Computer Keyboard Hacking

October 22 2008, by John Messina

(PhysOrg.com) -- Swiss researchers from the Security and Cryptography Laboratory have demonstrated different ways of eavesdropping on wired keyboards from at least 11 different models. The keyboards range from the latest ones to the ones used in 2001. Test show that all these keyboards were vulnerable to at least four of their attacks.

The researchers found that most modern keyboards generate electromagnetic emanations that can be used to decipher the keystrokes remotely. They used some basic instruments to "sniff" these electromagnetic emissions, which eventually helped them to decipher the keystrokes typed.

By using a wireless aerial, keystrokes were sniffed from a computer located a meter away. Once the data is sniffed, it is converted into decipherable text with software developed by Vuagnoux.

Another test revealed that keystrokes, from a computer in an adjacent room 20 to 30 feet away, could be deciphered by using a larger antenna.

It has been conclude that wired computer keyboards, sold in stores, generate compromising emanations that make it not safe to transmit sensitive information.

Electromagnetic eavesdropping dates back to as early as the mid 1980s, if not earlier. But Researchers say many of today´s keyboards have been adapted to prevent those attacks from working. Current research now shows that even these keyboards are vulnerable to electromagnetic sniffing.

It can be seen that such attacks would be limited due to electromagnetic interference from other electrical devices. The other thing that makes the attack unfeasible is the amount of sophisticated equipment required. Given all the fuss and expense, why not just use a more conventional method.

Compromising Electromagnetic Emanations of Keyboards Experiment 1/2

Compromising Electromagnetic Emanations of Keyboards Experiment 2/2

Related links:
lasecwww.epfl.ch/keyboard/
www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf