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

Δελτίο 83
16 Ιουλίου 2007

Data on Americans Mined for Terror Risk
Associated Press (07/10/07), L. J. Jordan

The US government is engaged in a data-mining effort to collect and store information on US citizens to help find potential terrorists, insurance frauds, and corrupt pharmacists, according to a Justice Department report sent to Congress this week. Justice told Congress that records on identity theft, real estate transactions, motor vehicle accidents, and Internet drug companies are being examined to find connections between occurrences. Additionally, the report disclosed government plans to build a database that will be used to asses the risk posed by people considered potential or suspected terrorists. The chairman of the Justice Department's Senate oversight committee said the database was "ripe for abuse," and the American Civil Liberties Union immediately questioned the quality of the information that would be used to label someone as a terror threat. Justice's Dean Boyd said the data-mining databases are strictly regulated to protect privacy and civil liberties. The report said that all but one of the databases, the one intended to track terrorists, have been operating for several years. The terrorist-tracking database, or System to Assess Risk (STAR), is still under construction and is design to help counter-terror agencies narrow the field of people who pose the greatest possible threat, not to label anyone a terrorist, Boyd said. The Justice report also said that STAR might be used to create a list of terror suspects from other sources, including Data Mart. Data Mart is a collector of government information, as well as travel data from the Airlines Reporting Corp., and other information from private data collectors, which may including information such as voter and vehicle registration.

Happy Birthday, Dear Viruses
Science (07/13/07) Vol. 317, No. 5835, P. 210; R. Ford; E. Spafford

This year marks the 25th anniversary of the genesis of the first computer virus. In 1982, a high school student in Pittsburgh wrote a virus that infected Apple II systems. The virus is known as the "Elk Cloner" and did little more than copy itself to floppy disks and display bad poetry, a minor irritation compared to the viruses of today. After Elk Cloner, the problem of malware grew slowly in the early 1980s, but became major news in 1988 when the "Morris Worm" spread worldwide and caused outages across the still young Internet. Since then, numerous viruses and pieces of malware have made news, created fear and headaches for everyone with a computer, and caused billions of dollars in damage. Some of the more memorable names include the Michelangelo virus, SQL.Slammer, Code Red, Nimda, Concept, and Melissa. Today, the greatest risk is financial damage from stolen information and identity theft, and attacks are far more quiet to avoid getting noticed. Instead of displaying a message or erasing a computer's hard drive, malware turns computers into spam machines, platforms for other attacks, or secretly records financial information and passwords. Despite the best efforts of researchers, programmers, and security experts, malware is not going to go away anytime soon. Cell phones continue to become more advanced, and as handheld mobile devices are used for computing tasks, cell-to-cell malware will become prevalent. Computers are difficult to make and keep secure, and humans are normally the reasons viruses manage to bypass security measures.

Security Paper Shows How Application Can Steal CPU Cycles
Ars Technica (07/11/07), J. Reimer

At the annual Usenix security symposium, D. Tsafrir, Y. Etsion, and D. Feitelson presented their paper, "Secretly Monopolizing the CPU Without Superuser Privileges." The researchers presented a proof-of-concept program that allows a specified task to "cheat" and consume more CPU cycles than the operating system would normally permit. The program was designed for Unix-based systems, though it could theoretically be altered to affect any multitasking operating system. The program in the paper, called "cheat," can run as a regular non-administrative user. Theoretically, a task could hide by arranging for its process to run immediately after the CPU interrupt "tick," and stop running right before the next tick. By avoiding the ticks, the standard operating system would never notice the task is running. Without any modification to an operating system, all methods of monitoring tasks would not display the cheating task. Seven different operating systems were tested as potential platforms for the attack, and only Mac OS X was immune to the cheat attack, but only because it uses a different scheduling algorithm for its timers. The researchers say they doubt cheat-like attacks will become common because while they could be used to avoid detection, using most of a computers CPU would noticeably slow the computer and raise suspicion. However, programs could be written to cheat a little bit, and would be extremely difficult to detect and remove. The researchers say it is possible to protect the operating system against cheat attacks, but performance suffers as a result.

Bootable Disc Makes for Safer Banking, Researcher Claims
Computerworld Australia (07/10/07), S. Springell

Bond University professor and computer science researcher P. Krishnan has developed a secure software application that bypasses the problem of viruses completely for sensitive transactions such as online banking. Krishnan and his team at Bond's Software Assurance Center created a security system for home users tentatively called BOSS, or Bank on Secure System. The user places the BOSS CD into the PC and reboots the computer. Instead of the usual operating system loading, the BOSS system loads first. Once loaded, a browser opens with a graphical keyboard for extra security. Normal online banking can then be conducted. When the user is finish, the original operating system is restored by removing the CD and rebooting. Krishnan says the BOSS system works because viruses on a computer's hard drive are inactive when running the BOSS CD, and that banks and home users would not have to change their hardware or software. Krishnan's next step is to continue his research into a formal verification system for the software. "Verification is very hard because you need to mathematize the whole thing and the system is too big for that," Krishnan says. "But it is the only way to ensure that something works."