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

Δελτίο 53
21 Δεκέμβρη 2006

Congress and Tech: Little to Show
CNet (12/11/06), D. McCullagh

The 109th Congress, which concluded over the past weekend, was rather ineffective in passing technology-related legislation during its two-year life span. The politicians went home for the holidays before a vote could be taken on raising the number of available H-1B visas, which is currently set at 65,000 per year. Microsoft's top lobbyist, J. Krumholz, commented, "Without an increase in the number of H-1B visas and green cards issued each year, our nation loses the opportunity to benefit from the contributions of highly educated and skilled workers from around the world. American business and society in general will be worse off." Web censorship and filtering legislation did not have much more success: While a bill targeting the protection of children on social networking sites passed in the House, it died in the Senate. A House subcommittee let another bill protesting Chinese Web censorship expire without much debate, and voting on a bill that would require Web labeling was put off until February. Net neutrality regulations were defeated soundly in the House, and a Net neutrality amendment was rejected by a Senate committee that voted 11-11 when a majority was needed. Democrats tried to reinsert the amendment into a broader bill being voted on in the Senate, but the vote never happened. Copyright and digital rights management has not received much attention ever since the Grokster file-swapping case. The issue of making "broadcast flags" mandatory for hardware makers was brought up, but Congress avoided voting on the matter. A temporary extension of the R&D tax credit was passed as part of a larger tax relief, but a popular tax credit for R&D was not. The day they adjourned, Congress send an anti-pretexting bill to the President, which would make it a federal crime to buy or sell private phone information, but which exempted police and spy agencies.

New University of Maryland Technologies Could Move Video Surveillance to New Level, AScribe Newswire (12/11/06)

University of Maryland electrical and computer engineering professor R. Chellappa has created an artificial-intelligence-based real-time computer video monitoring system that can identify suspicious activities or individuals, which may remove some of the burden from security guards who must monitor many video screens simultaneously. Chellappa, a pioneer in pattern recognition and computer vision software, developed a digital signature for the human gait, called "human gait DNA." Deviations in this normal gait pattern cause asymmetries that the system can recognize and analyze, but for now a concealed object not effecting one's gait would not be noticed. Gait is also used to identify specific individuals, as is face recognition software. To locate and observe actual pedestrians, Chellappa has used corrective algorithms to compensate for changing light, shadows, and viewing angles. Other recognition technologies are currently being worked on with support from the Department of Homeland Security, including an algorithm to estimate the heights of subjects in the field of view of a camera, and a program that can find unattended packages using a structured representation known as attribute grammars.

Report Blames Denver Election Woes on Flawed Software
Computerworld (12/13/06), T. Weiss

Ineffective software design, poor IT management, and the release of a critical application without being tested were the cause of Denver's election-day debacle, concludes a new report. Voters were met with as much as three-hour long waits at polls, causing an estimated 20,000 to go home without voting. The "ePollBook" electronic poll software, supplied by Sequoia Voting Systems, was designed to let people vote at any polling location in the area, but "decidedly subprofessional architecture and construction" led to the difficulties, according to the Fujitsu Consulting report. The report stated that "The ePollBook system is a poorly designed and fundamentally flawed application that demonstrates little familiarity with basic tenets of Web development. Due to unnecessary and progressive consumption of system resources" the system grew slower the more heavily it was used. Another problem experienced on election day was that Web sessions didn't expire without an "exit" button being clicked by the user, which tied up a great deal of the system's resources. According to activity logs, 90% of the user sessions were not closed using this button, but by a user simply shutting down the browser. Fujitsu also pointed out the fact that the system was not stress-tested, calling such an oversight "naive ... at best," especially given the importance of the event it was deployed for. Fujitsu recommended that Denver get the Sequoia application fixed or use another platform. The report concluded, "Given the increasing criticality of technology in conducting elections and the sensitivity of personal data in the DEC's possession, this casual approach to technology cannot be permitted to continue."

Engineering Professors Work to Secure Software-Defined Radio Technology
Virginia Tech News (12/14/06), L. Crumbley

Software-defined radio (SDR) technology will be the focus of a three-year project by engineering researchers at Virginia Tech. Although SDR technology is found in the two-way communications devices of tactical military forces and emergency responders, there are concerns about the reliability and security of the software, which is used to handle the signal processing for transmission and reception. Lead researcher J.-M. Park says the team will try to answer some important questions about the security of SDR technology. "What are the security threats if an adversary were able to install malicious software on an SDR, and what counter measures would be effective against such attacks? These problems are unique to SDR networks and have not been studied in a systematic way by the network security community," says Park. The research could result in the development of SDR technology that is better able to withstand attacks, and the emergence of improved security standards. SDR technology has also become a key component for wireless mesh networks, and some observers believe it could help relieve traffic on the radio spectrum through its ability to locate vacant areas.

E-Voting Requires Long-Term Strategy: IDC
Washington Technology (12/12/06), E. Butterfield

IDC Research has released a study showing that, despite spending almost $3.8 billion since 2002 on e-voting systems, state and local governments are far from achieving an accurate, secure, and timely voting process. The study, "Improving Voting System Investment, Credibility and Transparency," found that minimal strategy was used to deploy the new systems acquired after the 2000 election. The result of this lack of planning was intricate new systems that are just as unproven and controversial as the systems they replaced, according to the study. While easier to use, the new equipment has security problems, as they were bought with initial costs in mind, ignoring upkeep. Improvements in standards, funding, auditing capabili-

ties, and transparency is recommended. The study also recommended that governments keep records on lifecycle expenses to aid future purchases.

Project Aims to Bolster Java Open Source Security, Quality
Linux Insider (12/12/06), J. Lyman

Fortify Software and FindBugs Java plan to provide additional reviews of open source code written in Java through a collaborative initiative called the Java Open Review (JOR) Project. Most open source programmers have embraced the effort to help improve the security of software and eliminate errors in applications, says Fortify chief scientist B. Chess. JOR will examine open source projects for bugs and security holes, and make its findings available to the open source software community. In addition to identifying security and quality errors, it will provide an analysis of errors per 1,000 lines of code. JOR will even offer more specific information on coding errors to aid programmers in their efforts to address any problems. "As software becomes increasingly intricate, FindBugs and Fortify Software want to provide open source developers automated tools to help find defects in complex code bases, as well as defend against an ever-growing pool of sophisticated hackers," says Chess. "Noone is helping the Java open source community, and we want to fix that."

An Ominous Milestone: 100 Million Data Leaks
New York Times (12/18/06) P. C3; Zeller, Tom Jr.

Wired News senior editor K. Poulsen announced on his blog last Thursday that with announcements from UCLA (800,000 records stolen), Aetna (130,000 records stolen) and Boeing (320,000 records stolen), over 100 million records had been stolen since the ChoicePoint breach almost two years ago. While perpetrators of the Aetna and Boeing laptop thefts were probably not after personal records, the same cannot be said for the UCLA data theft, where a hacker had been accessing the university's database of personal information for over a year before being discovered. A Public Policy Institute study, using data from the Identity Theft Resource Center, showed that of the 90 million records stolen between Jan. 1, 2005, and March 26, 2006, 43% were at educational institutions. "College and university databases are the ideal target for cyber criminals and unscrupulous insiders," says Guardium chief technology officer R. Ben-Natan. "They store large volumes of high-value data on students and parents, including financial aid, alumni and credit card records. At the same time, these organizations need open networks to effectively support their faculty, students and corporate partners." While some claim that 100 million is a modest estimate, Indiana University Center for Applied Cybersecurity Research director F. Cate says the threat posed by loss of personal data is exaggerated because people are too quick to equate the loss of data with its illegal use. However, others argue that once a Social Security number or birthday is stolen, it can be used indefinitely since these never change. Criminals have not yet devised ways to make use of the massive amounts of information they have obtained, but this inability will not last forever. While Congress has failed to pass data security legislation, 18 states now allow citizens to freeze their credit lines, and seven more allow victims of identity theft to do so.

Configuration: The Forgotten Side of Security
Linux.com (12/12/06), B. Byfield

Configuration-centered security, also known as security architecture or proactive security, is often overlooked in favor of reactive measures such as anti-virus programs or security patches, even though it is more efficient. The configuration security approach involves making

the computer system's design and installation a security component. "The right time to apply best practices is during system design," says MIT professor emeritus J. Saltzer. "That way, installation, configuration, and daily use will automatically tend to be more secure." Saltzer says the stress on reactive rather than proactive security is partly driven by vendors who roll out flawed systems, and partly by organizations who erroneously consider security to be an IT-only issue. A major reason why configuration-centered security is ignored is the tendency to balance security against user convenience, with convenience typically having priority. A system's design and configuration should proceed with five objectives in mind, according to K. Watson with Perdue University's Center of Education and Research in Information Assurance and Security: These objectives include building for a particular purpose and inclusion of the bare minimum for fulfilling that purpose; protection of idle data's availability and integrity; safeguarding dynamic data's confidentiality and integrity; disablement of all redundant resources; and restriction and recording of access to required resources. Watson notes that an emphasis on constructing secure and resilient systems at the outset makes reactive security less necessary later on. Among the suggestions experts offer for improving security awareness are enforcing a clear security policy, the removal of "a culture of blame," and inclusion of "a clear line of escalation."