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

Δελτίο 112
12 Απρίλη 2008

ACM Committee on Women Honors Worldwide Leader in Cryptography Research
AScribe Newswire (04/01/08)

ACM's Committee on Women in Computing (ACM-W) has named Shafi Goldwasser the winner of the 2008-2009 Athena Lecturer Award. Goldwasser is known for her outstanding research in cryptography, complexity theory, and number theory. For example, Goldwasser teamed up with S. Micali and C. Rackoff for research on interactive and zero-knowledge proofs that have helped provide the foundation for the secure transmission of information over the Internet. Her work with U. Feige, L. Lovasz, S. Safra and M. Szegedi in the area of complexity theory led the way to the modern approach for showing the difficulty of approximating the solution of NP-complete problems. Goldwasser is the RSA Professor of Electrical Engineering and Computer Science at MIT, and she also is a professor of computer science and applied mathematics at Weizmann Institute of Science in Israel. Goldwasser is scheduled to address the ACM Symposium on Theory of Computing, sponsored by the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT), in Washington DC, in May 2009. ACM will honor Goldwasser with the award, which includes a $10,000 honorarium provided by Google, at the ACM Annual Awards Banquet on June 21, in San Francisco.

Centers Tap Into Personal Databases
Washington Post (04/02/08) P. A1; R. O'Harrow

Fusion intelligence centers created by states following the 9/11 terrorist attacks have access to personal information on millions of Americans, and one even has access to top-secret data systems at the CIA, according to a document obtained by the Washington Post. The centers were established to identify potential threats and improve how information is shared. The centers use law enforcement analysts and computer systems to collect and combine otherwise separate pieces of information. A document that lists resources used by fusion centers shows how a dozen of the centers in the northeast United States have more access to commercial and government databases than previously disclosed. The centers use a variety of data resources and software programs that find patterns and display connections between people. Most of the centers subscribe to Web-based information brokers that deliver instant access to billions of records on individuals' homes, cars, phone numbers, and other information. Some of the fusion centers draw from records of currency transactions and almost 5 million suspicious-activity reports filed by financial institutions with the Treasury Department's Financial Crimes Enforcement Network. "Fusion centers have grown, really, off the radar screen of public accountability," says the Center for Democracy and Technology's J. Dempsey. "Congress and the state legislatures need to get a handle over what is going on at all these fusion centers."

Voters Trust Touch-Screen Machines, Studies Show
IDG News Service (03/26/08), R. Weiss; G. Gross

American voters are becoming more comfortable with electronic-voting methods, reveals two new studies. A study by the Brookings Institution found that voters are generally more

comfortable with some models of touch-screen machines than with paper ballots that use buttons and dials. Another study, "Trends in American Trust in Voting Technology," by InfoSentry Services, found that public trust in direct recording electronic (DRE) machines is about the same as in 2004. Two-thirds of the 1,000 respondents to the telephone survey said they trust DREs, while 68% trusted DREs in 2004. The Brookings researchers tested five DRE systems and found that the error rate of the worst-performing machines could reach 3% during a presidential race, and in more complex races the voting error rate was even higher. University of Maryland professor P. Herrnson, lead author of the Brookings study, notes that a 3% error rate is enough to change the outcome of an election. Voters generally approved of verification systems such as printouts that come with some DRE machines, even though the verification systems did not significantly improve the error rate, and often caused confusion, prompting voters to seek help from poll workers. University of Rochester professor and study co-author R. Niemi says he expected voters who participated in the study to favor paper ballots because they are more familiar with those systems, but people generally gave DRE machines higher marks because of ease of use and confidence that their votes would be recorded as cast.

Cybercrime Is in a State of Flux
Guardian Unlimited (UK) (03/27/08), G. Knight

Cybercriminals are increasingly using a technique known as fast flux to hide the location of phishing sites, spamming sites, botnets, and illegal malware. Fast flux enables a machine on a botnet to frequently change the DNS records of a phishing or spamming site. When the DNS records of a phishing or spamming site are changed, the machine on which the site is hosted also changes. As a result, shutting down the phishing or spamming site requires shutting down every single machine on the botnet, since each of these machines hosts the same site. In addition, the constant changing of the DNS records means that the botnet's Command & Control server cannot be found. The use of this technique is a growing problem, says R. Mc Ardle at TrendLabs EMEA. "Normally the DNS servers will be hosted on networks that are infamous for being difficult to shut down, such as the networks offered by the Russian Business Network," he says. "In the past we had only one malicious Web server to clean up before the threat would be neutralized, now we need to shut down thousands--most of which are home PCs." Several organizations have proposed solutions to help solve this problem. For instance, the Anti-Phishing Working Group has proposed introducing a policy that would shut down a site across the Internet, instead of simply shutting it down on an Internet service provider's servers. Meanwhile, ICANN has proposed that registrars uniformly authenticate any requests for configuration changes to name servers and establish a minimum "time-to-live" threshold for a name server record.

Canadian Voting Machine Enters American Political Machine
InterGovWorld.com (03/27/08), R. Lombardi

The University of Ottawa's Scantegrity, originally a proof of concept called Punchscan, is an open-source program designed to provide end-to-end verifiable voter results, says PhD student A. Essex. "Scantegrity gives voters a privacy-preserving receipt," says Essex. "It does not show other people how you voted, but it does allow you to have a way to check to ensure your vote gets counted." The concept is similar to the confirmation numbers issued by hotels, Essex says, which allow hotel customers to look up their confirmation number, but it does not display the room number. Scantegrity also features software independence, which means if a software error is made, the mistake can not go through the process undetected, Essex

says. The software also contains a tool that performs a cryptographic self-audit to verify computations. The development team plans to invite the Ottawa Linux users group to review the system to help make it more secure. It is unlikely the technology will ever be used in Canada, which still uses paper and pencil ballots and has such strict regulations that even the type of pencil is regulated, but it could find a home in the United States. Scantegrity team leader D. Chaum says two American municipalities have expressed interest in using the program, and Essex says it has been presented to several American organizations in an effort to attract research funding. "The question now is whether our technology will be certifiable," Essex says. "A group of election experts and scientists is saying a window should be allowed to give new voting technologies a chance, and there's legislation pending to allow that."

European Union, NATO to Tackle Cyber-crime
Associated Press (03/31/08)

Cybersecurity experts are meeting in Paris this week to discuss how governments should counter and prevent cybercrimes designed to cripple the Internet and cause data loss, theft, and fraud. G. deKerchove, who coordinates anti-terror efforts for the European Union's 27 countries, says an attack that shuts down the Internet could significantly amplify a terror attack. Participants at the meeting also will discuss new guidelines for cooperation between police and investigators and Internet service providers. At the meeting the Council of Europe will review the implementation of the Convention of Cybercrime, the only legally binding international treaty to address online crime such as hacking and Internet fraud. University of Cologne computer law lecturer M. Gercke says the challenges posed by cybercrime are different from conventional terror attacks because computers exchange data so quickly across international boarders. "Compared to regular terror attacks, it is much easier for the offenders to hide their identity," Gercke says. "There are at least 10 unique challenges that make it very difficult to fight computer-related crime." At a separate meeting in Romania, a NATO summit debated its guidelines for coordinating national cyber defense efforts.

US Reveals Plans to Hit Back at Cyber Threats
ZDNet (04/02/08)

The US Air Force Cyber Command (AFCYBER) is just as focused on being able to attack through the Internet as it is on defending US cyber infrastructure. A senior US general says AFCYBER is developing capabilities to inflict denial of service, confidential data loss, data manipulation, and system integrity loss on its enemies. These cyberattacks could be combined with physical attacks. US Eighth Air Force Lieutenant general R. Elder says offensive cyberattacks in network warfare make kinetic attacks more effective. "Cyber gives us a huge advantage but adversaries look at our capabilities and see areas they can undermine," he says. "We need to protect our asymmetric advantage--on the one hand by having people further exploit cyber, and on the other by having mission assurance." The problem is made more important by the military's reliance on the public Internet. The US military infrastructure runs through the public Internet system to both launch and defend against attacks, and military networks such as the Global Information Grid are linked to US government and critical national infrastructure systems, which are linked to the public Internet. Adversary systems are subverted through public channels by the US military, but it also leaves the military open to attack through the same channels, Elder says. Other concerns for the military include the possibility of supply-chain vulnerabilities, where holes are introduced into chipsets during manufacturing that an adversary could later exploit, as well as within electronics. Elder says AFC-

YBER also needs to develop the ability to quickly pinpoint where an attack is coming from and be able to retaliate, and to deter potential attackers.

Security Pros Launch Open-Source CERT
eWeek (04/03/08), R. Naraine

With backing from Google, security consulting firm Inverse Path, and the Open Source Lab at Oregon State University, a group of computer security professionals created the Open Source Computer Emergency Response Team (oCERT), a new organization designed to be the go-to place for security incident response when an open-source project has been affected. OCERT will include T. Ormandy and W. Drewry from the Google Security Team, A. Barisani and R. Holland from Inverse Path, and M. Holtmann from Intel. In addition, active open-source distributions or projects with a good record of being responsive to dealing with security-related problems will be asked to join and actively participate in the oCERT effort. The team and its backers will work to manage advance vulnerability warnings, coordinate the patch release notification process, and punish vendors that delay offering security fixes. In addition, oCERT will provide security vulnerability mediation for the security community, and maintain reliable security contacts between registered projects and vulnerability researchers that need to get in touch with a certain project about infrastructure security issues. Barisani says oCERT hopes to reduce the impact of a security incident on smaller projects that have some or no infrastructure security.

US Moots System for Data Sharing on Cyber Threats
Financial Times (04/09/08) P. 2; K. Allison

Department of Homeland Security secretary M. Chertoff yesterday outlined plans for a "Manhattan project" for cybersecurity that would increase the sharing of information on potential threats between government and industry. US authorities already share some threat information with a few companies, but there is no centralized system for sharing information about online security threats. Chertoff says closer coordination between government and industry is essential because a successful large-scale attack online would have a widescale impact on the country and the world. "The federal government does not own the Internet ... and it does not own the nation's cyber networks," Chertoff says. "We can't be serious about national security or national cybersecurity without engaging private industry." Chertoff says the government is working to develop capabilities to detect cyber attacks before they damage computer systems and that information will be shared with IT groups, financial services companies, and utilities to help them protect their networks, he says. Chertoff says the cybersecurity project is not a stepping stone to government control over the Internet. "We have no interest or intention of duplicating a system where the government tries to sit over the Internet and prevent things coming in they don't like," he says.

Vote Device May Get Push
Milwaukee Journal Sentinel (04/07/08), A. Johnson

Wisconsin is considering forgoing federal certification of a new vote-counting device and may test the device itself in an effort to simplify and quicken the tallying of votes in November, says K. Kennedy, director of the state's Government Accountability Board. The device, the Hybrid Accumulator Activator Transmitter (HAAT), consolidates totals from electronic touch-screen voting machines and optical scanners, creating a single tally, which local election officials say could significantly speed voter returns on election night. Kennedy's com-

ments are in response to concerns from local officials that advances in technology and regulations intended to ensure the integrity of elections are actually slowing tallies at a time when voters expect near instantaneous results. D. Chapin, who directs the Pew Center for the States' electionline.org, says that such conflicts are a constant undercurrent across the country, and the slower results are because districts are both learning new equipment and making sure the results are correct. "With each new technology or rule, we see the value in terms of the integrity of the election," says Milwaukee Election Commission deputy director N. Albrecht. "But it almost always requires additional resources and time." Kennedy says that because Wisconsin's requirement for federal testing is a rule, and not a law, it may be easier to amend than in other states. Chapin says Wisconsin's decision will be watch closely across the country as many states tire of the slow pace of federal testing.