

## RE: Wireless Keyboard Security

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-03/0389.html>

---

**From:** Beauford, Jason (*jbeauford\_at\_EightInOnePet.com*)

**Date:** 03/23/05

Date: Wed, 23 Mar 2005 09:08:50 -0500

To: "Badger, Jared" <Jared.Badger@acs-inc.com>, <security-basics@securityfocus.com>

Firstly, Eve needs to get a life.

Although the scenario is certainly plausible, the range must quite close (I believe) in order to capture those radio waves, something like 6' maybe. I would tend to think it's a lot easier to purchase a hardware keystroke logger and drop it on the back of Alice's PC where it would not be noticed as opposed to coming in with a laptop with some big dish antennae on it.

Plausible – certainly, easy to pull off without getting caught – not so easy.

Required expertise – I have no idea.

jmb

-----Original Message-----

From: Badger, Jared [mailto:Jared.Badger@acs-inc.com]

Sent: Tuesday, March 22, 2005 6:13 PM

To: security-basics@securityfocus.com

Subject: Wireless Keyboard Security

Hello All,

I was wondering if anybody out there has researched security of wireless keyboards. Although I'm sure many people have very interesting opinions, what I need is solid technical information.

SCENARIO:

A sneaky eavesdropper, Eve, would like to find out some gossip on her neighbor, Alice. Eve knows that Alice uses Yahoo for her email, and would just love to be able to log in to Alice's Yahoo mail account. But she doesn't know Alice's password. But luck, it seems, may be in Eve's corner, as Alice has recently installed a snazzy new wireless keyboard/mouse combo on her home computer. Eve, using her formidable knowledge of radio and electronics, sets up an antenna to pick up

## SecurityFocus BASICS: RE: Wireless Keyboard Security

keyboard transmissions from Alice's house. After some persistence, Eve's laptop records a username, alice@yahoo.com and a password, "opensesame". Eve, ecstatic, logs on to Yahoo with the captured password and reads Alice's email, discovering lots of juicy secrets.

Although this Alice/Eve scenario is fictional, it seems plausible. For a true story, see:

<http://www.pcworld.com/howto/article/0,aid,108712,00.asp>

My job involves reviewing computer security at a bank, and I was very surprised to see that nearly all of the computers at one of my branches are using these wireless mouse/keyboard combos. It seems like this could be a potentially serious security risk, so I would like to do some research on this topic. If these manufacturers have incorporated strong security measures, then I would like to know what they are. Or if not, then it would be better to know than not to know so as to take appropriate precautions. (see the above PCWorld story. Note that only 4000 combinations are used, trivial for a computer to crack) Of particular interest to me are:

1. How possible/easy/difficult is it to eavesdrop and capture keystrokes from a wireless keyboard using passive means only? What equipment/expertise does this require? (I am thinking it would probably take at least a spectrum analyzer, receiver, a laptop, and some custom software) What about taking the keyboard apart and reverse engineering it?
2. How easy/difficult would it be to take control of a computer without having physical access to the keyboard at the console? What equipment/expertise would this require? (Probably at least the same as above, plus a transmitter)

One example of a wireless keyboard/mouse combo is displayed here:

<http://www.microsoft.com/hardware/mouseandkeyboard/productdetails.aspx?id=0>  
14

By entering the following FCC ID's into the FCC website, you can get quite a bit of interesting information.

FCC ID's: C3KKB9 (keyboard), C3K1008 (mouse)

<https://gullfoss2.fcc.gov/prod/oet/cf/eas/reports/GenericSearch.cfm>

There are many docs, including photos and lab tests, on the associated pages. For example, FCC docs show that this particular keyboard transmits on a frequency of 27.095 – 27.195 MHz. From the internal photos, it doesn't seem there are enough electronics to perform advanced encryption.

## SecurityFocus BASICS: RE: Wireless Keyboard Security

Certainly somebody knows how to do this. Has anybody tried? Been successful? Failed? Any information on common manufacturers (Logitech, Microsoft, Kensington, etc.), commonly used encryption/decryption, frequencies, encoding, signal power and range, etc. would be most appreciated.

Thanks in advance,

Jared Badger, CISSP