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

Δελτίο 164
5 Δεκέμβρη 2009

Trust Linux!
ICT Results (11/20/09)

A consortium of 23 research and business partners, working on the European OpenTC project, have developed open source software and applications for trusted computing (TC) environments using openSUSE, a commercially available version of the Linux operating system. Building TC support in openSUSE involved compiling a trusted software stack for Linux, developing universal virtualization layers, and creating TC and trusted platform module management software. The developers say the accomplishment represents a breakthrough in TC technology as openSUSE is now the first operating system to offer full TC support. The OpenTC platform continually monitors the computer for changes, ensuring that only trusted, verified software is running. "Until now, TC had been implemented for specific applications, such as Microsoft's BitLocker hard drive encryption in Windows Vista and Windows 7, or the fingerprint reader on some HP laptops," says OpenTC project manager H. Petautschnig. "With the OpenTC platform, we are extending the TC environment to the full operating system and beyond."

'Fingerprinting' RFID Tags: Researchers Develop Anti-Counterfeiting Technology
University of Arkansas (11/19/09), M. McGowan

Univ. of Arkansas researchers have developed a new method for preventing the cloning of passive radio frequency identification (RFID) tags. The method prevents the production of counterfeit tags by focusing on one or more unique physical attributes of individual tags, instead of the information stored on the tags. "It is easy to clone an RFID tag by copying the contents of its memory and applying them to a new, counterfeit tag, which can then be attached to a counterfeit product--or person, in the case of these new e-passports," says Arkansas professor D. Thompson. "What we've developed is an electronic fingerprinting system to prevent this from happening." The researchers determined that all RFID tags have a unique fingerprint due to variances in radio frequency and manufacturing. By using an algorithm that repeatedly sent reader-to-tag signals, the researchers found that radio frequencies in RFID tags ranged from 903 MHz to 927 MHz, and increased in increments of 2.4 megahertz. The measurements showed that each tag had a unique minimum power response at multiple radio frequencies, and that power responses were significantly different even in same-model tags. Thompson says the different minimal responses are just one of several unique physical characteristics that enabled them to create an electronic fingerprint to identify tags with a high probability of detecting counterfeit tags.

Building Real Security With Virtual Worlds
University of Maryland (11/26/09), N. Tickner

Univ. of Maryland (UM) researchers are combining computerized modeling and group behavior predictions with video-game graphics to create virtual worlds that defense analysts can use to predict the results of military and policy actions. "Defense analysts can understand the repercussions of their proposed recommendations for policy options or military actions by in-

teracting with a virtual world environment," says UM professor V. Subrahmanian. "They can propose a policy option and walk skeptical commanders through a virtual world where the commander can literally 'see' how things might play out." Computer scientists have created a "pretty good chunk" of the computing theory and software needed to build a virtual Afghanistan, Pakistan, or another "world," Subrahmanian says. Maryland researchers have developed artificial intelligence software that uses data about past behavior of groups to create rules about the probability of a group's potential actions in different situations. The researchers also have developed "cultural islands," which give a virtual world representation of a real-world environment or terrain, populated with characters from that part of the world who follow a behavior model. They also have developed the CONVEX and CAPE forecasting engines, which focus on predicting behavioral changes in groups using validated and historical data. "We are now at the point where, with the help of the analysts, we can start thinking about building computer-generated models that can automatically adapt to changes in group behaviors and to conditions on the ground," Subrahmanian says.

Proper Use of English Could Get a Virus Past Security
New Scientist (11/27/09), R. Blincoe

Johns Hopkins University security researcher J. Mason says hackers could potentially evade most existing antivirus programs by hiding malicious code within ordinary text. Mason and colleagues have discovered how to hide malware within English-language sentences. Mason developed a way to search a large set of English text for combinations of words that could be used in malicious code. This potential weakness has been recognized in the past, but many computer security experts believed that the rules of English word and sentence construction would make executing an attack through the English language impossible. Machine code requires the use of character combinations not usually seen in plain text, such as strings of mostly capital letters. University College London security researcher N. Courtis says malicious code hidden in plain language would be "very hard if not impossible to detect reliably." Mason and colleagues presented their research at the recent ACM Conference on Computer and Communications Security, but were careful to omit some of their methodology to avoid helping potential hackers. "I'd be astounded if anyone is using this method maliciously in the real world, due to the amount of engineering it took to pull off," Mason says.

University Unites Industry, Gov to Tighten Energy Sector Cybersecurity
NextGov.com (11/24/09), J. Aitoro

A Rice University program created to engage the energy industry and government about protecting power plants from cyberattacks hosted Dale Meyerrose, former CIO for the Office of the Director of National Intelligence. University officials also recently heard speeches from security professionals at AT&T and Waste Management, as well as US Rep. M. McCaul, co-chairman of the Commission on Cybersecurity for the 44th Presidency and a member of the House Homeland Security Committee. Rice computer science professor D. Wallach created the multiyear program with C. Bronk, a fellow at Rice's Baker Institute for Public Policy, who used to work at the State Department's Office of eDiplomacy, where he helped launch a wiki that enabled employees around the globe to securely exchange information. The program is designed to help the industry in its efforts to organize and respond to a cyberattack. Wallach and Bronk plan to develop a private wiki for cybersecurity professionals and policymakers from the energy industry to "collect aggregate knowledge and create an institutional memory that everyone can draw on," Wallach says. They also see the development of policy objectives as a proactive way for the energy sector to engage the government on future regu-

lations. Wallach and Bronk add that the initiative could serve as a cybersecurity model for other sectors such as health care and transportation.

Research Group to Tackle Cybersecurity
InfoWorld (12/01/09), G. Gross

Carnegie Mellon University, the Massachusetts Institute of Technology, Purdue University, and Northrop Grumman have launched a five-year research effort to tackle the most complex problems in cybersecurity. Northrop Grumman's Robert Brammer says the Northrop Grumman Cybersecurity Research Consortium was created because the values for information services and systems have never been greater and the cybersecurity threats have never been greater. Brammer says large-scale cyberattacks are a "credible threat" in the coming years. "We need significant new technology developments, combined with improved security education, global standards, and understanding of security economics and psychology," he says. The participating universities were chosen because of their long-term, cutting-edge cybersecurity research. The consortium will work on several projects, including software analysis, secure computer design and forensics, improved software, and next-generation secure networks. E. Spafford, executive director of Purdue's Center for Education and Research in Information Assurance and Security, says the cybersecurity threat is not new. "It's one that many of us have been warning about for nearly three decades, Spafford says. "The problems have been anticipated and seen in advance. Unfortunately, none of the warnings have been taken seriously, particularly by the government." He says many government agencies have been combating cybersecurity issues after they have happened, instead of acting proactively.