

21 October 2008

By: Lucian Constantin, Web News Editor



Keystrokes can be decoded from keyboard electromagnetic radiations  
Associated Content, Inc.

## [Keystrokes Can Be Sniffed Without the PC Being Compromised](#)

*By picking up the electromagnetic radiations wired keyboards emit*

Two Swiss researchers have demonstrated, in James Bond-like experiments, that sniffing the keystrokes from a wired keyboard is possible by capturing the electromagnetic radiations that are emitted when the keys are pressed. The researchers devised four methods of attack, one of which successfully decodes the pressed keys from a distance up to 20 meters, through an office wall, with a rather simple wireless antenna.

The knowledge that computer systems generate compromising emanations or Tempest radiation is dated back to the 1960s, the military organizations being the first to run tests with it. However, it was believed that modern wired keyboards had been constructed in order to overcome this problem. Martin Vuagnoux and Sylvain Pasini, two researchers from the Security and Cryptography Laboratory at Ecole Polytechnique Federale de Lausanne in Switzerland, set out to prove that many keyboards sold today are still vulnerable to this type of attacks.

One of their attack techniques has been based on a previous more generic [research](#) by Markus G. Kuhn and Ross J. Anderson, from the Computer Laboratory at the University of Cambridge. This technique is already known in the security industry as the Kuhn attack. The two Swiss researchers have used in their test 11 different wired keyboards, USB and PS2, external and embedded in laptops, which were bought after 2001. All of the tested keyboards have been found vulnerable to at least one of the four attacks.

The first test involved a very basic antenna constructed from a one-meter long wire and situated close to the keyboard. The keyboard was powered with the help of a laptop running on battery. The AC power source of the laptop has been disconnected and its screen closed in order to prevent any interference. The words "trust no one" have been typed on the keyboard and successfully displayed on another monitor after decoding and filtering the captured electromagnetic emanations from the keyboard.

The second experiment used a more powerful wireless antenna situated in the next room, around 20 meters away and the same keyboard setup. The same precautions have been taken to avoid interference from other sources like LCD monitors. The word "password" has been typed on the keyboard and successfully sniffed and displayed on a monitor in the room with the antenna.

Even though a real-life application would be different than this controlled experiment where interference from other sources was eliminated, the researchers claim it can be done with more sophisticated and expensive equipment. "We generally use a receiver tuned on a specific frequency. However, this method may not be optimal: the signal does not contain the maximal entropy since a significant amount of information is lost," wrote Vuagnoux and Pasini on a [website](#) they specifically set up to present their experiments. "No doubt that our attacks can be significantly improved, since we used relatively inexpensive equipments," they add.

The researchers released two video recordings of the experiments and announced that more details would be disclosed in a research paper that would be published soon.

Compromising Electromagnetic Emanations of Keyboards Experiment 1/2

Compromising Electromagnetic Emanations of Keyboards Experiment 2/2