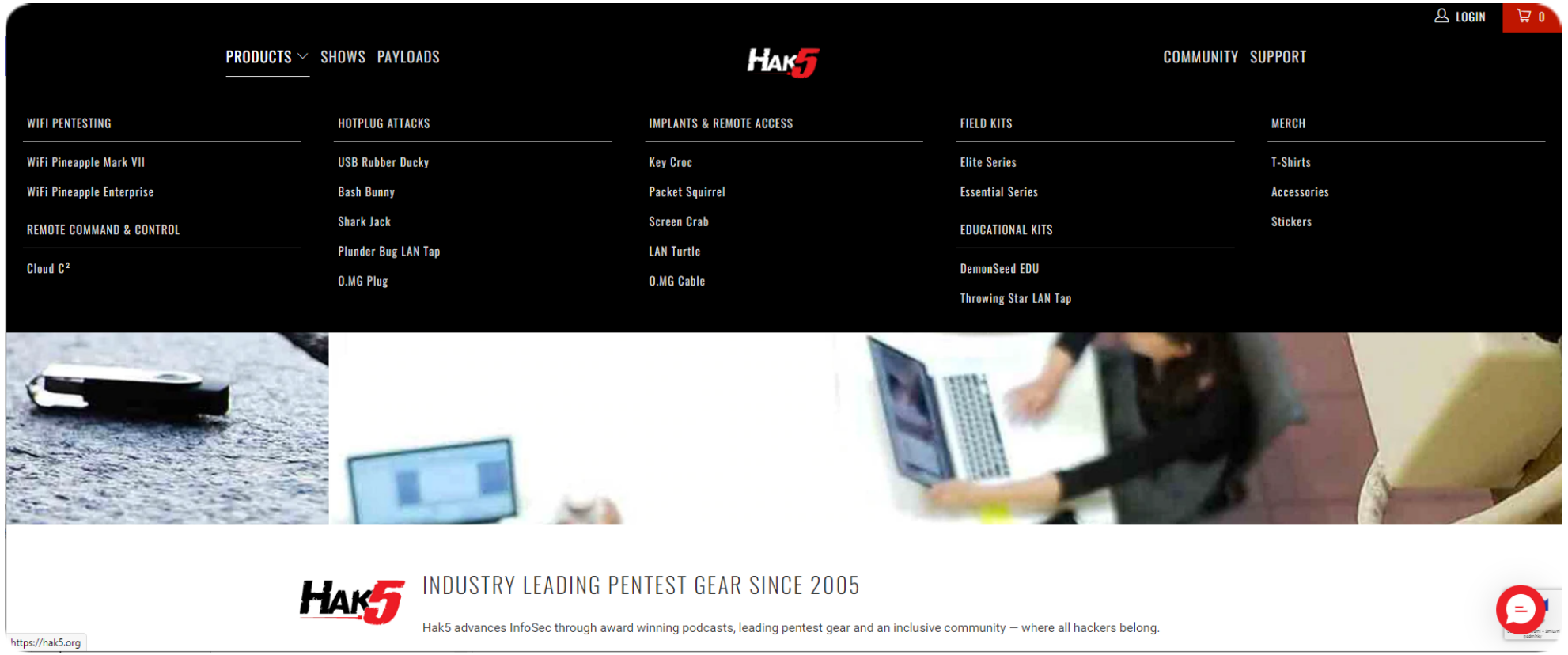
Electronic Attack Vectors

2023

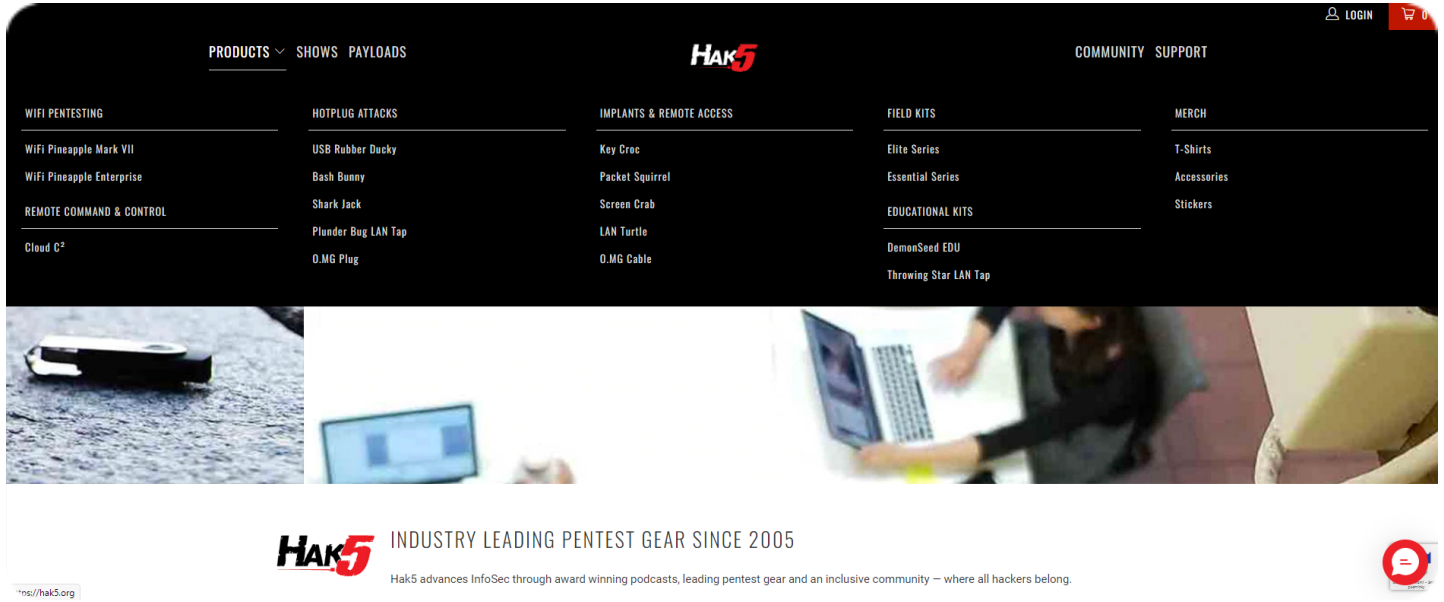
Tomas Rosa

Evaluation of Popular Red Team Toolbox Gadgets



Plausibility Analysis

1. Plausibility of the suggested scenarios
2. Technology limits
3. Detection
4. Countermeasures



Display Data

Imagine this would happen in CEO’s private meeting room

Screen Crab

Screen grabber for HDMI, based on Lontium chipset for signal bridging and conversion

Captures either single frames or video, results stored locally on SD card and possibly also at C2 cloud

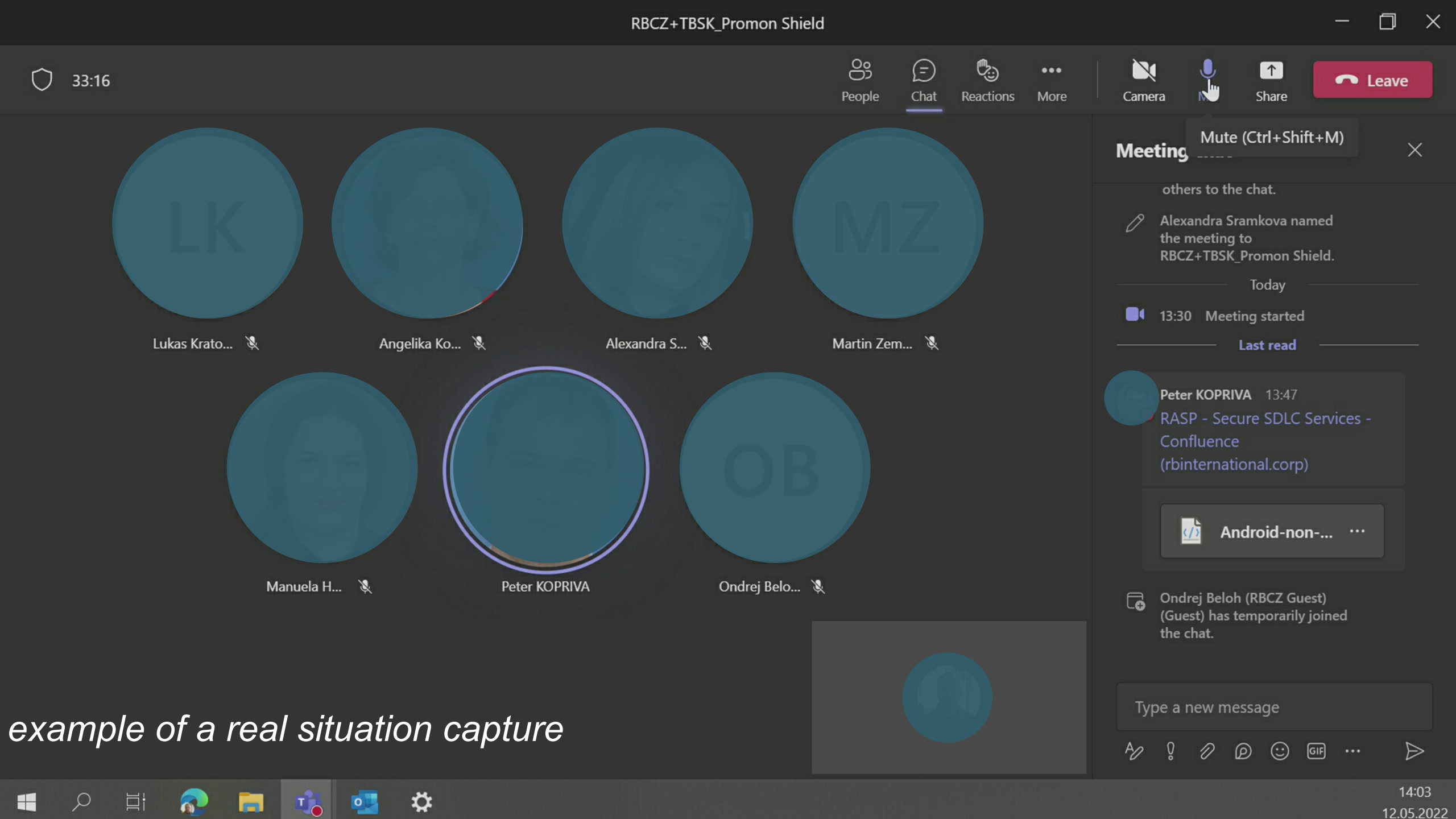
Remote management via C2 cloud

Plausibility Analysis

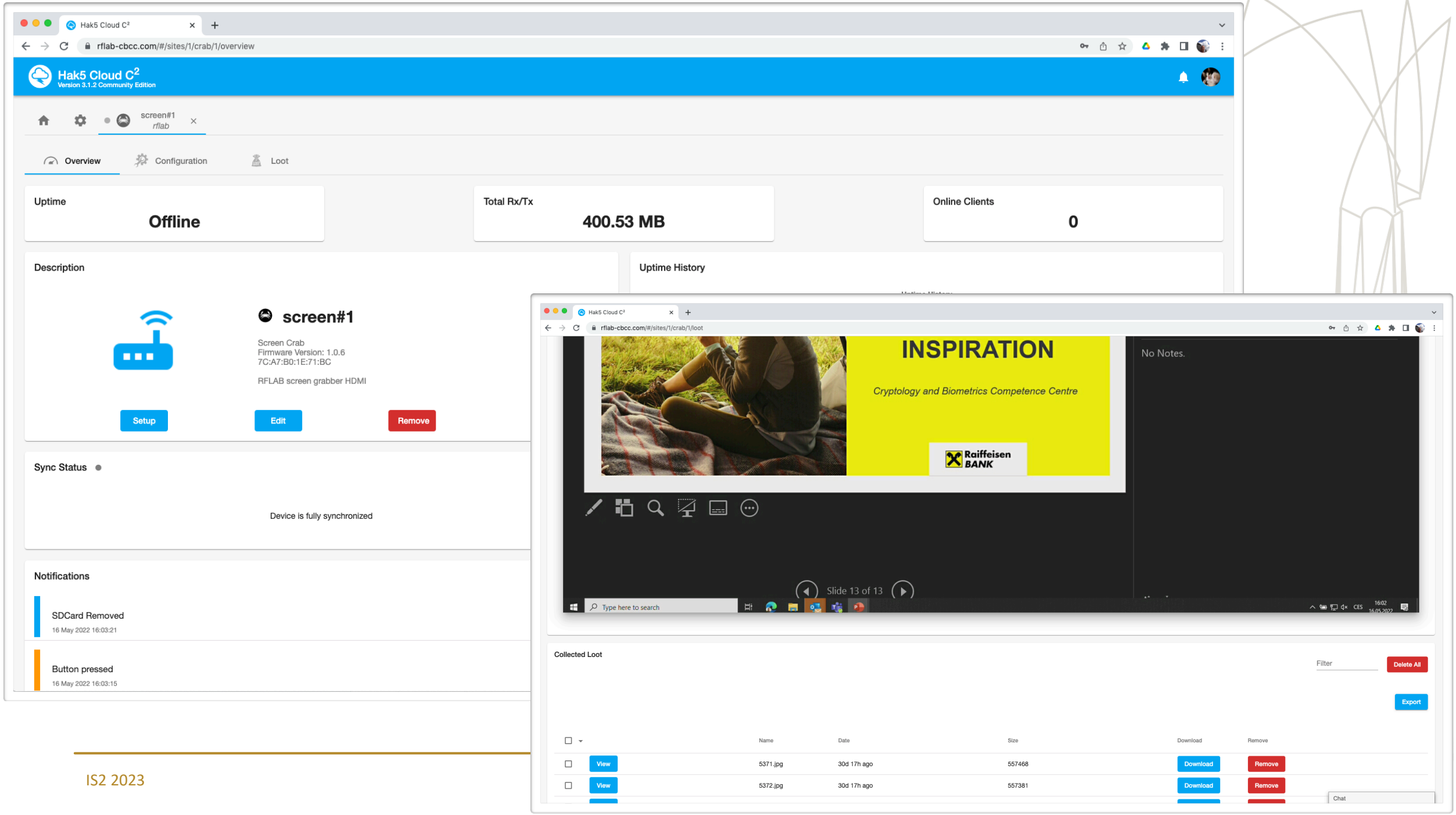
1. Plausible with small operational issues
2. HDMI signal is generally unprotected, certain limits are imposed by available chipsets
3. Can be detected as LONTIUM adapter
4. Consider encrypted video links for highly sensitive areas and regular physical inspection of exposed cables

screen crab

original parts



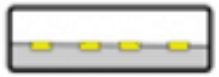
example of a real situation capture


Hak5 Cloud C²
rflab-cbcc.com/#/sites/1/crab/1/overview
Hak5 Cloud C²
Version 3.1.2 Community Edition
screen#1
rflab
Overview
Configuration
Loot
Uptime
Offline
Total Rx/Tx
400.53 MB
Online Clients
0
Description
screen#1
Screen Crab
Firmware Version: 1.0.6
7C:A7:B0:1E:71:BC
RFLAB screen grabber HDMI
Setup
Edit
Remove
Uptime History
Sync Status
Device is fully synchronized
Notifications
SDCard Removed
16 May 2022 16:03:21
Button pressed
16 May 2022 16:03:15
rflab-cbcc.com/#/sites/1/crab/1/loot
INSPIRATION
Cryptology and Biometrics Competence Centre
Raiffeisen BANK
No Notes.
Slide 13 of 13
Type here to search
Collected Loot
Filter
Delete All
Export
Name
Date
Size
Download
Remove
View
5371.jpg
30d 17h ago
557468
Download
Remove
View
5372.jpg
30d 17h ago
557381
Download
Remove
Chat

The Wonderful World of USB

USB 2.0 is getting old and dated, but its exploits are new and fresh

USB 1.0
12mbps



Type A

Type B

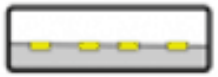
Mini-A

Mini-B

Micro-A

Micro-B

USB 2.0
480mbps



Type A

Type B

Mini-A

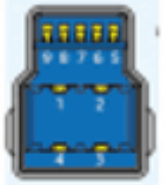
Mini-B

Micro-A

Micro-B

USB 3.1
Gen1
(Previously 3.0)
5gbps

Type A

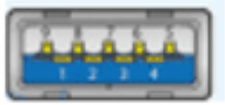


Type B

Mini-B

Micro-B

USB 3.1
Gen2
10gbps



Type A

Type-C

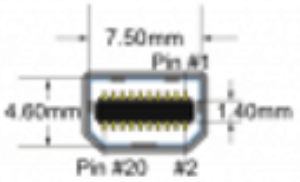
USB 3.2
20gbps

Type-C

Thunderbolt
2
20gbps

THUNDERBOLT

Mini DisplayPort
Connector

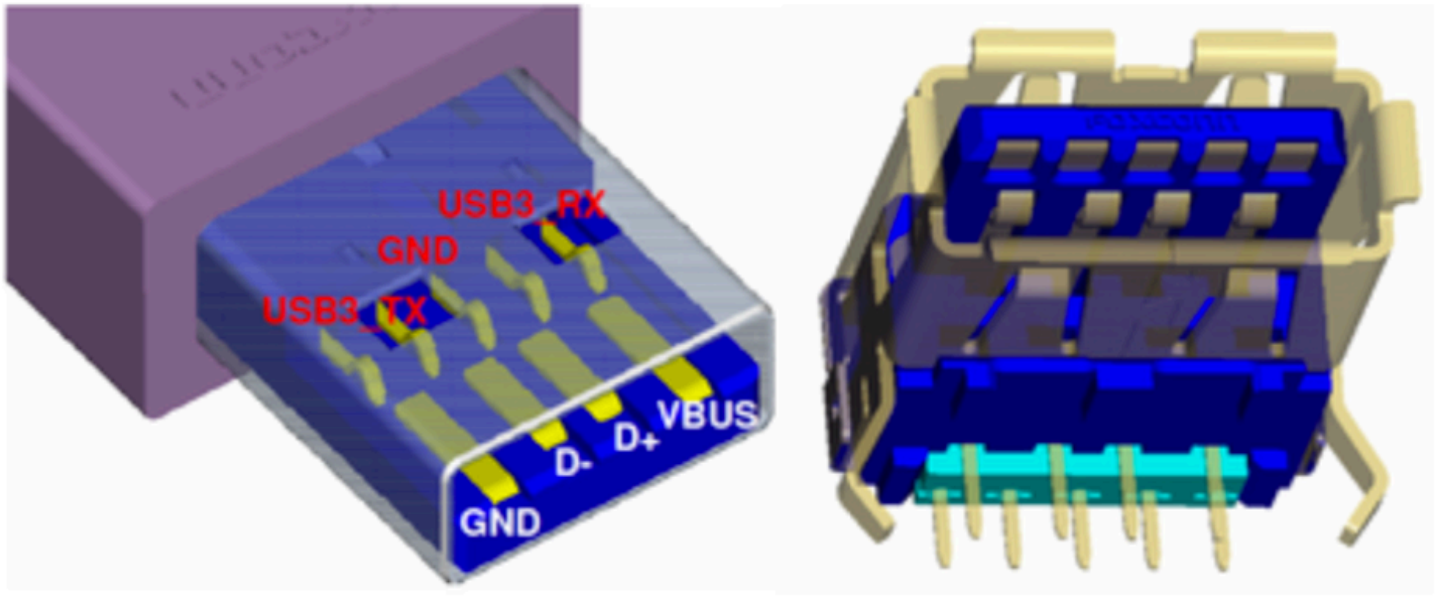


Thunderbolt
3
40gbps

THUNDERBOLT

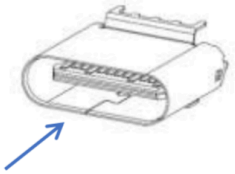
Type-C

Connector Stacking - USB 3.0/3.1 Example



USB Type-C® – Functional Model

- USB 3.2 / *USB4™* data bus
  - Two sets of TX/RX pin pairs, supports x1 and x2 operation
- USB 2.0 data bus
  - Two pin sets on host, one set on device – strapped together within the host and device
- Two power buses
  - VBUS and VCONN
- Two sideband pins (SBU1/SBU2)
  - *SBTX / SBRX for USB4*
- CC – Configuration Channel
  - Two CC pins in connector
  - One CC wire in cable



Looking into the product receptacle:

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
GND	TX1+	TX1−	VBUS	CC1	D+	D−	SBU1	VBUS	RX2−	RX2+	GND
GND	RX1+	RX1−	VBUS	SBU2	D−	D+	CC2	VBUS	TX2−	TX2+	GND
B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1

Looking into the cable or product plug:

A12	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1
GND	RX2+	RX2−	VBUS	SBU1	D−	D+	CC	VBUS	TX1−	TX1+	GND
GND	TX2+	TX2−	VBUS	VCONN			SBU2	VBUS	RX1−	RX1+	GND
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12

Lane 1 ***Lane 0***

O.MG Cables

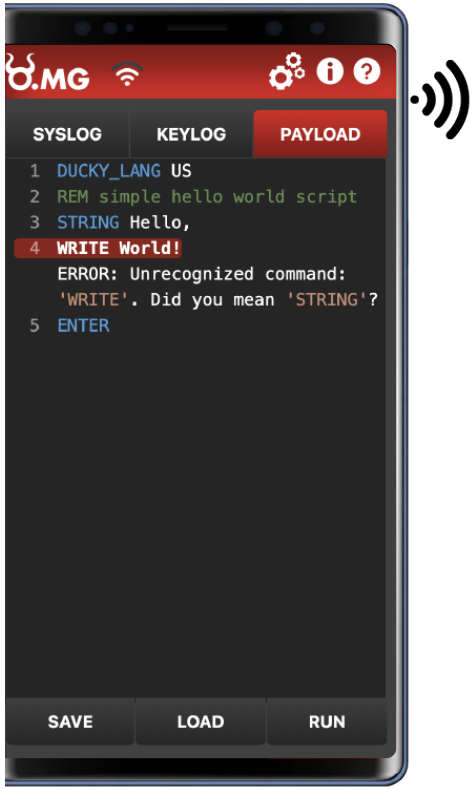
USB HID sniffing and data injection

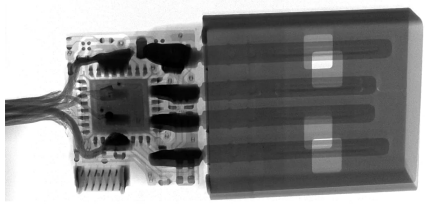
Remote control through embedded WiFi

Low-Speed device with certain Full-Speed sniffing capability, HID typing of 125 characters per second

Plausibility Analysis

1. Plausible, both attended and unattended scenarios
2. Low-speed bus profile limits the data capacity
3. There is an original forensic detector available (discerns active vs. passive cables); *the cable can stay totally quiet and show up for very a precise amount of time*
4. No robust prevention on the USB device layer, needs to be counted in





O.MG Cable Detector

Designed to discern active vs. passive cables based on power analysis on USB 2.0 power supply lines

Uses allowlists not to alarm on original active cables by Apple, etc.

Plausibility Analysis

1. Plausible, worked well with several different cables and devices
2. Its focus on power analysis is both the main strength and weakness
3. Challenging to do similar thing for USB-C
4. Malicious device designer viewpoint can move to USB-C, try to use a clever power management, or try to mimic those predefined original accessories templates to suppress alarms

Bash Bunny

High-Speed quad-core multi profile device, HID typing 570 chars/second

Payloads and exfiltration results stored locally on SD card

Remote connection possible via network tethering

Plausibility Analysis

1. Plausible, both attended and unattended scenarios
2. Big potential due to the **multiple profiles coherently acting together**
3. Detectable heuristically, O.MG cable detector does not apply
4. No robust prevention on the USB device layer, needs to be counted in

USB Rubber Ducky (2022)

HID emulator

Payloads and exfiltration results stored locally on SD card

High-Speed USB 2.0 device, A/C connector, HID typing 150 chars/second

Listens also to HID OUT endpoint for LED indicators broadcasts, simple coder/decoder is included with the base firmware

Plausibility Analysis

1. Plausible, both attended and unattended / dormant scenarios
2. Actually a prequel to Bash Bunny, inclusion of HID OUT makes it a budget and space saving alternative; sample exfiltration speed measured at 15.2 bps
3. Detectable heuristically on a device layer due to its somewhat exotic nature, O.MG cable detector does not apply
4. No robust prevention on the USB device layer, needs to be counted in

How to trap the active user?

AUDIOPi

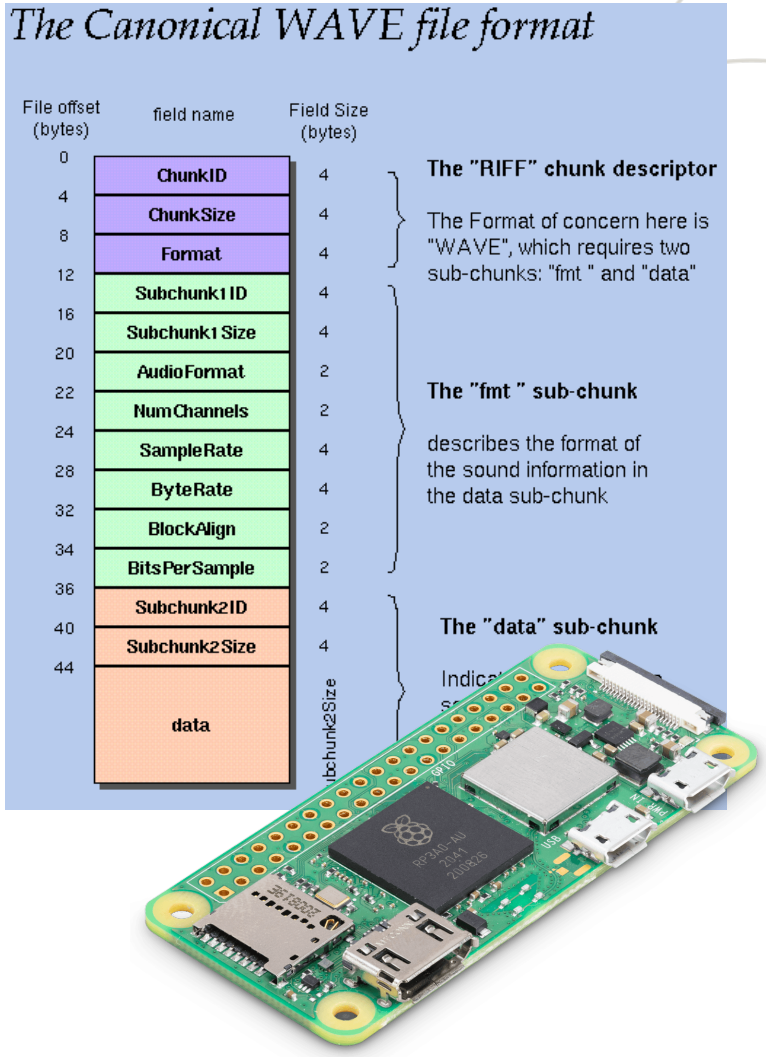
Fake audio card for fast-speed data transfer

Payloads and exfiltration results stored at SD card and-or transferred to C2

High-Speed USB 2.0 device, AUDIO profile, built on Raspberry Pi Zero 2 W

Plausibility Analysis

1. Plausible, both attended and unattended / dormant scenarios
2. Can be seen as yet another profile candidate for Bash Bunny, fully operable through PowerShell script
3. Detectable heuristically on a device layer due to a possibly unusual audio traffic
4. No robust prevention on the USB device layer, needs to be counted in



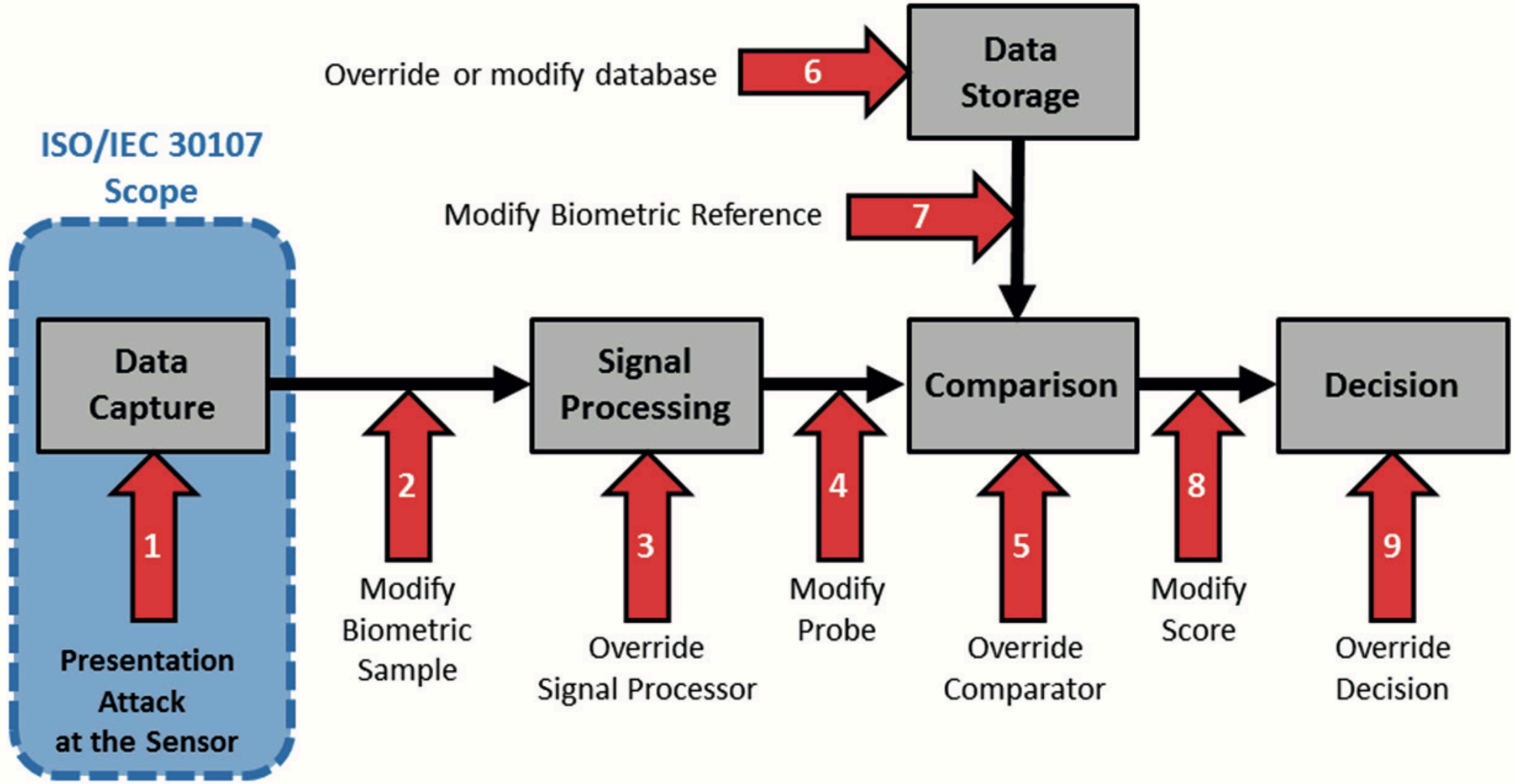
Mobile devices SW/HW integrity

Implications for biometrics

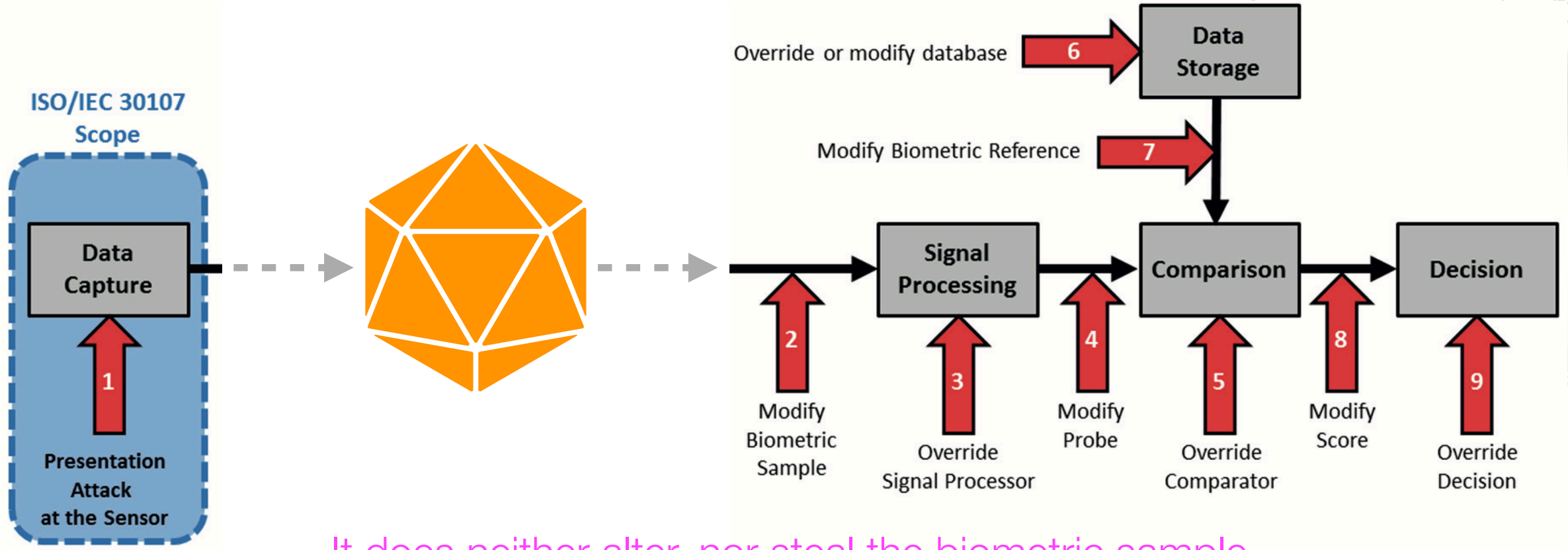
Remember

Attackers have their mobile devices **under their full control**

Biometric Spoofing Detection by ISO/IEC 30107



However, a wormhole attack is out of scope!



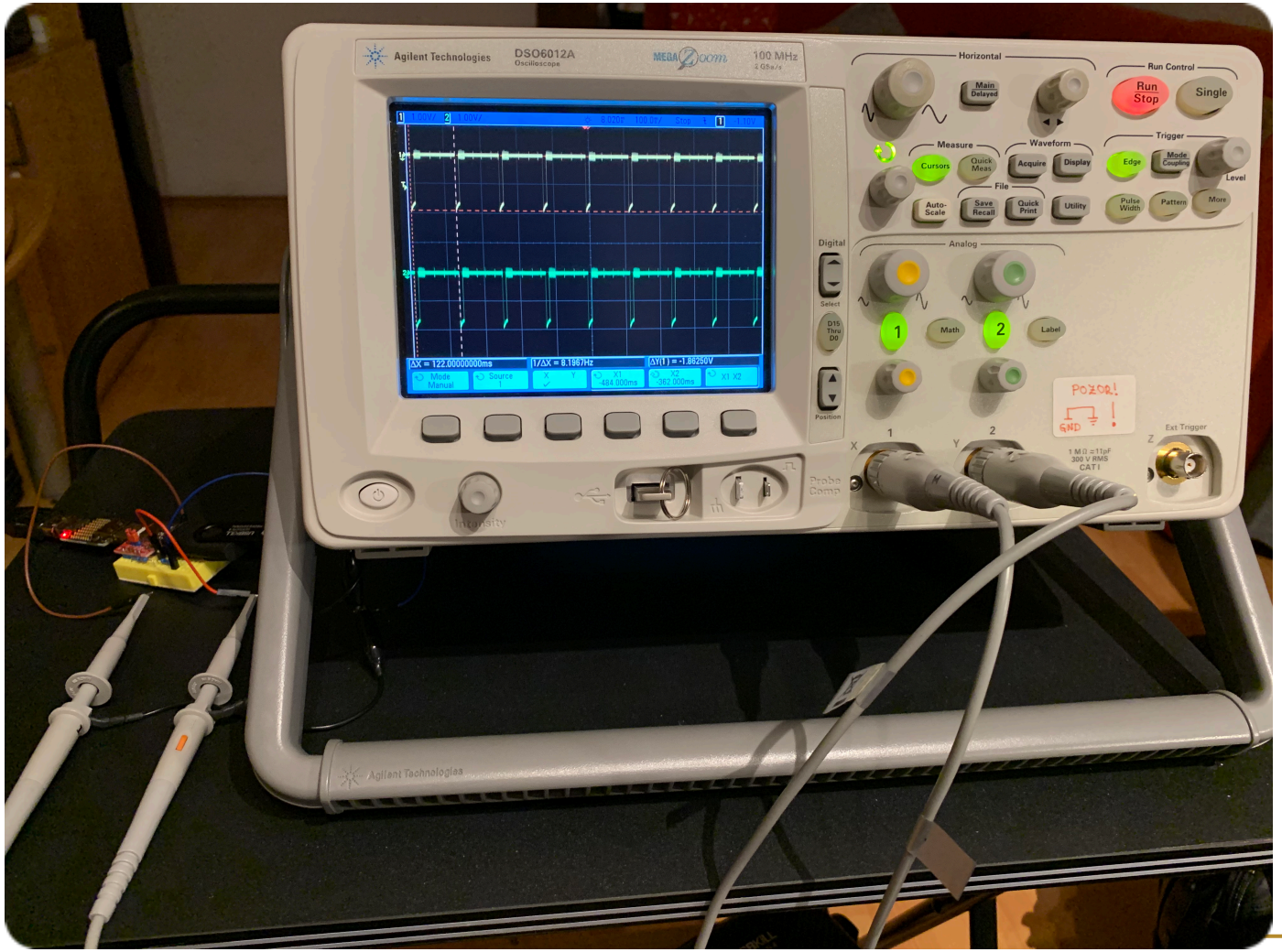
It does neither alter, nor steal the biometric sample.
It just makes two distant endpoints communicate like they were close together.

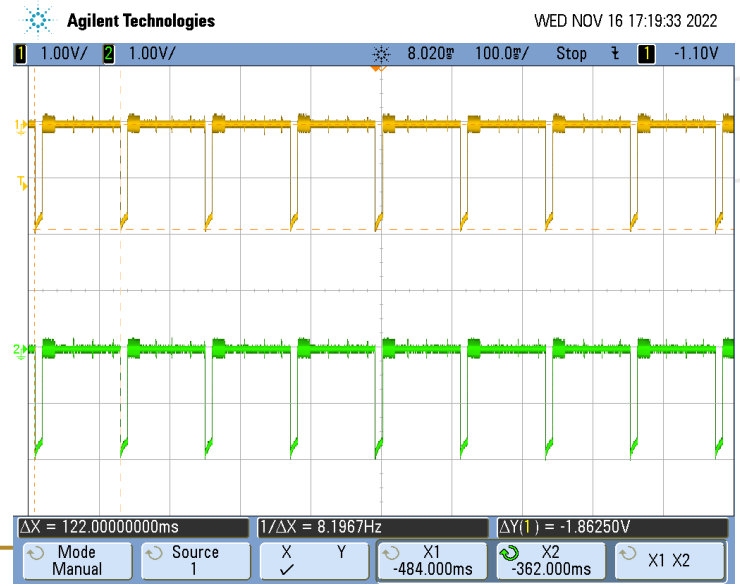
Should Everything Else Fail

DoS is always an option

USBKill

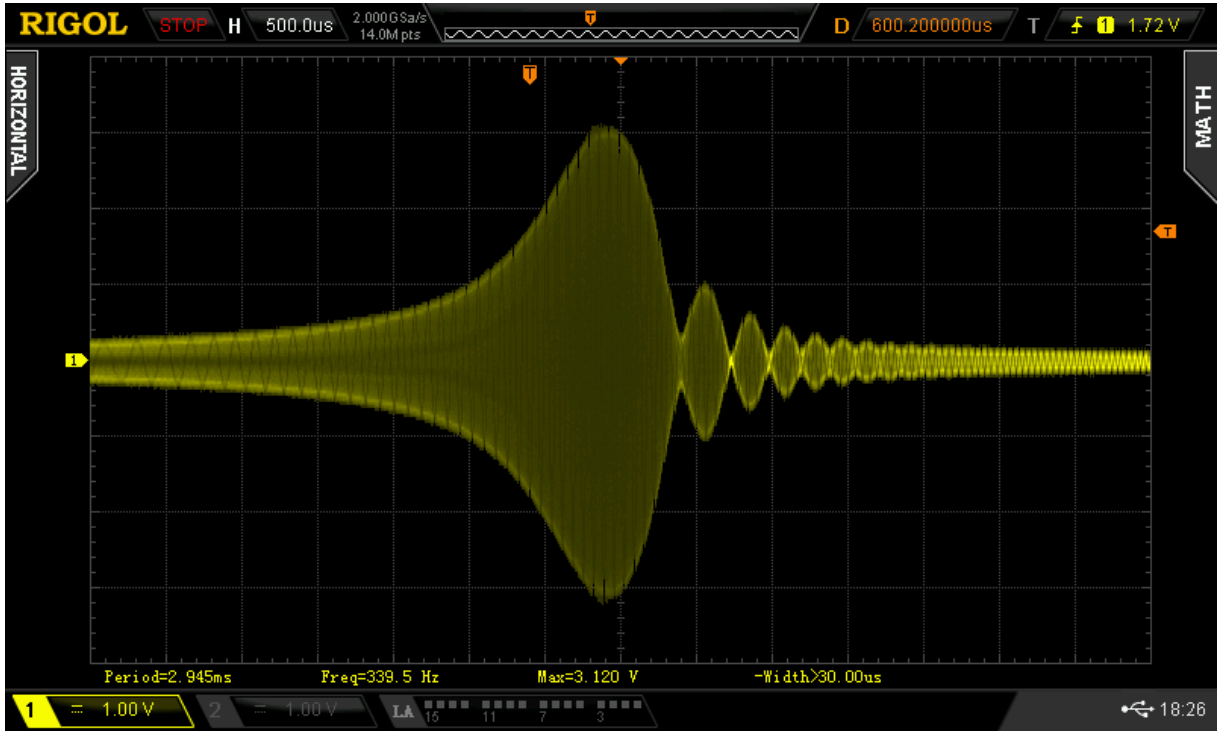
USB D+ and D-, vertical scale 101 V/div



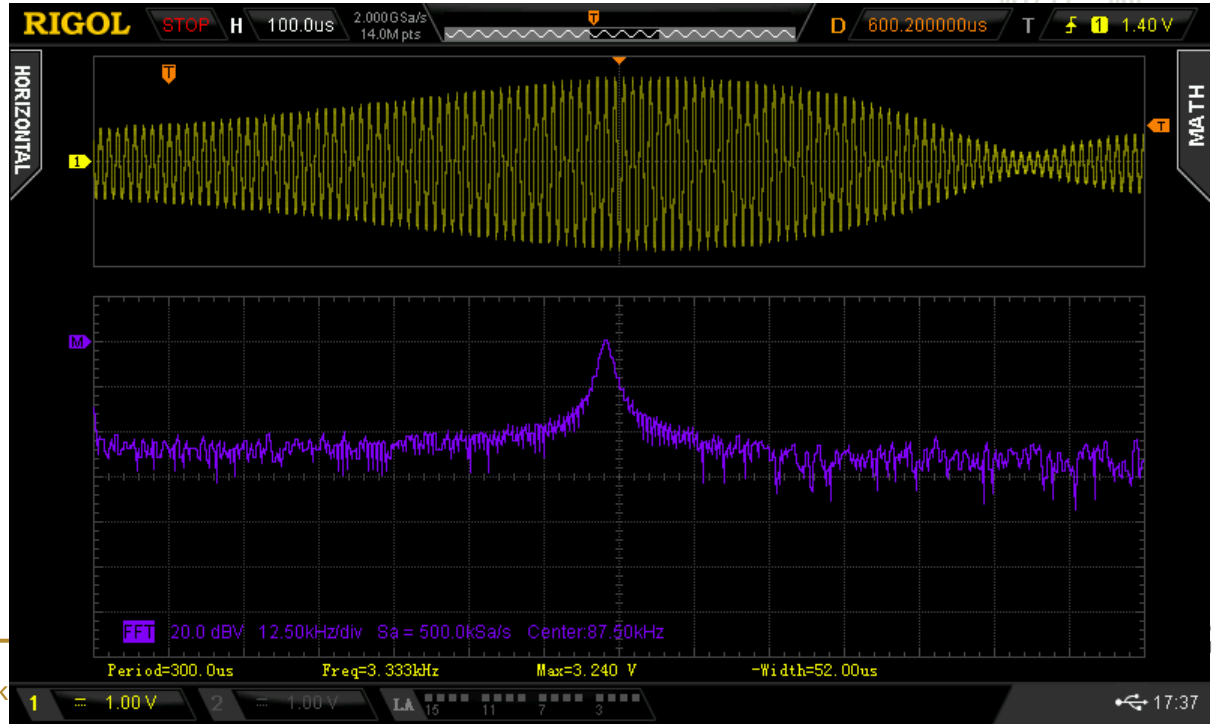


Contactless Micro-EMP Variant (NFCKill)

NFCKill Near-Field Magnetic Pulse (35 mm axial distance)



Probably, there is a high-voltage generator discharged instantly into a primary coil, producing typical high-energy transients



- Roughly 30-times higher peak value than for a regular NFC terminal (ACR122) in the same setup
- Will further raise sharply when approaching a closer distance
- Static discharge-like sensing observed at < 1 cm distance, their cause and effect remains unknown

Conclusion

It is the hardware integrity that can allow for software integrity, *not vice versa*