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

Δελτίο 120
12 Ιουνίου 2008

Call It Predictable: Cellphone Users Are Easy to Find
New York Times (06/05/08) P. A23; J. Schwartz

New research that followed 100,000 cell phone users in Europe suggests that most people follow strict patterns and can be found in one of a few locations at any time, and that people generally do not travel far from home. Even when people do travel long distances, they still display similar patterns. The researchers say that being able to create general rules and algorithms defining people's movement could lead to computer models used for understanding emergency response, urban planning, and the spread of disease. Northeastern University Center for Complex Network Research director and project author A.-L. Barabasi says that reducing individual behavior into electronic datasets creates huge opportunities for science. The researchers tracked 100,000 cell phone users selected at random from a population of 6 million for 6 months, with a user's location being revealed whenever one of them made a phone call. Previous efforts to track people's movements have used various currencies and complex formulas to predict behavior, but the researchers say cell phones work better because people tend to carry them wherever they go.

A New Way to Protect Computer Networks From Internet Worms
Ohio State University Research News (06/04/08)

Ohio State University researchers have developed a technique that can automatically detect Internet worms within minutes of when a worm has infiltrated a computer network. Ohio State University's N. Shroff says Internet worms spread very quickly, and can flood the Internet with junk traffic or overload computer networks and cause them to shut down. For example, in 2001, the random scanning worm Code Red infected 350,000 machines in less than 14 hours. The key to detecting worms early, the researchers found, is to monitor the number of scans that machines on a network send out. When a machine starts sending too many scans, a sign that it has been infected, it should be isolated and checked for viruses. Shroff says the difficult part of developing the technique was figuring out how many scans were too many, as machines perform scans naturally when users search for Web addresses and perform other tasks. The researchers used simulations to test their method against the Code Red worm and the SQL Slammer worm of 2003, simulating how far the virus would spread depending on how many networks on the Internet were using the same containment strategy. In the simulations, the researchers were able to prevent the spread of Code Red to less than 150 hosts on the entire Internet 95% of the time. To deploy this technique, network administrators would have to install software to monitor the number of scans on their networks and to allow for some downtime among computers during quarantine, which Shroff says would not be a problem for most organizations.

Second Annual National Institute on CyberLaw: Expanding the Horizons
Association for Computing Machinery (06/06/08)

The 2nd Annual National Institute on CyberLaw: Expanding the Horizons, co-sponsored by ACM and scheduled for June 18-20 in Washington, DC, will investigate developments involving the Internet and computers, particularly in the domains of business law, criminal law, and intellectual property. Issues to be covered at the event include identity theft, pornography and sexual predators on the Internet, computer crime and procedure, the future of ICANN and control of the Internet, civil copyright enforcement, ethics for managing electronic documents and evidence, digital forensics, and tracking, data mining, and marketing of data acquired from Internet users. There will also be a debate on the NSA Wiretap Program and the US Constitution, with panelists that include Time Warner's D. Kris, Electronic Privacy Information Center director M. Rotenberg, and A. McCarthy, director of the Foundation for Defense of Democracies' Center for Law and Counterterrorism. A discussion titled "Criminal Aspects of Identity Theft: Financial Records, Data Mining, and Online Threats" will be presented by D. Purdy of Allenbaugh Samini, US Homeland Security Department chief privacy officer H. Teufel, and C. Painter of the US Dept. of Justice. The final session, titled "The Future of Computing, the Internet, and the Law: Legal Developments in Virtual Reality," will be moderated by program chair A. Grosso of Andrew Grosso & Associates, while featured speakers will include University of San Francisco School of Business Management professor J. Allen, IBM Systems & Technologies Group executive S. Mortinger, S. Kane of Drakeford & Kane, and FTI Consulting managing director M. Rasch.

China's Cyber-Militia
National Journal (05/31/08) Vol. 40, No. 29, P. 16; S. Harris

China-based computer hackers, including those working on behalf of the Chinese government and military, have deeply intruded into US federal and corporate information systems, stolen strategic information from American executives prior to business negotiations in China, and accessed US electric power plants, possibly causing major outages, according to US government officials and computer security experts. Among those sounding such warnings is former Cyber Security Industry Alliance President T. Bennett, who says these incidents emphasize the poor security of critical US electronic infrastructure, as well as government and company officials' lack of acknowledgment of such vulnerabilities. Another information-security expert says that hackers in China have been aggressively mapping the technology infrastructure of American companies, leading to concerns that such mapping is a prelude to information theft, network corruption, and other malevolent activities. "The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction," says federal counterintelligence official J. Brenner. "It's a kind of cyber-militia." At a recent hearing, Rep. J. Langevin (D-R.I.) criticized the private sector's "half-hearted approach" to enhancing security, while Cybrinth CEO S. Spoonamore says US officials should be more forthcoming about system breaches if the security of US electronic infrastructure and the sensitive information and operations embedded in that infrastructure is to be fortified. Military analysts say China's aggressive pursuit of offensive cyber-capabilities is one tool in a series of "asymmetric" warfare tactics to counter US military might, which neither China's nuclear arsenal nor armed forces can match. The US military is preparing for the day when China or any other nation or hacker group launches a full-bore cyberattack against the country's critical infrastructure through programs such as the Air Force's Cyberspace Command.

Information at Thieves' Fingertips
Times Union (06/05/08), L. Rulison

The New York State Cyber Security Conference recently hosted cyber security experts who demonstrated some of today's biggest cyber security threats. University at Albany professor S. Goel and a team of researchers demonstrated how easy it is to steal personal information off of "swipeless" credit cards by using small sensors, a laptop, and special software. "The lesson is that as we advance technology, we're creating new vulnerabilities we're not aware of," Goel says. One of the cards the team demonstrated on was the American Express Blue card, which features a RFID chip to enable quick swipeless payment. American Express spokeswoman M. Faust says the security measures used in the card and the company's payment system would make any information downloaded from the card useless. Other speakers at the convention discussed threats facing consumers, businesses, and government agencies in the age of wireless Internet and advanced computing technology. Keynote speaker P. Gray, a senior security strategist for Cisco Systems and a 20-year veteran of the FBI, says terrorists and nation states are constantly trying to attack the United States and government agencies through cyberspace. New York's cyber security office director W. Pelgrin says the threats range from international terrorists to teens trying to pull pranks, though such "pranks" could cause significant damage. "The amount of malicious activity out there is just getting louder and louder," Pelgrin says.

Secret Messages Could Be Hidden in Net Phone Calls
New Scientist (06/02/08), P. Marks

Polish information scientists are developing a system for hiding messages in Voice over Internet Protocol (VoIP) phone calls. W. Mazurczyk of the Institute of Telecommunications in Warsaw says it is possible to replace some of the voice data packets that someone is sending with a hidden message because VoIP uses the data transmission routine User Datagram Protocol (UDP). With UDP, packets are not guaranteed to arrive in the same order they were sent, and a voice message can survive if some go missing, which means there is an opportunity to embed a message. "We intentionally hold on to secret message packets for some time before sending them," Mazurczyk says of the "steganographic" system for VoIP networks. "This means when they are received they will not be treated as voice packets but as lost ones." Mazurczyk is working with K. Szczypiorski, and they hope to limit the number of packets needed to maintain audio quality, as degradation would suggest someone may be eavesdropping to pick up a message hidden in a call.

To Fight Cyberwars, Air Force Recruits Part-Time Geeks
Christian Science Monitor (06/05/08) P. 3; J. Lasker

The year-old Air Force Cyber Command (AFCYBER) is striving to recruit enough cyberwarriors to establish the United States' cyber supremacy. The Air Force is recruiting in new places and is relying heavily on the Air National Guard to find enough computer experts. For example, the 262nd Information Warfare Aggressor Squadron, an Air National Guard unit in Washington state, has recruited guardsmen that work at Microsoft, Adobe, and Cisco Systems. Meanwhile, the 177th Information Aggressor Squadron in Kansas draws from Sprint and Boeing. Air Force secretary M. Wynne says the military must capitalize on the talent and expertise of the Guard and Reserve members who may have direct ties and significant experience in the high-tech industry. In addition to recruiting experienced high-tech workers, the Air Force may make exceptions to their recruitment standards and accept ex-hackers who may have committed computer-related crimes or have a felony conviction for unlawfully cracking a network. The Air Force's focus on cyberwarfare is raising questions abroad over what will happen if the United States deploys offensive operations against foreign Web sites and systems. The Air Force has already hinted that it may use offensive tactics. "The pervasive nature of pro-jihad Web sites represents a tangible and highly visible example of how our adversaries use elements of cyberspace against us," Wynne says. "We cannot allow our adversaries to operate freely there." There are also questions surrounding the military's recruitment of IT professionals. Some worry that cyberwarriors from Cisco or Microsoft could use their inside knowledge of a company's product to help disable a foreign country or that back doors will be written into popular programs.

Researchers Look to Cut Quantum Cryptography Costs
eWeek (05/29/08), B. Prince

National Institute of Standards and Technology researchers are supporting a new method that will lower the cost of quantum key distribution. NIST researchers have outlined a technique called detection-time-bin-shift (DTBS), which is based on NIST's previously developed conventional fiber-based QKD system. DTBS uses time-division multiplexing of a single photon detector between two photon bases in a QKD system. The DTBS QKD system generates sifted keys at a rate of more than 1 Mbps with a quantum bit error rate of less than 2% over 1.1 kilometers of fiber. The researchers set up an optical component to make the diagonally polarized photons rotate another 45 degrees so they arrive later and in a separate time bin at the same detector than the horizontal/vertical polarized photons. This means that one pair of detectors can be used to record information from both kinds of polarized photons in succession, reducing the required number of detectors from four to two. In another protocol, called B92, the researchers were able to lower the number of necessary detectors from two to one. The researchers have gone a step further so that the most common polarization-based protocol, known as BB84, now requires one detector instead of four.

Tapping Computer Science for a More ACCURATE Vote
National Science Foundation (06/09/08), D. Cruikshank

A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE), created in 2005 with a $7.5 million grant from the National Science Foundation (NSF), is part of NSF's Computer and Information Science and Engineering directorate's CyberTrust program. ACCURATE project head and Johns Hopkins University professor Avi Rubin is an expert in information security who was drawn to ACCURATE by the challenges associated with improving voting technologies. He says that once the researchers started examining the issue from a scientific perspective, they discovered that a more holistic approach was needed to understand how computers, touch screens, and other technologies work together in elections. To accomplish this, ACCURATE unites experts from various academic fields to find areas that need additional research and to determine how to apply existing technology and research insights to voting systems. One tool that resulted from ACCURATE is AttackDog, which can examine more than 9,000 different ways a voting system can be attacked. The program contains assumptions about each kind of potential attack and countermeasure to create an attack tree. As new potential attack methods become apparent, AttackDog can be updated to consider new threats. Stanford University professor D. Dill, who developed AttackDog, says the program is an example of how ACCURATE uses computer science tools and techniques to help local officials improve the security of their elections.

Dartmouth Launches Network Security Study
Dartmouth News (06/10/08), S. Knapp

Dartmouth researchers are about to launch the Dartmouth Internet Security Testbed (DIST), a project that will study the school's wireless computer traffic to understand how it's being used and how to protect it. Dartmouth computer science professor and DIST principal investigator D. Kotz says the campus environment enables the researchers to examine live network activity at scale and in real time. DIST will develop and evaluate current sensing methods to monitor Dartmouth's multiple wireless networks. Kotz says DIST's scope and scale are unique within the academic research community, and that the project will improve network security technology and practices for all Internet users. For example, DIST could help detect unauthorized access points, which can be used to steal users' passwords. The study has been designed to protect the privacy of all campus network users. The researchers will not examine any of the content of wireless network traffic, and instead will view only the header information. The headers indicate the size and origin of the data, but not the type of data or anything about the contents of the communication. The identity of individual wireless devices will be replaced with random identifiers.

New Zealand Gov't Looks to Boost Confidence in E-voting
Computerworld New Zealand (06/06/08), S. Bell

New Zealand is considering allowing voters to cast electronic ballots up to 17 days before the general voting period and to re-vote if they have concerns over whether their selections were recorded correctly. The country's Chief Electoral Office has released the draft strategy document in an effort to boost confidence in the electronic voting system. New Zealand could conduct limited pilots for advance voting and re-voting electronically during the 2011 or 2014 elections, and the earliest general e-voting is likely to be offered is 2017. Still, "there will need to be a period of extensive public consultation, and policy and legal work in support of new legislation," says the Electoral Office in the strategy document. New Zealand could approach authentication through the government log-on service, which is being used for other government transactions. The strategy document says the potential for malfunctioning machines, a mass denial-of-service attack, and undue influence warrant taking a cautious approach.

'Net Engineer Argues Firewalls Are a Security Distraction
Computerworld Australia (05/30/08), S. Bell

The focus on firewalls has led corporate network experts to spend less time on security in the end system, says B. Carpenter, the former head of the Internet Engineering Task Force. Carpenter, currently a lecturer at the University of Auckland, discussed the history of the Internet as well as its challenges while giving the Institution of Engineering and Technology's annual Prestige lecture. During his "The Internet, where did it come from and where is it going?" address, Carpenter suggested that firewalls have lessened the momentum of end-to-end transparency for the Internet. He said the extended addressing scheme, IPv6, will replace the need for address translation, but Internet users are so used to conventional firewalls. There are some similarities between his view of end-to-end transfer of data and David Isenberg's concept of a "stupid" network, but he adds that the edge of today's complex networks might be difficult to define, which has also been suggested by Victoria University's John Hine. "The basic principle is still valid," Carpenter said. "It's not obvious that you will make money out of putting very complex services very deep in the network."