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

Δελτίο 9
10 Φλεβάρη 2006

Torvalds Says DRM Isn't Necessarily Bad
CNet (02/03/06) S. Shankland

Linus Torvalds recently issued a posting to the Linux kernel mailing list contending that the restrictions on digital rights management (DRM) proposed in the update to the GPL threaten to compromise security. "Digital signatures and cryptography aren't just 'bad DRM.' They very much are 'good security' too," Torvalds wrote. The Free Software Foundation has explicitly repudiated the use of DRM in tandem with GPL software in the draft update, though Torvalds maintains that DRM is useful for signing software with secret keys, or for enabling computers to run only versions of software that are demonstrably authorized. Torvalds has already announced that Linux will continue to operate under the existing version of the GPL, in a move that is seen as a slight to the Free Software Foundation. Although the DRM provision is intended to stop the practice of companies such as TiVo implementing only authorized versions of Linux, Torvalds believes that the market should dictate the behaviour of hardware companies, rather than software developers, noting that if programmers object to the proprietary provisions of a hardware company, they can shop elsewhere. Torvalds claims the proposed GPLv3 oversteps its bounds in the name of a crusading ideology, whereas GPLv2 simply offered a level playing field where all source code is equally accessible. As far as the content of movies is concerned, Torvalds suggests that people use an open license from an organization such as Creative Commons, which would eventually render DRM encryption obsolete if enough content was licensed in that fashion.

Increasingly, Internet's Data Trail Leads to Court
New York Times (02/04/06) P. A1; S. Hansell

The Justice Department's recent request to four major Internet companies--America Online, Yahoo!, Microsoft, and Google--for data about their users' search queries has drawn attention to the issue of Internet privacy. Although America Online, Yahoo!, and Microsoft have complied with the request, Google has refused it. The case does not involve information that can be linked to individuals, but it has cast new light on what privacy, if any, Internet users can expect for the data trail they leave online. In many cases, the answer is clouded by ambiguities in the law that governs electronic communications such as telephone calls and email. Under the 1996 Electronic Communications Privacy Act, a court order is generally required for investigators to read email, although the law is inconsistent on this, treating unopened items differently from opened ones. However, the law is unclear about what standard is required to force Internet companies to turn over search information to criminal investigators or civil litigants. "The big story is the privacy law that protects your email does not protect your Google search terms," said O. Kerr, a professor at the George Washington University Law School and a former lawyer in the computer crime section of the Justice Department. Other lawyers contend that the law that provides protection for email content, or even the Fourth Amendment protection against unreasonable searches, could be applied to data about Web searching, although the issue has not been tested in court.

Millions Required for RFID Research
RFID Journal (02/03/06) M. Roberti

The RFID Academic Convocation drew 100 top-end users and academics involved in RFID last week. The participants learned about RFID collaboration opportunities around the globe, established fundamental research areas that would meet industry RFID requirements, and laid out a plan for market opportunities and technologies. "Those of us in the industry came away with a better understanding of the research being done around the world, and I think the researchers came away with a better understanding of the needs of the various industries represented at the event," says T. Ng, director of emerging technology at McKesson. Network protocol standards, specialized tags for airplane and auto parts, applications for micro- and nano-manufacturing technologies, and new bio and material sciences development in packaging were identified as research areas that need funding. Over the next five years, more than $100 million could be needed for such research areas, according to S. Miles, a researcher at the MIT Auto-ID Labs and chair of the RFID Academic Convocation conference committee. An "Internet of Things" could result from such research efforts, says J. Williams, director of the MIT Auto-ID Labs, host of the gathering. "The Internet of Things to make billions of physical objects visible over the Web will require a secure and scalable infrastructure that is more challenging to build than the original Internet," he says.

College Receives Training Grant for Cybersecurity
Maryland Gazette (02/01/06) Sedam, R. Sean

Montgomery College is set to form a partnership with other area community colleges, universities, high schools, and the Metropolitan Washington Council of Governments to develop and operate a regional cybersecurity centre called the CyberWATCH (Cybersecurity: Washington Area Technician and Consortium Headquarters) project. The project will be funded by a $3 million grant from the National Science Foundation over a period of four years. "There is a demand in this area for skilled cybersecurity technicians who can protect our nation’s information against intrusion," says CyberWATCH director D. Hall. One of the centre's goals will be to address the shortage of cybersecurity technicians and training programs in the area. Montgomery College will build and maintain a remote information technology security lab, create a program in cybersecurity training, and develop internships for students and training and externships for faculty. The consortium, which will allow students from specific schools to log on to the lab and learn router, switch, firewall, workstation and server security, includes the University of Maryland, College Park, George Mason University, and George Washington University, among others.

Electronic Voting on Rise, Study Says
Associated Press (02/07/06), R. Tanner

The United States is doing away with old voting systems because they are prone to error, but problems still should be expected in the November elections because so many voters will be using unfamiliar equipment. "You throw that many people in on something new, you're always bound to see something go wrong," says K. Brace, president of Election Data Services, which tracks election equipment. According to a new survey from the political consulting firm, this fall at least 80% of voters will use new machines that are either ATM-style touch-screen units or devices that ask users to fill in the blanks. Ten percent of voters will use a lever machine, and 3% will use punch cards, which were the subject of the contested votes in Florida during the 2000 presidential election. At that time, about 20% of voters used levers, and approximately 17% used punch cards. Meanwhile, critics of the new voting systems maintain that they can be manipulated, and the charges have prompted 25 states to pass laws that require the equipment to verify votes and to yield paper receipts. After the 2006 elections, approximately 48% of the nation's 170 million registered voters will have used a new voting system.

'Net Neutrality' Debate Heats Up at Senate Hearing
Wall Street Journal (02/08/06) P. B7; E. A. Brown

Several Internet companies and Google are urging Congress to pass a law that would ban telecommunications networks from charging consumers more for some services and controlling what they can get off the Internet. The "net neutrality" debate has been heating up for some time now after some phone companies suggested they plan to bill companies for delivery of specific Internet services while Congress is considering amending the 1996 telecommunications act. Net neutrality is the idea that network operators should be neutral providers of Internet content and consumers should have the option of accessing whatever they want on the Internet. "There are 250,000 networks that make up the Internet," says Google's V. Cerf. "They are compensated by its users. Allowing broadband carriers to control what people see and do online would fundamentally undermine the principles that have made the Internet such a success." Cerf has been a strong advocate for net neutrality and also says the openness of the Internet is being threatened, and that a new law would protect consumers by limiting they ways carriers can interfere in the decisions of their Internet users. National Cable and Telecommunications Association CEO K. McSlarrow disagrees with Cert and is requesting that lawmakers refrain from making premature legislative decisions. Senate Commerce Committee Chairman Sen. T. Stevens (R-Alaska) plans to introduce net neutrality legislation in the beginning of March.

The Spy Who Didn't Shag Me
Slate (02/06/06), A. Schaffer

While the Senate is investigating the legality of the Bush administration's warrantless surveillance program, University of Pennsylvania computer scientists have developed simple, inexpensive methods for eluding the eavesdropping net. Phone taps commonly rely on the absence of a C-tone, the sound conveyed when a receiver is on the hook, to trigger recording. C-tones can be created by playing two frequencies in tandem, tricking the wiretap by simulating the noise that a phone makes when the receiver is idle. Military phones with C-tone buttons can be found on eBay, or, alternatively, the parts to generate the sound can be purchased at Radio Shack. UPenn computer scientist Matt Blaze tested a variety of wiretapping devices, and found that the older loop extender systems were especially susceptible to the C-tone trick. The government more commonly uses CALEA systems now, which the FBI claims are nearly impervious to the C-tone defense--a claim that Blaze disputes. In presenting his findings at the International Federation for Information Processing Conference on Digital Forensics last week, Blaze also presented tricks that can stymie software intended to intercept e-mail, Web traffic, and file sharing. Since all the information that travels over the Internet is contained in packets, Blaze dispatched decoy packets, carrying bogus information and packaged in such a way to ensure that only the eavesdropper would receive them, not the original recipient. Blaze took advantage of the different ways of routing and processing packets, ensuring that the eavesdropper and the intended recipient would receive different versions of the same message.

Nuclear War Over Software Patents?
Business Week (02/06/06). L. Woellert

When Free Software Foundation founder R. Stallman voiced his concerns about software patents undermining innovation in 1991, he was largely ignored and branded an alarmist. With the draft update to the GPL, he is now seeking to limit the growth of patent-protected digital content and proprietary software. While Stallman readies for an embittered struggle between open-source advocates and defenders of the proprietary software model, IBM is leading a coalition of open-source groups, including Red Hat and Open Source Development Labs, to improve the quality of patents and guard against attempts to patent work already in use. The group will start by compiling a list of prior art, which runs counter to Stallman's strategy of completely sheltering GPL code from the patent process. The draft update also restricts GPL code from being used to protect movies and music. Stallman's vision would provide universal access to free software, effectively undermining the current patent protections, which has sparked staunch opposition from the entertainment industry, as content distributors use open-source code to safeguard their digital property rights, while Linux powers a growing number of devices, such as the TiVo digital video recorder. L. Torvalds has already repudiated GPL v3, setting the stage for what could be a showdown between Stallman and the free software ideologues and the larger and more pragmatically-minded open-source community. The looming confrontation could undermine the availability of GPL software, which has many observers hoping that IBM will be able to broker a solution that continues the flow of innovation.

It's Time to Arrest Cyber Crime
Business Week (02/02/06) P. Horn

Profits from cyber crime were higher than profits from the sale of illegal drugs for the first time last year, according to V. McNiven, the US Treasury Department advisor. "Cyber crime is moving at such a high speed that law enforcement cannot catch up with it," McNiven says. Cyber crime is now driven by profit with an estimated 85% of malware created specifically for profit. The FBI lists fighting cyber and technology crime at number three on its list of top 10 priorities. Since cyber criminals are becoming more organized, experts say a new approach to fighting cyber crime is needed in three key areas: people, policies, and technology. The "people factor" aspect of the solution is figuring out how hackers work and what makes them tick. Behavioral insight will help fight intrusions as well as extrusion into the network. Policy is another issue that must be dealt with by organizations by establishing expectations for behaviors and outcomes in order to create a secure business environment. The implementation of security policies allows companies to protect their data. More than 40 organizations recently came together to form the Data Governance Council, a group designed to go beyond the traditional approaches to security, privacy, compliance, and operational-risk policy. Technology such as encryption is another challenging issue companies must face and learn how to extend it to every touchpoint on the network. It is estimated that more than half of all corporate data is on someone's PC, PDA, or cellular phone. Cyber crime is now the crime of the 21st century, but with the right people, policies, and technology in place, it can be fought, writes IBM Research vice president P. Horn.