Joey Queppet
10/18/2018
ENGL 202C

The Hardware Components of a USB Rubber Ducky

New enthusiasts in cyber security can be a fascinating rewarding endeavor. and world is full of confusing names and acronyms that can confuse new enthusiasts. In this document, I will be describing one such pieces of technology. The USB Rubber Ducky is a computer penetration device produced by Hak5 that stores a malicious payload, connects as a HID (**H**uman **I**nteractive **D**evice) and executes its payload automatically as a series of keyboard presses.

One of many vulnerability leveraging devices offered by Hak5, the USB Rubber Ducky is a device geared towards physical or social engineering attacks. On the outside, it resembles a standard USB thumb drive or memory stick, which acts as simple office camouflage. On the inside, it resembles a microSD to USB Type-A adapter which can fool less tech savvy victims. When plugged into a victim computer, the processor tells the victim computer it is a HID keyboard. This causes the computer to accept input from the device without requiring security permission. Then, it executes an internal script as a series of button presses, virtually typing the malicious script and actions into the victim computer. The payload, or injected script, can have any number of customized effects on the victim computer. Examples of possible effects include stealing files or installing remote access points. The primary hardware components of the USB Rubber Ducky covered in this document are the casing, circuit board, USB adapter, replay button, indicator LED, memory adapter, processor, and JTAG interface.

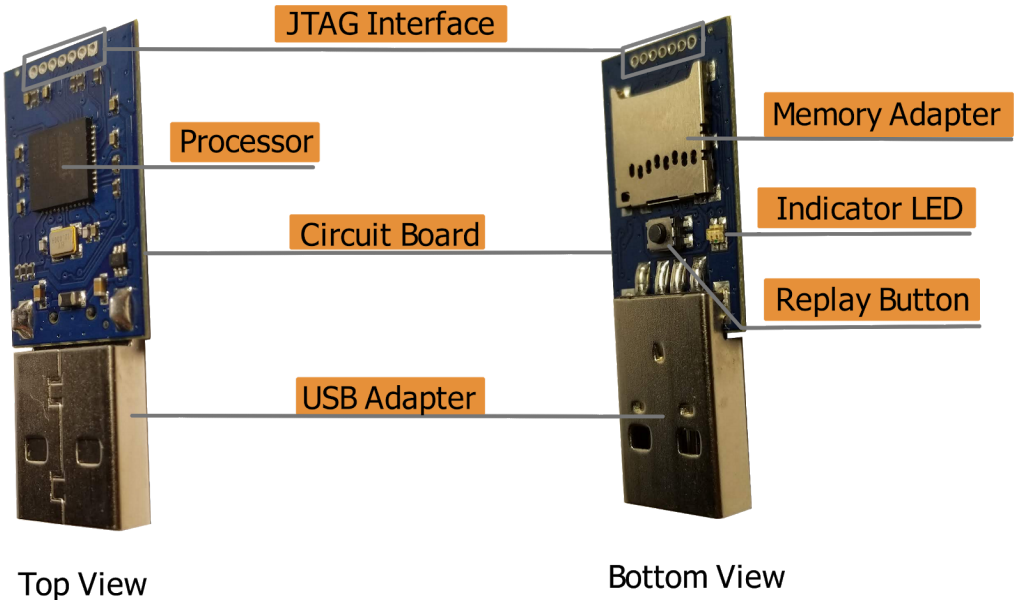

Figure 1.
Queppet, Joseph. “USB Rubber Ducky Without Casing.” 2018. PNG file.

Casing

The casing of the USB Rubber Ducky is composed of standard injection mold plastic with aluminium highlights. An example of a USB Rubber Ducky contained in it's casing is displayed in Figure 2. This casing can be opened by applying pressure along the seam of the top and bottom half, allowing for easy access to the internal hardware components of the USB Rubber Ducky. This generic casing serves multiple purposes:

- Camouflages the device as a generic USB thumb-drive
- Allows the device to blend into most office or school environments
- Entices curious victims into plugging in the device and activating the malicious script hosted inside the device

Figure 2.

"rubber_ducky_800x." *hak5,* cdn.shopify.com/s/files/1/0068/2142/products/rubber_ducky_800x.jpg?v=1494296097

Circuit Board

The circuit board is a blue printed silicon board which houses the copper connections between the various hardware components attached to the board. The connections transmit power or data between the components. Also, embedded into the board are various circuits, transistors, and minor hardware components not discussed in this document. Below in Figure 3, you can see the blue circuit board with it's embedded components.

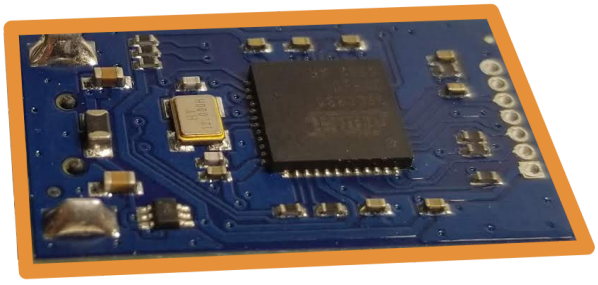

Figure 3.
Queppet, Joseph. "USB Rubber Ducky - Circuit Board." 2018. PNG file.

USB Adapter

The front adapter is a USB Type-A standard adapter which allows the USB Rubber Ducky to be inserted into most personal computers and laptops. When plugged in:

- The computer powers the device through this adapter
- The adapter allows input to pass from the device to the computer

This removes the need for an internal power supply for the USB Rubber Ducky, and gives it an simple input path to the computer.

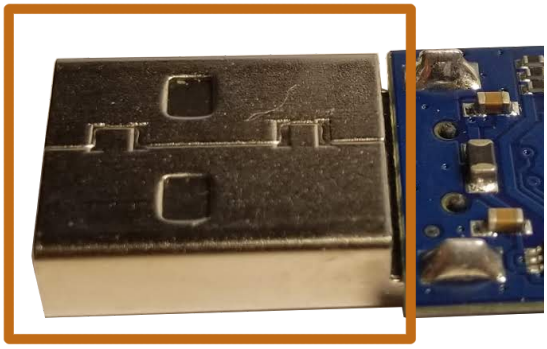

Figure 4.
Queppet, Joseph. “USB Rubber Ducky - USB Type-A Adapter.” 2018. PNG file.

Replay Button

The replay button is a small black button located on the bottom of the USB Rubber Ducky which executes the payload of the device when clicked. Some computers are not very responsive. So, if a payload is introduced too quickly, the victim computer could miss the automated payload execution because it has not finished acknowledging the device. If this situation occurs, the computer will either miss the payload entirely, or receive only part of the payload. To address this issue the user can press the button and launch the payload again. It is also useful when error testing, allowing the user to determine if the payload is set to activate to early, or is simply not working.

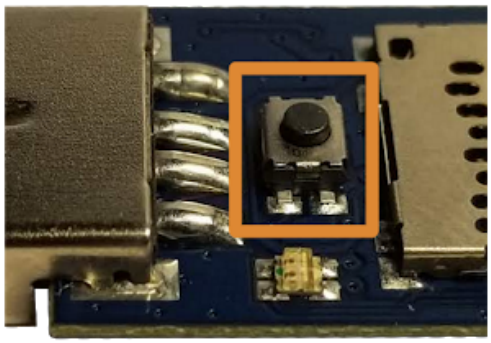

Figure 5.
Queppet, Joseph. “USB Rubber Ducky - Replay Button.” 2018. PNG file

Indicator LED

The indicator LED is a red and green LED located on the bottom of the USB Rubber Ducky which identifies the current connective state of the device. The LED can appear in four different states:

- Green, when the USB Rubber Ducky is communicating with the victim computer correctly
- Red, when the USB Rubber Ducky is not communicating with the victim computer
- Blinking red, when the USB Rubber Ducky is powered but can't read the microSD card
- Off, the USB Rubber Ducky is not powered

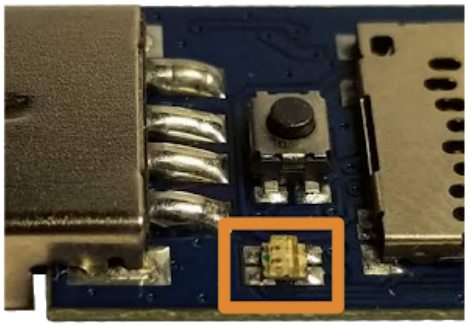

Figure 6.
Queppet, Joseph. "USB Rubber Ducky - Indicator LED." 2018. PNG file

Memory Adapter

The memory adapter is an adapter on the bottom side of the USB Rubber Ducky which can accept microSD type memory cards. This adapter can power the memory card and transmit data from the memory card to the processor. While not limited to a specific microSD brand, the USB Rubber Ducky requires that the connected microSD has specific software installed on it to be read properly. This software can be cloned from official Hak5 Github accounts.

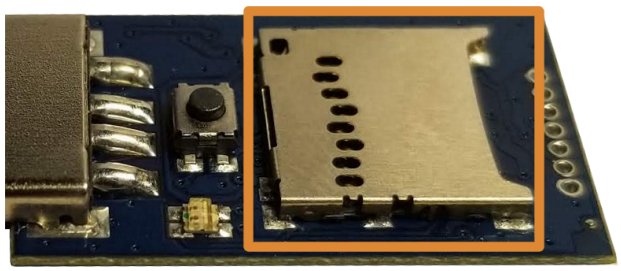

Figure 7.
Queppet, Joseph. "USB Rubber Ducky - Memory Adapter." 2018. PNG file

Processor

The processor is the board's CPU chip that controls the device and allows for quick write times to the victim computer. The processor is designed to automatically run on boot, and execute a special type of script called Ducky script from an inserted microSD. The processor has multiple functions. On the highest level, the processor:

- Translates the stored Ducky script into a series of keyboard button presses
- Emulates a HID keyboard and inputs these button presses automatically into the victim computer
- The speed of the 60 MHz 32 bit processor in the USB Rubber Ducky allows the device to input keyboard presses at a rate of 1000 words a second (Hak5).

Once inserted, the processor can effectively execute its payload within seconds. And, once the payload is executed the processor enters a listening state. In the listening state the processor does not performing any other action until the USB Rubber Ducky is either reinsierted or the replay button is pressed.

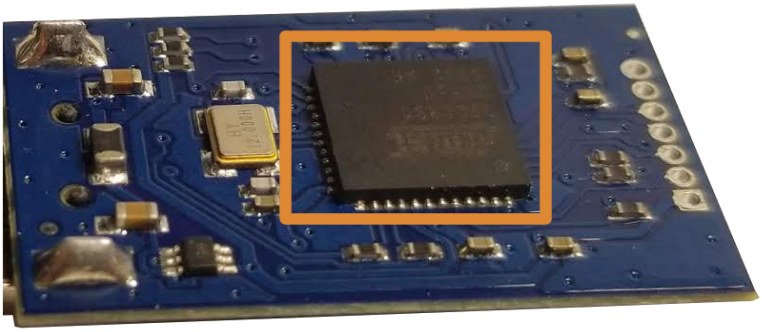

Figure 8.
Queppet, Joseph. "USB Rubber Ducky - Processor." 2018. PNG file

JTAG Interface

The JTAG interface, or **J**oint **T**est **A**ction **G**roup interface, is a series of seven holes on the circuit board which let the user test the interconnections and functionality of the hardware within the USB Rubber Ducky. The ability to test these interconnections means the user can make changes to the hardware of the device. And, the interface allows the user to modify the software of certain hardware components, such as the flash memory linked to the processor (Corelis). These two facets of the JTAG interface allow the user to modify the device by adding custom hardware or software functionality to it. This freedom gives users the option of adding new aftermarket functionality to the USB Rubber Ducky.

Figure 9.
Queppet, Joseph. “USB Rubber Ducky - JTAG Interface.” 2018. PNG file

Works Cited

Corelis. “What Is JTAG? A Guide to the IEEE-1149.1 Standard.” *JTAG Boundary-Scan, In-System Programming, & Bus Analyzers - Corelis*, Corelis Inc., 2018, www.corelis.com/education/tutorials/jtag-tutorial/what-is-jtag/.

Hak5. “USB Rubber Ducky.” *Hak5*, shop.hak5.org/collections/hak5-gear/products/usb-rubber-ducky-deluxe.