Assignment -2

Team :

K.Siva Jyothi

K.Lokesh Teja

K. Venka Tesh

Hari Chandra Prasasd

Section : M

Course Code: CSE18R394

Title : Hacking Gadgets

USB Rubber Ducky

To the human eye, the USB Rubber Ducky looks like a normal USB flash drive. Plug it into a computer, however, and the machine sees it as a USB keyboard — which means it accepts keystroke commands from the device just as if a person was codifying them in.

Everything it types is trusted to the same degree as the stoner is trusted, so it takes advantage of the trust model erected in, where computers have been tutored to trust a mortal. And a computer knows that a mortal generally communicates with it through clicking and codifying.

What can Usb Rubber Ducky do?

Previous version of Rubber Ducky could carry out attacks like

1.creating a fake Windows pop-up box to harvest a user's login credentials

2. causing Chrome to send all saved passwords to an attacker's webserver.

But these attacks had to be carefully crafted for specific operating systems and software versions and lacked the flexibility to work across platforms.

New version Rubber Ducky aims to overcome these limitations. It ships with a major upgrade to the Ducky Script programming language, which is used to produce the commands that the Rubber Ducky will enter into a target machine. While former performances were substantially limited to writing keystroke sequences, Ducky Script 3.0 is a point-rich language, letting druggies write functions, store variables, and use sense inflow controls (i.e., if this. also that).

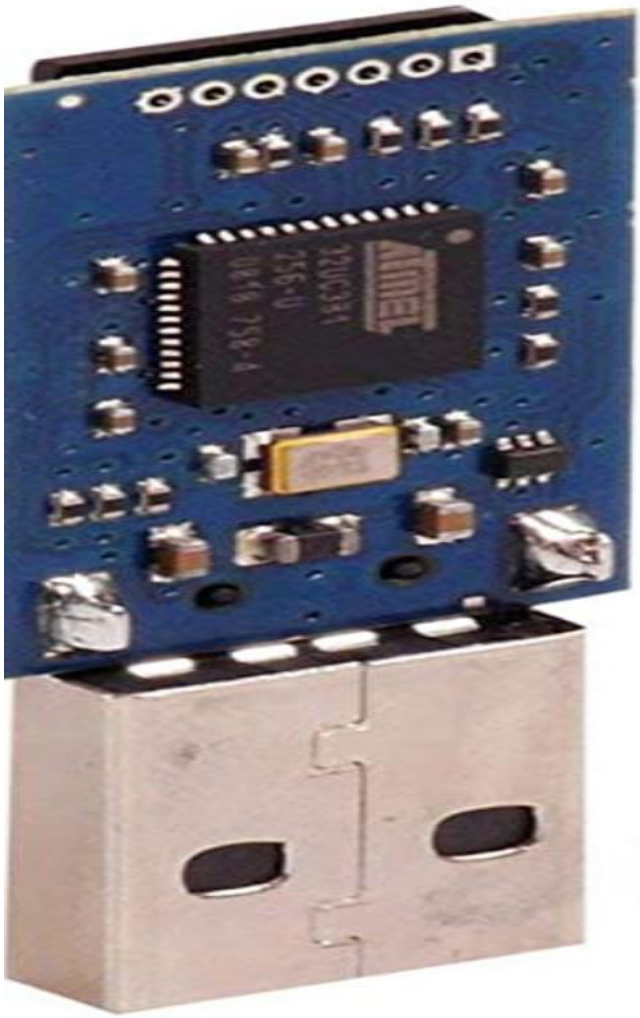
That means, for illustration, the new Ducky can run a test to see if it's plugged into a Windows or Mac machine and conditionally execute law applicable to each one or disable itself if it has been connected to the wrong target. It also can induce pseudorandom figures and use them to add variable detention between keystrokes for a further human effect.

May be most impressively, it can steal data from a target machine by garbling it in double format and transmitting it through the signals meant to tell a keyboard when the Caps Lock or Num Lock LEDs should light up. With this system, an attacker could plug it in for a many seconds, tell someone, Sorry, I guess that USB drive is broken, and take it back with all their watchwords saved.

How much of a threat is it?

New Rubber Ducky was his company's most in- demand product at Def Con, and the 500 or so units that Hak5 brought to the conference vended out on the first day. safe-deposit box to say, numerous hundreds of hackers have one formerly, and demand will probably continue for a while.

It also comes with an online development suite, which can be used to write and collect attack loads, also load them onto the device. And it’s easy for druggies of the product to connect with a broader community a “ cargo mecca ” section of the point makes it easy for hackers to partake what they ’ve created, and the Hak5 disharmony is also active with discussion and helpful tips.



WiFi Deauther Watch

The Deauther Watch(now in interpretation 3) is both utilitarian and simple. At its core, it's just an ESP8266, a cheap simple Wi- Fi chip that's in tons oftech. However, you presumably have several of these chips in your home right now, If you have Wi- Fi light bulbs.

On top of the chip, there's a little screen and battery that runs a simple Deauther tool written by a programmer called Spacehuhn. With it, you can protest any device off of a2.4 G Wi- Fi network. It should be noted that the Dstike isn't a jammer, which you should surely not buy, as Spacehuhn explains a jammer works by creating a ton of magpie noise, which can intrude with effects like exigency services and is veritably presumably illegal in your area. bias like the Dstike watch or any analogous device running the Deauther tool work by using deauthentication frames to tell a device to dissociate from a Wi- Fi network. You're principally getting someone’s phone or laptop to quit being connected. Check Plagiarism Grammar.

What can Deauther Watch do?

Deauther watch can knock a device off of its Wi-Fi network, which is very annoying. You can also do a beacon attack, which lets you create a fake access point with names of your choice, or a probe attack, which can be used to confuse Wi-Fi trackers.

It lets you monitor Wi-Fi traffic and, of course, also has a clock (with NTP time server synchronization) and a powerful laser pointer because if you are already wearing something that looks like that, you may as well take it to its logical conclusion.

Like all ESP8266 development boards, you can also get it to run other software if that is your thing. It should be worth noting, however, that the ESP8266 chip only works on 2.4GHz Wi-Fi, so the script doesn't pose a risk to every network

Conclusion:

watch is just a fun package for the whole thing, this is presumably one of the more accessible hacking tools out there. However, there showing you how to set it up, If you want to try your hand at intruding around with this stuff for your own particular security testing for coming to nothing. In addition to the OLED screen, the watch features a accessible web interface that you can use to connect via your smartphone or PC. Just make sure you use it on your own networks rather of

being a little stinker. You could also(hear me out then) just use it as a watch. It’s just a raw black PCB in a clear plastic quadrangle, but occasionally the severely functional is just what you need. suppose of it as a kind ofanti-Apple Watch brutal and simple with a focused purpose and a Hackers-inspired sense of style.

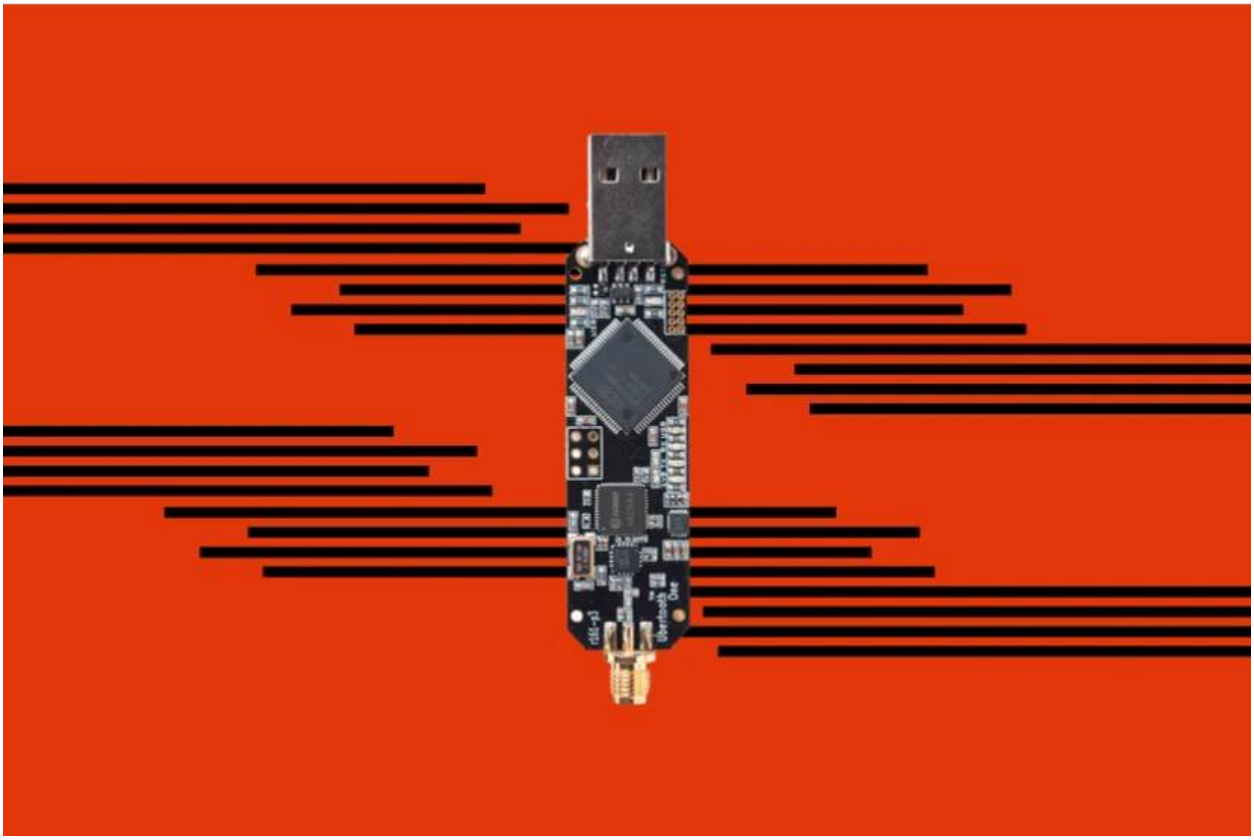
Ubertooth One

Ubertooth One is the most notorious Bluetooth hacking tool we can find on the request. It's an open source2.4 GHz wireless development platform suitable for Bluetooth hacking. marketable Bluetooth monitoring outfit can fluently be priced at over$,000, so the Ubertooth was designed to be an affordable indispensable platform for monitoring and development of new BT, BLE and analogous wireless technologies.

Ubertooth One is designed primarily as an advanced Bluetooth receiver, offering capabilities beyond that of traditional adapters, which allow for it to be used as a BT signal sniffing and monitoring platform. Although the device hardware will accommodate signal broadcasting, the firmware currently only supports receiving and minimal advertising channel transmission features.

What can Ubertooth One do?

The Ubertooth One is a small, open- source USB device with an antenna powered by an ARM Cortex- M3 chip and a CC2400 wireless transceiver. Plug it into your computer’s USB harborage, and you can whiff and cover Bluetooth signals from near bias.



he Ubertooth One was the first affordable Bluetooth sniffer, and it was a game- changer in a lot of ways. You can configure it to snoop on Bluetooth Low Energy bias using Wireshark, Kismet, and colorful other software(including at least one program used by the government).

But it does have some severe limitations about what it can do. It's primarily for targeting the newer BLE standard, which is still useful because utmost of the inventions in Bluetooth in the last many times have revolved around BLE rather than the Bluetooth Classic standard. It's not, still, particularly good at smelling Bluetooth Classic, and so that limits the range of what it can do for aged bias.

While the Ubertooth One isn't going to be as useful as a marketable Bluetooth sniffer, there's still quite a bit you can do with it or a analogous device. There are tons of BLE bias out there, and numerous people do n't suppose about Bluetooth as a vulnerability. That said, while the device is robust and has had a lot of support, there have been inventions within the space since it was created. Companies like Adafruit and Nordic Semiconductor also offer cheap dongles for smelling BLE bias and colorful other attacks. You can indeed use the inventor mode of an Android phone to hitch Bluetooth logs, along with both Linux- and macOS- grounded computers. Programs like Wireshark and Bettercap allow you to prize quite a bit of information from Bluetooth bias. With a little bit of work, you can reverse mastermind Bluetooth bias like heart rate observers, blood pressure observers, Bluetooth lockers, and much further. Or you could just reverse mastermind a light, connect it to Home Assistant, and turn it on with a Python script.

Conclusion:

The design itself is mature, robust, and veritably well- proved for people that want to get out there and learn. Programs like Wireshark are actually fairly straightforward. But there are more intuitive bias than this bone for a neophyte trying to get into pentesting and hacking, and far easier places to start (like, say, the WiFi Nugget, for illustration, or indeed the Flipper Zero). And for a lot of people, an Android phone or a laptop with Kali Linux would get you enough far.

Raspberry Pi 4

The RaserPi 4 Model B is the latest version of the low- cost Raspberry Pi computer. The Pi is not like your typical device; in its cheapest form it does not have a case, and is simply a credit- card sized electronic board-- of the type you might find inside a PC or laptop, but much lower. It costs as little as$ 35, although you might want to choose with its 4 GB of RAM for its better all-round performance.

Pi boards as media centers, file servers, retro games consoles, routers, and network-level ad-blockers, for starters. However that is just a taste of what's possible. There are hundreds of projects out there, where people have used the Pi to build tablets, laptops, phones, robots, smart mirrors, to take pictures on the edge of space, to run experiments on the International Space Station

Pi 4 being faster, able to decode 4K video, benefiting from faster storage via USB 3.0, and faster network connections via true Gigabit Ethernet, the door is open to many new uses. It's also the first Pi that supports two screens at one -- up to dual 4K@30 displays -- a boon for creatives who want more desktop space.

How to work with raspberry?

It's obviously not going to be the same as a high-end laptop, as you're still talking about running a computer on a mobile-targeted processor, but as mentioned the performance is good enough that there's little to complain about.

With the gradual move from software to online services, the browser is increasingly the only application that a computer needs to run, and on that front the Pi 4 excels, thanks to the extra memory and the Raspberry Pi Foundation's work on optimizing Raspbian's default Chromium browser.

In fact, in the weeks after the Pi 4's release, the areas that are lacking on the Raspbian desktop tend to be related to video playback, although this is due to be addressed by a future software update, and work is continuing on improving 4K playback on media center operating systems such as Libre ELEC.

However, the Pi works also well as a thin-client, as I found when I tested its capabilities when running it as a thin client for Windows 10, with performance being almost indistinguishable from running a modern Windows 10 PC, save for the very slow transfer of data to USB sticks. This was based on a Pi 3, so a Pi 4 with its true Gigabit Ethernet should work even better as a thin client.

Latest version of the Raspberry Pi's official OS has the Chromium browser, the open-source browser that Chrome is based on. As mentioned, its performance on the 4GB Pi 4 is good, with little lag even on heavy sites, with the only wrinkle being screen tearing on YouTube video at launch, although this is due to be fixed with an update.