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

Δελτίο 16
24 Μάρτη 2006

CFP 2006 Explores Computer Freedom and Privacy Issues
Association for Computing Machinery (03/17/06)

Amid debates over government surveillance of citizens, the amassing of personal information databases, and Internet censorship, ACM's Computers, Freedom and Privacy 2006 conference will explore the technologies at the epicenter of these issues. The CFP 2006 conference, titled "Life, Liberty and Digital Rights," will be held May 2-6, at the L'Enfant Plaza Hotel in Washington. Panels, discussions, workshops, technical demonstrations and keynote speakers will tackle many information technology security and privacy issues culled from today's headlines. Participants include internationally acclaimed experts on electronic voting, government surveillance, Internet governance, digital rights management, adware and spyware, and federal privacy laws, among others. The conference also features tutorials, plenary and concurrent sessions, and provocative Birds-of-a-Feather sessions. Highlights of the conference include the Big Brother Awards and the EFF's Pioneer Awards, which recognize milestones as well as dubious distinctions in the online world.

Internet Panel Mulls Defenses Against New, Potent Attacks
Associated Press (03/16/06), T. Bridis

A new form of cyberattack being dubbed by some as "distributed reflector denial of service" that focuses on the computers that help direct Internet traffic worldwide will be a focus of ICANN's security committee at its upcoming meeting in New Zealand. The attacks, though similar in nature to typical denial of service ones, are far more potent, requiring fewer hacked computers to launch and much simpler to amplify. Researchers have detected around 1,500 such attacks first launched late last year that briefly shuttered commercial Web sites, large ISPs, and leading Internet infrastructure firms. VeriSign chief security officer K. Silva said that attacks earlier this year used just 6 percent of the Internet's more than a million name servers to flood networks but that the attacks in some instances outpaced 8 gigabits per second, a mega-assault by typical standards. ICANN security committee head S. Crocker says, "It's like they built a better bomb by having it enriched." Columbia University Internet researcher S. Bellovin says, "A lot of this stuff will take a while to clean up." Possible fixes to vulnerabilities include filters that block out forged data traffic and new limits on specialized name server computers.

Google Prevails in Copyright Fight
Wall Street Journal (03/17/06) P. B4; K. Delaney

A lawsuit accusing Google of copyright infringement, defamation, and other instances of wrongful conduct was dismissed by federal Judge R. Barclay Surrick on March 10. Internet publisher G.R. Parker filed the lawsuit in US District Court in Philadelphia, alleging that Google's archiving of copyright material Parker posted on the Usenet community of electronic bulletin boards constituted a breach of copyright, and that its inclusion of excerpts from his site in its search results was an act of copyright infringement. Surrick maintained in his ruling that those activities, along with Google's caching of Web pages, was not infringement, and he

cited a January decision in Nevada District Court supporting Google's practice of making copies of cached Web pages accessible to users via its search results. Thelen Reid & Priest attorney W. Patry noted that the Parker decision dismissed the claims of copyright infringement without raising the issue of "fair use." However, some legal experts said Parker's ruling did not establish binding precedent by definition, and they did not concur on whether his decision demonstrates any trend in judicial analysis, when weighed against other recent court opinions in lawsuits filed against Google. Last month, a Los Angeles federal judge concluded that Google's image-search service probably infringed on the copyrights of the Perfect 10 adult-entertainment company by displaying thumbnails of its images, but he dismissed Google's liability when users clicked on the images and gained access to third-party sites showing pictures purloined from Perfect 10. Google litigation counsel M. Kwun declared that Surrick's decision establishes the consistency between Google's service and copyright law principles, but Parker, who plans to appeal the ruling, claimed that Google's "entire business model is based on freeloading on other people's content."

Let Me Hear Your Body Talk: UH Scientists Mine Biomedical Data
University of Houston News (03/15/06)

A team of five researchers from the University of Houston is attempting to train computers to obtain health information from their users in an NSF-funded study. Through computer-powered non-invasive imaging applications, the researchers are studying brain activity, human learning, and cognitive impairment, as well as facial-expression analysis and biometric security. "The project will involve a hybrid software system designed to acquire, analyze, integrate, securely store, and visualize large volumes of data obtained from a human subject in real time," said G. Zouridakis, associate professor of computer science and project leader. Zouridakis and his team are building on existing information technology practices to develop software tools for practical application in biomedicine. Each of the five researchers has a different area of specialization and works in a different lab. The grant is designed to bring their diverse perspectives together, such as Zouridakis' work with dense-array scanners to analyze the electrical, magnetic, and infrared features of brain activity and computer science professor M. Garbey's work in high-performance computing and computational life sciences. Associate professor I. Kakadiaris is the founder and director of the Computational Biomedicine Lab, home to pioneering research in cardiovascular informatics and multispectral biometrics. Associate professor I. Pavlidis directs the Computational Physiology Lab, and has developed a computer system to conduct touchless physiological monitoring. Assistant professor R. Vilalta's research has focused on massive data analysis in the hopes of extracting meaningful patterns. The researchers will collect data from test subjects with sophisticated sensing systems such as thermal cameras, multimodality brain activity scanners, and 3D geometry video cameras.

Researchers: Impact of Censorship Significant on Google, Other Search Engine Results
Network World (03/15/06)

Country-specific search engines that have free-speech restrictions often produce different results for searches, according to researchers from Indiana University. F. Menczer, associate professor of informatics and computer science, and M. Meiss, a computer science doctoral student, are behind the CenSEARCHip project, which comes at a time when Google, Yahoo!, and MSN are developing different versions of their search engines for specific countries. Menczer and Meiss have set up a Web site that details the differences in the query results generated by such search engines, and provides side-by-side query results. Meiss says conduct-

ing a search on political topics such as human rights and democracy will lead to different result in queries. Although the US search site would provide text references and images of the Chinese government crackdown on protestors, in response to a query on Tiananmen Square, the Chinese site would deliver results primarily for hotel and tourist information. "We wanted to explore the results returned by major search engines and in doing so to foster an informed debate on the impact of search censorship on information access throughout the world," says Menczer.

Calit2 Researchers Deploy Disaster Communications Network at San Diego Mardi Gras Festivities, UCSD News (03/13/06), M. Curran, D. Ramsey

Researchers from the California Institute for Telecommunications and Information Technology (Calit2) teamed up with San Diego law enforcement to create a wireless mesh network, stringing together wireless boxes, cameras, laptops, cell phones, and a satellite dish to provide real-time information to first responders during Mardi Gras festivities. The tests of the network during Mardi Gras proved that it could be used to disseminate video feeds and other information during an emergency or disaster. "This was the real world converging with research, prototyping, developing, and improving tools," said Calit2 UCSD director R. Rao, a professor of electrical and computer engineering in the Jacobs School of Engineering. To simulate disaster conditions, the researchers acted as if the communication network in a 24-block area of downtown San Diego was already down when setting up the network. Each camera installed contained a networking box to link back to the police command center, and police can monitor the video feeds on their cell phones. The small screen made it difficult to see in great detail, but the camera feeds to the police command posts were of high quality. Police also tested a wireless system for tracking the locations of fellow officers and equipment. While inclement weather forced the researchers to outfit the equipment with hastily assembled rain gear, the system met their expectations and all the devices functioned satisfactorily.

Association for Computing Machinery Honors Pioneers of Verification Tools for Safe, Secure Software
AScribe Newswire (03/16/06)

ACM has named Robert S. Boyer, J Strother Moore, and Matt Kaufmann, all of the University of Texas at Austin, the winners of its Software Systems Award. Boyer, Moore, and Kaufman are the developers of the Boyer-Moore Theorem Prover, a formal tool that computer scientists have used to verify the safety and security of critical hardware and software. Such a tool is helpful when dealing with applications such as embedded medical devices, spacecraft and aircraft controls, and autonomous vehicles such as self-driving cars. The award, which carries a $10,000 prize, was created to honor institutions and individuals who have developed software systems that have been influential over the years in their concepts and commercial acceptance. According to the award citation, the latest version of the tool, ACL2, is "the only simulation/verification system that provides a standard modeling language and industrial strength model simulation in a unified framework." Boyer is a professor in the Computer Sciences, Mathematics, and Philosophy Departments; Moore holds the Admiral B. Inman Centennial Chair in Computing Theory; and Kaufmann is a senior research scientist. They will be honored at the annual ACM Awards Banquet on May 20, 2006, in San Francisco.

RFID World Still Reacting Strongly to Virus Research
TechWeb (03/16/06) Sullivan, Laurie

Some radio frequency identification (RFID) technology experts are taking issue with a paper presented at the IEEE conference in Pisa, Italy, that suggested RFID could spread computer viruses. A third-year PhD student from Vrije Universiteti in Amsterdam, Melanie Rieback, created an artificial virus for her paper, "Is Your Cat Infected With a Computer Virus?" that suggested RFID tags have the potential to spread viruses through readers into poorly written middleware applications and into enterprise backend systems and databases. K. Ashton, vice president of ThinkMagic and co-founder of the Massachusetts Institute of Technology Auto-ID Center, says Rieback actually demonstrates a self-replicating piece of SQL code, and not a virus, in the paper. RFID tags store numbers, and are very unlikely to accept executable code via a virus. "The student researchers think a database picks up the information from a tag and puts it in the buffer, and that's not what happens," adds Gartner vice president of research J. Woods. However, Woods says in theory the arguments for buffer overflow, and software vulnerabilities could compromise RFID systems. Moreover, some RFID experts say the industry should do a better job of testing applications, while others say companies that deploy the technology should make sure they secure the technology.

Judge Grants Google a Reprieve
Wall Street Journal (03/20/06) P. B4

US District Judge J. Ware ordered Google on Friday to provide 50,000 randomly selected address for Web sites from its databases. However, the judge also ruled that Google does not have to hand over information regarding consumer Web-search queries to the Justice Department. Judge Ware felt that if Google handed over the queries to the Justice Department that they would lose the trust of some of their users. "This is a clear victory for our users," said Google in a statement. The Justice Department wanted to use the information from Google to defend the Child Online Protection Act. "The next time the government comes calling, it will pile so much more on its side of the scale, a better explanation of its need and a more compelling set of facts that the court will have no choice but to compel Google to turn over search queries," says Paul Ohm, an associate professor at the University of Colorado School of Law. Some experts agree that government requests may actually be granted in the future.

DOD Seeks Army of Cyborg Bugs
Computerworld (03/15/06) Songini, Marc L.

DARPA's Hybrid Insect Micro-Electrical-Mechanical Systems (HI-MEMS) program is calling for proposals to develop insect cyborg-scouts that can be controlled remotely. The insects would carry sensors and a wireless transmitter enabling them to relay information about conditions in locations inaccessible to human soldiers. DARPA wants to develop an insect capable of being directed to within five meters of a target at a 100-meter range with an electric remote control or a GPS application. DARPA has yet to determine the technical specifications of the insect scouts, though it has suggested that they could serve as "micro unmanned air vehicles" to access areas too remote or dangerous for humans, such as enemy buildings or caves. Previous attempts to use insects to gather intelligence have been limited by unreliable performance, which the HI-MEMS project seeks to correct with a dependable control interface. DARPA says the body of an insect, as it passes through its metamorphic stages, would renew itself around foreign objects, such as a gas sensor, a video camera, and a microphone. "Inserting MEMS devices during such stages could enable assembly-line like fabrication of hybrid insect-MEMS interfaces, providing a considerable cost advantage," according

to a DARPA report. DARPA is also interested in swimming devices, provided that the insect can stay still until it is directed to move by its handler. Powering the device and controlling the locomotion are among the project's central challenges.

Enigma Project Cracks Second Code
BBC News (03/15/06)

Thousands of online codebreakers continue to use distributed computing power to decrypt three German codes that Allied forces were unable to crack during World War II. Participants in the M4 Project, named after the M4 Enigma machine Germany used to encode its messages, have one remaining code to crack. The remaining code is actually the first message the online codebreakers attempted to crack, and all combinations available on German army and three-ring Enigma machines have been tried. However, they did not try combinations associated with the sophisticated four-ring Enigma used to encode the messages. The online codebreakers recently cracked a message that provided information about the aftermath of a battle with an Allied vessel, and it followed the first breakthrough on Feb. 20, 2006, involving a code that proved to be a confirmation of a message from the commander of a German U-boat. War experts at Bletchley Park were unable to crack the messages sent in 1942 because Germany used a new code book and a different version of the Enigma machine. Amateur historian R. Erskine discovered the codes and passed them on to a cryptography journal in 1995 as an exercise for codebreakers.