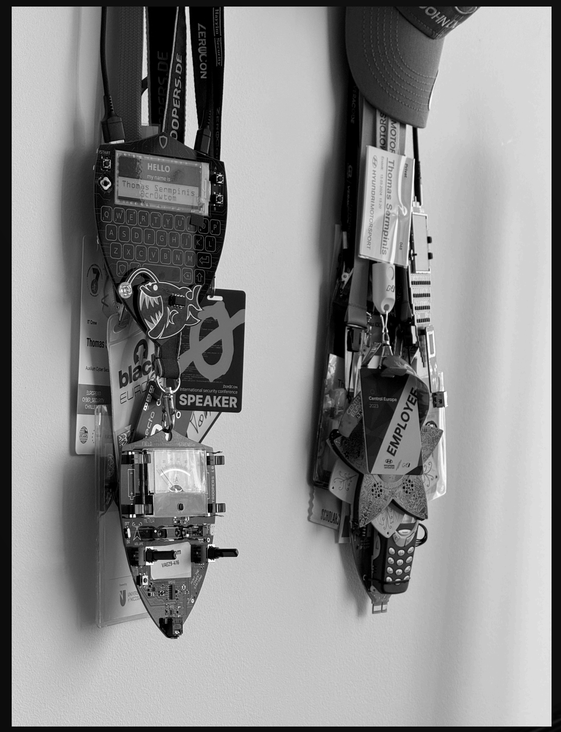
20
STARRING
THOMAS SERMPINIS
NEED FOR SPEED
THE FIGHT FOR OWNERSHIP

WHO AM I

- **Thomas Sermpinis (@cr0wtom)**
  - *Technical Director of Auxilium Pentest Labs by Day*
  - *Automotive Security Researcher by Night*
- **Hack Everything, Everywhere, All at Once (*and Legally*)**
- **Speaker and ASRG member**
- **For more: cr0wsplace.com**

AUXILIUM
Pentest Labs



Typhoon AUXILIUM Pentest Labs cr0w's place labs

GOALS

- Explore the world of tuning from a security researchers point of view
- Understand and analyse the state of automotive security, ownership and privacy
- Present unique (and hopefully interesting) real world use-cases
- Educate the new, the old and the bold
- Endorse and push more hackers to automotive

Typhoon AUXILIUM Pentest Labs cr0w's place labs

챕터 #0

THE STARTING LINE

DISCLAIMER

The researcher of this talk, has no actual experience, academic or technical, with actual vehicle tuning. His experience comes solely from security research and penetration testing in the automotive industry.

Apologies for any mistakes or misconceptions regarding tuning and the history of it. Please come find me after the talk in case you have any strong objections.

HISTORY LESSONS

HISTORY LESSONS

Early Modifications

17th - 18th
Century

Typhoon AUXILIUM Pentest Labs cr0w's place labs

HISTORY LESSONS

Early Modifications

17th - 18th Century

Hot Rodding

20th Century

Typhoon AUXILIUM Pentest Labs cr0w's place labs

HISTORY LESSONS

Early Modifications
17th - 18th Century

Hot Rodding
20th Century

Muscle Cars
50s - 60s

Typhoon AUXILIUM Pentest Labs cr0w's place labs

HISTORY LESSONS

- **Early Modifications** — 17th - 18th Century
- **Hot Rodding** — 20th Century
- **Muscle Cars** — 50s - 60s
- **Tuner Culture** — 70s - 80s

Typhoon AUXILIUM Pentest Labs cr0w's place labs

HISTORY LESSONS

Early Modifications	17th - 18th Century
Hot Rodding	20th Century
Muscle Cars	50s - 60s
Tuner Culture	70s - 80s
Import Tuning Scene	90s - 00s

Typhoon AUXILIUM Pentest Labs cr0w's place labs

HISTORY LESSONS

Early Modifications	17th - 18th Century
Hot Rodding	20th Century
Muscle Cars	50s - 60s
Tuner Culture	70s - 80s
Import Tuning Scene	90s - 00s
Drifting	90s

Typhoon AUXILIUM Pentest Labs cr0w's place labs

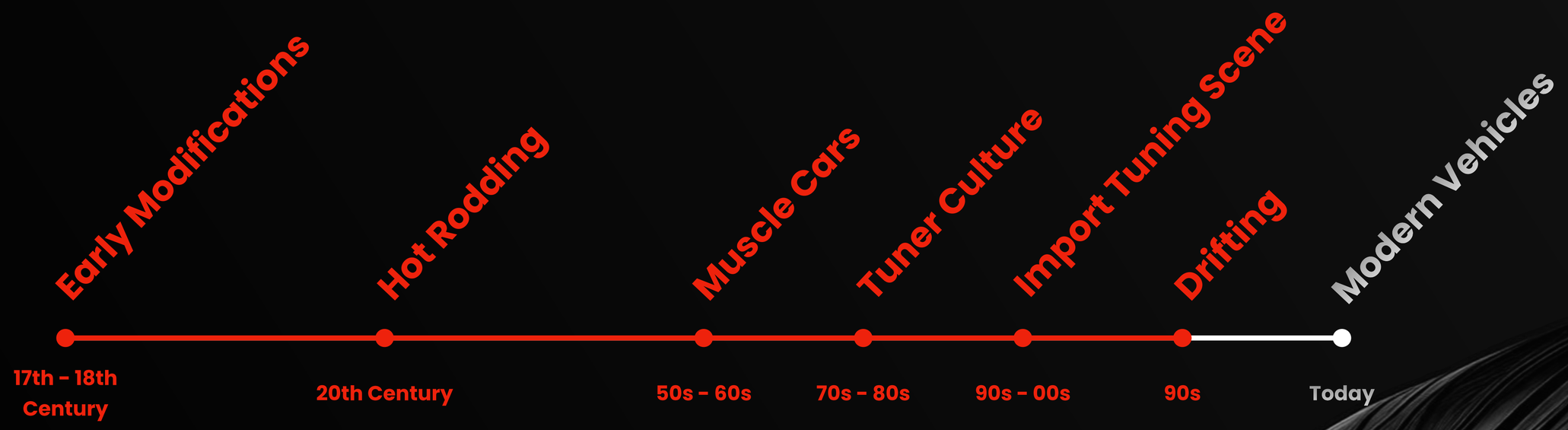
HISTORY LESSONS

Early Modifications	17th - 18th Century
Hot Rodding	20th Century
Muscle Cars	50s - 60s
Tuner Culture	70s - 80s
Import Tuning Scene	90s - 00s
Drifting	90s
Modern Vehicles	Today

Typhoon AUXILIUM Pentest Labs cr0w's place labs

HISTORY LESSONS

A SECURITY PERSPECTIVE



MODERN VEHICLES
A RETROSPECTIVE

- **Automotive OEMs and Suppliers**
  - Usually, 100+ year old industries or new "technology first" companies
  - Fundamental differences, resulting in different core values, and final results

- **Entertainment and constant need for connectivity, pushed both to implement technological advancements and integration**

MODERN VEHICLES

A RETROSPECTIVE

Typhoon AUXILIUM Pentest Labs cr0w's place labs

MODERN VEHICLES
A RETROSPECTIVE

SECURITY

Typhoon AUXILIUM Pentest Labs cr0w's place labs

MODERN VEHICLES
A RETROSPECTIVE

SECURITY OWNERSHIP

Typhoon AUXILIUM Pentest Labs cr0w's place labs

MODERN VEHICLES
A RETROSPECTIVE

SECURITY

OWNERSHIP

PRIVACY

Typhoon AUXILIUM Pentest Labs cr0w's place labs

MODERN VEHICLES
A RETROSPECTIVE

- **UN Regulation No. 155 - general requirements for Vehicle Cybersecurity**
  - Provides a set of standards that must be met in order to ensure the safety of road vehicles
  - The regulation requires the operation of a certified cybersecurity management system (CSMS)
  - Provides legal basis for so-called “Over-the-Air” (O.T.A.) updates to on-board vehicle software.
- **In summary:** Trying to shape the completely unregulated mess that exists right now

MODERN VEHICLES
A RETROSPECTIVE

- **Biggest caveats?**
  - Penetration testing is solely based on the Risk Assessment (TARA)
    - *No "real" security in the end*
  - Monitoring of vehicles has no "real" restrictions
    - *Opt-out is not really a "thing" at this point*
    - *Privacy is an afterthought, even considering that data shared are insignificant most of the times*
  - Ownership is not a matter of consideration when designing a vehicle with security in mind at this point

THE STATE OF OWNERSHIP

- **Complete Ownership**
  - All purely mechanical vehicles
  - Some modern vehicles with "focus" on tuning
    - e.g. Toyota Supra
  - Still requires a lot of reverse engineering to do something meaningful

- **Partial Ownership**
  - Vehicle is purchased and all features are accessible by the owner
  - Most systems are locked with proprietary measures
  - Altering those systems requires specialised equipment and significant reversing effort
  - Most modern vehicles

- **Zero Ownership**
  - Several functions are restricted under paywall
  - Strong security implementation
  - Backend connectivity requirement
  - OTA Updates for "bug" fixing
  - Monitoring and intrusion detection

THE STATE OF OWNERSHIP

- **Complete Ownership**
  - All purely mechanical vehicles
  - Some modern vehicles with "focus" on tuning
    - e.g. Toyota Supra
  - Still requires a lot of reverse engineering to do something meaningful

- **Full Ownership**
- **Full Privacy**
- **Zero Security**

- **Partial Ownership**
  - Vehicle is purchased and all features are accessible by the owner
  - Most systems are locked with proprietary measures
  - Altering those systems requires specialised equipment and significant reversing effort
  - Most modern vehicles

- **Zero Ownership**
  - Several functions are restricted under paywall
  - Strong security implementation
  - Backend connectivity requirement
  - OTA Updates for "bug" fixing
  - Monitoring and intrusion detection

THE STATE OF OWNERSHIP

- **Complete Ownership**
  - All purely mechanical vehicles
  - Some modern vehicles with "focus" on tuning
    - e.g. Toyota Supra
  - Still requires a lot of reverse engineering to do something meaningful

  - **Full Ownership**
  - **Full Privacy**
  - **Zero Security**

- **Partial Ownership**
  - Vehicle is purchased and all features are accessible by the owner
  - Most systems are locked with proprietary measures
  - Altering those systems requires specialised equipment and significant reversing effort
  - Most modern vehicles

  - **Partial Ownership**
  - **Full Privacy**
  - **Partial Security**[1]

- **Zero Ownership**
  - Several functions are restricted under paywall
  - Strong security implementation
  - Backend connectivity requirement
  - OTA Updates for "bug" fixing
  - Monitoring and intrusion detection

THE STATE OF OWNERSHIP

- **Complete Ownership**
  - All purely mechanical vehicles
  - Some modern vehicles with "focus" on tuning
    - e.g. Toyota Supra
  - Still requires a lot of reverse engineering to do something meaningful

  - **Full Ownership**
  - **Full Privacy**
  - **Zero Security**

- **Partial Ownership**
  - Vehicle is purchased and all features are accessible by the owner
  - Most systems are locked with proprietary measures
  - Altering those systems requires specialised equipment and significant reversing effort
  - Most modern vehicles

  - **Partial Ownership**
  - **Full Privacy**
  - **Partial Security[1]**

- **Zero Ownership**
  - Several functions are restricted under paywall
  - Strong security implementation
  - Backend connectivity requirement
  - OTA Updates for "bug" fixing
  - Monitoring and intrusion detection

  - **Zero Ownership**
  - **Zero Privacy**
  - **Good Security[1]**

챕터 #1

THE WHEEL SPIN

And how I got into the car tuning community.

MY STORY

NDA

MY STORY

ebay Shop by category

ecu | All Categories | Search | Advanced

Related: ecus & computer modules · east carolina university · ecm · pcm · ecu pirates · engine control module · ecus, cdis & computer modules · east carolina ... Include description

Category

- All
- eBay Motors
  - Car & Truck ECUs & Computer Modules
  - Car & Truck Oxygen Sensors
  - Motorcycle & Scooter ECUs, CDIs & Computer Modules
  - Other Auto Performance Electrical Components
  - Other Automotive Diagnostic Service Tools
  - More +
- Coins & Paper Money
  - France Coins
- Show More +

Brand

- BMW (59,300)
- Chevrolet (29,491)
- Dodge (39,580)
- Ford (120,808)
- Honda (31,856)
- Mercedes-Benz (42,142)
- Nissan (51,425)
- Toyota (58,210)

see all

Type

NextGear Auto Parts | Cars - Trucks
49K items sold
Shop Store on eBay→
Sponsored

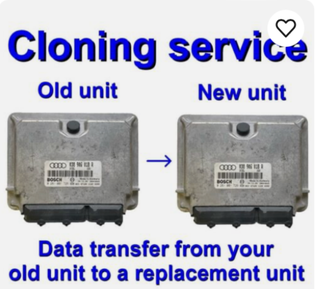
1,900,000+ results for ecu | Save this search | Shipping to Greece

All | Auction | Buy It Now | Condition | Delivery Options | Sort: Best Match

Find parts that fit

We need more information about your vehicle to confirm fit.

Year | Make | Model | Trim | Engine | Add vehicle

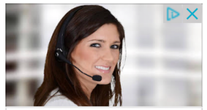


VAG (VW+AUDI+SEAT+SKODA) ECU/PCM EDC17 MED17 ECU cloning service / Immo data
New (Other)

EUR 104.07
or Best Offer
+EUR 24.64 shipping estimate
from United Kingdom
10 watchers

Customs services and international tracking provided
bestpricepartsuk (377) 100%

Sponsored



Chat with an expert Online Now

A Technician Will Answer Your Questions in Minutes. Chat Now.

JustAnswer

Open

MY STORY

ebay

Hi Serbinis, your order is being shipped!

Tracking Number: [redacted]

Track order

Tracking data usually becomes available within a few hours after the shipment.

Your order will ship to: [redacted]

Estimated delivery: [redacted]

JAGUAR F TYPE CONVERTIBLE 3.0 TELEMATICS CONTROL MODULE DPLA70718NP

Total: GBP 25.00
Order number: [redacted]
Item ID: [redacted]
Seller: ek_autoparts

ebay MONEY BACK GUARANTEE

MY STORY

OPEN QUESTIONS

- PIN mapping?
- Power requirements?
- Wake-up sequence?
- Communication endpoints?

OPEN QUESTIONS

Where do we actually start from?

THE HARDWARE

- **Hardware is usually the last resort during our penetration testing projects**
  - And the one where most mistakes are made
  - Higher chances of getting full access to the unit (or the underlying firmware)
  - In cases that critical information is required, hardware evaluation might come as the first step
    - *e.g. missing knowledge of start up sequence*

HARDWARE TESTING CHECKLIST

- Analyse the target board
- Analyse the hardware components
- Find schematics and data-sheets online
- Discover testing points and map them to the hardware components
- Find the proper debugger and connect to the testing points
- Bypass the protections (if any) and elevate your access to the target

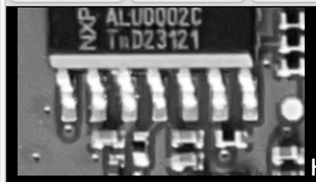
dnt
QUALCOMM
MDM6200
BN7-9
E241200
OK
JBC
OK
multicomp PRO

File Edit Insert Format Tools Tree Search View Bookmarks Help

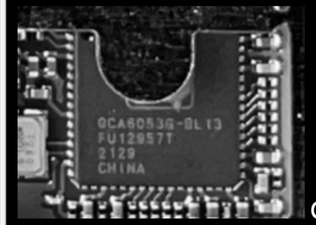
- BMW - RR ECU
  - Hardware Enumeration
  - Harware
    - SoCs

Harware | Hardware En... | BMW - RR ECU

BMW - RR ECU / Harware / SoCs

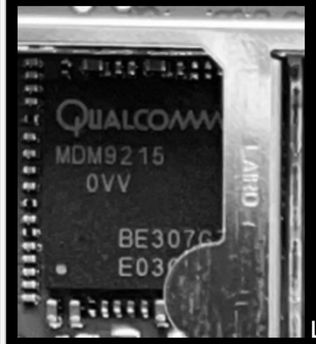


High-Speed CAN Transceiver with Standby and Sleep Mode
https://www.nxp.com/docs/en/data-sheet/TJA1043.pdf



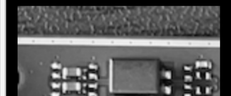
Qualcomm® APQ8053 SoCs for IoT
https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/apq8053-socs-product-brief_87-pg760-1-b.pdf

---

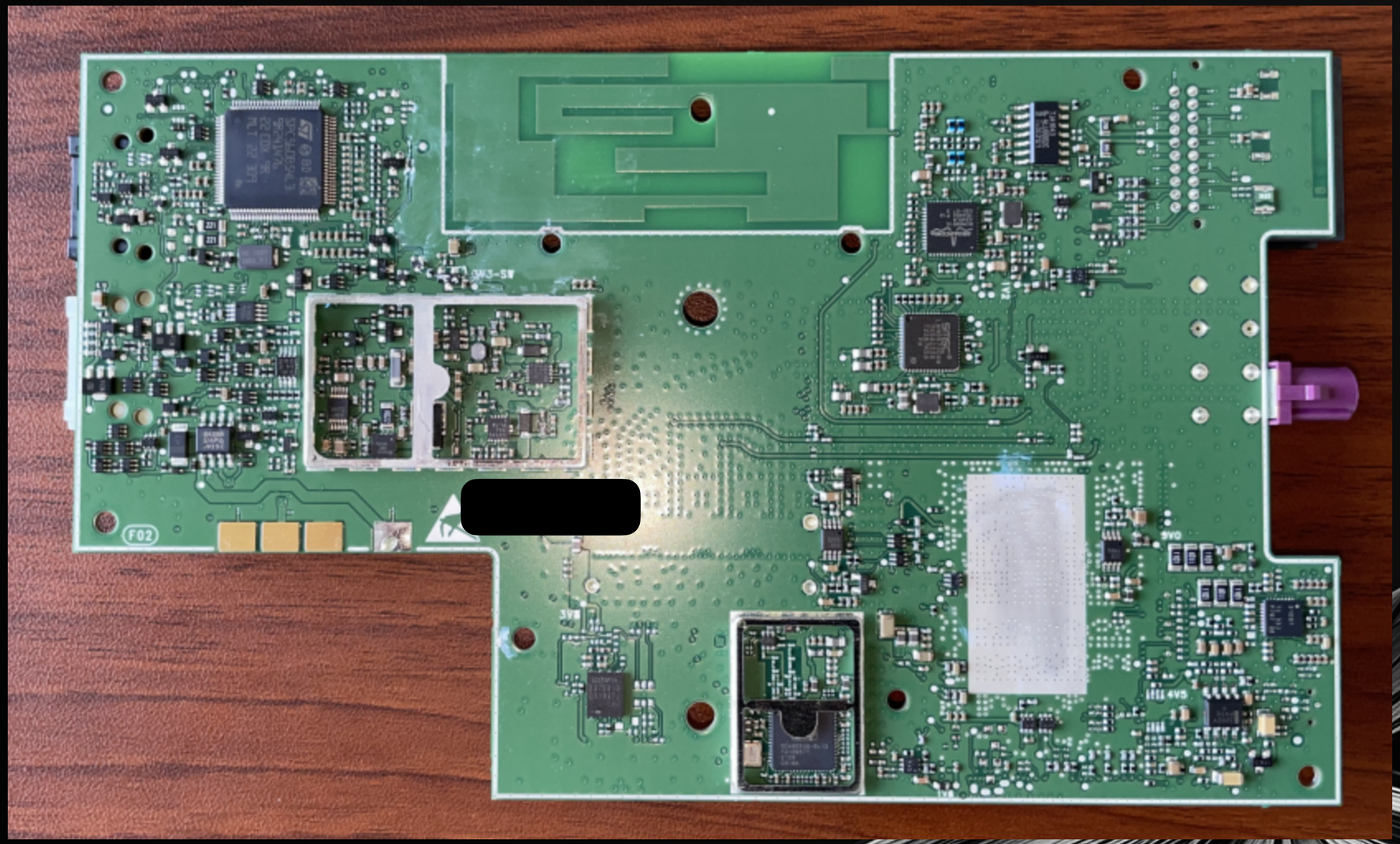


LTE/4G Modem Chip

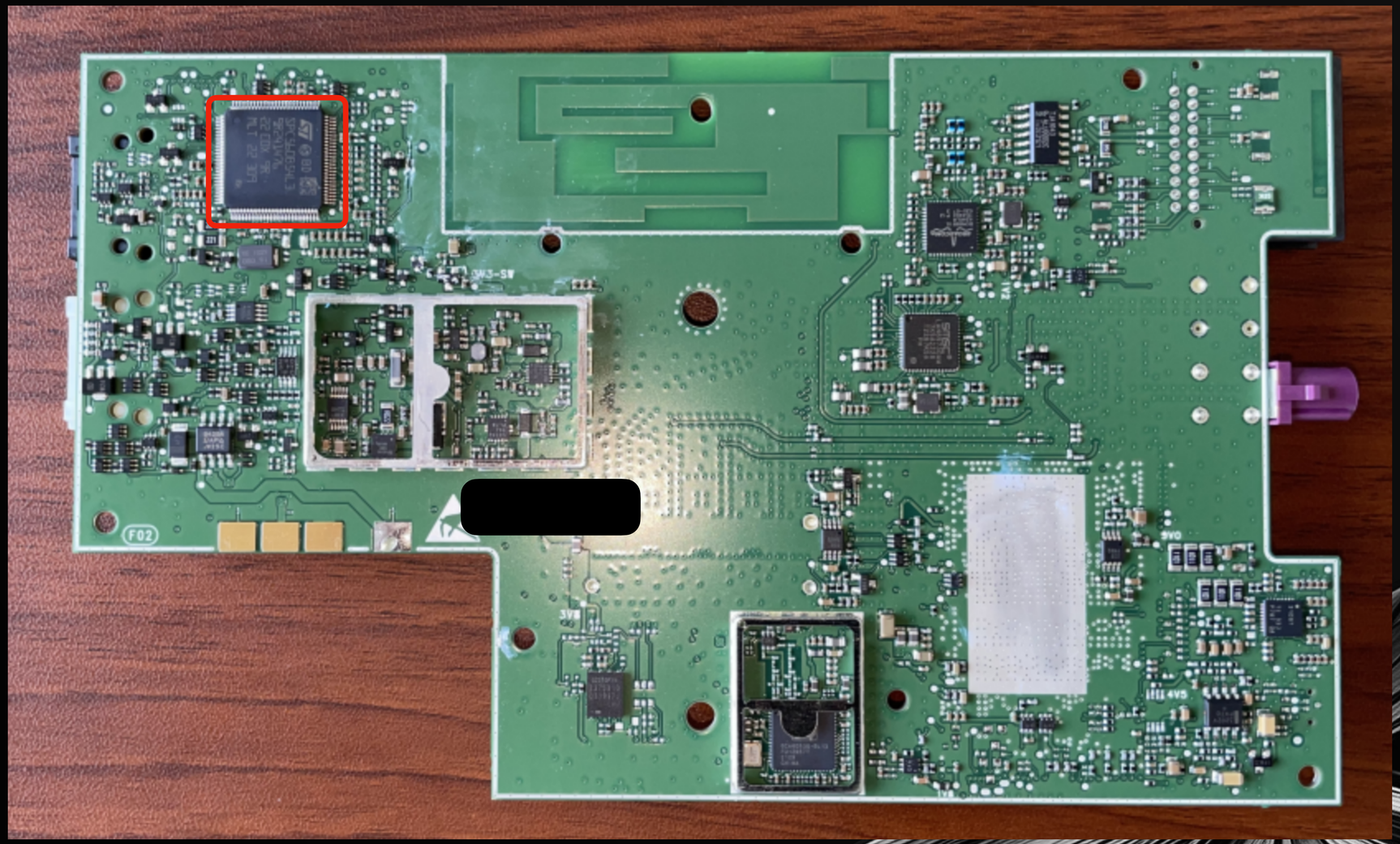
CMOS QUAD 2-INPUT NAND SCHMITT TRIGGER
https://www.ti.com/lit/ds/symlink/cd4093b-q1.pdf?ts=1694496622695



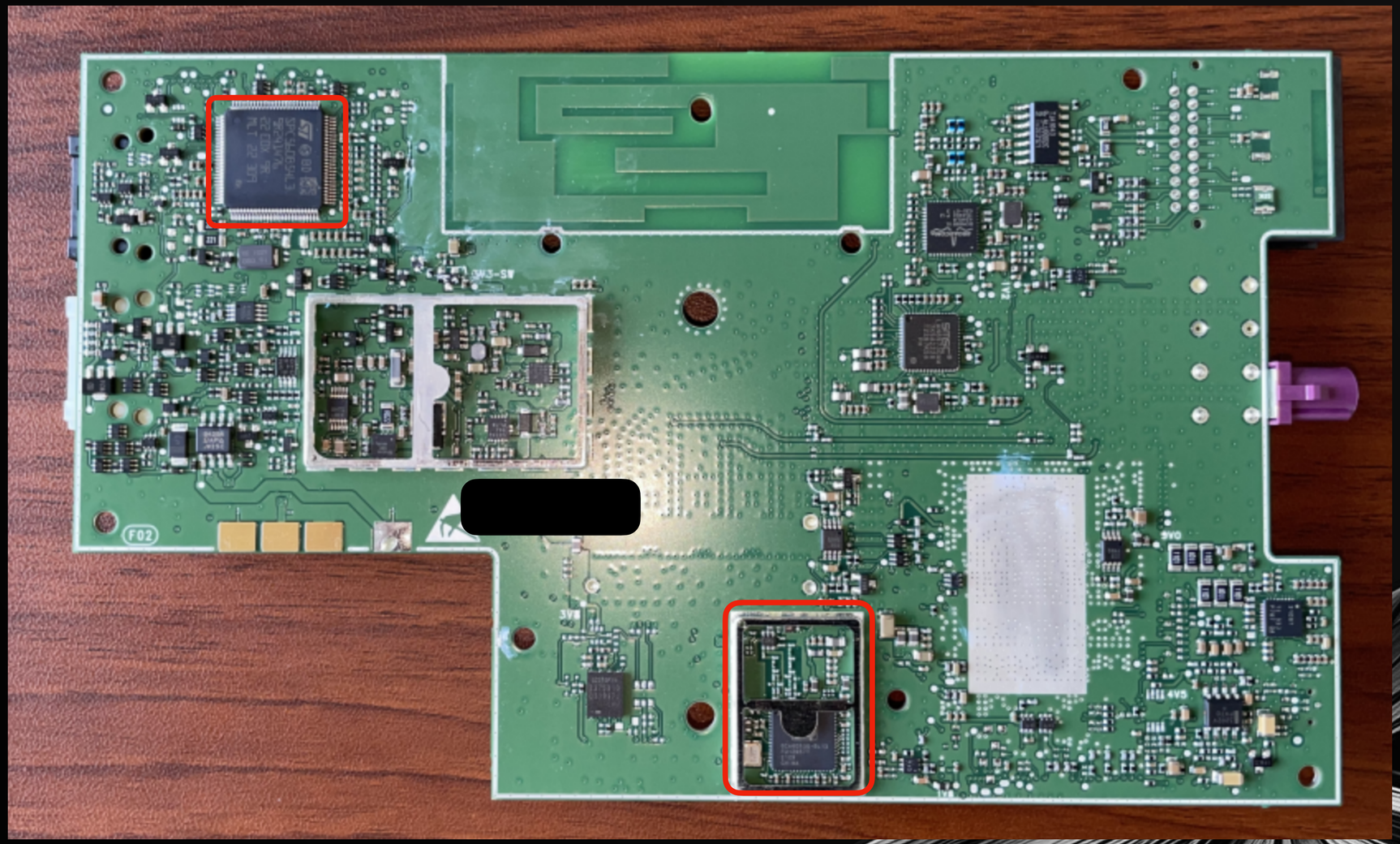
THE HARDWARE



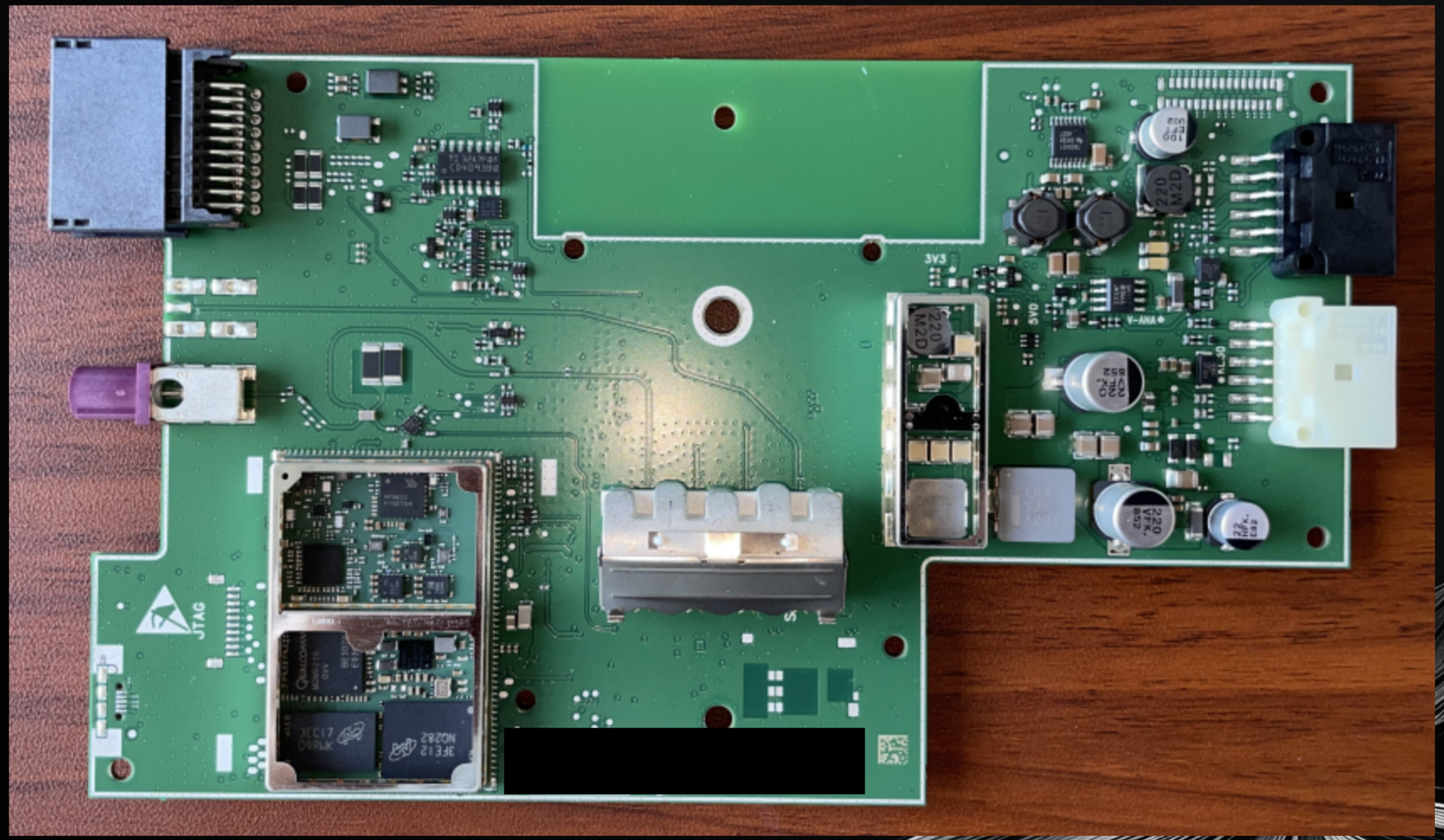
THE HARDWARE



THE HARDWARE

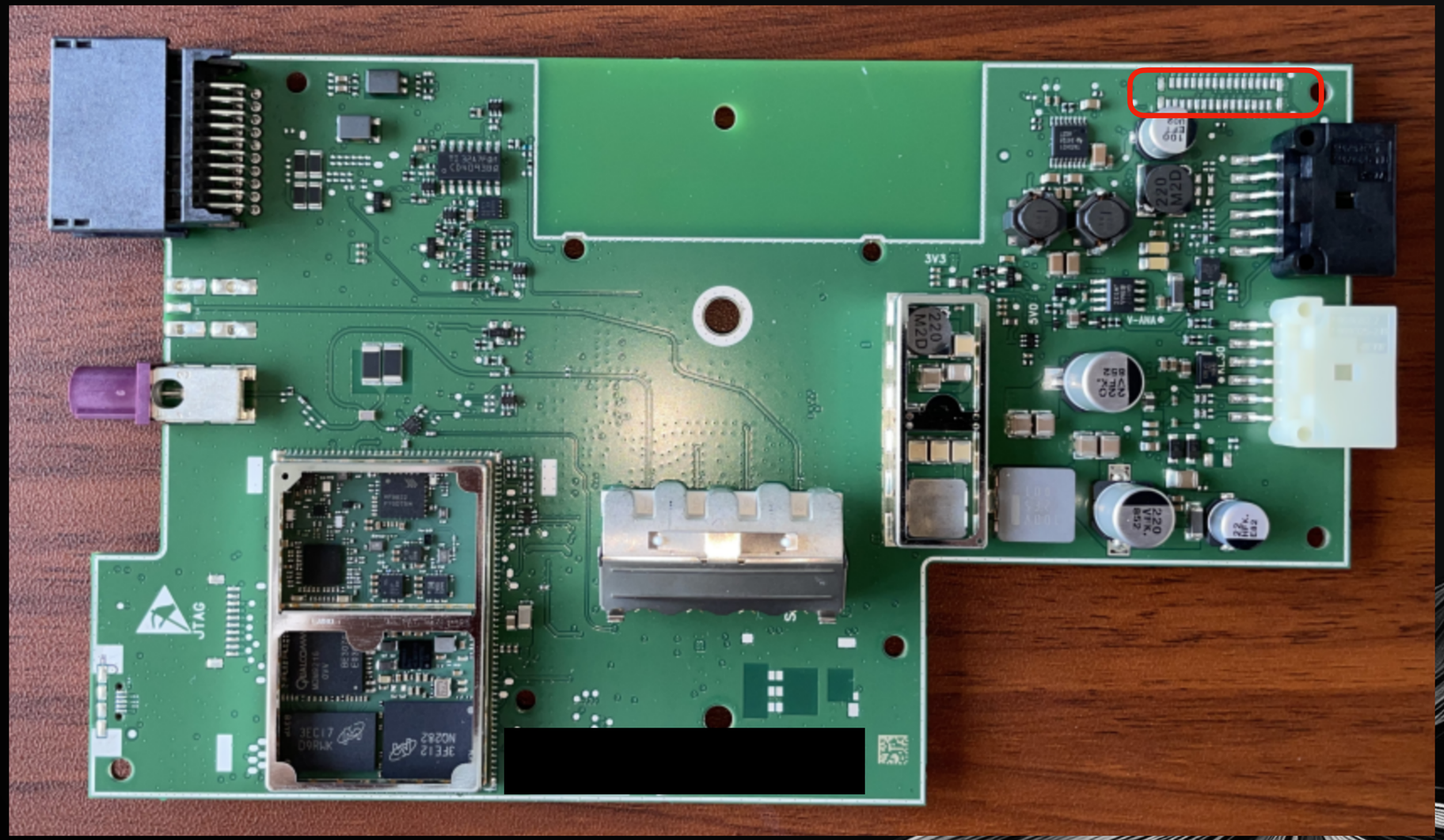


THE HARDWARE



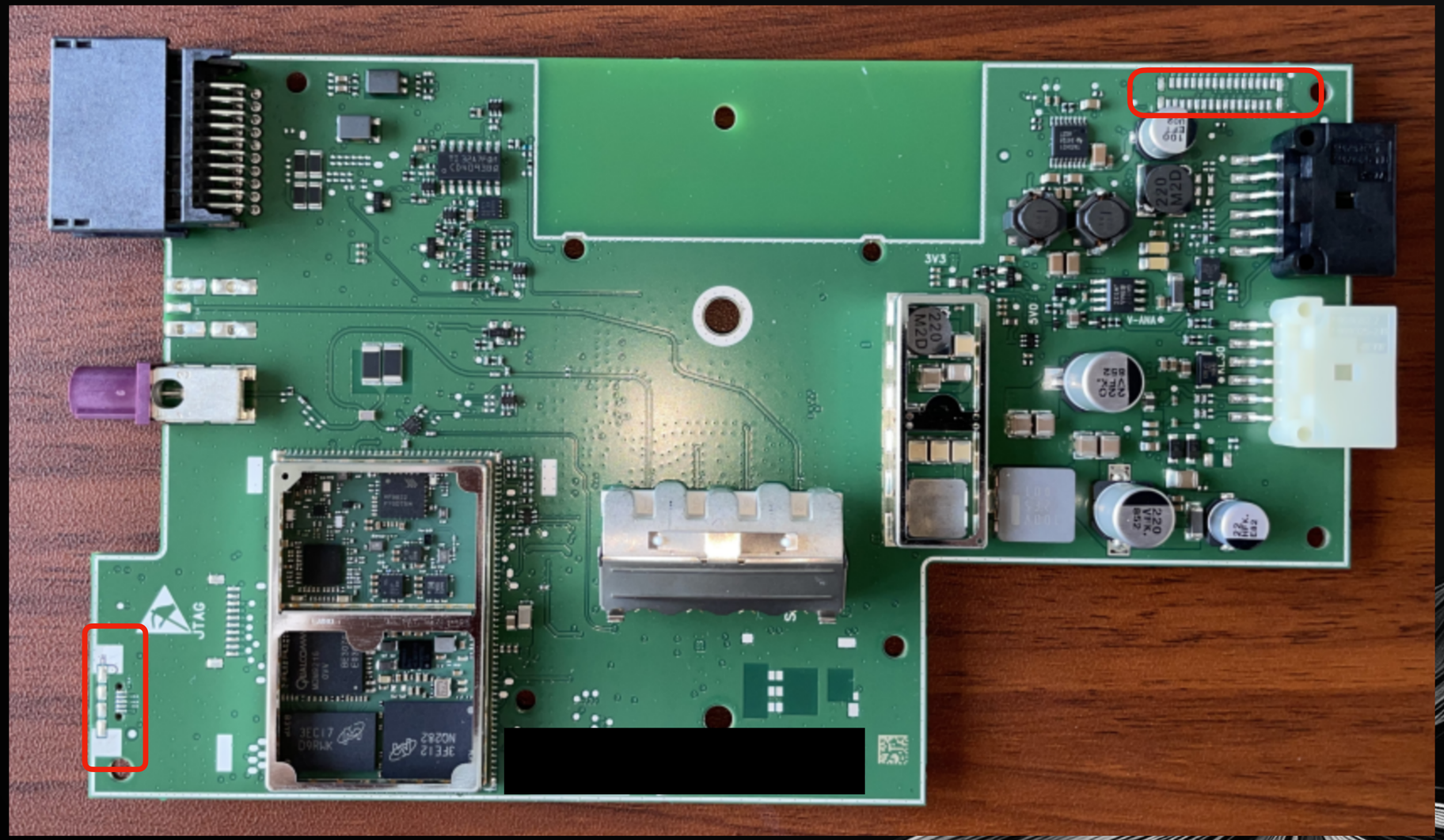
Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

THE HARDWARE



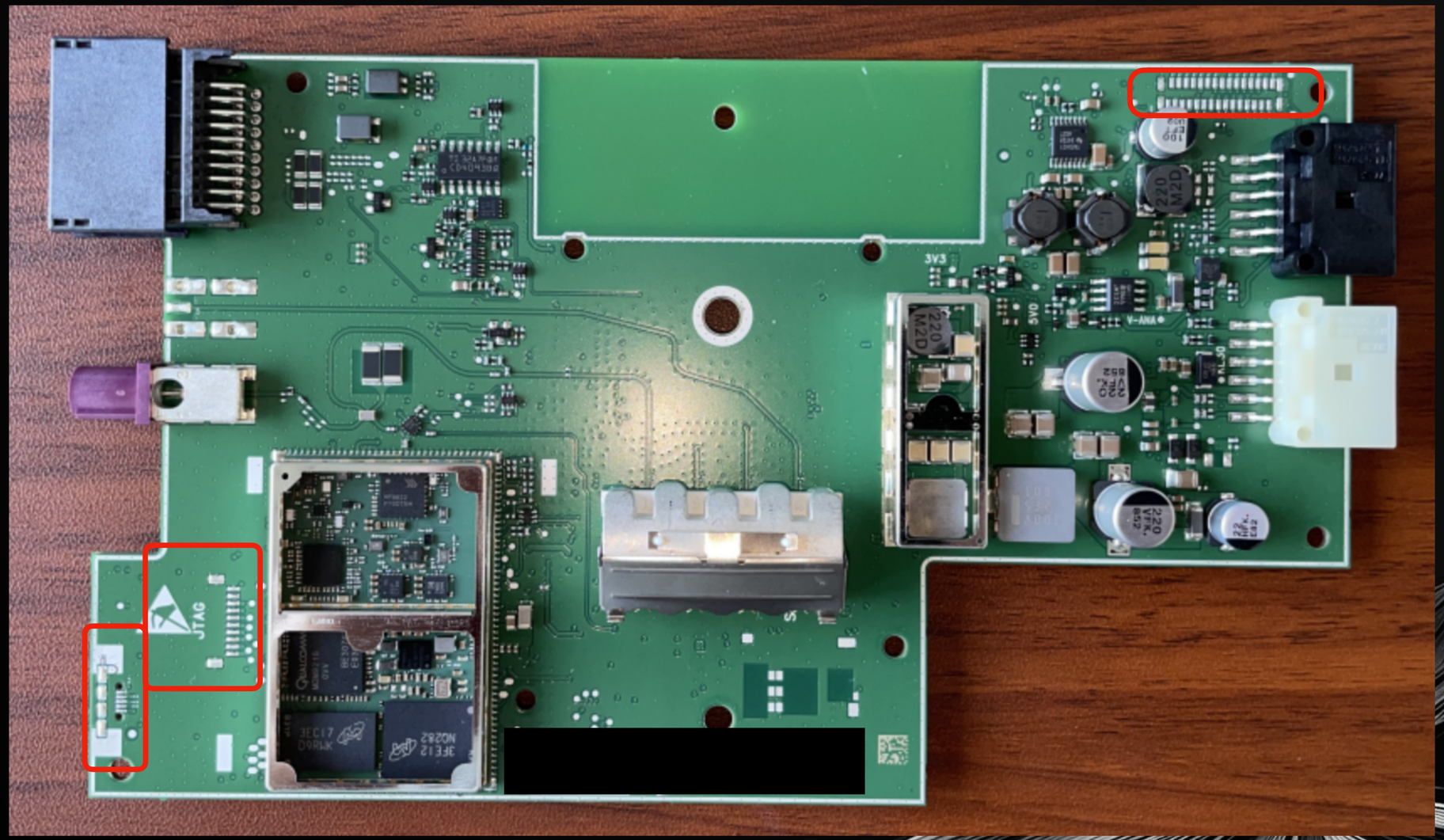
Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

THE HARDWARE



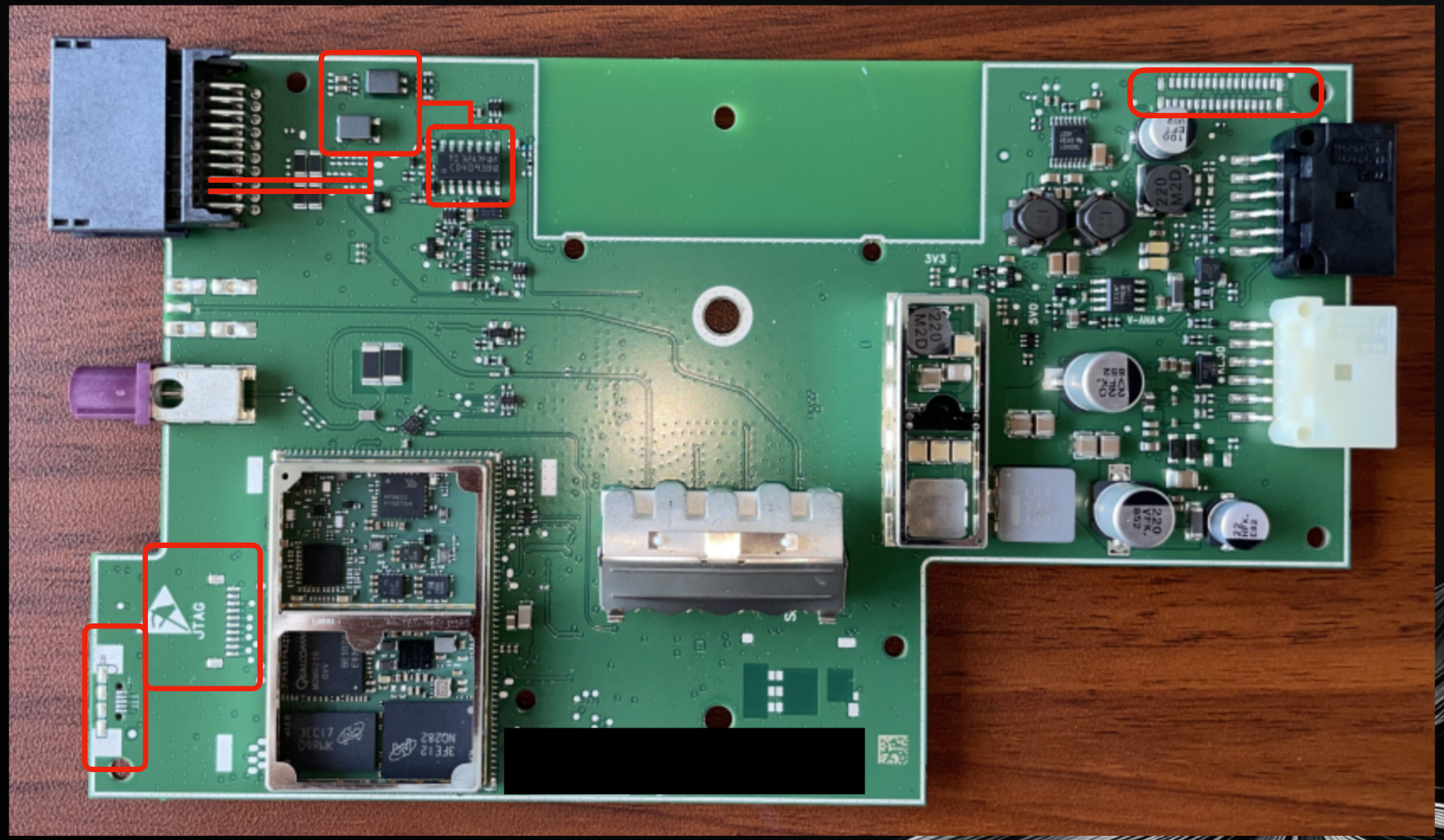
Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

THE HARDWARE



Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

THE HARDWARE



Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

THE HARDWARE

```
  File "/home/tsermpinis/.local/lib/python3.11/site-packages/can/interfaces/socketcan/socketcan.py", line 794, in _send_once
    raise can.CanOperationError(
can.exceptions.CanOperationError: Failed to transmit: No buffer space available [Error Code 105]
```

Supersprint
Jaguar Forums
register now

10-24-2023, 03:55 AM #1

Cr0wTom
Junior Member
Thread Starter

Join Date: Oct 2023
Location: Prague
Posts: 5
Likes: 0
Received 0 Likes on 0 Posts

Direct Connection to F-Type TCU?

Hello everyone,

I am a researched and enthusiast, and I just bought a JAGUAR F TYPE CONVERTIBLE 3.0 TELEMATICS CONTROL MODULE. I am pretty sure it's not so new, it's probably from a 2015 vehicle, but I would still like to dig deeper into the mechanisms used in this ECU. While I managed to get some usefull info from this forum (and thank you all for that), I would like to ask some questions and see if there is someone that can help me a bit with the issues I am facing:

1. From the attached picture, you can see that my ECU comes with a 32pin connector, the connector came stripped and with no information, so I started reverse engineering it. My findings so far are:
   - VCC, 12V power on pin 11
   - GND in several spots, PINs 3, 8, 16, 24, 30
   - CAN High on pins 27 and 29
   - CAN Low on pins 28 and 30
2. The ECU draws 0.03 A of power, which is signifficantly low and probably means that the ECU is either not booting, or is at a sleep state and waits for an ignition signal.
   - Is there an ignition Pin? is it any of the 32pins on the connector?
3. CAN does not seem to supply anything useful, and is not answering to any application layer protol (e.g. UDS, XCP, etc.)
   - Is there a known wake-up sequence used by Jaguar / Land Rover for those ECUs?
   - Are there application layer protocols implemented?
   - Should a 120Ohm resistor used in between me and the ECU, to properly communicate over CAN?
4. I discovered another "pair" of cables from the connector, which leads to two different MOSFETS, should I evaluate these pins further?

This is the state I am in right now, and I would appreciate any help/information that you can supply regarding my efforts. Are there any wiring diagrams online that I can find for cheap? Are there any public information regarding this connector, the CAN implementation of Jaguar, UDS implementation, hardware specifications?

Thank you all in advance.

Best,
Thomas

Featured Sponsors
Vendor Directory

Supersprint
Jaguar Forums
register now
Featured Sponsors

10-24-2023, 03:55 AM #1

C

Cr0wTom
Junior Member
Thread Starter

Join Date: Oct 2023
Location: Prague
Posts: 5
Likes: 0
Received 0 Likes on 0 Posts

Hell

I am
dig
me

1. F
2. T
3. C
4. I

This
info

Thai

Best
Thor

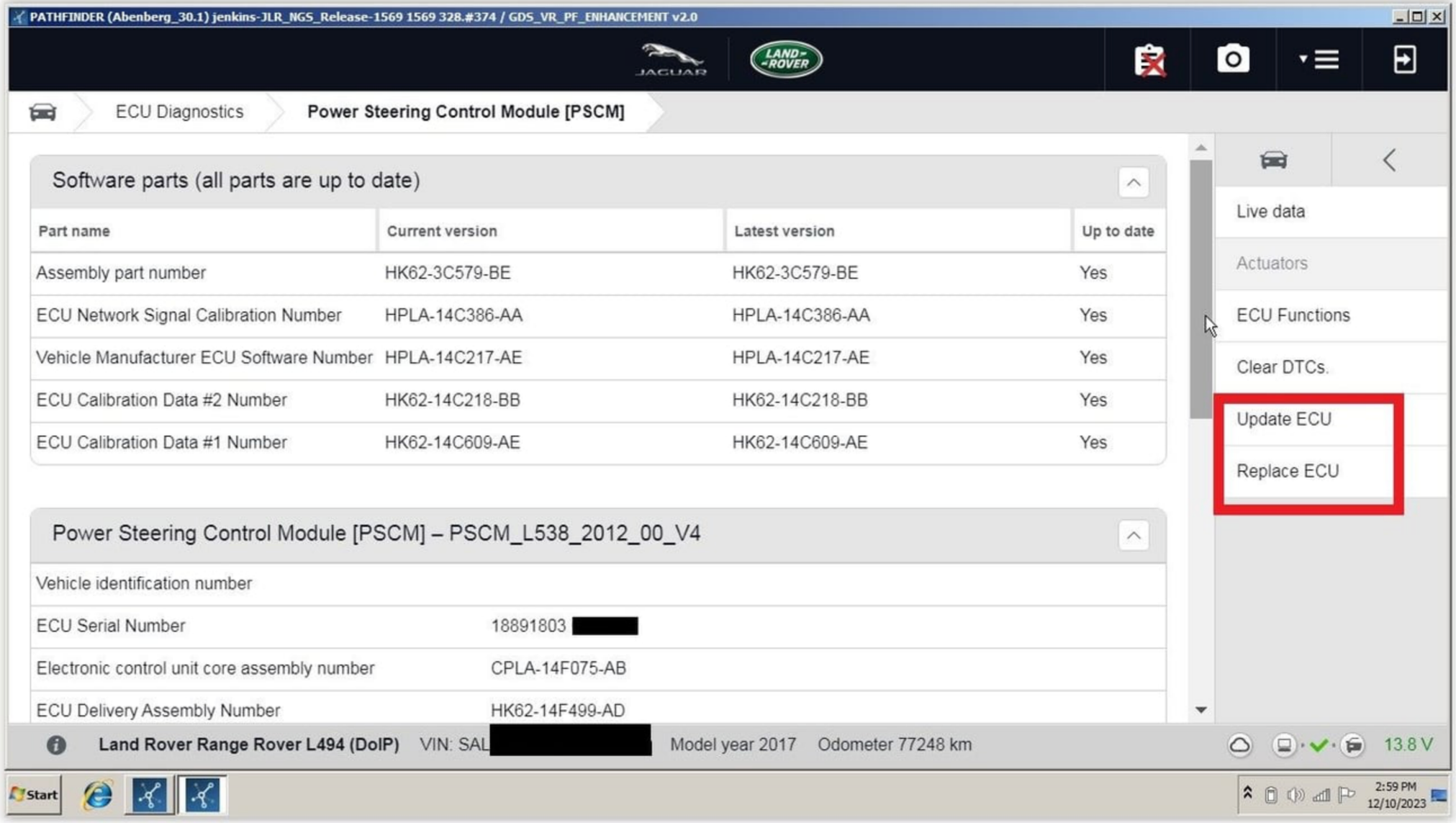
10-24-2023, 07:18 AM

Rondog
Senior Member

WOw! Way over this old man's head. But I applaud you for the knowledge you have learned!!

MoscowLeaper
Senior Member
Join Date: Apr 2012
Location: Israel
Posts: 601
Likes: 12
Received 333 Likes on 187 Posts

Even in a PathFinder the modules are referred as ECU's 🙂
Have a look - exact module is PSCM (Power Steering Control Module), but replace and update option refers to it as an ECU. Same for all the others actually.



For a 2014-2017 TCU:
Local config file 00020000-0002FFFF

Jaguar Land Rover (JLR) Pathfinder & VCI Interface Package

£2,248.48 – £6,245.21 ex. VAT

Or pay £749.49/month for 3 months - interest-free

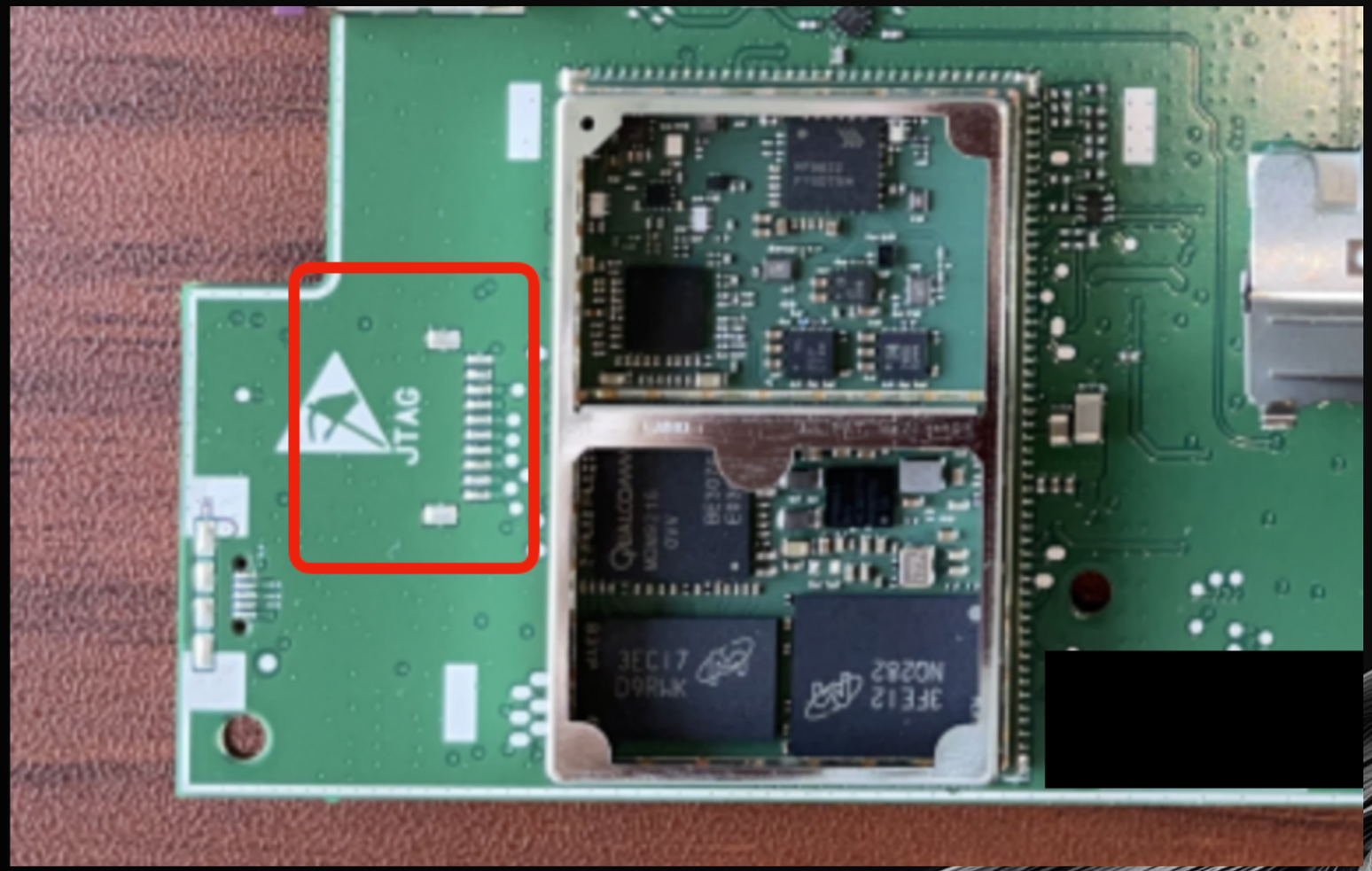
iwoca Pay financing is available to UK Limited businesses at checkout.

Choose package

Tools Only	£2,248.48 ex. VAT
Panasonic Toughbook CF-D1 (Grade A) Rugged Tablet Bundle	£3,896.72 ex. VAT
Dell Latitude 5430 Rugged Laptop - Standard Bundle	£5,255.21 ex. VAT
Dell Latitude 5430 Rugged Laptop - Mid Range Bundle	£5,845.21 ex. VAT

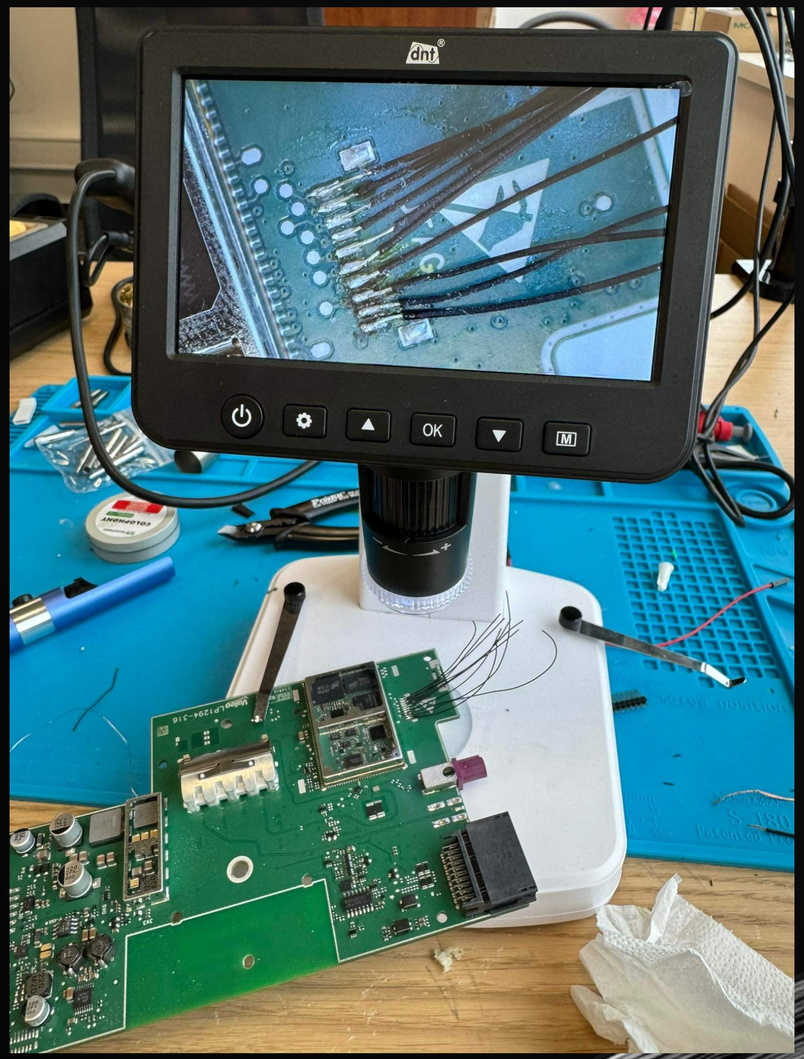
See more options

THE HARDWARE

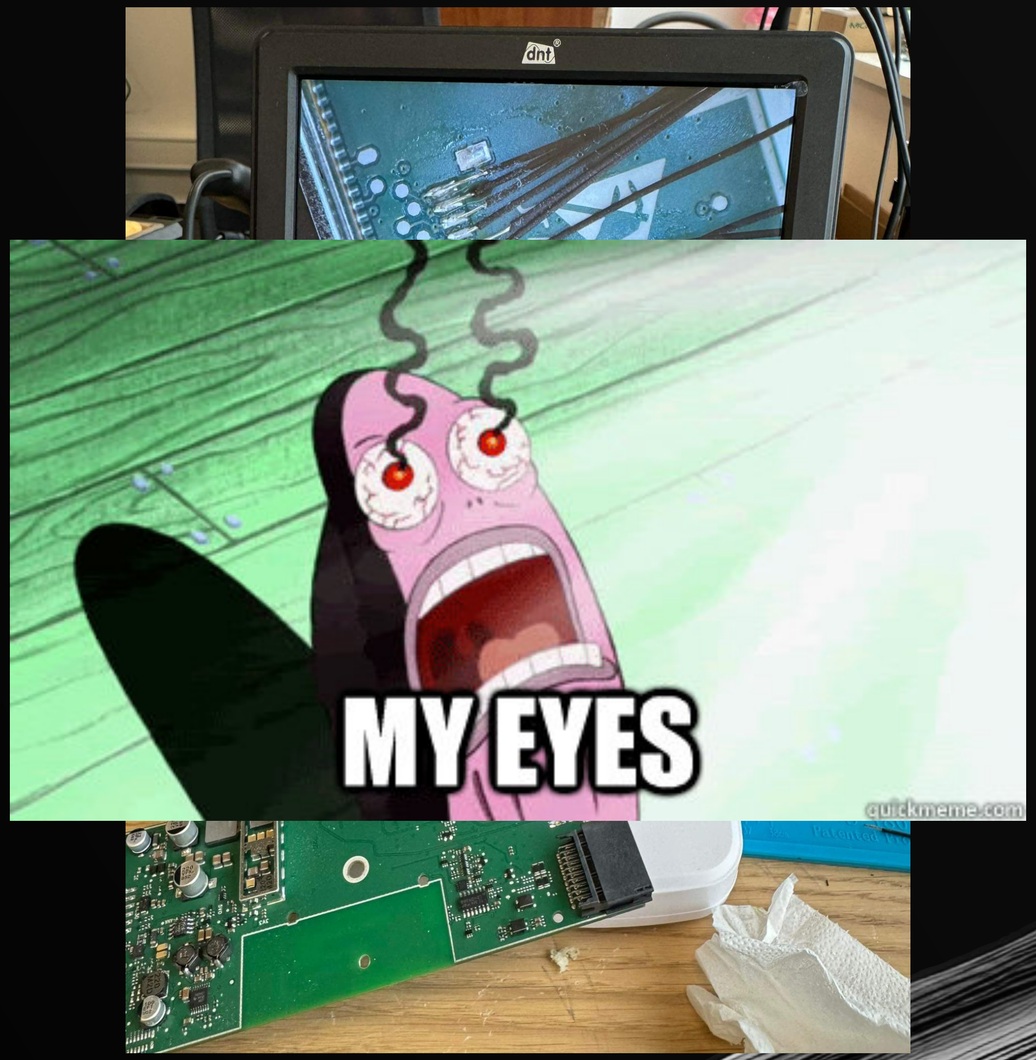


Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

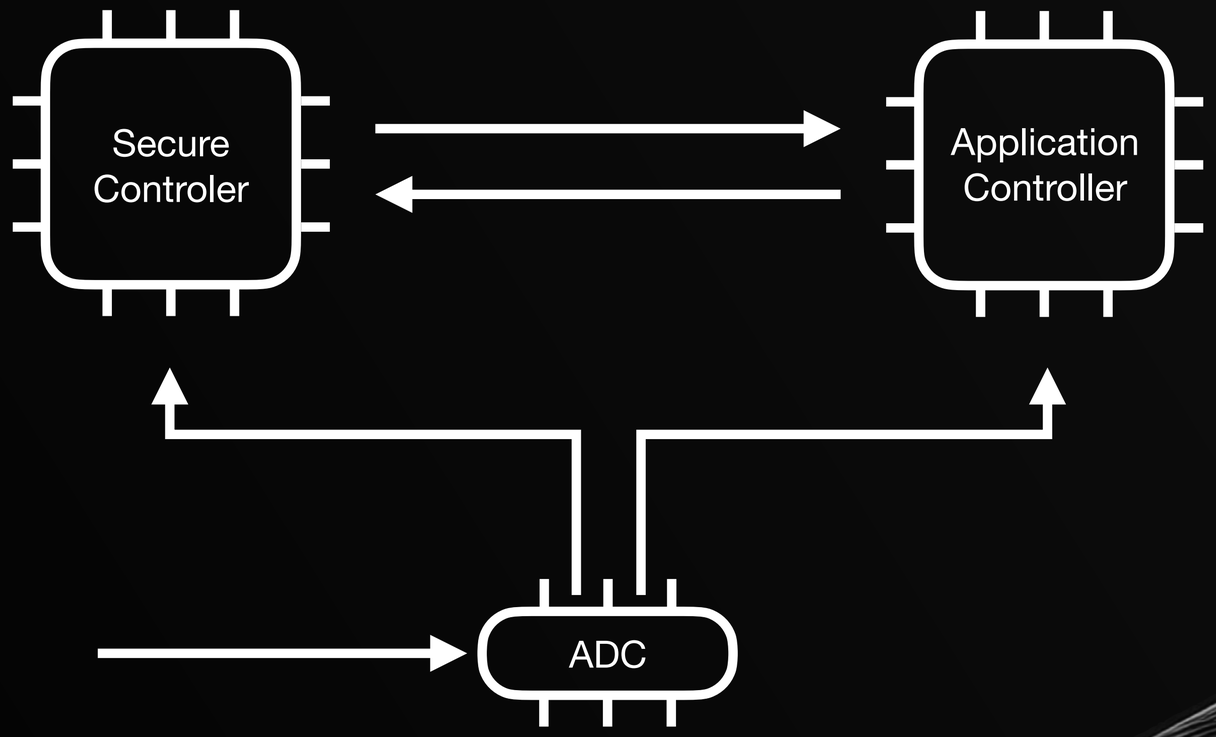
THE HARDWARE



THE HARDWARE

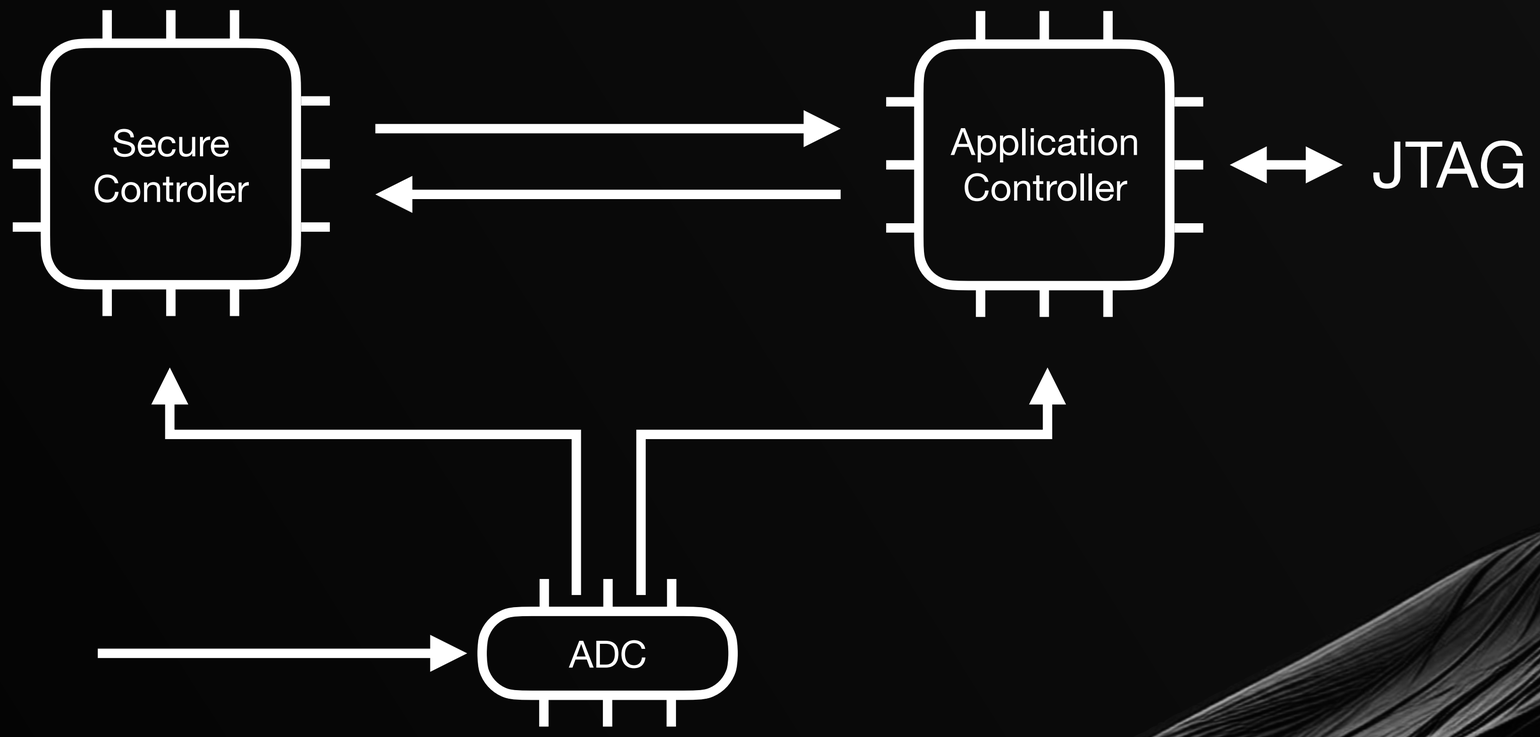


CASE 1 - THE 2 SOCS



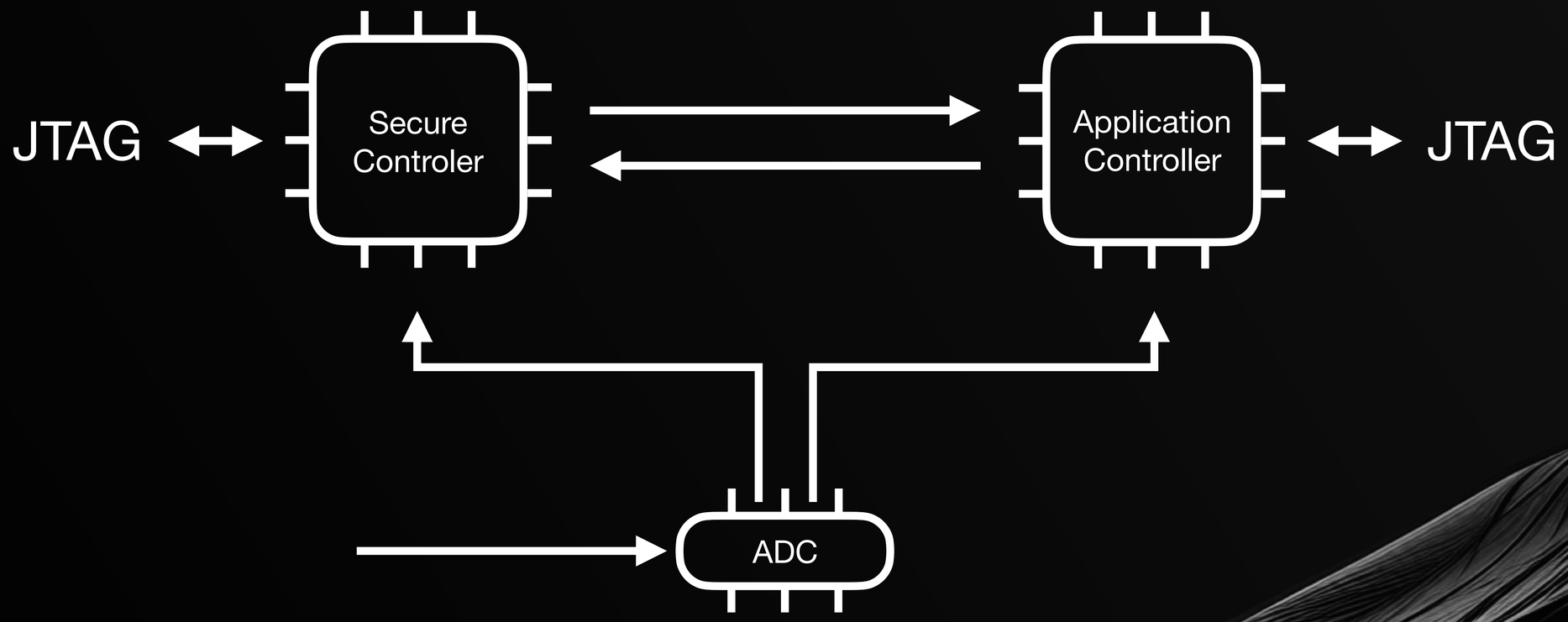
Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

CASE 1 - THE 2 SOCS



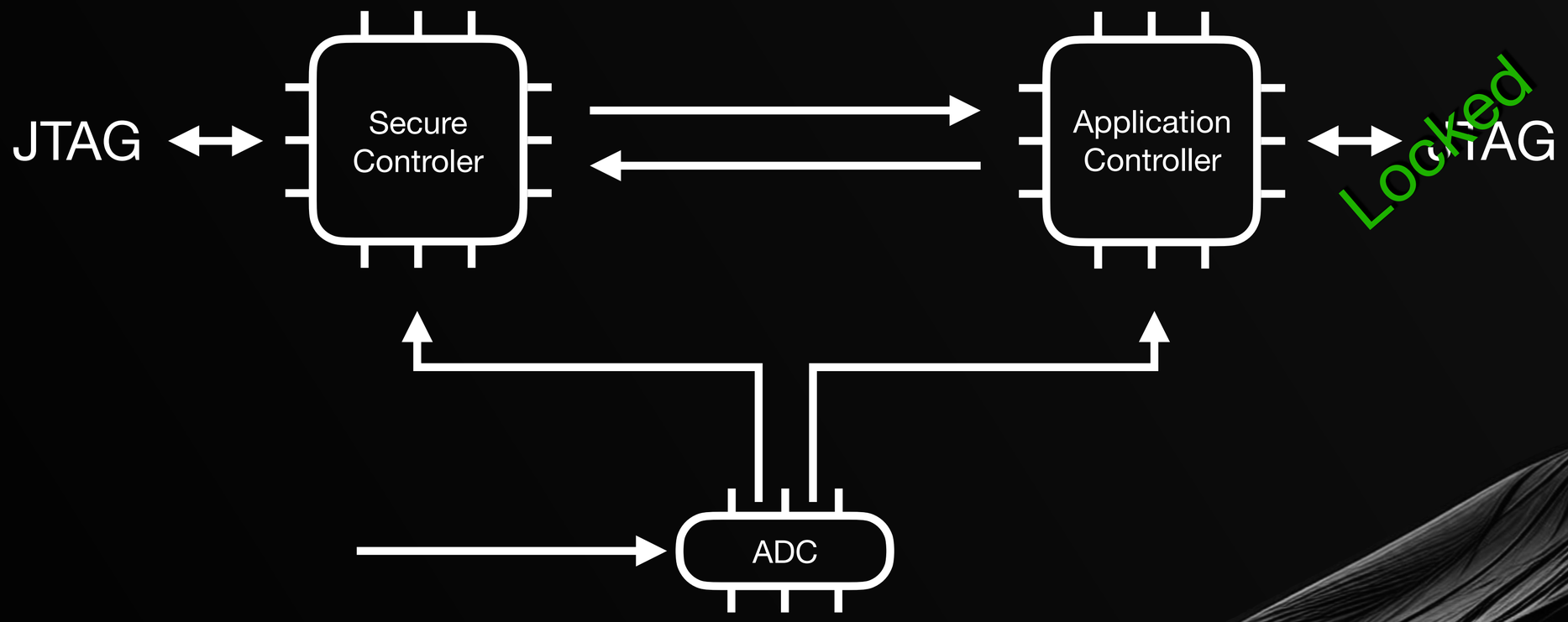
Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

CASE 1 - THE 2 SOCS

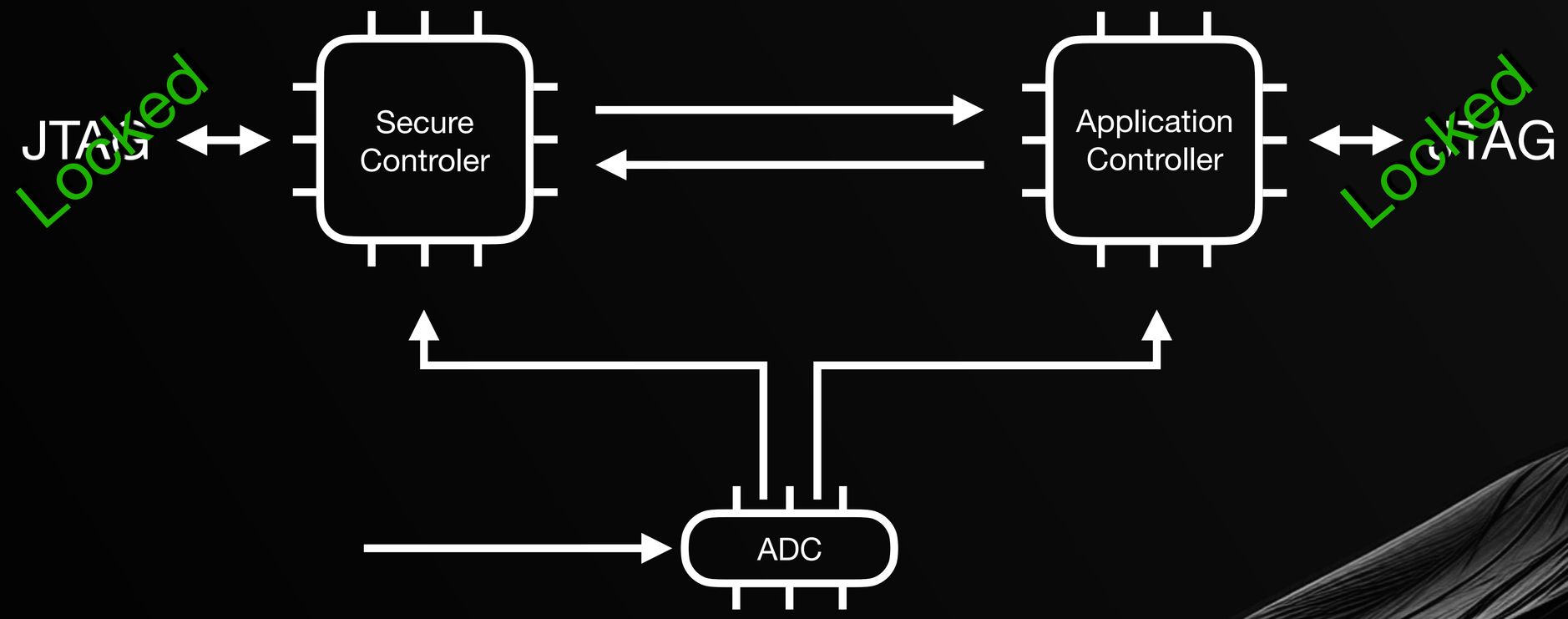


Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

CASE 1 - THE 2 SOCS

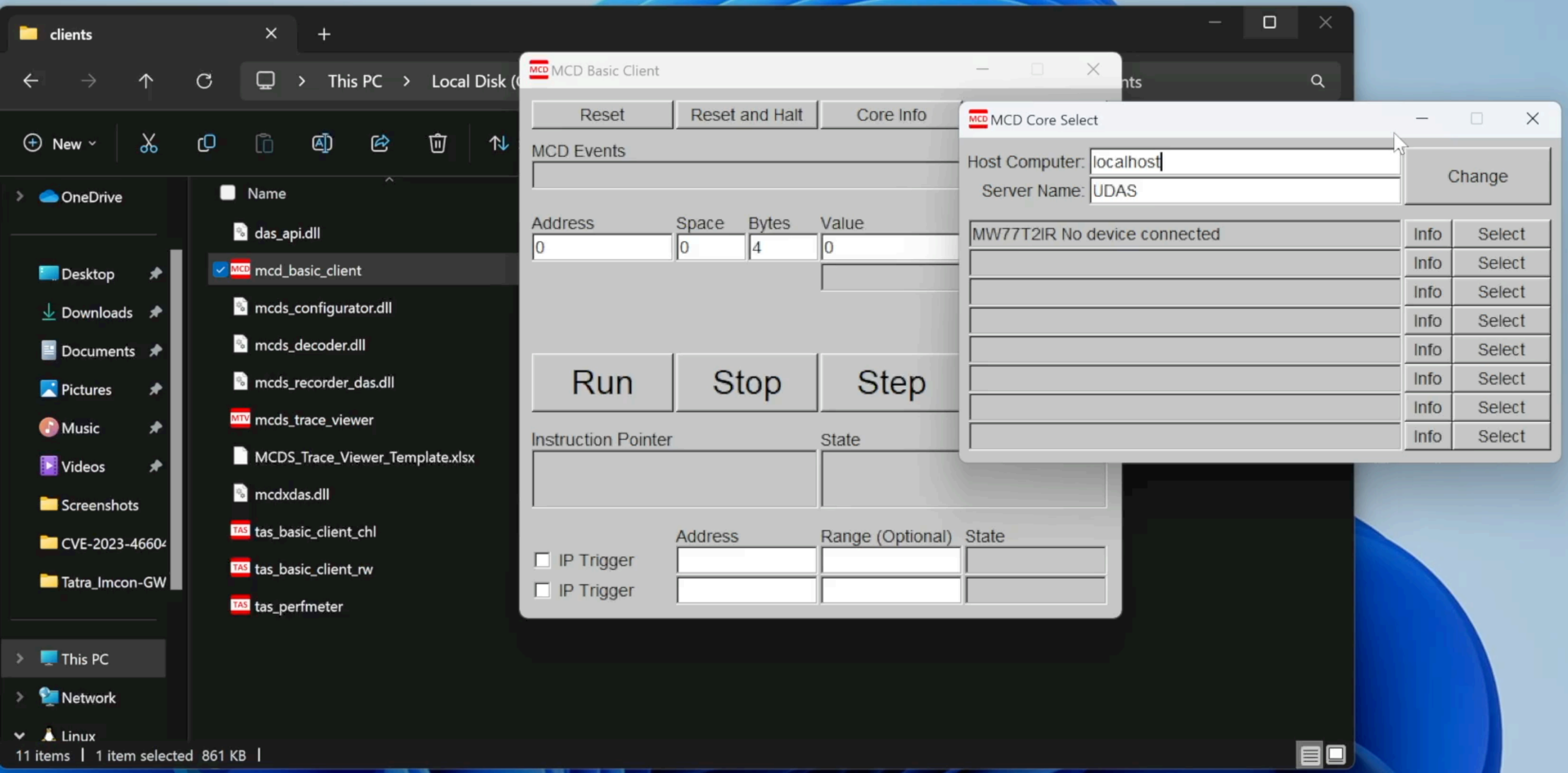


CASE 1 - THE 2 SOCS

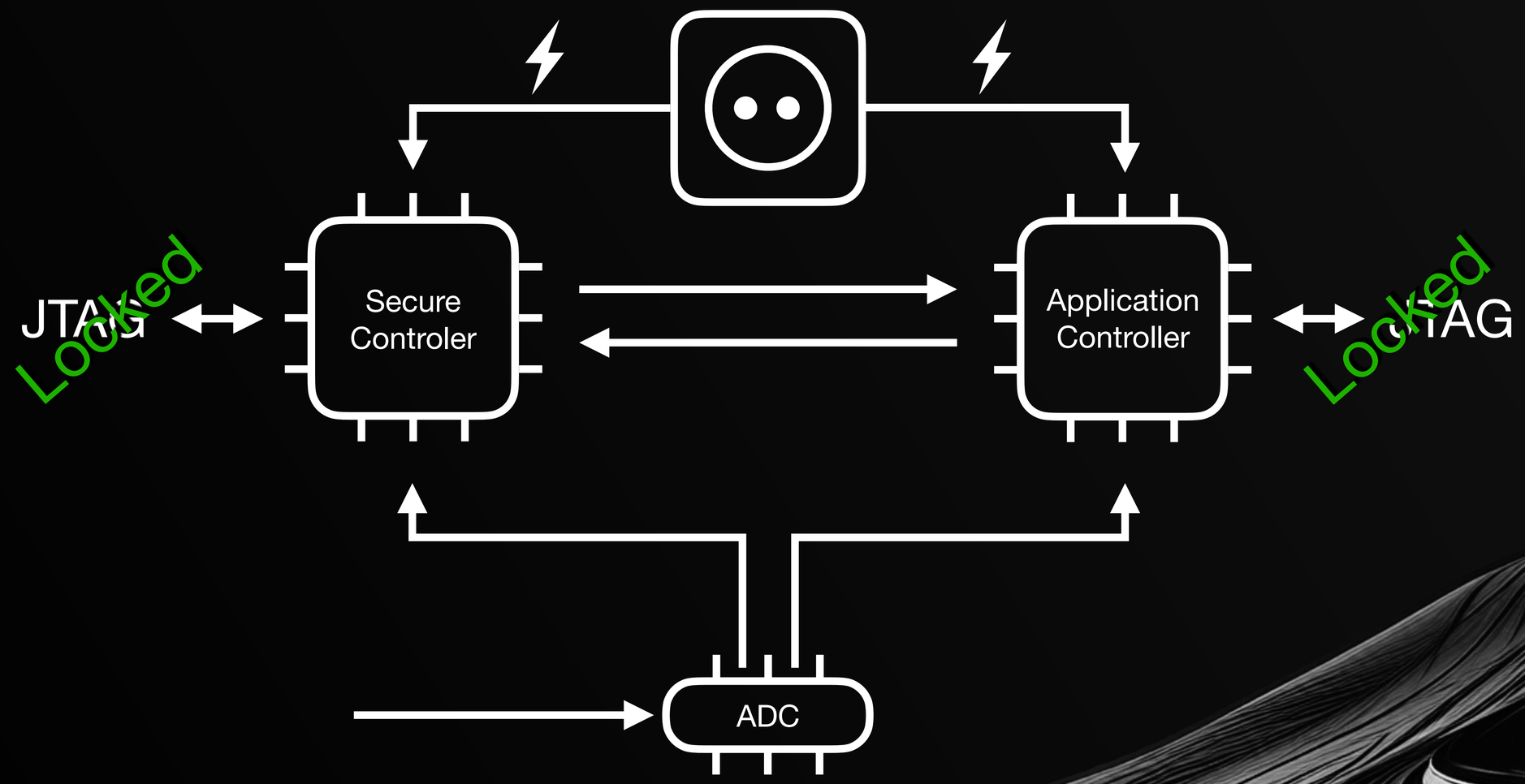


Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

DEMO

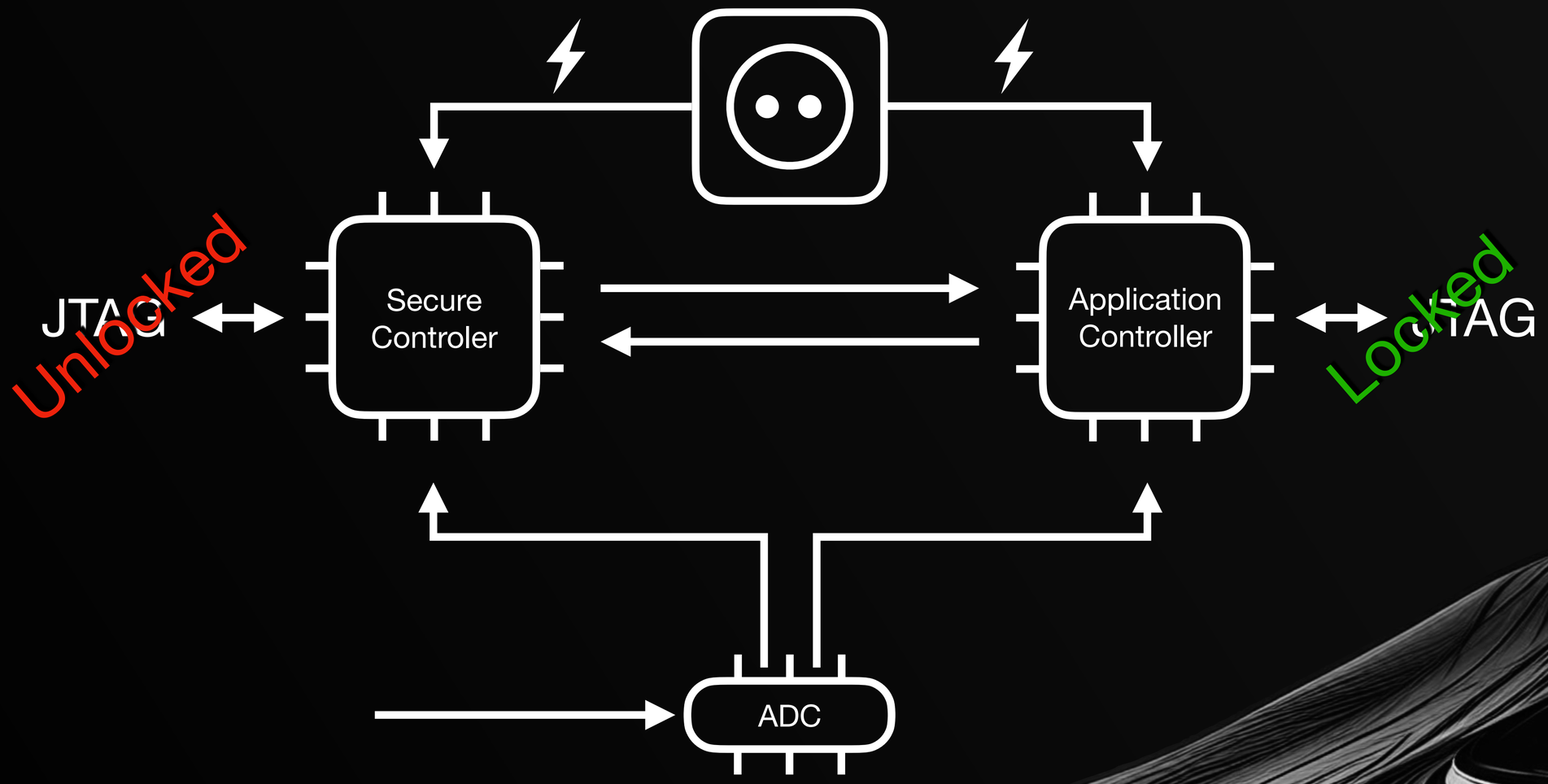

clients
This PC
Local Disk
New
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
CVE-2023-4660
Tatra_Imcon-GW
This PC
Network
Linux
Name
das_api.dll
mcd_basic_client
mcds_configurator.dll
mcds_decoder.dll
mcds_recorder_das.dll
mcds_trace_viewer
MCDS_Trace_Viewer_Template.xlsx
mcdxdas.dll
tas_basic_client_chl
tas_basic_client_rw
tas_perfmeter
11 items | 1 item selected 861 KB
MCD Basic Client
Reset
Reset and Halt
Core Info
MCD Events
Address
Space
Bytes
Value
0
0
4
0
Run
Stop
Step
Instruction Pointer
State
Address
Range (Optional)
State
IP Trigger
IP Trigger
MCD Core Select
Host Computer:
localhost
Server Name:
UDAS
Change
MW77T2IR No device connected
Info
Select

CASE 1 - THE 2 SOCS



Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

CASE 1 - THE 2 SOCS



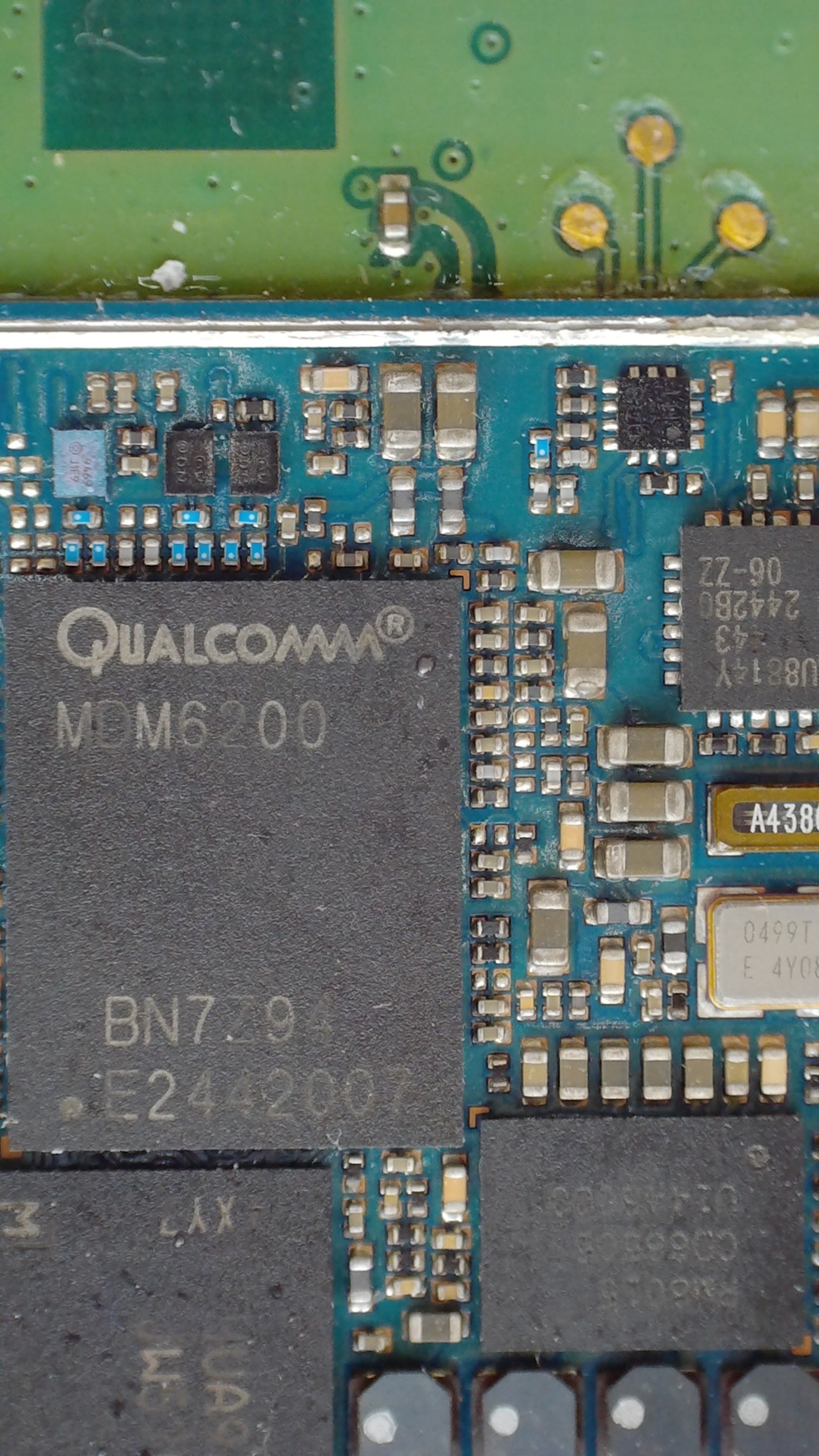
Typhoon
AUXILIUM Pentest Labs
cr0w's place labs

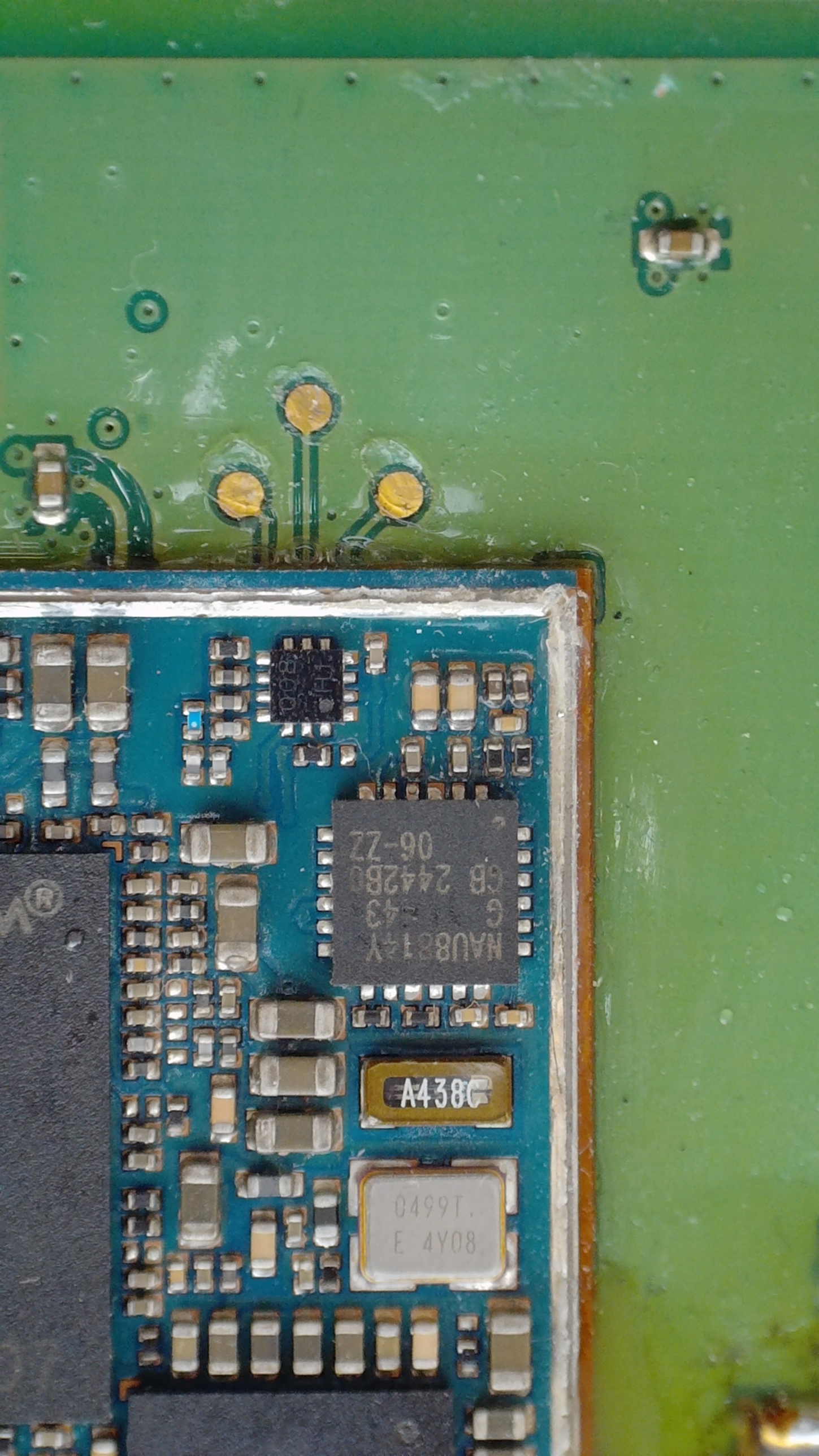
CASE 1 - THE 2 SOCS

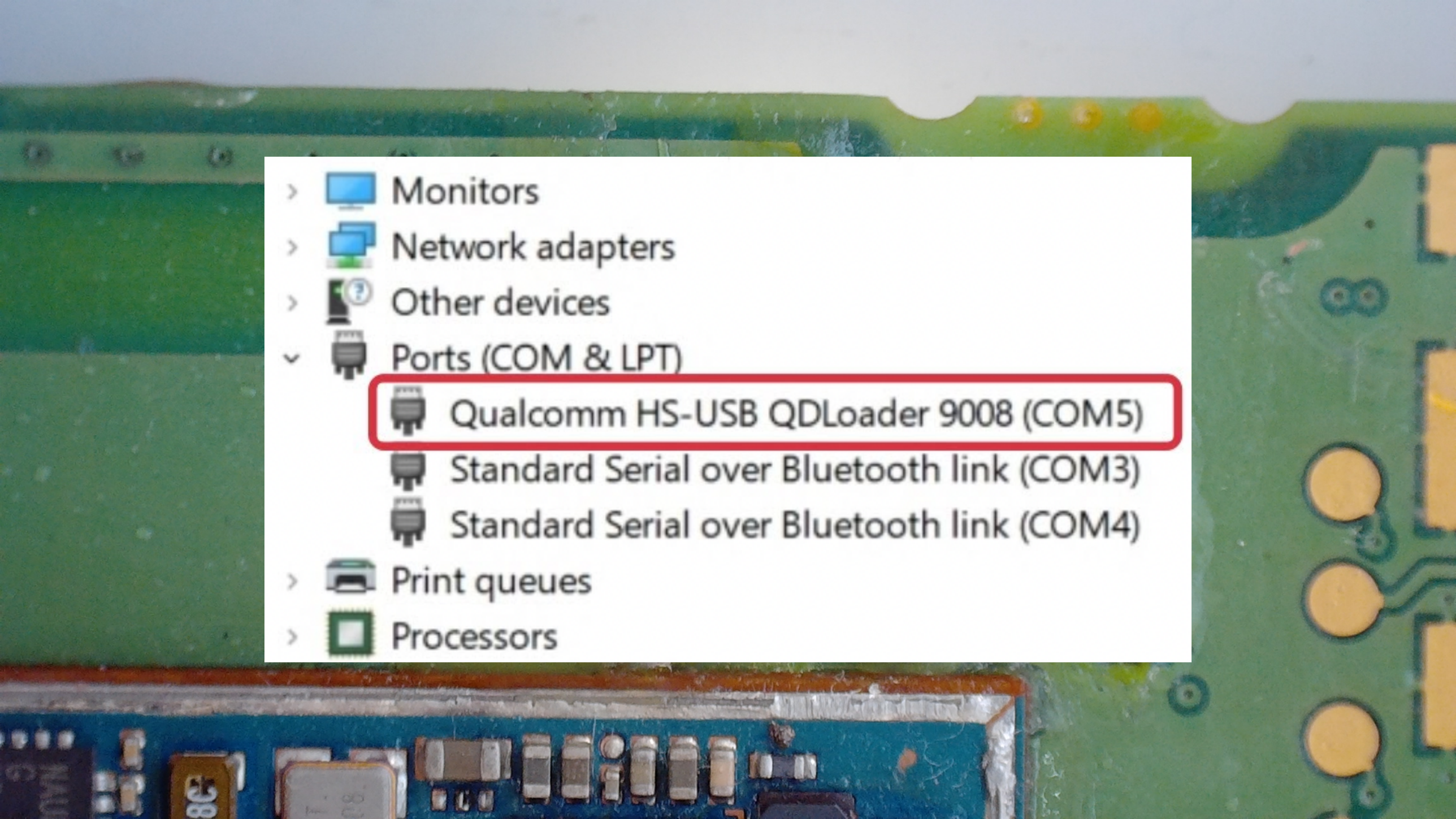
Typhoon AUXILIUM Pentest Labs cr0w's place labs

CASE II - SECRET PINS LEADING TO SECRET MODES

- **Security through obscurity is a really common tactic in hardware security mitigations**
- **Secret pins is a really common way of including debug functionality in the unit, but obscuring it under random pins that need to be shorted**
- **One such example is Qualcomm EDL Mode**
  - To enable, it's as easy as shorting the two dedicated pins responsible for enabling EDL functionality
  - After that, a full dump and re-flash of the firmware can be achieved
    - *Main reason behind it - De-bricking*


QUALCOMM®
MDM6200
BN7.9
E244200
A438
0499T
E 4YO


NAU8214Y
A438C
0499T.
E 4Y08


Monitors
Network adapters
Other devices
Ports (COM & LPT)
Qualcomm HS-USB QDLoader 9008 (COM5)
Standard Serial over Bluetooth link (COM3)
Standard Serial over Bluetooth link (COM4)
Print queues
Processors

THE HARDWARE - IS THAT ALL?

- **Many more hardware attack paths exist**
- **Some are more lab oriented, while others are more applicable to real world**
- **For the OEM: Debug and other easily accessible interfaces need to be protected**
  - e.g. JTAG, UART, SPI, I2C are some of the common attack paths that attackers start with
- **For the tuner/owner: CAREFUL enumeration of hardware is your best bet when approaching an ECU blindly**
  - Be careful, these are some fragile puppies (talking from experience 😭)

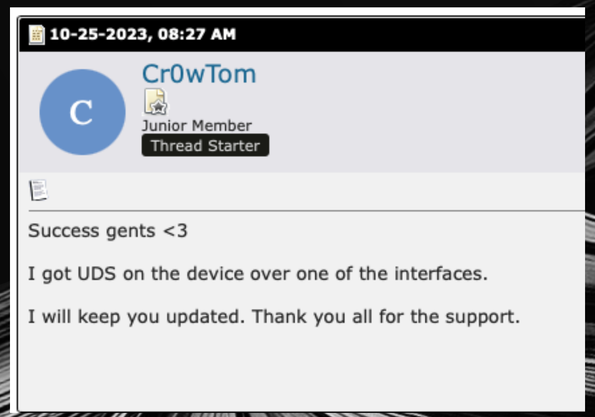
챕터 #2

THE DRAG

And how a diagnostics protocol can reveal all the secrets.

GETTING SOMEWHERE

- **After dumping the firmware, I started reverse engineering**
  - Only to later discover that my problem was insufficient power supply 🙄
  - Be ALWAYS careful with the voltage you are supplying in undocumented hardware, you can fry it, faster than chicken wings 🍗
- **UDS was discovered and the game is on!**



CASE III - UDS DIAGNOSTICS AND PATCHES OVER PATCHES

- UDS stands for Unified Diagnostic Services, an application layer protocol for communication between electronic control units in automotive electronics
- Allows diagnostic functions such as reading and erasing fault codes, programming, testing, and monitoring of ECUs
- Consists of several “services" which can be used to perform specific actions
- A really common authentication scheme in UDS is the Security Access service (0x27)
  - Allows elevated access to authenticated users

CASE III - UDS DIAGNOSTICS AND PATCHES OVER PATCHES

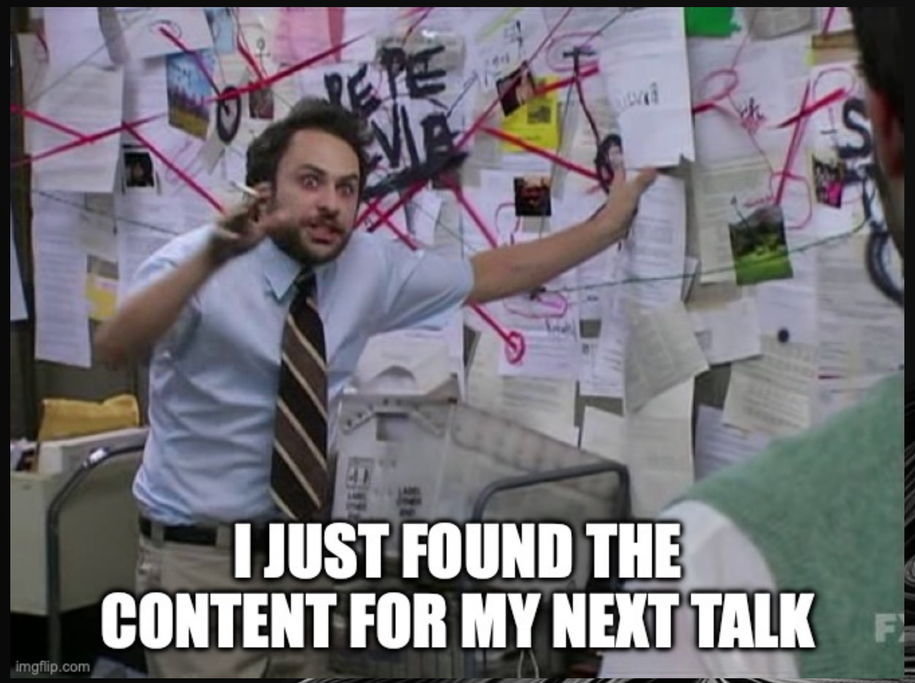
- Service 0x11 – ECUReset
- 90% of target ECUs, come with no authentication or pre-condition for hard ECUResets
- This means that any ECU which allows execution of this service, can be immediately interrupted by hard reseting it

CASE III - UDS DIAGNOSTICS AND PATCHES OVER PATCHES

FIXED
VMware Fusion File Edit View Virtual Machine Window Help
Kali Linux
File Actions Edit View Help
cr0wtom@kali-m1: ~/Tools/caringcaribou/tool
candump can0,7D5:7D4

CASE III - THE AFTERMATH

- **Responsibly disclosed finding in one of the biggest OEMs**
  - Vulnerability was accepted
  - Directly affects the ADAS system of the vehicle
  - Applicable to 3 different models, and 4-5 years of MY
  - CVEs are yet to be assigned :'(



Typhoon AUXILIUM Pentest Labs cr0w's place labs

챕터 #3

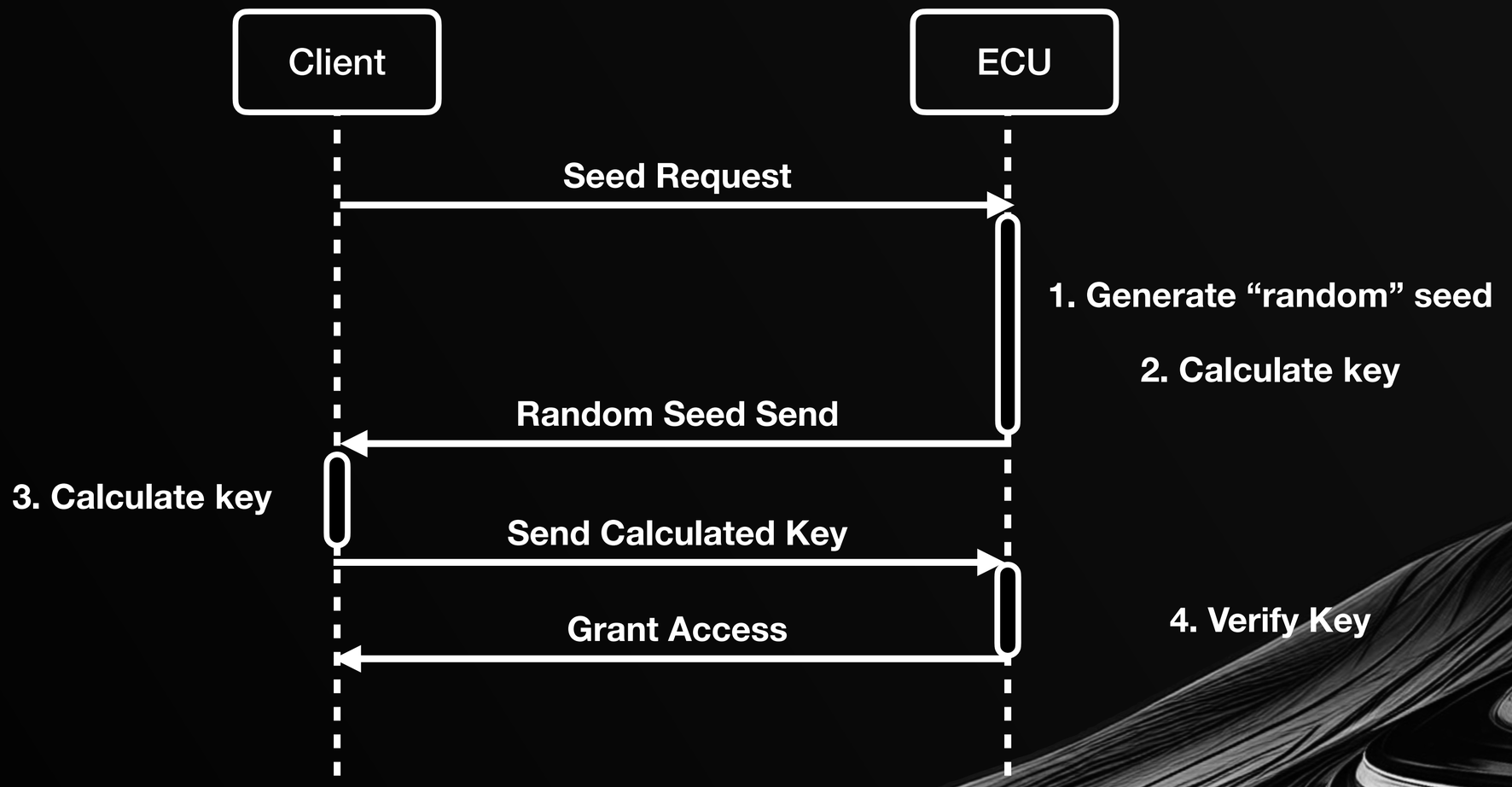
THE SPEED

And the challenges of randomness in an abstract world.

SECURITY ACCESS SEEDS

- **The security access UDS service (0x27), implements a challenge response mechanism, including:**
  - A secret key
  - A secret calculation algorithm
  - A random seed
- **Main use for access control purposes**
  - Full ECU reprogramming can be considered the holly grail of a security access bypass

SECURITY ACCESS MECHANISM



Typhoon AUXILIUM Pentest Labs cr0w's place labs

SEEDS - HONEST QUESTIONS

- What is the secret key?

Typhoon AUXILIUM Pentest Labs cr0w's place labs

SEEDS - HONEST QUESTIONS

- What is the secret key?
- What is the secret calculation algorithm?

Typhoon AUXILIUM Pentest Labs cr0w's place labs

SEEDS - HONEST QUESTIONS

- What is the secret key?
- What is the secret calculation algorithm?
- What is the source of randomness?

Typhoon AUXILIUM Pentest Labs cr0w's place labs

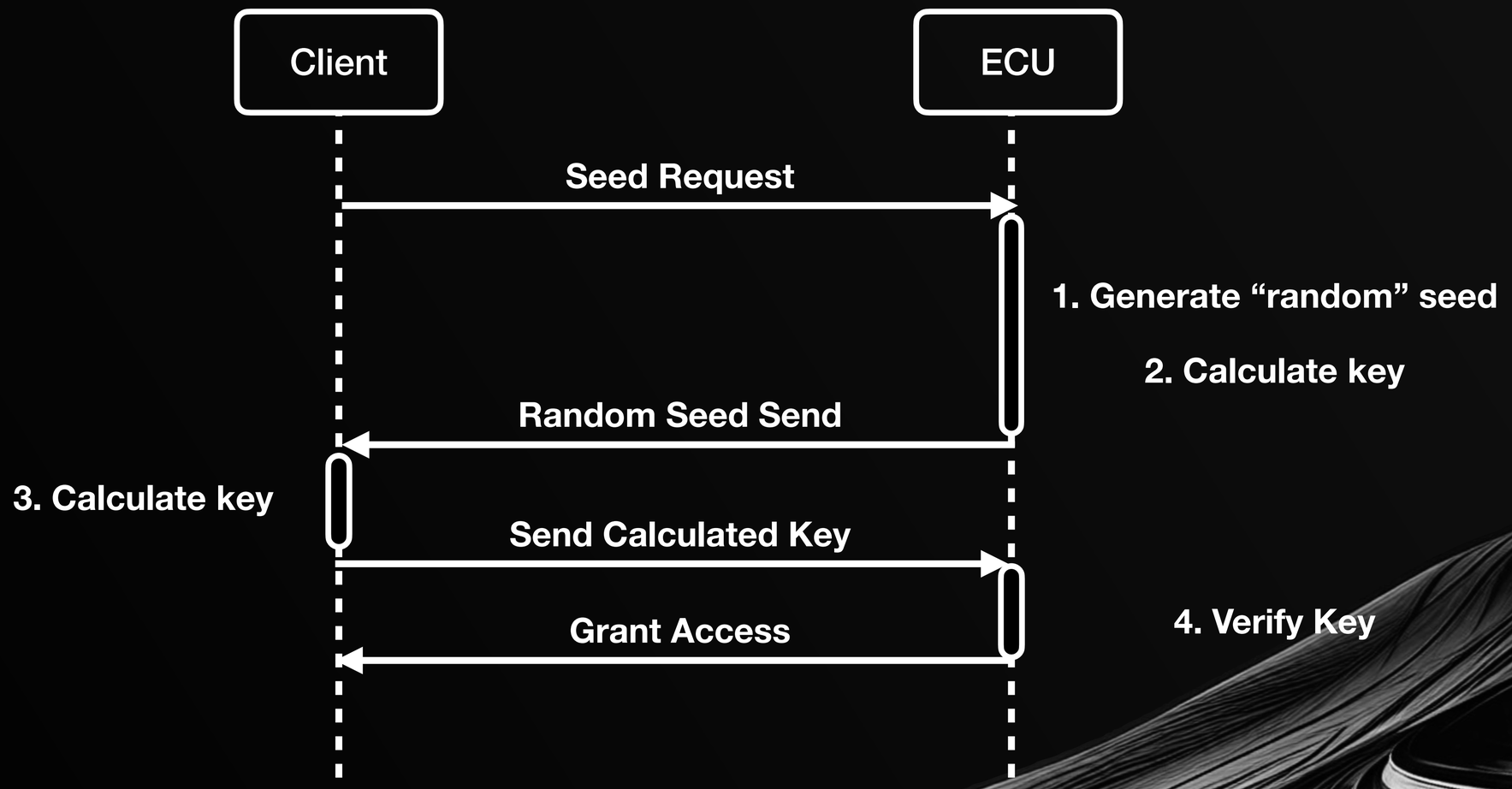
TRUE RANDOMNESS

- **While "true" randomness "might" exist in nature, it's extremely difficult to achieve in deterministic machines**
  - Computer systems are deterministic machines
  - Processing power needs to be used as efficiently as possible
  - Even if possible, due to the deterministic aspect of machines, can ultimately be controlled (in some cases)

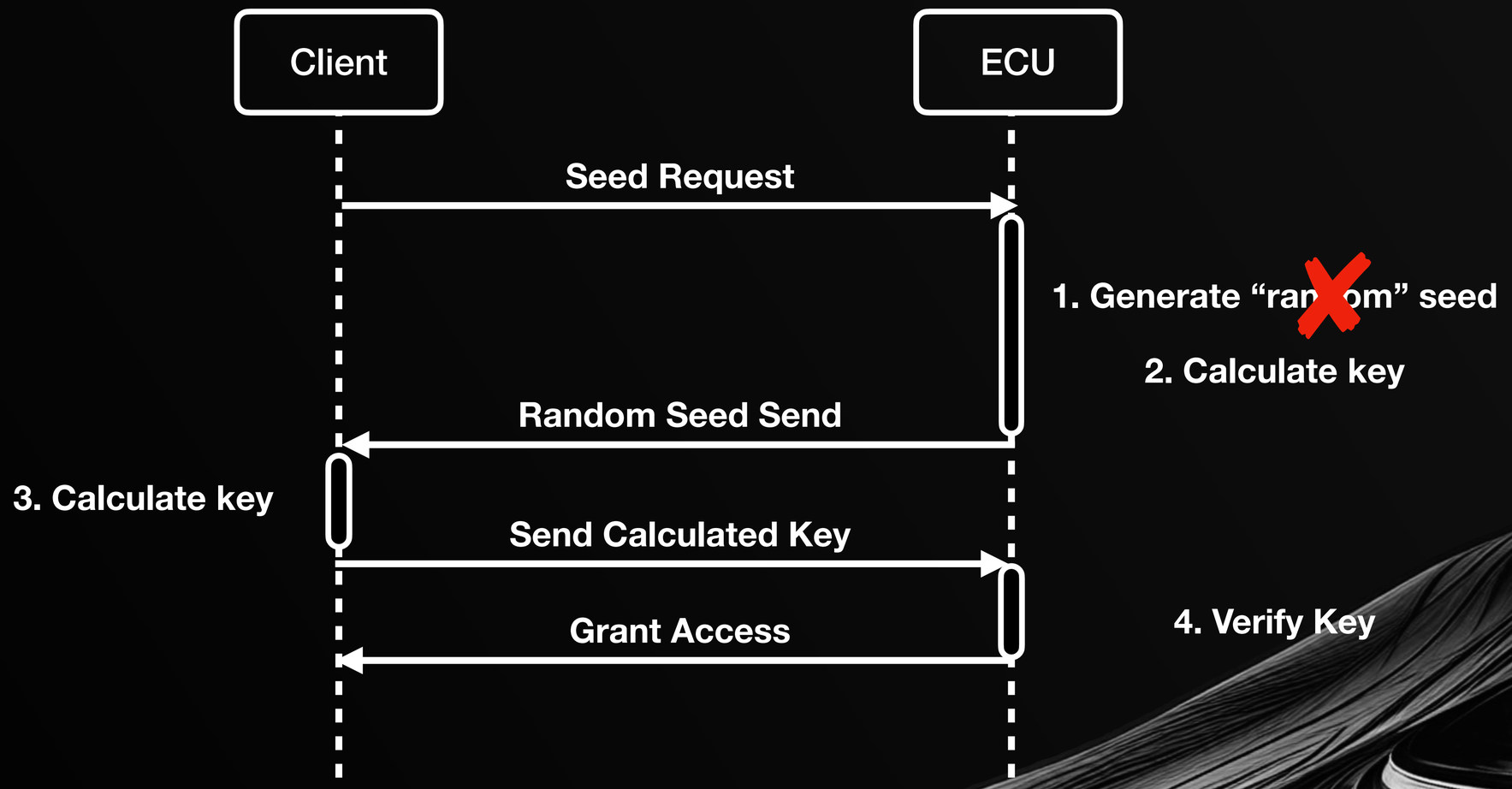
DEMO

```
Security Access Seeds captured:
d fb b
e fc b
f fd b
0 fd b
1 fe b
2 ff b
c 00 b
b 01 c
a 02 b
9 03 b
8 04 b
7 05 b
7 06 5
6 07 5
5 08 6
4 09 5
3 0a 5
2 0b 6
1 0c 5
0 0d 6
f 0d 5
```

SECURITY ACCESS MECHANISM



SECURITY ACCESS MECHANISM



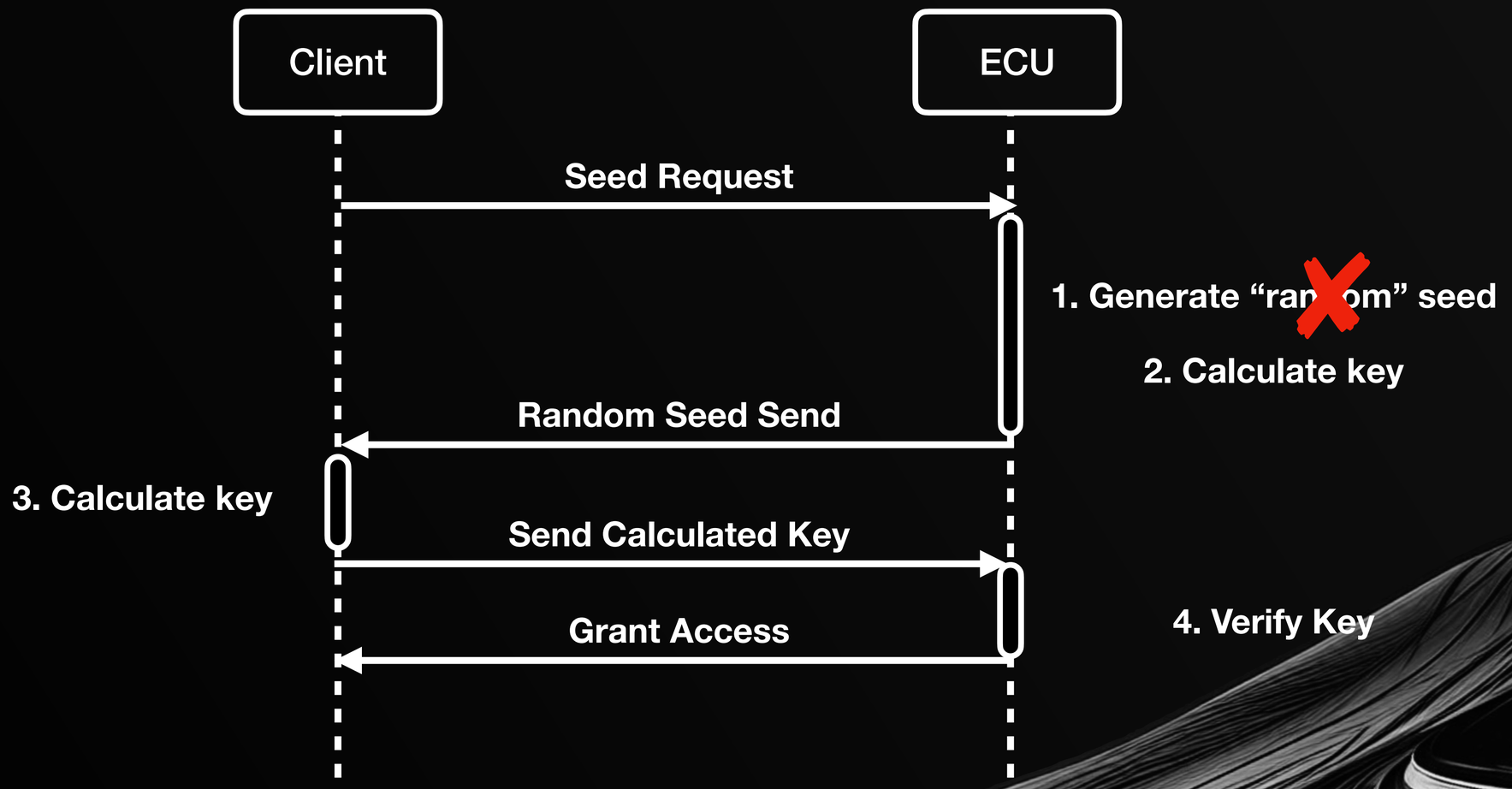
TRUE RANDOMNESS

Decompile: FUN_000192f6 – ([redacted].bin)

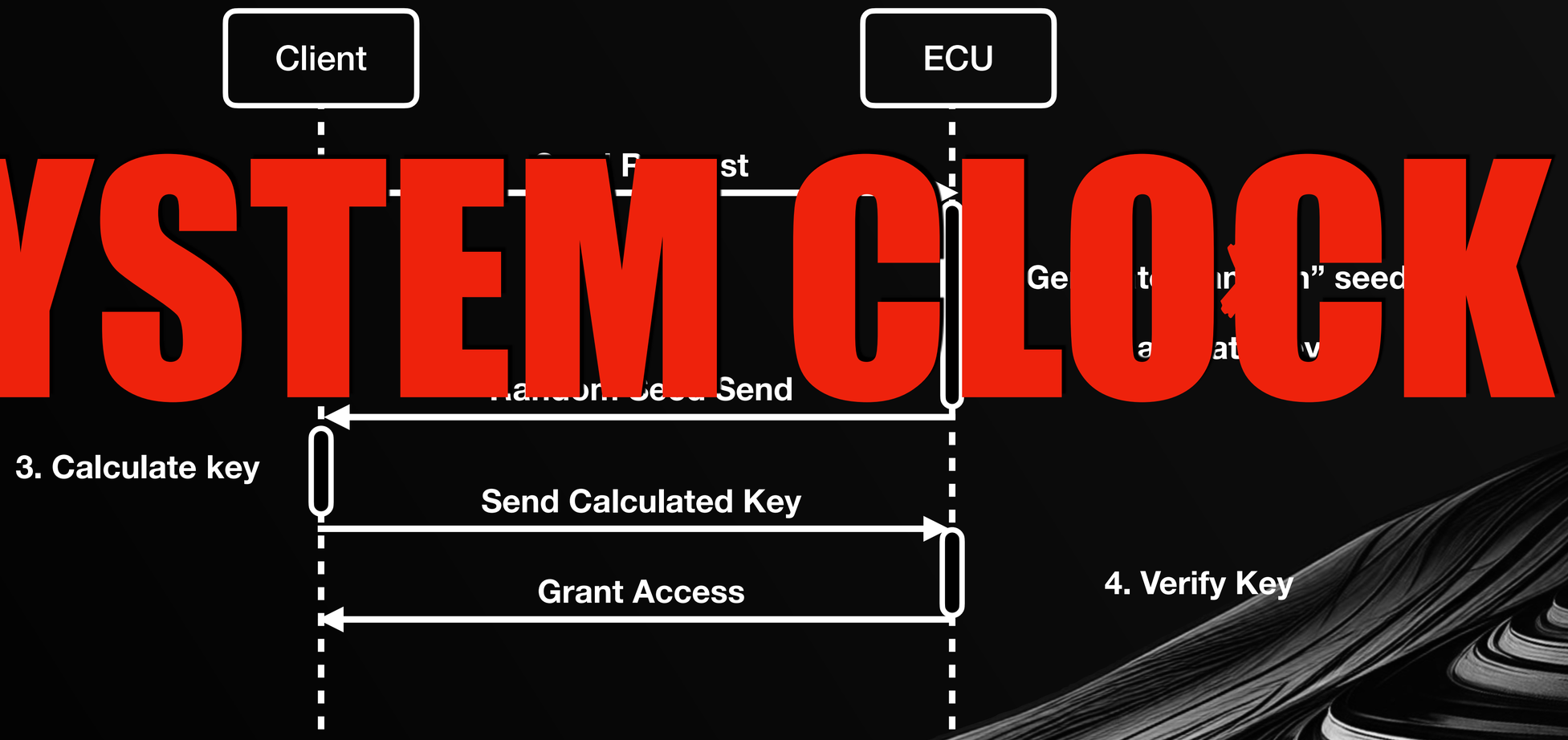
```
1
2  void FUN_000192f6(void)
3
4  {
5    undefined4 uVar1;
6    ushort uVar2;
7    undefined2 uVar3;
8    char cVar4;
9    char cVar5;
10   byte bVar6;
11   int iVar7;
12   int iVar8;
13   uint uVar9;
14
15   cVar4 = DAT_d000df5f;
16   bVar6 = DAT_d000dfd8;
17   cVar5 = DAT_d000df60;
18   if ((byte)(cVar4 - 1U) < 3) {
19     iVar7 = STM_TIM0;
20     iVar8 = STM_CAP;
21     uVar9 = STM_CLC;
22     uVar9 = uVar9 >> 8 & 7;
23     uVar2 = DAT_d000df58;
24     DAT_d000df50 = 0;
25     uVar1 = Ramd0000fcc;
26     DAT_d000df5a = ~uVar2;
27     DAT_d000df54 = uVar1;
28     DAT_d000df40 = CONCAT44(iVar8 * uVar9,iVar7 * uVar9);
29   }
30   uVar3 = DAT_d000df58;
31   DAT_d000df60 = cVar5 + '\x01';
32   DAT_d000dfd8 = bVar6 + 1 & 7;
33   (&DAT_d000dfc8)[bVar6] = uVar3;
34   return;
35 }
```


Typhoon AUXILIUM Pentest Labs cr0w's place labs

TRUE RANDOMNESS



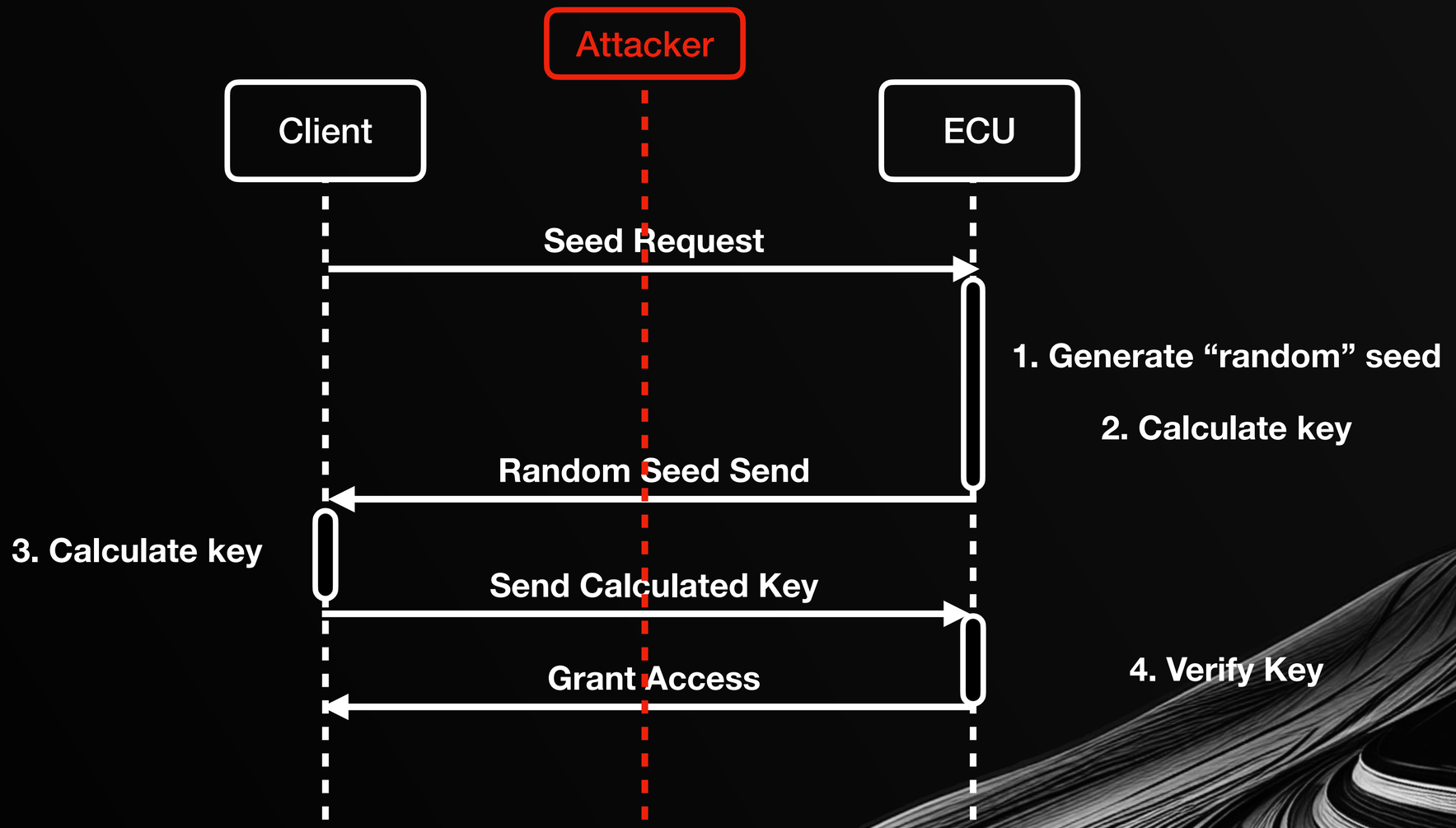
TRUE RANDOMNESS



CASE IV - CONTROLLING THAT SEED

- **CAN - Physical and Data link layer communication in ECUs**
- **On "higher layers", data is exchanged without encryption**
- **Obscurity of proprietary messages acts as a layer of "protection"**
- **Protocols on top of CAN are also unencrypted**
  - Interception, injection and replication are all applicable
- **Protections like SecOC (Message Authentication) can be implemented**

CASE IV - CONTROLLING THAT SEED



CASE IV - CONTROLLING THAT SEED

- **As CAN is unencrypted, an attacker with a MITM position can effectively intercept a seed/key pair**
  - OTA Updates
  - Service departments
  - Malicious Taps in between the lines
  - etc.
- **Even if we have a seed/key pair, how do we bypass the rest of the restrictions that apply?**

CASE IV - CONTROLLING THAT SEED

- What is the secret key?
- What is the secret calculation algorithm?
- What is the source of randomness?

Typhoon AUXILIUM Pentest Labs cr0w's place labs

CASE IV - CONTROLLING THAT SEED

- What is the secret calculation algorithm?
- What is the source of randomness?

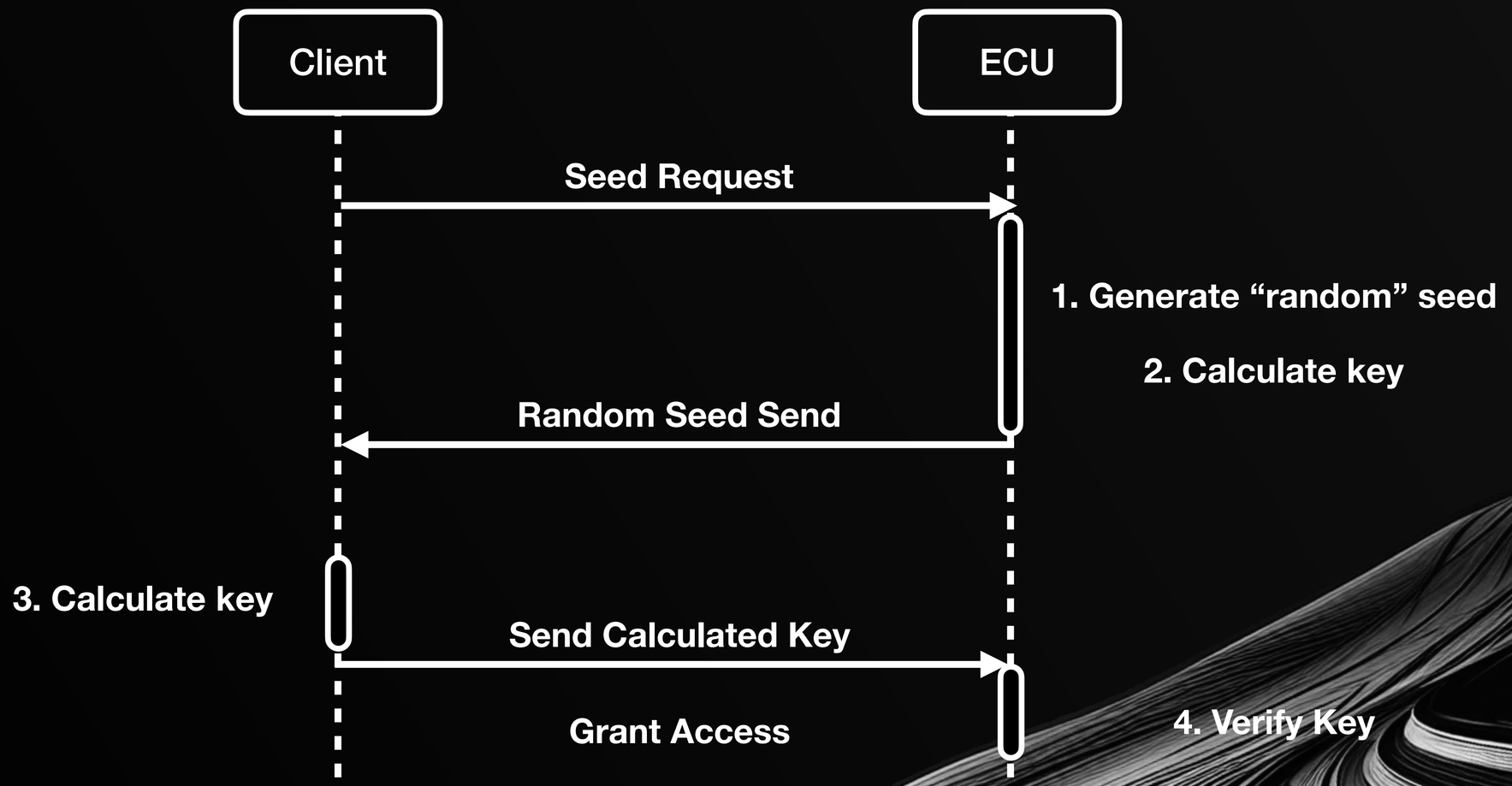
Typhoon AUXILIUM Pentest Labs cr0w's place labs

CASE IV - CONTROLLING THAT SEED

- **What is the source of randomness?**

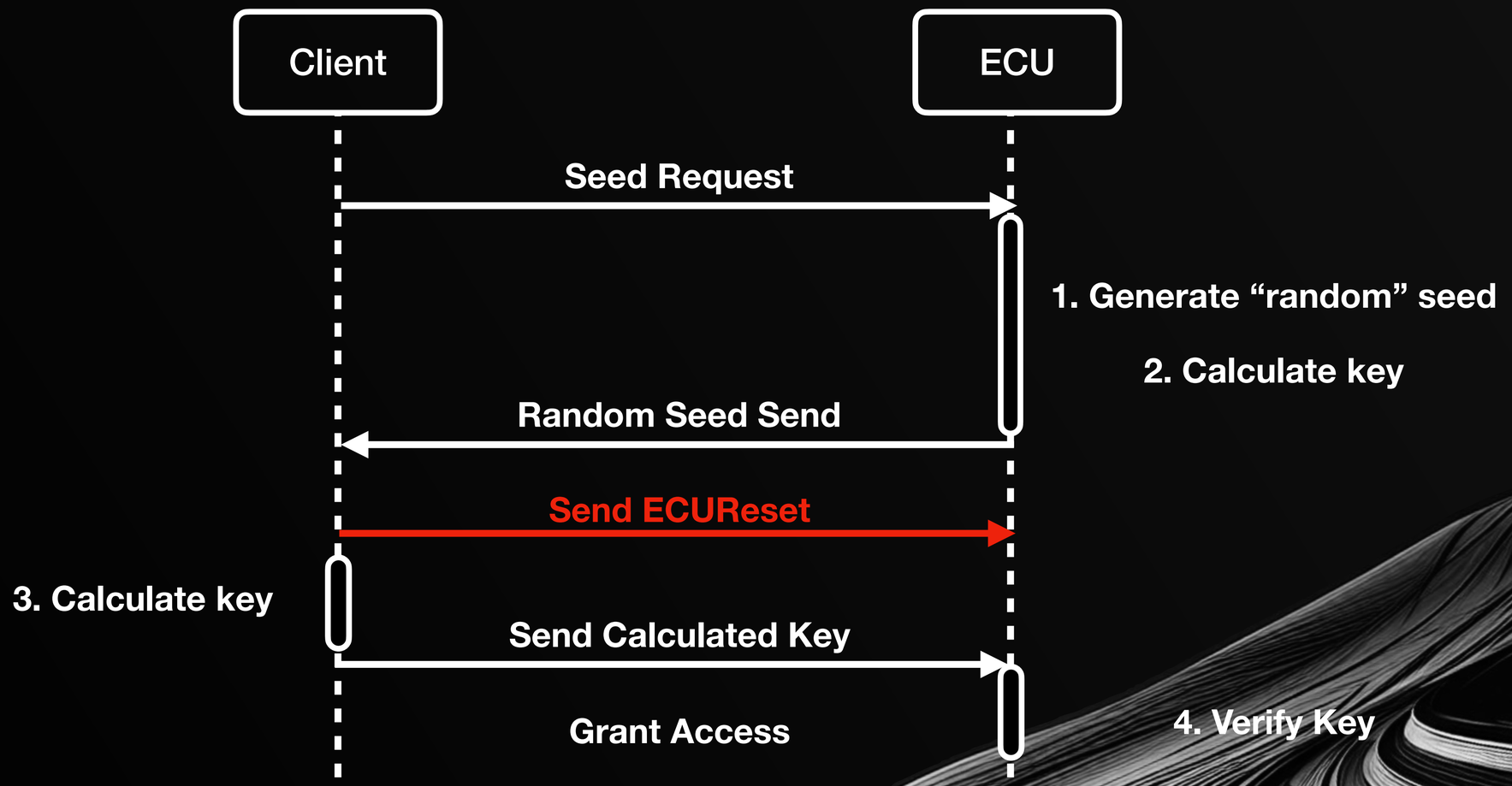
Typhoon AUXILIUM Pentest Labs cr0w's place labs

CASE IV - CONTROLLING THAT SEED

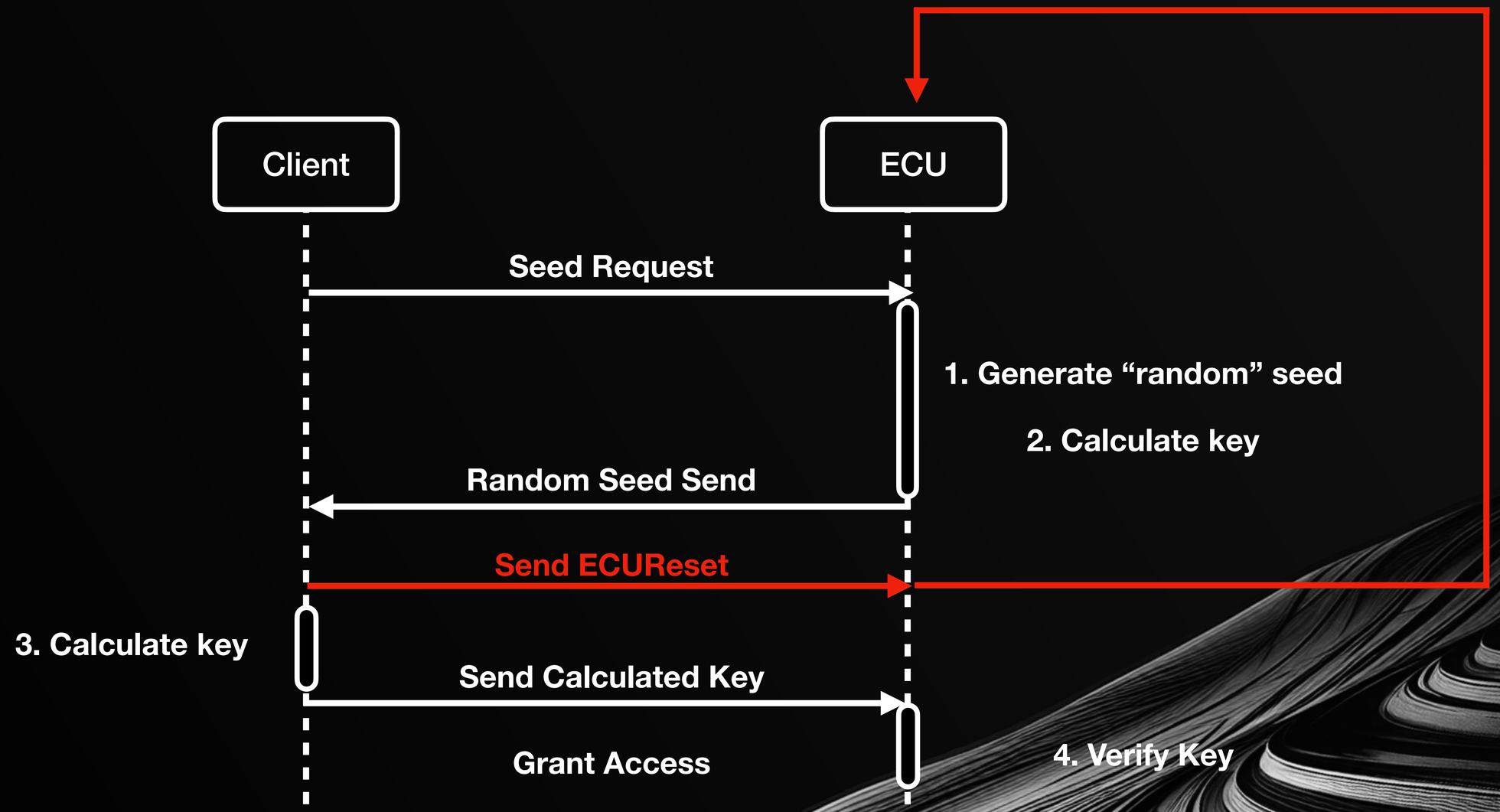


Typhoon AUXILIUM Pentest Labs cr0w's place labs

CASE IV - CONTROLLING THAT SEED

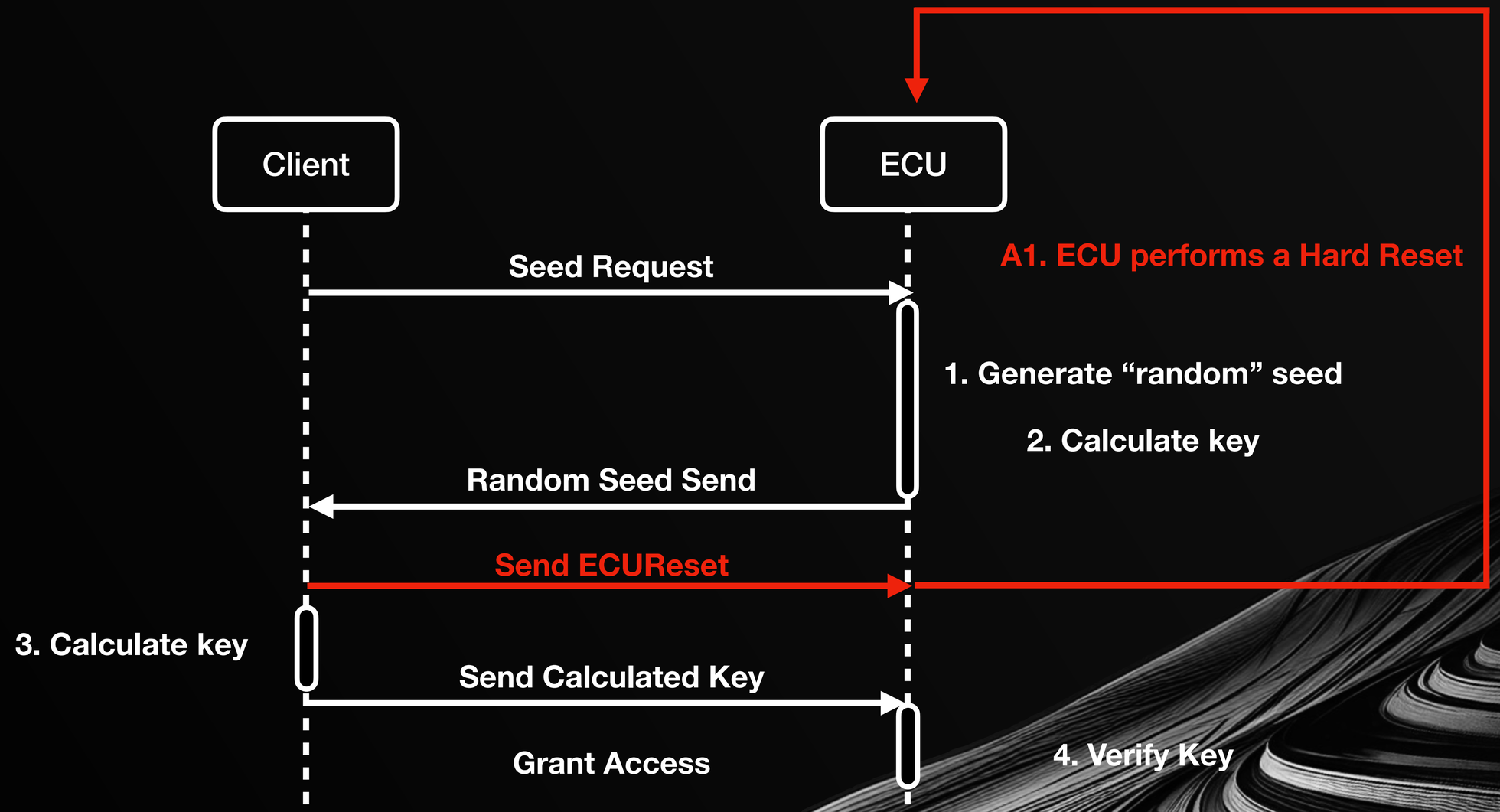


CASE IV - CONTROLLING THAT SEED

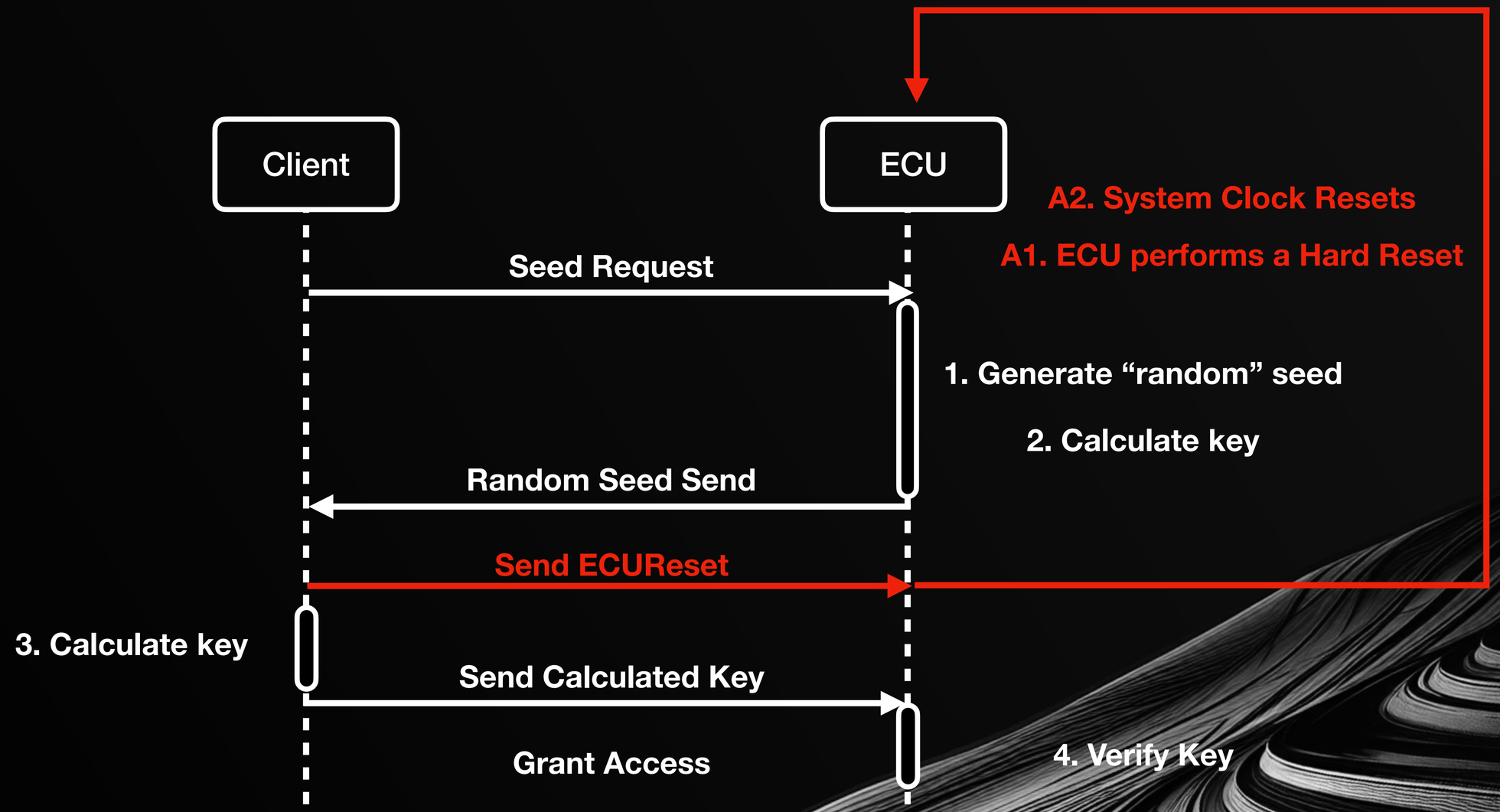


Typhoon AUXILIUM Pentest Labs cr0w's place labs

CASE IV - CONTROLLING THAT SEED



CASE IV - CONTROLLING THAT SEED



DEMO

CASE IV - CONTROLLING THAT SEED

- **First seed capture demo, revealed that seed generation has an iterative algorithm**
  - Assumption is that it's based on the system clock of the device
- **A hard ECUReset from UDS, should push the unit to perform a full power cycle**
  - As a result the system clock should reset to 0
- **While our assumptions should result in seed control, we saw no duplicates in our second demo**

CASE IV - CONTROLLING THAT SEED

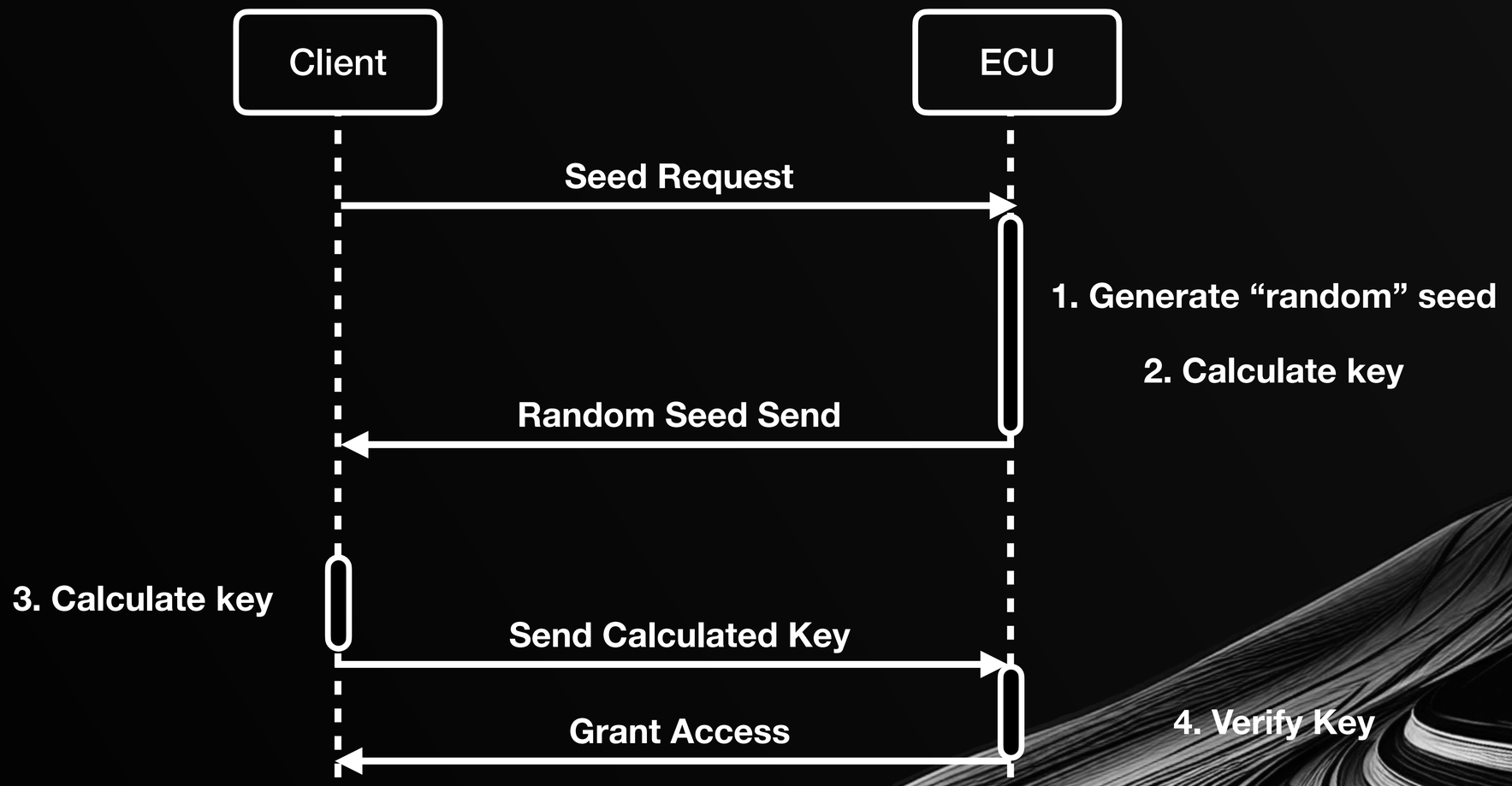
The answer is once again...

CASE IV - CONTROLLING THAT SEED

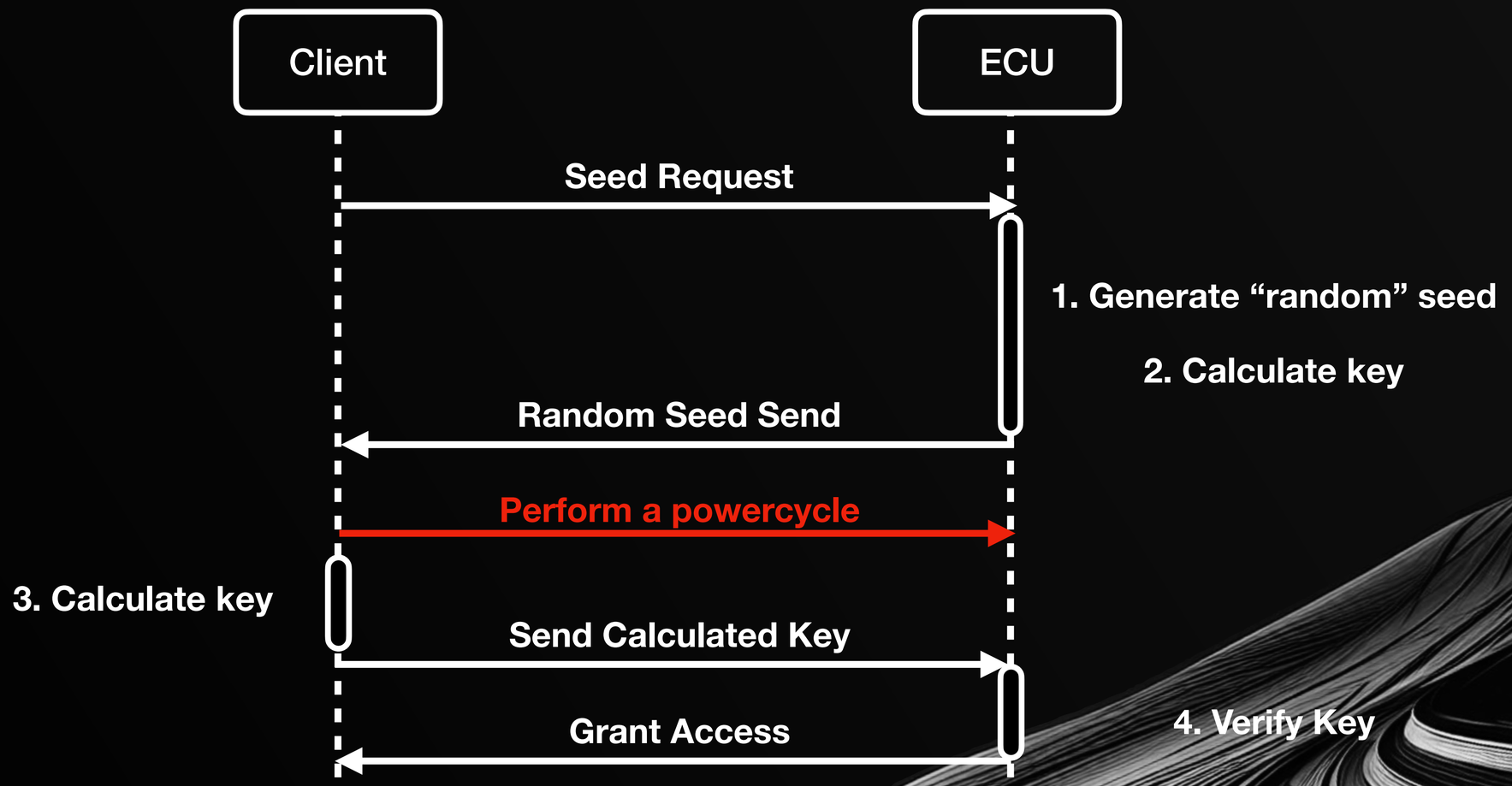
CASE U - THE FINALE

- What if the ECU is restricting software powercycles for safety reasons?
- What if there were more ways to control a powercycle?
- What if we had a nice relay?

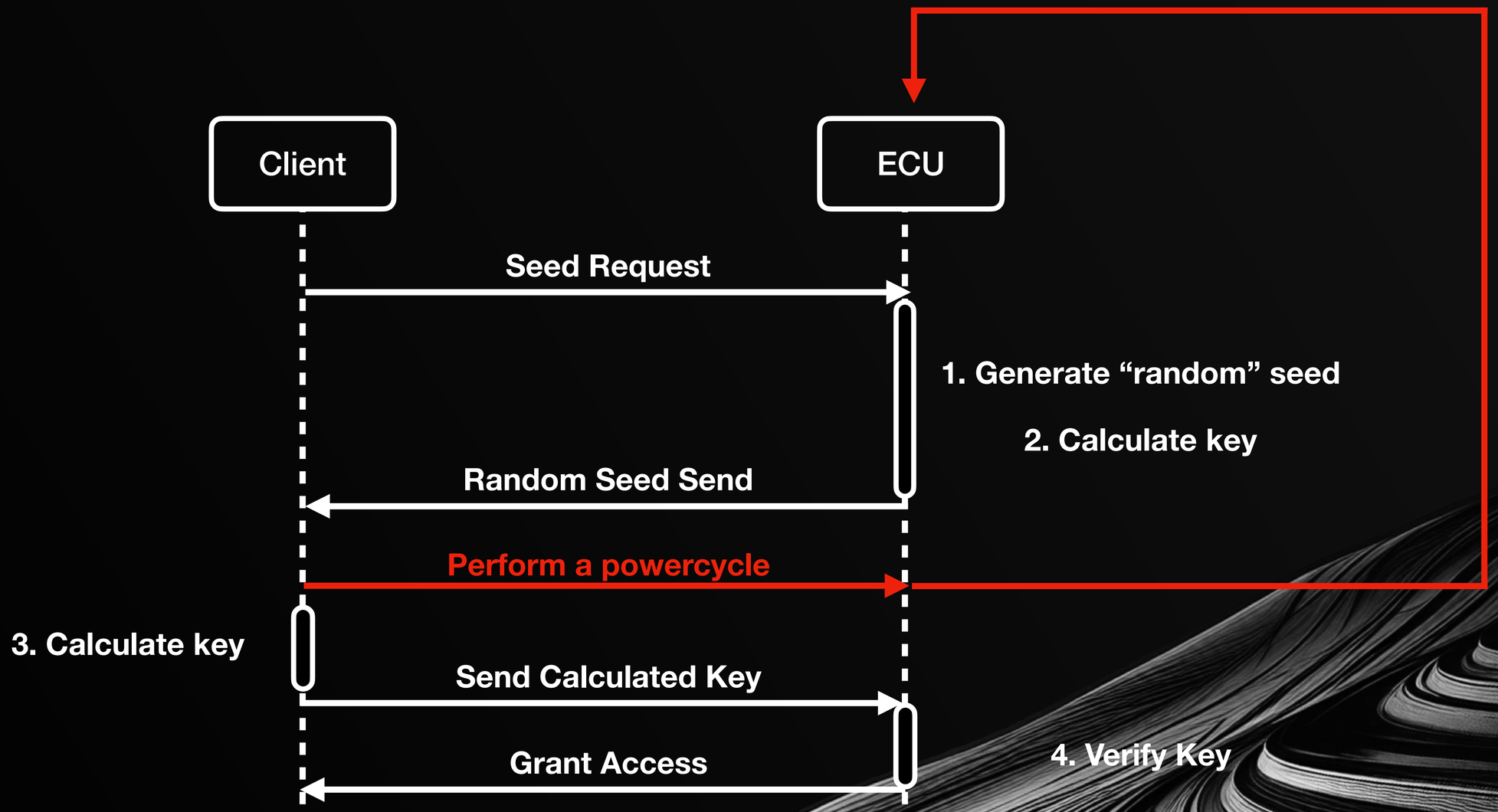
CASE U - THE FINALE



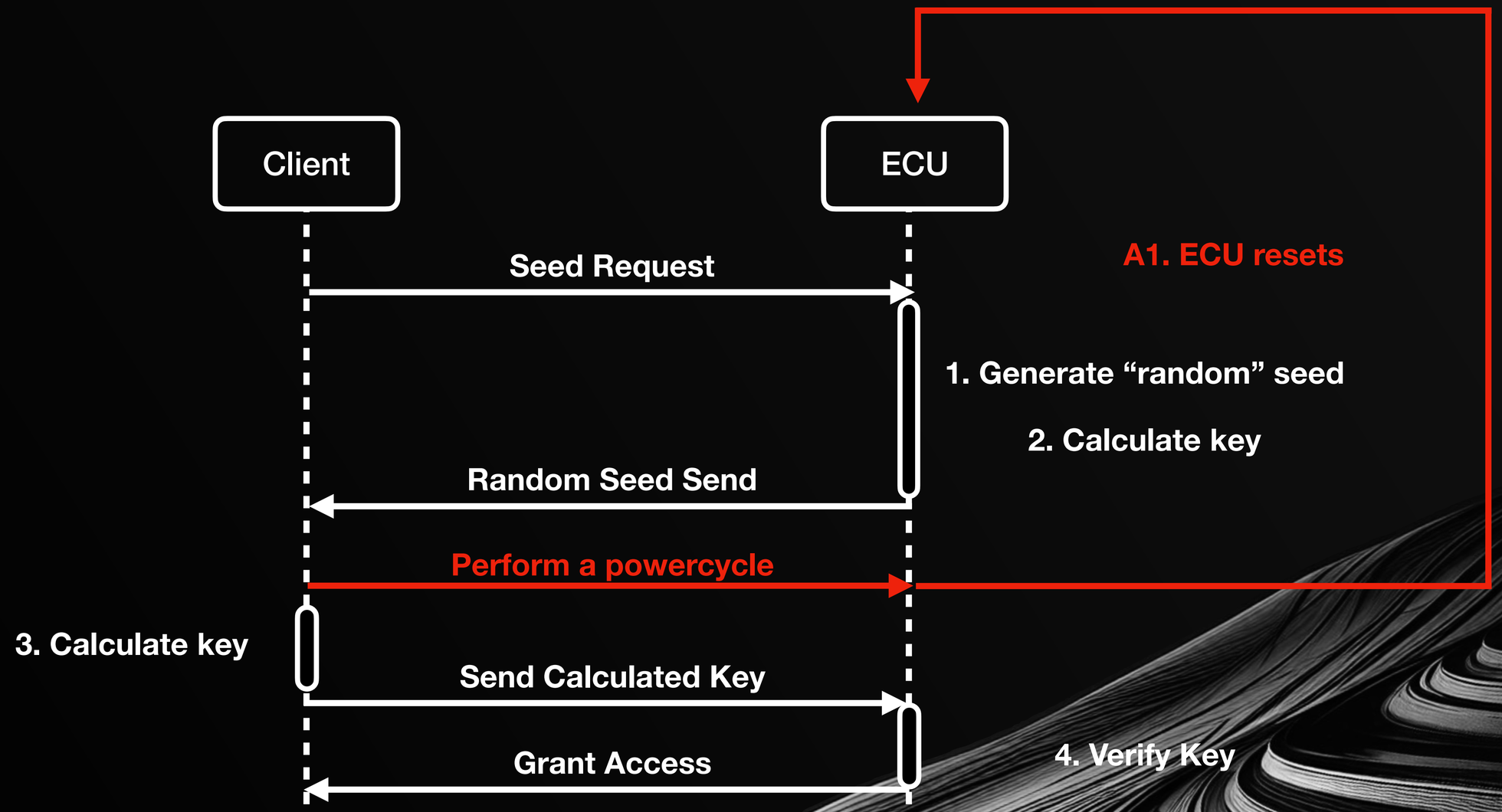
CASE U - THE FINALE



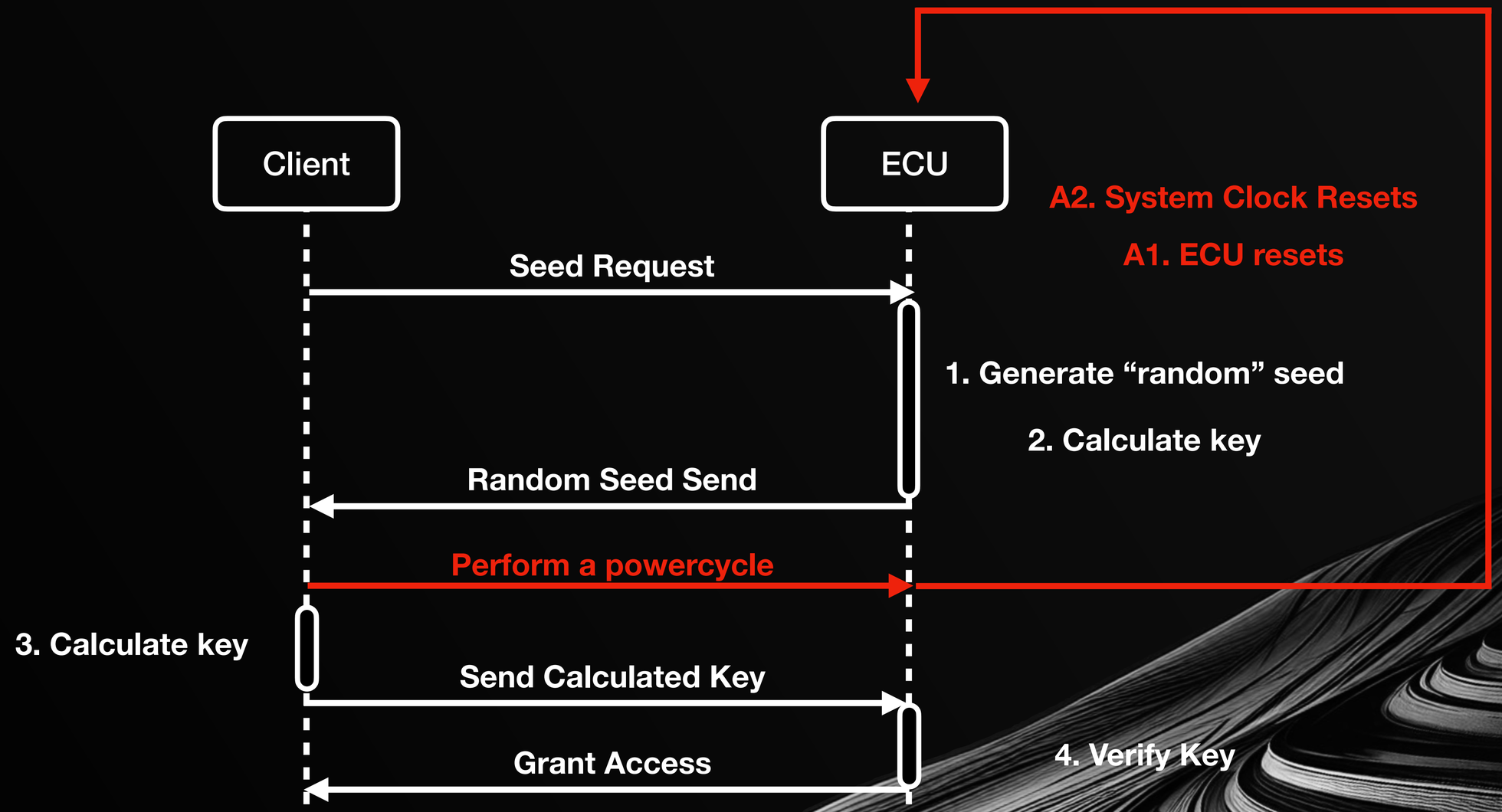
CASE U - THE FINALE



CASE U - THE FINALE



CASE U - THE FINALE



THE FINAL DEMO

And the only one you need

MY TWO CENTS

- **With this method we can effectively bypass several other mitigations:**
  - Restricted ECUReset[1]
  - Restricted bootloader access[1]
  - Restricted debug access ports
- **It is mainly applicable to test-bench setups, where we can effectively control the power supply of the ECU**
- **Can be applied to full vehicle, if it uses battery isolators**
- **Mainly utilised in heavy duty vehicles**

1.https://troopers.de/troopers22/agenda/tr22-993-uds-fuzzing-and-the-path-to-game-over

cr0wtom@kali-m1: ~/Tools/caringcaribou/tool

File Actions Edit View Help

```
┌──(cr0wtom㉿kali-m1)-[~/Tools/caringcaribou/tool]
└─$ python3 cc.py -i can0 uds_fuzz seed_randomness_fuzzer -d 1.102 10032701 0×7d4 0×7d5
```

```
┌──(cr0wtom㉿kali-m1)-[~/Tools/caringcaribou/tool]
└─$ candump can0,7D5:7D4
```

[1] 0:zsh* "kali-m1" 13:44 04-Jun-22

챕터 #4

THE FINISH LINE

And where the f@@k did ownership go.

THE HARD TRUTH

And now that we compromised the ECU, what?

THE HARD TRUTH

- **Can we change parts of the memory, and still use the ECU?**
  - Will the bootloader signature verification work?
- **If we tamper the compromised Bootloader, will the ECU still work?**
  - If the ECU works, will the rest of the vehicle work?

THE HARD TRUTH

THE HARD TRUTH

- **For Security:** Amazing, we just "killed two birds with one stone"
- **For ownership:** Good luck!

Typhoon AUXILIUM Pentest Labs cr0w's place labs

THE HARD TRUTH

Reminds you of something?

Typhoon AUXILIUM Pentest Labs cr0w's place labs

THE HARD TRUTH

THE HARD TRUTH

THE HARD TRUTH

THE HARD TRUTH

Do we actually own anything at this point?

THE HARD TRUTH

- We don't, but that's not how it has to be!
- Solutions can be implemented, which will make both sides "happy"
- Perfect solution might not exist, but who's perfect?

THE CONTROVERSIAL OPINION

- **Complete ownership of a vehicle can be allowed in a per user basis**
  - Vehicles are not mobile phones, they can pose a serious safety risk in the streets, not only for drivers and passengers, but also for pedestrians

- **While we proved that manufacturers are not doing their best, standards are developed to be followed and be challenged.**

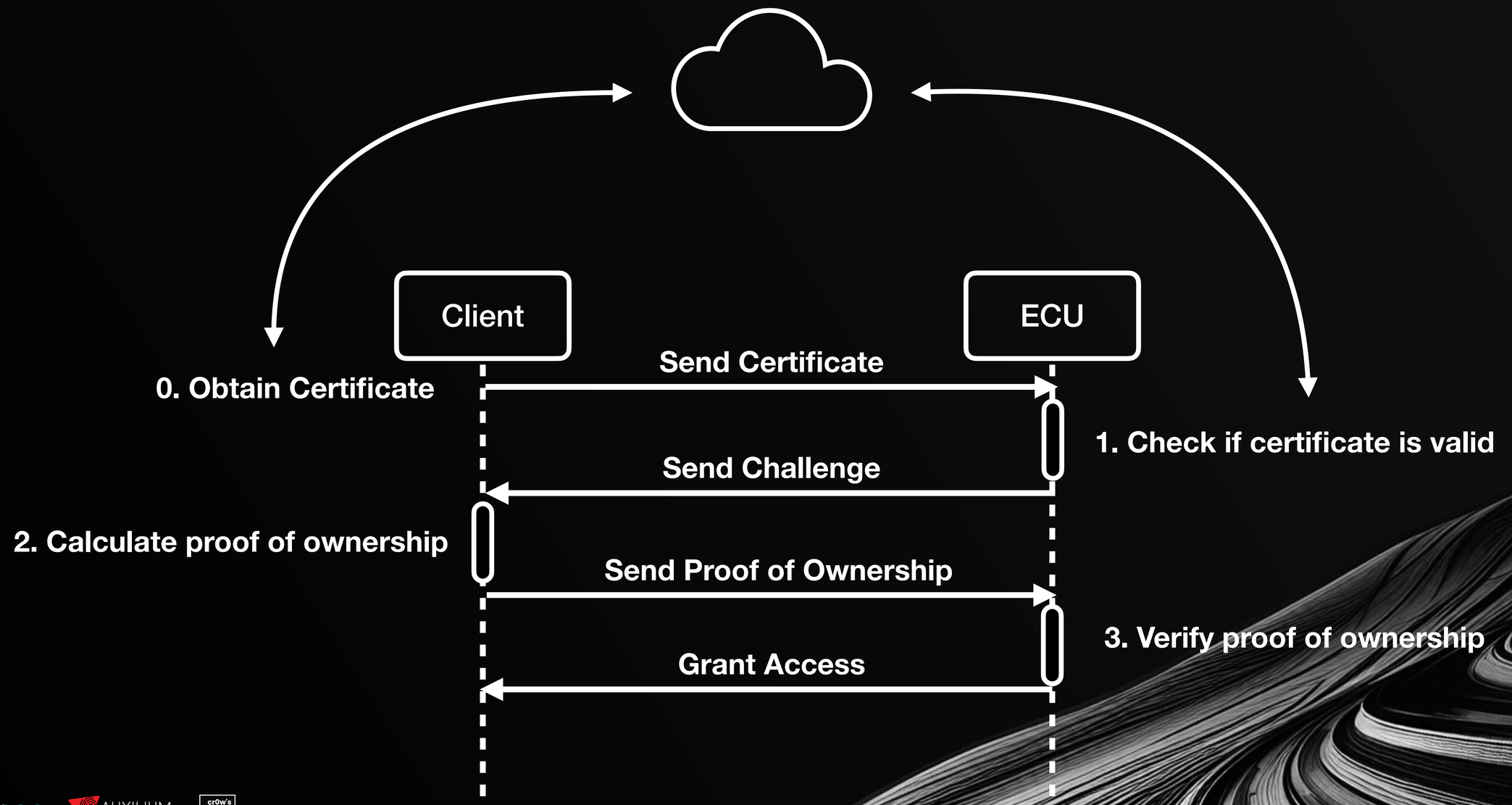
THE CONTROVERSIAL OPINION

- Tuning does not have to compromise security in order to achieve a goal
- Properly implemented User Access Control, can give access to specific functionality for tuning, but not to the whole vehicle and IP
- It can even be extended to "complete access" after EOL, with ultimate purpose to develop standardised aftermarket components to reduce waste and maintenance cost

MOVING FORWARD

- **UDS Service 0x29 (Authentication), already uses certificates for authentication**
  - With APCE, a PKI can also be implemented
- **Different levels of access can be created, maintained and managed by manufacturers**
- ***Users interested in tweaking their vehicles can register to obtain a "tuning specific certificate" which will unlock partial ownership of their vehicle***
  - ***Same can be done for developers***

MOVING FORWARD



Is there light in the end of the tunnel?

OPENAI / ARTIFICIAL INTELLIGENCE / TECH

OpenAI researcher resigns, claiming safety has taken ‘a backseat to shiny products’

Illustration: The Verge

/ Jan Leike’s departure shines a spotlight on a growing rift inside ChatGPT maker OpenAI.

By Kylie Robison, a senior AI reporter working with The Verge's policy and tech teams. She previously worked at Fortune Magazine and Business Insider.

May 17, 2024 at 8:32 PM GMT+2

29 Comments (29 New)

THE END

경청해 주셨어 감사합니다

Typhoon

Thomas Sermpinis
@CrOwTom | https://crOwsplace.com