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

Δελτίο 47
06 Νοέμβρη 2006

US Investigates Voting Machines' Venezuela Ties
New York Times (10/29/06) P. 1; T. Golden

The federal government is looking into last year's takeover of an American electronic voting machine manufacturer by a Venezuelan company. Smartmatic Corp. was a fledgling firm before being chosen by the Venezuelan government to handle the country's election machinery. Several months before this decision, another small voting machine company, owned by some of the same people as Smartmatic, received a $200,000 investment from a government agency and joined Smartmatic in its bid for Venezuela's electronic voting contract. Smartmatic then acquired Sequoia Voting Systems, which has voting equipment in place in 17 states and the District of Columbia. Recent public documents do not clearly show involvement of the young engineers who started Smartmatic, and the company has been restructured into an intricate web of offshore companies and foreign trusts. C. Maloney, congresswoman from New York said, "The government should know who owns our voting machines; that is a national security concern.. There seems to have been an obvious attempt to obscure the ownership of the company." The Miami Herald revealed that Bitza, the company that received a $200,000 investment from the government, was inactive before receiving the money from the Venezuelan Finance Ministry, which took a 27% stake in the company. Only weeks before Bitza and Smartmatic won their contract, Omar Montilla, former adviser to Chavez on election technology, was appointed to Bitza's board. Sequoia's M. Stoller insists that "no foreign government or entity, including Venezuela, has ever held any stake in Smartmatic." Some Sequoia voting machines experienced delays and irregularities in Chicago during the March primary. Some of these problems were due to a software component that transmits results to a central computer that was developed in Venezuela.

'Gambits' Are a Risk to Internet Domain System
International Herald Tribune (10/29/06), V. Shannon

ICANN Chairman Vint Cerf is cautioning against undue haste in integrating non-Latin characters within the Domain Name System. Not pointing a finger at anybody, but mentioning China and the International Telecommunication Union (ITU), Cerf says that politics and allegations that the US has too much control of the DNS could lead to a splintering of the World Wide Web. "My concern is the potential for suddenly choosing another path after ICANN has already put in six years of work on this," says Cerf. "Either they will fail, or they will break the Internet." Presently, only 37 Western characters can be used in Internet addresses. ICANN has begun to implement a plan that would allow tens of thousands of other characters from the world's various languages to be used, but testing has shown the potential for problems. "It is turning out to be quite difficult to integrate this very large character set in a way that is safe and stable and will work with many applications for many decades to come - to future-proof it," says Cerf. The comments come on the eve of the first ever UN-sponsored Internet Governance Forum in Athens and a week before the ITU will open a three-week conference in Turkey in which the internationalization of Internet governance is sure to be a key topic.

At 30, Crypto Still Lacks Usability, Experts Say
CNet (10/28/06), J. Evers

Thirty years of public key cryptography were recently celebrated and remembered by experts in Mountain View, Calif. Much of the discussion centered on the obstacles presented by the US government, which were lifted in 1996. B. Snow, a retired technical director at the Natioal Security Agency, was present to provide the government's perspective. "This, for us, was a weapon," Snow said. "And this was possible free release of weapons and we needed to defend the nation to other nations who could be opponents at the time." J. Bidzos, who was chief executive of RSA in 1986, recalled the difficulty presented by the NSA in moving cryptography out of the research stage and into development: "We found ourselves competing with NSA, especially in the 90s." One of RSA's first customers, R. Ozzie, currently chief software architect at Microsoft, was working on securing what would become Lotus Notes in 1986 when he ran into government restrictions. "I had no clue," he said. "Initially we had wanted to use hefty keys...We had spent years working on it, and after the 3rd meeting (with the government), I thought we were dead." With the rise of Web 1994, borders were eliminated and the need for secure electronic commerce arose. Government export regulations were eased by 1996, allowing widespread adoption of cryptography. While the government has taken a completely opposite view on cryptography, often requiring it, "the remaining issue that is big today on the plate is lack of quality on the products," said Snow. With Microsoft, Ozzie plans to incorporate encryption into products, taking compliance issues into consideration. "In early years, we as an industry could blame the system for controlling the pace of innovation because the government was throwing up roadblocks," explained Ozzie. "At this moment in time, it's laziness on the part of the industry in terms of not embracing architecture and the importance of human interface in design of secure systems."

Rutkowska: Anti-Virus Software Is Ineffective
eWeek (10/26/06), R. Naraine

Stealth malware researcher Joanna Rutkowska recently demonstrated a way to infect Windows Vista with a rootkit and introduced Blue Pill, a new concept that uses AMD's SVM/Pacifica virtualization technology to create "100% undetectable malware." Hardware virtualization, in her opinion, "has been introduced a little bit too early; before the major operating system venders were able to redesign their systems so that they could make a conscious use of this technology, hopefully preventing its abuse." Blue Pill operates by creating a hardware virtual machine and moves the native operating system to this virtual machine, becoming a "hypervisor" itself. The native system doesn't even realize it's been moved to a virtual machine. Rutkowska explains that operating systems need to be aware of such virtualization and have their own hypervisor. In her opinion, "we need at least two to three years to implement a foolproof protection against hardware virtualization-based malware." Her ideal solution would be "integrity checking of all system components," but she realizes the difficulties involved. Blue Pill is an example of this undetectable, Type III, malware, which "does not introduce a single byte modification into kernel, or other processes' memory." The only chance for detection would be finding side effects. Rutkowska believes it is better to have "a good integrity-based scanner, even if it's not capable of detecting Type III malware, rather than having a classic anti-virus product which only tries to find the known 'bad things.'" Stealth malware can silently subvert an operating system without being noticed, so to Rutkowska, the most pressing concern is not the complete prevention of malware infections, but the ability to detect them.

The Economics of Information Security
Science (10/27/06) Vol. 314, No. 5799, P. 610; R. Anderson; T. Moore

The economics of information security has recently emerged as a field characterized by prosperity and rapid momentum, write University of Cambridge researchers R. Anderson and T. Moore. The assembly of distributed systems from machines owned by principals with different interests demonstrates the increasing value of incentives in assuring reliability. Indeed, incentives are coming close to equaling technical design in importance. Anderson and Moore note, for instance, that public disclosure of vulnerabilities gives vendors an incentive to correct bugs in subsequent product releases. "Consumers generally reward vendors for adding features, for being first to market, or for being dominant in the existing market--and especially so in platform markets with network externalities," the authors write. "These motivations clash with the task of writing more secure software, which requires time-consuming testing and a focus on simplicity." The new information security economics discipline offers key insights into general topics as well as into specific security issues such as bugs, phishing, spam, and law enforcement strategy. General issues include peer-to-peer system design, the best balance of effort by programmers and testers, the reasons behind the erosion of privacy, and the politics of digital rights management. Anderson and Moore point out that the work of information security economics researchers has begun to reach into other disciplines, including general security economics and dependability economics.

The Next Voting Debacle?
IEEE Spectrum (10/06) Vol. 43, No. 10, P. 12; S. Cherry

Help America Vote Act (HAVA) guidelines disqualify people from voting in all but one of the 50 states if they are not on the voting rolls, and this could disrupt the November elections because the databases that contain the rolls have been around for a short time and were not all built in compliance with best database industry practices. The HAVA rules were set up to address the lack of coordination between state and county governments in maintaining voter rolls. HAVA gives states a variety of options in responding to mismatches between a voter's registration information in the database and the data in other databases, and state officials in Texas, Washington, California, South Dakota, and Iowa have used this latitude to jettison many registrants, according to the New York University School of Law's Brennan Center for Justice. Most mismatches are related to new voters, voters who change their name, and those who relocate; typos made by election officials can also cause mismatches, which is frustrating to people such as the Brennan Center's W. Weiser, who says such errors could be avoided through automated techniques developed by database experts that many states did not use. States are required by law to "verify" the voter rolls, but they do not have to necessarily take action against registrants whose names or addresses are unverifiable. The massive mismatch purges in California and elsewhere may have been partly stimulated by the opinion of a lawyer in the Justice Department's Civil Rights Division, who told Maryland officials that mismatches between a registration application and motor vehicle or Social Security records should make the applicant ineligible for addition to the voter rolls. The final decree over a mismatch highlights a basic problem in terms of voter eligibility as well as HAVA: An excessively simple, law-mandated way to register and vote makes it easy to cast multiple ballots and commit other forms of voter fraud, while an overly difficult registration process results in voter disenfranchisement.

Voters in Fla., Texas Complain of E-Voting Glitches

Computerworld (11/01/06), M. Songini

Allegations were made in Miami-Dade County, Fla. that e-voting machines flipped votes, meaning the candidate chosen was not the one registered by the machine. Officials denied these claims. "I'm happy to report that there are no glitches in any of the electronic voting machines at Miami-Dade early voting locations," said L. Sola, supervisor of elections for the county. Subsequent investigation of the Election Systems & Software machines also reported no problems. Sola explained that when a machine is reported to be malfunctioning, it is closed until a technician is available. He assures that no votes were lost. Neighboring Broward County also experienced reports of vote flipping on the same company's machines. P. Corwin, assistant to the Broward County administrator, said that such problems are common for a small portion of voting machines. Several complaints have also come out of Texas concerning vote flipping, but Texas Secretary of State R. Williams contacted the Florida judges who assured him that a fingernail or some other object had inadvertently hit the wrong button. A spokeswoman for Williams points out that "this only serves to emphasize the importance of the summary screens, where a voter can make sure the correct ballots are cast." A. Rubin, e-voting critic and Maryland election judge, said, "While most of my comments about e-voting have to do with security threats that are invisible, I am also discouraged by the widespread technical problems that are not just noticeable, but screaming for attention."

GAO: Better Coordination of Cybersecurity R&D Needed
Government Computer News (10/31/06), P. Wait

The Government Accountability Office (GAO) has issued a report stating that the federal government is doing an insufficient job of coordinating R&D on cybersecurity matters and must improve its information sharing and collaboration efforts concerning cybersecurity. The director of the White House's Office of Science and Technology Policy has been called upon to create a strict time line for compliance with the federal cybersecurity R&D agenda, released in February 2003 by the National Strategy to Secure Cyberspace. "Most cybersecurity technologies "offer only single-point solutions by addressing individual vulnerabilities," the GAO report states. "As a result, many researchers have described the use of these types of near-term solutions as being shortsighted. Research in cybersecurity technology can help create a broader range of choices and more robust tolls for building secure, networked computer systems." Cybersecurity R&D funding is divided between a number of agencies: Homeland Security, which allocated about $17 million of its funds in fiscal 2006 to the subject; DoD, which was provided with about $150 million in fiscal 2005 by the federal government for cybersecurity R&D; and NSF, which requested about $94 million for their effort in fiscal 2006.

Tech's Threat to National Security
Business Week (11/02/06), S. Hamm; D. Kopecki

The Dept. of Defense's use of software that has been outsourced has led to concern that malicious programming could endanger national security. In 2001, the Defense Security Council noticed a significant rise in "suspicious attempts" by hackers abroad, and declared that foreign software companies and applications developed overseas were potentially a bigger threat than domestic hackers. In one of two attacks since July, a bureau of the Commerce Department had to cut off Internet access and get rid of virus infected computers due to an attack by Chinese hackers. "It's clearly a legitimate and present security concern," as the use of high-tech combat systems continues to increase, says P. Kaminsky, a member of the Defense Science Board. A DoD task force is currently in the final stages of creating a recommendation for how to deal with the fact that the military uses software bought from overseas developers. There is much concern among the industry that the Pentagon will force tech suppliers to eliminate elements of overseas production, or return to purchasing too many custom-made products, both of which would drive prices up significantly. "Most of the software the DoD uses has elements that are written overseas, and that isn't a problem," says William Schneider Jr., chairman of the Defense Science Board "The problem is in ultrasensitive defense applications where they are mission-critical" and the highest degree of confidence in the software is required. Vendor screening and software testing has been stepped up by the pentagon recently, but costs are rising for extensive testing on increasingly sophisticated weapons systems.

Quantum Attacks Worry Computer Scientists
Security Focus (10/31/06), R. Lemos

While quantum computers may one day be capable of unprecedented calculations, they are incredibly vulnerable to failure caused by unauthorized activity when networked together. D. Lidar, an associate professor in electrical engineering, chemistry, and physics at the University of Southern California, and L.-A. Wu, a research associate in the Chemical Physics Theory Group at the University of Toronto, are working on ways of defending quantum computer networks against something as small as a read access to a single qubit on one machine, which would require a network-wide reset. Their solution has been to only send messages at prearranged, seemingly random intervals, use long average wait times between legitimate network connections, and fill the rest of the network time with decoy transmissions. Performance advantages could be maintained while reducing the chance of a successful attack. "We would not want to use this method against any threat beside malware, because it is not efficient," says Lidar. "We are talking the network down for a long period of time." Quantum computers must be protected against "stray cosmic rays and things like that--if they interact with this stuff, then something changes and the computer crashes," according to J. Lowry, a principal scientist at the Internet service provider BBN, and member of the company's research team working on the DARPA quantum network. "The thing is that people could do that on purpose." Lidar doesn't know what form an attack would come in; data destruction or circumventing a calculation would be the easiest. He says, "Quantum malware to us just looks like any malicious instruction sent to an attacker. As long as we can keep the local nodes free from malicious intruders and build a heavily fortified castle around them, we can assume the ancilla qubits are malware free."

Phishers Beware
CITRIS Newsletter (10/06), J. Shreve

Researchers at CITRIS' Team for Research in Ubiquitous Secure Technology (TRUST) have developed tools that help defend Internet users against online identity theft. "The threats and risks and vulnerabilities change everyday. It's moving at a very fast pace. All the tools, processes, and policies, and procedures are reactive for the most part. And the attackers are in a global environment, attacking from foreign countries we can't reach out to...We're inundated," says R. Rodriguez, former secret service agent who directed the Secret Service West Coast Electronic Crime Taskforce and is now working with CITRIS. Rodriguez approached J. Mitchell and D. Boneh of Stanford University with his concerns three year ago, and the two have now completed five Web browser extensions: one encrypts passwords so they cannot be used by a thief; another alerts users when they have landed on a fake site; two protect Firefox users against malicious programs that track the sites they visit; and the last is a resource that blocks passwords from any keylogging software embedded on an unknowing user's computer. "One of our best outcomes for us would be to have some of the ideas we've developed in our prototype software get adopted and built into browsers," says Mitchell. Social and legal aspects are also being addressed, including more effective notices to warn users of the risk of downloading unknown software.