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

Δελτίο 107
27 Φλεβάρη 2008

Princeton Researchers Envision a More Secure Internet
Princeton University (02/15/08), T. Riordan

Some of Princeton's top brains have divergent ideas about fortifying the security of the Internet, with L. Peterson offering the Global Environment for Network Innovation (GENI) as a much-needed platform for investigating and validating potential security solutions. Peterson says GENI is particularly important as a tool that would allow the research community to significantly shape the Internet's future and counter industry's increasingly pervasive influence. He believes the network offers the optimum path for tackling the Internet's security challenges, arguing that "the network needs to be able to quarantine compromised machines so that we can limit their collateral damage." E. Felten, director of Princeton's Center for Information Technology Policy, focuses on short-term, high-impact research, and is convinced that many of the Internet's security problems can be traced to how technology is used rather than the technology itself. R. Lee, who heads the Princeton Architecture Lab for Multimedia and Security, stresses that security should be an element of system design, and wants to embed basic security features within hardware. Her lab has demonstrated that such an innovation can be accomplished without hiking up the hardware's power consumption or impacting its performance. Felten does not agree with Peterson and Lee's contention that online security can be adequately shored up by trust features incorporated into hardware or networks, while Princeton computer scientist and GENI participant J. Rexford sees advantages to approaches espoused by all three researchers. "GENI would really open up the intellectual space in thinking about the Internet," she says, even as she works on incremental security enhancements such as the improvement of routing protocols.

Friendly 'Worms' Could Spread Software Fixes
New Scientist (02/14/08), T. Simonite

Microsoft researchers are working to make it easier to distribute useful pieces of information such as software updates and patches by designing the updates to behave more like computer worms, spreading from computer to computer instead of having to be individually downloaded from a central server. The research used to develop such a technique may also help defend against malicious worms. Software worms spread by infecting a computer, self-replicating, and probing computers to find a new host. Microsoft research Milan Vojnovic says that method is inefficient because the worm wastes time exploring groups, or "subnets" of computers that contain few uninfected hosts. Vojnovic and his team have designed smarter strategies. The ideal approach would be to use prior knowledge of how uninfected computers are distributed on a subnet, but a company distributing a patch after a worm attack rarely has such extensive information. To compensate, the researchers have developed strategies that would allow their beneficial worms to learn from experience. A worm starts by contacting a potential new host, and after finding one uses a targeted approach to contact other computers on the same subnet. If the worm finds many uninfected hosts it stays on the subnet, but if most computers have already been updated, it switches subnets. Software patches that spread like worms could be faster and easier to distribute, and better countermeasures can be developed by understanding how malicious worms spread.

With Improvements, E-Voting Could Be Good, Says Researcher
CNet (02/16/08), R. Vamosi

Princeton graduate student J. Halderman discussed ways to improve e-voting machines during his keynote address at the ShmooCon computer hacker conference. Halderman said that direct-recording electronic (DRE) voting machines are essentially computers and are susceptible to the same problems, including viruses, bugs, and crashes. Halderman said the most troubling aspect of DRE machines is that a single person could launch an attack on all the voting machines in a county or state. During a study of Diebold DRE machines, Halderman found that the company provided potential attackers with an upgrade process that was easy to manipulate. Using a specific file name could allow a hacker to inject malicious code into one or more voting machines, and because the PCMIA card can be used to load a specific ballot within a precinct, county, or state, a single altered card could spread the infection to numerous machines. Halderman said that improvements to e-voting machines could make them reliable, which he said would please voters, since many prefer using them over paper-based systems. E-voting machines provide faster reporting, offer more accessibility to disabled voters, and allow for better and less-expensive vote auditing if paper receipts are added to the system.

Mistakes, Not Hackers, Are to Blame for Many Data-Security Glitches on Campuses, Report Says, Chronicle of Higher Education (02/12/08), J. Young

Hackers were not responsible for the increase in the number of colleges that reported computer-security incidents in 2007, according to a study conducted by A. Dodge, the assistant director for information security at Eastern Illinois University. The study, which analyzed reports on computer security by news and computer-security organizations, found that while the number of colleges that reported computer-security incidents rose from 65 in 2006 to 112 last year, the number of attacks committed by intruders remained essentially flat. Instead, the increase in the number of computer-security incidents at colleges was due to an increase in the number of mistakes made by college officials and an increase in the number of thefts of property, the study concluded. Dodge found that 49 colleges unintentionally released sensitive information in 2007, up from 20 the previous year. Meanwhile, 36 colleges reported 39 cases of theft of college computers or storage devices last year, up from 26 cases of theft at 24 institutions in 2006. E. Spafford, director of the Center for Education and Research in Information Assurance and Security at Purdue University, warned against drawing too many conclusions from the study, since it relies on other reports and has only been taken for two years. "Campus systems continue to be prized because of high bandwidth, number of systems (particularly student-owned), and collections of personal information of people with good credit histories," he says.

Replicating Virtual Servers Vulnerable to Attack
Network World (02/15/08), T. Greene

J. Oberheide, a PhD candidate at the University of Michigan, says there is a big security risk related to virtualization. He says that one of the most attractive features of virtualization--the ability to spontaneously replicate virtual servers in order to meet demand--increases the risk of attacks such as data theft and denial of service. Oberheide attributes this increased risk to the fact that authentication between machines is weak when a virtual machine moves from one physical server to another, and because virtual-machine traffic between physical machi-

nes is unencrypted. However, there are two solutions to these problems, Oberheide says. A short-term solution is to install hardware-based encryption on all the physical servers that might send or receive virtual machines, while a long-term solution is to incorporate strong authentication into virtual machine software. Oberheide has developed a proof-of-concept tool he used in a lab to launch man-in-the-middle attacks against virtual machines as they moved from one physical server to another. Nemertes Research analyst A. Antonopoulos says Oberheide's work is fascinating, and adds that virtual servers face much more basic challenges. "Our entire security infrastructure has been built around a static model, and as we're virtualizing everything else, the virtualization of security is lagging by a tremendous amount," he says. "That's causing real problems in architecture decisions today."

A Method for Stealing Critical Data
New York Times (02/22/08) P. C1; J. Markoff

Princeton University researchers have devised a unique and simple methodology for stealing encrypted information stored on computer hard disks. The technique involves literally freezing the computer's dynamic random access memory chips, which have been demonstrated to retain data for seconds or even minutes after power has been cut off. The data, like the chips, is frozen in place by chilled air, allowing the keys to be read by the researchers using pattern-recognition software. Princeton computer scientist E. Felten wrote in a Web posting that the application of liquid nitrogen to the chips allows them to retain their data for hours without power. He noted that this breakthrough "is pretty serious to the extent people are relying on file protection." The experiment offers clear proof that Trusted Computing hardware does not apparently halt potential intrusions, the researchers said. They said they employed special utilities in the Windows, Macintosh, and Linux operating systems to compromise encrypted data, and reported that they started probing the utilities for vulnerabilities last fall after noting a reference to the persistence of data in memory in a 2005 technical paper authored by Stanford computer scientists. "This is just another example of how things aren't quite what they seem when people tell you things are secure," says SRI International researcher P. Neumann.

Securing Cyberspace Among Top Technological Challenges of 21st Century, Panel Says
Network World (02/19/08)

Securing cyberspace was recently named as one of the top 14 technical challenges for this century by a National Academy of Engineering panel. The panel said that electronic computing and communication contain some of the most complex challenges engineering has ever faced, including ensuring the confidentiality and integrity of transmitted information, deterring identity theft, and preventing electronic terrorist attacks that could disable transportation, communication, and power grids. The panel noted that serious breaches of security in financial and military computer systems have already taken place, and that identity theft is a growing problem, but research and development in security systems has not progressed much beyond a strategy amounting to fixing problems and cobbling together security patches after vulnerabilities are discovered. Other great technological challenges the panel identified include advancing health care informatics, improving virtual reality, engineering better medicine, and preventing nuclear terror. The National Science Foundation agrees with the panel and cited cybersecurity as an area it wants the United States to invest more resources in.

Black Hat Conference: Experts Develop Cybersecurity Recommendations for Next President, InformationWeek (02/20/08), N. Hoover

Members of the recently convened Cyber Commission for the 44th President discussed the goals of the panel during the recent Black Hat security conference in Washington. The commission will spend the next nine months coming up with recommendations for creating a national cybersecurity policy. "This is one of the central issues for national security and we want to make sure it doesn't go away," says J. Lewis, director of the technology and public policy program for the Center for Strategic and International Studies, which supports the panel. The commission is not a government-mandated commission, but its membership, which includes two sitting members of Congress and J. Dixon, former executive director of the National Cyber Security Division at the Dept. of Homeland Security, could give the panel some clout. The panel plans to focus on defining a clear command and control structure for federal cybersecurity, standardizing technology procurement procedures across federal agencies, and determining the research and development agenda.

Scientists Demand an Ethical Education in Computer Engineering
Innovations Report (02/21/08), F. Flores

Computer engineers could become the depersonalized tools of other parties if they do not receive a solid ethical education, concludes a new report from researchers at Carlos III University of Madrid (UC3M). Ethics is ultimately about personal freedom because it guides computer engineers along their destiny of personal growth as they find new ways to bring good into the world, suggests study co-author M. Gonzalez from the Complutense University of Madrid. The discussion of ethics in information technology essentially involves the differing ideas of consequentialism (that good actions are determined by the consequences) and deontologism (that right or wrong is independent of the consequences). The researchers studied the different ethics systems and came up with a model, "moderate deontologism," or rational behavior based on rules and consequences. The most correct ethical position takes the conesquences of actions into consideration while recognizing the barriers necessary for respecting human dignity. UC3M will take a cross-sectional approach to professional ethics for new computer engineering degrees offered in the incoming academic year. G. Genova, another study co-author, says that "the subject is important enough to warrant specific intellectual and rigorous treatment."

Researchers Say Sharing Is the Key to Privacy for EPC Tags
RFID Journal (02/14/08), M. O'Connor

ThingMagic's Advanced Development Group cofounder and head R. Pappu, RSA Laboratories principal research scientist A. Juels, and Carnegie Mellon university graduate student B. Parno have published a paper describing a process that can protect RFID tag data and address consumer privacy concerns without sabotaging existing efforts to integrate RFID throughout the supply chain. The process is based on threshold or secret-sharing cryptography, which uses a secret key to encrypt a number, then divides that key into multiple pieces. Anyone attempting decryption must collect a certain number of those pieces to figure out the key. The researchers call their technique privacy-through-dispersion. For example, when a product is first manufactured, it is given an electronic product code (EPC) and packed along with numerous identical products. At a distribution center, the pallet is broken down, and a single case containing the product, which is still in close proximity to several identical products, is sent to a store location. At the store, the product is stored or shelved with identical products, but when a consumer picks up the product, it is removed from the presence of the other identical products and loses its ability to be scanned because not enough pieces of the key are present.

Pappu and Juels plan to arrange the first real-world tests of privacy-through-dispersion using pharmaceutical products in a closed-loop supply chain.

DNS Inventor Warns of Next Big Threat
Dark Reading (02/11/08), K. Higgins

At the Network and Distributed System Security Symposium, researchers from Google and Georgia Tech presented their study on DNS resolution path corruption and malicious alteration of DNS answers. The new DNS attacks consist of DNS servers manipulated by hackers that redirect unsuspecting users to malicious sites. Georgia Tech's D. Dagon, C. Lee and W. Lee, and Google's N. Provos documented roughly 17 million open-recursive DNS servers, finding that nearly 70,000 were conducting malware-based operations through DNS queries. While DNS entries can be rewritten to prevent malicious sites, hackers have joined the ranks of security experts in infecting DNS resolution paths via viruses or malicious URLs. "Companies are rewriting DNS answers, ideally to improve the user experience, but also to expose the users to ads," says Dagon. "But DNS vendors aren't the only ones commercializing the alteration of DNS traffic. Malware authors also use this technique to exploit victims." Researchers say the modification of DNS answers still needed to be thoroughly explored, but DNS inventor P. Mockapetris warns it is only a matter of time before DNS attacks result in sizeable losses. Mockapetris says users connecting through public wireless ports are at risk for hackers' manipulated DNS servers, adding that successful DNS attacks could cost enterprises up to $100 million.