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

Δελτίο 27
1 Ιουνίου 2006

Privacy Worries Over Web's Future
BBC News (05/24/06), J. Fildes

As researchers continue to develop the Semantic Web, major privacy issues could arise because of the confluence of multiple sources of data about people and places, according to Hugh Glaser of the University of Southampton, though he admits that it will be several years before even the Semantic Web programs that have already been developed become available to the public. When Tim Berners-Lee invented the Web in 1989, it was impossible to predict how integral it would become to everyday life. The current Web has major limitations, however, including the fact that the majority of its information cannot be read by a computer. Developers of the Semantic Web are trying to bring order to the jumble of photographs, calendars, public records, and other items so that computers can create a coherent and composite statement of a person, place, or thing. "Imagine if you can link real-time prescription data for flu remedies with geographical data," said Nigel Shadbolt of the University of Southampton. "You can do real-time epidemiology and see flu outbreaks as they happen." The Semantic Web could also create personalized weather forecasts with information provided by global positioning systems. While the extended reach of the Semantic Web would make for a much smarter platform, it could also tap into confidential information as it searches for multiple sources, such as health records, purchasing histories, or contact information. "All of this data is public data already," said Glaser. "The problem comes when it is processed." That said, researchers will have many years to address the security concerns, and some argue that rather than presenting an entirely new problem, the Semantic Web merely complicates the security concerns that already plague the existing Web.

Too Much for NSA to Mine?
Government Computer News (05/22/06) Vol. 25, No. 13, P. Wait

The controversy over the NSA's covert program of collecting data on millions of phones calls placed by normal citizens begs the question of how well the agency will actually be able to mine the vast quantities of information it is amassing. Although the NSA is not revealing any details about its databases or the technologies that it is using to maintain and search them, the Electronic Frontier Foundation (EFF) reports that AT&T's Daytona call detail record (CDR) database, which was reportedly made accessible to the NSA, exceeds 312 TB. Assuming that figure is accurate and that Verizon and BellSouth provided access to databases of similar sizes, the NSA could have more than 900 TB of data on its hands, requiring massive storage capacity, intense computing power, and sophisticated analytical software. Access to the bulk of the database in real time is critical for effective data mining, though some believe the NSA is frozen out of much of its own information by virtue of its sheer size. "My impression--strictly a professional guess--is that at least 75% of what NSA 'knows' is...offline and not accessible," said Robert Steele, CEO of OSS.net. "You cannot do good pattern analysis, including historical comparisons, without massive online storage." SGI has begun developing computers with terabyte-scale active memories, the largest containing 13 TB, which is not enough memory to handle even 1.5% of the three CDR databases put together. Moreover, a computer's capacity for memory space is limited by its amount of address bits on chips, ac-

cording to SGI's B. Mannel. "Some of our customers who already have big-memory databases are looking for something beyond [what they have], but they have power and footprint problems," Mannel said, adding that the storage architecture must be overhauled to incorporate enough RAM to access the entire database.

When It Comes to Privacy, Gender Matters
UW News (05/23/06)

Researchers at the University of Washington have found that women are more concerned about security in public places than men are, challenging the notion that people no longer expect their privacy to be respected once they leave their homes. Indeed, almost a quarter of the men and women involved in the study said that any amount of video capture is an invasion of their privacy. Most people in either gender did not object to on-campus video capture, though a majority of women found off-campus surveillance unsettling. Of the nearly 900 people included in the survey, 780 were told beforehand that a camera mounted at the top of a tall campus building was monitoring their movements and relaying the image to a plasma screen set up inside the building. Most men and women did not object to the display within the office, but a majority of women expressed discomfort at the idea of sending their images to an off-campus apartment or some other remote location, suggesting that the university community is perceived as more trustworthy than the outside world. Most men and women agreed that they would not be comfortable with being recorded, as opposed to having their images displayed in real time, though nearly twice as many women as men did have reservations about real-time display. "Over half (55%) of the participants we surveyed expressed some concern for having their image in a public place collected and displayed elsewhere," said P. Kahn, associate professor of psychology and one of the lead authors along with UW Information School professor B. Friedman, both of which are co-directors of the UW's Value Sensitive Design Research Lab. The study will be published in next month's Journal of Human Computer Interaction.

'Google Hacking' Attacks Rising
Massey News (05/19/06)

Researchers at Massey University report that Google hacking attacks are on the rise and that many Web sites in New Zealand are more vulnerable than people suspect. Hackers who use Google's search engine to uncover sensitive personal information pose a threat to businesses, governments, and other organizations that store individuals' data. The study conducted a vulnerability comparison of Web sites in New Zealand with those in Australia, the United States, and the Czech Republic, and found New Zealand's to be the least secure. Using carefully chosen keywords, the researchers ran 170 queries each day for three months, and found that sites with the organizational domain names .co and .org were the most vulnerable. The vulnerabilities remained open for an average of 60.96 days, or 57% of the testing period, and the problem is not likely to solve itself. "Security on the Web is likely to remain an ongoing battle," said Ellen Rose, a senior lecturer at the Institute of Information and Mathematical Sciences. "On the one side, hackers will continue to employ new tactics, using tools like Google in unforeseen ways. Security experts must try to minimize exposure by detecting problems and putting countermeasures, such as security audits, in place. Google hacking vulnerability should be included in these security audits."

Hacking Your Prius
CNet (05/22/06), D. Terdiman

Toyota Prius owners are increasingly finding ways to hack into their vehicles' systems to alter factory specifications in an attempt to get more miles per gallon. "In the 1950s, it was all about getting more speed. Now, instead of getting more horsepower, it's about getting more miles per gallon," said P. Torrone of Make Magazine. Rising gas prices and concerns over an emerging energy crisis have exacerbated the tendency of hybrid-car owners to override factory-set features. Hackers have been able to modify the car so that it runs mostly on battery power, raising the car's fuel efficiency to nearly 100 miles per gallon. Prius owners have also executed hacks to alter other features, such as the beeping noise that some late model cars make when put into reverse. Early Prius adopters have formed a closely knit community to share information about methods for hacking the car's systems, and as a class are likely to have the expertise to execute such hacks, according to D. Watson, president of Coastal Electronics, a company that promotes Prius modification kits. Toyota acknowledges that some owners will take steps to modify their cars, though it does not condone the behavior, particularly the hack that enables users to operate the GPS navigation system while the car is in motion. Watson counters that Toyota made an arbitrary distinction when it decided which features users could and could not operate while driving the car due to safety concerns. The feature that enables the Prius to run almost entirely on battery power at low speeds is available on models sold in Europe and Asia, but Toyota claims that the US regulation requiring it to offer an eight-year warranty for its power system prevents it from including the option in models sold in the United States.

Champion of Cyberspace Faces Its Biggest Case Yet
San Francisco Chronicle (05/23/06) P. A1; B. Egelko

The Electronic Frontier Foundation (EFF) will face what could be the most significant case of its 16-year history when a federal judge hears dismissal motions from both AT&T and the Bush administration in a suit alleging that AT&T broke the law by handing over tens of millions of communications records to the NSA. The EFF has been alternatively praised as a champion of the common man and condemned as the enemy of the free market. "Their first instinct is to mistrust corporations, organizations competing in the market, to not have faith that competition will solve problems," said P. Ross of the Progress and Freedom Foundation. The EFF counters that it is in favor of the free market, but it warns against the alignment of government, private industry, and technology. "In different moments, each of these are friends of civil liberties," said Jennifer Granick, executive director of the Center for Internet and Society and an EFF supporter. "Sometimes they conspire in some combination of the three to be a challenge to civil liberties." The EFF has struggled to convince the courts that it is attempting to safeguard essential freedoms, such as the right to have a private conversation. The group was outmaneuvered by the entertainment industry last June when it failed to frame the argument over downloading music around stifling innovation, as opposed to stealing intellectual property. The foundation has vigorously campaigned against the stipulations of the 1998 Digital Millennium Copyright Act, including the rule barring users from bypassing piracy protections, though the law has generally help up in the courts.

The Fight Against V1@gra (and Other Spam)
New York Times (05/21/06) P. 3-1; T. Zeller

As email filtering technologies have become more sophisticated, bulk emailers have begun sending larger, image-based messages in an attempt to slip past antispam filters. While end users are no longer inundated with the same volume of unwanted email that they faced just a few years ago, spam is still a major problem for network operators. Inbox filters nearly elimi-

nate the amount of bulk messages that users receive, though spam still accounts for around 70% of all Internet traffic, in spite of the numerous regulatory initiatives enacted throughout the world designed to combat the problem. Between one-half and three-quarters of all spam is produced by zombie computers. Spammers who work out of countries with lax law enforcement such as Nigeria or Russia have little incentive to cease their operations, particularly when they can turn handsome profits by eliciting responses from less than 1% of the up to 200 million messages that they send out daily. Antispam groups have developed technologies to determine whether the borders of images in spam email have been generated randomly, a tactic that bulk emailers have recently adopted to evade filtering tools. "There are loads of different kinds of obfuscation," said MessageLabs senior antispam technologist N. Johnson. "They've realized that people are looking for V1agra spelled with a '1' and st0ck with a 'zero' and that sort of thing, so they might try some sort of meaning obfuscation," he added, such as "referring to a watch as a 'wrist accessory'" rather than a 'Rolex.' Johnson also described a particularly impressive spam trick in which spammers used incorrect spelling and HTML code in such a way as to evade detection by software programs but appearing correctly to viewers. MessageLabs' M. Sergeant says the company has also developed a database of "scam DNA" which uses pattern analysis to find spam that uses language common enough to avoid detection otherwise.

Perils of Transitive Trust in the Domain Name System
Cornell University (05/06), V. Ramasubramanian; E. G. Sirer

The complexity of the domain name system (DNS) is such that a vulnerability in a little-known nameserver can have serious ramifications while trust relationships are hard to particularize and weave together, write R. Venugopalan and E.G. Sirer with Cornell University's Department of Computer Science. A reliance on transitive trust engenders a situation where trust relationships can change without even the most assiduous name owners realizing it. The authors' survey of the trusted computing base in DNS reveals its great extent and potential inclusion of over 400 nodes; an average name relies on 46 nameservers, while the average in certain top-level domains tops 200. One third of domain names can be hijacked with publicly-known exploits through DNS, enabling hackers to wreak mischief. The survey also finds that 10% of the namespace is controlled by some 125 servers, one-fifth of which are run by educational institutions that may lack sufficient inducements and resources to practice integrity enforcement. Name security on the Internet can be fortified by the implementation of DNSSEC, although the authors caution that this solution still depends on the same physical delegations as DNS during lookups. DNSSEC must be more widely adopted in order to be truly effective, and even the support of DNSSEC by all nameservers cannot eliminate the disruption of name resolution by denial of service attacks on Web services. Ramasubramanian and Sirer reason that network administrators must have more familiarity with DNS vulnerabilities and exercise greater diligence over their trust relationships.

Will Your Vote Count in 2006?
Newsweek (05/29/06) Vol. 147, No. 22, P. 14; S. Levy

With experts calling the recently reported vulnerabilities in e-voting machines the most serious ever discovered, Americans' confidence in the integrity of the election process is in jeopardy, writes S. Levy. Diebold claims that the flaw uncovered last month by Finnish security expert Harri Hursti was designed to enable the machines to easily receive software upgrades, though that feature also invites the possibility that anyone with an elementary familiarity with the machines could install malicious code in a matter of minutes. Hackers could prog-

ram the machines to fail on Election Day or, worse still, manipulate the ballot-counting functions to switch votes from one candidate to another. That type of software is capable of disguising itself so that even authorized technicians would be unable to detect its presence. "If Diebold had set out to build a system as insecure as they possibly could, this would be it," said Avi Rubin, a professor of computer science at Johns Hopkins University. Concerns over the security of e-voting machines have sparked calls for including a mechanism to produce paper receipts in the event that a manual recount is necessary. "When you're using a paperless voting system, there is no security," said D. Dill, a professor at Stanford University. Twenty-six states have already moved to implement a paper-recording mechanism, though a legislative initiative that would bar paperless voting throughout the country is stalled on the House floor. Six years after the disastrous election of 2000, US voters will head to the polls this year still uncertain if their votes will be accurately recorded, Levy gloomily concludes.

Certified Reputation--How an Agent Can Trust a Stranger
University of Southampton (ECS) (05/16/06), T. D. Huynh; N. Jennings; N. Shadbolt

Current approaches to building computational trust models, interaction trust and witness reputation, are limited, and the authors propose Certified Reputation (CR) as a trust model that circumvents these shortcomings by addressing agents' lack of direct experience and the difficulty in finding witness reports. Through CR, agents can dynamically supply third-party references about their earlier performance in order to build up trust among prospective interaction partners. This allows the rapid establishment of trust relationships while keeping costs to the involved participants low. Certified reputation of a target agent involves a number of certified references on how that agent behaves on specific tasks supplied by third-party agents (ratings), which are collected and retained by the target agent itself and made available to any other agent desiring to assess its level of trust for future interactions; through these ratings, the targeted agent can demonstrate its performance as judged by previous interaction partners in order to earn potential partners' trust. The authors acknowledge that the CR data will likely exaggerate an agent's projected behavior because a rational agent, being able to select which ratings to present, will only advertise its best ratings. Still, CR spares agents various expenditures associated with tracking down witness reports in terms of resources, time, and communication, and enables agents to assess trust for themselves, removing the need for a centralized service; this establishes compatibility between CR and open multi-agent environments. The authors' evaluation of CR shows that the model can help agents choose better interaction partners faster than with other computational trust models. Their future plans include developing a technique to automatically adapt the accuracy tolerance threshold while the system is running via the analysis of recorded performance levels of service providers with whom an agent has interacted to ascertain the probable inconstancy of honest ratings.

Creating and Operating National-Scale Cyberinfrastructure Services
CTWatch Quarterly (05/06) Vol. 2, No. 2, C. Catlett; P. Beckman; D. Skow

The authors use the TeraGrid project as an example of the costs and functions associated with the provision of a national cyberinfrastructure, with a focus on the software infrastructure and policies that are necessary to combine a variety of elements into a reliable and persistent national-scale facility. A grid facility's software components include science applications, middleware, infrastructure support services, and the tools for configuring community-developed systems or "Science Gateways," which most often take the form of Web portals. "We have partnered in the TeraGrid project not only with gateway providers but also with other grid facilities to identify and standardize a set of services and interaction methods that

will enable Web portals and applications to invoke computation, information management, visualization, and other services," state the authors. A national-scale grid facility taps software infrastructure that supplies a set of common services, an architecture that enables unique facility exploitation, and the infrastructure required to coordinate the user-supportive efforts of resource providers. A successful grid facility involves close collaboration and cooperation between all participating organizations, and the identification of specific common service coordination and provision responsibilities, which in most grid projects is a function executed by a system integration team. A general-purpose grid facility must adjust to its user community's changing ideas and requirements, and the optimal model for user support is one that fully harnesses all available human links to users and their problem domains, most frequently by having the user support personnel local to the resource providers. Each of the facility's resource providers will supply documentation and training for locally provided resources and services, and proactively integrating these materials requires a communication framework that offers structure and common interfaces and formats for the materials, as well as the curation of the general systems. A national grid facility must use an operational infrastructure as its platform, while collaboration systems and processes that support virtual and distributed teams must be carefully attended to.

While You Were Reading This, Someone Ripped You Off
Wired (05/06) Vol. 14, No. 5, P. 166; A. Newitz

Hackers are exploiting increasingly pervasive radio frequency identification (RFID) technology to beat security measures and steal or vandalize valuable information as well as physical items. The information carried on most commercial, passive-emitting RFID chips is rarely encrypted because it is so expensive, and this increases the danger that these chips can be cloned or that the data they hold can be corrupted. Although writable areas of RFID chips can be locked, many organizations fail to do so because they are unfamiliar with the equipment's operation or because the data fields must be regularly updated; using unlocked tags is often a more convenient option. Examples of RFID hacking include the recording of data on RFID-based price tags, which hackers can then upload to tags of other items, and the disabling of car antitheft devices through the use of a cloner to capture an encrypted RFID signal and a computer to crack it. "The world of RFID is like the Internet in its early stages," explains RSA Labs research manager A. Juels. "Nobody thought about building security features into the Internet in advance, and now we're paying for it in viruses and other attacks. We 're likely to see the same thing with RFIDs." Next-generation, RFID-equipped digital passports will reportedly have unbreakable encryption, but Juels thinks a brute-force attack could compromise the data since the encryption keys rely on passport numbers and birthdates that are structured and guessable.

Europe: No Patents for Software
ZDNet UK (05/25/06), I. Marson

The European Commission (EC) appears to have reversed its stance on software patents, according to a statement the EC made last week regarding the Community Patent legislation. A year ago, the EC said the European Patent Office (EPO) would continue to make patents available for computer programs that provide some technical contribution, but a week ago the EC said there would be no software patents under the new Community Patent legislation. "The draft Community Patent regulation confirms in its Article 28.1(a) that patents granted for a subject matter (such as computer programs), which is excluded from patentability pursuant to Article 52 EPC, may be invalidated in a relevant court proceeding," the EC said. The

statement came in response to a question Polish European Parliament member Adam Gierek posed in April regarding the impact of the Community Patent legislation on EPO's practice of granting software patents. The new position was a surprising and confusing one for groups that oppose patents on computer programs in Europe. P. Hintjens, president of the Foundation for a Free Information Infrastructure, is just as concerned about having an independent appeal process as he is about the invalidation of software patents in court because of the potential cost of civil litigation for small companies. "Therefore, software patents not yet taken to court will impose an enormous burden on the industry," Hintjens says.

Finding Computer Files Hidden in Plain Sight
Ames Laboratory (05/24/06)

While criminals or terrorists are likely to arouse the suspicion of government agents by sending encrypted files over email, software programs now enable a practice known as steganography, where files are hidden within other files, such as photographic images. Researchers at Iowa State University and Ames Laboratory have been exploring the emerging discipline of detecting those hidden files, or staganalysis. JPEG files and other electronic images are perfect for concealing such files because they can be found by the thousands in any given computer and can be emailed by anyone or found all across Web. With the aid of steganographic, or stego, techniques, users can make slight alterations to the color values of an image to conceal the bits of data that comprise a secret file, or payload, that can represent anything from unlawful financial transactions to child pornography. "We're taking very simple stego techniques and trying to find statistical measures that we can use to distinguish an innocent image from one that has hidden data," said Clifford Bergman, professor of mathematics at ISU. "One of the reasons we're focusing on images is there's lots of 'room' within a digital image to hide data. You can fiddle with them quite a bit and visually a person can't see the difference." Ones and zeros can represent the payload file, which the stego program compares to the ones and zeros of the image file's pixel values. The recipient can then retrieve the secret file by decrypting and reconstructing the payload's data string. The researchers are developing a system known as an artificial neural net (ANN) to help review and detect hidden files within images. They trained the ANN with a database of "clean" images and then altered them using stego techniques to greatly expand the database and provide a basis for comparison. The ANN identified 92% of the stego images in preliminary tests, while only flagging 10% of clean images, and the researchers hope to refine it further.

Invention IDs Computer Users by Typing Patterns
University of Alabama (05/24/06)

M. Brown, associate professor of computer science at the University of Alabama, and his former graduate student J. Rogers were awarded a patent for a technique to identify a person based on the way they type their name 13 years ago. Rogers based his thesis on the technology, but until recently, when they sold the patent for around $15,700 each, the pair had received little recognition from the discovery. Brown drew part of his inspiration for the invention from Thomas Edison, who as a telegraph operator learned to identify who was on the other end of the wire by the patterns of dots and dashes. Any computer with a standard keyboard can identify who is using it with Brown's invention, which has obvious applications to improving security. "Rather than replace passwords, this technology would probably best be used to add another layer of authentication," Brown said. "It could reduce the need for measures such as changing your password every six weeks." To develop their program, which creates an individual "fingerprint" based on the exact time a user presses a key, Brown and Rogers

trained a neural network, though Brown is still unsure if the technology distinguishes between the physical structure of the user's hand or the manner by which humans mentally break up words as they type, or a combination of the two, perhaps combined with other unknown factors.

Security Expert Recommends Net Diversity
Network World (05/22/06) Vol. 23, No. 20, P. 19; C. Marsan

E. Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security, says the three biggest threats to information security that multinationals are likely to face are the deployment of cost-saving or feature-enhancing resources (such as VoIP and wireless) without careful consideration of the consequences; the erosion of the network perimeter through the advent of advanced communications technologies; and excessive dependency on a small set of suppliers, leading to a situation in which a weak or failing platform type can cripple an organization. Embedding diversity within every critical infrastructure can address the threat of network homogeneity, says Spafford. "This helps ensure that some of your infrastructure will be maintained so that you can send and receive email and surf the Web even if one of your common configurations is completely blown away by some kind of attack or some kind of bug," he explains. To minimize the other two threats, Spafford recommends instilling a thorough understanding of any new technology's risks and trade-offs, and a new emphasis among IT executives on shielding individual hosts or constructing well-defined sectors. Network diversity will obviate the need for an enterprise to shut everything down and restart in the event of an automated, unobserved attack. Spafford rates network attacks by insiders such as disgruntled employees as the most potentially damaging, although he says outsider threats are growing as law enforcement fails to keep pace with the increase in online criminal activity. He gives most big multinationals a B in terms of information security, and remarks that government agencies' security is "not particularly good," while that of charities, state governments, and universities is downright shoddy.

Meet the Hackers
BusinessWeek (05/29/06)No. 3986, P. 58; S. Ante; B. Grow; R. Olearchyk

Russian computer hackers distinct from their predecessors for their youth, organization, and brazenness are among law enforcement's most wanted cybercrooks. Factors contributing to their notoriety and success include their country's strong technical universities, low salaries, and beleaguered court system. D. Golubov, a 22-year-old Ukrainian, was arrested last year for a series of cybercrimes, including credit-card fraud, allegedly perpetrated by an international gang of hackers he masterminded; yet he was released on a personal recognizance bond from two Ukrainian politicians who defended his character. Russian-born L. Kuvayev, 34, was named in a lawsuit filed by the state of Massachusetts last May accusing him and six accomplices of sending millions of spam emails to peddle illicit products through American and international Web-hosting servers, in violation of the 2003 CAN-SPAM Act. State officials think Kuvayev, who Spamhaus ranks as one of the world's three leading spammers, may have taken refuge in Russia, where antispamming laws are nonexistent, before he was sued. Federal law enforcement officials believe Kuvayev was making over $30 million annually through his spamming business, and he and his co-defendants were ordered by the court to pay $37 million in civil restitution for sending approximately 150,000 illegal emails. The 2005 FBI Computer Crime Survey estimated that $67 billion is lost every year to computer crime, while 87% of the 2,066 surveyed companies admitted to a security incident.