought up, Rivest suggested that paper will play a role in the next election, despite complaints by election officials that "all that paper" is too cumbersome. He said that voter verified paper audit trails are a way to make sure that votes are "cast as intended" but cannot ensure that they are "counted as cast." A system known as "mix nets" offers a way to make sure that votes are counted as cast and that voters retain their anonymity throughout the process. Mix nets would encrypt randomly re-assorted votes while going through several proxy servers. Each voter would receive a copy of the encryption and be able to consult a public bulletin to check that their vote was counted correctly without revealing who they voted for. Rivest also stressed the importance of human poll workers and the need for national standards.

How to Read Signs of Safe Software
Government Computer News (04/02/07) Vol. 26, No. 7, Buxbaum, Peter A.

The development of metrics for software assurance is still in its infancy, according to speakers at the DHS-DOD Software Assurance Forum in Fairfax. T. Sager, chief of the vulnerability analysis and operations group at the National Security Agency, said being able to pick the 10 best software security solutions out of a field of thousands requires some sense of measurement, an ability to determine which solutions are the best. Microsoft has been developing metrics to reduce the level of vulnerabilities in its software, including internal measurements for the assurance of the software it ships, according to senior director of security engineering strategy S. Lipner. He said the metrics are aimed at improving future product versions, and Microsoft wants to assess products before they are shipped. Microsoft has developed two software assurance metrics. The first, known as Relative Attack Surface Quotient, measures such things as default configurations, open ports, permissions services, and the number of ActiveX controls available by default, Lipner explained. The second metric is informally known as the "vulnerability coverage method," and basically functions like an independent community of researches reporting vulnerabilities in new versions of Microsoft products. Reported vulnerabilities are analyzed by a team at Microsoft, who then determine if the vulnerability has been removed from updated versions of the product; if the vulnerability has not, the team decides if it should be removed.