|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| IOT REDBOOK  Hardware Requirement |
| |  |  |  | | --- | --- | --- | | Navneet Mishra, Jacob Victor |  |  | |

**Table of Contents**

[Bus Pirate 1](#_Toc174104)

[JTAGulator 1](#_Toc174105)

[ChipWhisperer 2](#_Toc174106)

[Hack RF One 2](#_Toc174107)

[Ubertooth One 3](#_Toc174108)

[Killerbee 3](#_Toc174109)

[Attify Badge 4](#_Toc174110)

[Break Away Headers 4](#_Toc174111)

[Jumper Wires 4](#_Toc174112)

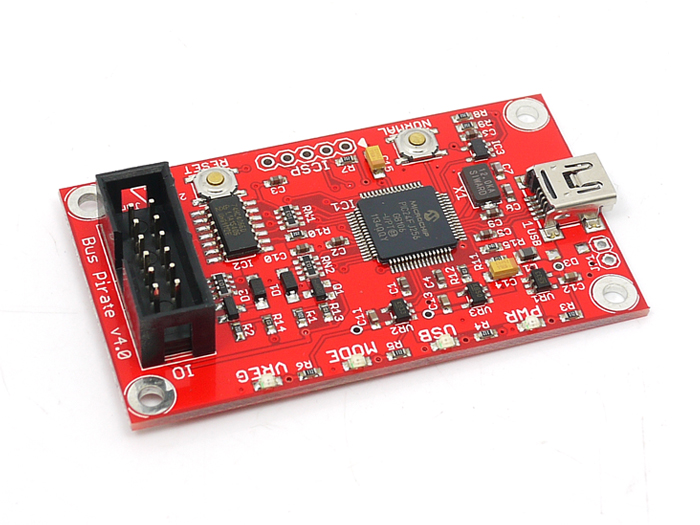
[Multimeter 5](#_Toc174113)

[Price Estimate 5](#_Toc174114)

# Bus Pirate

It supports most of the most commonly used protocols like UART, SPI, JTAG/SWD and a whole lot of more protocols. Connect to a router’s UART and you get the shell access. You can use it to dump both SPI and I2C Memory. You can initialize JTAG/SWD interface for controllers and processors which could be used to dump the firmware and debug the code to find exploits.

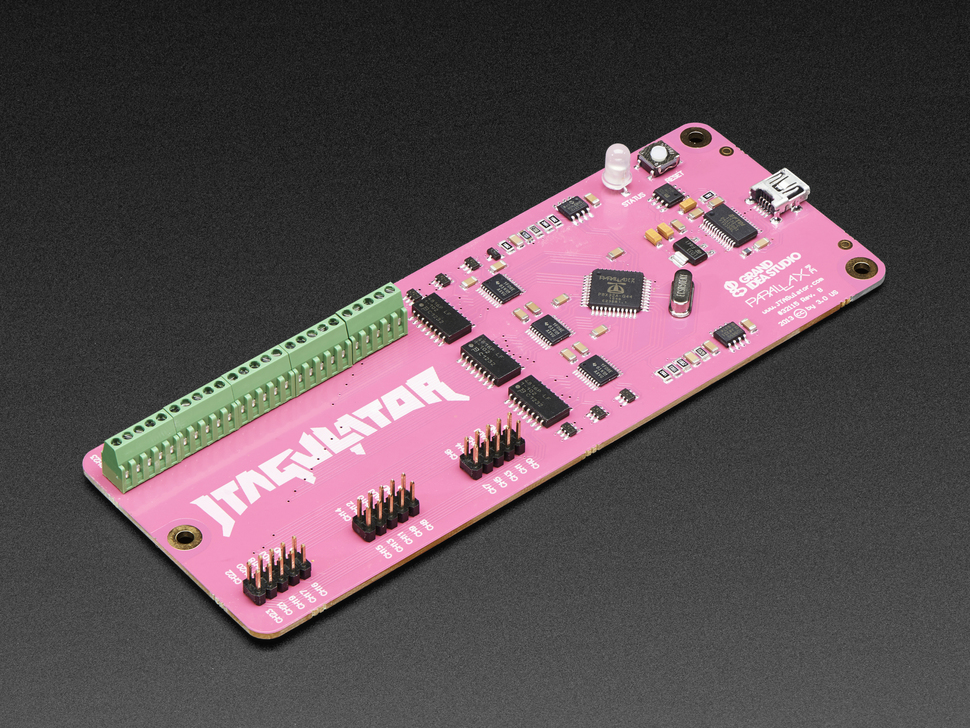
You can also sniff communication like I2C and SPI and see how the device is communicating with the sensor or EEPROM and reverse engineer it to exploit the system. It can also act as a logic analyzer and PWM generator.



# JTAGulator

Now we have a target device and bus pirate to access the device. The next question is where do I connect? You can trace the pcb tracks and find it. But in case of complex devices, the number of layers and via are more and it is complicated to identify the JTAG pins unless you chemical etch the board or X-Ray the board which is an expensive affair.

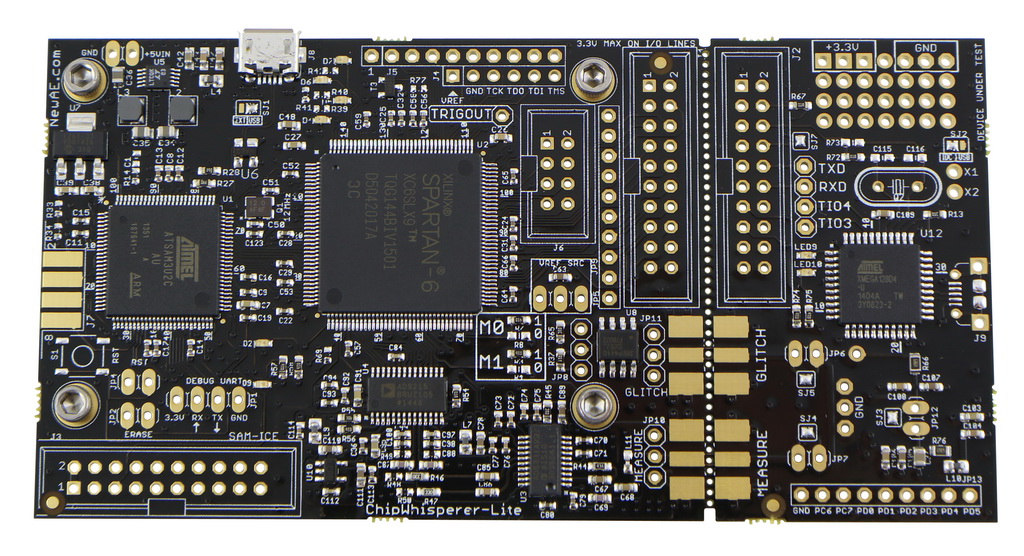
Joe Grand has created a hardware which had around 24 GPIOs which could be connected to the unknown pins and pads of the board and the device will automatically scan for the JTAG pins and returns the JTAG pinouts of the target board. This is very handy when your target board is complicated and uses an unmarked processor/controller. JTAGulator can also do UART scanning and baud rate identification.



# ChipWhisperer

This is an amazing tool built by Colin O’Flynn and it is used for advanced penetration testing that involves hardware side channel analysis and voltage/clock glitching attack to gain access to the target device, find encryption keys and various attack vectors. The software toolchain is user-friendly which allows the user to perform an attack on the hardware in a simple manner without the need to understand the core logic of programming the FPGA or the ADC acquisition.

It also comes with a standard target board which could be used to experiment with side-channel analysis and glitching attacks. This device is powerful enough to glitch a full-fledged Android phone too. There is large set of [documentation](https://wiki.newae.com/Category:Examples) regarding the usage. It is the best starter tool if you’re into IoT testing and wants to exploit it further deep.



# Hack RF One

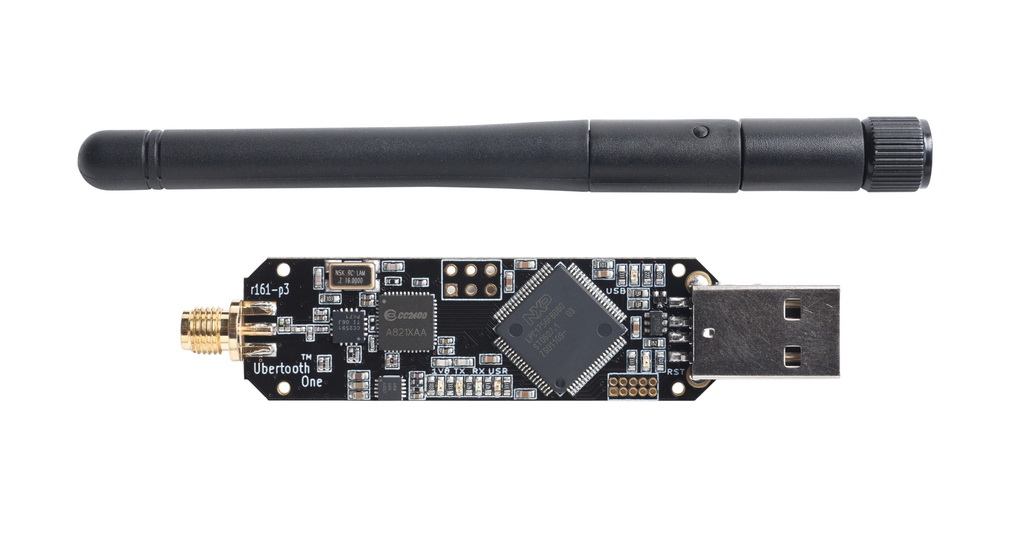
Majority of the IoT devices have some sort of wireless communication, be it a typical RF or a Zigbee or a LoRa. If you want to test the wireless security, HackRF is the tool for the job. HackRF is an advanced software defined radio with the range of 1MHz to 6GHz. Unlike your RTL SDR, Hackrf can transmit and receive radio waves but it is half-duplex, which makes it easy to perform air-borne attacks like replay attacks, fuzzing, and jamming. It can sniff wide range of wireless protocols from GSM to Z-wave. With the help of GNURadio toolset, you can build your own wireless protocol and test it against a target device.



# Ubertooth One

Most of your smart device comes with Bluetooth ranging from a smartwatch to a smart buttplug. Now it is absolutely necessary to penetration test this wireless protocol. Ubertooth is a Bluetooth ISM sniffer which is used to sniff all the communication that is happening in the L2CAP layer of your Bluetooth communication.

Unlike HackRF, Ubertooth takes cares of the channel hopping and capture all the packets and saves it in a Wireshark file. Mike Ryan has created a script around it, which can find the Bluetooth keys and is also transmitted through the air which is used to encrypt the communication, can be recovered and the communication can be reverse engineered for sensitive information. Once a Bluetooth communication has been reverse engineered using Ubertooth it could be used to exploit the device further.

[](https://payatu.com/wp-content/uploads/2017/11/ubertooth-one-052-1024.jpg)

# Killerbee

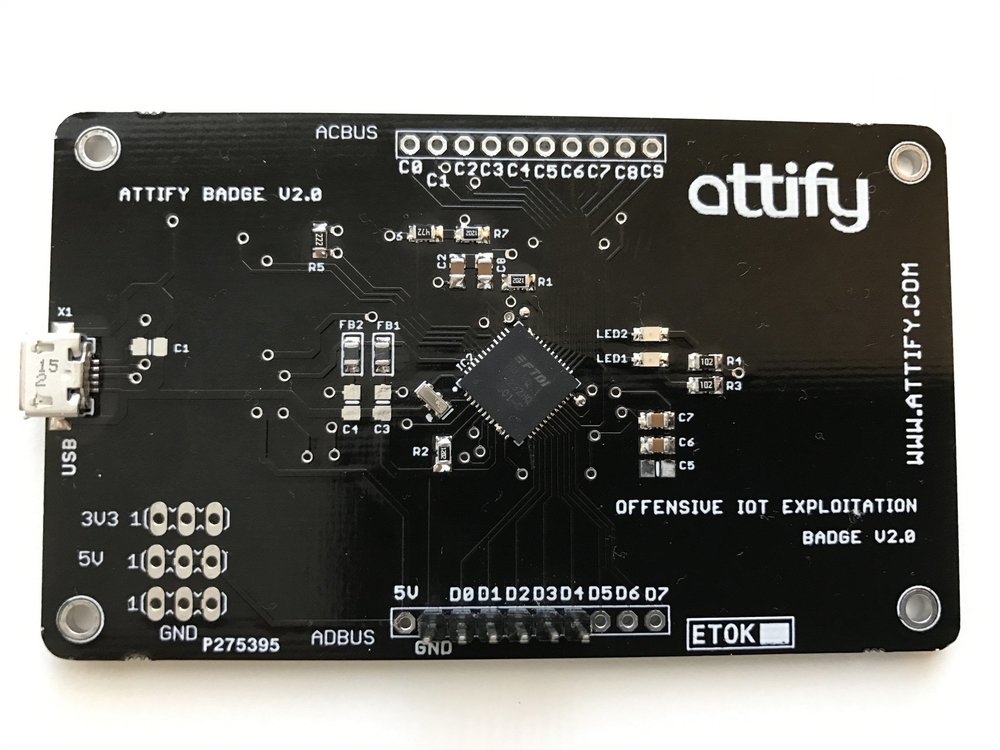
If you’re into industrial IoT/M2M or wireless sensor nodes, you might have encountered wireless protocols like Zigbee, 6LowPAN or Thread. These are IEEE 802.15.4 based wireless protocol which is mostly used for industrial application. Now most companies have started using it for commercial use like a home security system or home automation.

[KillerBee](https://github.com/riverloopsec/killerbee/) is a wireless penetration testing framework for 802.15.4 based wireless protocols. It allows you to perform attacks like replay attack, fuzzing, and packet analysis and lets you write your own exploit using SCAPY. It also supports wardiving. It supports all protocols that works with IEEE 802.15.4 protocol. It is a very user-friendly toolset written around python. Most easily available hardware dongle is RZUSBStick by Atmel.

[](https://payatu.com/wp-content/uploads/2017/11/image5.png)

# Attify Badge

It is a hardware tool that allows you to interact with various hardware interfaces and ports such as UART, SPI, I2C, JTAG, GPIO and so on.

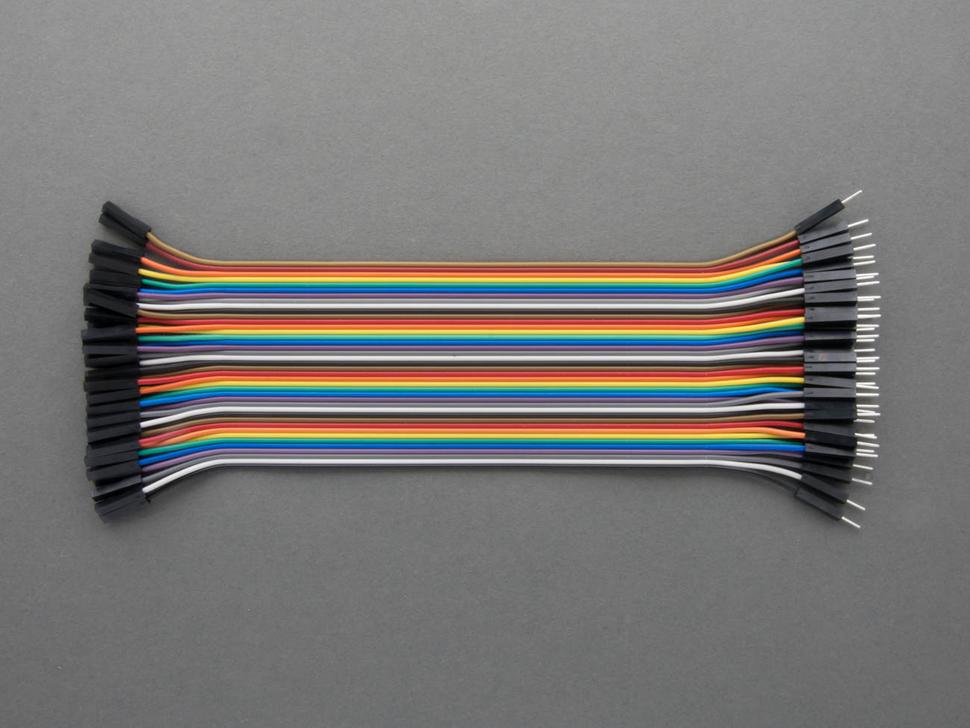


# Break Away Headers

This header is especially useful when you need to connect a PCB to a solderless breadboard. Each header can be broken apart to your preference to fit custom PCBs or general custom headers.



# Jumper Wires



# Multimeter



# Price Estimate

|  |  |  |
| --- | --- | --- |
| **Hardware** | **Approximate price($)** | **Where to buy** |
| Bus Pirate | 38 | [SeeedStudio](https://www.seeedstudio.com/Bus-Pirate-v4-p-740.html) |
| JTAGulator | 200 | [AdaFruit](https://www.adafruit.com/product/1550) |
| ChipWhisperer Lite | 250 | [Newae](http://store.newae.com/chipwhisperer-lite-cw1173-32-bit-basic-board/) |
| Hack RF One | 300 | [Sparkfun](https://www.sparkfun.com/products/13001) |
| Ubertooth One | 120 | [Sparkfun](https://www.sparkfun.com/products/10573) |
| Killerbee | 93 | [Digikey](https://www.digikey.com/product-detail/en/microchip-technology/ATAVRRZUSBSTICK/ATAVRRZUSBSTICK-ND/1886204) |
| Attify Badge/ Exploit Nano | 40-45 | [Attify](https://www.attify-store.com/products/attify-badge-assess-security-of-iot-devices), [expliot.io](https://expliot.io/products/expliot-nano) |
| Break Away Headers, Jumper Wires | 200 INR₹ | [Thingbits](https://www.thingbits.net) |
| Multimeter | 500-1000₹ | Amazon, Flipkart |