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

Δελτίο 24
12 Μάη 2006

Data Breach Notification Law Unlikely This Year
IDG News Service (05/05/06), G. Gross

While Congress seemed poised to work swiftly to pass a data breach notification bill after the highly publicized security failures in the first half of 2005, such legislation now appears unlikely to materialize before this year's session expires. There have been more than 10 bills introduced since 2005 addressing when companies are required to notify their customers in the event of a data breach that could compromise sensitive personal information and whether consumers should be allowed to freeze their credit scores in the wake of such a breach. In addition to the conflicting provisions of the different proposals, five congressional committees have asserted jurisdiction over the legislation. Two bills have emerged from committee in the Senate and are awaiting debate on the floor and two more are pending on the House floor. The Senate and House are looking to adjourn for the year on October 6 to give legislators a month to campaign for the November elections, and they will both be out of session for most of August. The remainder of their time will most likely be focused on hot-button issues such as immigration and rising gas prices. The future of the bills remains uncertain despite bipartisan support for the issue, said J. Assey, a Democratic counsel in the Senate Commerce, Science, and Transportation Committee. "It's unclear what Congress will do," he said at an ACM conference. "Going into the next Congress, I fell certain these issues will return." One of the most contentious points in the debate is what should trigger a notification requirement, given that companies will have an obvious incentive to downplay the severity of a breach to their customers.

RFID: Beyond the Drive for Five
Design News (04/24/06) Vol. 61, No. 6, P. 48; C. Murray

Although radio-frequency identification (RFID) tags have not yet reached the much-desired nickel price point, the tremendous strides the technology has made in terms of cost and performance should not be discounted. The price of RFID chips has been falling about 5% to 10% a year for the past six years, concurrent with technological improvements; RFID tags are being used in applications that were unheard of 10 years ago, regardless of the failure to cut their price down to five cents a unit. RFID tags are expected to be incorporated into low-cost everyday objects, which will eventually lead to an "Internet of things" wherein virtually everything is networked through the Web, predict researchers. The Internet of things cannot be realized without low-cost RFID tags, but researchers anticipate that everyday items will include RFID via integration into the corrugate of cardboard boxes during manufacture. Ongoing initiatives in this area will play a vital role in reducing the price of RFID, because it removes the need for certain tag components. Price is still one of the few advantages bar codes have over RFID tags, which is why efforts to drive the tag cost down to five cents are still going strong. Among the techniques RFID chip makers are employing to lower costs is "self-adaptive silicon," which generates special transistors featuring gates that can store bits of memory. S. Sarma, associate professor of mechanical engineering at MIT and research director for MIT's Auto-ID Center, says, "These RFID technologies will co-exist with the bar code for a long time into the future. But they will provide information that a bar code can't...The question now is the tipping point. When do you get to the percentage that causes you to say, 'I'm going to put the tag inside the corrugate?' In the next year, we could see it happen."

Voting Glitch Said to Be 'Disastrous'
Inside Bay Area (CA) (05/10/06), I. Hoffman

A recently discovered vulnerability in Diebold's touch-screen voting machines has election officials scrambling to understand and contain the risk. A hacker with minimal specialized knowledge of Diebold's system and an off-the-shelf component could load software onto the machine to disable it or alter vote counts in a matter of minutes. "This one is worse than any of the others I've seen. It's more fundamental," said D. Jones, a University of Iowa computer scientist. "In the other ones, we've been arguing about the security of the locks on the front door," he said. "Now we find there's no back door. This is the kind of thing where if the states don't get out in front of the hackers, there's a real threat." Finnish computer expert H. Hursti discovered the flaw while working with Black Box Voting in March, and quietly spread word of the glitch to several prominent computer scientists who advise states on voting machines. Pennsylvania, California, and Iowa have directed their election officials to seal the machines with tamper-proof tape until election day, though California advised its counties that intend to use only Diebold machines in their upcoming elections that the threat is low, and that tampering would be easily detected by voters from the paper read-out and by officials once they recount 1 percent of their precincts' paper ballots. California Assistant Secretary of State for elections S. Lapsley downplayed the risk, arguing that "it assumes access and control for a lengthy period of time." Scientists disagree, noting that hackers could work out plans ahead of time, and that it only takes a minute to install the software, a hole that apparently originated from Diebold's efforts to make it as easy as possible to update the software inside its systems. ACM's US Public Policy Committee has released a report on Statewide Databases of Registered Voters.

CFP 2006: Life, Liberty and Digital Rights
TidBITS (05/08/06), J. Porten

Participants at ACM's recent Computers, Freedom, and Privacy (CFP) conference met in Washington, DC, to discuss the effect of technology on society, focusing especially on the ways that governments can use information against their citizens. CFP has historically facilitated an honest discussion between the hacker, security, privacy advocate, and law enforcement communities. A panel debating the different approaches to privacy law in the United States, Canada, and the European Union noted the difficulty that Europeans have faced in implementing centralized privacy laws, while the United States still maintains a patchwork of national and local laws. Participants debated privacy in the context of a world where information flows freely and governments maintain massive databases of personal information, often over the objections, or without the knowledge, of their citizens. A panel discussing the Bush administration's domestic surveillance program questioned the legality of both the government agents and telecommunications companies involved, noting that under the Foreign Intelligence Surveillance Act, employees of private companies found to be complicit in illegal surveillance are subject to criminal prosecution, a provision that has raised questions about AT&T's collaboration with the NSA to deliver vast troves of telecommunications traffic. In another discussion, Apple drew severe criticism for its implementation of DRM. In the closing keynote address, science fiction author V. Vinge contrasted two historical visions of a technology-driven future: the dark, Orwellian world where privacy has completely succumbed to ubiquitous government intrusion, and the cyberpunk world controlled by the anarchist hacker. Vinge suggested that liberty has gradually eroded as humans have fallen prey to a melange of technologies and laws that are steadily (and at times, inadvertently) waging war on the last vestiges of privacy.

USC Hacker Case Pivotal to Future Web Security
InformationWeek (05/09/06), L. Greenemeier

The trial of Eric McCarty, the 25-year-old San Diego resident who claims that he hacked into the University of Southern California computer system only to call attention to its vulnerabilities, could become a referendum on acceptable practices of security research, especially if he is convicted and sentenced to the maximum of 10 years in prison. Everyone agrees that McCarty violated the law, though the ethical legitimacy of his actions is being hotly debated, and many security researchers believe the maximum penalty is extreme, particularly since McCarty has been cooperating with the FBI. McCarty hacked into a SQL database that contained the Social Security numbers, birth dates, and other identifying information for more than 275,000 USC applicants dating to 1997. McCarty initiated a SQL injection after he found a vulnerability in the login system of USC's application Web site. The university then took the site down for two weeks to fix the flaw. Security professionals have mixed feelings about McCarty's actions. "McCarty was trying to prove a point," said Digital Defense's R. Fleming. "Part of me commends him for saying, 'Hello, wake up.' But he crossed an ethical boundary because he didn't have permission to test that system, and he broke the law." The online document called RFPolicy informally lays out the basic protocols for researchers to communicate with vendors and developers to address vulnerabilities. RFPolicy has no legal authority, however, and it does not provide a method for legally entering someone else's IT environment and testing Web applications. Security experts worry that if McCarty is sentenced to jail, many white-hat researchers will either stop looking for flaws or stop reporting them for fear of legal reprisal. "If the good guys aren't going to do this research, that's a bad thing because the bad guys certainly won't stop," says WhiteHat Security founder J. Grossman.

Cell-Phone Tracking: Laws Needed
Wired News (05/08/06), R. Singel

The cell phone industry and privacy advocates are urging Congress to adopt clear, standardized rules regarding the use of mobile phones to track suspects. At ACM's recent Computers, Freedom, and Privacy Conference, a panel agreed that Congress should write rules governing what level of suspicion police need to have before tracking people through their cell phones. Law enforcement is currently allowed to track suspects using their cell phones without probable cause, a practice the Justice Department says is sanctioned by a combination of wiretap laws governing stored communications plus a law that lets law enforcement learn the phone numbers people dial. However, eight out of the 10 judges who have published decisions since August have rejected the DOJ's legal arguments. "We've seen an avalanche of...decisions rejecting the government's hybrid theory," said K. Bankston, a lawyer with the Electronic Frontier Foundation, during the panel discussion. "For several years, the DOJ has been successfully pulling the wool over the eyes of magistrates." Bankston added that some of the legal uncertainty may be resolved soon, since the DOJ has filed an objection in at least one case. Other members of the panel, including Catholic University of America law professor C. Fishman, did not understand the fuss over law enforcement tracking cell phones without a probable cause. "The government has legitimate reasons to follow people," he said. "This is the technology law enforcement needs to get the probable cause to search you, arrest you, and throw you in jail."

DNS Security: Most Vulnerable and Valuable Assets
IT Observer (05/08/06)

A survey conducted by Cornell University's Computer Science Department mined public data to determine: The most vulnerable assets of the Domain Name System (DNS); the servers most likely to be assaulted because they control the biggest chunk of the namespace; and the existence of servers with known vulnerabilities and the domain names they affect. The survey found that attackers can gain a tremendous advantage by exploiting the architecture of the legacy DNS, which creates many non-obvious dependencies between names and nameservers. The higher the number of nameservers on which a domain name depends, the bigger the trusted computing base, which leads to a larger number of dependencies, a bigger attack profile, and greater susceptibility to attack. According to the survey, a routine DNS name depends on 46 nameservers on average, while the most vulnerable top level domain names are ranked .ua, .by, .al, .sm, .mt, .va, .pl, and .it, from highest to lowest; the bulk of country code TLDs average more than 100 dependencies per name. The survey ascertained the most valuable DNS assets by evaluating how important a role a DNS nameserver plays in name resolution, and found that a nameserver is involved in the resolution of 166 externally visible names, on average. Furthermore, 67 hostnames appearing in Yahoo!+DMOZ depend on the nameserver ranked 5000, 29 publicly visible Web sites rely on the nameserver ranked 10000, and the median number of externally visible names served is four. In addition, institutions that may be ill-equipped or unwilling to assume DNS functionality operate many important servers. Information about the most vulnerable and most valuable DNS assets was then combined with data about established bugs in servers to infer that one in three Internet names can be hijacked by well-known, scripted exploits; among this percentage is www.fbi.gov as well as every other name residing in the fbi.gov domain.

Defining Trust
SC Magazine (04/06) P. 26; D. Kaplan

K.D. Campara co-chairs the Object Management Group's (OMG) Architecture-Driven Modernization Special Interest Group, which seeks to prevent terrorists from funding their malicious activities through the exploitation of insecure US networks by building a framework that would evaluate risk and detail the characteristics and elements that make up trustworthy software. This effort is supported by the federal government, whose operations depend on the security and trustworthiness of software. Campara says tool vendors and software manufacturers must shoulder the burden of following a best possible practice, and she thinks the framework would establish standardized design criteria and automated procedures for tool vendors and software makers to adopt to make sure their products are reliable and trustworthy. "Tool vendors will be building tools based on this framework because they will know that there is a market for them, while software suppliers will use those tools to improve and clean up software products," says Campara. James Madison University computer science professor S. Redwine reasons that a universal software assurance framework would carry benefits for buyers as well as sellers. "It would separate out the people who have convincing arguments and evidence of why you should have confidence in software from those that don't, in a rather clear way," he notes. OMG expects to release a request for proposal (RFP) for the model, which will be open to all OMG members, by November or December; a standardized code analysis process does not currently exist, and creating one will require a concentration on following authoritative coding processes, says A. Nadalin of IBM Software. N. Mead with the Software Engineering Institute expects some vendors will initially be resistant to the idea of a universal framework, if conforming to it requires a substantial amount of labor.