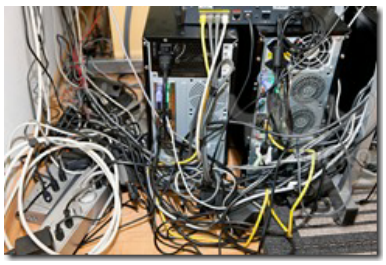
Security Sidebar: Hacking Wireless Keyboards

John Wagnon, 2015-26-01



Remember the good old days when 500 clunky wires, plugs, etc were absolutely critical in order to set up and configure a simple workspace? Yeah, me too. Now, most of our peripheral devices are wireless, and rightfully so. However, we have to remember that our wireless devices obviously communicate with the mothership computer in some way. Most wireless mice, keyboards, and other peripheral devices use the 2.4 GHz band as the preferred frequency range for communication, although some use the 27 MHz band. Either way, Radio Frequency (RF) waves are flowing freely between your wireless device and your computer as you type away on that keyboard.

This is great and all, but it begs the question on the security of said RF waves…do you have any idea if the data flowing from your wireless device is secure or not? I would venture a guess that most people have no idea. They just go to their local electronics store (or favorite website), find the coolest looking wireless mouse/keyboard combination they can find, buy it, plug it in, and celebrate the fact that they don't have to concern themselves with those pesky wires anymore.

Well, a guy Samy Kamkar recently reminded us all that we should, in fact, be concerned about the transmissions between our wireless devices and our computers. Samy released a cool new device that looks like a USB wall charger (in fact, it *is* a functioning USB charger), but it's super-secret purpose is a keystroke logger that records all the keystrokes of a nearby wireless keyboard. This device, known as "KeySweeper", connects to Microsoft wireless keyboards and passively sniffs, decrypts, and records all the keystrokes and sends them back to an operator over the Internet via an integrated SIM card. There's also a really cool web based backend that uses jQuery and PHP to log all keystrokes and provide a web interface for live monitoring of the keystrokes. What's more, the KeySweeper continues to operate even when unplugged because it's equipped with an internal battery that powers the device when it's not connected to AC power. Then, when it's plugged back in, the battery automatically recharges. Here's a picture of the harmless looking device:

Think of all the people who would love to have this "charger" as a nice office gift for their USB-connected devices!

This specific device works against Microsoft wireless keyboards by using some really creative sniffing tools and techniques. Typically a sniffer needs to know the frequency and the MAC address to do its thing. Well, most (if not all) wireless Microsoft keyboards use the 2.4 GHz channel, and their MAC address conveniently always begins with 0xCD. This significantly helps in creating a passive sniffer that listens to the sweet sounds of wireless Microsoft keystrokes.

The other critical hurdle to overcome in sniffing these wireless transmissions is the issue of encryption. Contrary to popular belief, Microsoft does actually encrypt the wireless transmissions from keyboard to computer. However, the encryption algorithm is suspect at best. In their research on wireless sniffing, Thorsten Schroder and Max Moser found that the keystrokes are encrypted by using a simple XOR with the MAC address.

Samy Kamkar took this information and found that he could decrypt the keystrokes even without knowing the MAC address at all! Further, he discovered that he could alter the keystrokes as they passed from the keyboard to the computer (he promises more information on this in the future).

Here's a quick diagram of the "USB charger" as it sits in close proximity to a wireless keyboard:

The power of the transmission signal on most wireless keyboards is about 30 feet. So, as long as the KeySweeper is in that range, it should work as advertised. While this particular device works against Microsoft keyboards, rest assured that other devices could be built to work against other keyboard manufacturers as well (Logitech, etc).

It's a crazy wireless world out there…so be careful the next time someone randomly offers you a "free USB charger that would be perfect for your office." You might want to crack that thing open and make sure it's not full of microcontrollers, flash chips, and SIM cards…

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com