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

Δελτίο 5
20 Γενάρη 2006

"Waging War Through the Internet"
San Francisco Chronicle (01/15/06) P. E1; J. Arquilla

While the US anti-terrorist effort over the last four years has focused on tracking al Qaeda and other terrorist organizations and thwarting their attempts to stockpile sophisticated weaponry, the threat of Internet-based threats that could devastate communications, energy, and transportation networks has largely gone ignored. Terrorists could remotely transmit a virus that takes down power to a vast swath of the country, or manipulate the controls that link hydroelectric dams with gas and oil pipelines and chemical plants. Top-level government agencies such as the Dept. of Defence have already come under attack, as have nuclear and waste treatment plants. One current attack threatening US military and scientific networks, Titan Rain, appears to come from China, where some of the world's most skilful hackers live. The annual financial cost of settling claims resulting from cyber attacks exceeds $B 40, roughly the same amount as the insured losses stemming from the September 11, attacks. Though the consequences would not be as dire, a major cyber attack is far more likely than terrorists acquiring and using a nuclear warhead. Al Qaeda is already presumed to have dispatched at least one agent to the US to study computer science, and the number of hackers is steadily growing. The traditional focus on preventing violent attacks on domestic soil has only exacerbated the cyber threat, as it is now extremely difficult for terrorists to plan and execute a physical attack, leaving cyber terrorism a logical recourse. The US also suffers from an overconfidence about its cyber defences, placing too much faith in firewalls and other security applications that can easily be circumvented by new or slightly altered viruses. Even in the military, strong Internet encryption is not generally employed. Moreover, the US should be attacking the terrorists' systems with the same vengeance that we pursue their operatives in caves and spider holes, writes J. Arquilla, professor of defence analysis at the US Naval Postgraduate School in Monterey.

“New GPL Free at Last"
Wired News (01/16/06); M. Baard

Free Software Foundation (FSF) founder R. Stallman released a draft of GPLv3 earlier this week, the first update to the GNU Public License since 1991. The new version contains language prohibiting the application of GPL code to digital rights management, and imposes restrictions on the patent rights that developers can claim for their programs licensed by the GPL. Curtailing digital restrictions and patent rights is consistent with Stallman's copyleft principal that guided the original version of the GPL, where developers could release their code without worrying about a commercial entity appropriating it and imposing usage restrictions, creating an atmosphere of intellectual freedom that engendered projects such as the Linux operating system. The GPLv3 draft comes amid renewed fears of corporate encroachment into independent software development, as Stallman cites the increased use of digital rights management (referred to by the FSF as handcuffware), and a growing number of software patents. The FSF's E. Moglen notes that the draft also contains enforcement provisions and language concerning remote services. The draft will be debated over the next year, though Stallman believes that it could not be more timely, given the patent crush that threatens the open-source software community. Microsoft, for instance, was recently awarded a patent for the FAT file system format, which could end the distribution of Linux if Microsoft opts to collect royalties.

“Congress Takes Aim at 'Analog Hole'" TechNewsWorld (01/17/08); Mello Jr., P. John

A bill pending before the House of Representatives designed to close the analog hole to guard against piracy of CD and DVD has drawn the ire of many civil libertarians and technologists. Congress is also reviewing the broadcast flag, which regulates the guards against the distribution of television content on the Internet. While Rep. J. Sensenbrenner (R.-Wisc.) referred to the broadcast flag as the counterpart of the analog hole, the Consumer Electronics Association's M. Petricone notes that the broadcast flag is a voluntary, evolutionary development, while the analog hole is simply a strong-arm effort by content holders that has no consensus. He also notes that the vague language of the legislation could be applied to any piece of software code that could convert data from analog to digital. Hardware makers object to the precedent that the legislation would set by requiring them to prove that their products will not be used by pirates. The Electronic Frontier Foundation's F. von Lohmann objects to the provision in the legislation that requires all devices capable of analog to digital conversion to be able to tag digital content originating from an analog source. "In order for that to work," he said, "they have to have the federal government require every technology to detect this mark of the beast and obey it." The two marking technologies that the bill refers to, CGMS-A and VEIL, are unlikely candidates for such universal protection, says Lohmann, as CGMS-A has been around for years, but is largely unused, and, to his knowledge, VEIL has never been used to protect content.

"Mass Spying Means Gross Errors" Wired News (01/18/06); J. Granick

While mass government surveillance is fast becoming precedent in the age of terrorism, there are limitations on the technology in use that could have troubling consequences for citizens, writes J. Granick, executive director of the Stanford Law School Centre for Internet and Society. The communications Assistance for Law Enforcement Act (CALEA) mandated that phone companies augment their networks with mass surveillance capabilities, though the CALEA-directed spying initiative collects data at a far greater pace than the Justice Department can issue warrants, indicating that law enforcement might automate the system with voice recognition technology that calls for human monitoring when it encounters a hit. Law enforcement could also introduce facial recognition technology in airports and other public venues, funnelling the information into large government databases. While the FISA law does not authorize mass surveillance without probable cause, some legal and intelligence experts believe that it should. Harvard law professor Charles Fried argues that mass surveillance is an imperative, claiming that despite its dubious legal status, human spying would be minimal in the first stages of the program. Fried also claims that the algorithms and scan techniques used to mine government databases must remain classified, and argues that a mass surveillance program will be doomed to failure if its details are publicly released. However, Granick says the effectiveness of mass spying is tenuous, as terrorists are accustomed to modifying their speech and correspondence to elude surveillance. Regardless of its success rate, mass surveillance will inevitably produce false positives, and without enough agents to follow up on the hits, such a program could misinform law enforcement and disrupt innocent citizens' lives more than it combats terrorists.