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

Δελτίο 60
8 Φλεβάρη 2007

Florida Shifting to Voting System With Paper Trail
New York Times (02/02/07) P. A1; A. Goodnough; C. Drew

Florida Governor C. Crist yesterday announced that the state will do away with touch-screen voting machines in favor optical-scan machines in time for the 2008 election. This decision, coupled with proposed federal voting legislation requiring independent audit abilities, could signal the end of touch-screen machines. "For Florida to be clearly contemplating moving away from touch screens to the greatest extent possible is truly significant," said VoteTrust USA director W. Stewart, stressing the symbolic importance of Florida in US elections. Many other states have called for paper trails, although no decision has been made as to whether they will scrap touch-screen machines or simply retrofit them with printers. The 15 Florida counties that already have touch-screen machines in place will be allowed to use them in the early voting before the 2008 elections. "The price of freedom is not cheap," said Crist. "The importance of a democratic system of voting that we can trust, that we can have confidence in, is incredibly important." He also announced that the state will work to help the blind and speakers of foreign languages use the optical-scan machines. A recent survey by Election Data Services found that 56% of US counties have purchased optical-scan machines, which experts say are cheaper than touch screens. Rep. R. Holt (D-N.J.) will propose a bill that requires a paper trail and authorized $300 million in federal money to implement the necessary changes.

UIC Team Ready to Get Medieval on Spammers
Chicago Sun-Times (01/31/07) P. 64; S. Guy

University of Illinois computer science department head P. Nelson has developed Spamalot, an anti-spam system intended to trick spammers into wasting time and money, or even getting themselves caught. "The whole idea is to create a system that starts a dialogue with the spammers or their systems, consuming their resources so the spammers can no longer send their messages inexpensively," said Nelson. Spamalot is set-up in an email account and is able to detect the type of spam it receives and respond in kind. Three different agents can be deployed based on the type of spam. Arthur handle Nigerian spammers, those who tell people that a rich oil baron has died and the sender needs to find someone's account to transfer the oil baron's money into. Patsy takes on requests to enter sensitive information in mortgage application and prescription medicine forms, and Lancelot goes after phishers. Lancelot works by providing phishers with a false password and user name that is coded so a bank can track it and shut down the computer from which it is used, and potentially prosecute the spammer. Another method to foil spammers is to have them call a monitored telephone line, a technique used by Nelson when he first had the idea for Spamalot. The system is currently being tested in the school's AI lab.

Project Analyzes Internet Security
The State News (01/29/07), K. Jourdan

Michigan State University professors R. LaRose and N. Rifon believe that continuing user education offers a way for computer users to be more proactive with computer security. The two conducted a national survey of 557 home Internet users last year and found that only about 10% said they felt safe when surfing the Web. "There are a lot of automatic protections available through software companies and Internet service providers, but they aren't totally protective," says LaRose, a telecommunication, information studies and media professor. Today, hackers and computer criminals are hoping that Internet users will open email attachments, click on pop-up advertisements, download files from the Web, and follow the instructions in phishing emails. The school plans to launch a campaign about the potential risks online. R. Wiggins, senior information technologist for Academic Computing & Network Services, says computer users should turn on a personal firewall, use current antivirus software, and stay alert. "We're trying to push the necessity aside from automatic protection but want user education to continue," says LaRose.

A Sense of Security
The Engineer Online (01/30/07)

An EU-funded project will develop a mobile device that monitors the vital signs of elderly users and can even predict falls before they happen. The Complete Ambient Assisted Living Experiment will implement wireless technology, GPS, and various sensors to keep track of physical parameters such as ECG monitoring, oxygen saturation, and heart rate. The fall detection system would use accelerometers that could tell the mobile device that a fall was about to occur. Rather than being in constant communication, the mobile device, a modified wireless phone, would collect data when a fall is predicted or vital signs show dangerous changes, in order to conserve bandwidth and power. GPS would be used to alert emergency response services to the user's location if the device's algorithm detected that they are in trouble. The project aims to use as many standard and commercially-available technologies as possible, including a Web cam set up with a simple PC to allow care takers to check in on the user at any time. "The key is we are planning an open system with plug-and-play architecture so the mobile sensor networks can accept any new sensors being plugged in," says Plymouth University School of Health Informatics' M. Boulos. He expects future projects to focus on niche markets such as blood-glucose sensors for diabetics. A prototype of the system should be ready for testing next year.

Demo '07 Conference Showcases Encrypted Messaging, Inkless Printing
InformationWeek (02/01/07), T. Claburn

Demo '07 showcased many new products as well as the emerging attitude of placing priority on the customer rather than technology. One example of the user-friendliness trend is the Ceelox program that allows users to embed hidden data in images, hopefully spurring the sharing of coded messages by both customers and advertisers. Shipwire.com, a startup, introduced a shipping service that lets customers outsource the shipping, receiving, and warehousing of products that is not linked to any online store. An online service by 6th Sense Analytics was on display that allows programmers to keep track of development done by dispersed collaborators. The Inkless printing system demonstrated by Zink uses paper that contains ink, opening up the possibility for devices such as digital cameras to print out images. A thin, multi-core system on a chip computing architecture was shown off by Wyse Technologies. The platform allows users to run Windows without a PC and without the performance suffering. Adobe's newest application Apollo received a lot of attention for its ability to let developers work on and offline on a desktop that can easily be synchronized.

Research Aims to Detect Online Terrorist Activity
CSO Online (01/07), D. Daniel

The Department of Homeland Security and researchers at Rutgers University, the University of Southern California, the University of Illinois at Urbana-Champaign, and the University of Pittsburgh are finalizing contracts for a project that will lead to the development of new technologies for monitoring terrorist activity online. The researchers are expected to begin work on improving information analysis and computational methods as soon as the contract details for the three-year, $10.2 million grant have been completed. Announced by DHS last July, the project is expected to encompass mathematics graph theory, dynamic data analysis, optimization, "machine learning," and statistical analysis. The researchers will explore these methods as they create algorithms that are able to delve into public sources such as news stories and blogs to find patterns and relationships that may help lead to the discovery of terrorist plans. The technology will have to handle the enormous amount of information online, changing sources, and its pace of flow. Moreover, the tools must determine the credibility of the information.

Study Finds Security Flaws on Web Sites of Major Banks
New York Times (02/05/07) P. C3; B. Stone

Harvard University and Massachusetts Institute of Technology researchers recently discovered that banks using images as a secondary security protocol on customer accounts are providing little added protection to those consumers. Supporters of the technology, known as site-authentication images, indicate that if consumers do not see their selected image on a Web site before entering their account password, they will opt not to enter their information. Participants in the study saw a maintenance or error message on the screen where their images were usually located, though the message contained obvious spelling errors. However, only two of 60 participants in the study opted not to enter their password when their images were disabled. MIT computer scientist S. Schechter says, "The premise is that site-authentication images increase security because customers will not enter their passwords if they do not see the correct image. From the study we learned that the premise is right less than 10% of the time." The imaging technology had been adopted by Bank of America, ING Direct, and Vanguard as a way to improve online banking security after a 2005 Federal Financial Institutions Examination Council study indicated that passwords alone were not enough protection against identity thieves. Federal guidelines expect banks to develop a secondary security system and have it implemented by January 2007, but the Council has not enforced the regulations yet. Harvard research R. Dhamija says the study showed that site-authentication technology is fundamentally flawed and can give users a false sense of security.

Quantum Cryptography Offers Spy-Proof Code
IT World Canada (02/01/07), N. Arellano

University of Calgary researchers are working with quantum physics to develop a code that becomes scrambled if it is compromised. Today's code relies on algorithms and is safe unless the device that produces the key is lost or stolen, or if a global registry key is lost, but quantum cryptography would encode data into light photon particles, the state of which would be altered if the code was intercepted. Only authorized recipients would have the keys needed to access the data, so if a third party tries to intercept the code using a man-in-the-middle plot, the code would clearly show it. The system also provides a higher degree of randomness, as a result of key exchanges that can occur many times without compromising data transmission

speed. University of Calgary Centre for Information Security and Cryptography physicist and principal researcher W. Tittel is working on transmitting the code key using light photons and the rest of the message via standard encryption methods. Once the key has been sent, and the recipient confirms a secure connection, the message can be sent. Tittel proposes a transmission rate of one million bps over 100 km. Analyst J. Quinn says that the deploying necessary fiber optics through desktops could be prohibitively expensive, and that hackers could get around this technology if quantum computing catches up with quantum cryptography. To these claims, Tittel responds that existing fiber networks could handle the transmission, that fiber optics could be selectively added for important personnel, and that quantum computers would not change the fact that photons would show signs of attempted interception. Tittel estimates that the technology is about 10 years from being ready for the market.

Schneier: In Touch With Security's Sensitive Side
Dark Reading (02/01/07), K. Higgins

People's thoughts and feelings about security, as interpreted through brain heuristics, will be the focus of security guru B. Schneier's talk at next week's RSA Conference, whose theme is the exchange between security and psychology. "If we in the [security] industry expect to build products, we need to understand our customers," Schneier argues. He characterizes security as both reality and a feeling, with the former based on likelihood and risk and the latter based on psychological responses to risk and "countermeasures" to security threats. Schneier says neuroscience can help describe the frequent disconnect between perception of risk and reality, which he traces to a lack of interplay between the sensory processing of the amygdala and the analytical processing of the neocortex, leading to situations in which emotion overrides logic. The security expert draws a direct link between the failure of products and vendors' lack of consideration for the psychological aspects of security in the design of the user interface. "My belief is that making you aware of [brain chemistry] goes a long way" toward making better security decisions, Schneier concludes. "If you can understand you are just reacting from fear, you have a better shot at... understanding these human biases. Hopefully you can short-circuit them and improve on them and make it so we are not slaves to this."