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

Δελτίο 37
27 Αυγούστου 2006

Military Research Aims to Develop Self-Configuring, Secure Wireless Nets
Network World (08/16/06), R. DeBeasi

Researchers from the government, academic, and corporate communities are developing a self-configuring network that could intelligently route and cache data and provide fast and reliable data sharing, while still adhering to the highest levels of security. The Knowledge Based Networking project draws on the concepts of artificial intelligence and the Semantic Web, and technologies such as the Mobile Ad-hoc Network (MANET), cognitive radio, and peer-to-peer networking. While the system is being built for soldiers in the field, the research could also be used in commercial applications. Current wireless technology is more about access than networking, said DARPA's Preston Marshall, adding that eventually a decentralized MANET could come to replace the current model of access points that connect wireless devices to a network. "The thing that's fundamentally different in a wireless environment is that the links are fairly unreliable...nodes join and leave the network more or less randomly," said D. Passmore of the Burton Group. MANETs would have no one point of failure, whereas existing networks can be shut down simply by removing an access point. Ideally, a MANET would be able to identify the best paths for routing data packets and select the optimal radio frequency to use through cognitive radio technology. While the artificial intelligence facet of this technology is still being developed, the military is already using the underlying software-defined radios that enable networks to switch signals on the fly. Beyond merely making decisions about the wireless spectrum, Preston envisions intelligent nodes that could automatically optimize the network. Similar to the concept of the Semantic Web, such a network could actually understand the meaning of the data it is transmitting.

Judge Rules Against Wiretaps
Washington Post (08/18/06), D. Linzer, E. Nakashima

The National Security Agency's (NSA) warrantless surveillance program to eavesdrop on Americans' telephone calls and emails, ostensibly to uncover terrorist activity, was declared unconstitutional by US District Judge A. Diggs Taylor on Thursday. She ruled that the program acts in violation of privacy and free speech rights, the constitutional separation of powers among the three branches of government, and the 1978 Foreign Intelligence Surveillance Act. In her 43-page opinion, Taylor wrote, "It was never the intent of the framers to give the president such unfettered control, particularly where his actions blatantly disregard the parameters clearly enumerated in the Bill of Rights." Efforts by the Bush administration and Sen. Arlen Specter (R-Pa.) to gain approval for legislation that would permit Bush to submit the NSA program to a clandestine court for legal review could be hindered by Taylor's decision. The judge ordered a cessation of wiretapping, although both sides in the ACLU's lawsuit agreed to wait until a hearing on Sept. 7. National security law experts have criticized the judge's ruling as poorly supported. "The opinion kind of reads like an outline of possible grounds to strike down the program, without analysis to fill it in," said Wake Forest University national security law specialist B. Chesney. Republican members of Congress also had harsh words to say about Taylor's decision, with Sen. M. DeWine (R-Ohio) claiming

that the deterrence of terrorist plots would be impeded if the surveillance program were halted. The Electronic Frontier Foundation hailed the ruling; EFF has filed a class-action lawsuit against AT&T, accusing it of working with the NSA and its surveillance program. EFF staff attorney K. Bankston says, "We now have a ruling on the books that upholds what we've been saying all along: that this wiretapping program violates the Constitution."

Sober Warnings About e-Voting Systems
CNet (08/17/06), E. Sinrod

In its analysis of three of the most widely used electronic voting systems, the Brennan Center for Justice at New York University found significant security and reliability flaws in each of them that could compromise the integrity of local, state, and national elections. With sufficient precautions at the state and local levels, the most serious vulnerabilities can be addressed, but few jurisdictions have implemented the necessary countermeasures to shore up their systems. The study analyzed the Direct Recording Electronic (DRE) system, which directly records a voter's choices with a ballot that appears on the screen; DRE with Voter Verified Paper Trail, which captures the vote both electronically and on paper; and Precinct Optical Scan, which enables the voter to mark a ballot with a pen and then carry it to a scanner. It would be fairly easy for someone to deploy software attack systems to alter vote counts or launch an attack on the system with a wireless device. New York and Minnesota are currently the only two states that prohibit wireless components on all voting machines. The Brennan Center report recommends automatic, routine audits that compare electronic tallies with voter-verified paper records after every election. The report also urges states to adopt wireless bans and randomly examine machines on Election Day for viruses and worms.

A Move to Secure Data by Scattering the Pieces
New York Times (08/21/06) P. C5; J. Markoff

When C. Gladwin, the software designer who sold his online music store Music Now in 2004, set about trying to digitize and secure the 27 GB of music, photos, and paper documents that he had been accumulating for years, he turned to an old technique employed by early cryptographers. The result was Cleversafe, an open-source project that secures data by breaking it down into pieces so that the files can only be reassembled by the computers that created them. The program could lower the cost of storing data on the Internet, Gladwin claims. "If we distributed data around the world this way, it would be a pretty resilient way to store data," said former ACM President D. Patterson, a computer scientist at the University of California, Berkeley. Gladwin is banking on the continued proliferation of digital data of all kinds, including new breeds of digital cameras that will drive demand for more secure and private backup applications. In developing Cleversafe, which will cut the amount of storage space required for secure backup by more than half, Gladwin drew heavily on the landmark paper "How to Share a Secret," written in 1979 by A. Shamir, a designer of the public-key cryptography algorithm. Gladwin designed a series of software routines to copy PC data into fragments of distributed file systems that could then be retrieved to reconstruct the original. Currently, Cleversafe runs on an experimental research grid located at 11 sites throughout the world, though Gladwin hopes that eventually a commercial network of tens of thousands or even hundreds of thousands of sites will emerge. Unlike existing storage projects, Cleversafe distributes data in encrypted chunks rather than making copies. The approach is similar to the SETI@Home project, which collects idle processing power from a network of computers to power a distributed supercomputer.

Paper Trail Flawed in Ohio Election, Study Finds
Computerworld (08/21/06), M. Songini

A new study funded by the Board of Commissioners of Cuyahoga County, Ohio, has once again called into question the reliability of electronic voting machines. The study claims that even the voter-verified paper trail produced by the Diebold machines was not reliable, noting that 10% of the paper votes were "either destroyed, blank, illegible, missing, taped together, or otherwise compromised." The study was conducted by the Election Science Institute (ESI), a San Francisco-based nonprofit dedicated to promoting the development of accurate, auditable election systems. "What we found is that when you take this [technology] out of the lab and put it in a real work environment with real voters, you're going to have some issues you need to resolve," said ESI's S. Hertzberg. In a letter to Cuyahoga County commissioners, Hertzberg wrote that the systems do provide some benefit for the voters, noting that they are easier to use than the old punch-ballot systems that they replaced. However, he also warned that the county should view the machines as a calculated risk, citing the 72% of polling places in which the study found a discrepancy between the paper ballots and the record on the machines' memory cards. Forty-two percent of those discrepancies entailed errors with 25 or more votes. The study also reported that 87 paper rolls and 28 voting machines were missing, and warned that printer malfunctions could cause serious election problems. A Diebold spokesman challenged the study's methods, claiming that the discrepancies resulted from matching paper records with the wrong memory cards. Diebold also expressed dismay that it was not allowed to participate in the analysis of the election. Ohio Secretary of State Kenneth Blackwell says the machines meet both state and federal requirements for certification, and that any problems are the result of flawed procedures or inadequately trained workers.

Tempting Data, Privacy Concerns
New York Times (08/23/06) P. C1; K. Hafner, T. Zeller

The three months' worth of search data inadvertently released to the public by AOL researchers poses a conundrum for researchers such as Cornell University computer science professor J. Kleinberg: They could sift through a dataset that could offer academic researchers an unprecedented glimpse into how people use the Web to retrieve information, or ignore the data out of respect for the users' individual privacy. Kleinberg, whose research focuses on algorithms for understanding and searching the Web, downloaded the data immediately, but decided against using it due to privacy concerns. The breach shines a spotlight on the long-running frustration of academic researchers that raw data about Internet usage is extremely difficult to come by, accessible only to a cadre of corporate researchers working at the large companies where the data is locked up. Many researchers claim that the data, which details the search queries of some 650,000 AOL users, is too valuable to ignore. The users are not personally identified in the data, but in some cases the search terms reveal enough information to infer an individual's identity. AOL moved quickly to take the data off of its research Web site, but numerous other sites had already downloaded the data, reposted it, and made it searchable. Academia, excluded from the fresh datasets routinely made available to researchers at companies such as Google, has in essence made do with the Alta Vista and Excite datasets for almost a decade, though they shed scant light on the habits of today's users. "The way people use search engines now is totally different," Kleinberg said. "Partly because what you expected to get out of a search engine back then was much less, so people didn't try anything too fancy." Everyone can agree that protecting privacy is important, said Jamie Callan, an associate computer science professor at Carnegie Mellon University and chairman of the ACM's special interest group on information retrieval. But, Callan claims, "there's also

a strong belief that it is very important for the scientific community to have access to data of this kind in some anonymized form."

The "Data Valdez" Versus the Privacy Ceiling
The Flowing Candy Bees (08/12/06)

With a group of researchers preparing to present a paper on the economic limitations of privacy violation at the ACM 2006 DRM workshop, which takes place October 30, 2006, in Alexandria, Va., the exposure of the search queries of some 658,000 AOL users seems almost prescient. The concept, known as the privacy ceiling, argues that forward-looking companies would scrupulously guard against privacy violations due to the liability of amassing large repositories of sensitive information. Liability can come from many sources, such as vicarious infringement, which companies can be liable for if it can be proven that infringement in fact occurred, that the company benefited from it, and that the company could have stopped it. Librarians reacting to the Patriot Act purged the records of their patrons' reading habits, creating their own privacy ceiling. Similarly, companies can be liable from their customers for privacy violations. AOL's case, which appears to have involved a simple miscalculation by a few employees, illustrates the principal that companies can limit their liability by reining in their data-collection practices. To curb the potential liability from disclosing customers' data, the authors of the report recommend that companies implement architectures with built-in monitoring capabilities to safeguard sensitive data. They go a step farther and advise companies to actually control their users' activities to the fullest extent that their architectures will allow. Finally, the authors recommend that companies build their systems around privacy alone, rather than trying to balance the demands of copyright holders.

Capturing Online Video Pirates
Technology Review (08/22/06), R. Roush

Popular online video-sharing sites have been fighting a losing battle as they try to curb the posting of material copied from movies and commercial TV broadcasts without the permission of copyright holders. For the most part, these services have been removing unauthorized content when they receive a complaint from the copyright holder, after it has already been posted. However, new technologies are emerging that can preemptively ferret out copyrighted material, such as a system in use on the video-sharing site Guba that compresses a video file to a mathematical expression and compares its "fingerprint" with a database of commercial videos, excluding any matches from the site. Another technology embeds a watermark in movies, enabling studios to trace bootlegged copies of a movie taken with a camcorder back to the original theater and movie showing. While fingerprinting may not be able to keep pace with the volume of TV programming broadcast every day, and watermarking does not actually catch pirates, the techniques could be a valuable defense for video-sharing sites against the same type of legal challenges that brought down Napster and MP3.com. Roughly one-fifth of movie content on video-sharing sites is pirated, according to Guba founder Tom McInerney. While pirated content can drive Web traffic and create advertising views, it can also attract unwelcome legal attention. The nuisance of dealing with a steady stream of takedown requests compelled Guba to develop its fingerprinting system, which uses wavelet technology to condense the video into compact mathematical representations. Computer vision technology measures the frequency of scene changes to generate a form of time stamp. The system screens every video uploaded to Guba, singling out those that match a fingerprint in the database for human review. The system identifies pirated content with a 99% accuracy rate, McInerney says.