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

Δελτίο 111
2 Απρίλη 2008

Technology Policy in the Information Age: Computer Security Experts Debate Political, Social and Economic Impacts, AScribe Newswire (03/24/08)

ACM is sponsoring the Conference on Computers, Freedom, and Privacy (CFP 2008) as a way to help shape the public debate on information and communications technologies. CFP 2008 will offer expert keynote speakers, panels, tutorials, and birds-of-a-feather sessions to help raise the level of discussion on how the country should approach technology in the years to come. The conference will feature leading technologists, policymakers, business leaders, and advocates who are experts on voting technology, online campaigning, social networks, anonymity online, P2P networks, cybercrime and cyberterrorism, information policy and free trade, media and concentration, network neutrality, electronic medical records, and copyright and fair use.

Americans Still Wary of Voting Machines for 2008
Agence France Presse (03/23/08)

Despite the growing use of computers in elections in the United States, many jurisdictions are reconsidering their voting technology amid growing concerns that the systems are vulnerable to software and hardware glitches, manipulation by hackers, and a variety of other problems. Five states that had revamped their voting systems after 2000 are undertaking a second overhaul because of their discontent over electronic machines, according to the Pew Center on the States. About 80% of the votes cast in the US include the use of computers, and about 38% use direct recording electronic (DRE) voting machines, reveals a study by the University of Iowa's J. McCormally. Many DRE machines do not leave a paper trail, which makes recounts or audits impossible. Computer scientist A. Dechert, who heads the Open Voting Consortium, says paperless touch-screen voting systems have failed in numerous cases. Verified Voting Foundation project director W. Stewart says the growing doubts over the reliability of paperless systems could be problematic during the 2008 presidential election. Stewart says it is highly probable that the election could come down to one state where a situation cannot be resolved because of an inability to recount electronic vote tallies. He says the most reliable systems are optical-scan devices in which voters mark their choice on paper ballots that are then read and tallied by computerized scanners.

Professor: Computers Plus People Equals Risk
IDG News Service (03/27/08), J. Kirk

London School of Economics professor of information systems I. Angell says companies are relying too much on technology to run their business, a dangerous practice given technology's inability to account for unpredictable situations. Angell says the problem is that business information systems make assumptions that do not necessarily match up with real-world events. Those assumptions are then used to make decisions, which leads to false conclusions. "When companies use the tools of technology to solve a problem, they may or may not succeed, but what is certain is that completely unexpected phenomena happen," Angell says. The conclusions made by computers are only as good as the numbers people put into them,

which can often be altered or misleading, he says. People now automatically believe whatever they see on the screen, which Angell calls a "glass cockpit effect." He believes that digital security needs to be redefined, and notes that the marginal events that lead to larger security problems are only noticed in hindsight.

NIST Unveils Tool to Foil Attacks via DNS
Government Computer News (03/25/08), D. Campbell

National Institute of Standards and Technology (NIST) network researchers S. Rose and A. Nakassis have written a paper that introduced a method federal systems administrators can use to protect their systems from the attacks launched over the Domain Name System (DNS). Rose and Nakassis say that DNS security extensions (DNSSEC) that are originally meant to protect DNS zone data contain an unintentional side effect that enables an attack precursor known as "zone enumeration." Although zone enumeration is possible without DNSSEC, the traditional methods of enabling zone enumeration are often impractical because they use time-consuming or processor-intensive brute force techniques that are often repelled by intrusion detection systems. Rose and Nakassis also note that there are several techniques that allow networks to realize the intended authentication and integrity benefits of DNSSEC while simultaneously "reducing DNS information leakage." Such techniques are important because the need to protect network operations with methods offered by DNSSEC will only increase as DNS becomes more and more important. In addition, the techniques could improve DNSSEC authentication and integrity protection, which would in turn protect DNS zones and stop attempts to compromise data.

UW Team Researches a Future Filled With RFID Chips
Seattle Times (03/31/08), K. Heim

Many experts believe that RFID tags will soon be ubiquitous, and will be used to monitor objects and people remotely. Leaders of the University of Washington's RFID Ecosystem project want to understand the implications of that shift before it takes place, and are conducting one of the largest experiments using wireless tags in a social setting. For more than a year, a dozen researchers have carried RFID tags around the computer science building, which is equipped with about 200 antennas that pick up any tag near them every second. The RFID tags are less intrusive than a camera, but more precise, and subjects frequently forget they are carrying them. The researchers have developed applications that allow people to use data from RFID tags to inform their social network where they are and what they are doing, and the project's Personal Digital Diary application detects and logs a person's activities each day and uploads them to a personal calendar so people can see what they did that day. "What we want to understand," says computer science professor G. Borriello, "is what makes it useful, what makes it threatening, and how to balance the two." However, there are some disadvantages to being tracked. Borriello says some systems, including US passports and driver's licenses, have been designed to divulge more information than necessary, which could lead to significant security and privacy issues.

Mashup Security
Technology Review (03/31/08), E. Naone

As a growing number of tools are developed to help people create their own online mashups, experts are examining how to eliminate mashup security risks. OpenAjax Alliance cofounder D. Boloker says that as mashups become more complex they start incorporating computer

code from multiple sources, which may include insecure code that could jeopardize a company's or user's systems. Web browsers were not designed with mashups in mind, Boloker says. Browsers contain a security feature called the same-origin policy that is intended to keep malicious code hosted on one site from obtaining information from another site. However, same-origin security forces Web applications to either sacrifice security or functionality, says Microsoft Research's H. Wang. Wang says that when a Web site creator embeds code written by a third party the same-origin policy no longer offers any protection. She has been working on solutions that provide a way for browsers to recognize code that comes from a third party and to treat that code differently. One solution is to enclose third-party code in a "sandbox" tag, which would allow the Web site to use the code but treat it as unauthorized content, with no authority outside the sandbox. IBM recently released a security tool called SMash that allows content from multiple sources to be displayed on a single page, and allows them to communicate safely. A secure communication channel monitors information sent between tools while maintaining their separate identities and sets of permissions.

IBM Project Seeks Privacy Controls for Users
IDG News Service (03/28/08), J. Fontana

The European Union is funding PrimeLife, a three-year IBM research project to develop technology that will ensure users can protect their privacy online throughout their lifetimes. IBM's Zurich Research Lab is working with 14 other partners from various countries, including Brown University on PrimeLife, which is short for Privacy and Identity Management in Europe for Life. IBM says it wants to create a toolbox that will act as an electronic data manager that gives users an overview of what personal data is used, when, and for what purposes. Users would be able to create privacy settings and preferences for applications, and would receive prompts when an application tries to obtain or use data for other purposes. "PrimeLife will interact with the open-source community, standardization bodies, as well as other projects so that they can pick up our technology," says J. Camenisch, PrimeLife project leader and research staff member for cryptography at IBM's Zurich Labs. Camenisch says that current standards and protocols have very limited or nonexistent privacy settings, and the goal of PrimeLife will be to integrate the project's privacy-enhancing technology with existing standards and protocols such as the Security Assertion Markup Language. The first goal of the project is to provide scalable and configurable privacy and identity management that integrates with emerging Internet services and applications.

Researchers Secure the Browser
eWeek (03/24/08) Vol. 25, No. 10, P. 16; R. Naraine

Researchers at the University of Illinois at Urbana-Champaign are constructing Opus Palladianum (OP), a new Web browser designed to prevent hacker attacks by partitioning the browser into smaller subsystems and using simple and explicit communication between subsystems. "[The Web] has become a platform for hosting all kinds of important data and businesses, but unfortunately, [existing] browsers haven't evolved to deal with this change and that's why we have a big malware problem," says University of Illinois professor S. King, who conceived of OP. King says three unique security features will be employed to demonstrate the browser architecture design's utility. Those components include flexible security policies that accommodate the use of external plug-ins without making third-party developers responsible for security; formal techniques to show that the address bar displayed within the browser user interface always displays the proper address for the current Web page; and a browser-level information-flow tracking system that allows browser-based attacks to be dissected

postmortem. OP is currently comprised of five main subsystems--the Web page subsystem, a network component, a storage component, a user-interface component, and a browser kernel--which all run within separate OS-level processes, King says. Communication between each subsystem and between processes, and interactions with the underlying operating system, are handled by the browser kernel. "The browser kernel implements message passing using OS-level pipes, and it maintains a mapping between subsystems and pipes," King says. He says the long-term goal is to devise a cross-platform Webkit version that will be distributed to the open-source community.