~/bashbunny


```
(\___/)
(='.'=)
(")_(")
```

Automating On-Site USB-Attacks

Presentation by: Sebastian Haas

CSPi
Technology Solutions

~/bashbunny/overview

- What is the Bashbunny?
- Similarities and differences to a Rubberducky
- Speed comparison with different keyboard emulators
- When to use?
- How to extend / high-level architecture
- Make it run more than two payloads
- Github repository etc.

~/bashbunny/what

- USB Device Emulator
  - Keyboard/HID Emulation
  - Network Emulation (RNDIS + ECM)
  - Storage Emulation (RW and RO)
  - Serial Connector
- Computer

~/bashbunny/diff

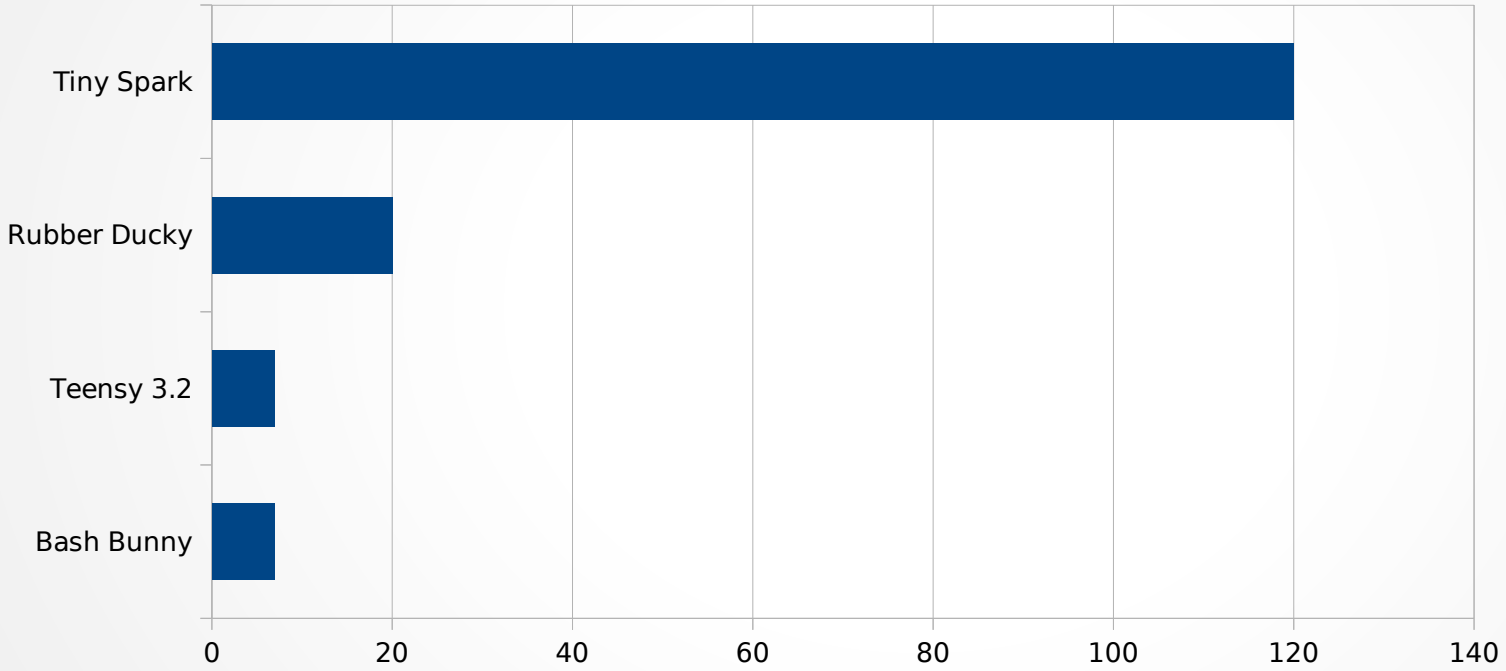
- Rubberducky
  - 60 MHz 32-bit processor
  - Several KB RAM
  - Some KB Flash
  - Scriptlang: Duckyscript

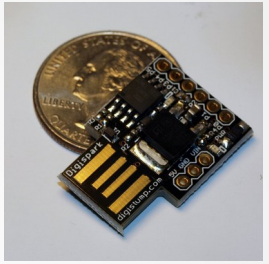
$44.99

- Bashbunny
  - 1.6 GHz Quadcore ARM
  - 512 MB DDR3 RAM
  - 8 GB Flash
  - Scriptlang: Extended Bash
  - RGB Indication LED (!)

$99.99

~/bashbunny/speed

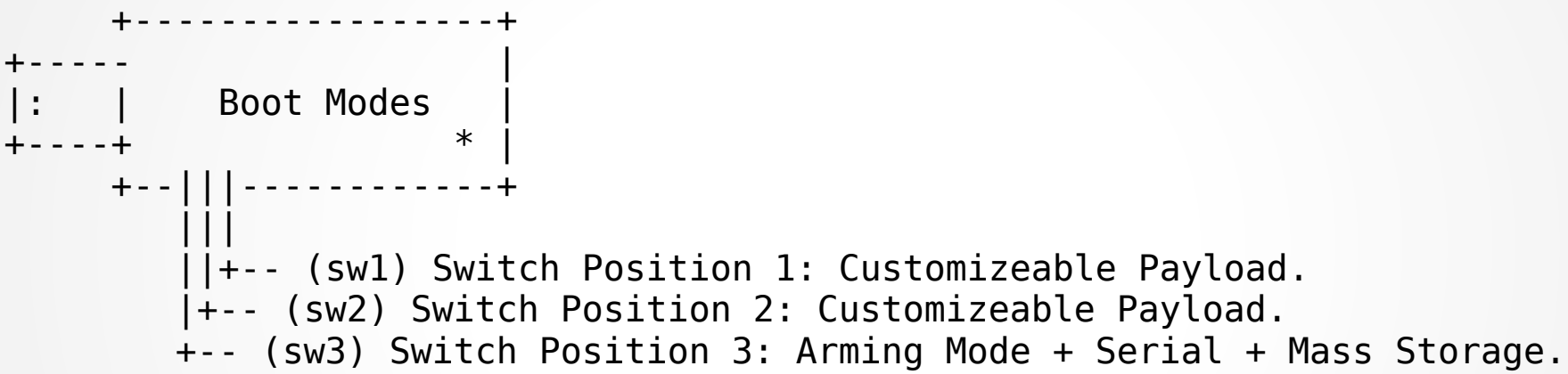




~/bashbunny/when

- On-Site attacks during security assessments
- Not-So-Legal™ attacks
- Task automation on offline systems

~/bashbunny/original

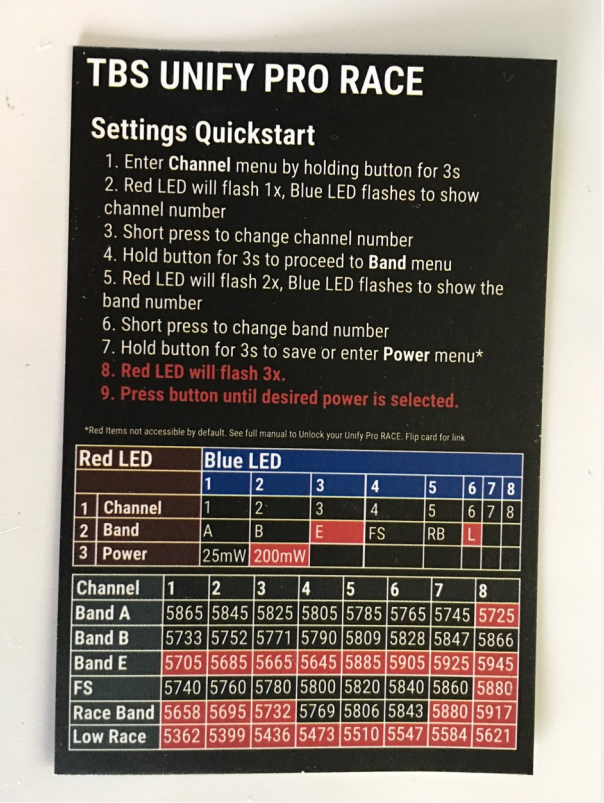


~/bashbunny/mods/HoppEye

How to extend a three position switch virtually?

- LED Pushbutton Sequencer

https://github.com/H8to/HoppEye



TBS UNIFY PRO RACE

Settings Quickstart

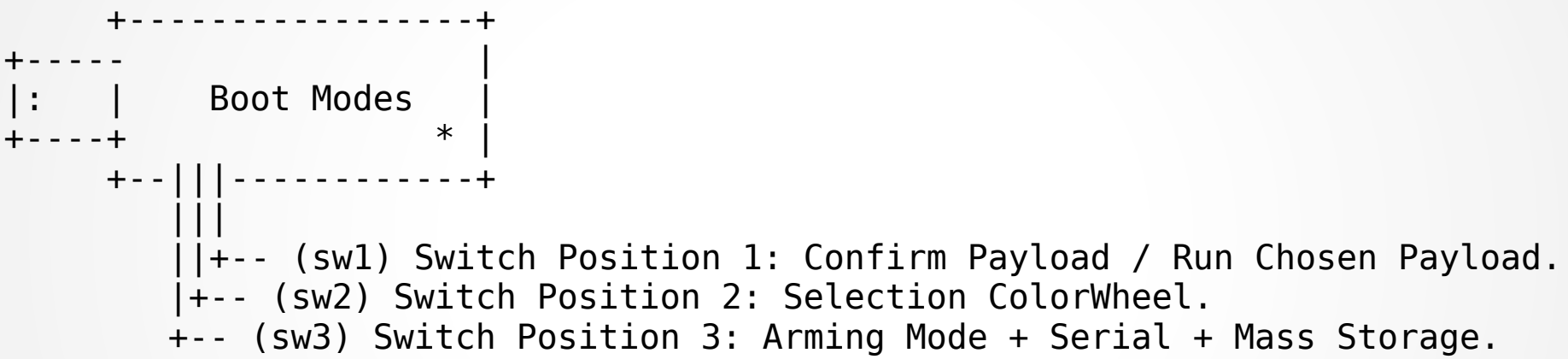
1. Enter **Channel** menu by holding button for 3s
2. Red LED will flash 1x, Blue LED flashes to show channel number
3. Short press to change channel number
4. Hold button for 3s to proceed to **Band** menu
5. Red LED will flash 2x, Blue LED flashes to show the band number
6. Short press to change band number
7. Hold button for 3s to save or enter **Power** menu*
8. Red LED will flash 3x.
9. Press button until desired power is selected.

*Red Items not accessible by default. See full manual to Unlock your Unify Pro RACE. Flip card for link

Red LED		Blue LED							
		1	2	3	4	5	6	7	8
1	Channel	1	2	3	4	5	6	7	8
2	Band	A	B	E	FS	RB	L		
3	Power	25mW	200mW						

Channel	1	2	3	4	5	6	7	8
Band A	5865	5845	5825	5805	5785	5765	5745	5725
Band B	5733	5752	5771	5790	5809	5828	5847	5866
Band E	5705	5685	5665	5645	5885	5905	5925	5945
FS	5740	5760	5780	5800	5820	5840	5860	5880
Race Band	5658	5695	5732	5769	5806	5843	5880	5917
Low Race	5362	5399	5436	5473	5510	5547	5584	5621

~/bashbunny/modified



~/bashbunny/original

Folder structure on the device:

```
payloads/
        switch1/
                payload.txt
        switch2/
                payload.txt
```

~/bashbunny/modified

Folder structure on the device:

```
payloads/
        payload_B_BluePayload/
        payload_G_Green/
        payload_OFF_empty/
        payload_W_network/
        payload_C_empty/
        payload_M_PoisonBunnyTap/
        payload_R_ReverseShellEmpire/
        payload_Y_empty/
        switch1/
        switch2/
                payload.txt <-- This is where magic happens
```

~/bashbunny/demo/demo/demo/demo/demo

Bash Bunny

```
(\___/)
(='.'=)
(")_(")
```

DEMO TIME!

Presentation by: Sebastian Haas

~/bashbunny/halt

kkthxb

~/bashbunny/man

- https://github.com/H8to/HoppEye
- https://twitter.com/H8_sec
- http://h8.to/

Questions?