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

Δελτίο 35
5 Αυγούστου 2006

Introverted IT Students More Inclined to Cyber-Crime
New Scientist (07/26/06), P. Marks

A recent study has found that introverted technology students are more prone to "deviant" computer conduct, contradicting earlier research that suggested that malicious computing activities are most often the product of extroverts. The researchers polled 77 Purdue University computer science students with an anonymous online questionnaire, asking questions about their involvement in deviant computing activities, some of which are unlawful, such as using another person's password, writing and dispatching a virus, and obtaining credit card numbers. "Of 77 students, 68 admitted to engaging in an activity that could be classified as deviant," said Purdue computer scientist M. Rogers. In a self-evaluation, the deviant students gave themselves a 10% higher ranking on a scale that measured introversion. Acknowledging the limited scope of the study, Marcus cautions against using the results to support sweeping generalizations. Rogers himself was involved in a 2003 survey of arts students at the University of Manitoba, Canada, that found an increased rate of "deviant" activity among extroverts. DataSec's J. Munsey believes that each personality type has a niche in the realm of computer misuse. Irrespective of the proportion of introverts and extroverts, Marcus says that he is alarmed by the fact that 88% of the students polled admitted to engaging in deviant behavior.

Homeland Security Awards $3 Million to Rutgers-Led Research Consortium
Rutgers University (07/26/06)

Rutgers University will receive a $3 million grant from the US Department of Homeland Security (DHS) to coordinate research projects into advanced information analysis and technology that could help indicate a potential terror threat to the nation. The university's Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) will head a consortium that will focus on finding patterns and relationships in news stories, open-source Web logs, and other accessible information, and rate the consistency and reliability of the sources. "The challenge involved in this endeavor is not only the massive amount of information out there, but also how quickly it flows and how fast the sources of information change," says DIMACS director F. Roberts. "We will develop real-time streaming algorithms to find patterns and relationships in communications, such as among writers who may be hiding their identities, and to rate information sources for their reliability and trustworthiness." Researchers from AT&T Laboratories, Lucent Technologies Bell Labs, Princeton University, Rensselaer Polytechnic Institute, and Texas Southern University will participate in the research projects. DHS also awarded grants to the University of Southern California, the University of Illinois at Urbana-Champaign, and the University of Pittsburgh for similar research, and Rutgers will coordinate the overall initiative.

Blind to Lead Way in E-Voting
Australian IT (07/25/06), C. Jenkins

The Australian government is considering a trial of electronic voting systems that could lead to the use of e-voting for next year's federal election. The government will decide on the e-

voting system recommendations of an electoral committee within six weeks, and the proposal also suggests that the trial involve people who are blind and visually impaired. Last week, the Australian state of Victoria announced that visually impaired people will be able to use e-voting systems to vote in its November elections. The e-voting systems used in Victoria will not tally votes, according to Michael Simpson, public policy manager of Vision Australia. Voters will receive smart cards in order to use the e-voting system, which will read the ballot options to voters via headphones, print their votes, and then return them to the ballot box. E-voting will allow voters to cast their ballots privately and independently, but there are concerns that the technology or results could be used to classify voters. "We are prepared to live with that downside because it is a huge step forward," says Simpson.

Hack-Proof Design
EDN (07/20/06) P. 47; W. Webb

The profusion of networked devices and the refinement of hackers' attack methods are fueling the urgency among embedded-system designers to prioritize security requirements. All security requirements must be addressed during the design phase, prior to the deployment of an embedded system product. The National Institute of Standards and Technology's Computer Security Resource Center offers security-related publications for designers outlining what kinds of challenges need to be met, such as the identification of data or proprietary information in need of protection, and identification of potential attackers and how sophisticated they are. Security measures to be considered include the physical isolation of networked systems, and the containment of sensitive equipment within rugged packaging that cannot be accessed without specialized gear. The Common Criteria for Information Technology Security Evaluation are internationally formulated guidelines for system security standards, which enables consumers, developers, and evaluators to particularize the security functions of a product in standards-protection profiles and evaluation-assurance levels. Users must confirm their identities before they can interact with a secure embedded system via authentication, while data encryption plays an important role when embedded systems link to a network or the Internet. Concurrent with improving security is device manufacturers' experimentation with new business models, such as the pay-as-you-go scheme in which customers agree to pay for a device as they use it and in return receive full functionality. Failure to pay gives the vendor license to withhold network-activation codes and disable the device, while bypassing activation or parts removal is thwarted by a strong security model.

Grad Students in San Diego Build Biometric Vending Machine
Contactless News (07/31/06), A. Williams

Graduate students at the University of California are outfitting a soda machine with a small computer, a barcode scanner, a fingerprint reader, and a Web cam to enable facial recognition. If someone wants a soda, he can simply place his thumb on the reader and it recognizes his account. The idea for the SodaVision project came from UCSD associate engineering professor S. Savage, who purchased a soda machine last year with an eye toward improving the system at UCSD's snack and soda cooperative. "I bought the soda machine and a touch screen and the fingerprint reader," Savage said. "We looked for a fingerprint reader that would work with our software and with Linux. Now they [the students] have actually torn [the fingerprint reader] apart and rewired it to work with the machine." The students created the interface, and they are now working on the facial-recognition technology. "Recognition requires detecting a face, morphing the face, running preprocessing on the face, looking up the face in the repository, running an election over many frames, and finally logging in the

user with the most votes in the election," wrote graduate student T. Duerig in a paper detailing the project. The system currently recognizes faces with 80% accuracy, but the researchers are hoping to reach 95%.