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

Δελτίο 144
30 Μάρτη 2009

Noise Could Mask Web Searchers' IDs
New Scientist (03/07/09), P. Marks

Microsoft researchers say that adding noise to search engine records could protect Web users' identities, and that implementing such a technique would be a major step toward provable privacy. Records of Web searches are extremely useful to software engineers looking to improve search technology, and can provide valuable insight for scientists exploring digital search behaviors. However, attempts to make search data anonymous have been mostly unsuccessful. Microsoft researchers K. Kenthapadi, N. Mishra, A. Ntoulas and A. Korolova say they have developed a safe way to release search data. The researchers propose publishing data associated only with the most popular queries, so that specific, rarely performed searches, such as for individual names or unique interests, cannot be used to identify people. The researchers also inserted noise into the data by adding digits to the data's figures. Korolova says that adding the noise gives the data provable privacy, and the amount of noise added defines the level of privacy that can be guaranteed. She says the added noise strikes a balance between guaranteeing privacy and providing useful data sets.

NIST Suggests Areas for Further Security Metrics Research
Government Computer News (03/09/09), W. Jackson

Scientists at the National Institute of Standards and Technology's (NIST) Computer Security Division have identified several areas that need to be researched to spur the creation of useful security metrics. One key area is the creation of formal models of security measurement and metrics. NIST scientists say the absence of these models and other formalisms has made it difficult to create security metrics that are useful in practice. Another area that needs to be researched is historical data collection and analysis. The scientists say that predictive estimates of the security of software components and applications that are being examined should be able to be derived from historical data collected about the characteristics of similar types of software and the vulnerabilities those applications experienced. The scientists observe that insights into security metrics could be gained by using analytical techniques on historical data in order to identify trends and correlations, discover unexpected relationships, and uncover other predictive interactions. Finally, the scientists say the development of computing components that are designed for measurement would be a significant step toward developing effective security metrics.

Berners-Lee: Semantic Web Will Have Privacy Built-In
ZDNet UK (03/12/09), T. Espiner

World Wide Web Consortium director Sir Tim Berners-Lee says the Semantic Web will improve online privacy protection by allowing Internet users to control who can access their data. Researchers have warned that the combination of personal information and a semantic Web could lead to privacy problems, including increased data mining. However, Berners-Lee says that teams working on the Semantic Web project are working to ensure that privacy principles are built into the Semantic Web's architecture. "The Semantic Web project is developing systems which will answer where data came from and where it's going to--the system will be architectured for a set of appropriate uses," he says. Berners-Lee also says the Semantic Web will be based on the principle that people who make a Web request for information held by third parties, such as a company or a government agency, will be able to see all the data those organizations will keep on them. The Semantic Web project will include accountable data-mining components, which enable people to know who is mining data on them, and it is exploring making the Web adhere to privacy preferences set by the users.

Many See Privacy on Web as Big Issue, Survey Says
New York Times (03/16/09) P. B5; S. Clifford

More than 90% of US citizens polled in a recent TRUSTe survey said that online privacy is a "really" or "somewhat" important issue, and just 28% said they were comfortable with advertisers using behavioral targeting; more than half of respondents said they were not. More than 75% of respondents agreed that the Internet is not well regulated, and said that naive users are at risk. In February, the US Federal Trade Commission (FTC) revised its suggestions for behavioral targeting rules for the advertising industry, including that Web sites should disclose when they are participating in behavioral advertising and ask users for permission to use their browsing history. FTC commissioner J. Leibowitz warns that intervention will be needed if the industry does not respond to the new suggested regulations. "Put simply, this could be the last clear chance to show that self-regulation can--and will--effectively protect consumers' privacy," Leibowitz says. More than half of the respondents in the survey said the government should be "wholly" or "very" responsible for protecting individuals' online privacy, although 75% of respondents also said that people should be wholly or very responsible for protecting their own privacy.

Researchers: Cheap Scanners Can 'Fingerprint' Paper
IDG News Service (03/09/09), R. McMillan

Researchers at University College London and Princeton University have developed a technique they say can identify unique information from any sheet of paper using a scanner. "We 've found a way to identify documents even when there was nothing additional printed on them," says University of Michigan professor A. Halderman, a former member of the Princeton team. "This is like an invisible serial number printed on every piece of paper ever made." The technique identifies the unique patterns in a piece of paper's fibers. The researchers say they can identify the patterns using a standard scanner and custom software. By rotating a page 90 degrees and scanning it multiple times, the researchers can isolate subtle differences in the paper's texture and create a unique digital map of its surface. This map can act as a fingerprint for the document. The researchers say that a well-preserved sheet of paper can be identified with near 100% accuracy, and error-correction software can be used to make a definitive identification of damaged paper. The researchers say the technique could be used to identify counterfeit money, tickets, or packaging containers. Companies could take a fingerprint of their labels when products are shipped, which would be verified later by the government or a company representative to spot fake products.

Sending Out Internet Warnings for Outages, Viruses
Science Daily (03/16/09)

An early warning system on the Internet could help Europe avoid deliberate or accidental outages, restrict the spread of new viruses, and ensure reliable services, say M. Hesse and N.

Pohlmann from the Institute for Internet Security at the University of Applied Sciences in Gelsenkirchen, Germany. The researchers say there is a growing need to improve the reliability and trustworthiness of the Internet, and that raising awareness of critical processes and components on the Internet is essential, particularly among those responsible for the Internet's continued operation. The Internet's greatest asset is its decentralized structure, but that asset also creates a problem in that it consists of almost 30,000 autonomous systems, each managed by individual organizations primarily within the private sector, and there is no governing body for the network. Unfortunately, the private organizations are exposed to a high level of competition, which eliminates the possibility of sharing important management information. If an early warning system is to be built and implemented, a change in attitude is needed. "The cooperation of companies, organizations, and governments is important to create a global view of the Internet," the researchers say.

Cyberattack Mapping Could Alter Security Defense Strategy
SearchSecurity.com (03/10/09), A. Howard

During a recent seminar at Harvard University, researchers from Sandia National Laboratories presented maps they developed of massive cyberattacks against large computer networks. The maps - which are made up of a series of colored dots, lines, and graphs -simulate a type of cyberattack known as a root attack, in which hackers try to gain control of a computer at its most basic level. Sandia's S. Goldsmith says the maps could help IT security professionals protect their networks from attacks. Goldsmith also has created intelligent white hat software agents that look for suspicious requests from internal or external sources. When the agents detect an attack, they cut off malicious agents from the group, which only authorizes authenticated data. He says the technology will enable networks to defend themselves. Goldsmith says that both aspects of Sandia's research could someday be used together to improve the effectiveness of enterprise intrusion-detection software.

White House Cyber Adviser--More Questions Than Answers
CNet (03/26/09), S. Condon

Comprehensive cybersecurity legislation being drafted in the US Senate would bring high-level government attention to serious cybersecurity problems. The legislation also would give a new White House official oversight over the US's critical network infrastructure, along with the ability to disconnect federal and critical networks should they be threatened by a cyberattack. However, cybersecurity experts are concerned that the proposed bill would create more uncertainties than it would solve. The bill acknowledges the large number of critical infrastructure networks in the private sector. Each has its own risk tolerances and ways of mitigating risk, and giving a single person the authority to disconnect any of those networks from the Internet means that person must have a thorough understanding of all of those systems. Instead of having one person decide to shut down a network, TechAmerica's L. Franz suggests establishing a series of steps that the public and private sectors could take together when faced with a threat. Another key issue is determining which threats pose the most risk. "Everybody is under attack, at some level, all the time," says Georgetown University's M. Blumenthal, the founding executive director of the Computer Science and Telecommunications Board. Blumenthal says that previous government experiences dealing with jurisdictional issues related to computer security should guide any new legislation.

Survey Suggests Economy Could Lead to Cybercrime Increase
Purdue University News (03/18/09), J. Bush

Researchers at Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) say the results of a new study show that companies worldwide are facing a growing number of cybersecurity threats, highlighting the need for businesses to be extra vigilant in protecting intellectual property. The study, "Unsecured Economics: Protecting Vital Information," found that companies lost an estimated $4.6 billion in intellectual property last year through cybercrime, and that the global recession may cause those losses to rise. The study found that cyberthieves have evolved beyond basic hacking and stealing credit card numbers and personal data to targeting intellectual property. In addition, the study found that an increasing amount of vital data, including intellectual property and sensitive customer data, is being lost in the transfer between companies and continents, and that the average company has $12 million worth of sensitive information stored abroad. The researchers also found that the global economy crisis is creating a "perfect storm" in information security risks as companies face increased pressures to reduce spending and cut staff, which could potentially result in weaker defenses and increased opportunities for cybercriminals. "We are connected around the world in this global economy, but we don't have the rules, the same laws, or the same attitudes about protecting information," says CERIAS executive director E. Spafford. "It's going to take cooperation among governments, private industry, and the people who work in the areas of information security to bring cybercriminals to justice and lessen the problem."

Scholarship Program Targets Need for Cybersecurity Skills
Government Computer News (03/23/09), R. Walker

The Scholarship for Service (SFS) program, jointly run by the National Science Foundation and the US Dept. of Homeland Security (DHS), is becoming a widely recognized, indispensable program, particularly at a time when government demand for highly skilled information technology security professionals is rapidly climbing. The SANS Institute's A. Paller says the US government is desperate for cybersecurity professionals. "We probably have only 1,000 of those people in the whole country, and we need between 10,000 and 30,000 in the next couple of years," Paller says. The SFS program was designed to increase and strengthen the federal government's core of cybersecurity professionals by underwriting two-year stipends for full-time students who specialize in information assurance at approved four-year colleges and universities in exchange for agreeing to serve at a federal agency in a cybersecurity position for at least two years. The program provides scholarships for tuition, room and board, and books. Since its creation in 2001, SFS has sent almost 900 students into federal cybersecurity positions. "We're looking for technologists who can build better mousetraps," says M. Kwon, director of DHS's US Computer Emergency Readiness Team. "We're looking for analysts who can get to the real crux of the threat, and we're looking for writers who can articulate our geeking and beeping so that management, Congress, and the public can understand what we're talking about."

Improving the Security of Internet Exchanges
National Center for Scientific Research (France) (03/13/09), C. Le Poulennec

M. Badra, a researcher at France's National Center for Scientific Research, has developed two new extensions to the TLS protocol, the main protocol used to secure exchanges over the Internet. The first extension involves the key exchange method. Keys are either symmetric or asymmetric. With a symmetric key, the same key is used for both encryption and decryption, and the key must be kept secret and sent over a secure channel before the data exchange. With asymmetric keys, a public key is used to encrypt the data, and the recipient uses a private key to decrypt the data. Badra has developed an extension that uses a new method for exchanging keys based on the association between an asymmetric algorithm and a symmetric key. A new key is generated at the start of each session and authenticated by the symmetric key, which is more reliable and more secure than current methods and simplifies the deployment of TLS in network equipment. The second extension involves the data-hashing function, which transforms the message into a message digest. Changing the message requires a change in the digest, and it is difficult to reconstruct the original message based on the digest. Badra's extension uses new hash functions to provide better protection against collision attacks, which occur when two different messages could have identical message digests. Both standards were recently published by the Internet Engineering Task Force.

Experts See Shortfall in Cybersecurity Research
InternetNews.com (03/19/09), K. Corbin

The US is not prepared to deal with the emerging threats against the country's digital infrastructure, warned cybersecurity experts at a recent US Senate Commerce Committee meeting. The experts also said that Congress needs to make information security and security education a bigger priority. "The simplest way to state this is the nation is under attack," said Purdue University professor E. Spafford, executive director of the Center for Education and Research in Information Assurance and Security. "It is a hostile attack, it is a continuing attack, and it has been going on for years, and we have been ignoring it." James Lewis, director of the Center for Strategic and International Studies, said cyberattacks threaten the long-term economic competitiveness and technological leadership of the United States. Senate Commerce Committee chairman J. Rockefeller (D-W.Va.) said he is encouraged by President Obama's focus on cybersecurity, but cautioned that time is critical as computers are increasingly being used to manage the country's infrastructure. Rockefeller said he plans to introduce legislation that would boost cybersecurity education at the university level. Spafford said the US needs more cybersecurity experts and noted that universities graduate just 50-60 Ph.D. in fields related to cybersecurity. "Of those perhaps 10-15 are going to return to their home countries to start businesses to compete against the US because our visa policies won't let them stay," he said.

Diebold Admits Systemic Audit Log Failure; State Vows Inquiry
Wired News (03/17/09), Z. Zetter

Premier Election Solutions admitted at a recent California state hearing that significant events, such as someone erasing votes on election day, are missed by the audit logs generated by its tabulation software, and this problem is endemic to all versions of the software. "The audit logs have been the top selling point for vendors hawking paperless voting systems," said California Voter Foundation president K. Alexander. "They and the jurisdictions that have used paperless voting machines have repeatedly pointed to the audit logs as the primary security mechanism and 'fail-safe' for any glitch that might occur on machines." Premier's Global Election Management System (GEMS) software is used to tabulate votes cast on the company's touch-screen and optical-scan machines. It is used in more than 1,400 election districts in 31 states. The initial investigation was set off by an incident in Humboldt County in which a Premier system lost nearly 200 ballots during the US presidential election in November. The company said the deletion was caused by a programming flaw in the GEMS software. Scrutiny of the audit logs by state officials revealed that the logs did not record critical information, making the tracing of the specific mechanism behind the deletion impossible. Furthermore, two of the logs featured a "clear" button that allowed officials to delete them, and although the button was eliminated in a later iteration of the GEMS software, three California counties still used the version with the button. California Secretary of State D. Bowen described the audit logs as "useless" and pledged to conduct a deeper probe of the issue.

Safer Net Surfing Is Goal of NIST Domain Name Security Experts
NIST Tech Beat (03/10/09), E. Brown

Scientists from the National Institute of Standards and Technology (NIST) are developing standards, guidance, and testing procedures designed to improve the security of the Domain Name System (DNS). Currently, the DNS system lacks the ability to authenticate the integrity of the source or response to the system, making it easier to redirect users away from legitimate addresses to Web sites that participate in phishing or other illegal Internet-based activity. NIST computer scientists led the development of new Internet Engineering Task Force standards to add digital signatures and associated key management procedures to DNS protocols. These additions, known as DNSSEC, let users validate the authenticity and integrity of the data and will supply the foundation for a new trust infrastructure for the DNS and protocols and systems that depend on it. NIST has posted a draft update of guidelines for DNS security, which is now available for public comment. Additionally, NIST recently provided technical assistance to ensure the security of the .gov top level domain. "We hope that the .gov deployment of DNSSEC will encourage rapid deployment in other sectors, including government contractors, trading partners, and general e-commerce sites," says NIST researcher S. Rose.