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

Δελτίο 125
12 Αυγούστου 2008

Attackers' Behavior Builds Better Blacklists
Security Focus (07/24/08), R. Lemos

Computer scientists at SRI International and the SANS Institute have developed the Highly Predictive Blacklist algorithm, a technique that determines an attacker's preference for victims' networks in order to prioritize additions to blacklists. The technique allows network owners to correlate attacks on their networks with attackers' preferences for other networks, using a system similar to Google's PageRank System. The researchers correlated attackers' choices in targets using firewall logs contributed by participants in the SANS Institute's DShield service. By matching the preferred victims of a known attacker, the researchers were able to develop per-network blacklists that perform better than either massive global lists or more focused local lists. "Our experiments demonstrate that our Highly Predictive Blacklist algorithm consistently creates firewall filters that are exercised at much higher rates than those from conventional blacklist methods," says SRI's P. Porras. The blacklists were created in three stages. First, the researchers removed any unreliable alerts from the logs submitted by contributors. Next, relevance-based rankings were used to prioritize attacks for each contributor. Lastly, the system gave priorities to patterns that match known malware propagation trends. The system was tested using 720 million log entries and found to outperform global and local blacklists in more than 80% of the cases.

A Photo That Can Steal Your Online Credentials
IDG News Service (08/01/08), R. McMillan

Researchers at the Black Hat computer security conference in Las Vegas next week will demonstrate an attack that could steal online credentials from users of popular Web sites. The attack uses a new type of hybrid software file the researchers have dubbed a GIFAR. By placing the file on Web sites that allow users to upload images, the researchers can circumvent security precautions and take over the Web page users' accounts. NGS Software's J. Heasman says the GIFAR is a Java applet in the form of an image. GIFAR is a contraction of the graphics interchange format (GIF) and Java Archive (JAR), the two file types that make up the applet. The researchers will demonstrate how to create the GIFAR, while omitting a few details to prevent it from being used for a widespread attack. To a Web server, the file looks exactly like a GIF file, but a browser's Java virtual machine will open the file like a JAR file and run it as an applet, giving the attacker an opportunity to run Java code on the victim's browser, which treats the applet as though it was written by the Web site's developers. The researchers say the attack could work on any site that allows users to upload files, possibly even sites that are used to upload banking card photos or sites such as Amazon.com. The GIFAR attack can be prevented by improving filtering tools so Web sites can detect the hybrid files, and Sun could also improve the Java runtime environment.

Cloud Computing's Perfect Storm?
Technology Review (08/07/08), J. Borland

Intel, Yahoo, Hewlett-Packard, and a group of three international research institutions recently announced they will be participating in a collaborative cloud-computing research initiative aimed at developing an Internet-based computer infrastructure stable enough to host a company's most critical data-processing tasks. The project could also lead to advancements in fields such as climate-change modelling and molecular biology. The six linked data centers, each one operated by a project sponsor, will be one of the largest experiments ever focusing on cloud computing. The large scale of the project will allow researchers to test and develop security, networking, and infrastructure components on a broad basis simulating an open Internet environment. To test this infrastructure, academic researchers will run real-world, data-intensive projects that could lead to new discoveries in data mining, context-sensitive Web searches, and communication in virtual-reality environments. Despite its promise, experts say the cloud-computing model remains technologically underdeveloped. The most progressive thinkers predict that companies will ultimately use remotely hosted cloud services to perform their most complex computing activities. Each of the companies involved in the new initiateve has a specific set of research projects planned, with most broadly focusing on operational issues such as security, load balancing, managing parallel processes on a large scale, and how to configure and secure virtual machines across different locations.

Open-Source E-Voting Gets LinuxWorld Test Run
Computerworld (08/06/08), T. Weiss

Computer engineer A. Dechert unveiled the open source electronic-voting system he helped develop at the recent LinuxWorld Conference & Expo. In December 2000, Dechert cofounded the Open Voting Consortium to research better ways to vote and to create an e-voting system that allows voters to make their selections on a screen, print their ballots, and then have the ballots scanned by reliable machines. Dechert says such a system leaves no ambiguity over what a voter intended, fixing a common problem found in punch-card systems and poorly designed ballot layouts. LinuxWorld attendees were able to view the system and vote in a mock election. The system runs on PC loaded with Ubuntu Linux and a free, open source e-voting application created by the consortium. Dechert says election officials can easily set up and create a ballot for any election using a special software tool. Some local voting jurisdictions are already in talks with the group about further exploring the system; however, for use in national elections, the system would have to be heavily analyzed and eventually certified as an election system, Dechert says.

Hacking Electronic Toll Systems
CNet (08/06/08), E. Mills

Attendees of the Black Hat 2008 security conference in Las Vegas were told that anyone with the right transponder reader could easily hack into the transponders used by drivers subscribing to electronic toll systems such as FasTrak and E-ZPass. Armed with the readers, hackers could steal unencrypted identification numbers off transponders, put the data onto their devices, and then stick the victim with the bill as they pass through tolls for free. Worse, data could be switched from a transponder installed in a vehicle used in a crime, thus providing the driver with an alibi. And while the identification number is not personally identifyable, it can be used to access customer information--including names, driver's license numbers, and credit card numbers--through the back-end database. N. Lawson, a security expert at security consultancy Root Labs who warned of the vulnerability at Black Hat, is designing a privacy kit for the FasTrak system used in the San Francisco Bay Area that will allow users to put a "kill switch" on a transponder, thus making it unreadable until it is turned on with a special button.

EFF Launches Coders' Rights Site at Black Hat Conference
Ars Technica (08/06/08), J. Timmer

The Electronic Frontier Foundation (EFF) is using the Black Hat USA conference to launch the Coders' Rights Web site, which is intended to help security researchers understand the legal issues involved when searching for and testing vulnerabilities in commercial software. EFF civil liberties director J. Granick is spearheading the project. "Coders who explore technology through innovation and research play a vital role in developing and securing the software and hardware we use everyday," Granick says. "Yet this important work can be stymied by bogus legal threats." The site contains cautionary information for anyone thinking about getting involved in testing for security threats. Many commercial programs come with end-user license agreements (EULA) that forbid any sort of disassembling of the compiled code, prohibiting anyone bound by the EULA from using a common method for finding vulnerabilities. Meanwhile, the legal enforceability of click-through agreements varies between jurisdictions, and developers that work with specific software development environments or toolkits may be subject to nondisclosure agreements that prevent them from revealing the inner workings of the software. Some security measures may also fall under laws governing trade secrets, and any discoveries concerning security measures taken to protect digital rights management protected content can face challenges from the Digital Millennium Copyright Act.