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

Δελτίο 96
12 Νοέμβρη 2007

Researchers Dig for Hidden Links in Spam
IDG News Service (10/31/07), J. Kirk

The links in spam messages are often used by filtering programs to determine if the message should be blocked, but spammers find loopholes by creating links that cannot be identified by filters but are still valid links, says University of Quebec software engineering professor C. Fuhrman. Spammers change and hide these links by altering the HTML enough to confuse filters but keep the links readable by browser rendering engines and email servers. Fuhrman believes that spammers test their altered links on Microsoft's Outlook program because it uses the same HTML rendering engine as the Internet Explorer browser. To find spammers' hidden links, Fuhrman is writing a program that uses Internet Explorer's rendering engine to parse out the links. Although some services already use algorithms to parse out the links in spam, the algorithms are hard to write and Fuhrman is interested in finding a way to parse messages without having to constantly tweak algorithms to keep up with new tricks used by spammers. Fuhrman says it is difficult to write a parser that will read links the same way Internet Explorer's rendering engine does because Microsoft's source code is secrete, so it is better to use the engine as part of the program. Any links that Internet Explorer's engine finds would be reported to a blocklist service. "I want to ultimately get it as a Web-based engine so that users can paste spam, and when it comes out, it will reveal the links," Fuhrman says.

Germany Seeks Expansion of Computer Spying
Los Angeles Times (10/30/07), K. Murphy

German law enforcement authorities want to expand government-sanctioned computer surveillance, citing the case of an abortive bombing in which plans for the attack were on the laptop of one of the suspects. "What this case showed us is that they are using laptops, they are using computers, and it would have been very, very helpful to track them down with online searches," says G. Schindler, director of the German Interior Ministry's counter-terrorism bureau. Germany is seeking authorization to plant clandestine Trojans into suspects' computers so that files, photos, diagrams, voice recordings, keystrokes, and other information can be scanned and recorded. This proposal does not sit well with a nation whose people carry bitter memories of official surveillance under past regimes. The Interior Ministry reports that laws authorizing online searches have already been passed in several European countries, and several more allow such searches or are in the process of adopting similar legislation. German parliament member H.-C. Stroeble says physical computer searches are already permissible with court approval, but secret searches would completely bypass legal procedures. "What we fear is that without any hint of a criminal background, police can secretly go into computers, maybe even the computers of political opponents, and spy them out, gaining access to personal data like photos, diaries, love letters, things like that," he says. M. Rotenberg of the Electronic Privacy Information Center says he has no awareness that searches via implanted software are being carried out by US authorities, but he notes that "it's also not clear, given the current view of the president on his powers to conduct electronic surveillance, that it hasn't been used."

Al Qaeda Hacker Attack Scheduled to Begin November 11th
InformationWeek (11/01/07), T. Claburn

DEBKAfile, an Israeli news site, asserts that Western, Israeli, Jewish, Shiite and Muslim apostate Web sites will be attacked by al Qaeda hackers beginning on Nov. 11. DEBKAfile claims that Bin Laden's "cyber legions" are getting even with Western surveillance systems that have persistently and effectively suppressed Al Qaeda's Web presence. The Dept. of Homeland Security emphasizes that DEBKAfile's report does not represent an official US alert, though the agency intends to seriously investigate the threat, as it does all threats. Although Forbes and Wired News have praised DEBKAfile for its journalism in the past, others debate the trustworthiness of the source. Nonetheless, software called Electronic Jihad 2.0 is obtainable online, and the most recent version of the software facilitates a distributed denial of service attack. Though the idea of Al Qaeda being involved in a cyberattack is worrisome, the menace is no more perilous than everyday security risks facing Internet users, says M. Zwillinger, a former cybercrime prosecutor with the Dept. of Justice. In addition, modern networks are better equipped to handle denial of service attacks than networks from several years ago, he says.

Setting a Cybersecurity Agenda for the 110th Congress
Government Computer News (10/31/07), W. Jackson

At the Congressional High Tech Caucus on Wednesday more than four dozen representatives and senators started work on an IT legislative agenda for the 110th Congress. Although numerous bills on computer crime, infrastructure protection, spyware, and data breaches have been introduced in both houses, and a number of bills are pending, few have made it to a vote, and even fewer have become law. At the caucus the Consumers Union's J. Kenney pushed for a strong national breach notification law to help protect personal identification from theft or exposure. "Industry and government are not investing in cybersecurity measures," Kenney says. "We need to create incentives to make these investments. One way to do that is requiring that consumers are always notified when their personal information is breached." Many in the information technology industry want to see a national standard replace the 35 different state notification laws, while the Cyber Security Industry Alliance says any notification law should include safe harbors for businesses that deploy strong, pre-breach security measures. Both Consumer Data Industry Association President S. Pratt and Homeland Security Department chief privacy officer H. Teufel III say collecting personal data can improve security and the resulting risks to privacy are an acceptable trade-off, arguing that data collection has been used to prevent fraud and that security and privacy go hand in hand.

Voting Out E-Voting Machines
Time (11/03/07), T. Padgett

Although they were once considered the solution to outdated paper-based voting systems, electronic and touch-screen machines have come under intense scrutiny, and a new bill in Congress would ban DRE machines in federal elections starting in 2012. "We have to start setting a goal on this," says Sen. B. Nelson (D-Fla.), who introduced the bill with Sen. S. Whitehouse (D-R.I.). "Voters have to feel confident that their ballot will count as intended." Trust in electronic voting is eroding as controversies over the accuracy of the machines are mounting. As a result of a tainted election in 2006, Florida Republican Governor C. Crist mandated the state return to an optical scan system in which votes are marked on a sheet, which is kept for auditing, and electronically scanned. Optical scanning is considered far mo-

re accurate, and is favored by the National Institute of Standards and Technology, which advises the US Election Assistance Commission. The Nelson-Whitehouse legislation would also require routine audits of at least 3% of the precincts in all federal elections, and would possibly mandate that all voting machines create a paper trail as early as the 2008 election. Some worry that many states may not be able to incorporate paper trail technology by the 2008 election, but D. McCrea, head of the Florida Voters Coalition, believes that not only is it feasible but that it is also vitally important. "It will be a challenge, but the voter fairness issue involved here is too important," McCrea says.

The University's Role in Advancing Data Encryption, Part 2
TechNewsWorld (11/01/07), A. Burger

Technological innovations, new legislation and regulations, and pressing security needs are factors driving the increase of collegiate and university encryption technology research, and areas that industrial and academic investigators are considering as possible application centers include nanotechnology, quantum cryptography, and the supply chain. CipherOptics' J. Doherty says network performance is an important area that should not be ignored, even as most encryption research efforts are focused on the creation of more robust encryption algorithms. "Today's high-performance networks must be able to meet the latency requirements of delay-sensitive applications such as voice and video over IP," he notes. "While there may be a niche market for security over performance types of solutions, broad adoption of new encryption algorithms will be determined by speed as much as they are by security." Such is the nature of research being conducted by the Rochester Institute of Technology's networking, security, and systems administration department, whose researchers conclude that the selection of a wide-area network encryption solution involves consideration of not just performance, but also how well the technology satisfies organizational requirements and other non-performance related factors. Higher education institutions such as Southwestern Illinois Community College are incorporating encryption into their courses and curricula and using it to safeguard data on campus. The college's C. Leja says the possibility of making a data assurance course with an encryption component a required course is under discussion. She points out that colleges and public and private sector organizations are also being spurred to deter identity theft and find applications for encryption technology by new legislation and the introduction of payment card security standards. "Higher education provides open and secure access for its students, and encryption offers a clear path to secure sensitive data and support an open, mobile environment," she says.

UMass Researchers Describe New Approach to Tag Security
RFID Journal (11/01/07), M.-C. O'Connor

University of Massachusetts Amherst researchers have discovered a way of securing RFID tags against tag cloning and fraud. Passive RFID tags contain volatile memory composed of memory cells, a circuit representing a single piece of data. When a RFID scanner powers up the tag, the chip's memory cells produce a unique fluctuating electrical pattern before creating the ID and any other information stored on the chip. The fluctuating electrical pattern is unique to each RFID tag and can be used to authenticate the tag the next time it is scanned. The pattern can also be used to encrypt the tag's encoded data, securing it against being read by an unauthorized scanner. An end user could apply a tag's unique pattern to a randomness extractor as part of a hash cryptography process, creating a string of random numbers that could be used to generate keys to decrypt the stored tag data. Reading the data could be done with any scanner, but changing the data would need to be done with specialized software to

generate the keys needed to decrypt the data. Only RFID tags that use volatile, static random access memory generate the pattern, meaning EPC Gen 2 tags, widely used in supply chain applications for tracking and tracing products, are unable to use the same security system as they use nonvolatile, electrically erasable, programmable, read-only memory chips, which a-re less expensive than volatile memory.

Targeting Internet Terror
Baltimore Sun (11/07/07) P. 4A; S. Gorman

President Bush on Nov. 6 requested $154 million in preliminary funding for his plan to launch a program targeting terrorists and others who would attack the US through the Internet. Former government officials say the initiative is expected to become a seven-year, multi-billion-dollar project intended to track threats in cyberspace on government and private networks. The project would be run by the Dept. of Homeland Security, but use resources from the NSA and other intelligence agencies. As many as 2,000 people would staff the initiative, and the first goal would be developing a comprehensive cyber security program. Lawmakers, who only recently received briefings on the initiative, continue to have concerns over whether the program has adequate privacy protection, as well as other questions. One former government official familiar with the project says total startup costs could reach $400 million. "The proposal may be long overdue, but there are too many questions on how it will be implemented and how it will avoid the fate of past failed plans that remain unanswered," says chairman of the House Homeland Security Committee Rep. B. Thompson (D-Miss.). "I hope the answers to those questions will come shortly so that cyber security no longer remains on the government's back burner." Thompson expressed specific concerns over the legality of the program and whether it provides sufficient privacy protections. Sen. J. Lieberman (I-Conn.), who chairs the Senate committee overseeing Homeland Security, says he is "encouraged that the Dept. of Homeland Security is finally taking a strong, leadership role in domestic cyber security." He says that without knowing the details, the initiative "appears to be a step toward better protection of government computers and information."

'Suicide Nodes' Defend Networks From Within
New Scientist (11/01/07), P. Marks

University of Cambridge researchers have developed a computer defense system that mimics how bees sacrifice themselves for the greater good of the hive. The approach starts by giving all the devices on a network, or nodes, the ability to destroy themselves, and take down any nearby malevolent devices with them. The self-sacrifice provision provides a defense against malicious nodes attacking clean nodes. "Bee stingers are a relatively strong defense mechanism for protecting a hive, but whenever the bee stings, it dies," says University of Cambridge security engineer T. Moore. "Our suicide mechanism is similar in that it enables simple devices to protect a network by removing malicious devices--but at the cost of its own participation." The technique, called "suicide revocation," allows a single node to quickly decide if a nearby node's behavior is malevolent and to shut down the bad node, but at the cost of deactivating itself. The node also sends an encrypted message announcing that itself and the malevolent node have been shut down. The purpose of the suicide system is to protect networks as they become increasingly distributed and less centralized. Similar systems allow nodes to "blackball" malicious nodes by taking a collective vote before ostracizing the malicious node, but the process is slow and malicious nodes can outvote legitimate nodes. "Nodes must remove themselves in addition to cheating ones to make punishment expensive," says

Moore. "Otherwise, bad nodes could remove many good nodes by falsely accusing them of misbehavior."

Computer Scientist Fights Threat of 'Botnets'
University of Wisconsin-Madison (10/31/07), B. Mattmiller

University of Wisconsin-Madison computer scientist P. Barford is developing Nemean, a new computer security technique for detecting network intrusions. Barford says the problem with current detection systems is the high number of false positives. Hackers have become so capable of disguising malicious traffic that security systems create thousands of false positives. Most network-intrusion systems compare traffic against a manually collected database of previously recognized attack signatures. Nemean automatically generates intrusion signatures, making the detection process faster and more accurate. A test comparing Nemean against current technology on the market showed that both systems had a high detection rate of malicious signatures, 99.9% for Nemean and 99.7% for the commercially available technology, but Nemean had no false positives, compared to the 88,000 false positives created by the other system. "The technology we're developing here really has the potential to transform the face of network security," Barford says. Barford's research was supported by the National Science Foundation, the Army Research Office, and the Dept. of Homeland Security. "This is an arms race and we're always one step behind," Barford says. "We have to cover all the vulnerabilities. The bad guys only have to find one."

Why VoIP Is the Next Target for Spammers
Guardian Unlimited (UK) (11/01/07), S. Hargrave

Email spam filters have become so good at preventing unsolicited marketing messages from making their way into users' inboxes that it has become rare for spam to actually be read, says Columbia University computer science professor H. Schulzrinne. As a result, spammers are increasingly choosing to send their unwanted messages to voice over Internet protocol (VoIP) accounts instead of email inboxes, Schulzrinne says. He notes that while such attacks on Internet telephony accounts--known as "spit" (spam over Internet telephony)--are still very rare compared to email spam, spammers are finding it tempting to target VoIP because a ringing phone is a lot harder to ignore than an email message. In addition to spam, VoIP accounts are also prone to a type of phishing called "vishing." In vishing attacks, a fraudster can choose the name and number that will be displayed on the victim's caller ID. This allows fraudsters to claim that they are calling from their victim's bank and trick them into supplying personal information that can be used to steal money from online accounts or commit identity theft. IBM's J.-P. Ballerini says vishing will likely become the most common type of attack on VoIP accounts because it is more likely to lead to money for spammers.