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

Δελτίο 33
14 Ιουλίου 2006

Software Tools Detect Bugs by Inferring Programmer's Intentions
University of Illinois at Urbana-Champaign (07/06/06), J. Kloeppel

University of Illinois computer science professor Y. Zhou and her students have developed a suite of tools can that identify and correct software bugs by inferring the intentions of the programmer. The tools work by making observations of how the programmer writes code. "Most bug-detection tools require reproduction of bugs during execution," Zhou said. "The program is slowed down significantly and monitored by these tools, which watch for certain types of behavior. Most of our tools, however, work by only examining the source code for defects, requiring little effort from the programmers." Code in large programs is often copied and pasted, which, while saving a significant amount of time, is a frequent cause of bugs. Using data mining techniques, Zhou's CP-Miner searches through programs for copy-pasted code and scans for consistent modifications. CP-Miner, which can scan 3 million to 4 million lines of code in less than 30 minutes, has already found numerous bugs in some of the most popular open-source applications. Since large programs often rely on implicit rules and assumptions, Zhou and her students developed the PR-Miner tool to determine when those rules have been broken. Like CP-Miner, PR-Miner uses data-mining techniques and works very quickly. Zhou and her students have also developed tools to help software keep running even in the presence of bugs, such as the Rx recovery tool. Zhou says, "Rx is avoidance therapy for software failure. If the software fails, Rx rolls the program back to a recent checkpoint, and re-executes the program in a modified environment." Another tool, Triage, identifies and diagnoses the nature of a failure at the end-user site and helps the programmer work to correct it.

DHS Outlines Plan to Protect Critical Telecommunications Infrastructure
RCR Wireless News (07/05/06), H. F. Weaver

The federal Department of Homeland Security has released the National Infrastructure Protection Plan (NIPP) designed to protect US critical infrastructure, including IT and communications networks. Key to the plan will be a risk-management approach that tailors protection according to the characteristics of individual sectors. Each sector has been assigned to a specific department, and essential to the plan will be cooperation from private companies, including the sharing of sometimes confidential information. "The National Infrastructure Protection Plan is the path forward on building and enhancing protective measures for the critical-infrastructure assets and cyber systems that sustain commerce and communities throughout the United States," says Homeland undersecretary for preparedness G. Foresman. "The NIPP formalizes and strengthens existing critical-infrastructure partnerships and creates the baseline for how the public and private sectors will work together to build a safer, more secure and resilient America."

Concerns About Fraud Continue to Plague Users of Electronic Voting Machines
Computerworld (07/03/06), M. Songini

A new report warns of vulnerabilities in e-voting machines that could disrupt upcoming elections unless precautions are taken. The report was compiled over 18 months by a task force of computer scientists and voting machine experts set up by the Brennan Center for Justice at the New York University School of Law. In recent years, half of manual voting machines throughout the country have been replaced by e-voting systems, such as touch-screen and optical-scan machines, notes L. Norden, a Brennan Center attorney and chairman of the task force. Election officials have turned to electronic systems to comply with federal requirements, though Norden said security procedures have not necessarily kept pace with the technology. The report identified 120 potential e-voting threats, noting the absence of a detection system for malicious software attacks in most states. Critics of e-voting security include I. Sancho, elections supervisor for Leon County, Fla., who said the report confirms his gravest fears, but others are less convinced. "The fundamental premise of the Brennan report and many activists is that it's easy to rig a machine to throw an election," said M. Shamos, a professor at Carnegie Mellon University. "It isn't." The report calls for elections officials to remove wireless components, randomly audit paper records, and decentralize the administration and programming of the machines. Norden said there is still time to implement these precautions before the November elections, and every secretary of state in the country is receiving a copy of the report.

FBI Plans New Net-Tapping Push
CNet (07/07/06), D. McCullagh

Sen. M. DeWine (R-Ohio) intends to introduce legislation that would make it a requirement for ISPs to set up wiretapping hubs for law enforcement monitoring and for networking equipment manufacturers to incorporate backdoors for surveillance, according to FBI agent B. Smith in a private conference with industry representatives on July 7. DeWine's bill would amend the 1994 Communications Assistance for Law Enforcement Act (CALEA) to the effect that any maker of "routing" and "addressing" hardware would be required to offer upgrades or other "modifications" necessary to the enablement of Internet wiretapping; extend wiretapping requirements to "commercial" Internet services if the FCC believes it to be within the "public interest;" coerce ISPs to filter their customers' communications to spot, for example, voice over Internet Protocol (VoIP) calls only; and jettison the current legal requirement that Justice must annually issue a public "notice of the actual number of communications interceptions" as well as the "maximum capacity" needed to handle all the legally authorized wiretaps that federal agencies will "conduct and use simultaneously." The FBI says CALEA must be expanded in order to beat terrorists and other criminals who are exploiting technologies such as VoIP. "The complexity and variety of communications technologies have dramatically increased in recent years, and the lawful intercept capabilities of the federal, state and local law enforcement community have been under continual stress, and in many cases have decreased or become impossible," states a summary accompanying the draft bill. However, critics say the legislation infringes on Internet users' privacy, while the bill's political outlook is also muddied by continued debate concerning supposedly unlawful eavesdropping by the National Security Administration.

Seeking to Tighten the Net Against Attack
IST Results (07/10/06)

In an effort to shore up the Internet's defenses against cyberattacks in a time of rapid broadband uptake, the IST-funded DIADEM Firewall project has created a comprehensive security application for broadband services, with particular emphasis on denial-of-service attacks and

mitigating the effects of an attack. Distributed denial-of-service (DDoS) attacks, which overwhelm the target network by marshalling thousands of zombie computers to make simultaneous requests of the network's bandwidth, affected more than 13% of businesses in the United Kingdom in 2004. DDoS attacks can impose severe customer service costs on broadband service providers, as well as disrupting the broadband experience for residential users. "There is no doubt that denial-of-service attacks are a growing issue as more and more services, such as online games, IP telephony, television over IP, and e-shopping are provided to broadband users through the Internet," said Y. Carlinet, DIADEM Firewall project coordinator. "It is a crucial and vulnerable aspect of broadband security and will become even more so in the future as more users move over to broadband connections." The project created a network-based distributed detection and reaction system to be managed centrally by network operators, unlike the current system, where each user is responsible for his own security. In shifting the burden of security back to the network provider, the DIADEM Firewall project developed new intrusion-detection algorithms and policy-based techniques that enable automated configuration and decision making. The main difficulty that the project encountered has been to convince the major network operators that they need to take responsibility for security through centrally administered policies.

DHS Lags in Appointing Cybersecurity Czar
National Journal's Technology Daily (07/05/06), H. Greenfield

Nearly a year has passed since Homeland Security Department (DHS) Secretary Michael Chertoff created the position of a Cabinet-level cybersecurity czar in an effort to make sure the department can address possible past and emerging threats in the best way possible. The position has yet to be filled since it was first announced on July 13, 2005. The effort to appoint someone to the position started two years ago in Congress. Some see this as indicative of the lack of attention that exists in most senior levels of government. "The department is incompetent," says Rep. Z. Lofgren (D-Calif.). "When you say no one is home [at Homeland Security] it's not a joke." Lofgren, along with a House cybersecurity subcommittee, helped pass House legislation that would create a cybersecurity czar with authority in Homeland Security. Now many members of Congress and other groups are starting to question whether DHS National Cyber Security Division director A. Purdy can effectively manage the Internet in a disaster situation. "What we concluded is if there were a major cyber disruption, our nation would not be able to restore or rebuild the Internet," says T. Freeman at the Business Roundtable. "Our CEOs feel that the Internet is vital to the exchange of information that's vital to our nation's economic security and to our security in general." Lofgren says there needs to be a cybersecurity czar present at Cabinet meetings to successfully rebuild the Internet if a cyber disruption does occur.

DOE's Federated Model Aims to Identify Security Threats
Network World (07/05/06) Garretson, Cara

Last fall, Argonne National Laboratory started the Federated Model, an information-sharing project to be used by government, research labs, universities, and organizations that want to share or view information on different attempts by IP addresses to access networks and how organizations have dealt with the attempts. The Federated Model has about a half-dozen members and is steadily growing. The lab, a division of the Department of Energy (DOE), is trying to add features to the project such as an RSS feed that notifies members when new information has been added, according to S. Pinkerton, manager of network services for the lab, which operates out of the University of Chicago. Members will eventually be able to

stop an attack by following the examples and actions of fellow members. If a member of the Federated Model is the victim of an attack from a particular IP address, then another member will be able to block that IP address from the network. "We're reinforcing the idea that we could be smarter, and more prepared," says Pinkerton.

Election Corrections
US News & World Report (07/09/06), S. Brush

Nearly six years after the disastrous 2000 election, and four years after the passage of the Help America Vote Act (HAVA), significant problems remain in the nation's voting systems, despite the expenditure of billions of dollars to replace outdated equipment. "We've made some substantial progress," said House Minority W. Hoyer (D-Md.), who co-sponsored the 2002 election reform law, "but there is a lot left to be done." Much of the $3.8 billion earmarked under HAVA went to replace lever and punch-card machines, though $800 million has yet to be appropriated. Thanks to the new systems, around 1 million votes were recorded in 2004 that would not have been counted in 2000, the Caltech/MIT Voting Technology Project found. While the improvements may be cause for celebration, the security flaws that have accompanied the new machines have touched off a fierce debate among lawmakers, election officials, and security experts. In at least seven states, activists have filed lawsuits to block the use of e-voting machines that do not produce a verifiable paper trail. With the passage of legislation requiring voter-verified paper trails, 26 states have tried to put security concerns to rest, though a recent study by the Brennan Center for Justice at New York University found that the three most commonly used systems are vulnerable to more than 120 security threats, such as implanting malicious software in a machine via a wireless device. Another HAVA provision, the creation of statewide voter databases to ensure that no eligible voters are left off the registration lists, has taken a backseat to the security debate, though it too has turned out to be costly and time-consuming to implement. The absence of national oversight of the election process is also troubling, as the US Election Assistance Commission, created under HAVA, is still struggling to solidify its funding and authority.

Trust in Global Computing
IST Results (07/12/06)

The same security concerns that plague the Internet also threaten to undermine the promise that access to distributed mobile resources holds for global computing. To shore up global-computing resources, researchers working under the MYTHS project have developed "type-based" theories that express an unvarying aspect of a program or code. "Your piece of software, alone and out there in the wild, doesn't know who to trust and who not!" says project coordinator V. Sassone. "That is why closed networks exist. In a global computing environment you do not have the reassurance of a closed network--you are dealing with agents that you cannot trust." Software agents face their greatest challenge in environments where they have limited information--environments where other agents might not be trustworthy. Improved security will be essential for the ongoing development of the Internet and agent-based services. Domains will have to restrict agents' access, while agents themselves will need to guard against attacks. Type-based security can be verified simply by inspecting the code, while in other applications the programs must actually be executed to ensure security, according to Sassone. The MYTHS researchers concentrated on the fundamental aspects of programming languages and the core elements that enable static detection of security violations. The team developed methods to control resource access, conduct crypto-protocol analysis, and manipulate XML data.

WPI to Host Gathering of Indoor Personnel Location and Tracking Experts
Worcester Polytechnic Institute (07/07/06)

Early next month, Worcester Polytechnic Institute will host a conference for researchers in the emerging field of indoor personnel location and tracking. Indoor positioning tracking has proved a unique challenge, as the signals from GPS satellites, though capable of pinpointing one's location to within a few feet, have trouble inside buildings, where their accuracy is degraded by bouncing off walls and other surfaces. The WPI's personnel location and tracking research group is developing radio and radar technology to determine the location of first responders inside buildings. The participants in the August workshop will include representtatives from private industry, academia, and government agencies. Among the technological solutions the workshop attendees are investigating are enhanced GPS, inertial navigation and dead reckoning, which tracks direction and distance using gyroscopes and accelerometers, and RFID, though each technology has its drawbacks. Enhanced GPS, which augments GPS satellite signals with other positioning information, such as cell phone towers, has yet to achieve the level of accuracy required by first responders. The gyroscopes used in inertial navigation must be frequently realigned. RFID applications can only be used inside buildings that have preinstalled monitoring stations. The WPI research group is developing an alternative system that exploits the principles of orthogonal frequency division multiplexing (OFDM), which relays high-speed data over both wired and wireless channels, and integrates into the radio spectrum. First responders would wear transmitters that continuously emit OFDM signals, while vehicles surrounding the building would be equipped with receivers to detect and decipher the signals through complex, custom-made algorithms.

The Plot to Hijack Your Computer
BusinessWeek (07/17/06), No. 3993, P. 40; B. Elgin; B. Grow

IT-Harvest estimates that spyware accounts for 11% of all Internet ad business, but its method of attracting business--by surreptitiously installing advertising programs, which then cause pop-ups to appear on the screen and inhibit, even cripple, the computer's performance--has engendered a great deal of public scorn and triggered a lawsuit by New York Attorney General Elliot Spitzer against one spyware company for false advertising, trespassing, and computer tampering. It is feared that spyware and its practitioners could seriously, perhaps irreparably tarnish the online ad industry. Critics charge that the people who run spyware companies--one of the most infamous being Direct Revenue, which Spitzer's lawsuit targets--are greedy opportunists who cynically exploit consumers, as demonstrated by widescale ignorance of consumer complaints. Spitzer says he discovered instances in which Direct Revenue spyware was downloaded with misleading user agreements or a complete lack of disclosure. Though Direct Revenue has made reforms, notably dropping its most devastating spyware programs, as verified by computer security firms and anti-spyware activists, the company is still considered to be the root cause of many irritations. Trend Micro spyware research manager A. Arnott reports that Direct Revenue is still rated by the public to be one of the 10 most-despised spyware firms. Savvy consumers can lower the risk of their systems getting infected by spyware by using widely available security software and avoiding online offers of free products.