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

Δελτίο 165
30 Δεκέμβρη 2009

Scientists Promise an End to Web Attacks
V3.co.uk (12/07/09), D. Neal

Research on new encryption technology that has the potential to make cyberattacks "computationally impossible" will be presented at the ASIACRYPT 2009 Security and Cryptology Conference in Japan. P. Morrissey, N. Smart and B. Warinschi from the University of Bristol's Dept. of Computer Science will demonstrate how the technique can be used to prevent attacks such as denial of service. The approach also provides two-factor authentication that does not overburden users. The researchers will discuss how to transfer information between databases in a truly encrypted way in a second paper. Also, researchers from Bristol will present a third paper on the "basic constructions in cryptography," which they argue could be applied to applications such as the Web browser.

In Shift, US Talks to Russia on Internet Security
New York Times (12/13/09) P. A1; J. Markoff; A. Kramer

The US government has reversed its policy toward bolstering cybersecurity by initiating consultation with Russia, rather than the other way round. Officials familiar with the negotiations say the Obama administration understood that more countries are developing cyberweapons and that halting a global cyberweapons arms race required a new strategy. In November, a delegation led by a Russian Security Council member convened in Washington, DC with members of the US National Security Council and the Depts. of State, Defense and Homeland Security, and several weeks later the United States agreed to talk about cyberwarfare and cybersecurity with representatives of the United Nations committee on disarmament and international security. Russia has espoused the idea that an international pact is the best instrument for tackling the growing challenges posed by military operations to civilian computer networks, and people familiar with the discussions say the US's resistance to the concept has started to wear down. V. Sokolov with Russia's Institute of Information Security says the latest round of discussions signals the opening of negotiations between the two powers on a possible cyberspace disarmament treaty. An anonymous US State Department official says the United States has not resisted the idea of such a treaty, and that it is hoping to use the discussions to boost international cooperation in combating cybercrime. In contrast, the official says Russia has been pursuing the restriction of cyberweapons development. US officials involved in the negotiations say that in addition to the cyberweapons ban, Russia is focusing on a prohibition against cyberterrorism, which they claim is an attempt to ban "politically destabilizing speech."

Carnegie Mellon Researcher Says Privacy Concerns Could Limit Benefits From Real-Time Data Analysis, Carnegie Mellon News (12/17/09), B. Spice

Carnegie Mellon University (CMU) computer scientist T. Mitchell says society will be unable to capitalize on real-time data analysis technologies unless questions are resolved regarding how much of a person's life can be observed and by whom. Mitchell notes that data-mining techniques are increasingly being applied to personal activities, conversations and move-

ments, such as deducing people's movements and patterns by monitoring their smartphone. "The potential benefits of mining such data range from reducing traffic congestion and pollution, to limiting the spread of disease, to better using public resources such as parks, buses, and ambulance services," he says. "But risks to privacy from aggregating these data are on a scale that humans have never before faced." Mitchell says technology could help limit the misuse of data. One potential approach is to mine data from numerous organizations without ever aggregating data into a central repository. For example, individual hospitals could analyze their medical records to see what treatments work best for a particular flu strain, and use cryptography to encode the results and protect patient privacy, releasing only the findings. Mitchell says a public discussion about how to rewrite the rules of data collection, ownership, and privacy will be even more important than technological solutions. "Until these issues are resolved, they are likely to be the limiting factor in realizing the potential of these new data to advance our scientific understanding of society and human behavior, and to improve our daily lives," he says.

As Attacks Increase, U.S. Struggles to Recruit Computer Security Experts
Washington Post (12/23/09) P. A1; E. Nakashima; B. Krebs

Cyberattacks are increasing in frequency and sophistication at a time when the US government is struggling to address a shortage of proficient computer security experts. This shortage comes as the Pentagon is trying to staff a new Cyber Command that melds offensive and defensive computer security capabilities while the US Dept. of Homeland Security (DHS) plans to expand its own cybersecurity force by as many as 1,000 people over the next three years. Realizing that meeting this goal will be difficult, DHS is focusing on training people already in the federal government in cybersecurity skills. In November, the Government Accountability Office warned a Senate panel that the number of scans, probes, and attacks reported to the DHS' US Computer Emergency Readiness Team has increased by more than 300%. M. Kwon, former director of the readiness team, says that for years federal law forced most civilian agencies to spend their cyberfunds on security audits instead of on building a robust security program. K. Evans, the Bush administration's information technology (IT) administrator, points out that most federal IT managers do not know what advanced skills are required to counter cyberattacks. The National Science Foundation's Scholarship for Service program, which pays for up to two years of college in exchange for an equal number of years of federal employment, is a key element in the US government's initiative to cultivate cybersecurity talent. However, the private sector often offers much higher salaries for cybersecurity personnel than the private sector.

Obama Cyber Czar Choice Worries About Smartphones, Social Networking
Network World (12/22/09), T. Greene

Howard Schmidt, US President Obama's choice for cybersecurity czar, has previously worked in both the public and private security sectors and also has written a book on defending the Internet. He is expected to focus on a number of issues as he begins his new job. For instance, Schmidt - who helped produce the "National Strategy to Secure Cyberspace" while working for the Bush administration - could use the government to promote education and research and push vendors to make more secure products. "What is the government doing to make sure universities and companies have dollars to do research that will enhance security?" Schmidt said in an earlier interview. He added that there is research and development that needs to be done that may not improve homeland security but may make the Internet more secure. Schmidt also will likely work to make cybersecurity as big a priority as physical se-

curity. In addition, Schmidt could call for increased security on smartphones and other mobile devices, since he has said that cybercriminals will increasingly target these devices as they become more and more like computers. Finally, Schmidt will likely work to counter threats from terrorists to the US's cyberinfrastructure. Schmidt has said that terrorists are most likely to target financial institutions' IT networks, though attacking those systems will be difficult because of all the work the financial services industry has done to protect itself.

Securing the Information Highway
Foreign Affairs (12/09), Vol. 88, No. 6, P. 2, W. Clark, P. Levin

The cyberinfrastructure of the United States is under the constant threat of attack, and the US government must take quick and decisive action to protect these vital assets, write former NATO Supreme Commander W. Clark and P. Levin, CTO and Senior Adviser to the Secretary at the US Veteran Affairs Department. The authors draw parallels between cyberthreats and biological diseases, and note that "bodily immune systems work best when they are autonomous, adaptable, distributed, and diversified; so, too, with electronic security." They write that "as with their biological analogues, healthy electronic systems will focus protection at the gateways to the outside world (such as a computer's ports), rapidly implement sequential reactions to invading agents, learn from new assaults, remember previous victories, and perhaps even learn to tolerate and coexist with foreign intruders." Clark and Levin say the existence of a vulnerability will inevitably be discovered by a cybercriminal, and professionnal saboteurs will likely be unable to resist the lure of embedding intentional security holes. However, Clark and Levin note that the complete eradication of all threats to electronic security is both technically infeasible and unaffordable. "The best the United States can achieve is sensible risk management," they argue. "Washington must develop an integrated strategy that addresses everything from the sprawling communications network to the individual chips inside computers." Diversification of the US digital infrastructure is a starting point, while securing the hardware supply chain is an additional step. The adaptability of hardware means that the current configuration and deployment of computer networks will not have to undergo a fundamental shift.