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

Δελτίο 80
27 Ιουνίου 2007

ISS Computer Woes Concern Europe
BBC News (06/18/07), I. Klotz

The recent failure of two computer systems on the International Space Station (ISS) has raised concern about the Columbus laboratory and the Automated Transfer Vehicle (ATV), two additions with the same systems. The Columbus laboratory is scheduled to be launched in December, and the ATV large supply vessel is scheduled to be launch early next year, but the European Space Agency (ESA) has launched an investigation to see if the same problem might occur with those two systems. The ESA formed a team that joined the multi-national effort to fix the ISS computers. The Columbus laboratory has similar computers, but the ATV has completely identical ones, so the ESA wants to ensure any corrective action is taken before the two sections are launched. The computer systems on the ISS control the rocket-steering system the station uses to maintain proper alignment with the sun for heat and energy, and with the earth for communications. The computers also control life-support equipment, though that equipment can also be operated manually. Engineers have not yet been able to identify a specific cause for the computer malfunction, but NASA and Russian engineers believe the failure was caused by a change in the electrically charged plasma field that occurred when astronauts from the shuttle Atlantis attached a new metal beam with a huge pair of solar wings. NASA space station program manager Mike Suffredini says such sensitive problems could continue to occur as the space station continues to change.

Watching Virus Behavior Could Keep PCs Healthy
New Scientist (06/15/07), T. Simonite

A prototype anti-virus system developed at the University of Michigan uses the "fingerprint" of virus activity to more effectively identify viruses. The system obtains such fingerprints by intentionally infecting a quarantined computer with viruses. Conventional anti-virus software monitors systems for suspicious activity and then tries to determine the source by checking for virus signatures, which makes it difficult to spot new pieces of malware and track different variations. The University of Michigan team studied the files and processes malware created and modified on an infected computer, and developed software that uses the information gathered to identify malware. The prototype is capable of defining clusters of malware that operate in similar ways, and can create a kind of family tree that illustrates how superficially different programs have similar methods of operation. In tests on the same software, the prototype was able to identify at least 10% more of the sample than five leading anti-virus programs. The prototype also always correctly connected different pieces of malware that operate similarly, while the best anti-virus program was only able to identify 68% of such links.

Army, Air Force Seek to Go on Offensive in Cyber War
GovExec.com (06/13/07), B. Brewin

The Air Force held its industry day for its Network Warfare Operations Capabilities solicitation in San Antonio on June 14, 2007, after announcing in April that it wants tech firms to

provide technology that will enable the service to go on the offensive against those who launch cyberattacks. In May, the Army released a similar announcement, and the service expects to receive responses from the computer industry by the end of June. The cyberattacks that the Army and Air Force plan to launch are referred to as offensive information operations (OIOs), and the services are also interested in technology that will prevent enemy computer systems from detecting and countering OIOs. According to the request for information from the Air Force's 950th Electronic Systems Group, the technologies would help to "disrupt, deny, degrade or deceive an adversary's information system." The solicitations are consistent with the offensive cyberattack capabilities that Marine Gen. J. Cartwright, commander of the Strategic Command, discussed during a hearing of the House Armed Services Committee in March. If "we apply the principle of warfare to the cyber domain, as we do to sea, air and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary, to deter actions detrimental to our interests," Cartwright said.

FBI: Operation Bot Roast Finds Over 1 Million Botnet Victims
Network World (06/13/07), M. Cooney

The FBI and the Dept. of Justice announced that their ongoing cyber-crime investigations have so far detected over 1 million victims of botnet crime. Operation Bot Roast aims to interrupt and dismantle botherders and has caught three major botnet operators so far, including "Spam King" R. A. Soloway. Bots are considered to be one of the top industry scourges. Their destructiveness is illustrated by a report from Mi5 describing how Mi5 installed a Web security beta product at a company with 12,000 nodes and identified 22 active bots, 123 inactive bots, and 313 suspected bots within one month. The discovered bots had caused 136 million bot-related episodes. In addition, after examining over 4.5 million Web pages, Google researchers reported that 10 percent of Web pages were booby-trapped with malware, and 16% seemed to contain dangerous code. By accidentally permitting access to their computers, unknowing computer owners permit their computers to be employed as vehicles for crimes such as denial-of-service attacks and phishing. Botnets are also increasingly threatening to national security, due to their ability to be widely distributed. Operation Bot Roast plans to inform the unwitting owners of hijacked computers. Meanwhile, citizens can guard against botnets by adhering to strong computer security practices.

Denial-of-Service Attacks: Street Crime on the Web
New Scientist (06/06/07) Vol. 194, No. 2607, P. 30; J. Giles

Malefactors are increasingly using denial-of-service (DoS) attacks--the practice of crippling Web connections with a flood of traffic--to steal money from unaware Web site owners, and the method's persistence is aided by the fact that individual users and small companies generally cannot afford anti-DoS safeguards. "There are more players, better players, in the market than just a year ago," notes Arbor Networks computer security specialist J. Nazario. One of the most common techniques to launch DoS attacks is to contaminate computers with bot software that lies dormant on the compromised PC until it is instructed to link with the target Web site, and the simultaneous accessing of the site by massive numbers of bot-infected PCs can often cause the server to crash. University of California, San Diego researchers determined that over half of the more than 68,000 DoS attacks perpetrated between 2001 and 2004 targeted home users or small businesses, and among the more serious kinds of attacks are those used to hold sites for ransom. University of Washington computer networks expert T. Anderson thinks Web sites must be more selective in who they communicate with if DoS at-

tacks are to be countered, and he and his colleagues have developed a protocol for online information exchange in which sites insert a token in the code they share with visiting computers, which would be interpreted by software installed at the site's ISP as proof of legitimate communication. The distribution of these tokens would be halted if the site is attacked, spurring the ISP to impede incoming connections upstream to prevent the site from seizing up.

REAL Nightmare
Governing (06/07) Vol. 20, No. 9, P. 24; E. Perlman

Although states are not bound to follow the 2005 REAL ID Act, a federal law that aims to fight terrorism by improving security for state driver's licenses, some have nonetheless been very vocal about what they say are problems with the legislation. One of the biggest complaints among the states is the high cost of following the REAL ID Act's recommendations, which include verifying drivers' original identity documents--such as birth certificates and Social Security cards--when they show up at DMV offices to get a new license or renew their old one. According to the National Governors Association, states are likely to spend at least $11 billion of their own money over the next five years to get REAL ID up and running. The biggest factor contributing to this expense is the more than 2.1 million hours of computer programming states will need to adapt their systems for new requirements for things such as eligibility verification and database design. Another concern is that REAL ID needs to be supported by a variety of databases containing citizens' personal information if the program is to work nationwide, a big worry for some states and civil liberties groups. Though states can always opt out of REAL ID, as Montana and Washington have already done, doing so could create major inconveniences to their residents because they would not be able to use their driver's licenses to board airplanes or enter secure federal facilities. Although the legislation may be burdensome to states, it is nonetheless important that states implement its recommendations because they address the known vulnerability with state-issued drivers licenses: The ability of criminals, such as terrorists, to use identity documents to obtain a fraudulent drivers license, said the Dept. of Homeland Security's R. Knocke. "Shame on us if we don't take steps to fix it," he said.

Saving the Internet
Harvard Business Review (06/07), J. Zittrain

Berkman Center for Internet & Society co-founder J. Zittrain comments that the openness of the Internet and PCs is responsible for both their incredible success and their vulnerability to abuse, and he warns that one solution to this vulnerability--"tethered appliances" that can be instantly modified by vendors or service providers, but not users--could rob the Internet of its creative connectivity, and endanger companies whose business models rely on drawing and communicating easily with clients online. Zittrain writes that the advantages and disadvantages of the combined Internet/PC reside in its generativity, which he describes as "a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences." Generativity is defined by four core elements: The strength of a system or technology's leverage on a series of possible tasks; adaptability to a spectrum of tasks; ease of mastery; and accessibility. The two chief benefits of generativity are innovative output (new things that enhance people's lives) and participatory input (the opportunity to link and collaborate with others, and creatively express one's individuality). The dark side of generative technologies is their potential for use in malevolent endeavors, which include fraud, vandalism, malware, spam, pornography, and assaults against Web sites and the Internet's integrity. "The fundamental tension is that the point of a PC is to be easy for users to reconfigure

to run new software, but when users make poor decisions about what new software to run, the results can be devastating to their machines and, if they are connected to the Internet, to countless others," Zittrain explains. Reducing or eliminating the role of the PC as the hub of the IT environment by opting for tethered appliances will stymie technical innovation and remove the "safety valve" that maintains the honesty of information appliances, the author warns. Without such innovation, new social networks, communities of interest, and experiments in collective intelligence will be hindered, stunting the growth of new forms of culture, political activism, and participation.

Court Prohibits Access to Touch-Screen Source Code
Computerworld (06/19/07), M. Songini

The dispute over the Congressional seat for the 13th district of Florida reached another milestone when a federal court ruled that it would not allow the examination of source code on supposedly malfunctioning touch-screen voting machines. Democrat C. Jennings, who lost the highly contested and controversial election to Republican V. Buchanan by only 369 votes, had asked that the software be examined to determine if flawed e-voting machines caused voting irregularities. Jennings claims the iVotronic touch-screen systems made by Elections Systems & Software did not count about 18,000 votes. A Jennings spokesman said that a three-member legislative task force appointed by the US House Committee on Administration is investigating the vote count disparity. "They have the ultimate authority in this matter and are moving quicker than the courts ever have," the spokesman said. An investigation is also being conducted by the Government Accountability Office, and a preliminary ruling is scheduled for the end of July.

US Should Draw Warning From Estonian Web Site Attacks
Congressional Quarterly (06/18/07), M. Berger

After the statue of a World War II Soviet Soldier was removed in April, the Web sites of Estonia's prime minister, Parliament, banks, and newspapers were flooded with malicious data in an attack that some have linked to the Russian government. The attack, which lasted until mid May, was made worse by programs called bots, which took over computers and were manipulated to send additional messages to the government networks. Though such denial-of-service attacks are becoming less and less common, US officials are nonetheless concerned that an attack similar to the one in Estonia could disrupt the federal government's networks. One potential threat is China, which has developed a highly sophisticated, broadly-based capability to attack and degrade computer systems in the United States, Maj. Gen. P. Breedlove with the Joint Chiefs of Staff told the House Armed Services Committee last week. Former White House cyber-security expert P. Kurtz says the unorganized nature of the attack point's to the Internet's vulnerability. "The lesson is a more organized attack with advanced planning can really disrupt the critical information infrastructure," Kurtz says. Although he calls the US "a big fat target," he says the US's infrastructure is better able to withstand such attacks. Still, Kurtz says the threat of cyber-warfare is a growing concern worldwide. Arbor Networks security researcher J. Nazario says communication between Internet service providers and network users is crucial to withstanding such attacks. He says that many government installations are very well protected and have good contacts with the ISPs that are providing the traffic for them. He adds that good mitigation techniques are also in place.

Computer Privacy Expert Warns of Growing Risks to Social Security Numbers
AScribe Newswire (06/21/07)

A. Anton, representing ACM's US Public Policy Committee, testified Thursday before the House of Representative's Subcommittee on Social Security that the theft of social security numbers (SSNs) has become the primary method used to steal an individual's identity, allowing criminals to fraudulently access and open credit cards, banking accounts, and other financial services. Anton urged Congress to strengthen SSN privacy and reduce the nation's reliance on SSNs for personal identification. Anton, an associate professor of software engineering at North Carolina State University, cited the fact that more than 36 million Americans have had their identities stolen since 2003, and more than 155 million personal records have been compromised since 2005. Anton said, "Two key factors have enabled the explosion of identity theft in today's environment. One is the common use of SSNs as a de facto national identification number; the other is current computing technology that enables the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization." Anton urged banks, credit agencies, and government agencies to require stronger proof of identity, such as passports, military IDs, or licenses with a photograph to verify personal identity, after which a secondary authenticator, such as a secret shared password or PIN, should be used for subsequent transactions. Anton also suggested removing and prohibiting the display of SSNs in public records, requiring secure or encrypted transmission of records or documents containing SSNs and other personally identifiable information, requiring electronic security for files and devices containing SSNs, and substituting a unique number generated by the database management system to replace SSNs as the primary key in databases.

E-Vote 'Threat' to UK Democracy
BBC News (06/22/07)

An Open Rights Group (ORG) report says the risk involved with replacing paper ballots for touch screens far outweighs any benefit that may result from the change. The group, which based its conclusions on observations of local elections' e-voting trials in May, said until e-voting is made more reliable, easier to oversee, and has proven its integrity, it should not be used. Observations made during local elections using e-voting in England and elections using electronic counting systems in Scotland led the ORG to express "serious concerns" about e-voting. In England, kiosks, laptops, touch screens, and mobile phones have all been tested for e-voting systems. The ORG's primary concern is that e-voting is currently a "black box" system that prevents voters from seeing how their votes are recorded or counted, which the ORG argues makes election oversight impossible and wide open to error and fraud. The report criticized the lack of a rigorous certification method to ensure hardware and software systems are well protected. The report also called for usability testing to ensure the elderly and housebound can easily access e-voting schemes. The ORG said it was a serious mistake to accept the conveniences of e-voting while ignoring the risk that such systems could destroy confidence in voting as a whole, and that all e-voting trials should be stopped so problems can be fixed before e-voting is more widely used.

Security Study Pokes Holes in Advanced Authentication Claims
Ars Technica (06/20/07), J. Hruska

A new study by researchers at Harvard University and the Massachusetts Institute of Technology raises concerns about the potential effectiveness of image authentication systems, which banks consider to offer better security protection than simple passwords. Image authentication systems reportedly offer an additional layer of security, as users are presented with an image that was previously chosen, usually when passport input is required. For the

study the researchers divided the participants into three groups. The first group was told they were doing normal banking activities on a Sunday afternoon, while the second group was told to focus on security. The third group used their own user ID and passwords at the Web site of their own bank. The researchers tested the response of the participants when the login showed "https://" rather than "http://," and all 63 users provided their login data and password. Next, image authentication images were removed and replaced with a generic "this service is being upgraded" tag, and 58 out of 60 participants continued and entered their data. Finally, the researchers created a dramatic warning page that said the security certificate for the Web site may not be safe, and 30 out of 57 people still proceeded to log in. Broken down by group, the results reveal that 22 of the second group continued despite the warning page, and eight of 14 using their own information did so as well. The research shows that 97% of the participants entered their login information and continued when they were provided with a clear message that there were problems with the image authentication system and that it may not be secure.

Murky Trade in Bugs Plays Into the Hands of Hackers
New Scientist (06/16/07) Vol. 194, No. 2608, P. 30; C. Biever

Computer security consultant Charlie Miller believes the security of the Internet could be improved if researchers were offered financial incentives to search for and report software bugs, as the increasing complexity of software has made finding such vulnerabilities tougher and more time-consuming. As a result, many "white-hat" hackers no longer feel bragging rights alone are enough compensation for bug-hunting, which only serves to improve the chances of "black hat" hackers finding and exploiting the bugs for criminal purposes. Companies are offering money for zero-day bugs, which they use to create patches for customers who use their anti-intrusion products, but Miller says a typical payoff from these firms--estimated by University of Cambridge researcher A. Ozment to be between $2,000 and $10,000--is not enough to coax the top researchers to seek out bugs. Compensation for bugs is based on the severity of the vulnerability as judged by the buyer, which requires the bug hunters to disclose all their information on the bug to the company before an offer is made. This is a situation where Miller says the researcher has "no leverage at all." Compounding the problem is the existence of a black market for bugs run by malevolent hackers willing to pay top dollar, which can be a great temptation for researchers who feel they are not being fairly compensated. One alternative to offering more money for bugs is for companies to be more honest about how much they are willing to pay, giving researchers a clearer picture of how much a bug is worth before attempting to sell it. R. Bohme of Germany's Dresden University of Technology says such a strategy could also encourage firms to produce less buggy software.

Planned Worker ID Called Vulnerable
San Francisco Chronicle (06/25/07) P. A4; C. Lochhead

Various proposals to control illegal immigration rely on an electronic employer verification system that a Dept. of Homeland Security study criticizes as susceptible to identity theft, employer abuse, data inaccuracies, and privacy breaches, which could only be addressed through heavy enforcement. The detection of identity theft is not designed into the Web Basic Pilot system, and the size of such a system seriously complicates practical application, according to experts such as [[SRI International]] Computer Science Laboratory scientist P. Neumann, who cited the approach's many shortcomings in recent testimony before Congress on behalf of ACM. He said lawmakers often have unrealistic hopes for technological solutions to social problems, and referred to a series of government software development blunders

that include "many highly visible projects that have been late, over budget, or indeed abandoned after many years and large expenditures." Others mentioned that it was possible to build such a system, acknowledging that it would likely cost billions of dollars and require an immense technical effort. The DHS study concluded that the system is vulnerable to anyone disguised as an employer to gain access, and Neumann said there is no doubt that criminals would start creating "phishing" emails claiming to be from the DHS requesting worker data from unwitting employers. M. Aitken with the Society for Human Resource Management predicted that the increasing security of immigration documents will raise the likelihood "that US citizens' identities are going to be stolen and fraudulently used for employment by those who don't want to come out of the shadows," to the degree that the situation "will be worse than what we have now." ACLU legislative counsel T. Sparapani warned that the system would empower the government to refuse people the right to work on an unprecedented scale, while being ultimately ineffective.

New York Legislators Keep E-Voting Software in Public Hands
Computerworld (06/25/07), M. Songini

New York state voting activists are pleased that this year's New York senate and assembly session ended without changing the state's strict e-voting software escrow law. Activists were worried that pressure from the e-voting industry would force changes in the law that requires voting system vendors to place all source code and other related software in escrow for the New York State Board of Elections so it can be examined as necessary. The law also forces a voting system vendor to waive all intellectual property and trade secret rights if the software needs to be reviewed in court. Microsoft, whose Windows software is used in some e-voting devices, sought to amend the law to avoid the strict escrow provisions. New Yorkers for Verified Voting executive director B. Lipari says concerned citizens created a swell of support in the legislature to ensure the law remained unaltered and that about 3,000 constituent calls created a forceful reminder to lawmakers of their commitment to strong voting laws. "The voting machine vendors have known for two years what our laws said," says New York state assemblywoman B. Lifton. "We're holding firm on our current state law which calls for open source code." Lipari says Microsoft's proposed changes would ruin the source code escrow and review procedures in the current law. Microsoft says it does not make its source code available for escrow under election law because of concerns that the code could be disclosed to third parties without adequate protections for intellectual property rights.

When Computers Attack
New York Times (06/24/07) P. 4-1; S. Schwartz

Doomsayers have long been forecasting the digital equivalent of Pearl Harbor, when America's enemies attack US computer networks in the hopes of crippling vital infrastructure, but experts claim the reality of a cyberwar scenario is considerably less extreme. A. MacPherson of the University of New Hampshire reports that, unlike physical attacks, recovery from cyberattacks requires less of an effort, given the resilience of the Web. Although the US government has been preparing for a major digital assault, experts believe the United States gears up for cyberattacks every day through exposure to malware, meltdowns, glitches, and crashes, while there are very few points in the network where a single computer malfunction can cause a systemwide crash. Furthermore, human beings are also resilient, and a loss of services through one kind of medium can be offset through improvisation. Still, D. McPherson with Arbor Networks thinks a full-scale cybertattack could have enormous ramifications, although he contends that the effects of cyberwarfare on the Internet will be much sub-

tler than anticipated, in that "certain parts of the system won't work, or it will be that we can't trust information we're looking at." There is general consensus among experts that cyberwarfare is unlikely to resemble the recent blockage of online access to Estonian banks and government offices via distributed denial of service attacks, which was eventually attributed to tech-savvy activists protesting the relocation of Soviet-era war memorials, rather than the Russian government.