TU Graz

SCIENCE
PASSION
TECHNOLOGY

Analysis of Low-level iOS Lightning Protocols

Andreas Karner

Master Thesis Defense, September 2023

Motivation

- Mobile Devices are attractive for attackers
  - Increased relevance and functionality
  - Managing financial bank account
  - Second factor for multifactor authentication
  - Data treasure
- Battery driven
  - Recharging of the battery is mandatory
  - Primarily tethered, introduces a **security threat**

Juice Jacking attack

Theorem (Definition [Men+15])

Juice-Jacking attacks exploit the unawareness of the users that charging cables do not only convey power, but also provide access to the USB interface and therefore, can be leveraged by an attacker to steal sensitive data or install hidden malware on the device.

Research Questions

- Attack
  - Feasibility of Juice Jacking attacks without commodity adapters
  - Attack Scope, complexity, and costs
  - Defeat existing mitigations [Kum20; Loe+16]
- Mitigation
  - Feasibility of mitigating Juice Jacking attacks concerning Apple Lightning devices
  - Improve existing mitigations [Kum20; Loe+16]

Major contribution

- TuWire - Attack
  - Malicious charging cable
  - Infiltrates Apple iPhone
  - Bypasses existing mitigations
- Lightning Condom - Mitigation
  - Lightning-to-Lightning adapter
  - Mitigates Juice Jacking Attacks
  - Improves existing mitigations

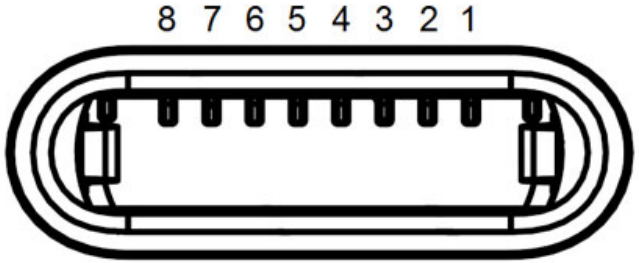
Minor Contribution

- Apple protocol stacks
  - `lib_idbus` — C-library for IDBUS
  - `lib_iap` — C-library for iAP
  - `nero` — Zephyr RTOS [1] module for Nero

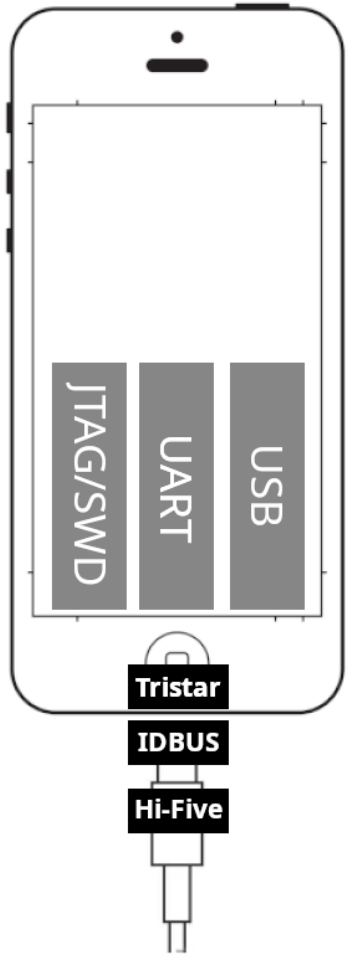
[1] https://zephyrproject.org/intro-to-zephyr-rtos/

Accessory Link Specifications

- Lightning Connector [Sat]
  - Adaptive 8-pin connector
  - Female-Plug - Tristar IC chip
  - Male-Plug - HiFive IC chip
  - Pinout:



Pin 1	GND	Ground
Pin 2	L0p	Lane 0 positive
Pin 3	L0n	Lane 0 negative
Pin 4	ID0	Identification/cc
Pin 5	PWR	Power (charger
Pin 6	L1n	Lane 1 negative
Pin 7	L1p	Lane 1 positive
Pin 8	ID1	Identification/cc



Credit: Nyan Satan [Sat]

- IDBUS Protocol [Sat; Ami18; sta22]
  - Single-wire protocol between Tristar and HiFive IC
  - Request high-level protocols (iAP, USB, etc.), serial numbers and enables charging
- iAP Protocol
  - High-level protocol to modify system behavior (launch Apps, USB mode, HID handler, etc.)
  - Requires authentication via challenge signature
- Nero [2] Protocol
  - Screen mirroring protocol via USB (device/host)

[2] https://github.com/danielpaulus/quicktime_video_hack

Attack

TuWire [3]

[3] https://youtu.be/imAbaG3W6TI

Figure: Schematic of the malicious TuWire charging cable.

- Raspberry Pi Pico
  - IDBUS
    - Perform IDBUS and charging handshake
    - Unlocks access to iAP and USB interfaces
  - iAP
    - Perform iAP handshake including authentication procedure
    - Register HID handlers for HID event injections (mouse + keyboard)
    - Switch into USB Host mode

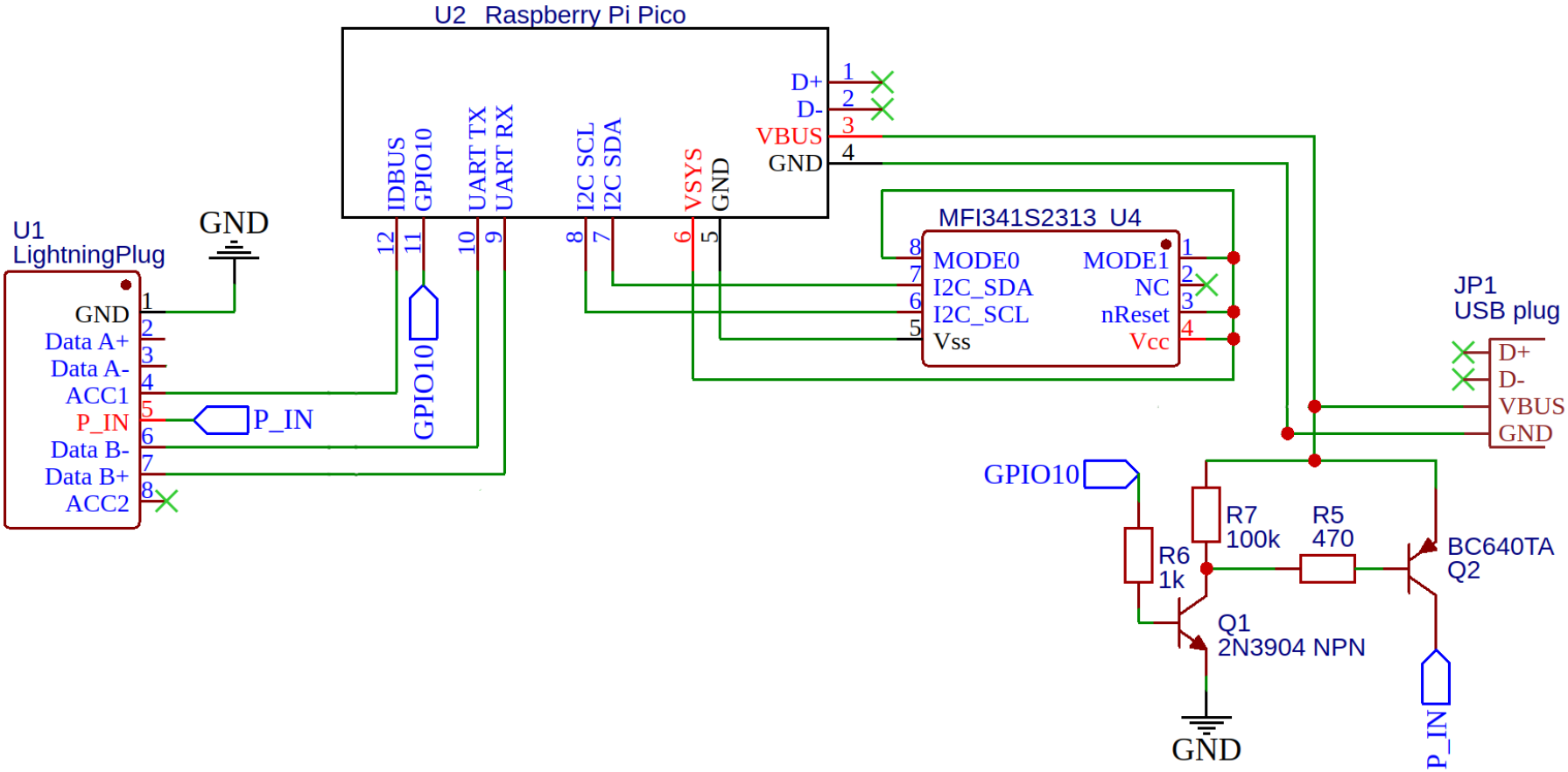


Figure: Schematic of the malicious TuWire charging cable.

- Raspberry Pi Pico
  - IDBUS
    - Perform IDBUS and charging handshake
    - Unlocks access to iAP and USB interfaces
  - iAP
    - Perform iAP handshake including authentication procedure
    - Register HID handlers for HID event injections (mouse + keyboard)
    - Switch into USB Host mode
- STM32F723e-DISCO
  - Nero
    - Perform Nero handshake
    - Stream device screen content to storage

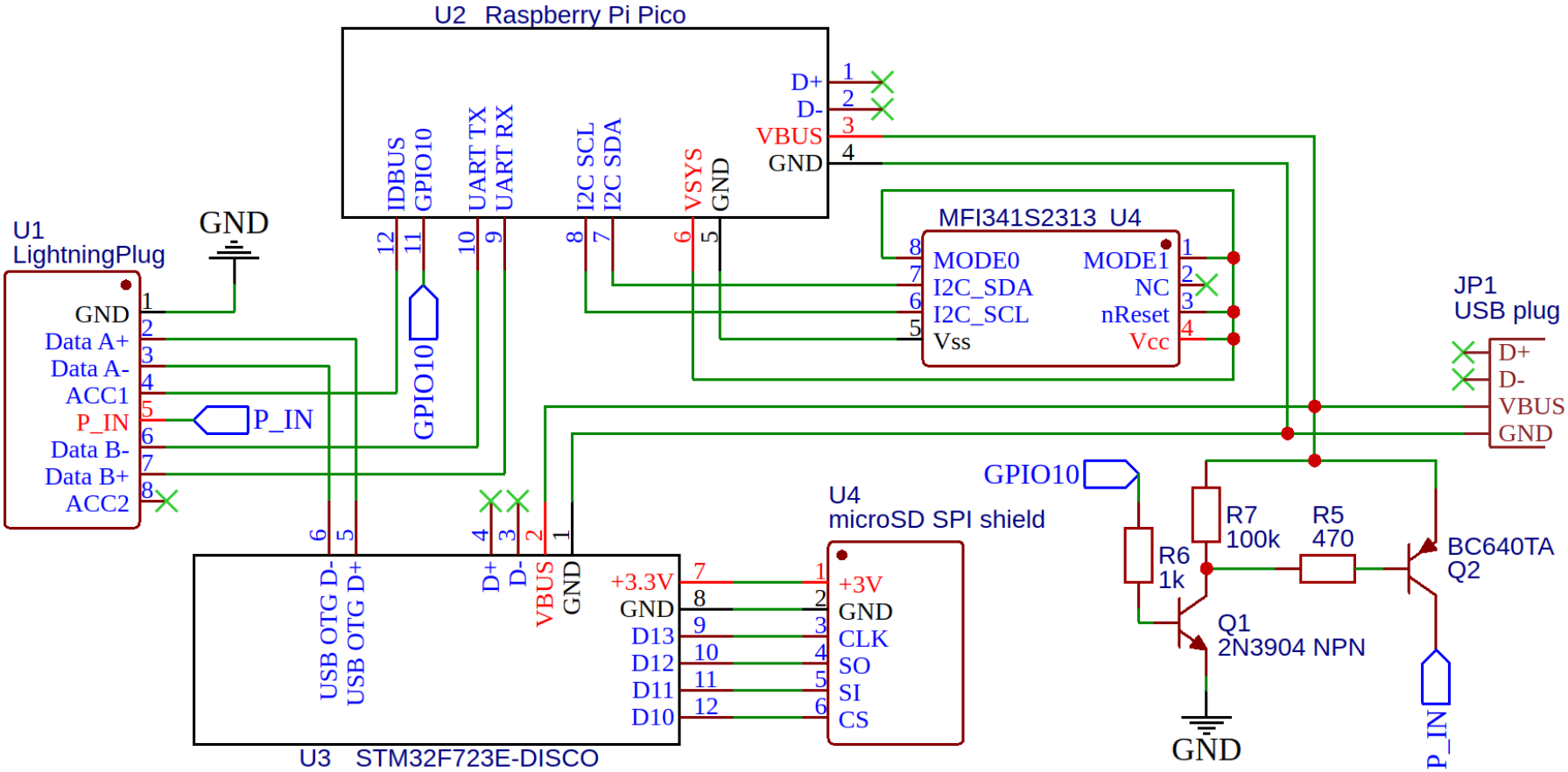


Figure: Schematic of the malicious TuWire charging cable.

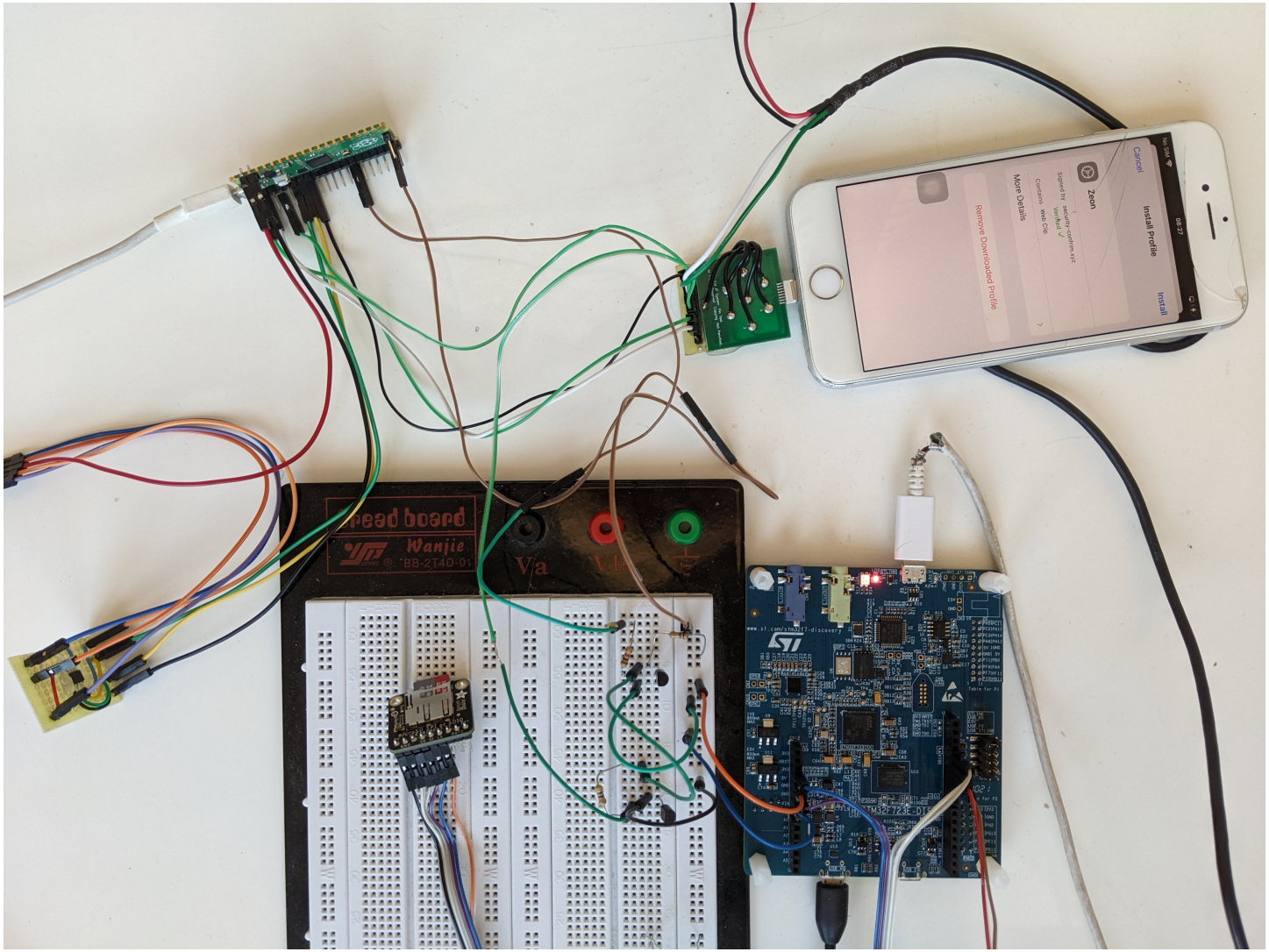


Figure: Experimental setup of TuWire.

- Wifi credential extraction
  - Request credential via iAP protocol
  - Confirm approval via iAP HID event injection
- Custom MDM profile enrollment
  - Control device via iAP HID event injection
  - Enroll custom MDM profile on device
- Capture screen content
  - Request frames via Nero protocol
  - Optionally store frames on flash or SD card

- IDBUS Handshake (vs official Lightning cable)
  - Runtime Overhead: 2.37 % (228 μs)
- iAP (Device control)
  - Authentication process: 3.51 s
  - WiFi extraction: 5.02 s
  - MDM profile enrollment: 21.05 s
- Nero frame throughput (vs official Haywire adapter)
  - Without storage: 86.53 % (1454.37 kB/s)

- TuWire challenges
  - ✓ Feasibility of Juice Jacking attacks without commodity adapters
  - ✓ Attack Scope (moderate)
  - ✓ Attack Complexity (moderate)
  - ✓ Attack Costs (< 100 €)
  - ✓ Defeating existing mitigations [Kum20; Loe+16]

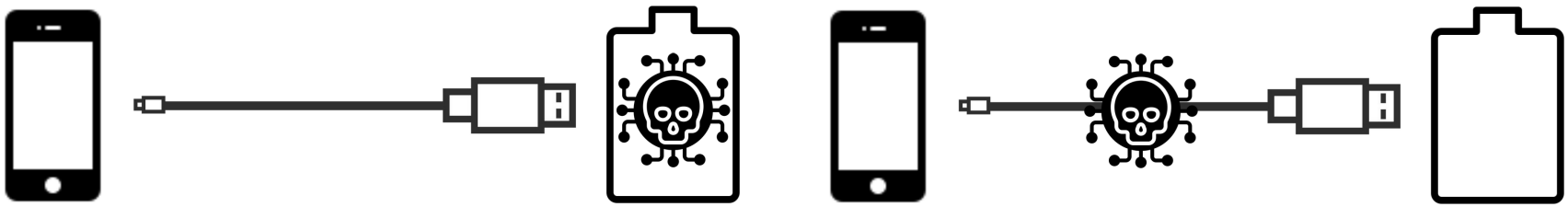


Figure: Defeat existing mitigations by moving attack logic from outlet (left subfigure) into charging cable (right subfigure)

Mitigation

Lightning Condom [4]

[4] https://youtu.be/olzWqD0d64o

Figure: Schematic of the LIGHTNING CONDOM to mitigate Juice Jacking attacks.

- Raspberry Pi Pico
  - IDBUS
    - Secure IDBUS handshake
    - Proxying and filtering IDBUS messages
  - Resistor Network
    - Sampled by the Apple device
    - Classifies Condom as charging-only cable
    - Specifies the maximal current (1A selected)

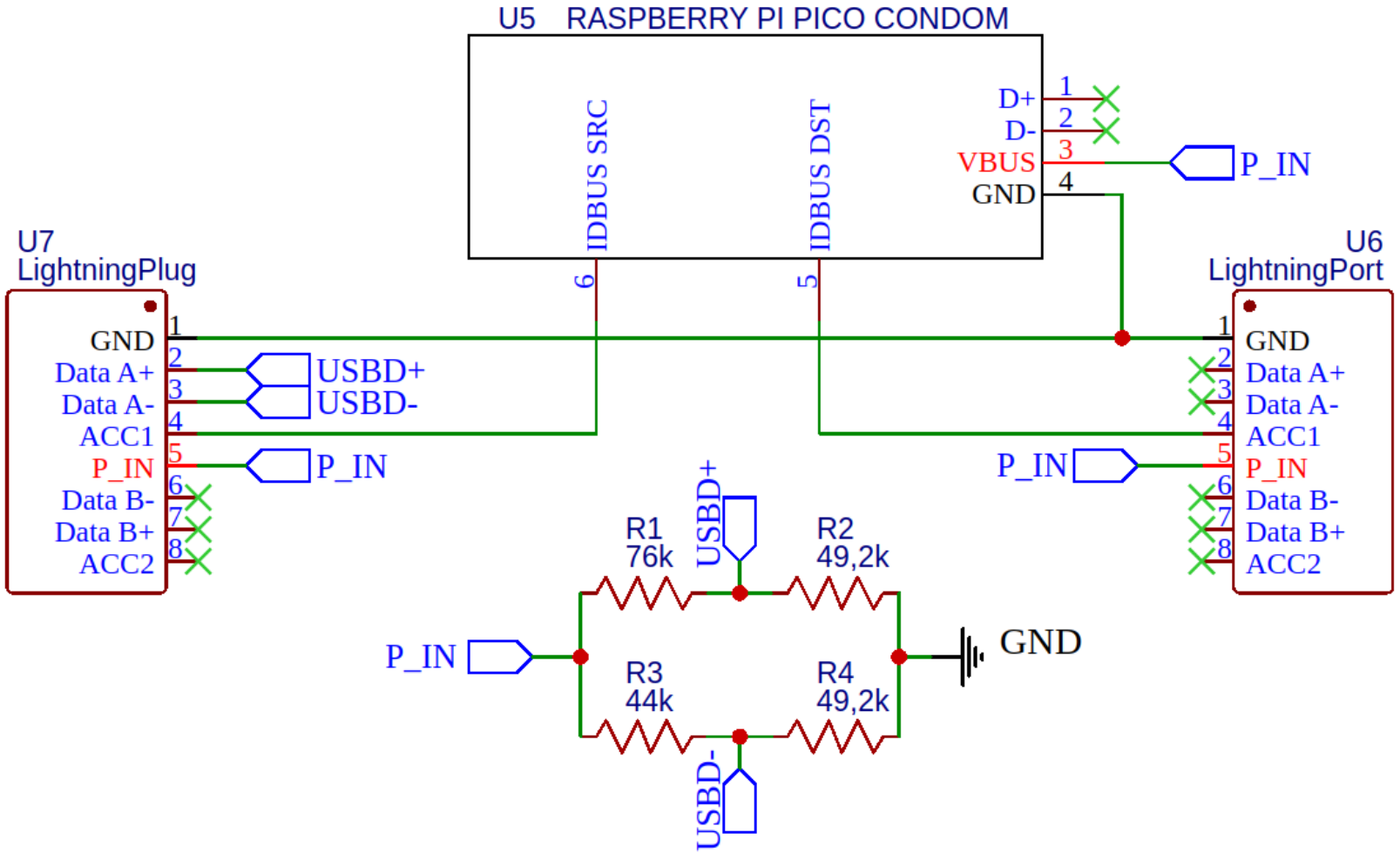


Figure: Schematic of the LIGHTNING CONDOM to mitigate Juice Jacking attacks.

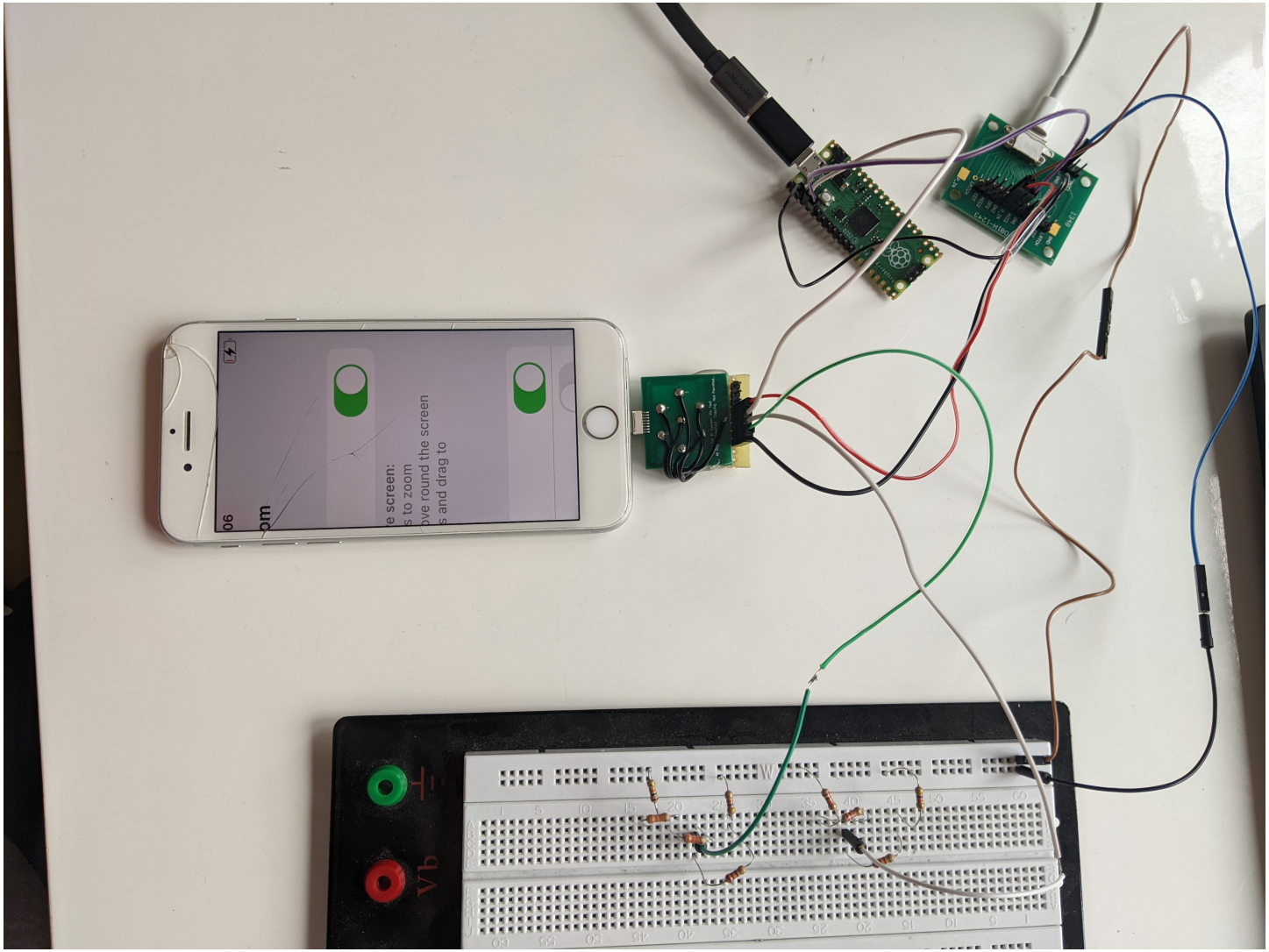
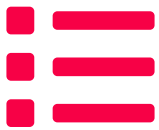


Figure: Experimental setup of the LIGHTNING CONDOM.

- IDBUS Handshake (active bus time)
  - Unsecure: $\sim$ 9 ms
  - Secure: $\sim$ 39 ms
  - Overall Overhead: > 4 times
- Charging Current
  - Unsecure: $\sim$ 600 mA
  - Secure: $\sim$ 400 mA
- Successfully mitigates Juice Jacking attacks
  - Prevents USB exposure to host computer
  - Mitigates TuWire successfully

- Mitigation challenges
  - ✓ Feasibility of mitigating Juice Jacking attacks concerning Apple Lightning devices
  - ✓ Improving existing mitigations [Kum20; Loe+16]

Summary



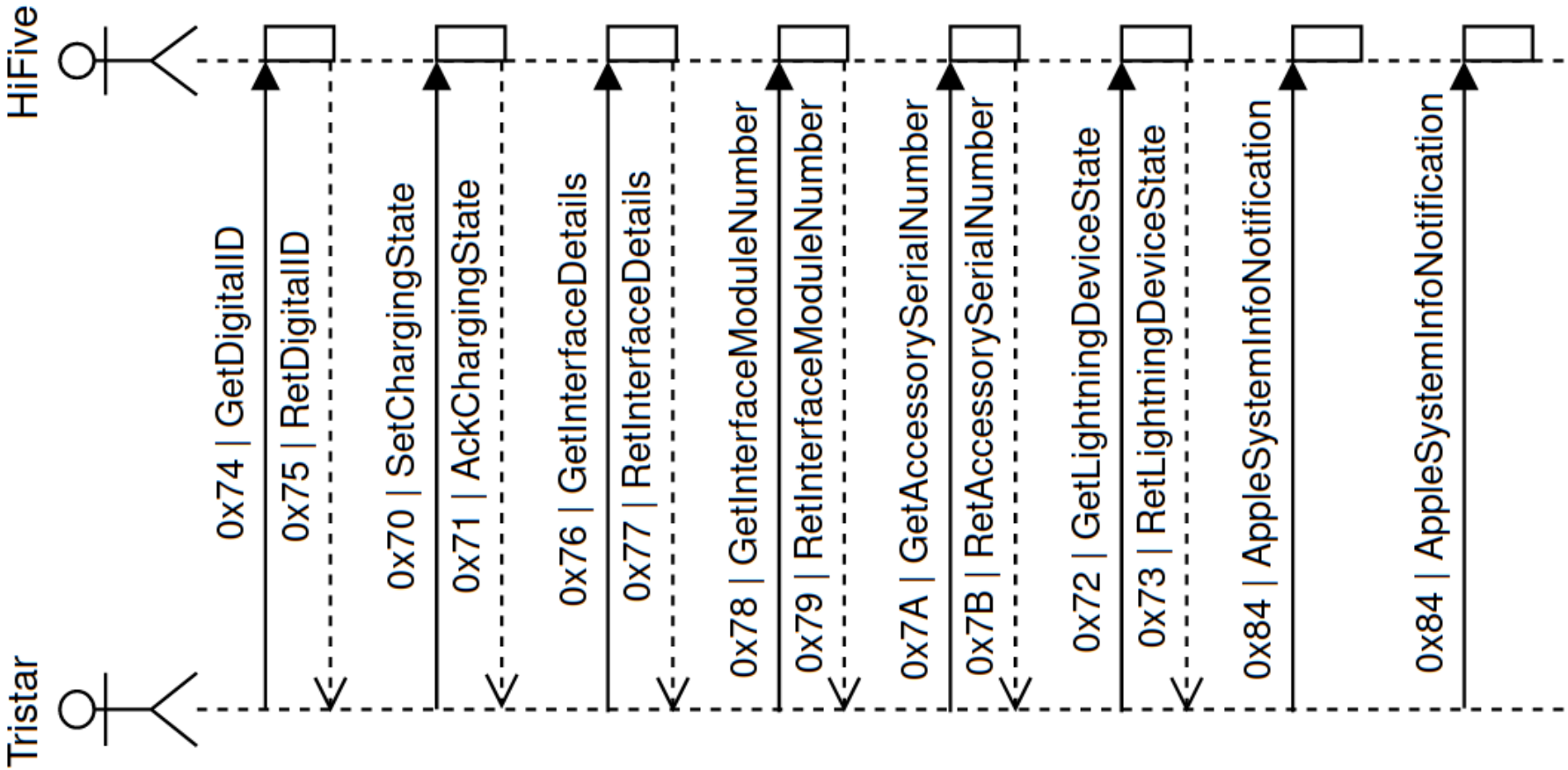
- Software Libraries: IDBUS, iAP, Nero
- TuWire - State-of-the-art Attack Approach
  - Successfully assembled malicious charging cable
  - Leverages solely Apple protocols
  - Successfully attacked target device (iPhone 7)
- Lightning Condom - Novel Mitigation Approach
  - Successfully assembled mitigation object
  - Mitigates Juice Jacking attacks reliably
  - Extends existing mitigation approaches

Q&A

Thank you for your attention

Appendix

IDBUS Handshake

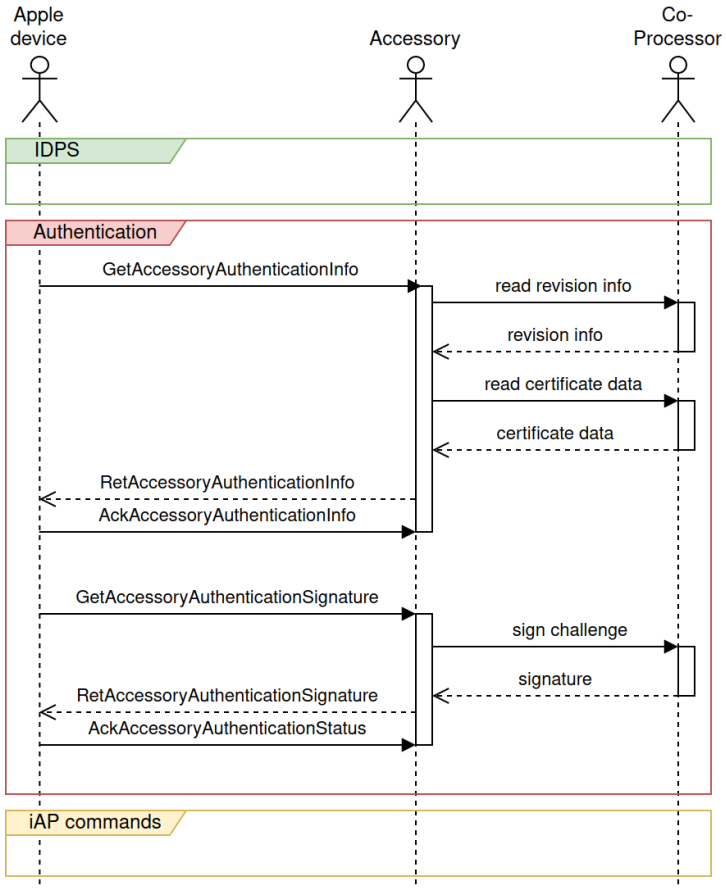


TuWire IDBUS Evaluation

IDBUS Communication Partner	Avg. Response Time (us)	Overall Time (us)	Avg. Retry Count
Lighting-to-USB	22.82	10188	0
TuWire with logging	507.38	13199	0
TuWire without logging	44.12	10416	0

Table: Comparison of the average response time, overall handshake time, and retry count between the TuWire's IDBUS stack and an official Lightning-to-USB cable.

iAP Handshake

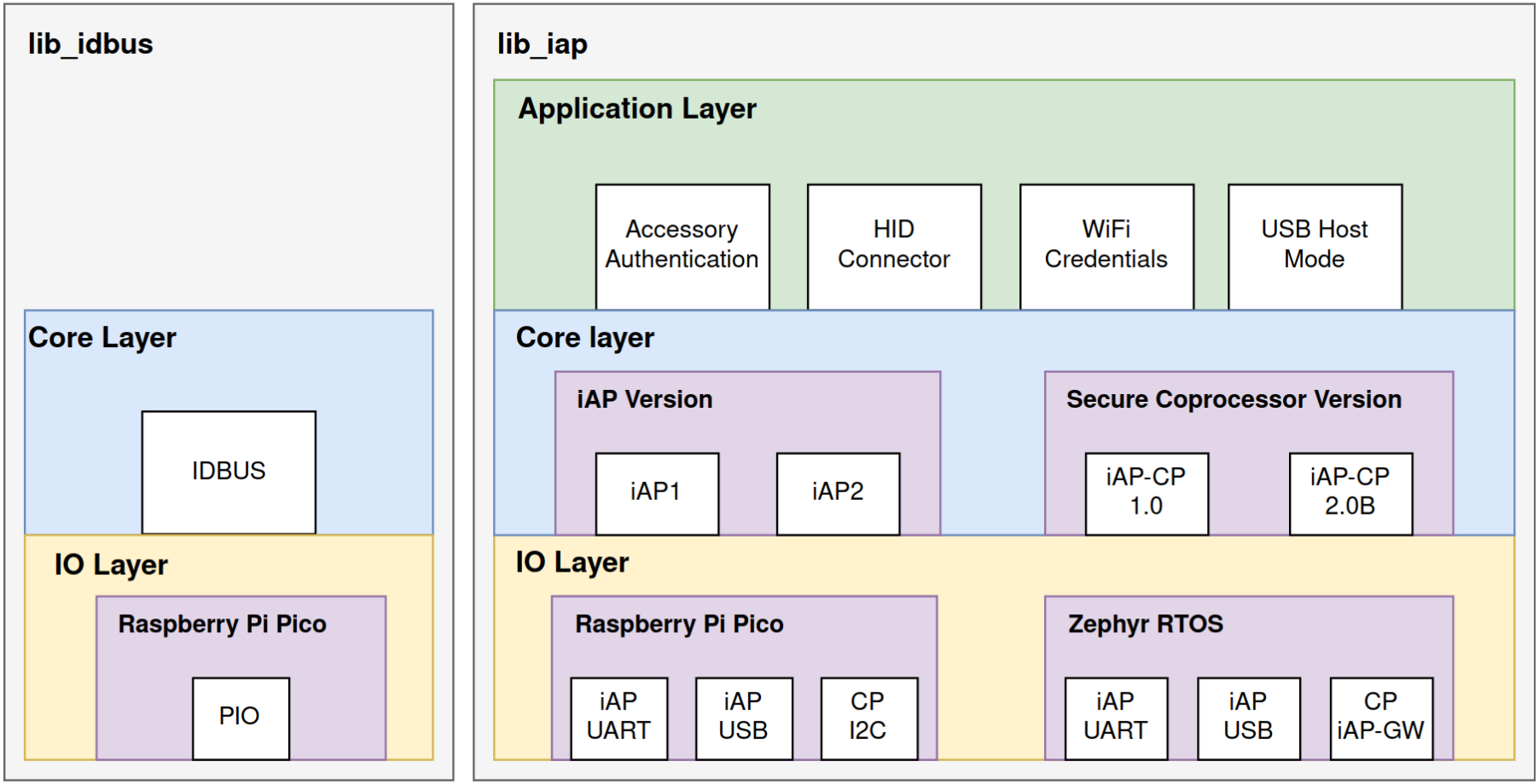


TuWire iAP Evaluation

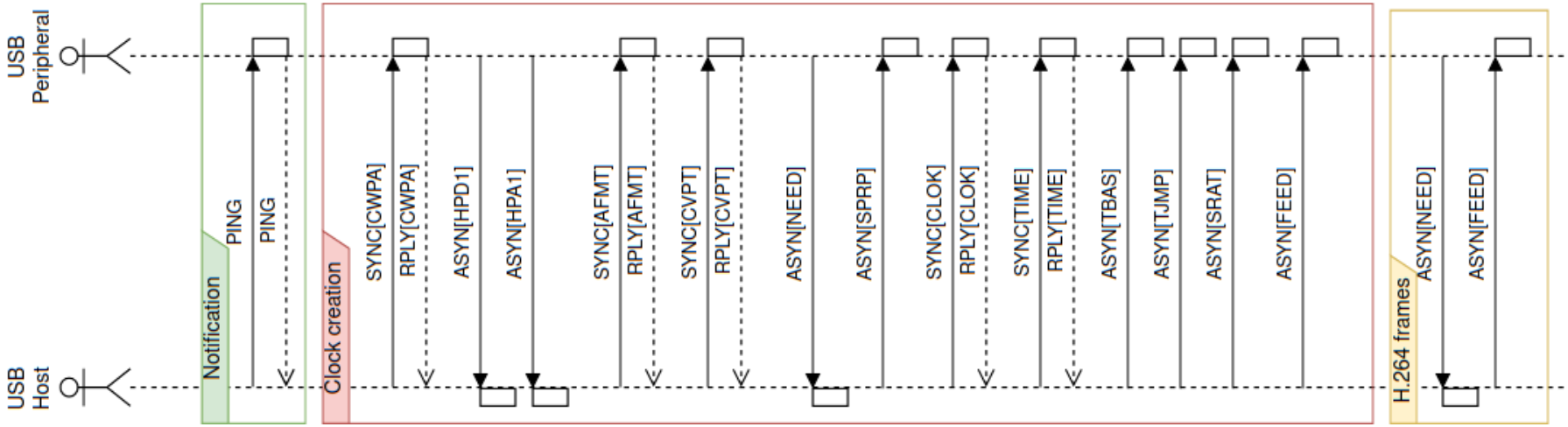
iAP Task	Overall Duration (s)
iAP authentication	3.51
Enabling charging	0.20
HID handlers registration	1.70
WiFi credential extraction	5.02
MDM profile enrollment	21.05
USB host mode activation	0.03

Table: Runtime of all performed iAP tasks by TuWire.

IDBUS/iAP library stack



Nero Handshake

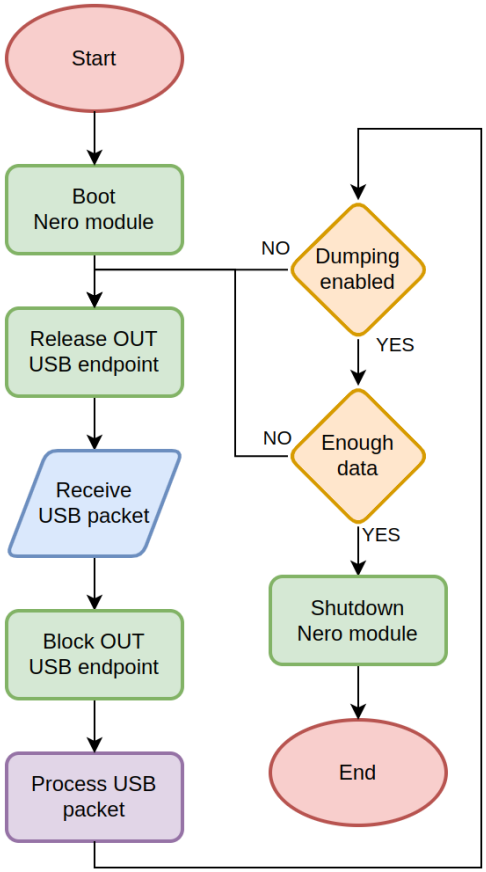


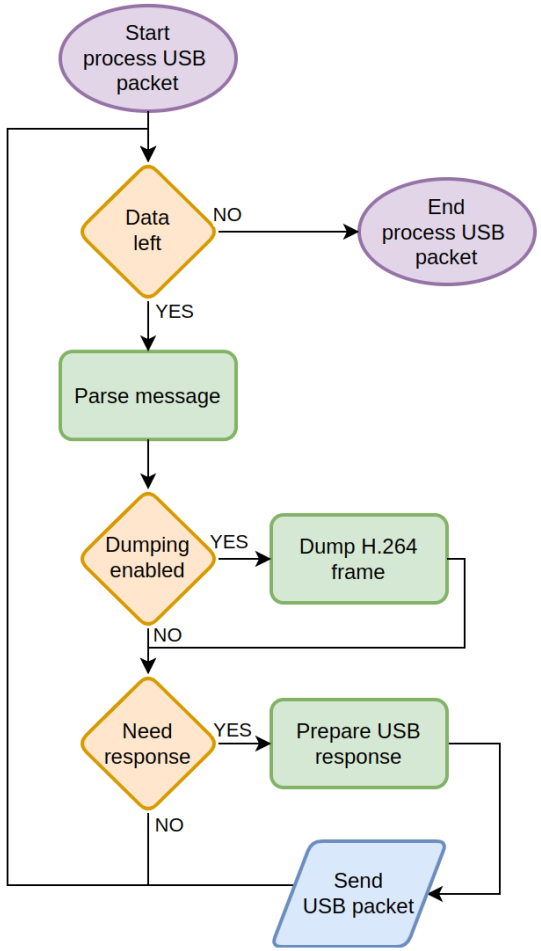
TuWire Nero Evaluation

Nero Implementation	Overall Handshake Time (ms)	Frames Throughput (kB/s)
Haywire	738.72	1680.67
TuWire without storing	136.72	1454.37
TuWire with flash memory	148.08	105.71
TuWire with SD card	159.87	387.74

Table: Handshake duration and frames throughput of the Haywire adapter and TuWire

Nero module


Start
Boot
Nero module
Release OUT
USB endpoint
Receive
USB packet
Block OUT
USB endpoint
Process USB
packet
Dumping
enabled
NO
YES
Enough
data
NO
YES
Shutdown
Nero module
End

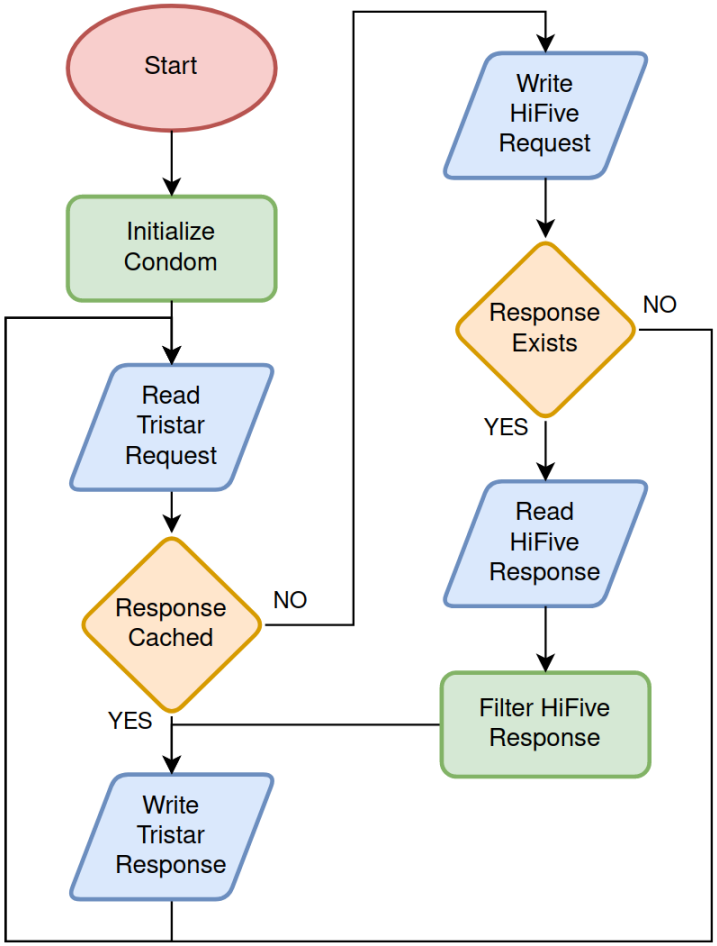

Start
process USB
packet
Data
left
NO
End
process USB
packet
YES
Parse message
Dumping
enabled
YES
Dump H.264
frame
NO
Need
response
YES
Prepare USB
response
NO
Send
USB packet

Lightning Condom Evaluation

IDBUS Transaction	Secure (us)	Insecure (us)	Overhead
Digital ID	9025	1140	7.91
Charging State	3398	589	5.76
Interface Details	5033	1314	3.83
Interface Module Number	7394	2230	3.31
Accessory Serial Number	7350	2230	3.29
Lightning Device State	3629	767	4.73
Apple System Info Notification	3606	953	3.78
Overall	39435	9223	4.27

Table: Message types and associated commands of the IDBUS protocol.

Condom flowchart



Further Work

- IDBUS and iAP protocol fuzzing
- TuWire Feed Streaming
  - stream video feed to cloud and analyze in near real-time
- Expand Device Compatibility
  - feedback loop between Nero feed and HID controller
- USB-C Connector
  - investigate if TuWire is applicable to iPhones

Bibliography I

[Ami18] Ramtin Amin. **Tristan**. https://web.archive.org/web/20180524101120/http://ramtin-amin.fr:80/tristar.html. Accessed: 2022-09-14. 2018.

[Kum20] Yuvraj Kumar. **Juice Jacking - The USB Charger Scam**. *Available at SSRN 3580209* (Apr. 2020).

[Loe+16] Edwin Lupito Loe et al. **SandUSB: An installation-free sandbox for USB peripherals**. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). 2016, pp. 621–626. DOI: 10.1109/WF-IoT.2016.7845512.

[Men+15] Weizhi Meng et al. **Charging me and I know your secrets! Towards juice filming attacks on smartphones**. Proceedings of the 1st ACM workshop on cyber-physical system security. 2015, pp. 89–98.

Bibliography II

[Sat] Nyan Satan. **Apple Lightning**. https://web.archive.org/web/20230211225113/https://nyansatan.github.io/lightning/. Accessed: 2022-09-14.

[sta22] stacksmashing. **The hitchhacker's guide to iPhone Lightning & JTAG hacking**. DEFCON 2022. 2022.