

5 December 2007

By: Bogdan Botezatu, Hardware Editor



From Blue Screen of  
Death to Black Keycap  
of Death?  
The Web

## [The Dark Side of Hardware - Wireless Keyboard Keylogger](#)

### *Microsoft's wireless keyboard allows keystrokes interception*

A Swiss vulnerability testing laboratory, Dreamlab Technologies, developed a method of intercepting the keystrokes coming from a wireless Microsoft keyboard. Microsoft's product is using the 27 MHz radio spectrum for computer communication, and the Microsoft Wireless Optical Desktop 1000/2000 keyboard is no exception to the rule. The ethical hacking team has analyzed the 1000/2000 keyboard model and found that the wireless signal could be easily intercepted by a common radio receiver anywhere in a 10 meter range. They have practically built a wireless hardware keylogger out of a radio receiver, a soundcard and some software programs. In order to prevent signal interference or even non-legitimate access, the signal is encrypted, but the security company said that the encryption algorithm is so weak that it is merely useless. "Dreamlab Technologies successfully cracked the encryption key used in Microsoft's Wireless Optical Desktop 1000/2000 keyboards", said the company officials. "As most products in Microsoft's Wireless Desktop range are based on the same technology, Dreamlab does not consider them to be secure either." Given the fact that the signal can only travel a short, 10-meter range, can give the user a fake sensation of security, but in reality, the signal can be picked up in a much wider area if using special aerial antennas. The company refused to give any additional details regarding the methods they used for defeating the encryption protection, since encryption levels usually take a long time before changing. Moreover, it is in the ethical hacking division's policy not to reveal such 'juicy' details before a fix has been issued. Although the Swiss center has tested only Microsoft products up until now, they expect a wide range of keyboards from other manufacturers to be affected by weak encryption schemes. The company has already notified the producers about these functional issues and a fix is expected soon. The company has posted a video to show the wireless keylogger modus operandi. The video is available [here](#).