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

Δελτίο 148
10 Μάη 2009

Panel Advises Clarifying US Plans on Cyberwar
New York Times (04/30/09) P. A18; J. Markoff; T. Shanker

A report based on a three-year study by a panel assembled by the National Academy of Sciences says the US does not have a clear military policy on how to respond to a cyberattack. The report, "Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities," says the United States needs to clarify both its offensive capabilities and its planned defensive response. Admiral W. Owens, a former vice chairman of the joint chiefs of staff and an author of the report, says the notion of "enduring unilateral dominance in cyberspace" by the US is not realistic, in part due to the low cost of the technologies required to mount attacks. Owens also says the idea that offensive attacks are non-risky military options also is incorrect. The report's authors included several scientists and cyberspecialists. The report says the United States should create a public national policy regarding cyberattacks based on an open debate about the issues and urges the United States to find common ground with other nations on cyberattacks to avoid future military crises. The Pentagon National Military Strategy states that cyberattacks on US commercial information systems or transportation networks could have a greater economic or psychological effect than a relatively small release of a lethal agent. The effort to project a lack of clarity is seen as being important to keeping adversaries uncertain of the severity of a US counterattack, which has historically been an essential element of deterrence.

Software: The Eternal Battlefield in the Unending Cyberwars
Computerworld (04/27/09), G. Anthes

Cybercriminals still have the upper hand on the Internet despite nearly two decades of technological advancement, and Carnegie Mellon University professor W. Scherlis says the cybercrime problem is being exacerbated by three information technology trends. These trends include a migration from functional system silos to interconnected, enterprise, and cross-enterprise systems; decentralization of IT responsibility; and the very rapid propagation of actions throughout networks and systems. Cornell University's F. Schneider believes a much more effective cybersecurity approach would concentrate on accountability rather than prevention, whereby cybercriminals would be kept in check if they could be apprehended and held accountable rather than blocked. The realization of this concept is being impeded by a widespread expectation of online anonymity, and by inconsistencies of local law and custom that could complicate the prosecution of cyberattackers outside the US. Microsoft's S. Charney argues for a fundamental revision of cybersecurity, first by the establishment of end-to-end trust that supports strong authentication at every boundary and tier in computing. Microsoft's S. Lipner says many components of the end-to-end trust model already exist, such as the tamper-proof Trusted Platform Module. Also needed is the implementation of a mechanism for auditing events to deliver accountability. Scherlis says users also can take action. He recommends that users "be absolutely rigorous about configuration management and configuration integrity, both during development and ceaselessly during operations."

Computer Hackers R.I.P. - Making Quantum Cryptography Practical
Institute of Physics (30/04/09)

Researchers from Toshiba and Cambridge University's Cavendish Laboratory say quantum communication is possible with practical components for high-speed photon detection. In their paper, "Practical Gigahertz: Quantum Key Distribution Based on Avalanche Photodiodes," the researchers discuss using an attenuated laser as a light source and a compact detector as a decoy protocol to guard against third-party attacks. The erroneous information would confuse all intruders except the compact detector. "With the present advances, we believe quantum key distribution is now practical for realizing high bandwidth information - theoretically secure communication," the researchers say. The high-speed detectors would receive information at higher key rates, would receive more information faster, and would make quantum key distribution easier to use. The researchers note that secure communication is of considerable interest to governments, banks, and large businesses.

Cyber-Command May Help Protect Civilian Networks
Washington Post (05/06/09) P. A4; E. Nakashima

The US Pentagon is considering establishing a new cybercommand to oversee government efforts to protect military computer networks and to assist in protecting civilian government networks, says National Security Agency (NSA) director Lt. Gen. K. Alexander. The new command would focus on better protecting US military computers by combining the offensive and defensive capabilities of the military and the NSA. The NSA also wants to provide technical support to the US Dept. of Homeland Security (DHS), which is responsible for protecting civilian networks from cyberattacks. Alexander says it makes sense for DHS and the Defense Department to use the same security technology. Former top DHS cybersecurity official A. Yoran says the NSA has significant depth and expertise, but cautions that the effort must be transparent. "DHS needs to be very, very cautious about its participation in a program like that because you could fundamentally erode the trust DHS needs in order to be successful in its broader security mission," Yoran says. Any effort involving the NSA that goes beyond protecting military networks requires careful legal analysis, according to Yoran. Alexander says a variety of questions need to be answered before attempting a partnership with DHS, including what is the framework for sharing classified threat signatures, how to operate at network speed in a defendable manner, and what is the legal and operational framework.

Unmasking Social-Network Users
Technology Review (05/06/09), E. Naone

University of Texas at Austin researchers have found that, combined with readily available data from other online sources, social network data can reveal sensitive information about users. Using the photo-sharing site Flickr and the microblogging service Twitter, the researchers were able to identify a third of the users with accounts on both sites by searching for recognizable patterns in anonymized network data. Both Twitter and Flickr display user information publicly, so the researchers anonymized much of the data to test their algorithms. The objective was to determine if it was possible to extract sensitive information on individuals using the connections between users, even if almost all of the personally identifying information had been removed. The researchers found that extracting information was possible provided they could compare patterns with those from another social-network graph in which some user information was accessible. Texas professor V. Shmatikov notes that social network data, particularly the patterns of friendships between users, can be valuable to advertisers. However, he says releasing that information also makes the networks vulnerable. The researchers found that non-anonymous social network data is easy to find. "Every person does a few quirky, individual things which end up being strongly identifying," Shmatikov says. Carnegie Mellon University professor A. Acquisti says the research points to the difficulty in maintaining privacy online. "There is no such thing as complete anonymity," Acquisti says. "It's impossible."

How Hackers Can Steal Secrets From Reflections
Scientific American (04/27/09), W. Gibbs

Even the best electronic security may not be enough to protect sensitive data from dogged hackers, and researchers have been able to extract information from the flashes of light-emitting diodes on network switches or the reflection of screen images off an eyeball. Swiss Federal Institute of Technology graduate students M. Vuagnoux and S. Pasini observe that commonplace radio surveillance equipment can pick up keystrokes as they are typed on a keyboard in a different room, and they are preparing a conference paper detailing four unique ways that keystrokes can be inferred from radio signals captured through walls at distances up to 20 meters. These side-channel exploits are untraceable and very difficult to defend against, yet computer security researchers have devoted little attention to the problem. Although many of these attacks require specialized knowledge and equipment, Max Planck Institute for Software Systems fellow M. Backes contends that reflection-based attacks can be carried out by anyone with a $500 telescope and a digital camera. Eyes and other curved surfaces are particularly useful in reading reflections as they reveal wide swathes of their surroundings. Privacy filters applied to laptop screens to prevent over-the-shoulder eavesdropping can aid reflection exploits, as the filters raise the brightness of the reflection on the viewer's eyes. It is doubtful that side-channel attacks will become as ubiquitous as spam, malware, and other network hacking tools. As University of Cambridge Computer Laboratory scientist M. Kuhn notes that "you have to be close to the target, and you must be observing while a user is actively accessing the information." These methods will probably be employed to infiltrate specially selected targets such as the computer systems of financiers and high-level corporate and government officials.

Examining Social Networking for Terrorists to Find People Behind Terrorist Attacks
Inderscience Publishers (05/05/09)

Social Design Group's Y. Maeno and University of Tokyo professor Y. Ohsawa have developed a new approach to analyzing social networks that could help find the covert connections between the people responsible for terrorist actions by revealing the nodes that act as hubs in a terrorist network and backtracking to individual planners and perpetrators. The researchers say their approach also could help prevent future attacks. Maeno and Ohsawa say that along with disaster recovery management, terrorist attacks create the added pressure of short-term responses to the terrorists themselves and the long-term need to identify and weaken the covert operations and infrastructure of the organization behind the attack. Combining the prior understanding of expert investigators with graph theory and computational data process should make it possible to analyze a terrorist network and reveal latent connections and patterns. The approach involves the discovery of nodes, which are the hubs in a network where different members of the network are connected. Members usually have one or two connections, nodes have several connections, and critical nodes have many more. To test the validity of their approach, the researchers applied their technique to the network used by the organization behind the 9/11 attacks and were able to find some connections that were not known before the attacks.

Researchers Take Over Dangerous Botnet
Dark Reading (05/04/09), K. Jackson-Higgins

University of California-Santa Barbara (UCSB) researchers temporarily commandeered an infamous botnet known for stealing financial data and found that the threat it represents is even greater than had been originally assumed. The Torpig/Sinowal/Anserin mini-botnet targets organizations and users to steal bank account information or other sensitive personal data. It is considered more dangerous than big-name botnets because of its small scale and stealthiness. Torpig uses drive-by download attacks as its initial mode of infection, and upon infection the botnet can unleash crafty phishing attacks that produce bogus but authentic-looking Web pages and forms that trick users into exposing their credentials. The UCSB researchers accumulated approximately 70 GB of data for the 10 days they were in control of Torpig, and in that period the botnet stole banking credentials of 8,310 accounts from more than 400 financial institutions, including PayPal, Capital One, E-Trade, and Chase. Nearly half of the 1,660 stolen debit and credit card accounts the researchers counted belonged to victims in the US. "The level of sophistication, the amount of data that it is able to steal, and the fact that it has been active for more than three years is truly remarkable," says UCSB researcher B. Stone-Gross. The researchers' disclosures provoked debate on whether the information they exposed about Torpig, its workings, and its victims could compromise efforts to eventually undo the botnet. "This [research] does create a road map ... for the [botnet] criminals to fix, and not just for others to exploit," says RSA's Sean Brady.