

Press release

Berne, 30 November 2007

World first: Dreamlab Technologies Switzerland cracks wireless keyboard encryption

Wireless keyboards and mice are becoming an increasingly common sight on desks. However, wireless hardware carries large hidden risks. Swiss IT security company Dreamlab Technologies AG has shown that it is possible to capture and decrypt keystrokes, meaning that user names, passwords, bank details or confidential correspondence can be very easily eavesdropped.

Although the trend in wireless communication in peripheral devices such as keyboards and mice is moving towards Bluetooth, market leaders such as Logitech and Microsoft rely on cost-efficient, tried-and-tested 27 MHz radio technology. Using just a simple radio receiver, a soundcard and suitable software, Dreamlab Technologies has managed to tap and decode the radio frequencies transmitted between the keyboard and PC/notebook computer. Although manufacturers of wireless keyboards partially prevent data from being tapped by using cryptography, unfortunately the encryption is weak and thus does not offer real protection. Max Moser from Dreamlab Technologies states: "Wireless communication is only as secure as the encryption technology used. Due to its nature, it can be tapped with little effort."

Dreamlab Technologies tested and successfully cracked the encryption key used within Microsoft Wireless Optical Desktop 1000/2000 keyboards. As most products in Microsoft's Wireless Desktop range are based on the same technology, Dreamlab Technologies does not consider them to be secure either. During the test, Max Moser and Philipp Schrödel of Dreamlab Technologies succeeded in eavesdropping traffic from a distance of up to ten meters using a simple radio receiver. With the appropriate technical equipment, larger distances are possible.

As an IT security competence centre, Dreamlab Technologies recognises the importance of responsible vulnerability disclosure. The manufacturer affected was informed immediately of the security loophole. Closing this loophole will be a drawn-out and difficult process for the manufacturer, and for this reason, Dreamlab Technologies is currently refraining from publishing details of the tool developed for the attack or precise details of how it was performed. Nicolas Mayencourt, CEO of Dreamlab Technologies, comments: "In order to achieve real security, uncertainties must be located and dealt with. Dealing with security loopholes in an ethical way means correctly informing the public and the manufacturer. The manufacturer must be given the opportunity to improve their product, while consumers are offered the chance to improve their security level. Only in this way can real security be achieved."

Dreamlab Technologies is an IT security specialist and an international company with offices in Switzerland, Germany and France. Since 1997, Dreamlab Technologies has been carrying out high-end security tests, providing consulting and training seminars, and implementing solutions based on best-in-class open standard technologies. Dreamlab Technologies is represented on the Board of Directors of ISECOM.org, and works according to the OSSTMM manual, the most widespread methodology used for comprehensive security audits.

Dreamlab Technologies maintains strategic partnerships with the most renowned international open source projects, leading technical universities and pioneering standardisation institutes (W3C). Dreamlab Technologies' aim is to enable its customers and partners to directly benefit from this wealth of experience.

For more information and a video demonstration of the attack, visit <http://dreamlab.net>

Contact for general queries	Nicolas Mayencourt, CEO Dreamlab Technologies AG CH -3011 Berne Switzerland	+41 31 398 66 66 nicolas.mayencourt@dreamlab.net http://dreamlab.net
Contact for technical queries	Max Moser, Senior Security Spezialist Dreamlab Technologies AG CH -3011 Berne Switzerland	41 31 398 66 66 max.moser@dreamlab.net http://dreamlab.net