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

Δελτίο 93
14 Οκτώβρη 2007

USC Student's Computer Program Enlisted in Security Efforts at LAX
Los Angeles Times (10/01/07), L. Gordon

The doctoral thesis of USC computer science student P. Paruchuri has led to a computer program that police at Los Angeles International Airport are piloting to bolster security. The idea is that the software would keep potential terrorists and criminals continuously unsure about where, when, and how frequently vehicles will be inspected at airport entrances. Paruchuri's work focuses on game-theory research on the random timing of police patrols and its impact on crimes such as home burglaries, and Los Angeles World Airports official J. Butts says the program affects police deployment and the regularity of vehicle searches in a way that "makes it virtually impossible to predict where resources might be deployed." The initiative stems from a federally sponsored USC think tank that utilized scholars in engineering, economics, political science, psychology, and computer science to assess and minimize the risks of terrorism. Paruchuri's thesis advisor, professor M. Tambe, says LAX's use of Paruchuri's research is "something that we, as researchers, dream of: creating research that is not only academically wonderful but something that is also very useful."

GPL Defenders Say: See You in Court
CNet (10/01/07), S. Shankland

The Software Freedom Law Center (SFLC) has filed a copyright infringement lawsuit against Monsoon Multimedia for its alleged failure to comply with the terms of the General Public License (GPL), and experts expect the case to call more attention to similar violations in court. At the center of the dispute is the BusyBox software, which is governed by version 2 of the GPL, which allows anyone to view, tweak, and distribute the software, provided modifications are also issued under the license. In addition, anyone distributing GPL software in an executable form that a computer can run is required to release the complete source code. "Simply coming into compliance now is not sufficient to settle the matter, because that would mean anyone can violate the license until caught, because the only punishment would be to come into compliance," says SFLC attorney D. Ravicher. He says the center is refusing to back down because "If you start getting a reputation for being a pansy, then people are going to conclude they don't have to do anything." Ravicher says that in most instances both parties make a good faith effort to resolve disputes with discretion, expediency, and little fuss. Although he says the Monsoon suit is not part of an overarching effort to build GPL case law, Hunton & Williams lawyer J. Harvey predicts that more GPL-related lawsuits will be launched.

Scientists Warn of 'Vocal Terror'
BBC News (09/14/07), L. Seward

Scientists at the recent British Association Festival of Science in York expressed concern that improving human speech technology could give rise to "vocal terrorism" in the next 10-15 years. Researchers said an inability to verify who was speaking could prove to be particularly problematic if the technology were to fall into the hands of terrorists. Scientists today are de-

veloping computerized speech based on models of a vocal tract, which helps produce a more realistic sound than the current method of copying sounds. "If we get to the point where we are synthesizing the actual shape of somebody's [vocal tract] based on analysis of their speech, then the speech we are producing should sound and look like the actual person," says D. Howard of the University of York. The researchers fear that someone could use the technology to impersonate the voice of a bank manager and place calls requesting confirmation of account information. People could use the technology to make prank calls or even to flawlessly render the voice of a country's leader in an act of vocal terror. "It's not scare mongering; it's tying to say to people, 'we have to think about these things,'" adds Howard.

Connecting the Dots
National Journal (09/29/07) Vol. 39, No. 39, P. 61; M. Perelman

The Automated Targeting System (ATS) has been cited by US Homeland Security Secretary M. Chertoff for enabling his department's Custom and Border Protection agency to link a chain of information that can thwart terrorist plots, and decried by privacy and civil-liberties groups for being the tool of a clandestine federal data-mining program that is collecting and storing highly personal information on travelers. The system has been employed by federal officials to perform risk assessments on people entering the country since 2002. "All the key characteristics of the Automated Targeting System--including the assessment, the basis for the assessment, the rules that apply, and the 'targeting activities'--remain shrouded in mystery," says the Electronic Privacy Information Center, which is opposing the ATS along with 40 other groups and individuals in the privacy and technology sectors. Homeland Security officials claim the system does not capture any racial, ethnic, or religious data and that the goal is to analyze behavior, relationships, and contacts among individuals and groups. Complaints prompted Homeland Security to announce a proposal to retain information in the ATS database for 15 years instead of 40, and to limit the purposes for which the government could use passenger data, provide individuals with access to data, and add a redress procedure not included in the original privacy proposal. Civil-liberties groups say the ATS bears an uncomfortable similarity to the Total Information Awareness data-mining program that the government terminated 4 years ago in response to public resentment. House Homeland Security Committee Chairman Rep. B. Thompson (D-Miss.) warned at one point that the ATS database "could be used as a warrantless well of evidence from which any law enforcement, regulatory, or intelligence agency could dip at will--without any probable cause, reasonable suspicion, or judicial oversight." Although Democratic leaders in Congress have voted to continue ATS funding, sources say they are carefully scrutinizing the privacy rule-making process.

Technology Could Enable Computers to 'Read the Minds' of Users
Tufts University (10/01/07) Thurler, Kim

Computers capable of responding to users' emotional states could be facilitated by methods developed by Tufts University researchers through the novel application of non-invasive and easily portable imaging technology. "Measuring mental workload, frustration and distraction is typically limited to qualitatively observing computer users or to administering surveys after completion of a task, potentially missing valuable insight into the users' changing experiences," says Tufts computer science professor Robert Jacob. His human-computer interaction group is collaborating with biomedical engineering professor Sergio Fantini in an analysis of functional near-infrared spectroscopy (fNIRS) technology that monitors blood oxygenation levels in the brain as a proxy for workload stress a user may undergo when executing a task of increasing difficulty. School of Engineering researcher Erin Solovey says,

"fNIRS, like MRI, uses the idea that blood flow changes to compensate for the increased metabolic demands of the area of the brain that's being used." Fantini says the specific area of the brain where the change in blood flow transpires should yield clues about the brain's metabolic changes and workload, which could act as a surrogate for frustration and similar emotions. A $445,000 National Science Foundation grant will let the researchers incorporate real-time biomedical data with machine learning to generate a computer user experience that is more in tune with users' mental load. The initial results of the team's experiments to detect the user workload experience with fNIRS will be presented at the ACM symposium on user interface software and technology, which takes place Oct. 7-10, in Newport, R.I. For more information on the ACM UIST Conference, visit http://www.acm.org/uist/uist2007/

Carnegie Mellon Researchers Fight Phishing Attacks With Phishing Tactics
Carnegie Mellon News (10/02/07) Spice, Byron

People who fall for phishing attacks and are conned into visiting a counterfeit Web site by spoof email are often vulnerable to such victimization because they ignore helpful educational material, but Carnegie Mellon University researchers have learned to use phishing techniques to expose would-be victims to such material. They sent their own spoof emails to lure people onto educational sites, and discovered that their targets were more likely to learn and retain more knowledge about recognizing bogus sites. The study involved three groups of 14 volunteers participating in role-playing exercises in which they processed a blend of phishing, spam, and genuine email. One group was given anti-phishing educational materials after they had been tricked by a phishing email, the second group was given the materials without first falling for the phishing email, and the third group received no anti-phishing educational materials. The first group spent over twice as much time studying the materials than the second group, while the second and third group's inability to identify phishing emails was about the same. The exercise was repeated a week later, and the members of the first group had substantially more success at identifying phishing emails than those in the other two groups. The results of the study will be presented Oct. 5 at the Anti-Phishing Working Group's (APWG) eCrime Researchers Summit in Pittsburgh. APWG said the number of unique phishing reports rose by over 5,000 between May and June, with an overwhelming number of attacks focused on the financial services domain.

'Dead Time' Limits Quantum Cryptography Speeds
NIST Tech Beat (09/27/07)

A new paper by researchers at the National Institute of Standards and Technology (NIST) and the Joint Quantum Institute (JQI) published in the New Journal of Physics posits that quantum cryptography speed will be restricted by technological and security issues unless a way is found to reduce "dead time" in the single-photon detectors receiving quantum-encrypted messages. This dead time is described as the period of time during which the detector has to recover after detecting a photon. Off-the-shelf single-photon detectors require about 50-100 nsec to recover before they can detect another photon, which is far slower than the 1 nanosecond between photons in a 1-GHz transmission. NIST physicist Joshua Bienfang reasons that the speed would increase if the dead time in single-photon detectors is lowered, and several groups are engaged in accomplishing this milestone. He also contends that faster speeds would be helpful in wireless cryptography between a ground station and a low-orbiting satellite.

The Lesson of Estonia

Information Security (09/07) Vol. 10, No. 8, P. 12; D. Denning

It seems unlikely that the cyberattack against Estonia in the spring of 2007 was an act of government-sponsored cyberterrorism, but the assault still deserves consideration, as it drove online activism to an unprecedented and troubling level, writes D. Denning of the Naval Postgraduate School. Internet-based protests have existed for over a decade, and automated software has been developed for bombarding targeted Web sites with page requests. More recently, the bonnet, which hijacks computers into a network that can send spam or launch DDoS attacks, has emerged as a powerful cyberattack tool. Allegedly, Estonian attackers used botnets in their DDoS assaults. That the hijacked computers came from around the world makes it less probable that the Russian government was behind the cyberattack, as some have speculated. According to Denning, the salient aspect of the cyberattack on Estonia is that the siege was able to persist for weeks and inflict costly and disruptive damage without the resources of a government sponsor. This implies that a few unaffiliated individuals can wreak substantial damage on a national scale. Al-Qaida and other terrorists already employ cyberattacks to cause financial damage and interrupt Web sites. Although current cyberterror lingo has been inflated to hype proportions, the United States must acknowledge the actual risk and grow more serious about defending against new cyberattack tools, Denning says.

Spam Weapon Helps Preserve Books
BBC News (10/02/07), P. Rubens

An anti-spamming weapon developed at Carnegie Mellon University is now aiding university researchers in the preservation of books and manuscripts. The CAPTCHA test consists of an image of letters or numbers that have been distorted and must be translated by humans in order to access Web sites. Most spam bots are incapable of solving such puzzles, but a CMU research team that is digitizing old books and manuscripts provided by the Internet Archive is using the CAPTCHA method to decipher words that cannot be read by optical character recognition software. These indecipherable words are distributed to Web sites around the globe where they are used as conventional CAPTCHAs. Visitors solve these "reCAPTCHAs," which are then sent back to CMU. To guarantee the correct deciphering of reCAPTCHAs, site visitors are shown images of two words to study, the contents of one of which is already known. "If a person types the correct answer to the one we already know, we have confidence that they will give the correct answer to the other," says CMU professor L.s von Ahn. "We send the same unknown words to two different people, and if they both provide the same answer then effectively we can be sure that it is correct." Von Ahn reports that popular sites' adoption of reCAPTCHAs is helping the system to translate about 1 million words daily for CMU's book archiving initiative.

CERT Advances Secure Coding Standards
Dark Reading (10/02/07), K. Higgins

CERT and Fortify Software have announced an alliance to automate compliance with CERT's C and C++ Secure Coding Standard. CERT is converting its guidelines into a coding format that will run on Fortify's Source Code Analysis tool, and the software module borne from this effort will be freely available from CERT, allowing other tool vendors to translate it to their products. Programmers who wished to employ the voluntary CERT guidelines on writing cleaner and more secure software in C and C++ were forced to mine the huge checklist manually, which Fortify chief scientist Brian Chess calls a tedious process. CERT obtains input from software developers and other organizations to help spot common programming mistakes that cause software bugs and supply secure coding standards through its secure

coding initiative, but Matasano Security's T. Ptacek says, "Product teams don't get better by reading secure coding standards. They get better by working with security testers, seeing how their code gets broken by attackers, and learning from the experience." What is needed is a top-down security commitment, which Ptacek says is beyond the abilities of many vendors. Though CERT vulnerability analyst R. Seacord acknowledges the importance of internal buy-in, he says it is impossible without guidelines on how to guarantee that security is a key consideration in software design. "There's a big need for a common language that security testers and software developers can speak so they can agree on what needs to be done and what needs to be taken seriously," maintains Ptacek. "I don't see the harm in what CERT is doing, but we should figure out the 'what' before we spend lots of time on the 'how.'"

Privacy Threats Are No Longer 'Terra Incognita'
The Star Online (10/01/07), M. Geist

Hundreds of privacy commissioners, government regulators, business leaders, and privacy advocates from around the world met for three days in Montreal last week to gain a better understanding of how new technologies such as ubiquitous computing, radio frequency identification devices, and nanotechnology will impact privacy protection. The theme of the International Data Protection and Privacy Commissioners conference was "Terra Incognita," a reference to not knowing what lies ahead as technology rapidly changes. At the conference US Secretary of Homeland Security M. Chertoff argued that governments will need to collect more data if they are to protect citizens in the years to come. For example, Chertoff said fingerprints can be used to increase surveillance, and he noted that a single fingerprint taken from a vehicle used in a bombing in Iraq was matched to one taken years ago at a US border crossing. Although the idea of a broad surveillance society made many privacy advocates cringe, Chertoff suggested that there will be little they can do about it. The conference focused on current privacy protection strategies such as privacy audits, privacy impact assessments, trust seals, and global cooperation. Although such measures have become more effecttive, there was a general feeling among the participants that more needs to be done.

West Is Taking Fight Against Terrorism Online
International Herald Tribune (09/30/07), D. Carvajal

Western nations are moving forward to establish online security perimeters with proposals to impede Web sites and to issue emails containing spyware that would keep an eye on jihadists, even though critics caution that such measures could give rise to censorship and privacy infringement. A series of anti-terrorism proposals will be unveiled by EU justice commissioner F. Frattini in November, and included in the proposals will be a package for the development of technology to block Web sites that post bomb-making recipes and other terrorist how-tos, and for the criminalization of online terrorist enlistment. "The Internet, as we all know, is abused for terrorist propaganda and also for disseminating information on how to make bombs," notes Frattini spokesman F. Roscam-Abbing. "What we want to achieve is to make that phenomenon punishable." Sweden, Germany, Australia, and other countries are individually seeking additional powers and technologies to ostensibly thwart terrorism online. Frattini and other public officials pledge that governments are balancing free speech and security to guarantee that Web sites are not used to share data in a way that constitutes a threat to public safety. Critics are worried about these plans since the EU nations are already moving to adopt a "data retention directive" mandating that ISPs will need to hold on to information about communications from six to 24 months to help in the identification of terrorism networks. "One way of viewing these trends is that the terrorists have won," says Uni-

versity of Cambridge computer security researcher R. Clayton. "They're making us change our society to counteract, not what terrorists are doing, but what they're threatening to do."

Dragonfly or Insect Spy? Scientists at Work on Robobugs
Washington Post (10/09/07) P. A3; R. Weiss

Researchers are developing insect-sized robots and insects augmented with robotic systems, or robobugs, that could be used for rescue missions, spying, or guiding missiles in combat. Although no government agency has admitted to successfully creating such a system, several, including the CIA and the Defense Advanced Research Projects Agency, have admitted to working on projects that, if successful, would result in such spy devices. In fact, the nation's use of flying robots has increased more than fourfold since 2003, with over 160,000 hours of robotic flight logged in 2006. However, creating insect-sized robots is a significant challenge. "You can't make a conventional robot of metal and ball bearings and just shrink the design down," says University of California Berkeley roboticist R. Fearing. The rules of aerodynamics change at such small scales and any mechanical wings would need to flap in extremely precise ways, a huge engineering challenge. Researchers at the California Institute of Technology have developed a "microbat ornithopter" that is capable of flight but smaller than the palm of a person's hand, and Vanderbilt University has developed a similar device. At the International Symposium on Flying Insects and Robots, Japanese researchers revealed radio-controlled flyers with four-inch wingspans that look like hawk moths. A known DARPA project, called the Hybrid Insect Micro-Electro Mechanical Systems project, is inserting computer chips into moth pupae, the stage between caterpillar and adult moth, with the hopes of creating insects with nerves that have grown around internal silicon chips, creating a "cyborg moth," so they can be controlled and used to take surveillance photographs.

UMass Amherst Researchers Improve Security for Credit Cards and Other Devices
University of Massachusetts Amherst (10/03/07)

University of Massachusetts Amherst researchers K. Fu, W. Burleson and D. Holcomb have created a cheap and efficient methodology for augmenting the security of radio-frequency identification tags. "We believe we're the first to show how a common existing circuit can both identify specific tags and protect their data," says Burleson, who presented the research at the annual Conference on RFID Security. "The key innovation is applying the technology to RFID tags, since they're such tiny devices with very small memories." Within the tags are passive systems that respond automatically to electromagnetic fields generated by radio antennas attempting to read the devices' memories, and this technology can be vulnerable to security breaches. The UMass Amherst researchers' security technique exploits the concept of random numbers, which are used to encrypt data transmitted by the tags, and a string of random numbers can be easily produced by machines with the appropriate hardware and software. However, RFID tags are not designed for random number generation, so the researchers' work takes specific machinery committed to that function out of the equation and instead employs special software that allows the tag readers to siphon out unique data from the tags' existing hardware. Variations in each tag's cells can also be tapped as individual tag identifiers, generating a unique fingerprint, Burleson says. The RFID Consortium for Security and Privacy is a collaborative effort between engineers and cryptographers that forms part of a research initiative underwritten by a $1.1 million National Science Foundation grant to enhance security for wireless "smart tag" gadgetry.

GTISC Releases Emerging Cyber Threats Forecast

Georgia Institute of Technology (10/02/07)

The Georgia Tech Information Security Center has published its annual forecasting report, the GTISC Emerging Cyber Threats Report for 2008, which describes the five key areas of security risk for enterprise and consumer Internet users. In 2008, cyber security threats are anticipated to grow and evolve in the areas of Web 2.0 and client-side attacks, such as social networking attacks, and targeted messaging attacks, including malware proliferation through video-sharing online and instant messaging attacks. Botnets, particularly the expansion of botnet attacks into peer-to-peer and wireless networks, are another significant area of concern. Threats aimed at mobile convergence, including vishing, smishing, and voice spam, are anticipated to be substantial, as are threats targeting RFID systems. The primary driver behind all five major threat categories in 2008 continues to be financial gain. GTISC recommends improved synchronization among the security industry, the user community, application developers, Internet service providers, and carriers. GTISC director Mustaque Ahamad anticipates that enterprise and consumer technologies will continue to converge in 2008, making it even more essential to protect new Web 2.0-enabled applications and the IP-based platforms they increasingly depend upon.