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

Δελτίο 109
14 Μάρτη 2008

The New Art of War
Washington Post (03/03/08) P. A15; W. Pincus

Recent testimony before the Strategic Forces Subcommittee of the House Armed Services Committee focused on preparing for war in space and cyberspace. Space threats have received a significant amount of attention in the past, so it was the possibility of cyberspace warfare that received the most emphasis at the hearing. Head of US Strategic Command Gen. K. Chilton said cyberspace is an "emerging war-fighting domain" and that potential enemies understand the US's reliance on the use of cyberspace and are constantly probing the country's networks to find competitive advantages, which is why the nation needs to develop defensive and offensive cyberspace systems. Several strategies and institutions have already been created to protect cyberspace, including the classified 2006 National Military Strategy for Cyberspace Operations, which concludes that "offensive capabilities in cyberspace offer both the US and our adversaries an opportunity to gain and maintain the initiative." The Strategic Command and Joint Chiefs of Staff personnel are developing contingency plans and carrying out operations that protect the government's computer networks through detection and coordinated counterattacks against intruders. Chilton said the government is working "to operate, defend, exploit, and attack in cyberspace."

Secure and Easy Internet Voting
Computer (02/08) Vol. 41, No. 2, P. 08; G. Beroggi

A modular and service-oriented architecture was tapped as the platform for a fully scalable and portable Swiss e-voting system that allows people to cast votes using the Internet or cell phones, using two-step encryption and redundant storage systems to maintain the authenticity and confidentiality of votes, writes director of Canton Zurich's Statistical Office G. Beroggi. The system seamlessly integrates with traditional ballot-box voting so that all citizens can vote, and no digital divide splits the population. Six weeks prior to the vote, the communities in the participating cantons enter the names of all citizens eligible to e-vote in the electronic ballot box, which opens four weeks before the vote. To vote, citizens use a password that they receive from the canton's Statistical Office by mail as part of their voting forms. Citizens can vote through the Internet by logging onto the e-voting Web site using ID numbers and following the site's directions for vote casting, and the system accepts the vote if it perceives a match between the security symbol the voters enter and the one they got in the mail. The two-step encryption process involves the voter's client computer first encrypting the votes and ID and authentication characteristics, and the e-voting system then checking the incoming votes for their structure and integrity before again encrypting them, with the votes stored within a database by a pair of redundant subsystems. On the day of the vote, the results from the regular ballot box are fed into the vote registration software, and the e-voting system transfers the e-vote to the voting system that manages the regular votes once the regular voting ballot box is closed. Rather than making source code available, the e-voting system depends on the ACM Statement on Voting Systems, which recommends that e-voting systems "embody careful engineering, strong safeguards, and rigorous testing in both design and operation."

Online Vote Discussed for Florida
Miami Herald (03/08/08), M. Merzer

Internet voting advocates say the technology should be used if Democrats decide to hold a second primary election in Florida. They say an online election would offer security at least equal to a ballot by mail, would attract more voters, and would cost about $3 million, or about half as much as a mail-in election. Internet voting played a major role in the 2000 Democratic primary in Arizona, the 2004 Democratic primary in Michigan, and was used in 164 countries and territories last month for Democrats living abroad. "Not only can we save the party money, we can get it done faster and we can increase access significantly," says Everyone Counts CEO L. Steele. Florida's Democratic leadership is considering a ballot by mail if someone picks up the estimated $4 million to $6 million cost, and state party spokesman M. Bubriski says he has not heard any serious consideration of conducting a re-vote primarily over the Internet. Johns Hopkins University computer science professor A. Rubin says that beyond Internet voting's security and privacy issues, he worries that voters could be coerced to vote a certain way by an abusive spouse or an overbearing employer. "I think it is a terrible, terrible idea to take such a meaningful primary and give an attacker the opportunity to compromise privacy or intercept votes and change them," he says. Still, electiononline.org director D. Chapin says many people believe that Internet-based voting is an inevitability and a primary is a good test for the technology.

'Gambling DNA' Helps Fight Online Fraud
New Scientist (03/05/08)

University at Buffalo researchers R. Yampolskiy and V. Govindaraju are developing a system that is capable of tracking how often and how much a poker player bets, increases a bet, bets everything, or folds, and then creating a "gambling DNA" that online casinos can use to determine their identity. The system flags behavior as suspicious when a player does something that is not in line with their personalized profile. Yampolskiy says the software achieves an authentication accuracy rate of 80% within an hour and improves as play continues. J. Schaeffer of the University of Alberta Computer Poker Research Group is not convinced that the software will be as successful with the best poker players. "If you are predictable, you can be exploited," he says. "Strong players try not to be predictable."

Unique Locks on Microchips Could Reduce Hardware Piracy
University of Michigan News Service (03/05/08)

University of Michigan and Rice University computer engineers' Ending Piracy of Integrated Circuits (EPIC) framework outlines a method for giving individual microchips a unique lock and key to prevent hardware piracy by tapping established cryptography techniques and subtly modifying the chip design process without impacting chip performance or power consumption. The keys would be retained by the patent holder, and used to securely instruct the chip to unlock itself. The enablement of EPIC protection would allow each integrated circuit to be fabricated with some additional switches that function in the manner of a combination lock, and that can each generate an unchangeable random ID number. Rather than being built with an ID number, the chips would be manufactured with the tools needed to produce the number upon activation. Chips fabricated within the EPIC framework would only work properly when they are activated, and activation would require the manufacturer plugging the chip into a phone line or Internet connection and letting it communicate with the patent holder. The chip would securely send its ID number to the holder, who would record the number, deduce the combination to unlock the chip, and securely transmit the key back to the chip. "The goal of a practical system like ours is not to make something impossible, but to ensure that buying a license and producing the chip legally is cheaper than forgery," says UM professor I. Markov.

Computer Security Team to Report Hacking Into Defibrillator-Pacemaker
New York Times (03/12/08) P. C4; J. Feder

Computer security researchers say they were able to gain wireless access to a combination heart defibrillator and pacemaker in a lab. The researchers were able to reprogram the device, and to cause it to deliver jolts of electricity that would potentially be fatal if the device was in a person. The researchers were also able to obtain personal patient data by monitoring signals from the tiny wireless radio that was embedded in the implant as a way to enable doctors to monitor and adjust it without surgery. However, the researchers say that people with implanted defibrillators or pacemakers are not at risk yet since the experiment required more than $30,000 worth of lab equipment and a sustained effort by a team of specialists from the University of Washington and the University of Massachusetts to interpret the data. Additionally, the device the researchers tested was placed within two inches of the test gear. The researchers say the test results suggest that too little attention is being paid to security for the increasing number of medical implants equipped with communication abilities. "The risks to patients now are very low, but I worry that they could increase in the future," says University of Washington lead researcher T. Kohno.

Military Networks Increasingly Are Under Attack
Wall Street Journal (03/12/08) P. A7; Y. Dreazen

Gen. K. Chilton, the top US commander in charge of cyberspace, said the nation's military networks are being targeted by an increasing number of attacks. Chilton said there is evidence that links China to many of the incidents, though he did not formally accuse the Chinese government of involvement. A recent Pentagon report said that China was expanding its military power into cyberspace, which angered the Chinese. Although the People's Liberation Army repeatedly denies being behind the hacker attacks, the US government has linked China to several cyber attacks, including the hacking of a Pentagon email system used by the Secretary of Defense's office. A 2007 Government Accountability Office report warned that the nation's infrastructure, including water-treatment and power plans, are at risk of being targeted by a cyber threat. Chilton said the military is concerned that the increasing number of "mining" attempts could just be the beginning of a growing cyber threat. He said hackers could eventually attempt to knock out classified networks or slow down the nation's government, media, and financial Web sites. "You don't shut the system down completely, but you slow it down," Clinton says. "I would consider that an attack."

Cyber Preparedness Symposium Leaves Unanswered Questions
Dark Reading (03/07/08), T. Wilson

At the recent National Symposium on Unifying Cyber Preparedness Efforts, industry leaders and academic researchers agreed that better collaboration is needed to prepare for cybersecurity threats, but they couldn't agree on how to work together or even on what the threats are. The half-day discussion wavered between defending against attacks on the nation's government and infrastructure to resolving specific consumer PC vulnerabilities. Capitol College organized the symposium to discuss how government industry, critical infrastructure providers, Congress, and academia can cooperate to build a cross-disciplinary effort to prepare for and fight cyber threats. "We're simply stalled, as a nation, when it comes to cyber security," says Capitol College's V. Maconachy, former head of the NSA's information assurance training program. "We can no longer wait for somebody to take the lead." Maconachy urged government, industry, and academia to pledge to get involved in the cyber security effort, and to identify, coordinate, and combine the "silos of excellence" in cybersecurity.