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

Δελτίο 65
14 Μάρτη 2007

E-Rescue Plans for Coping With Disasters
The Australian (03/06/07), J. Foreshaw

A four-year project led by the National ICT Australia (NICTA) is developing technology to help response efforts in the case of natural disasters or other emergencies. The Smart Applications for Emergencies (SAFE) initiative will include video surveillance with smart cameras, wireless mesh networking, planning, and information management. "We need to improve our game, in terms of how we operate across agencies, how we warn the community, and how we can better provide response and long-term response systems to enable more efficient deployment of resources post-disaster," says Safeguarding Australia project leader R. Iannella. A NICTA lab is currently building a demonstrator to prove that these technologies can be combined into an effective response system. NICTA's Smart Transport and Roads project is building test-beds on Sydney streets to trial wireless and sensing technology, eight of which have been completed. These test-beds include advanced video sensing and surveillance techniques, new traffic control systems, and multi-modal interfaces for control-room operations. As these technologies develop, they are expected to be applied to military, logistical, and airline systems. Many aspects of the SAFE project were on display at Techfest 2007, NICTA's annual technology showcase.

The Digital Building--Security Starts at the Door
Fraunhofer-Gesellschaft (03/07)

German researchers have developed digital building technology that blurs the line between IT and the physical world. The system, known as "facilityboss," enables rooms to be reserved using only the Internet, locks to be adjusted automatically and remotely to grant access to certain people on certain dates and to instantly alter accessibility, and all IT systems and electronic devices to be interconnected. "Facilityboss is a kind of operating system for the digital building, making it possible to link and control a wide variety of components in a building," says the Fraunhofer Institute for Secure Information Technology's T. Henkel. Building operations, from heating to computers, can be controlled from a single interface, which gathers information from a network of sensors throughout the building. RFID tags enable the building to know where various equipment is being used at any given time and enable people to access certain areas by identifying themselves. The radio-based locking system is comprised of cylinder locks with an integrated radio system and a PC that runs administration software. Each cylinder lock connects to the administration through an access point, allowing changes to be made remotely in the case that keys are lost or a new employee is hired. When a room is reserved for a certain time, those meeting there are able to gain access during the hours reserved. "The [locking] system combines the advantages of electronic locking systems with those of wireless communications," says the Fraunhofer Institute for Communications Systems ESK's M. Augel.

Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure

Honeyblog (03/05/07), V. Lam; S. Antonatos; P. Akritidis

Puppetnets are networks generated by malevolent Web sites for the purpose of indirectly misusing visiting Web browsers as unwitting tools for worm propagation, distributed denial-of-service attacks (DDoS), reconnaissance scans, and other attacks on third parties. Though the threat rating of puppetnets is lower than that of botnets, the regularity of client-side exploits could make puppetnets a serious problem in the future, according to the authors of a study presented at the recent ACM Conference on Computer and Communications Security. Unlike botnets, puppetnets are not critically reliant on the exploitation of specific deployment flaws or on social engineering strategies that fool users into installing malware on their computer; they also support a model where the attacker has only partial control over the actions of the participating nodes, while the dynamic nature of puppetnet participation makes puppetnets harder to track and filter. The authors contend that the use of puppetnets illustrates a flaw in the Web's design, namely that the security model is committed almost exclusively to shielding browsers and their host environment from malicious Web servers and servers from malicious browsers, thus ignoring the possibility of assaults directed against third parties. The power of a puppetnet depends on how popular a malicious Web site is as well as the users' browsing patterns. The authors offer several approaches for countering puppetnet attacks, although they are only partial solutions at best. Disablement of JavaScript will reduce the effectiveness of puppetnet-engineered DDoS attacks, reconnaissance probes, and worm propagation by at least one order of magnitude, while carefully implementing existing defenses can also mitigate the puppetnet threat to a certain degree. Other defenses evaluated include server-side controls and puppetnet tracing, server-directed client-side controls, client-side behavioral controls, and filtering that uses attack signatures, all of which have their pluses and minuses.

Last Month's Root-Server Attack Revisited
Register (UK) (03/09/07) Goodin, Dan

A factsheet released by ICANN shows that the Feb. 6 DDoS attack on six or more of the Internet's root servers only damaged two of the servers, both of which lacked a protective new load-balancing technology called Anycast. All of the other servers that were attacked had Anycast installed. ICANN's document states: "Anycast allows a number of servers in differrent places to act as if they are in the same place. So while there remains 13 locations on the network for root servers, the reality on the ground is that not only are there often dozens at one spot but dozens of servers in other locations that can also deal with requests." The Feb. 6 attack was a two-pronged assault, with the first assault lasting 2.5 hours and the second lasting 5 hours. Hundreds of zombies were responsible for the attacks, and while it is impossible to determine the geographic location of the attackers, experts believe they came from Korea or another location in the Asia Pacific region. The G-root (run by the U.S. Department of Defense and located in Ohio) and the L-root (run by ICANN and located in California) were damaged in the attack. Three other servers have yet to implement Anycast, but it is expected that they will now do so.

Aussie Video Surveillance Technology Leaves Rivals for Dead
Computerworld Australia (03/06/07) Pauli, Darren

National ICT Australia (NICTA) is developing intelligent surveillance technology that would be able to predict behavior and identify faces, even from a distance and if the angle is impaired. The operating system and software package makes use of sophisticated algorithms to analyze physical characteristics, appearances, and mannerisms from analog video data. The iBox is able to convert the data into a digital format for motion detection, facial recognition, and behavior prediction. David Snowdon, the operating system's developer, says public areas that demand high-level security such as airports and transit facilities would be a good fit for the system. "IBox overcomes the problems of traditional surveillance and sensory technology because it can be located at higher, lower, or more obscure angles while still making a positive ID with far less [facial] information," says Snowdon. "It could be used to detect whether someone is carrying a weapon-like object, or if they are planning to jump from a train platform and it can more accurately match facial characteristics to a database."