Dreamlab cracks the code to Microsoft's wireless keyboards

December 4 2007, by Lisa Zyga

Microsoft Wireless Optical Desktop 1000

Anyone using a wireless keyboard might be a little concerned with a recent announcement by the Swiss company Dreamlab Technologies.

The IT security center claims that it has developed simple technology that can "sniff out" the keystrokes typed on Microsoft´s Wireless Optical Desktop 1000 and 2000 keyboards. At distances of up to 10 meters, Dreamlab´s technology can capture and decrypt keystrokes that may contain information such as user names, passwords, credit card numbers, and confidential messages. With appropriate technical equipment, Dreamlab predicts that eavesdropping at even larger distances is possible.

Companies like Microsoft and Logitech use the 27 MHz radio band for communication between wireless keyboards and a computer. As Max Moser of Dreamlab Technologies says, "Wireless communication is only as secure as the encryption technology used. Due to its nature, it can be tapped with little effort."

Because Microsoft´s encryption technology uses only about 256 possible encryption keys, it did not take many tries for Dreamlab´s software to decode the data. In this case, just a simple radio receiver, a soundcard, and suitable software were enough to break the cryptography codes and tap into the radio frequencies.

Dreamlab says it immediately alerted the manufacturer to the security loophole, but it will be a long process to fix the problem. In the meantime, Dreamlab hopes that consumers using wireless keyboards will take caution when using any wireless keyboard.

Because Microsoft´s other wireless devices operate on similar technology, Dreamlab warns that these devices might also be prone to attacks. Some of these devices include the Wireless Optical Desktop 3000, Wireless Optical Desktop 4000 and other products in the 27 Mhz-based Wireless Laser Desktop series.

Dreamlab has not released the specific tools and methods used to break the code, but researchers at Dreamlab have created a presentation about their work explaining the procedures used and the pitfalls encountered during the analysis. They plan to present their work at future events, mainly for educational purposes. The company hopes that this information will make researchers more aware of the interesting topic of analyzing unknown radio-based data transmission.

More information:

Dreamlab´s white paper: "We know what you typed last summer"

Dreamlab´s Video