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

Δελτίο 108
6 Μάρτη 2008

STOP Terrorism Software
University of Maryland (02/25/08), L. Tune

Researchers at the University of Maryland Institute for Advanced Computer Studies (UMIACS) have developed the SOMA Terror Organization Portal (STOP), which enables analysts to query automatically learned rules on terrorist organization behavior, predict potential behavior based on these rules, and to network with other analysts examining the same material. Stochastic Opponent Modeling Agents (SOMA) is a formal, logical-statistical reasoning framework that uses data on the past behavior of terror groups in order to learn rules about the probable actions of an organization, community, or person in different situations. SOMA has generated tens of thousands of rules about the likely behavior of about 30 groups, including major terrorist organizations. "SOMA is a significant joint computer science and social science achievement that will facilitate learning about and forecasting terrorist group behavior based on rigorous mathematical and computational models," says computer science professor and UMIACS director V. Subrahmanian. "In addition to accurate behavioral models and forecasting algorithms, the SOMA Terror Organization Portal acts as a virtual roundtable that terrorism experts can gather around and form a rich community that transcends artificial boundaries." Four defense agencies use STOP, funded by the Air Force Office of Scientific Research, to perform queries and run a prediction engine, mark rules as useful or not useful, and leave comments about the rules.

The E-Voting Paradox
Government Computer News (02/25/08), W. Jackson

Computer scientists and researchers are extremely concerned over the accuracy and security of electronic voting machines, but voters are more concerned over usability, says University of Maryland professor P. Herrnson, director of the Center for American Politics and Citizenship. In his new book, "Voting Technology: The Not-so-Simple Act of Casting a Ballot," Herrnson says that field tests of different types of equipment and ballots found that usability was a more pressing concern to voters than security. He says the type of ballot used and other factors, such as squishy membrane keyboards or screen glare, are a major concern for voters. Since the Help America Vote Act was passed there has been a reduction in the residual vote, or the number of votes not cast for certain races during an election, but Herrnson says that is not necessarily a good measure of errors. People are more likely to vote for the wrong candidate by mistake than to intentionally skip a race or forget to vote, he says. M. Shamos, who runs the eBusiness Technologies program at Carnegie Mellon University's School of Computer Science and has been certifying voting systems for 27 years, calls the election voting system "the least reliable product in the US" He says the process suffers from a lack of standards, inadequate election worker training, and proprietary software. "There should be no trade secrets in voting technology," Shamos says.

Put Trust in Your Pocket: CSIRO's Trust Extension Device
CSIRO (02/19/08), J. Finlay

The Trust Extension Device (TED), a prototype portable device developed by Australia's Commonwealth Scientific and Industrial Research Organization (CSIRO), solves the problem of having trust restricted to specific, well-known computing environments. TED creates its own environment on an untrusted computer and establishes trust with a remote enterprise server before running an application. The user and the enterprise that issues a portable device containing a small operating system, a set of applications, and encrypted data must establish that they are trustworthy by proving their identities and that the computing environments are as expected, before TED accesses the remote server and a transaction takes place. "TED makes that trust portable, opening the way for secure transactions to be undertaken anywhere, even in an Internet cafe," says J. Zic of the CSIRO ICT Center. "Wherever you go, whichever machine you run on, you and the issuer can be confident both parties are known to each other, cannot engage in any malicious acts, and that the transactions are trusted." Banks could use the technology to provide authorized customers and employees with access to financial data, or to conduct financial transactions over the Internet.

Sniffing Out Insider Threats
EurekAlert (02/19/08), A. Ang

Researchers at the Air Force Institute of Technology at Wright Patterson Air Force Base are developing technology that could help find insider threats by analyzing email activity, helping identify malicious individuals hidden within groups of tens of thousands of employees. The technology uses data-mining techniques to search email and build a picture of social network interactions. The technology could be used to prevent security breaches, sabotage, and even terrorist activity that otherwise could have damaging results, says researcher G. Peterson. The same technology can also find individuals who feel alienated within an organization or identify any worrying changes in an individual's social behavior. Peterson says security efforts have tended to focus on external electronic threats, and points out that insiders pose the greatest threat to an organization. Peterson's defense against insider threats is based on an extended version of Probabilistic Latent Semantic Indexing, which can discern employees' interests from email and create a social network graph showing their various interactions. The research is reported in the International Journal of Security and Networks.

House Lawmakers Question Privacy in Cyber-Security Plan
Washington Post (02/29/08) P. D3; B. Krebs

The Bush administration's "cyber initiative" was the subject of a hearing Thursday before the House Homeland Security Committee. The initiative is largely classified, but unclassified portions of the project reveal that the federal government is focusing on limiting the number of connections between federal agency networks and the Internet, and closely monitoring networks for potential attacks by hackers and foreign adversaries. However, there are questions about the degree of monitoring and whether it would include networks operated by state and local governments, or the private sector, including government defense contractors. Some Democrats on the oversight panel expressed concern about privacy. "It looks a little like the fox is guarding the hen house," said Rep. B. Etheridge (D-N.C.). Dept. of Homeland Security undersecretary R. Jamison said his agency is drafting a privacy impact assessment, and will make it available to the public for review when it is completed. "There's a big difference between intercepting and reading email and reacting to suspicious traffic going across your network," said J. Lewis, director of the technology arm of the Washington-based Center for Strategic and International Studies.

Ohio 'Paper' Vote System to Debut With Flaws
University of Maryland (02/27/08), N. Tickner

A new paper/optical scan voting system that Cleveland and its suburbs will employ in the March 4 primary is burdened by major flaws that could increase the risk of voter error, say members of a research team from the universities of Maryland, Rochester, and Michigan. The system boasts centralized ballot counting, and the researchers say one potential problem is that voters will not have an opportunity to run their ballots through a scanner before submission. The researchers discovered that the computer could disqualify legitimate ballots as overvotes if there are erasures or stray marks on the ballots. "[Voters] should be very careful to avoid stray marks and to review their ballots closely," advises University of Maryland political scientist and team leader P. Herrnson. "If they want to make changes, they should ask for a new form instead of erasing." Herrnson also finds fault with the central count approach, noting its potential for insecurity. Herrnson's team compared the usability of several electronic voting and verification systems over a five-year period, and the results and recommendations are detailed in the book "Voting Technology: The Not-So-Simple Act of Casting a Ballot."

Get Out Your Pencils: Paper Ballots Make a Return
USA Today (02/29/08) P. 2A; R. Wolf

Ohio's Cuyahoga County may have had more election troubles than any other area in the nation. The switch from the punch cards used in 2004 to touch screens in 2006 led to crashed servers, printer jams, vanishing memory cards, and overwhelmed poll workers. This year, Ohio expects to simplify and solidify its system by switching back to paper ballots. Voters will fill in ovals the same way students do when taking standardized tests. Although the new voting system may be simple, switching back to it is not. Cuyahoga County had just 74 days to make the switch after Ohio Secretary of State Jennifer Brunner decided to ban touch-screen machines. Since then, the county has retrofitted 6,300 old punch-card voting stations, installed 15 high-speed scanners, and rewired the warehouse. The county has also printed 4,317 different ballots for use in different precincts, with appropriate choices for the 668 candidates and 47 issues that will be voted on. A total of 1,043,930 ballots were printed, 95,470 absentee ballots were mailed and 7,000 poll workers have been hired. Although the system is low-tech, it could still be problematic. Running out of ballots is a possibility, and because the ballots will be scanned in a centralized location instead of where the votes are cast, voters will not get the chance to correct any errors on their ballot, such as partially filled circles. In the general election in November, ballots will be scanned in the precincts, enabling voters to correct any mistakes on their ballot.

US Seeks Terrorists in Web Worlds
BBC News (03/03/08), C. Vallance

The US government is performing observational studies on normal behavior in online worlds in hopes of eventually developing techniques and tools for uncovering the anomalous activity of terrorist groups. The recent report that the Office of the Director of National Intelligence (ODNI) sent to Congress mentions the project, which is codenamed Reynard. The report describes Reynard as "a seedling effort to study the emerging phenomenon of social [particularly terrorist] dynamics in virtual worlds and large-scale online games and their implications for the intelligence community." After the baseline normative behaviors are identified, Reynard will "then apply the lessons learned to determine the feasibility of automatically detecting suspicious behavior and actions in the virtual world." The project is still in its early stages,

and will be for research and not operational purposes. ODNI did not reveal which online worlds it will study, and Second Life and World of Warcraft are viewed as not offering the level of security that would attract terrorists. Experts tracking terrorist groups say it is only a matter of time before Jihad worlds emerge online for educating recruits about their techniques.

Wireless Worms Will Follow Influenza's Example
New Scientist (02/26/08), W. Knight

The outbreak of a wireless computer worm that spreads among portable devices like a flu epidemic is a possibility, according to a new mathematical model developed by Imperial College London researcher C. Rhodes and BT researcher M. Nekovee. Their model considers a group of people carrying Bluetooth-enabled smartphones, each of which has a fixed range for linking to other phones in the crowd. Each member of the crowd moves in a straight line and at a fixed speed, giving a phone that is contaminated by a worm a fixed likelihood of infecting other devices while they are within range. Rhodes and Nekovee's work demonstrates that a wireless worm could most efficiently proliferate in a crowded environment and also jump between geographically scattered locations, just like a real virus. "Knowledge that person-to-person contact, or rather device-to-device contact, represents a major factor in how a Bluetooth worm spreads is definitely important," says Symantec Security Response researcher E. Chien. He adds that the disablement of non-essential Bluetooth communications during an outbreak "reduces the contact occurrences and would be analogous to wearing a surgical mask in areas of potential infection."

Researchers Hack 'Tamper-Proof' PIN Terminals
ZDNet UK (02/26/08), T. Espiner

Cambridge University researchers have successfully hacked the Ingenico i3300 and Dione Xtreme PIN terminals, which are widely used in Britain and are touted as tamper-proof. Cambridge's S. Drimer and S. Murdoch say the devices' anti-tampering measures can be bypassed by tapping the line of the PIN Entry Device/smartcard interface, where the data is unencrypted, using conductors linked to a logic board with a field programmable gate array through a thin wire. The Ingenico device features a user-accessible compartment to insert SIM cards that is not designed with tamper-proofing in mind. The researchers employed a paper clip as a conductor, which they inserted into the serial data line through a hole in the PCB and thus were able to capture both the PIN and card details. They also drilled into the Dione Xtreme from the rear without being detected, and tapped the data through the insertion of a 4-centimeter needle into a flat ribbon connector socket. Both terminals were certified by Visa as secure, but the researchers found that neither device complied with security standards. "What this shows is that PIN entry devices in the UK are very insecure," says Cambridge professor R. Anderson. "What's more, the [device] certification process is completely defective."