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

Δελτίο 160
10 Οκτώβρη 2009

Code Breakthrough Delivers Safer Computing
University of New South Wales (09/25/09), P. Trute

Computer researchers at the University of New South Wales and NICTA say they have proven that an operating-system kernel was 100% free of bugs. The team verified the kernel known as the seL4 microkernel by mathematically proving the correctness of about 7,500 lines of computer code in a project taking an average of 6 people more than 5 years. "What we have shown is that it's possible to make the lowest level, the most critical, and in a way the most dangerous part of the system, provably fault free," says NICTA researcher G. Heiser. The research could potentially improve the security and reliability of critical systems used by the medical and airline industries as well as the military. "The verification provides conclusive evidence that bug-free software is possible, and in the future, nothing less should be considered acceptable where critical assets are at stake," Heiser says.

New Digital Security Program Doesn't Protect as Promised
University of Texas at Austin (09/29/09)

The Vanish security system has been broken by a team of researchers from the University of Texas at Austin, Princeton University, and the University of Michigan. Developed by scientists at the University of Washington, Vanish is designed to protect a computer user's data by restricting the availability of the encryption key used to access it after a certain amount of time, such as eight hours. Vanish splits up the keys into many small pieces and stores them at many different places on the network, which makes the data look like digital gibberish. However, the team has developed a program, Unvanish, which is capable of collecting and storing anything that looks like a fragment of a Vanish key on the network, checking its archive of fragments and finding the pieces needed to decrypt a message. The researchers say Unvanish can make messages reappear long after they should have disappeared, close to 100% of the time. "A true self-destruction feature continues to be challenging to provide," says Texas professor B. Waters. Texas professor E. Witchel says that "our goal with Unvanish is to discourage people from relying on the privacy of a system that is not actually private."

Researchers Hijack a Drive-By Botnet
Technology Review (10/02/09), R. Lemos

A recent University of California at Santa Barbara (UCSB) study examined the damaging effects of the computer-infecting Mebroot botnet. The Mebroot botnet network corrupts normal Web sites and redirects their visitors to a domain that tries to infect their computers with malware. Once infected, the computers can be controlled by Mebroot programmers. The Mebroot botnet is difficult to track because programmers change the domain name daily using three Javascript algorithms similar to one used by the computer worm Conficker. Two of the algorithms use the day's date as a variable, but the third uses characters from the day's most popular key word search on Twitter. This is difficult for antivirus programmers to predict, making it harder to protect computers from invasion. "It is definitely one of the most advanced and professional botnets out there," says F-Secure's K. Kasslin. UCSB researchers tried to use the

algorithms against the Mebroot programmers, predicting upcoming domain names and booking them ahead of time, but the attackers responded by reserving the names more quickly. The researchers found that almost 70% of visitors to dangerous Mebroot domains were exposed to about 40 different methods of infection. About 35% were exposed to the 6 vulnerabilities that Mebroot uses. Study author and UCSB computer scientist G. Vigna says that computer users need to update their antivirus software more frequently to avoid infection.