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

Δελτίο 81
4 Ιουλίου 2007

Cyber Security Report Released
Computing Research Association (06/28/07)

Cybersecurity is the focus of "Toward a Safer and More Secure Cyberspace," a new report from the National Research Council of the National Academy of Sciences. The report identifies three broad areas of concern about security, with the first being that a lack of security will enable enemies to launch a cyberattack, in conjunction with a physical attack, to cause an enormous loss of life and billions of dollars in other damages. Secondly, the reports draw attention to the potential for billions of dollars in losses due to fraud and extortion if businesses are unable to shore up their cyberspace systems and networks. Finally, the report warns that a lack of cybersecurity may curb the use of technology in the years to come and lead users to discount the positive impact that IT can have on national competitiveness, in addition to national and homeland security. The report also includes a potential Cyber Security Bill of Rights that offers a set of 10 provisions. The points include availability of system and network resources to legitimate users; easy and convenient recovery from successful attacks; and control over and knowledge of one's own computing environment.

Solving the Web Security Challenge
CNet (06/28/07), M. Ricciuti; J. Evers

The gatekeepers of much of the world's most sensitive information are a handful of major corporations, and this carries troubling implications for Web security, especially since in many instances these companies are adapting standard desktop security methods to new Web applications. The security of online information is complicated by the ever-growing volume of data as well as the upsurge in hacker attacks, and factors such as these are triggering calls for independent oversight. SPI Dynamics researcher Billy Hoffman says there is plenty of information on security practices available, but what is missing is "an intermediary that says how these things apply to you as you build Web 2.0 or other applications." Industry-wide cooperation is one strategy to consider, but such an approach has been tried with other digital technologies, only to come up short and often lead to monopolization. Hoffman attests that standard bodies such as the World Wide Web Consortium should concentrate on devising unambiguous standards that establish solid baselines. Microsoft's P. Boden classifies the majority of online security problems as input validation errors, and he thinks Microsoft has an advantage over rivals because it received a fast education on Web security thanks to its extensive software history and experiences with Trustworthy Computing, and thus was able to create tools to help developers address bugs and test code quality. Although Microsoft, Google, and Yahoo claim to have fortified servers against attacks, email worms, phishing assaults, and other intrusions are still common, which plays into the argument for more industry collaboration. Security specialists at the "Big Three" companies see a need for additional work at the most basic level of software development, beginning with an effort to teach security to future employees while they are still university students.

H-P's Emerging Task: Deter Forgeries

Wall Street Journal (06/28/07) P. B3; J. Range; V. Agarwal

A Hewlett-Packard research and development lab in India is researching a way to mark paper documents with a bar code to prevent forgeries. Forgery is a big problem in India and one of the most common types of fraud. The project, called "Trusted Hardcopy," does not use holograms or water-marked paper and is capable of working on ordinary office equipment, mainly a computer, a scanner, printer, and software. The bar code acts like a digital signature and is intended to bring network-level security to paper documents. The bar code is used to authenticate the document and contains the information on the page. By including the information on the page in the bar code, any unauthorized changes to the document would be recognizable because the bar code would be unaltered. HP believes that government agencies, public offices, and companies will all be interested Trusted Hardcopy for official documents. Trusted Hardcopy is only one of several innovations being developed by HP designed to appeal to customers in emerging markets, primarily China and India. Another product is HP's "TVPrintCast," which sends data over television networks. Computing over television networks is potentially an extremely lucrative market in India, as televisions are far more prevalent than computers. In 2005, India had 500 million TV viewers but only 6.5 million Internet users. TVPrintCast would allow users, for example, to view a cooking program and simultaneously print out a copy of the recipe.

Security Issues and Programming
ZDNet (06/25/07), P. Murphy

Blogger P. Murphy notes that it is a widely held belief that security is a function, rather than an application, of programming language. He makes the case that "C code compiled and run in a safe code environment is as safe as Java run in a virtual machine--and, by extension, a Java virtual machine is itself as vulnerable as any other C application." C's greater simplicity in comparison to Java should help shield C against attack, which dovetails with the concept of using virtualization to maintain the separation of user processes. "Thus you can think of the PC's BIOS, ring zero, kernel, and user modes as switchable virtual machines, note that this hardware design has determined a lot of the software evolution around it, and conclude that much of today's PC "security" problem is ultimately rooted in a mistake," Murphy explains. "A mistake, not because virtualization was the wrong answer, but because a better answer was known: The use of typing instead of address based authorizations." He concludes that it is erroneous to regard a language such as C as being more hazardous than Java, since it is the whole execution environment that matters in the final analysis. Most of the risk on Windows and Unix stems from hardware, and by extension compiler design, as opposed to language design.

Handwritten Passwords
Technology Review (06/28/07), E. Naone

A new online authentication system called Dynahand could eliminate the need to remember multiple and lengthy passwords. Dynahand verifies user identity by asking the user to identify their own handwriting. University of Glasgow computer scientist and Dynahand researcher K. Renaud says requiring users to remember passwords is ridiculous and places an unrealistic burden on people. Biometric authentication, using physical attributes such as fingerprints or retinal scans, has become an alternative to passwords, but requires additional hardware. Dynahand eliminates the need for extra hardware and passwords. Dynahand only requires users to submit a variety of handwriting samples. To log in, the user must identify his or her writing out of a series of samples. Multiple tests can be used depending on the desired

level of security. The handwriting samples contain only digits because numerals are harder for an outside party to recognize than letters, and digits are displayed at random, so the handwriting is the only clue. The system uses an algorithm to analyze characteristics such as line width of all handwriting samples to be sure samples are distinct and do not confuse legitimate users. Renaud says a handwriting recognition system is particularly appealing to older users, who can find it difficult to remember multiple passwords, and dyslexic people, who sometimes chose weaker, shorter passwords intentionally because they have trouble remembering longer passwords. Renaud does not believe that Dynahand is secure enough to protect sensitive information such as bank accounts or health records, but that it would be appropriate for social sites where the user wants a private account but no real harm would result from a break in.