Security loophole found in Windows operating system

November 12 2007

A group of researchers headed by Dr. Benny Pinkas from the Department of Computer Science at the University of Haifa succeeded in finding a security vulnerability in Microsoft's "Windows 2000" operating system.

The significance of the loophole: emails, passwords, credit card numbers, if they were typed into the computer, and actually all correspondence that emanated from a computer using "Windows 2000" is susceptible to tracking.

"This is not a theoretical discovery. Anyone who exploits this security loophole can definitely access this information on other computers," remarked Dr. Pinkas.

Various security vulnerabilities in different computer operating systems have been discovered over the years. Previous security breaches have enabled hackers to follow correspondence from a computer from the time of the breach onwards. This newly discovered loophole, exposed by a team of researchers which included, along with Dr. Pinkas, Hebrew University graduate students Zvi Gutterman and Leo Dorrendorf, enables hackers to access information that was sent from the computer prior to the security breach and even information that is no longer stored on the computer.

The researchers found the security loophole in the random number generator of Windows. This is a program which is, among other things, a

critical building block for file and email encryption, and for the SSL encryption protocol which is used by all Internet browsers. For example: in correspondence with a bank or any other website that requires typing in a password, or a credit card number, the random number generator creates a random encryption key, which is used to encrypt the communication so that only the relevant website can read the correspondence. The research team found a way to decipher how the random number generator works and thereby compute previous and future encryption keys used by the computer, and eavesdrop on private communication.

"There is no doubt that hacking into a computer using our method requires advanced planning. On the other hand, simpler security breaches also require planning, and I believe that there is room for concern at large companies, or for people who manage sensitive information using their computers, who should understand that the privacy of their data is at risk," explained Dr. Pinkas.

According to the researchers, who have already notified the Microsoft security response team about their discovery, although they only checked "Windows 2000" (which is currently the third most popular operating system in use) they assume that newer versions of "Windows", XP and Vista, use similar random number generators and may also be vulnerable.

Their conclusion is that Microsoft needs to improve the way it encodes information. They recommend that Microsoft publish the code of their random number generators as well as of other elements of the "Windows" security system to enable computer security experts outside Microsoft to evaluate their effectiveness.

Source: University of Haifa