

Other Wireless: New Ways to be Pwned

Luis Miras © 2007

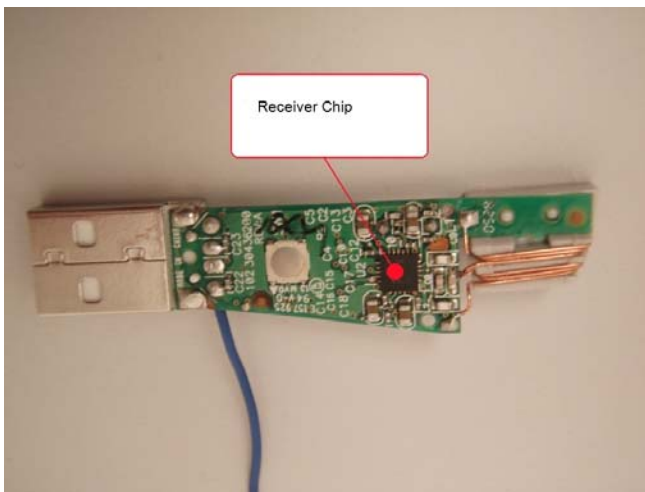
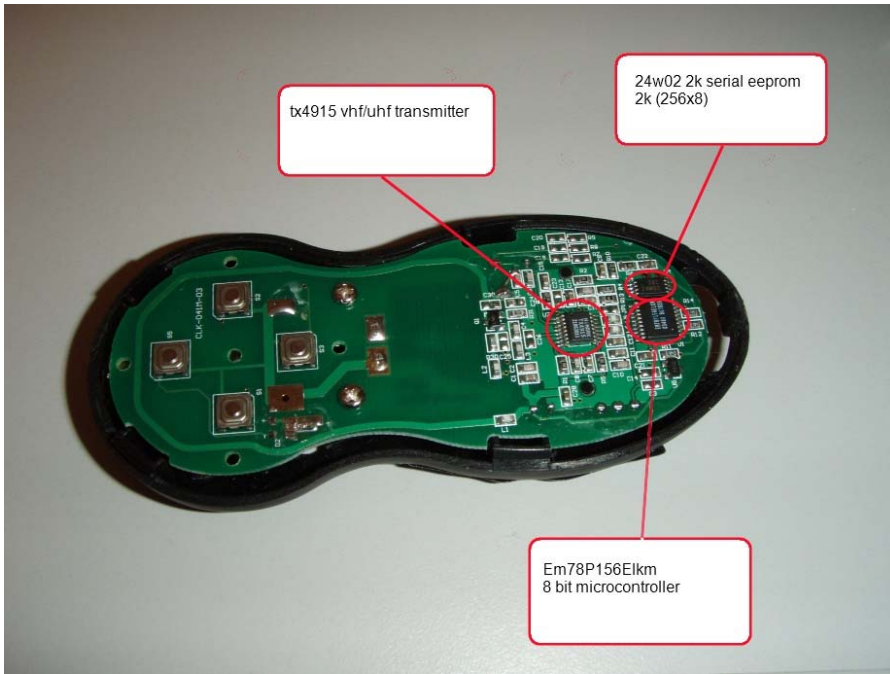
There have been numerous papers and attacks done on mainstream wireless technologies. These technologies would include 802.11, Bluetooth, and Cellular.

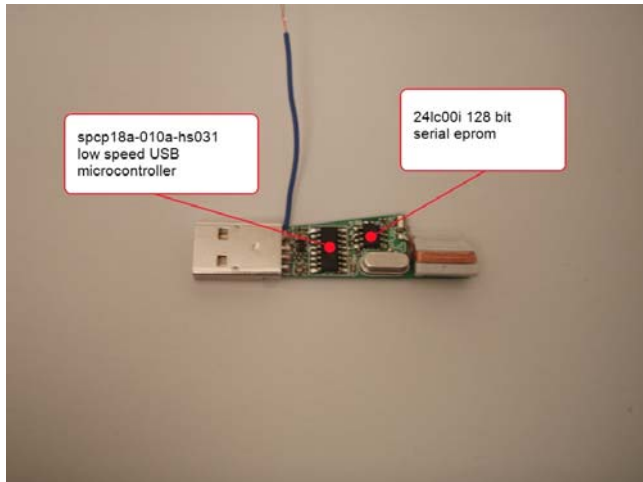
There are many RF devices that don't operate using the above protocols and standards. These devices are built using cheaper more cost effective chips. Many of the chips can only perform one way communication.

These devices include wireless RF presenters, mice, and keyboards. They operate on various bands such as 27 MHz, 900 MHz, and 2.4 GHz.

Device Internals

The devices are made up of two primary components, a transmitter and a receiver. The transmitter is the presenter, mouse, or keyboard. The receiver is usually a USB dongle.





Most of the devices consist of the same building blocks. The transmitter will contain a microcontroller, an eeprom, a transmitter chip, and some input.

The input can be buttons or the movements of a mouse. This data is fed into the microcontroller.

The eeprom holds the identification number for the device pair. A transmitter and receiver will usually have matching numbers burned in at the factory. This number is used to authenticate the transmitter.

The microcontroller runs the show. It receives the input data and reads the identification number. The data is processed and packaged into a protocol which is sent to the transmitter chip.

The transmitter chip doesn't usually contain logic. It is designed to transmit whatever is at the input.

The receiver will contain a microcontroller with built in USB functionality, an eeprom chip, and a receiver chip.

The receiver chip converts the RF data into a bit stream feeding into the microcontroller. This would be similar to data on shared Ethernet.

The microcontroller uses the identification number from the eeprom to determine if it should process the message. If it is addressed to the

receiver the data is processed and dispatched through USB to the computer.

HID

Human Interface Design (HID) is a method of communication between peripherals and computers. While HID is primarily used for USB devices, it can be used over different formats such as IR.

Attacks: passive and active.

Passive attacks will capture any data transmitted from the device to its corresponding dongle. This data can take various forms consisting of varying fields. The following is a breakdown of what we may expect for certain types of devices:

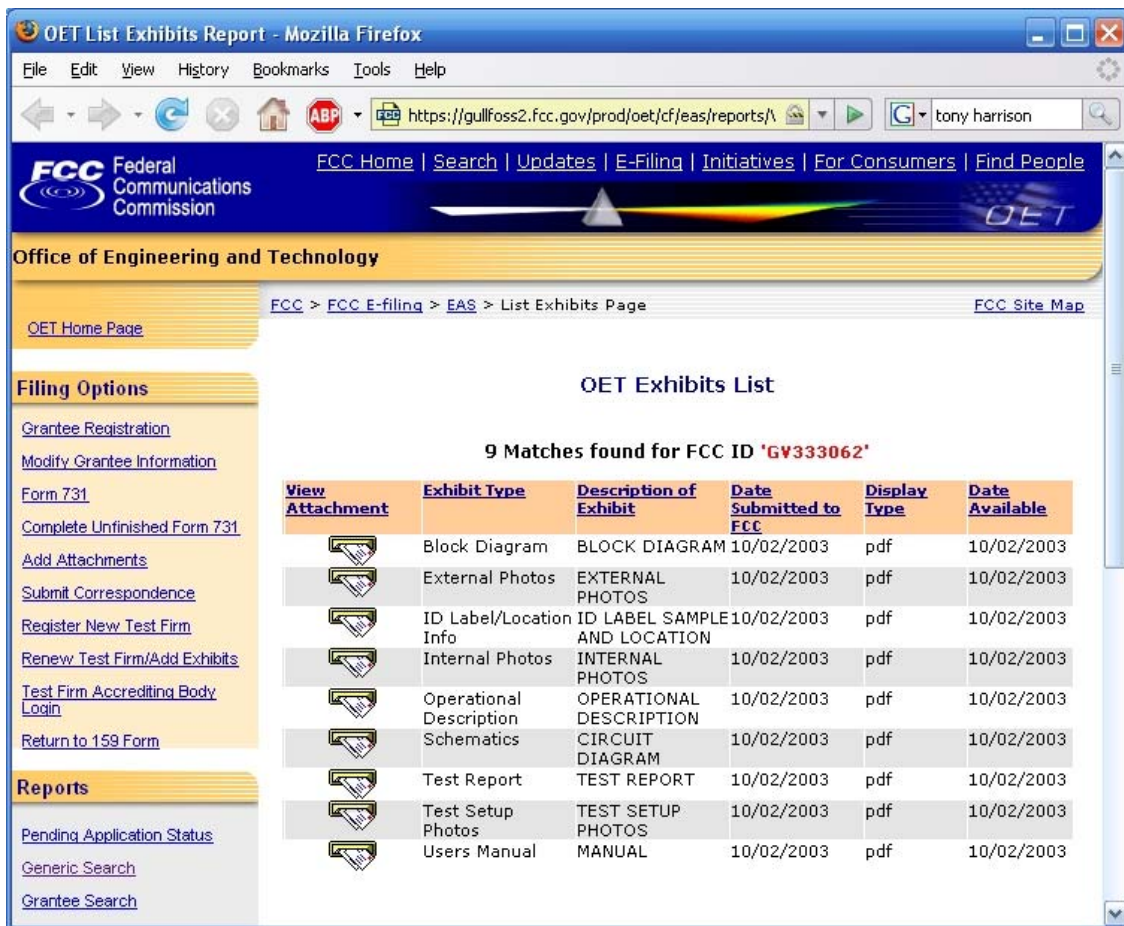
Wireless RF presenter - These devices usually register themselves as a HID keyboard. Although registered as a keyboard, this doesn't necessarily mean that all key codes can be sent from the transmitter to the dongle. Presenters usually have a very limited set of functionality. The forward and rewind slide functions are actually HID codes for 'page down' and 'page up'. These codes are generated by the dongle. In order to conserve power engineers the amount of data transmitted is kept to a minimum. Thus full key codes are not transmitted but rather a proprietary protocol is designed. Passive attacks would identify the ID of the device and what buttons were pressed. The button data isn't useful as it is just movement between slides. The ID number comes into play during active attacks.

Mice – These devices are registered as a HID mouse. The HID spec allows for relative and absolute movements, as well as buttons. Absolute movement would be used for a drawing pad or similar device. Passive attacks would identify the ID of the device as well as movement and buttons. The movement and button data is not very useful. Some have suggested that mouse movement and clicks could identify passwords that are clicked on the screen.

Keyboards – These devices register themselves as a HID keyboard. The keys are encoded into a proprietary protocol and the dongle converts them to HID codes. Passive attacks would allow the sniffing of possibly valuable data. This data could contain passwords.

Device Research

RF devices sold in the US need to be certified by the FCC. The FCC regulates RF traffic. The application includes internal and external photographs, label format and location, test report, users manual, schematics, block diagrams, and any other documentation. There is an option to claim confidentiality on some of the items above. The schematic, block diagrams and other design documentation are common items granted confidentiality. The application and supporting documentation are freely available to consumers. Confidential items are not available.



The screenshot displays the FCC Office of Engineering and Technology (OET) website. The browser window title is "OET List Exhibits Report - Mozilla Firefox". The address bar shows the URL "https://gulfoss2.fcc.gov/prod/oet/cf/eas/reports/". The page header includes the FCC logo and navigation links. The main content area is titled "OET Exhibits List" and shows "9 Matches found for FCC ID 'GV333062'". A table lists the exhibits with columns for View Attachment, Exhibit Type, Description of Exhibit, Date Submitted to FCC, Display Type, and Date Available.

View Attachment	Exhibit Type	Description of Exhibit	Date Submitted to FCC	Display Type	Date Available
	Block Diagram	BLOCK DIAGRAM	10/02/2003	pdf	10/02/2003
	External Photos	EXTERNAL PHOTOS	10/02/2003	pdf	10/02/2003
	ID Label/Location Info	ID LABEL SAMPLE AND LOCATION	10/02/2003	pdf	10/02/2003
	Internal Photos	INTERNAL PHOTOS	10/02/2003	pdf	10/02/2003
	Operational Description	OPERATIONAL DESCRIPTION	10/02/2003	pdf	10/02/2003
	Schematics	CIRCUIT DIAGRAM	10/02/2003	pdf	10/02/2003
	Test Report	TEST REPORT	10/02/2003	pdf	10/02/2003
	Test Setup Photos	TEST SETUP PHOTOS	10/02/2003	pdf	10/02/2003
	Users Manual	MANUAL	10/02/2003	pdf	10/02/2003

Implementing Attacks at the Chip Level

Data comes in from the RX chip and is decoded by the microcontroller if properly addressed. Thus this connection between the RX chip and the MCU needs to be severed and another MCU can be used to decode all data and hand it off to a computer. The computer can then extract the identification number (authentication data) and use it for active attacks.

Although it is tempting to use the current microcontroller and reprogram, it is usually not feasible. In order to save costs the chips are usually OTP (one time programmable).

On the transmitter side, the connection between the MCU and TX chip is severed. A separate MCU is connected directly to the TX chip. The MCU would prepare the data with a proper identification number and send it to the TX chip. The MCU can be receiving commands and identification numbers from a computer.

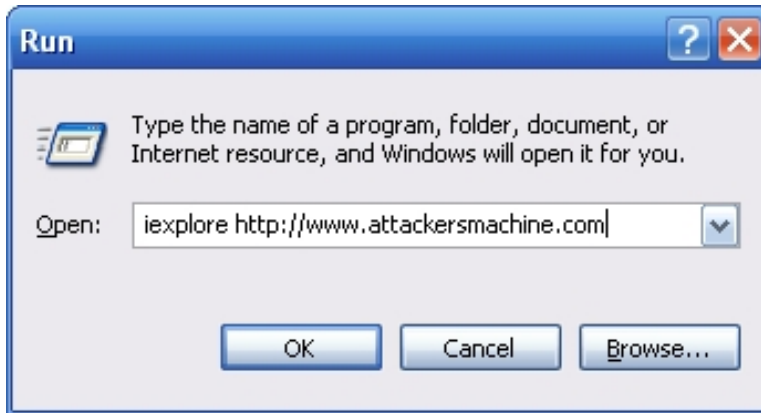
The above setups convert the RF circuitry into something like a network socket. Data is pushed on one side and arrives at the other side. No knowledge of RF is needed since OEM hardware is being used.

Implementing attacks against a target machine

Passive attacks have been discussed and unless the device is a keyboard, they are limited in effectiveness.

Active attacks fall under two categories: bind and non-blind. The attacks also differ based on the type of device being attacked.

The goal is running commands on the target system, whether using mice or keyboards. The run dialog box is a good location to insert commands. For a keyboard this consists of sending the windows and 'r' key combination.



A mouse is more difficult. A method of typing is available through Microsoft accessibility features. There is an on screen keyboard. Mice clicks function as keyboard presses.



The difference between blind and non-blind attacks only really matters with mice. The items being clicked on are not necessarily in the same location on every machine. If the mice can only send relative locations, mouse sensitivity comes into play.

A method to get some feedback is attempting to have Internet Explorer (or any browser) connect to an attacker controlled web server hosting a Trojan. Logs can be checked for downloads. If the target machine has not connected adjust the movement algorithm and try again.