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

Δελτίο 36
16 Αυγούστου 2006

Scratch-and-Vote System Could Help Eliminate Election Fraud
Technology Review (08/09/06), D. Graham-Rowe

A new lottery-style scratch-and-vote card that voters could verify might put to rest the security concerns that have long plagued electronic voting systems. With current touch-screen systems, "there is no way for an individual voter to know that his or her vote has been properly counted," said Microsoft's J. Bernaloh. "Even election officials cannot be certain that the systems are free of errors." Even with paper receipts, voters are still relying on other people and procedures to count their votes. While encryption-based systems can be audited to verify their accuracy, it is important to ensure that voting remains anonymous, says B. Adida of MIT's Computer Science and Artificial Intelligence Laboratory. Paper-based systems produce a unique number that can be traced back to identify a voter's name. S&V schemes can be used with existing election systems, including one recently developed by University of Newcastle-upon-Tyne cryptographer P. Ryan. Ryan's system places candidates' names on one side of the ballot in random order, with the tick boxes on the other. The voter tears the ticket in half after placing his vote, and a cryptographic code then matches the sequence of candidates on each side of the ballot. The challenge that Ryan's system faces is verifying that the encrypted information accurately correlates the order of candidates' names, but the S&V approach would secure the auditing process because it furnishes a paper ballot that would not pass through an election official's hands. A voter could simply scratch off the surface of the ticket to reveal a number that, when combined with a number that corresponds with the sequence of candidates and a public encryption key, would determine whether a ballot has been rigged. Voters could also use S&V cards to check to make sure that their votes have been counted after the election by verifying that the ballot code on their paper receipt matches the encryption code. Though new systems like these will be difficult to adopt on a widespread basis, they could represent a significant step forward in ensuring voting security, says M. Shamos, co-director of Carnegie Mellon University's Institute for eCommerce.

JitterBugs Could Turn Your Keyboard Against You, Steal Data
Penn News (08/07/06), G. Lester

Peripheral devices such as keyboards, microphones, and mice could pose an entirely new computer vulnerability, researchers at the University of Pennsylvania have found. Using a device known as a JitterBug, the researchers found that a hacker could physically bug a peripheral device and steal chunks of data by creating an all-but-imperceptible processing delay after a keystroke. The researchers built a functional JitterBug keyboard as proof of concept. "This is spy stuff. Someone would need physical access to your keyboard to place a JitterBug device, but it could be quite easy to hide such a bug in plain sight among cables or even replace a keyboard with a bugged version," said G. Shah, a graduate student in Penn's Department of Computers and Information Science. "Although we do not have evidence that anyone has actually been using JitterBugs, our message is that if we were able to build one, so could other, less scrupulous people." Unlike keystroke loggers, which have to be physically installed and then retrieved to collect data, the JitterBug needs only to be installed. The device can use any interactive network-related software application such as email or instant

messaging to relay the data, leaking it through split-second keystroke delays. Limited storage space on the device would prevent the JitterBug from recording every keystroke, but could be trained to record a certain type of activity prompted by a specific keystroke. "For example, one could pre-program a JitterBug with the user name of the target as a trigger on the assumption that the following keystrokes would include the user's password," Shah said. In one particularly alarming scenario, a manufacturer of peripheral devices could be compromised, inundating the market with JitterBugged devices. Shah's initial research suggests that cryptography could be used to protect against JitterBugged devices.

$2.4 Million to Develop Computing Security Technology
University of Pittsburgh News Bureau (08/07/06)

The University of Pittsburgh will serve as a University Affiliate Center (UAC) that will aid the US Department of Homeland Security (DHS) in its effort to gain the information analysis capability to analyze free text for potential terrorist activity. DHS will provide Pitt with $2.4 million over the next three years to develop advanced computing technology that can find common patterns in a wide range of information sources. "The goals of the work will be to identify facts and entities, as well as beliefs and motivations, expressed in text, and to create new methods for linking events and beliefs across documents, and tracking them over time," explains Janyce Wiebe, lead researcher and a computer science professor at Pitt. Cornell University and the University of Utah will participate in the Pitt UAC, which will work closely with the Institute for Discrete Science, the joint initiative of DHS and several National Laboratories that is working to improve the software algorithms and architectures used in a variety of computing applications. "The biggest challenge facing this critical area is the need for improved methods to quickly and accurately analyze, organize, and make sense of vast amounts of changing data," adds Jeffrey W. Runge, acting under secretary for Science and Technology. Rutgers University, the University of Illinois at Urbana-Champaign, and the University of Southern California are also serving as UACs, with each focusing on a specific area of research identified by Congress.

Debate Over E-Voting Is Still Plaguing Elections
National Journal's Technology Daily (08/09/06) Casey, Winter

The controversy surrounding e-voting systems, which has been raging since their rapid deployment in the wake of the disputed 2000 presidential election, shows little signs of subsiding. New complaints have emerged in Georgia about a primary election in which Rep. C. McKinney was roundly defeated. "Electronic voting machines are a threat to our democracy," McKinney said after the election. "So let the word go out: We aren't going to tolerate any more stolen elections." Diebold has reiterated its position that its machines are accurate and reliable. Meanwhile, several states have yet to comply with the 2002 Help America Vote Act, according to the Committee on a Framework for Understanding Electronic Voting. This year's primaries mark the first large-scale deployment of electronic voting systems, and the relationships between election officials and equipment vendors have become increasingly strained, the committee has found. The panel also warns that proper training for poll workers will be an important issue for the November elections.

Intrusion-Tolerant Middleware: The Road to Automatic Security
IEEE Security & Privacy (08/06) Vol. 4, No. 4, P. 54; P. Verissimo; N. Neves; C. Cachin

The concept of intrusion tolerance, a methodology designed to fortify computer systems against attacks and accidental faults by seamlessly addressing both issues via a common security and dependability strategy, is the heart of the Malicious-and Accidental-Fault Tolerance for Internet Applications (MAFTIA) project. Intrusion tolerance is a measure of last resort that acts after an intrusion but prior to a system failure, based on automatic methods dependent on local mechanisms and distributed protocols, and that combine detection, recovery, or masking tactics. Intrusion-tolerance mechanisms are selectively employed by the MAFTIA architecture to construct tiers of progressively more trusted components and middleware subsystems from untrusted elements such as hosts and networks. The architecture can be represented in at least three distinct dimensions: A hardware dimension comprised of the host and networking devices that make up the physical distributed system; the local support services supplied by the operating system and runtime platform in every node; and distributed software, the middleware layers that piggyback on the runtime and support each host's provided mechanisms as well as the native MAFTIA services of authorization, intrusion detection, and trusted third parties. The architecture can support components with different types and severity of attacks, intrusions, and vulnerabilities concurrently via architectural hybridization, which marries high performance at the level of controlled failure systems to high resilience at the level of arbitrary failure systems. This concept allows the realistic deployment of the wormholes model, a hybrid distributed-system model that assumes the existence of augmented distributed-system elements or wormholes that can provide stronger behavior than is postulated for the rest of the system. The MAFTIA middleware's layers, from lowest to highest, are the multipoint network (MN) module, the communication support services (CS) module, and the activity support services (AS) module. Each module feeds into failure detection and membership management.

IT Versus Terror
CIO (08/01/06) Vol. 19, No. 20, P. 34; B. Worthen

Data mining is the counterterrorism IT technology of choice for the US government and intelligence community, according to experts. "There is a real fear of not going down this path, because if there is value you don't want to be on the side that opposed [a data mining project]," notes former deputy director of the Defense Advanced Research Projects Agency's Information Awareness Office R. Popp. The government has thus far avoided viewing data mining in the context of IT value, preferring to call the apprehension of terrorists all the validation the methodology needs, according to former Homeland Security Department CIO S. Cooper. F. Cate of the University of Indiana's Center for Applied Cybersecurity Research maintains that "As far as the oversight process is concerned, it is clear that [data mining to prevent terrorism] is a disaster." Data mining experts argue that the government's antiterrorism IT strategy should be rigorously analyzed in the same manner that corporate CIOs vet company IT projects. Experts also recommend that the government avoid defining IT projects--those involving data mining in particular--too broadly, citing examples of systems such as Capps II and Secure Flight whose implementation is repeatedly delayed and whose generation of false positives is unacceptable. Still, there is a general consensus among data mining experts that the technique can effectively fight terrorism, provided that it is managed appropriately. Cate says, "There are some extraordinarily smart people [working on data mining systems], and I would be hard pressed to think that they are wasting their lives on something that doesn't work...But one of the things [the Defense Department's Technology and Privacy Advisory Committee] kept focusing on was that you have to be able to show that it works within acceptable parameters."