Media release

Berne, June 16th 2009

“Keykeriki” – Dreamlab Technologies and remote-exploit.org develop the first open 27Mhz wireless keyboard sniffer. It sniffs and records the signal of wireless keyboards and demonstrates their security risk level. And it can be used to demonstrate hacking-attacks for educational purpose.

Wireless keyboards are very popular in many offices and private homes. Even in the front office section of banks, they are frequently used. But they represent a big security risk – as dreamlab technologies already pointed out in a white paper published 2007. Wireless keyboards are risky, because they transmit a radio signal that is not enough protected. The newly developed portable universal receiver sniffs and records the signal of wireless keyboards and demonstrates their security risk level. The keykeriki-software and construction plans for -hardware are freely available online [www.remote-exploit.org].

Hardware

The hardware needs to be portable and small and to be able to adapt to future needs. Keykeriki is therefore built around a Texas Instruments TRF7900 chip controlled by an ATMEL ATMEGA microcontroller. For logging abilities an SDCard-interface is built into the board layout, as well as an additional USART channel for future hardware extensions (“backpacks”). The whole board can be powered directly via the USB-bus or a stable 5V-power source. When connected to a computer’s USB-port, one can use either a decent terminal application or the keykeriCTL software which is included in the software package of this project. All the schematics can be downloaded in eagle- and PDF-format as part of the project’s software package. Fully equipped boards will be provided in the near future.

Software

Because of the flexible hardware design, most features can be built in by software. This first release contains (among other features) radio frequency switching, signal strength display, deciphering of encryptions, sniffing and decoding of keystrokes of Microsoft 27Mhz based keyboards.

Extensions

Hardware extensions are easy to realize because two different interfaces, a second USART, I²C/TWI and SPI, are externalized. Therefore so called Backpacks e. g. an LCD display controller can be connected using the USART Interface.

The Future

Future extensions include amplification for antennas, support of other Microsoft keyboards and products of other producers, the constant amelioration of hard- and software and the parallel handling of several keyboards. Furthermore, a keykeriki able to send mouse- and keyboard-signals is intended.

Technical details can be found online: www.remote-exploit.org.

Dreamlab Technologies AG is an internationally operating company specialized in IT-Security. Established in 1997, Dreamlab Technologies performs high-end security test, consulting and education, and realizes solutions based on “best-in-class” open standard technologies. Dreamlab Technologies is an official education partner and representative of ISECOM (Institute for Security and Open Methodologies) for France, Germany and Switzerland. ISECOM is the editor of OSSTMM, today’s most popular security audit methodology.

Contact for general information	Rahel Schwab Dreamlab Technologies AG CH –3011 Berne Switzerland	+41 31 398 66 66 rahel.schwab@dreamlab.net http://dreamlab.net
Contact for technical details	Max Moser, senior security expert Thorsten Schröder, senior security expert Dreamlab Technologies AG CH –3011 Berne Switzerland	+41 31 398 66 66 max.moser@dreamlab.net thorsten.schroeder@dreamlab.net http://dreamlab.net