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

Δελτίο 117
21 Μάη 2008

Information Tags Along Everywhere You Go
Baltimore Sun (05/11/08) P. 1A; L. Kay

Consumers concerned about privacy have been turning to the Internet to find ways to remove or disable the radio frequency identification (RFID) tags that are now built into many products and consumer items, including passports and credit cards. As RFID technology becomes more prevalent in society, critics say the tags and signals could be used for nefarious purposes by anyone who would spy on an individual in an effort to steal their identity or target them in a specific attack. Authorities are starting to listen to these warnings. The US State Department recently incorporated metal shielding into the covers of new passports after critics demonstrated how information from the RFID tag in a passport could be read from a distance. Meanwhile, California enacted a law prohibiting employers from forcing employees to implant RFID tags in their bodies. The law, along with similar efforts in Wisconsin and other states, was spurred by an Ohio company that implanted a tag in employees who worked with confidential documents, as long as the employee volunteered. Critics say the real problem is that RFID tracking is virtually invisible and undetectable by the subject being targeted. However, even critics say the problem has not yet reached a crisis level. Some say that RFID tags are not practical targets, as hackers and criminals would rather target richer sources, such as corporate databanks that store consumer information. In the case of RFID passports, all information contained in the chip is already printed on the front page of the passport, so losing a passport with a chip is no more dangerous than losing an ordinary passport.

NSA Attacks West Point! Relax, It's a Cyberwar Game
Wired News (05/10/08), D. Axe

For four days in April, the National Security Agency (NSA) conducted attacks against custom-built networks at seven of the nation's military academies as part of the seventh annual Cyber Defense Exercise, a training event for future military IT specialists. One of the strategies deployed was a structured query language insert that was launched to lull the military students into a false sense of security, only to then unleash a stealthy kernel-level rootkit that broke into workstations and started deleting data and communicating with the home computer. The West Point cadets caught the rootkit by manually searching the workstation. For a second year in a row, the Army team beat teams from the Navy, Air Force, and Coast Guard academies. The teams had to design their systems to meet certain specifications set by NSA. All networks had to be capable of email, chat, and other services, and had to be up and running at all times despite any attacks or defensive measures. The West Point team used a fairly standard Linux and FreeBSD-based network with advanced routing techniques for steering incoming traffic in directions of the IT team's choosing. The network took three weeks to build. NSA says it tailored its attacks to be just slightly too hard for the best undergraduate teams to handle.

Electronic Voting System Tested at University
Newcastle University (05/14/08)

A new electronic vote capture and counting system developed at Newcastle University was recently given its first major test. The Pret a Voter system, created by Newcastle University professor P. Ryan, is designed to overcome the problems that have plagued computerized voting systems worldwide. Ryan says Pret a Voter is far less susceptible to error, hacking, and corruption than either manual counting or other electronic-voting systems. The test was conducted with the support of the Electoral Reform Services and Newcastle University's Center for Software Reliability and School of Computing Science. The test was an election between three charities, each trying to secure student votes. Student voters were given a paper ballot and asked to draw a cross by a candidate, but the positions of the candidates on each ballot were selected at random. After the cross had been drawn, the student tore off the list of candidates so it was impossible to tell which charity had been chosen. The strip of paper with the mark was scanned into a computer, along with the ballot's serial number, which allowed the computer to allocate the vote to the correct candidate. After the election, voters could check to see that their vote was correctly cast by logging on to a Web site and entering their ballot's serial number.

Linkoping University Researchers Break 'Unbreakable' Crypto
Linkoping University (04/21/08), L. Falklof

Researchers at Linkoping University in Sweden have discovered that quantum computing is not 100% secure. Quantum computing was considered unbreakable because quantum-mechanical objects cannot be measured or manipulated without being disturbed, and an attempt to copy a quantum-cryptographic key in transit would lead to extra noise that is noticeable and would not yield any usable information. However, J.-A. Larsson, associate professor of applied mathematics, and his student J. Cederlof have found that it is theoretically possible for an unauthorized person to extract the key and hide their activities by simultaneously manipulating the quantum-mechanical and regular communication needed for quantum cryptography. "The concern involves authentication, intended to secure that the message arriving is the same as the one that was sent," Larsson says. In an article in the journal IEEE Transactions on Information Theory, Larsson and Cederlof also describe a solution that would secure quantum cryptography.

Swarming Spy Bots That Share Information Being Built for Military
Computerworld (05/09/08), S. Gaudin

BAE Systems is creating microbots inspired by birds and insects for the US Army Research Laboratory. The robots could eventually be used by soldiers to locate nearby enemies, determine their positions and weaponry, and listen in on their conversations. BAE's A. Penkacik says the robots will operate as a distributed system, or swarm, to gather information and send it back in a unified stream. For example, a swarm of robots the size of large insects could contain one robot that captures video, another that records sound, and another that detects chemical agents. The robots will share the information and send it back to a command center or soldier in a unified message. BAE scientists recently started designing the system, which is expected to be a five-year project, but Penkacik says soldiers may be able to use basic models of the spy robots earlier than that while engineers continue to refine the machines. Penkacik says the biggest challenge is to make the robots work collaboratively. "We need to work on collaborative behavior with multiple robots so they can do distributed data fusion in an ad hoc network that's moving in real time," he says. "All the information you get from these different sensors is what we're looking at to create knowledge that helps the war fighter stay alive."

CFP 08 Computer Security Experts Debate Political, Economic, Social Impacts of Technology Policy, AScribe Newswire (05/15/08)

ACM's 2008 Computers, Freedom and Privacy Conference (CFP 2008), which unites renowned technology policy experts who will help shape public debate on technology issues, takes place May 20-23 at Yale University. CFP 2008 will feature representatives from both the Obama and McCain presidential campaigns, who will answer questions posed by panelists on the technology policy. On May 21, CFP 2008 attendees will launch a collaborative effort to write a letter to the next president of the United States asking about their priorities for technology policy during the next administration. Proposals will be posted on a wiki for review, and a draft letter will be circulated for signatures on a consensus document. The final letter will be sent to both presidential campaigns for their response. The project is intended to generate broad discussion on technology policy priorities among grassroots groups, and to highlight those viewpoints for future policy makers. CFP 2008 will also present panels, discussions, workshops, technical demonstrations, and speeches on key topics, including voting technology, online campaigning, social networks, network neutrality, electronic medical records, media concentration, cybercrime, and cyberterrorism.

Report: Government's Cyber Security Plan Is Riddled With New Spying Programs Wired News (05/15/08), P. Singel

The Bush administration's proposed National Cyber Security Initiative is criticized by a budget report from the Senate Armed Services Committee for being more about spying than about safeguarding government networks, for its planned use of unproven, early-stage technology, its secrecy, and the possible unlawful or inadvisable nature of its projects. "[S]ome of the projects support foreign intelligence collection and analysis generally rather than the cybersecurity mission particularly," the report says. "That is not to say that the proposed projects are not worthwhile, but rather that what will be achieved for the more than $17 billion planned by the administration to secure the government's networks is less than what might be expected." The initiative's alleged objective is to lower the risk of federal government networks being attacked and breached by extending the tools that currently shield classified networks to all federal government networks, and also to dramatically subtract the number of Internet connections in order to make the patrolling of the government's e-perimeter less difficult. Many of the plan's specific elements are of a classified nature, but in January US intelligence chief M. McConnell expressed a desire in the New Yorker that the National Security Agency should start monitoring the Internet. The Armed Services Committee's analysis says the whole project is effectively shut out from healthy public debate because the bulk of the initiative, including most of the non-classified data about the project, is flagged as being "For Official Use Only."