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

Δελτίο 123
13 Ιουλίου 2008

Flaws in Medical Coding Can Kill
Baltimore Sun (06/30/08) P. 1A; J. Rockoff

Microprocessors are increasingly being used in a variety of medical devices, and potential software errors in those devices are becoming a growing concern. Poor design and manufacturing, the traditional causes for device malfunction, are being replaced by erroneous computer code, and the impact of faulty code is becoming increasingly dangerous as automation technology enables doctors and nurses to spend less time monitoring machines. "The world of technology is allowing us to do things we never thought possible, and it's largely a great advance," says L. Kessler, director of the Food and Drug Administration's (FDA) Office of Science and Engineering Laboratories. "Where it gets to be scary is, we used to have more human intervention. With software doing more now, we need to have a lower tolerance for mistakes." Manufacturers test and inspect their products' software before putting the devices on the market, but they have been slow to follow the FDA's example of adopting new forensic technology because it is costly and still evolving. Consequently, the FDA is gathering evidence to show software companies the value of forensic testing. Finding a deadly flaw in medical software source code is an extremely complicated process, and computer scientists say traditional software checks are not good enough to find every mistake. The FDA's forensic software unit was launched in 2004, and now includes about 10 mathematicians, computer scientists, and a physicist. In 2006, after talking with computer scientists at North Carolina State University, the unit began using static analysis to uncover code errors. Static analyzers are also being used automakers, Microsoft, and other federal agencies.

Cisco, IBM, Intel, Juniper and Microsoft Fight Cyber Terror Together
Network World (06/27/08), T. Greene

Cisco, IBM, Intel, Juniper, and Microsoft have formed the Industry Consortium for Advancement of Security on the Internet (ICASI) in an effort to respond faster to "global, multivendor cyber threats." Such attacks have a wider impact because they target multiple products or protocols in products, and they pose problems for both end users and vendors. The forum will serve as a platform that encourages members to share critical data about specific attacks more readily. ICASI plans to improve practices for addressing multi-product security threats, and set security response standards that it can share with the rest of the industry. "To date there has not been a trusted vendor environment that allows companies to identify, assess, and mitigate multi-product, global security challenges together on the customers' behalf," the group said in a statement. "ICASI aims to fill this void."

Q&A: E-Voting Activist More Optimistic About This Year's Voting Systems
Computerworld (07/03/08), T. Weiss

Johns Hopkins University professor A. Rubin says in an interview that the kinds of e-voting problems activists are concerned about are the kinds of things "that don't necessarily have a noticeable manifestation." He says what is required is "a system that accommodates the ability to audit to be sure that the machines got the right result." He believes that safe, reliable,

and secure e-voting systems can be built by technology companies, and he cites the National Institute of Standards and Technology's recommendation of designing voting systems where a software failure does not have any possible effect on the election's integrity and accuracy. Rubin says the easiest route to software independence is designing a system that uses a paper ballot, while another option, currently in the research phase, is cryptography, which he thinks will ultimately be able to supplant paper. "I think if you take a different psychology, a different philosophy toward building systems, where you say we're going to use software as much as we can but we're not going to rely on it for security, you will actually design a pretty good voting system," Rubin says. He notes that the state of voting is much better than it was in November 2000, pointing out that most states have switched to paper records. Rubin believes most systems that employ paper ballots or optical scanning are likely to be software-independent.

Spying Has Few Legal Checks
Baltimore Sun (07/07/08) P. 1A; B. Olson

US citizens' communications, travel patterns, and spending habits are being monitored and analyzed for suspicious activity by domestic surveillance programs run by federal intelligence and law enforcement agencies, and these programs have few legal restrictions. Although protecting Americans' privacy is the goal of provisions contained in pending amendments to the Foreign Intelligence Surveillance Act, there is little oversight for surveillance programs that fall outside the bounds of FISA. Critics say the safeguards are not infallible, while Congress has often held back funding for surveillance programs because it is dissatisfied with the information the administration has provided about the programs. Such was the reasoning behind the House Appropriations Committee's recent decision to stall funding for an initiative by the National Applications Office to use American satellites for domestic purposes until August, when the Government Accountability Office will issue a report about how the program will address civil liberties and privacy concerns. Lawmakers say even in instances where Congress has received information about surveillance programs, their questions or concerns are frequently handled by the agency responsible for surveillance, which adds up to self-policing. Partially to address concerns about privacy, the Homeland Security Department has set up a privacy czar to guarantee that the technologies and programs initiated by the agency do not violate civil liberties or chip away at privacy laws, but some believe the position should be expanded to a Cabinet-level post in the executive branch. "We should have what Canada has, which is a minister of privacy, someone looking out for the privacy issues of Americans," says intelligence expert J. Bamford. "We have armies of people out there trying to pick into everyone's private life, but we have nobody out there who's an advocate."

UK Scientists Demo Graphic Passwords
CNet (07/01/08), C. Lombardi

The developers of the Background Draw-a-Secret (BDAS) software are showing off the graphic passcode system this week in London at the Royal Society Summer Science Exhibition. With BDAS, users scribble an image, rather than enter a letter/number combination. Users choose from a selection of base images, which will be visually overlaid with a grid, then "trace" the image on a touch screen. The unique drawing of the image becomes the passcode, and the chosen image will appear each time as the passcode prompt. Users doodle over the chosen image to get in, but their drawings do not have to exactly match the original sketch. "Studies have shown that people find it easier to remember images than words or numbers and our system has proven over 1,000 times more secure than people's normal passwords,"

says BDAS co-developer J. Yan, a computer science lecturer at the School of Computing Science at Newcastle University. He says the subjective nature of drawings makes graphic passcodes more secure, and the system is secure enough to be used for cash machines, computers, and mobile devices.

A Tax on Buggy Software
Forbes (06/26/08), A. Greenberg

D. Rice, an instructor at the SANS Institute and a former cryptographer for the National Security Agency and NASA, has published "Geekonomics: The Real Cost of Insecure Software," a new book that criticizes the software industry for its careless attitude toward security. Rice says the total economic cost of software security flaws is about $180 billion a year. Rice suggests creating a tax on software based on the number and severity of security bugs, even if the cost gets passed on to consumers, in order to hold software manufacturers accountable. He says hackers simply use tests to discover flaws in the software, which software publishers could do before hackers have access to the programs. The software companies control how much testing they do before programs are released, Rice says, and they do not have the right incentives to do the testing necessary to create secure software. He says the tax model would solve software problems in the same way that taxes help curb pollution from manufacturing. Rather than trying to stop manufacturing or prohibiting pollution, companies are taxed for the amount of pollution they create, motivating them to reduce emissions. Rice says software vulnerabilities, like pollution, are inevitable, so instead of requiring software to be secure, tax insecurities and allow the market to determine the price it is willing to pay for vulnerabilities in software. Software manufacturers who are the most insecure will pay the most. The tax will also create a system, similar to the safety star-rating system used for cars, to help consumers know what software is the most secure.

Major DNS Flaw Could Disrupt the Internet
Network World (07/08/08), E. Messmer

Security researcher D. Kaminsky has discovered a fundamental flaw in the Domain Name System (DNS) protocol that could allow an attacker to massively disrupt the Internet, causing CERT to issue an alert and major DNS software vendors to issue patches. Kaminsky says this is the first time such a coordinated multi-vendor synchronized patch release has ever been executed. Not applying the patch to the ISP infrastructure would allow a hacker to attack an ISP and redirect traffic however they wanted, Kaminsky says. Both current and older versions of DNS may be vulnerable, although patches may not be available for older DNS software. Kaminsky says the problem centers around a lack of sufficient port randomization related to the transaction ID of a query, but he is waiting to further discuss the vulnerability until most DNS patching has been completed. Kaminsky found the problem by accident about six months ago, and organized an industry-wide response that culminated in 16 researchers meeting at the Microsoft campus in late March to fix the problem. CERT Coordination Center's A. Manion says ISPs have been informed and several government agencies are working closely with CERT to correct the DNS flaw. Kaminsky says the DNS patch upgrade should go smoothly, but there is the potential that if the DNS patch is not applied correctly people could experience a "sudden outage."

Electronic Path to Bridge Safety
The Australian (Australia) (07/01/08), J. Foreshew

Australian researchers are developing bridge management software that uses an artificial neural network to predict the safety of 10,000 bridges in Queensland, Australia. Griffith University's M. Blumenstein says the artificial intelligence (AI) technologies used in the system will improve maintenance strategies and minimize costs. "We are trying to incorporate our technology into a bridge management system for the purpose of assisting predictions of bridge deterioration, inspection, and maintenance," Blumenstein says. He says the technology could save between 10-2% on bridge maintenance costs. The software uses the artificial neural network to learn from the historical performance of a bridge and predict future problems. The system can reconstruct the past by generating missing historical performance data on older bridges. "We are taking data that is available from inspection records and we are using that to back-predict and fill in the gaps to produce a larger historical record so we can predict future deterioration issues for bridges," Blumenstein says. The AI technologies are used in conjunction with routine inspections to generate data that fills in the large missing gaps between inspections. The goal is to be able to input variables such as bridge location, construction and material type, weather conditions, and traffic volume and predict the structural condition of the bridge. The researchers have tested the system using data from Maryland's Dept. of Transportation in the United States.

Identity Problems
National Journal (07/05/08) Vol. 40, No. 27, P. 22; E. Carney

Outfitting virtually all US citizens with fraud-resistant ID has proven to be a major challenge from a practical as well as emotional point of view, with a multitude of technical, legislative, administrative, and ethical obstacles impeding progress. Events and trends fueling the drive for more reliable IDs include the 9/11 terrorist attacks, the push to deter illegal immigration, credit-driven commerce, the threat of identity theft, and technological innovations in identity verification methods. A sore point among various parties is the Real ID Act, which has come under fire for being passed without public debate or hearings, and for receiving inadequate federal funding. Real ID sets up federal standards for issuing driver's licenses, and dictates that states must link their databases in order to enforce the law's prohibition on drivers holding licenses from multiple states, which critics warn would create an irresistible target for hackers and ID thieves. Some experts believe a national, biometric ID card is the solution. "Right now, we are proceeding in hundreds of different ways, for dozens of different ID, at tremendous expense," says R. Pastor, co-director of American University's Center for Democracy and Election Management. Privacy experts favor a scheme in which Americans carry multiple smart cards with different applications, arguing that a single ID would reduce Americans' security. "Uniformity in IDs across the country would create economies of scale" for snoops and could help bring about a surveillance society, warns the Cato Institute's J. Harper.

Study: Electronic Voting Increased Counting Errors in France
IDG News Service (07/09/08), P. Sayer

Polling stations using electronic-voting systems in four recent French elections suffered from more voting discrepancies than polling stations that used traditional paper ballots, concludes a new study. University of Nantes researcher Chantal Enguehard examined the discrepancies between the number of electors who signed the electoral register to confirm that they voted and the number of votes subsequently counted for each polling station. The study compared discrepancies from the 6,427 electronic-voting stations and the 14,624 paper-ballot voting stations used in both rounds of the 2007 presidential election and two subsequent elections. There were discrepancies between the number of signatures and the number of votes in about

19.8% of electronic-voting machines, compared to only 5.3% with paper-ballot voting stations. Also, the discrepancies were larger with electronic-voting machines. Enguehard says it is unlikely that voters' unfamiliarity with the machines is the cause for two reasons. First, the ratio of discrepancies between electronic and traditional stations got worse, not better, with time, and there was no correlation between the bureaus with discrepancies and the bureaus that received the most complaints about difficulties with the voting machines.

Senate Grapples With Web Privacy Issues
Washington Post (07/10/08) P. D3; P. Whoriskey

Despite support from leading technology companies and frequent consumer complaints, Congress has been unable to pass Internet privacy legislation. Following a two-hour Senate committee hearing on July 9 on Internet advertising and privacy, Sen. B. Dorgan (D-N.D.), who led the discussion, said the hearing primarily served to emphasize how little legislators understand about the subject. The hearing was called in response to fears that the massive volume of information that Internet companies are collecting on users is violating their privacy. The practice of assembling profiles on users to determine personal preferences and activities has been going on for years, but as Web sites have increasingly been united in large ad networks, the various profiles kept by smaller sites have been combined to create more detailed and widespread user profiles. Over the past year, some Internet Service Providers (ISP) have been experimenting with a practice that would provide even more detailed profiles, using a technology called deep packet inspection, which allows them to examine streams of data coming from a user's Internet connection. Critics of deep packet inspection compare the practice to wiretapping. At the hearing, representatives from companies that provide deep packet inspection services to ISP assured the panel that they were doing their best to preserve privacy. Experts say that before Congress can pass privacy legislation it must first decide what constitutes personally identifiable information, whether a person's Internet address should be considered private, should people be informed about data collection practices, and should users be allowed to see profiles compiled about them.