
# A set of critical vulnerabilities in Smart-UPS devices

Yuval Sarel, Research Team Lead
Gal Levy, Senior Researcher

Read more – armis.com/TLStorm




ARMIS®

# Who Are We?

TLStorm

Yuval Sarel, Gal Levy

Security Research Team at **Armis Security**

Focuses on Vulnerability Research of Embedded Devices

Discover Critical Vulnerabilities that impact **Billions of Devices**

Design and Innovate Security Solutions




# Agenda

TLStorm

- What is TLStorm?
- What is CPS (Cyber Physical)?
- From encrypted FW to RCE
- Implications
- Live demo!

# What is TLStorm?

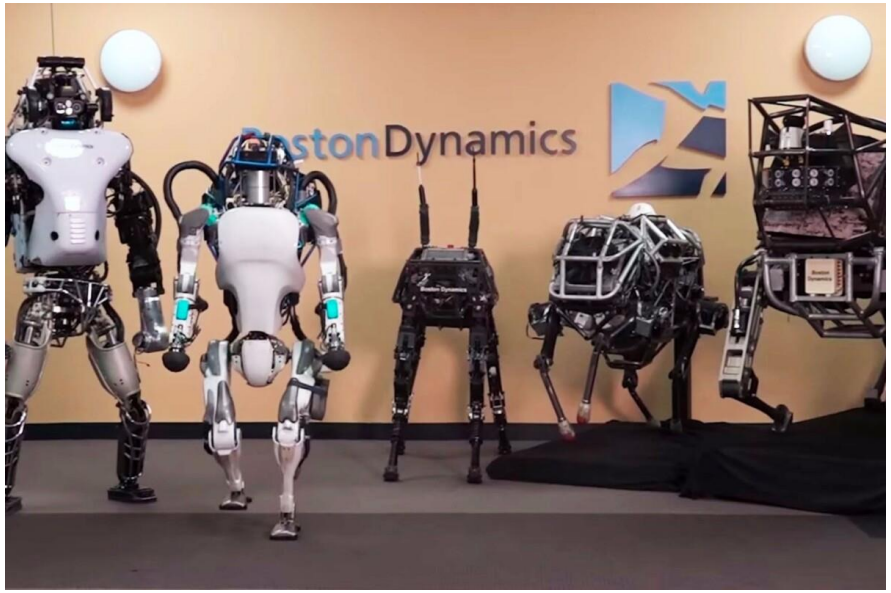
TLStorm

- 3 Critical vulnerabilities on APC's Smart-UPS product line
- RCE from the internet
- Physical damage
- "Over 20 million units sold" – APC
- 8/10 enterprises

# Cyber Physical Systems

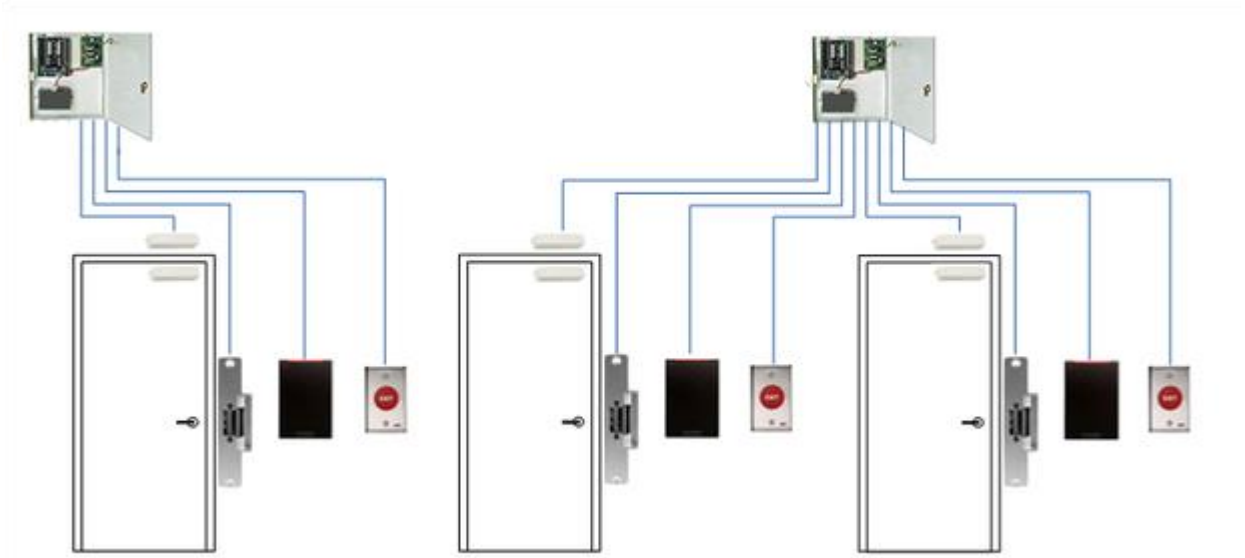
TLStorm

- CPS - Cyber Physical System
- “Connected computers with physical abilities”




# Cyber Physical Systems

TLStorm



# Cyber Physical Systems

TLStorm

# Cyber Physical Systems

TLStorm

# Cyber Physical Systems

TLStorm

# Cyber Physical as an Attack Vector

TLStorm

## Hack attack causes 'massive damage' at steel works

22 December 2014


The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

**A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.**

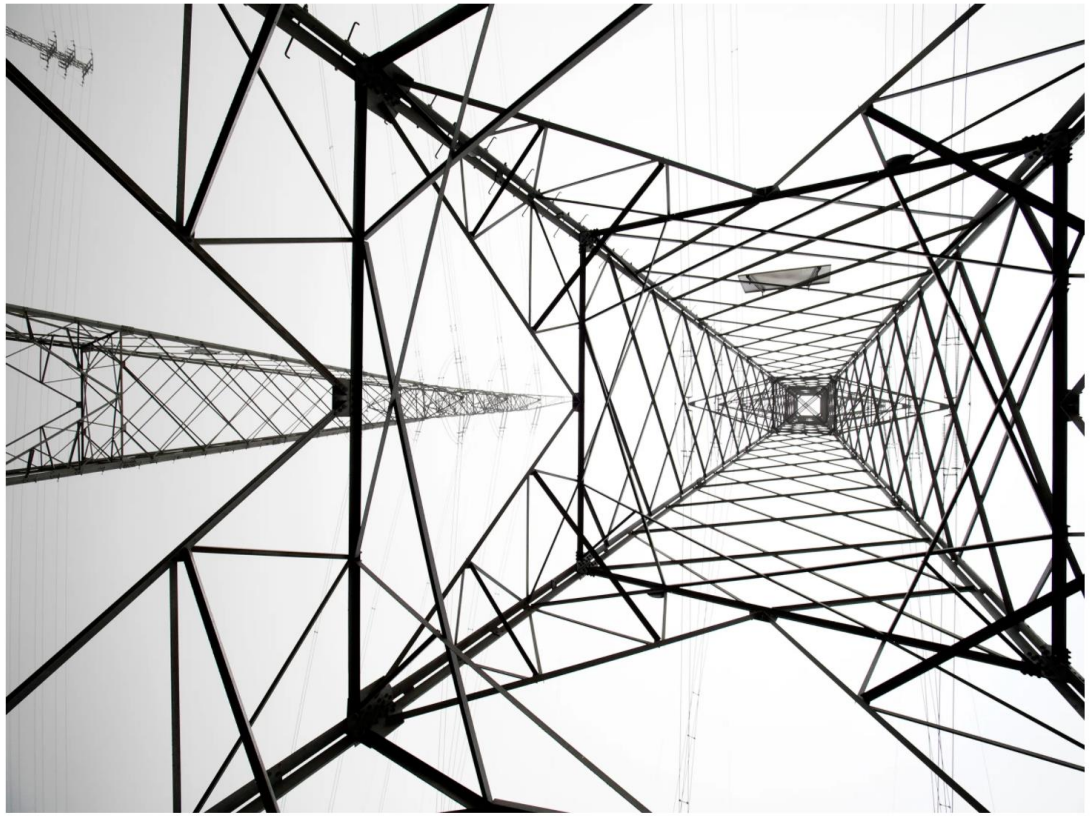
# Cyber Physical as an Attack Vector

TLStorm

KIM ZETTER SECURITY MAR 3, 2016 7:00 AM

## Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.



JOSE A. BERNAT BACET/GETTY IMAGES

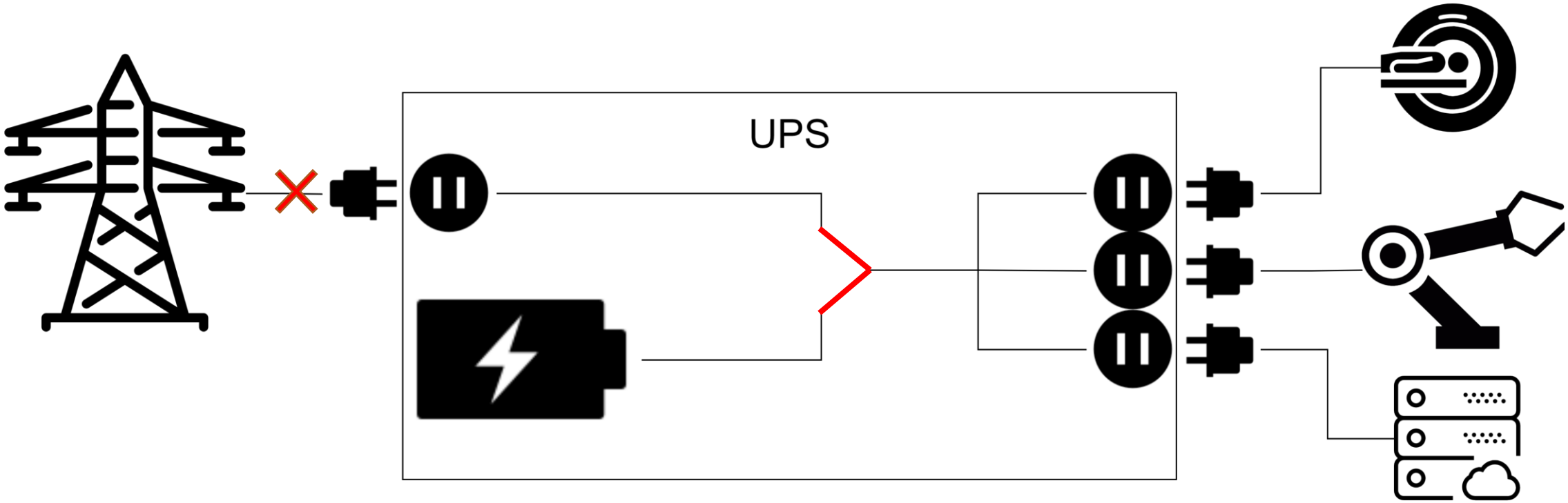
- "the first confirmed hack to take down a power grid"
- "…leaving more than 230,000 residents in the dark"
- "…First they [the attackers] reconfigured the […] **UPS**, responsible for providing backup power to […] the control centers…"

# UPS – Uninterruptible Power Supply

TLStorm

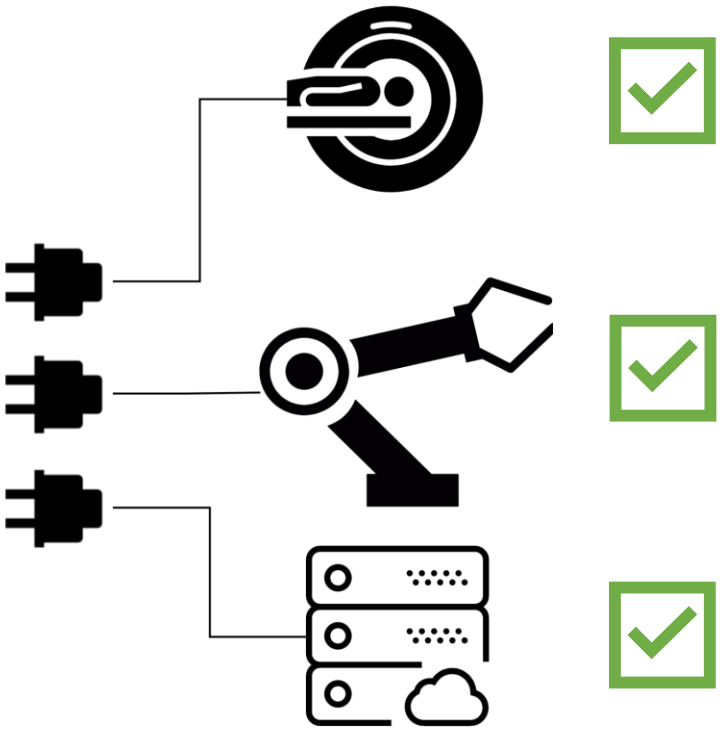
# UPS – Basic Operation

TLStorm



# UPS – Basic Operation

TLStorm

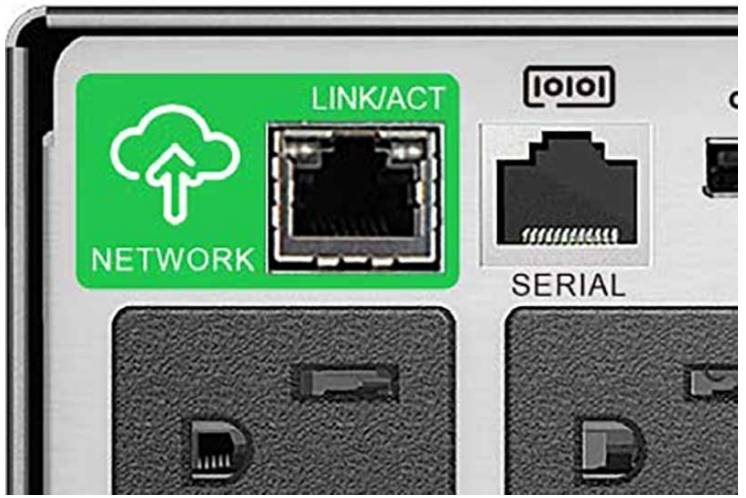


# UPS Vendor - APC

TLStorm

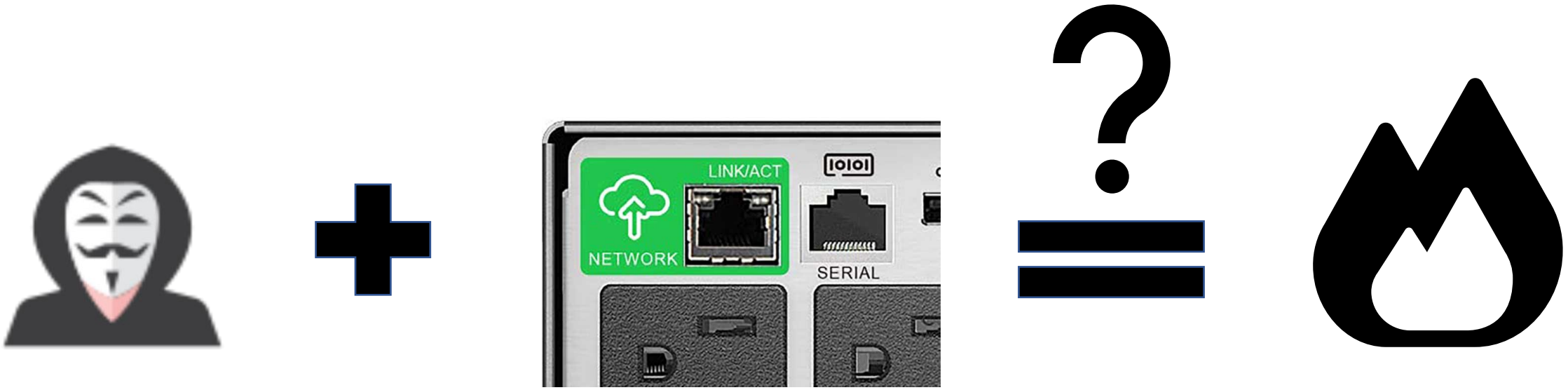
# Smart-UPS

- Analog device turned digital
- “Over 20 million units sold” - APC
- “SmartConnect”

# SmartConnect Attack Surface

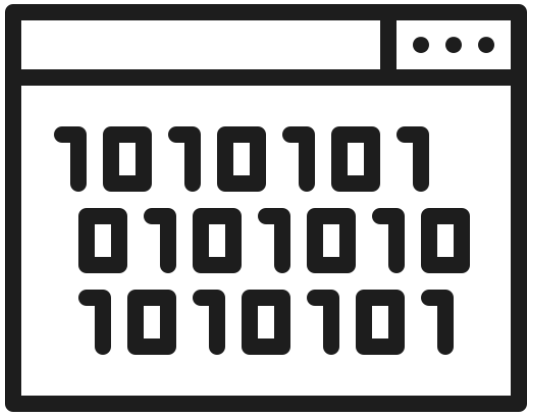
TLStorm



# Research Milestones

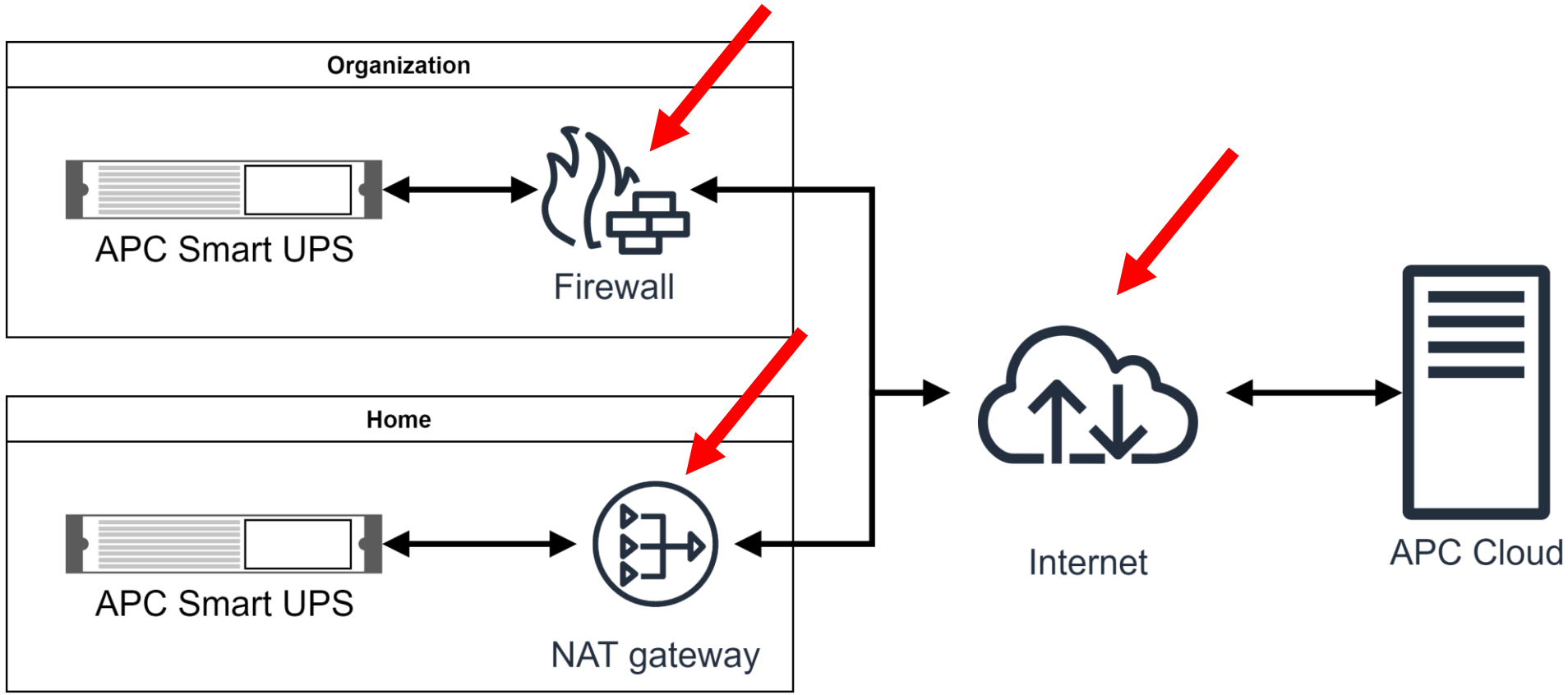
TLStorm

Internet Attack Vector → Remote Code Execution → Power Tampering



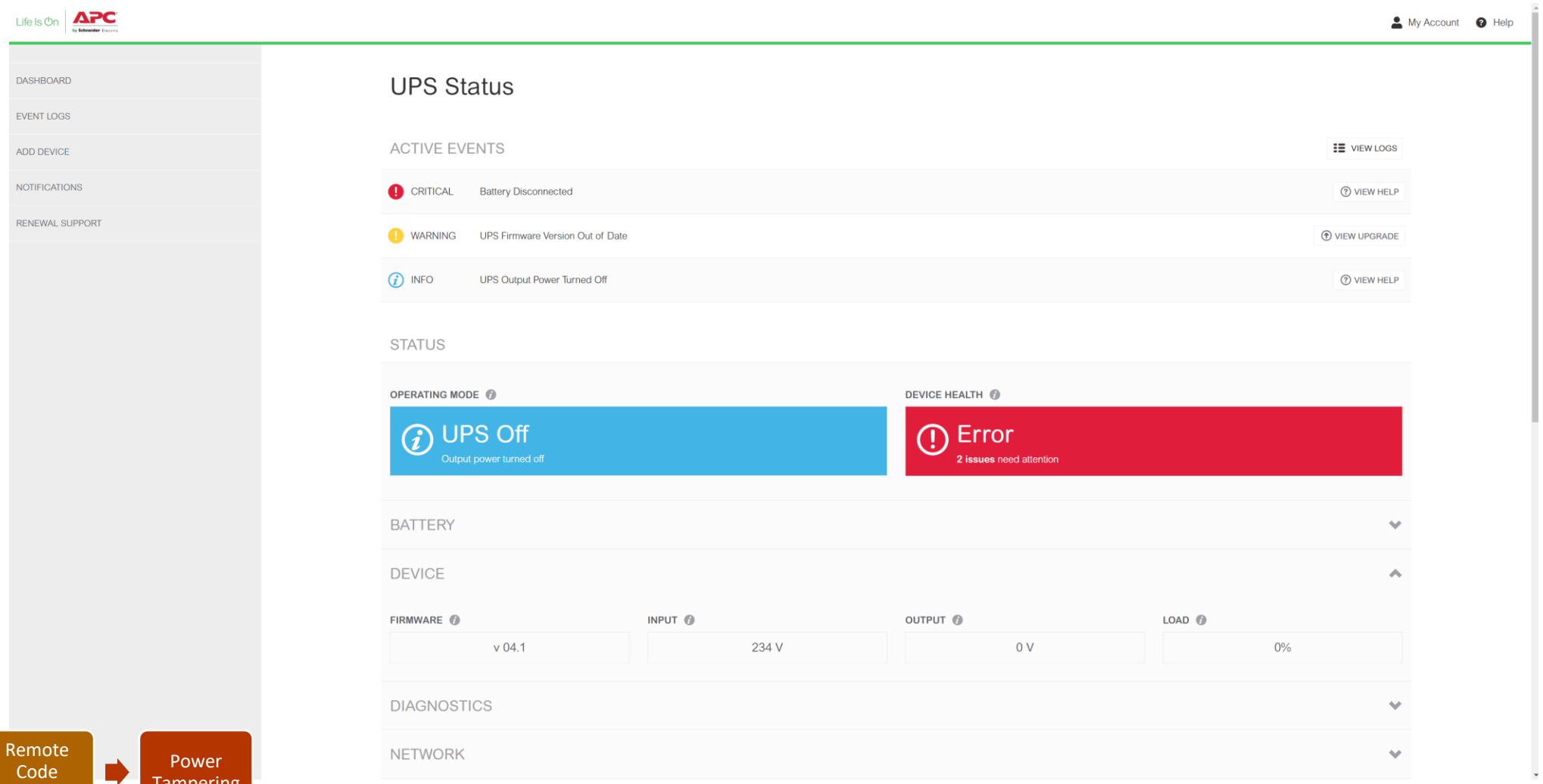

# SmartConnect - Overview

TLStorm




Internet Attack Vector → Remote Code Execution → Power Tampering

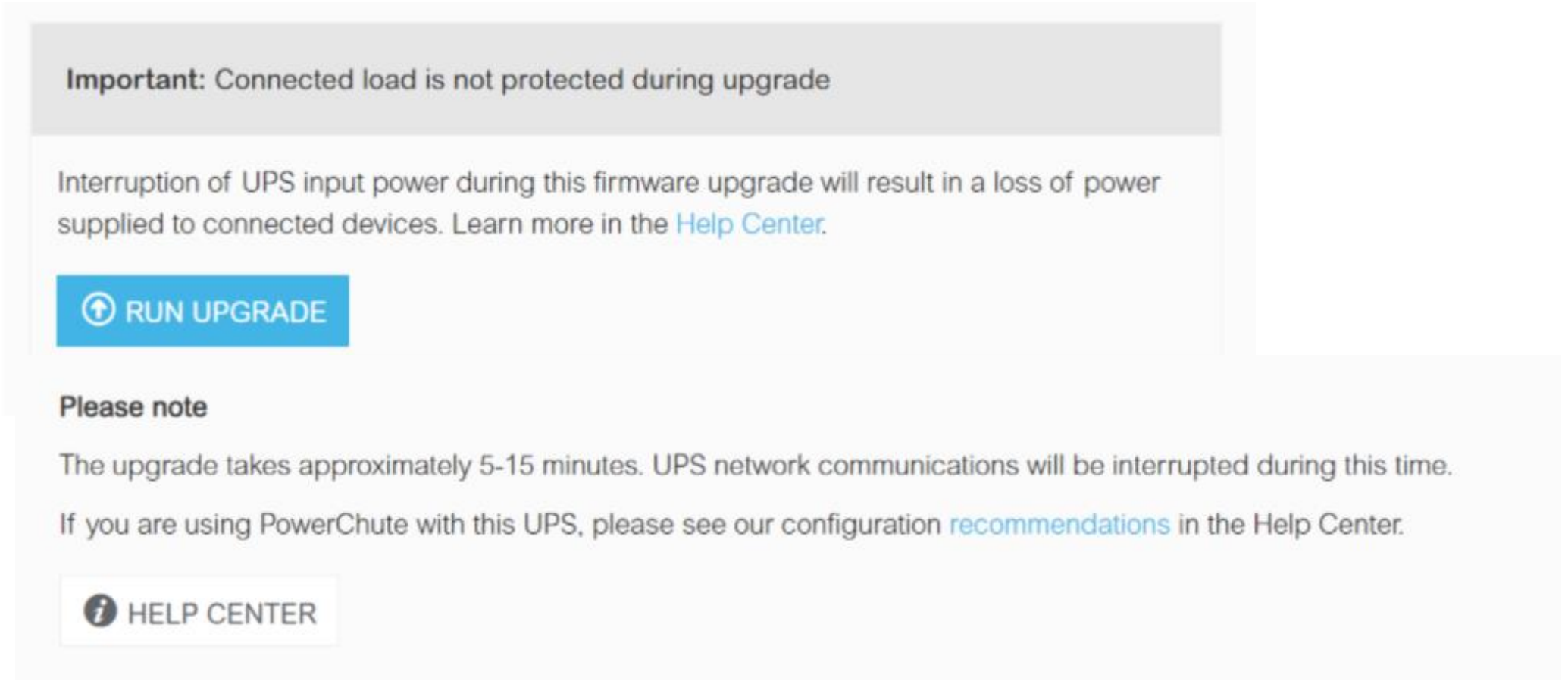
# SmartConnect - UI




Internet Attack Vector → Remote Code Execution → Power Tampering

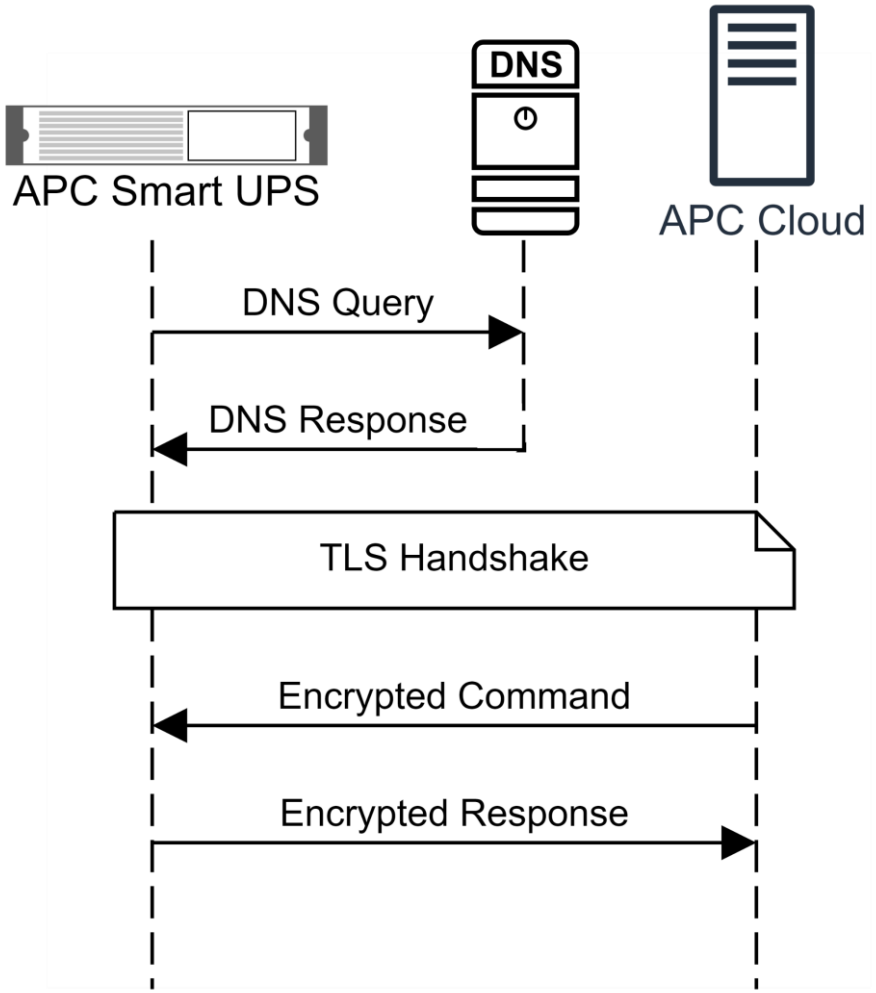
# SmartConnect – FW Update

TLStorm




Internet Attack Vector → Remote Code Execution → Power Tampering

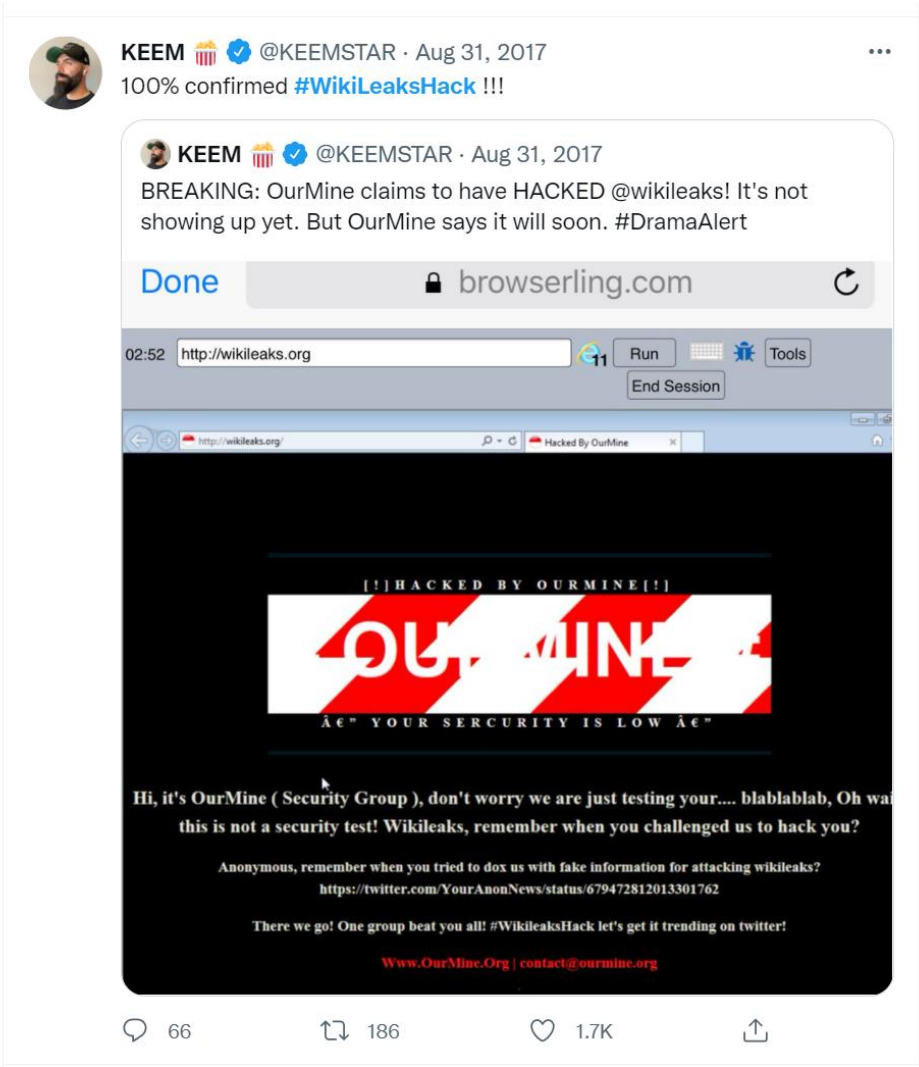
# SmartConnect – Connection Scheme




Internet Attack Vector → Remote Code Execution → Power Tampering

# DNS Spoofing

TLStorm




Internet Attack Vector → Remote Code Execution → Power Tampering

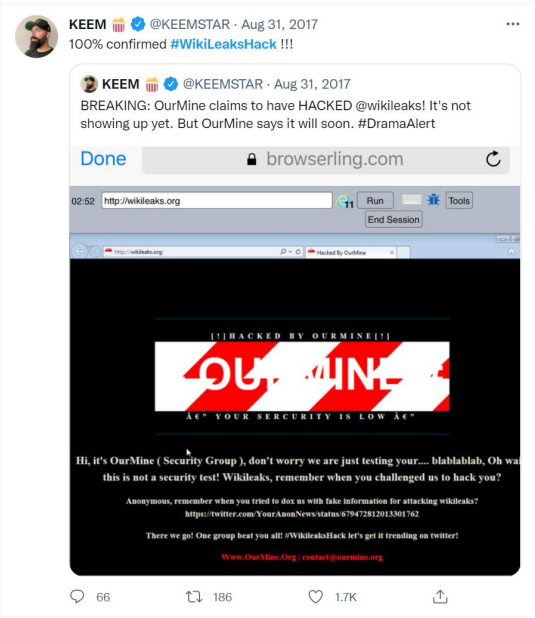
# DNS Spoofing

TLStorm

## DNS Poisoning Hits WikiLeaks

FRI | SEP 1, 2017 | 8:15 AM PDT

It has been trending on Twitter (#WikiLeaksHack), but in reality, it was a DNS poisoning served up by the hacker group OurMine.




Internet Attack Vector → Remote Code Execution → Power Tampering

# Research Milestones

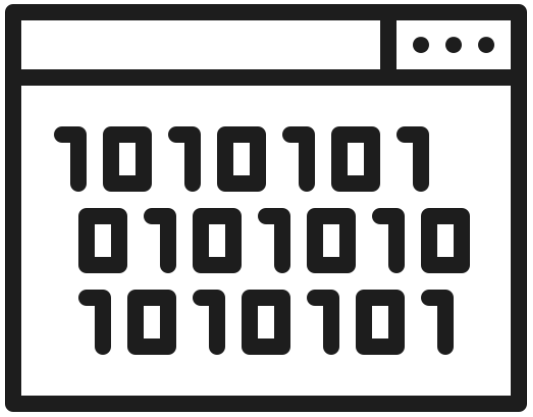
TLStorm

Internet Attack Vector

Remote Code Execution

Power Tampering

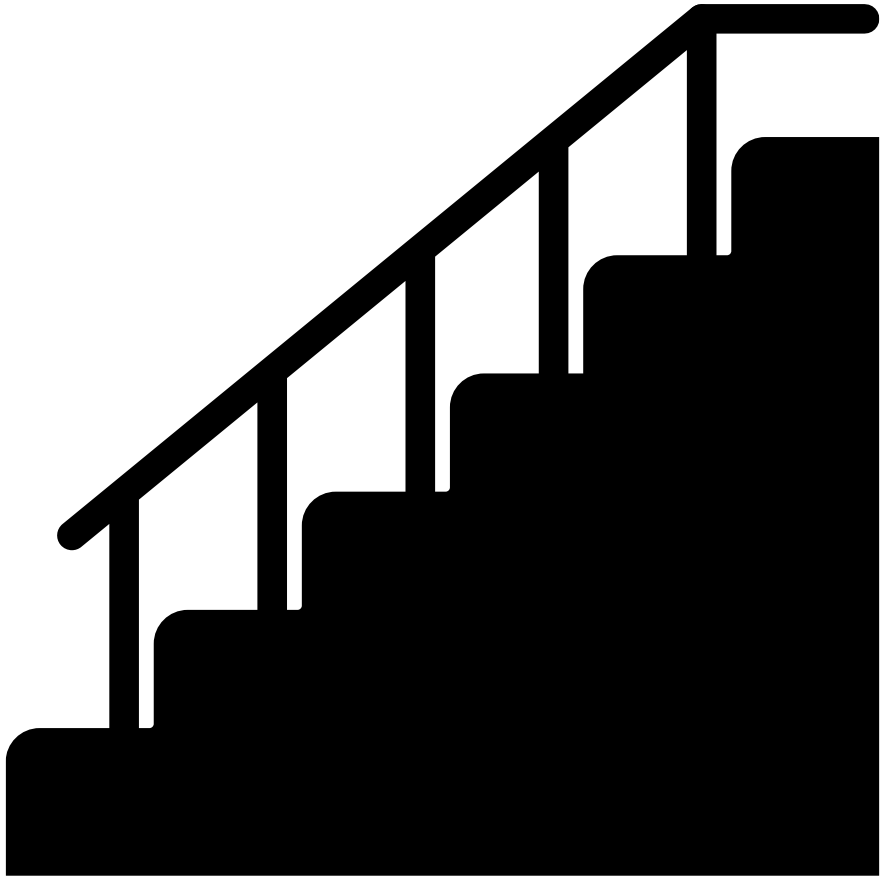
---




# RCE - Technical Steps

TLStorm

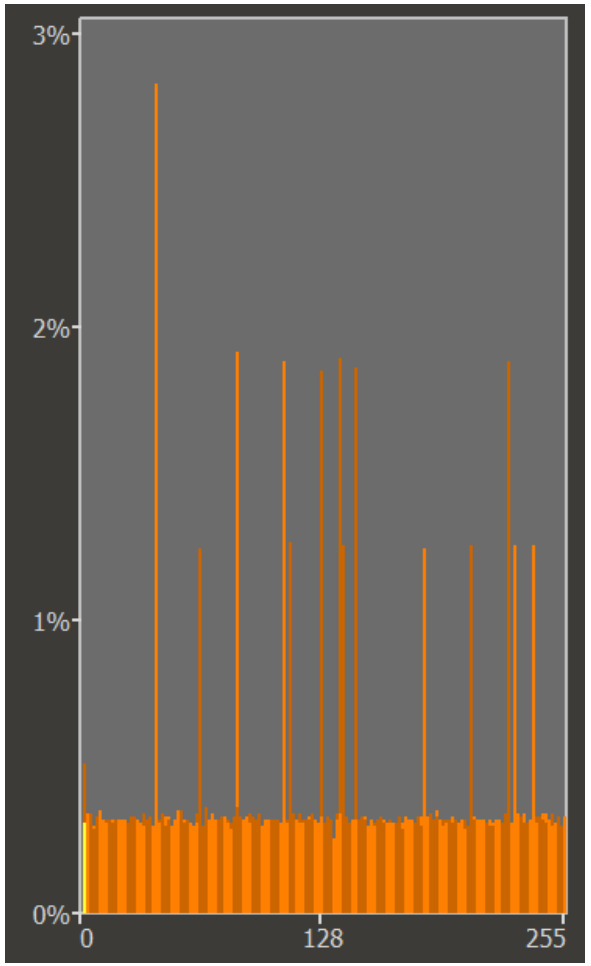
- Acquire FW for reversing
- Find RCE vulnerabilities
  - Pre-authentication
  - No user interaction
  - Internet access



# Initial Review

TLStorm

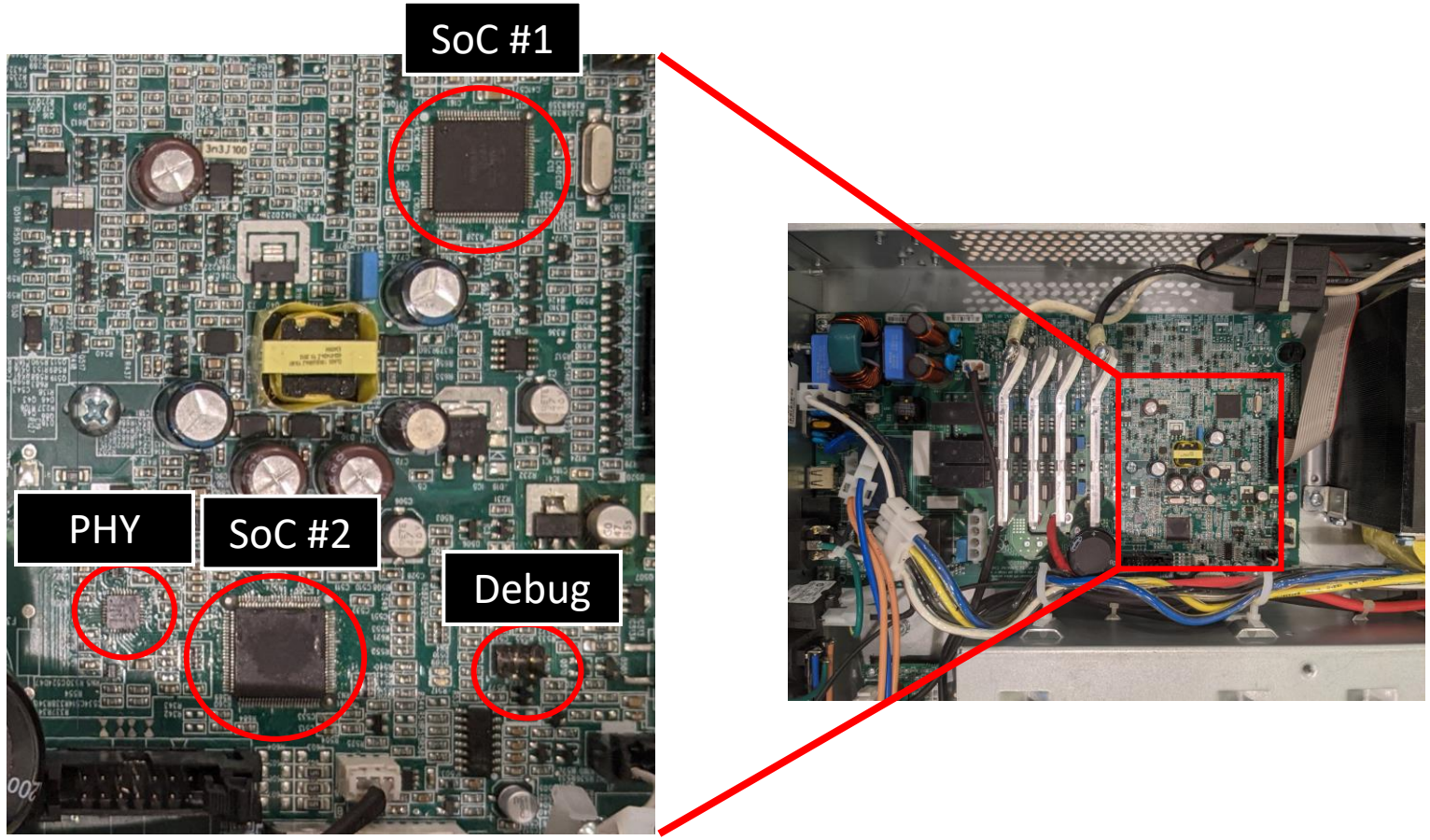
- File from update wizard
- Encrypted FW file
  - Characters are distributed (almost) equally
- Brute force failed




# FW Cracking

TLStorm

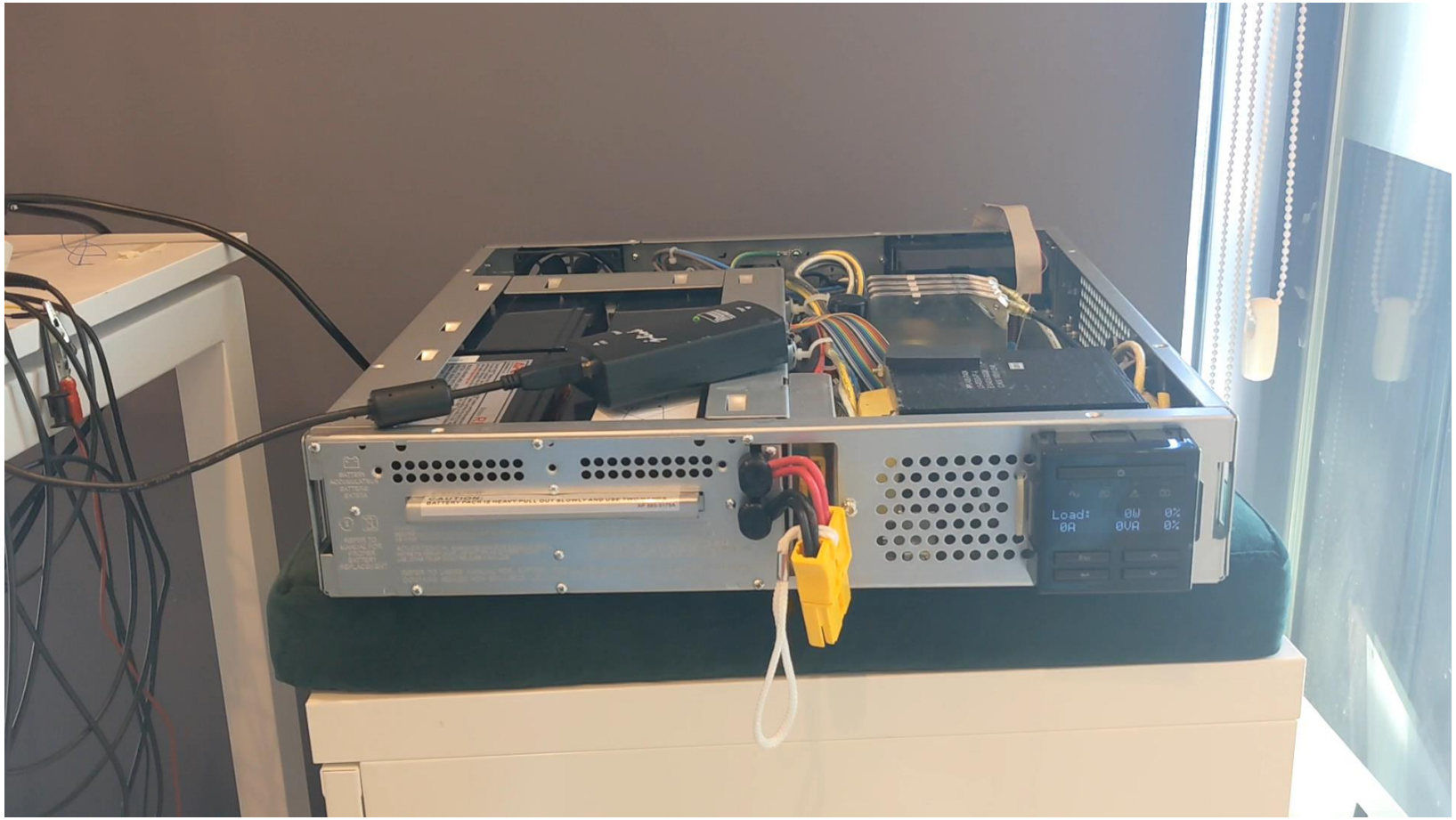
- 2 SoCs
- One closer to PHY
  - Uses Ethernet
- JTAG - debug interface




Internet Attack Vector → Remote Code Execution → Power Tampering

# Hardware Debugging

TLStorm

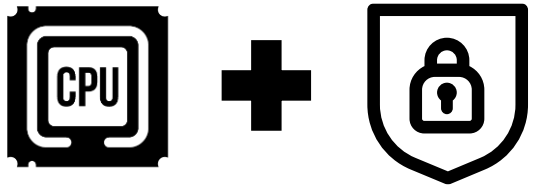



Internet Attack Vector → Remote Code Execution → Power Tampering

# Debugging Capabilities

TLStorm

- The Manual → CPU's datasheet
- RDP – read protection unit




### 2.6.3 Read protection (RDP)

[redacted]

No access (read, erase, program) to Flash memory [redacted] while the debug feature is connected [redacted]

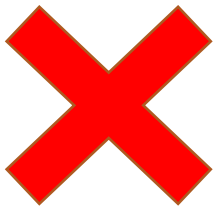
When Level 1 is active, programming the protection option byte (RDP) to Level 0 causes the Flash memory [redacted] to be mass-erased. [redacted]

Internet Attack Vector → Remote Code Execution → Power Tampering

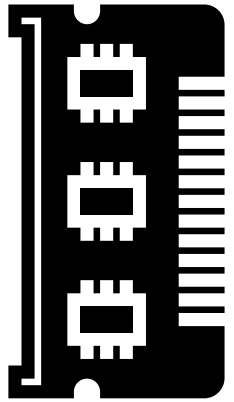
# RDP- Hardware Memory Protection

TLStorm


Flash Memory



RAM



# Smart-UPS Sub-Family – W/O SmartConnect

TLStorm


“With”

“Without”

Smart

RDP

FW Package Structure

Encryption A

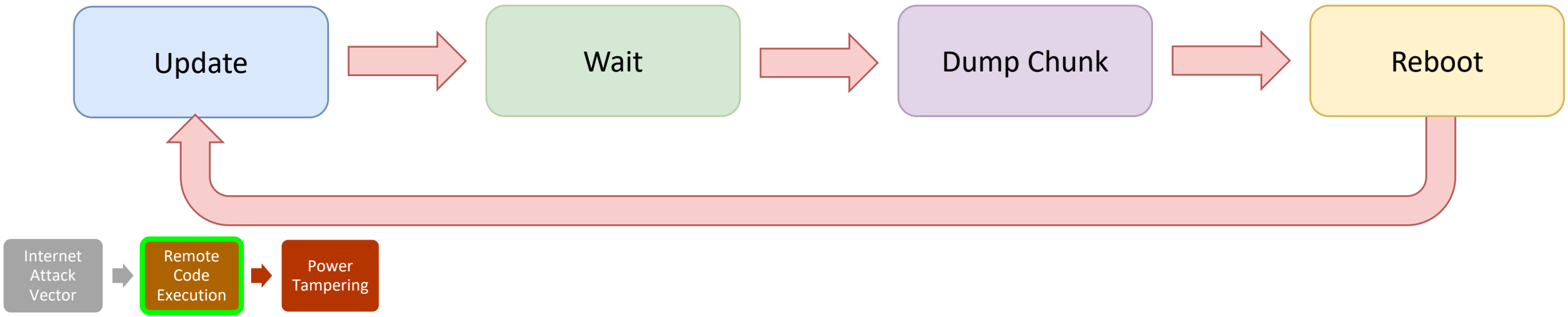
Encryption B


Internet Attack Vector → Remote Code Execution → Power Tampering

# Walking in The Dark

TLStorm

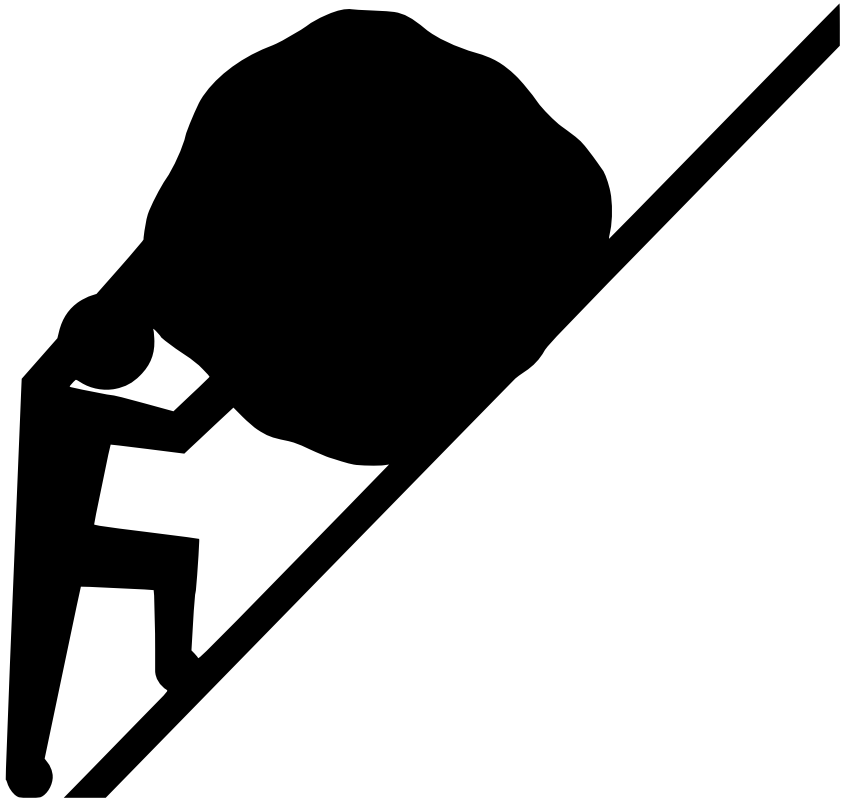
- Similar FW structure → Similar update process
- “Small” UPS update process:
  - Decrypting in chunks of 128 bytes
  - Chunk is stored in RAM
- Reminder – RAM is accessible w/ debug



# Running the Numbers

TLStorm

- Needs human interaction
  - Timing
  - Pressing buttons
  - Pulling battery
- Each iteration is ~5 minutes
- ~150K (FW size) / 128 (chunk size) = 1200

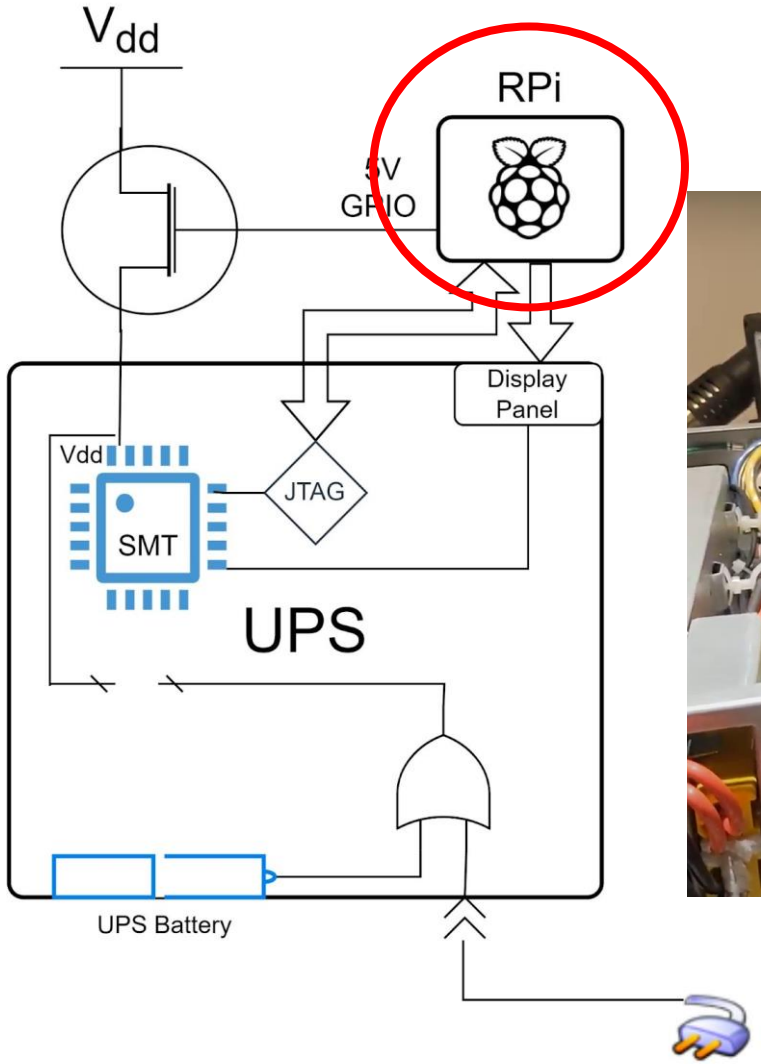


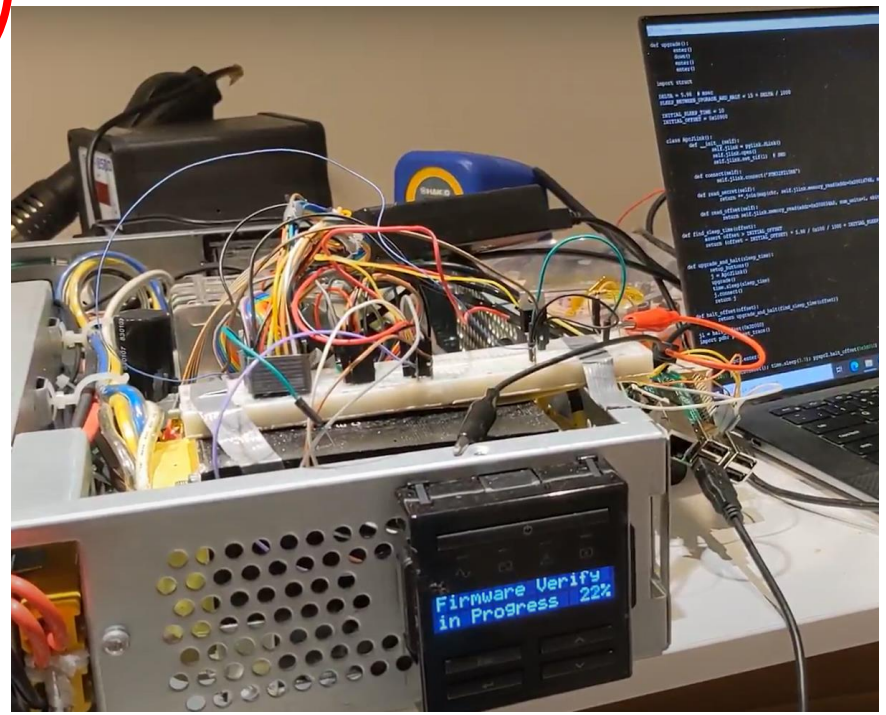
Internet Attack Vector → Remote Code Execution → Power Tampering

# Hardware Brute-Force

TLStorm

- An RPi will be the orchestrator:
  - Power
  - Buttons
  - Debug
  - Timing
- Bootloader = decryption

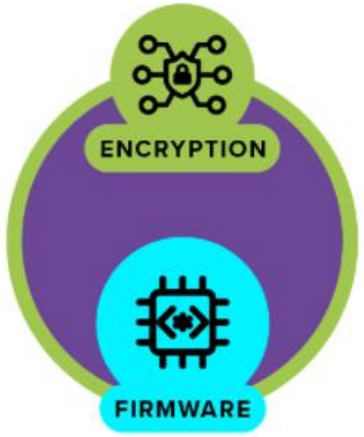


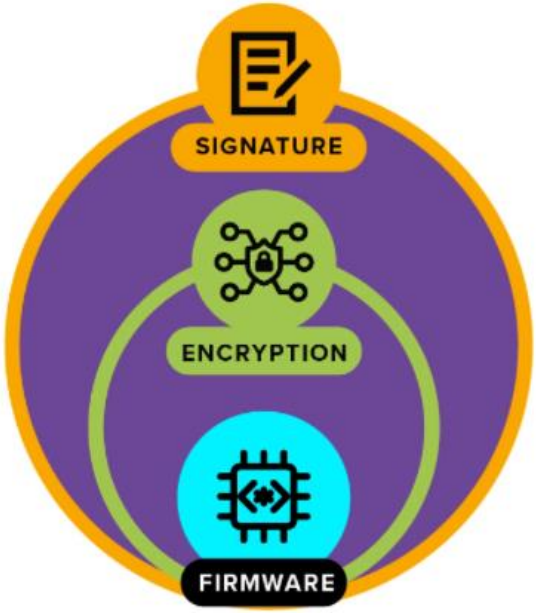

Internet Attack Vector → Remote Code Execution → Power Tampering

# Decrypted FW Findings

- FW is encrypted but **not** signed
  - Symmetrical encryptic
  - CVE-2022-0715
- Install malicious FW
  - USB
  - LAN → RCE



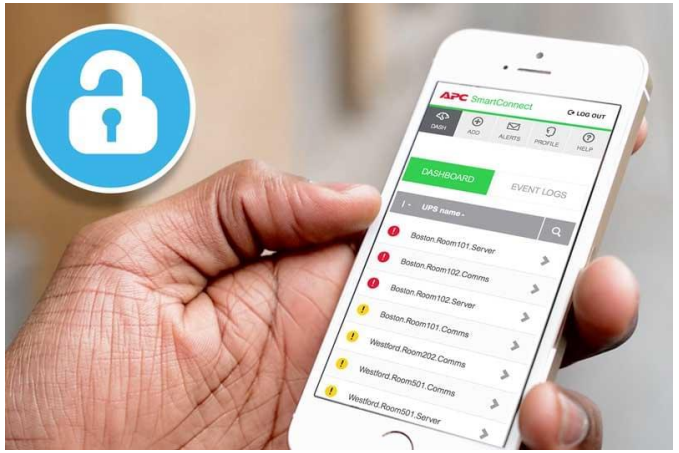

≠

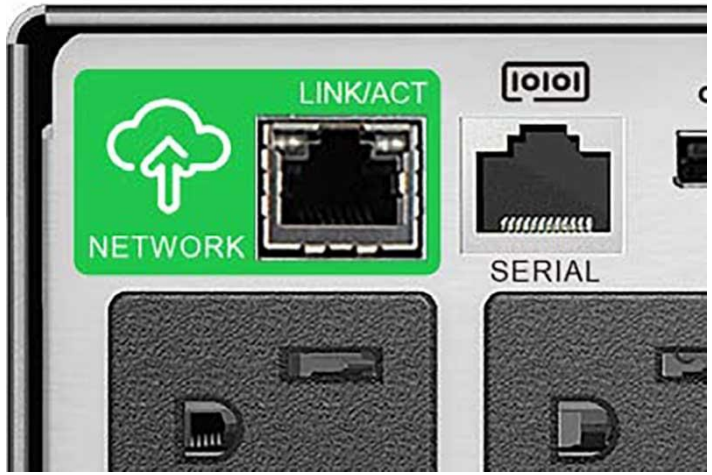



# SmartConnect Attack Surface

TLStorm

- SmartConnect = internet connectivity
- Connection is authenticated with TLS
- NanoSSL library by Mocana




MOCANA®

Internet Attack Vector → Remote Code Execution → Power Tampering

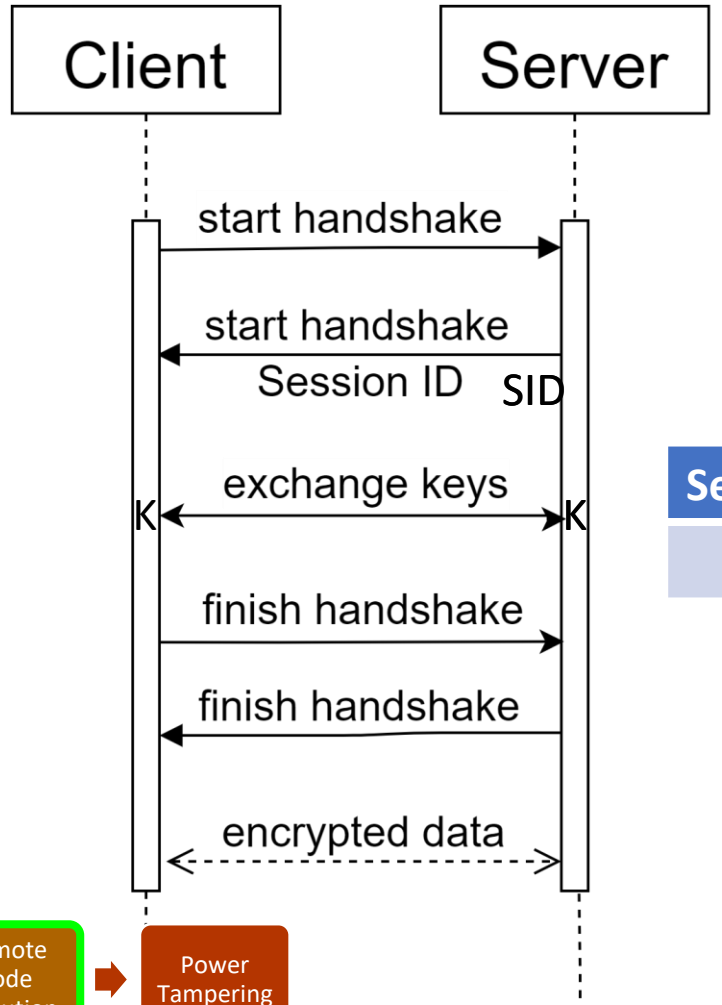
# External Risk

TLStorm

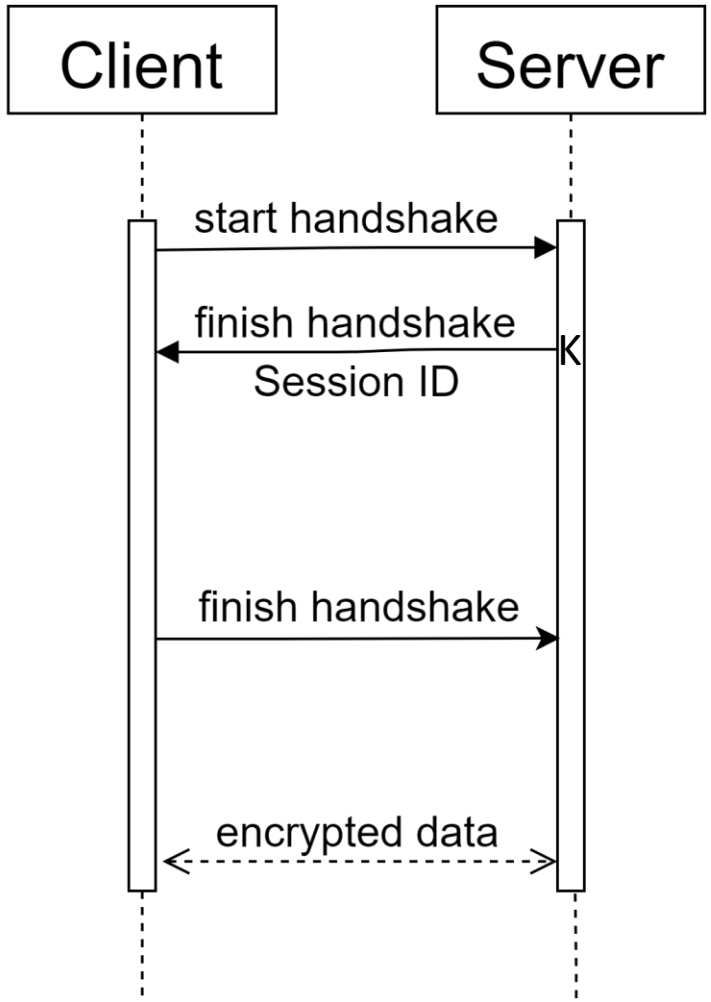
- External library brings in an external risk with it
- But also internal…
- Look for the “glue-logic”
- Return value is ignored by APC
- Result - two pre-authentication critical vulnerabilities:
  - TLS reassembly heap overflow
    - CVE-2022-22805
  - TLS authentication bypass
    - CVE-2022-22806

```
int recv_tls_async(ssl_t* ssl_sock)
{
    ...
    func_tbl->mocana_ssl_recv(ssl_sock, pbuf);
    ...
    if (ssl_sock->state == COMPLETE)
        handle_payload(ssl_sock);
    pbuf_free(pbuf);
    ...
}
```

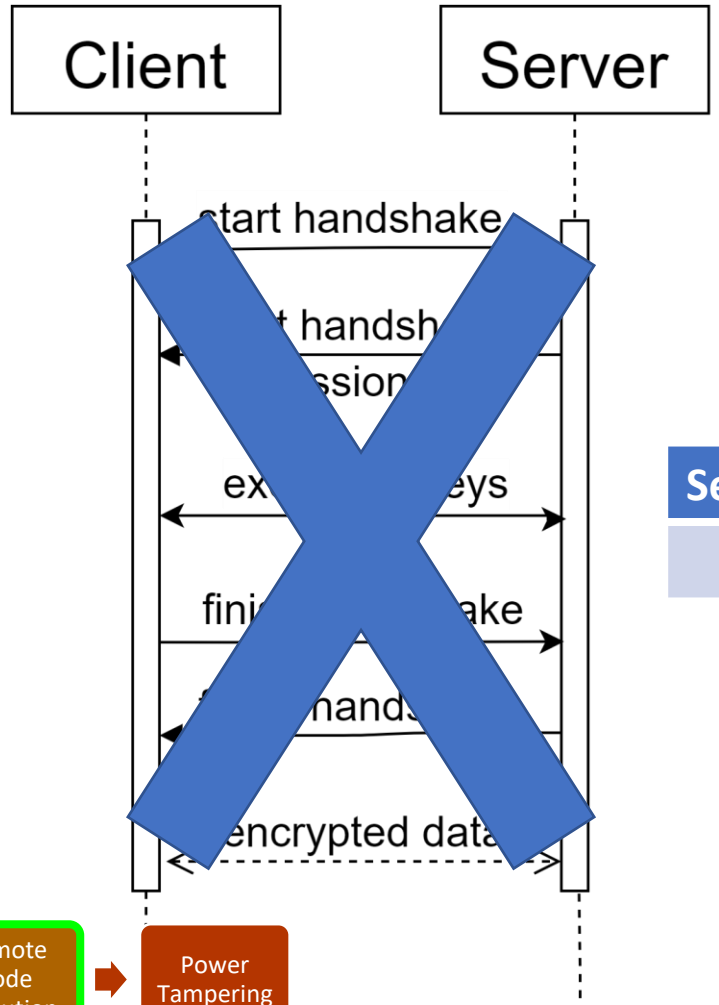
# TLS Resumption



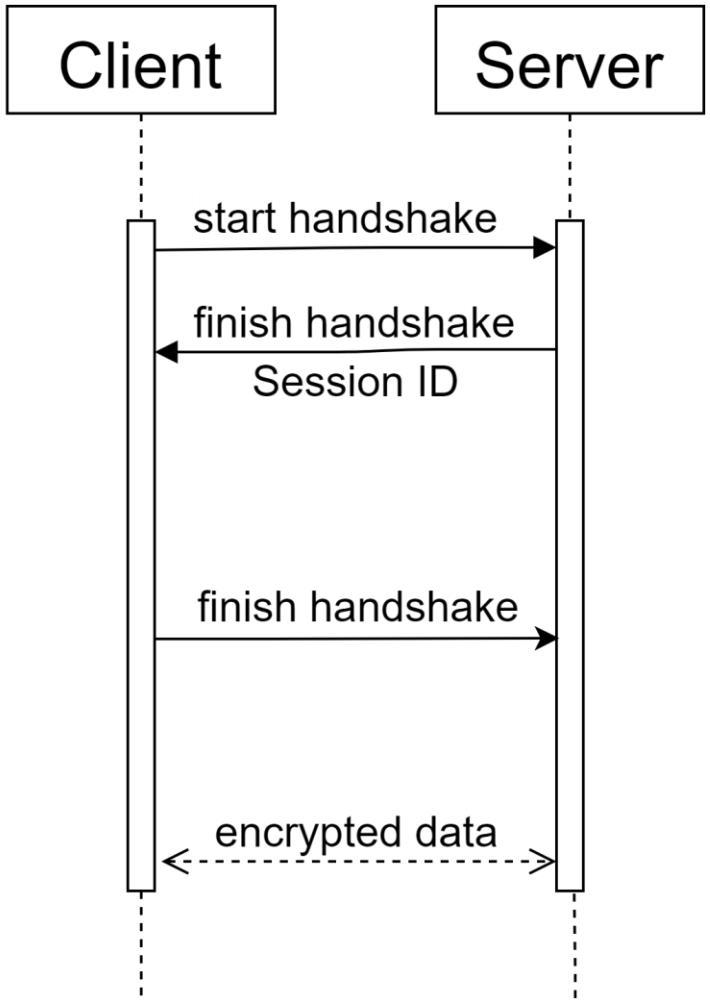

| Session ID | Master Secret |
|---|---|
| | K |




# Pre-Auth-Resumption




| Session ID | Master Secret |
|---|---|
| ? | ? |




Internet Attack Vector → Remote Code Execution → Power Tampering

# Mocana Handshake

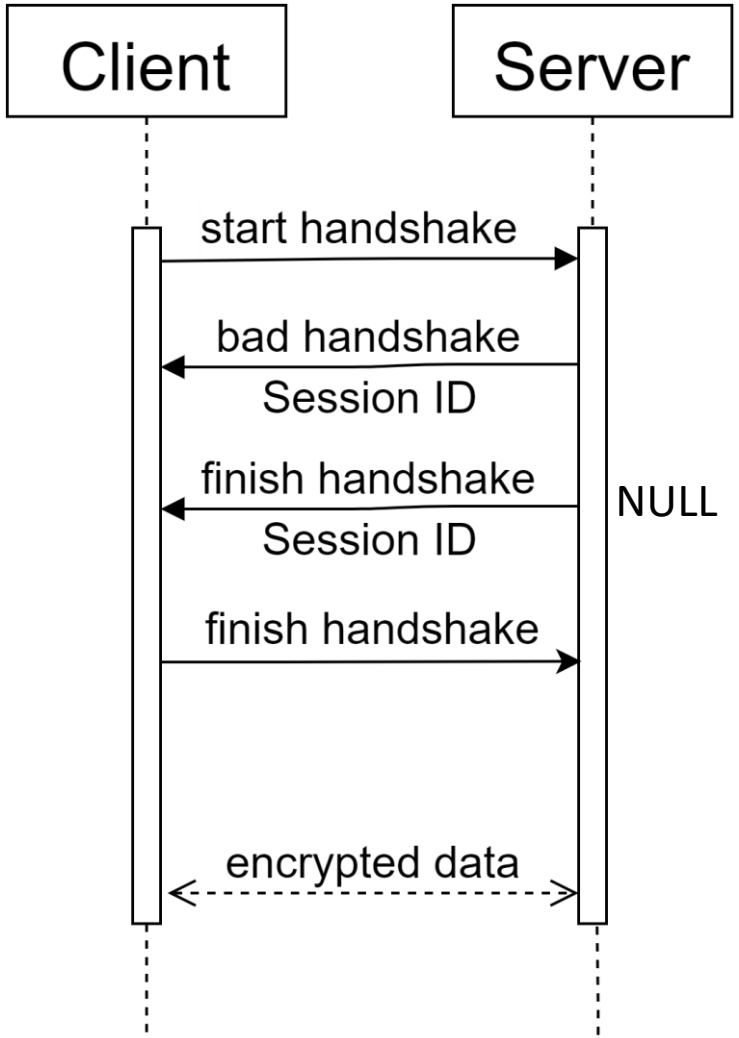
TLStorm

- Session ID is saved DURING handshake process
- Master Secret is generated AFTER successful handshake
- Session is not cleared in case of failure
- Partial control of the session object

```
int mocana_ssl_handshake(...)
{
    ...
    ssl_sock->resumption = FALSE;
    if (memcmp(session_id, ssl_sock->id, id_len))
        ssl_sock->resumption = TRUE;
    if ( !ssl_sock->resumption ) {
        memcpy(ssl_sock->id, session_id_pointer, id_len);
    }
    ssl_sock->cipher_suite = get_supported_suite(ssl_sock)
    ...
    if ( !ssl_sock->cipher_suite )
        return NO_CIPHER_SUITE;
    if ( ssl_sock->resumption ) {
        memcpy(ssl_sock->key, ssl_sock->cached_key, 48);
  ...
}
```

# Mocana Pre-Auth-Resumption

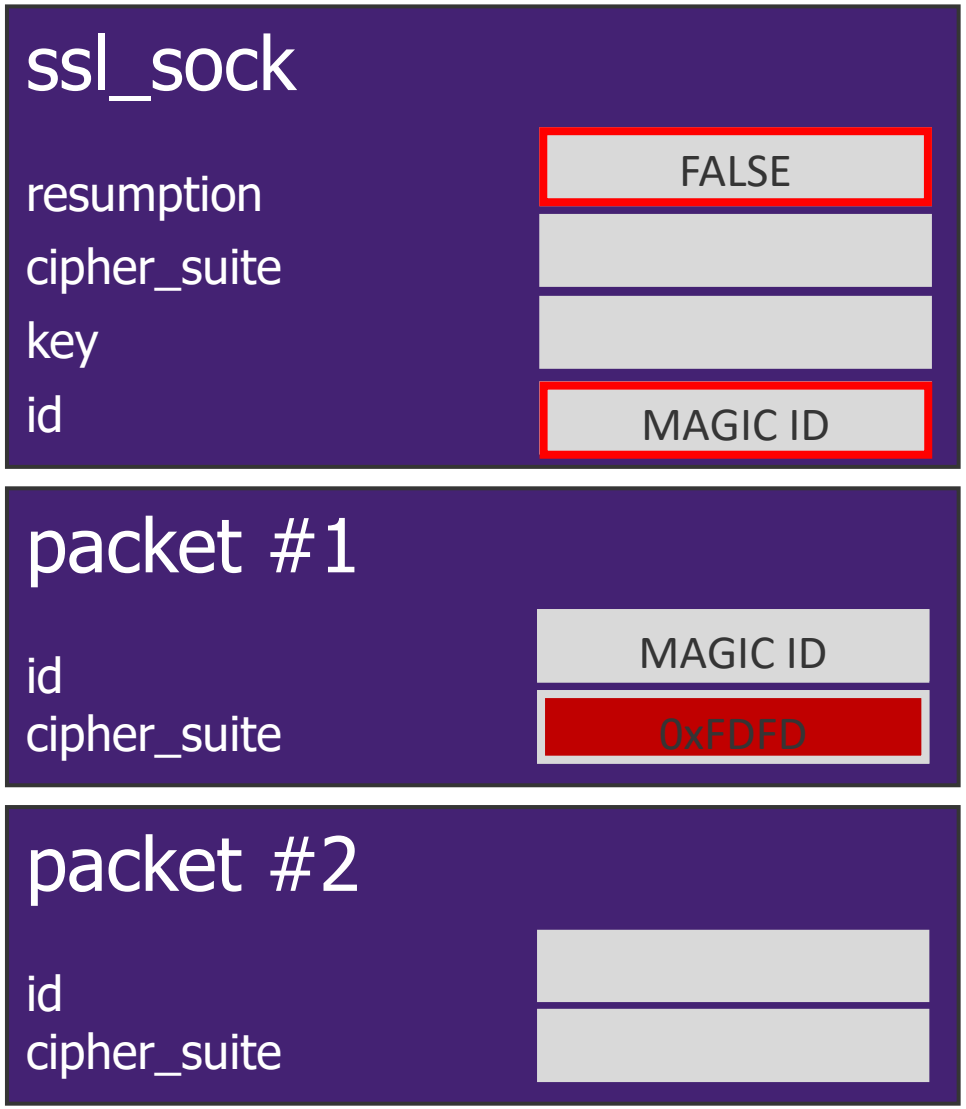
| Session ID | Master Secret |
| --- | --- |
| NULL | NULL |




Internet Attack Vector → Remote Code Execution → Power Tampering

# Pre-Auth-Resumption Debug View

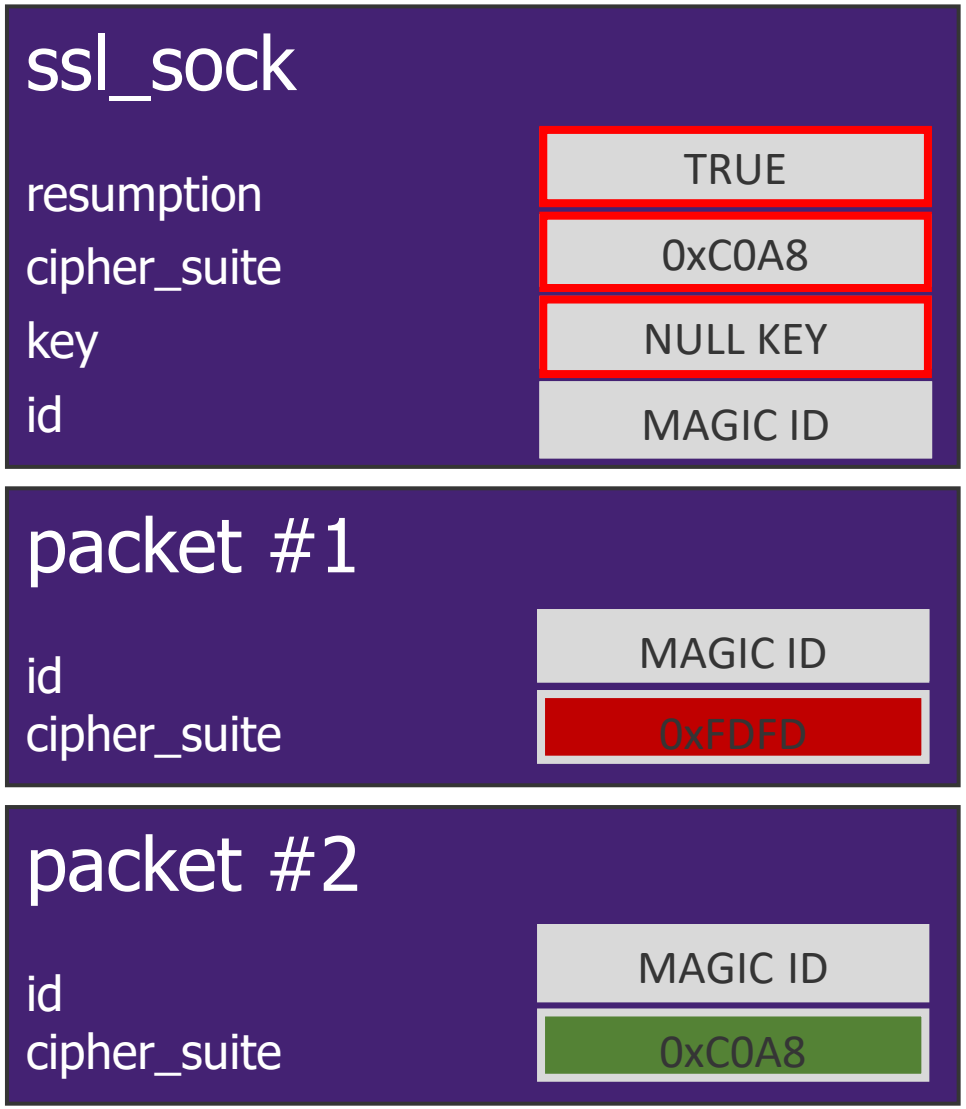
TLStorm




```
int mocana_ssl_handshake(...)
{
    ...
    ssl_sock->resumption = FALSE;
    if (memcmp(session_id_received, ssl_sock->id, id_len))
        ssl_sock->resumption = TRUE;
    if ( !ssl_sock->resumption ) {
        memcpy(ssl_sock->id, session_id_received, id_len);
    }
    ssl_sock->cipher_suite = get_supported_suite(ssl_sock)
    ...
    if ( !ssl_sock->cipher_suite )
        return NO_CIPHER_SUITE;
    if ( ssl_sock->resumption ) {
        memcpy(ssl_sock->key, ssl_sock->cached_key, 48);
  ...
}
```

# Pre-Auth-Resumption Debug View

TLStorm




```
int mocana_ssl_handshake(...)
{
    ...
    ssl_sock->resumption = FALSE;
    if (memcmp(session_id_received, ssl_sock->id, id_len))
        ssl_sock->resumption = TRUE;
    if ( !ssl_sock->resumption ) {
        memcpy(ssl_sock->id, session_id_received, id_len);
    }
    ssl_sock->cipher_suite = get_supported_suite(ssl_sock)
    ...
    if ( !ssl_sock->cipher_suite )
        return NO_CIPHER_SUITE;
    if ( ssl_sock->resumption ) {
        memcpy(ssl_sock->key, ssl_sock->cached_key, 48);
  ...
}
```

# What It Actually Looks Like

TLStorm

| Source | Destination | Protocol | Info |
|---|---|---|---|
| 192.168.137.3 | 192.168.137.1 | TCP | 50840 → 443 [SYN] Seq=6541 Win=2144 Len=0 MSS=536 |
| 192.168.137.1 | 192.168.137.3 | TCP | 443 → 50840 [SYN, ACK] Seq=1093576230 Ack=6542 Win=65392 Len=0 MSS=1460 |
| 192.168.137.3 | 192.168.137.1 | TLSv1… | Client Hello |
| 192.168.137.1 | 192.168.137.3 | TLSv1… | Server Hello |
| 192.168.137.1 | 192.168.137.3 | TLSv1… | Server Hello |
| 192.168.137.3 | 192.168.137.1 | TCP | 50840 → 443 [ACK] Seq=6596 Ack=1093576389 Win=1986 Len=0 |
| 192.168.137.1 | 192.168.137.3 | TLSv1… | Change Cipher Spec |
| 192.168.137.1 | 192.168.137.3 | TLSv1… | Finished |
| 192.168.137.3 | 192.168.137.1 | CoAP | CON, MID:12378, POST, TKN:05 b8 03 8c, /rd?ep=urn:dev:ops:00C0B7-itb-282 |
| 192.168.137.1 | 192.168.137.3 | CoAP | ACK, MID:12378, Empty Message, TKN:05 b8 03 8c |
| 192.168.137.1 | 192.168.137.3 | CoAP | CON, MID:39169, GET, TKN:65 9a c1, /5/0/3 |
| 192.168.137.3 | 192.168.137.1 | CoAP | ACK, MID:39169, 2.05 Content, TKN:65 9a c1, /5/0/3 |
| 192.168.137.1 | 192.168.137.3 | CoAP | CON, MID:33534, PUT, TKN:bb 20 d2, /10241/0/1 |
| 192.168.137.3 | 192.168.137.1 | CoAP | ACK, MID:33534, 2.04 Changed, TKN:bb 20 d2, /10241/0/1 |
| 192.168.137.1 | 192.168.137.3 | TCP | 443 → 50840 [ACK] Seq=1093576619 Ack=6879 Win=65055 Len=0 |

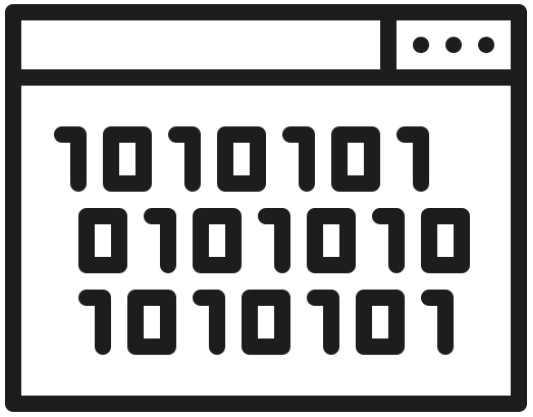
```
▾ Transport Layer Security
  ▸ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  ▸ TLSv1.2 Record Layer: Handshake Protocol: Finished
  ▸ TLSv1.2 Record Layer: Application Data Protocol: coap
▸ Constrained Application Protocol, Confirmable, POST, MID:12378
```

```
▾ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: TLS 1.2 (0x0303)
  > Random: 43f291cfe617d4d99e45ebe72daf64c2da281e119c214f524c7509a044a0044d
    Session ID Length: 32
    Session ID: a0813ed0d7d8b7e27dbea07da00a48137d01f9a5f230d753d2589397c2606a0d
    Cipher Suite: Unknown (0xfdfd)
    Compression Method: null (0)
```

```
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 70
    Version: TLS 1.2 (0x0303)
  > Random: 43f291cfe617d4d99e45ebe72daf64c2da281e119c214f524c7509a044a0044d
    Session ID Length: 32
    Session ID: a0813ed0d7d8b7e27dbea07da00a48137d01f9a5f230d753d2589397c2606a0d
    Cipher Suite: TLS_PSK_WITH_AES_128_CCM_8 (0xc0a8)
    Compression Method: null (0)
```

# Research Milestones

TLStorm


# IMPACT CATEGORIES

TLStorm

Network

Internet Attack Vector | Persistency/Stronghold

Power Connected Devices

Shutdown | ???

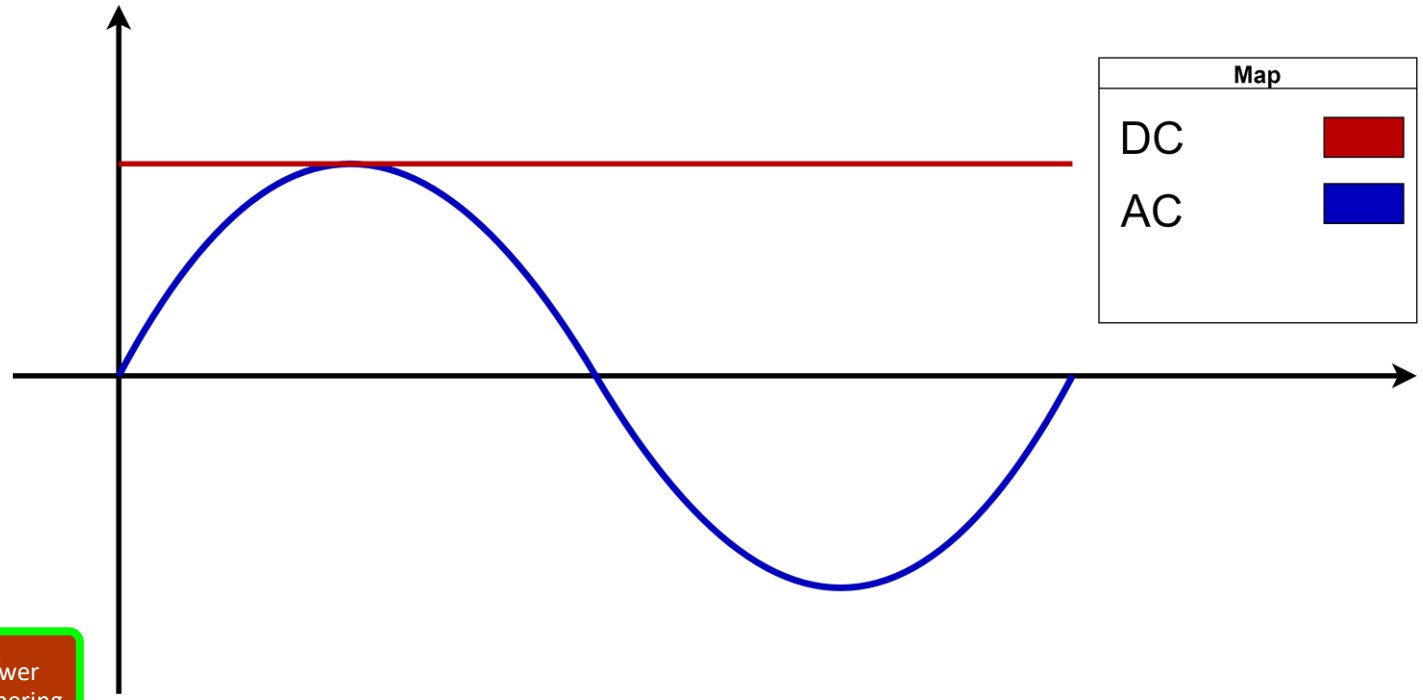
UPS

Brick | ???

Internet Attack Vector → Remote Code Execution → Power Tampering

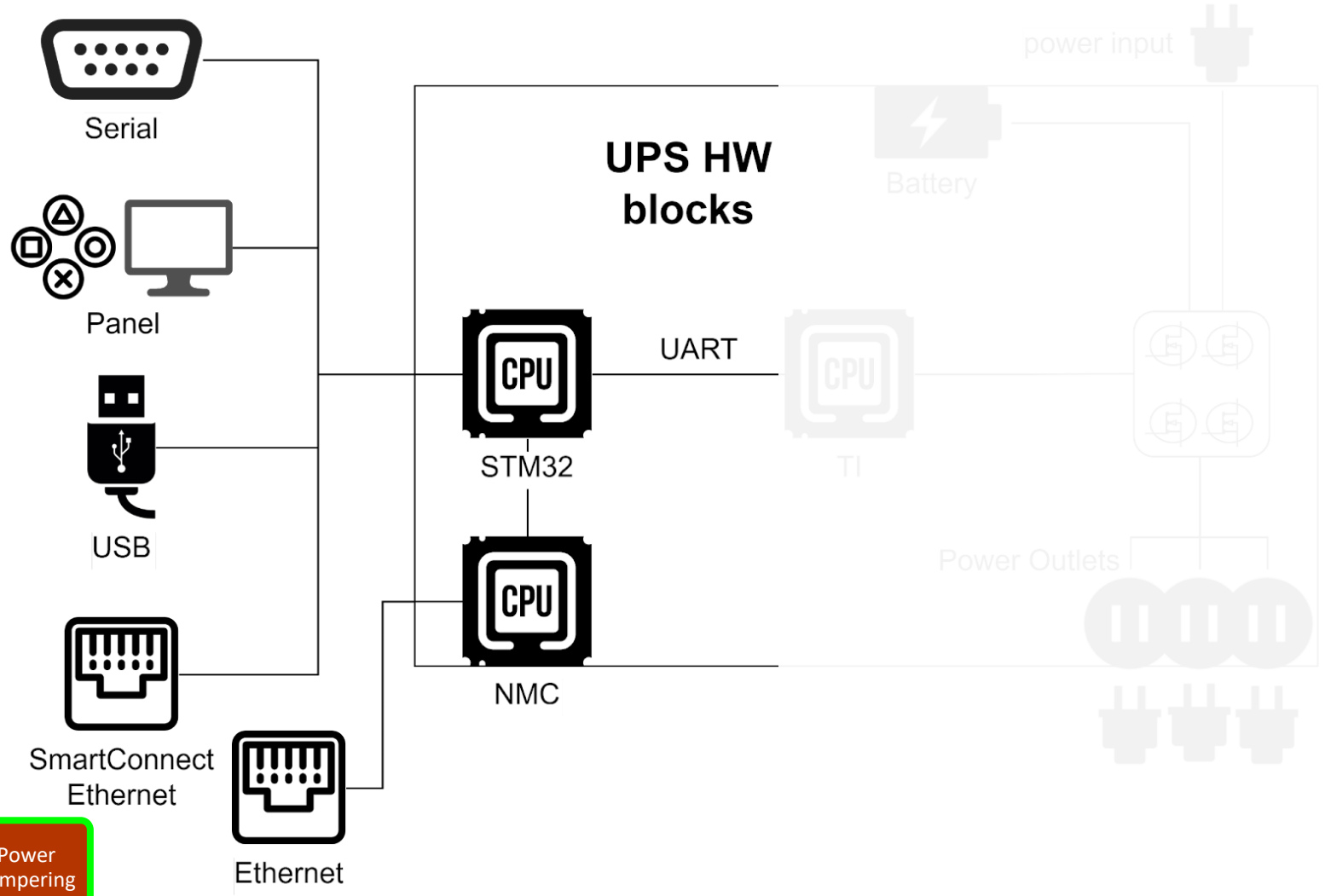
# Maximizing Impact

- Output via a battery meaning DC→AC converter
- Software is involved, but how much?



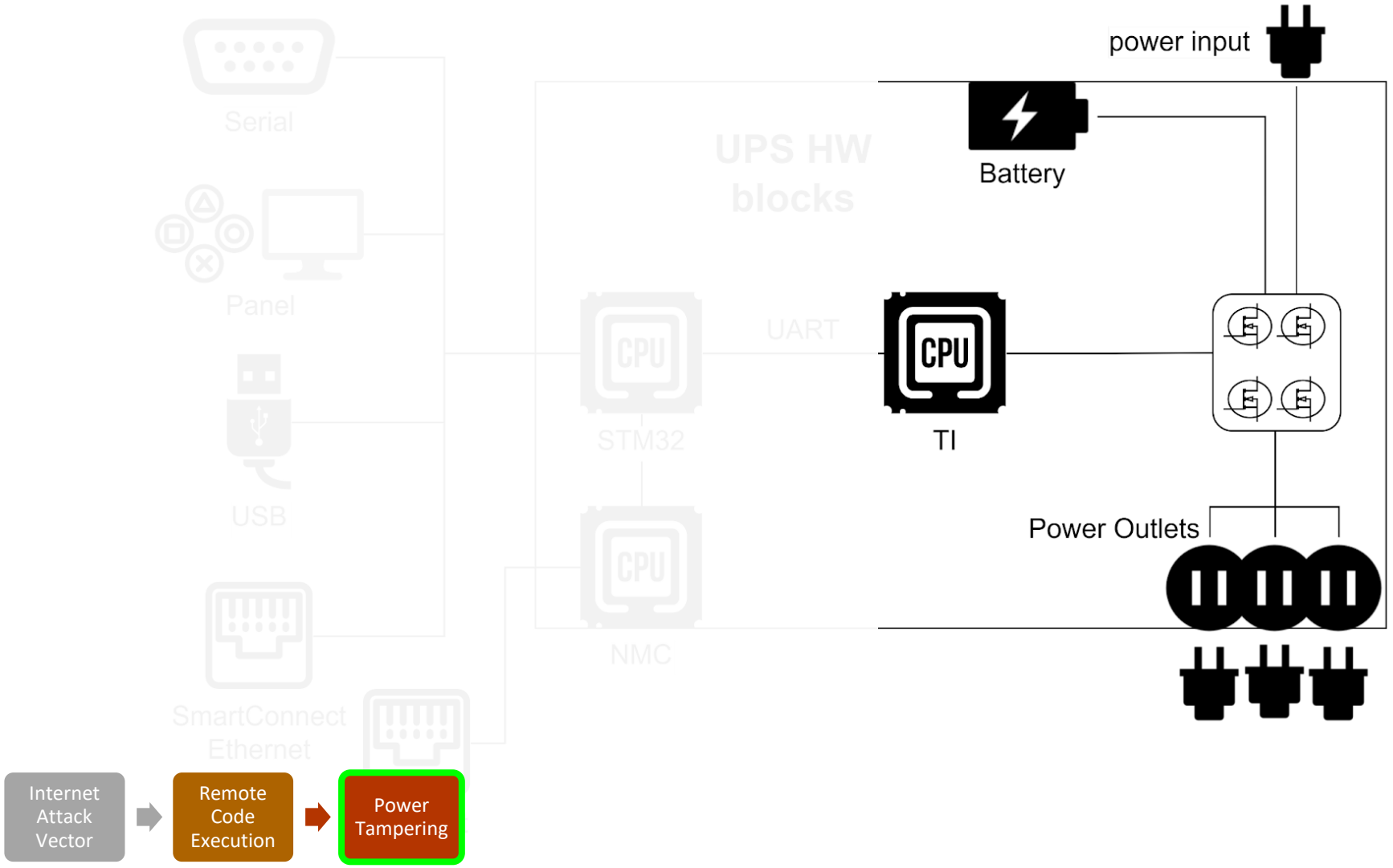

Internet Attack Vector → Remote Code Execution → Power Tampering

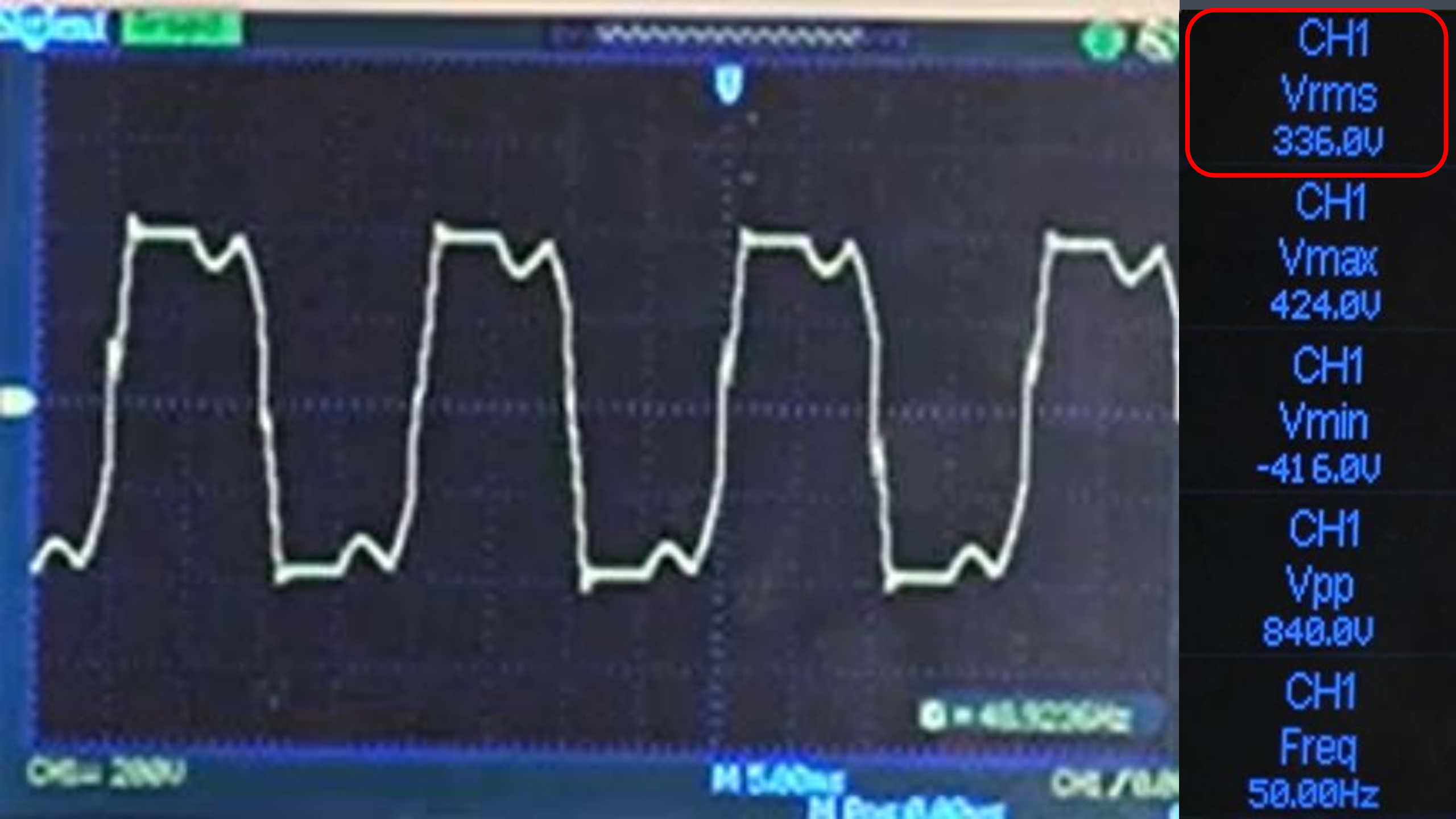
# Internal Architecture

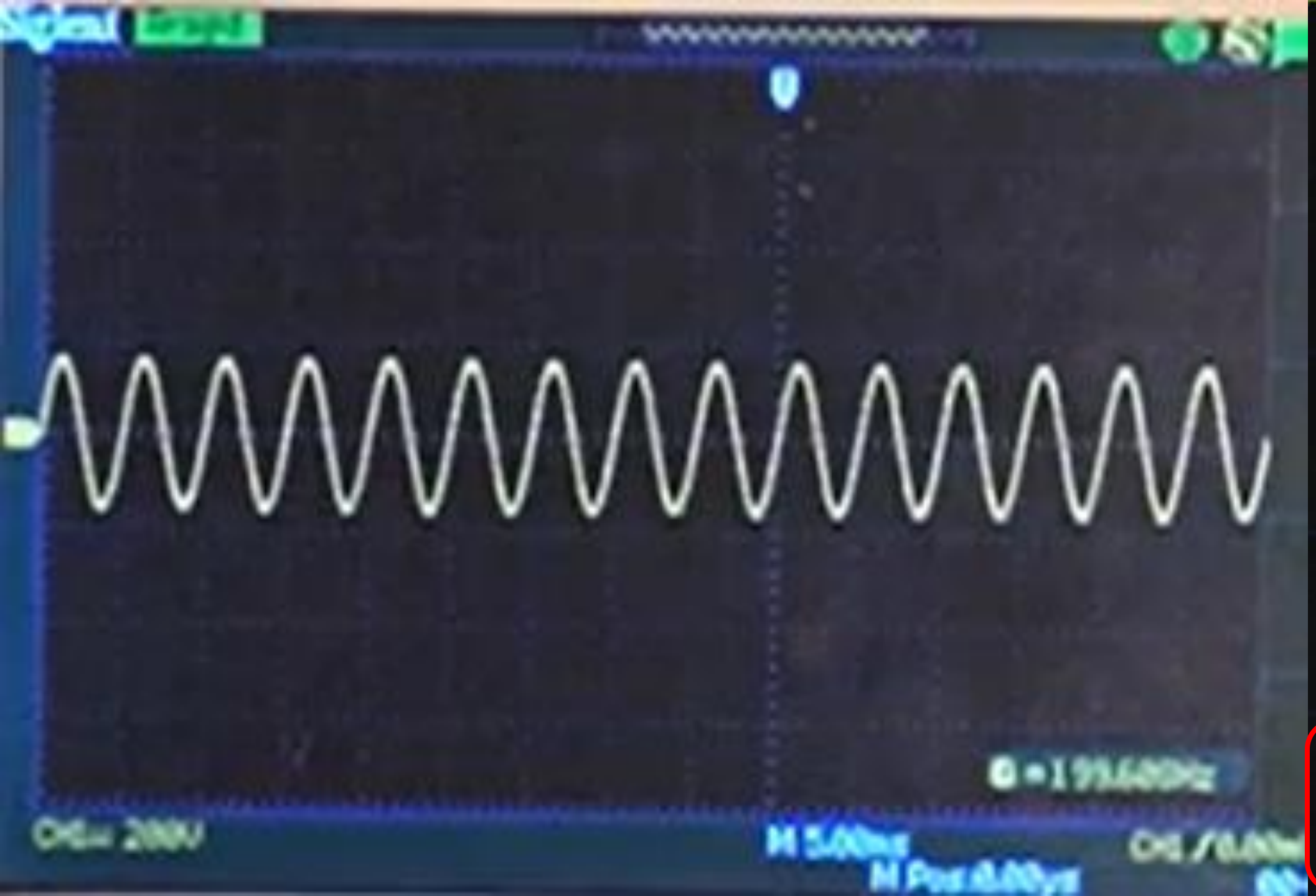



Internet Attack Vector → Remote Code Execution → Power Tampering

# Internal Architecture




CH1
Vrms
336.0V
CH1
Vmax
424.0V
CH1
Vmin
-416.0V
CH1
Vpp
840.0V
CH1
Freq
50.00Hz



CH1
Vrms
112.0V

CH1
Vmax
168.0V

CH1
Vmin
-168.0V

CH1
Vpp
336.0V

CH1
Freq
200.0Hz

# IMPACT CATEGORIES

TLStorm

Network

Internet Attack Vector | Persistency/Stronghold

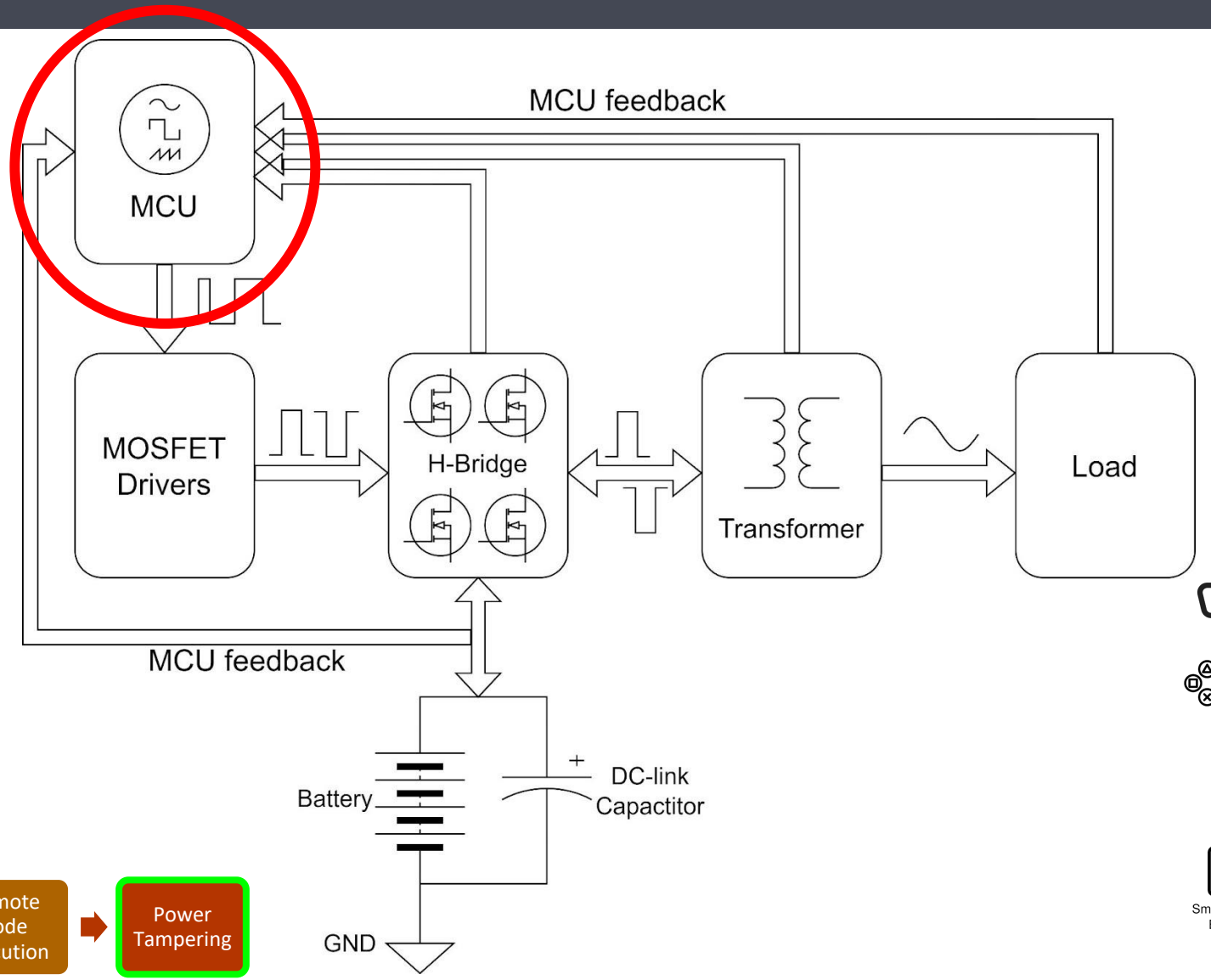
Power Connected Devices

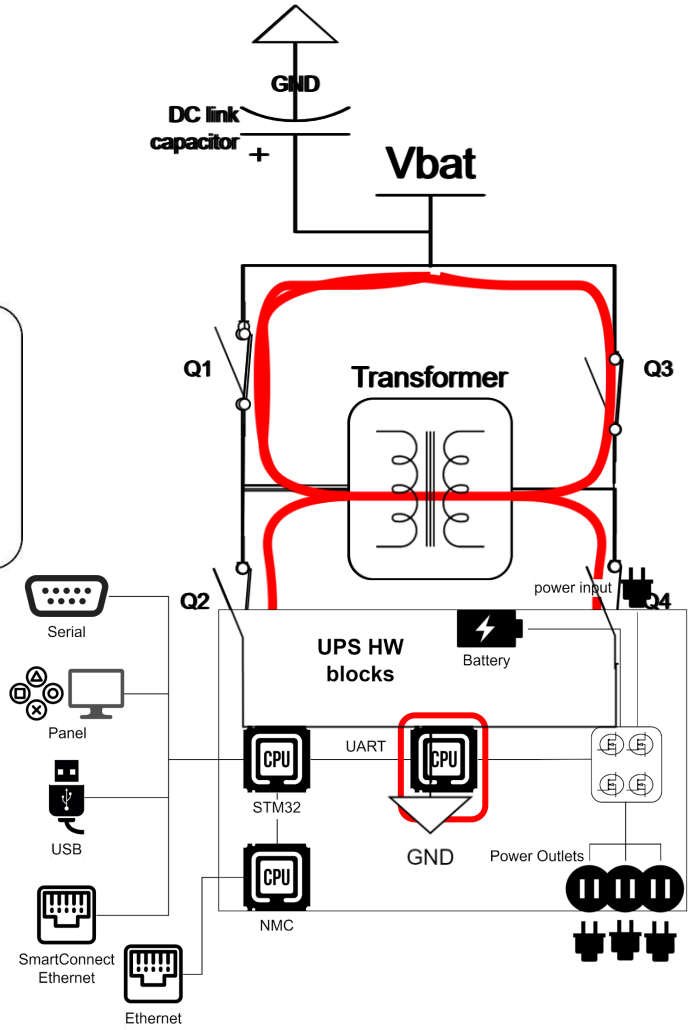
Shutdown | Power Tampering

UPS

Brick | ???

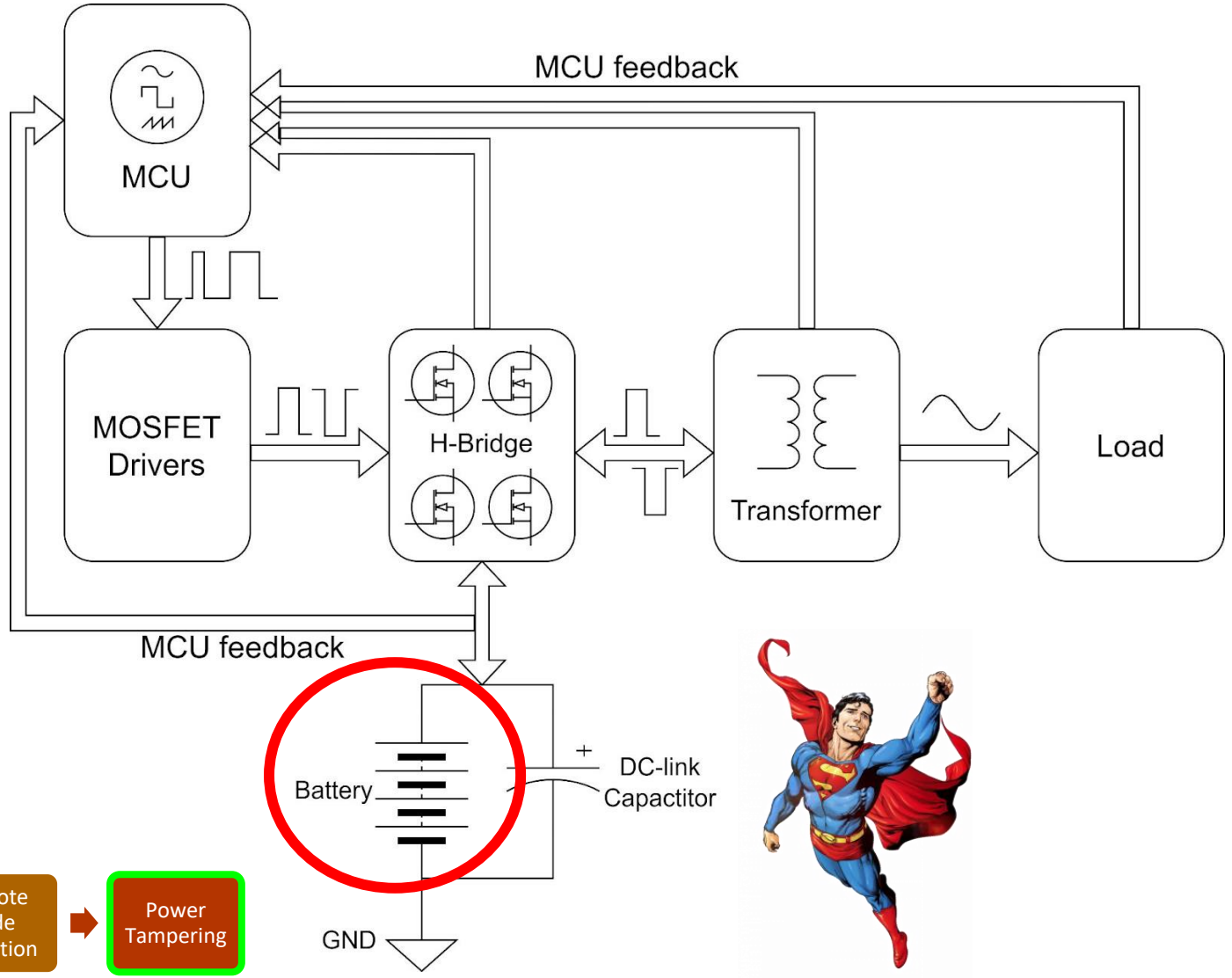
# Power Conversion Blocks




Internet Attack Vector → Remote Code Execution → Power Tampering

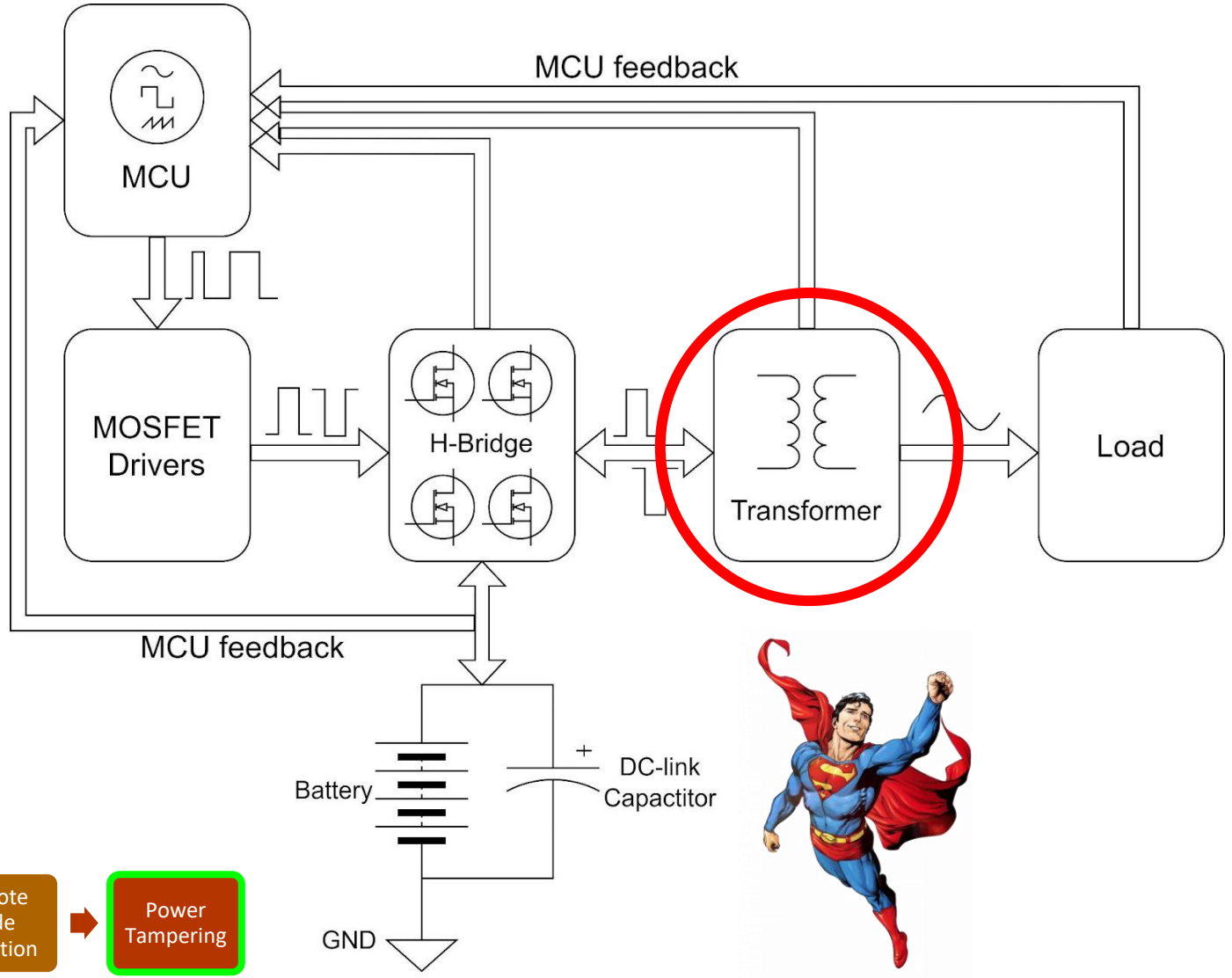
# Power Conversion Blocks



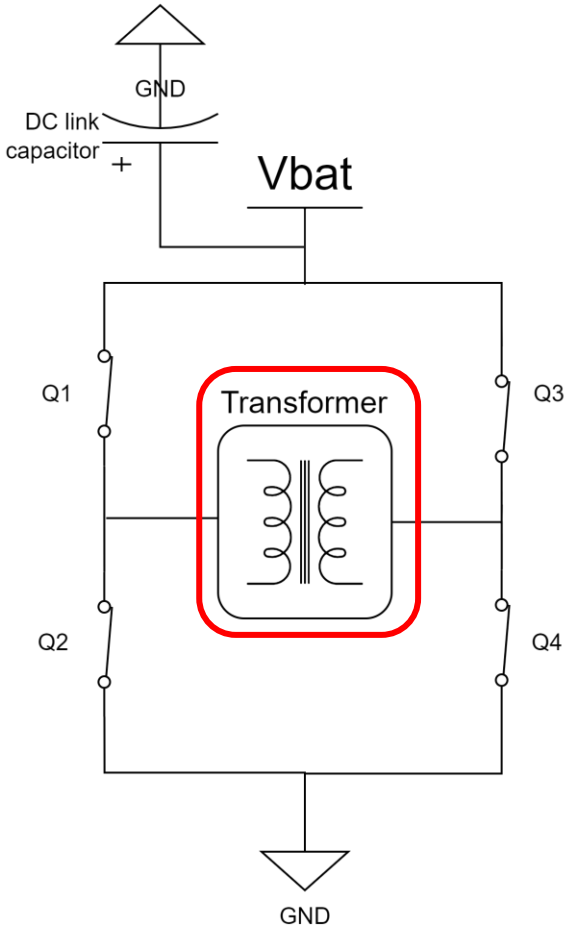



Internet Attack Vector → Remote Code Execution → Power Tampering

# Power Conversion Blocks

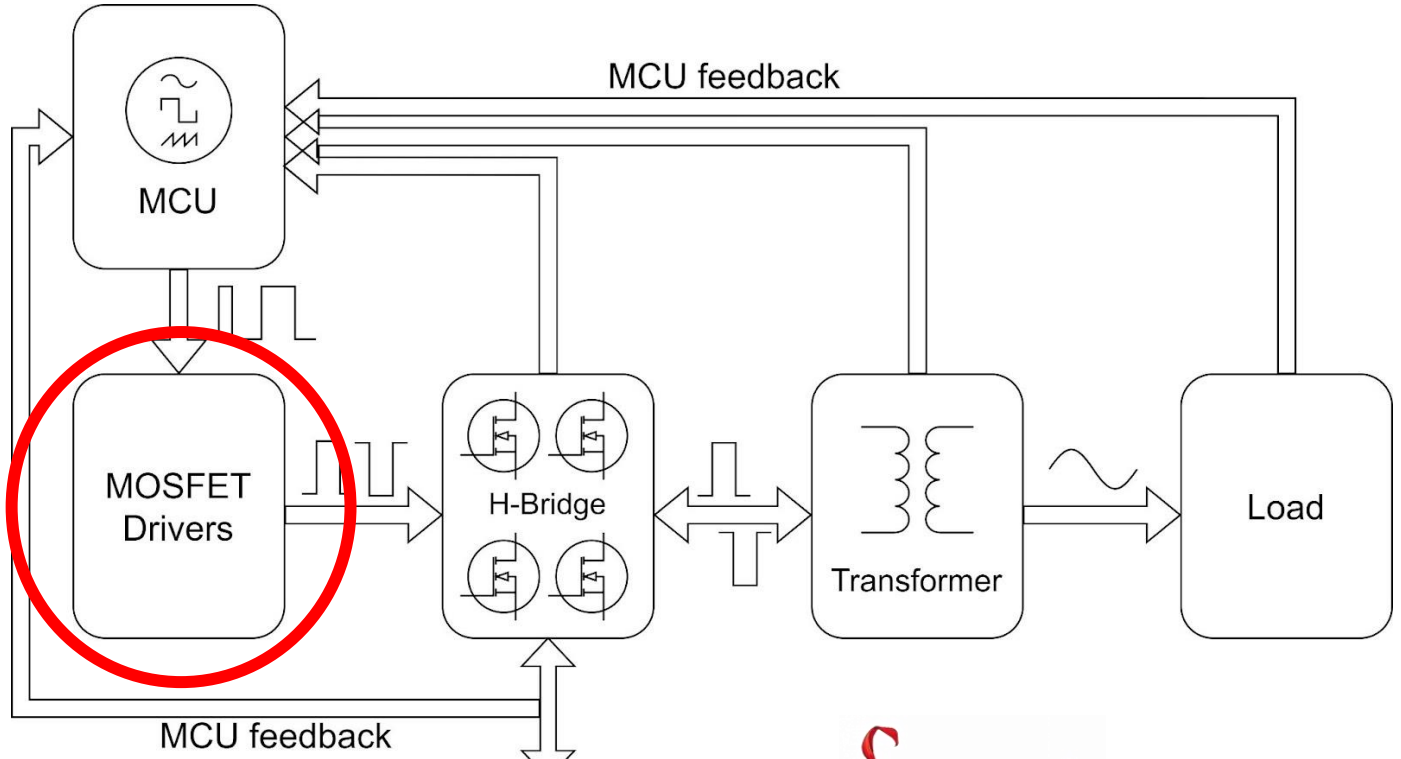




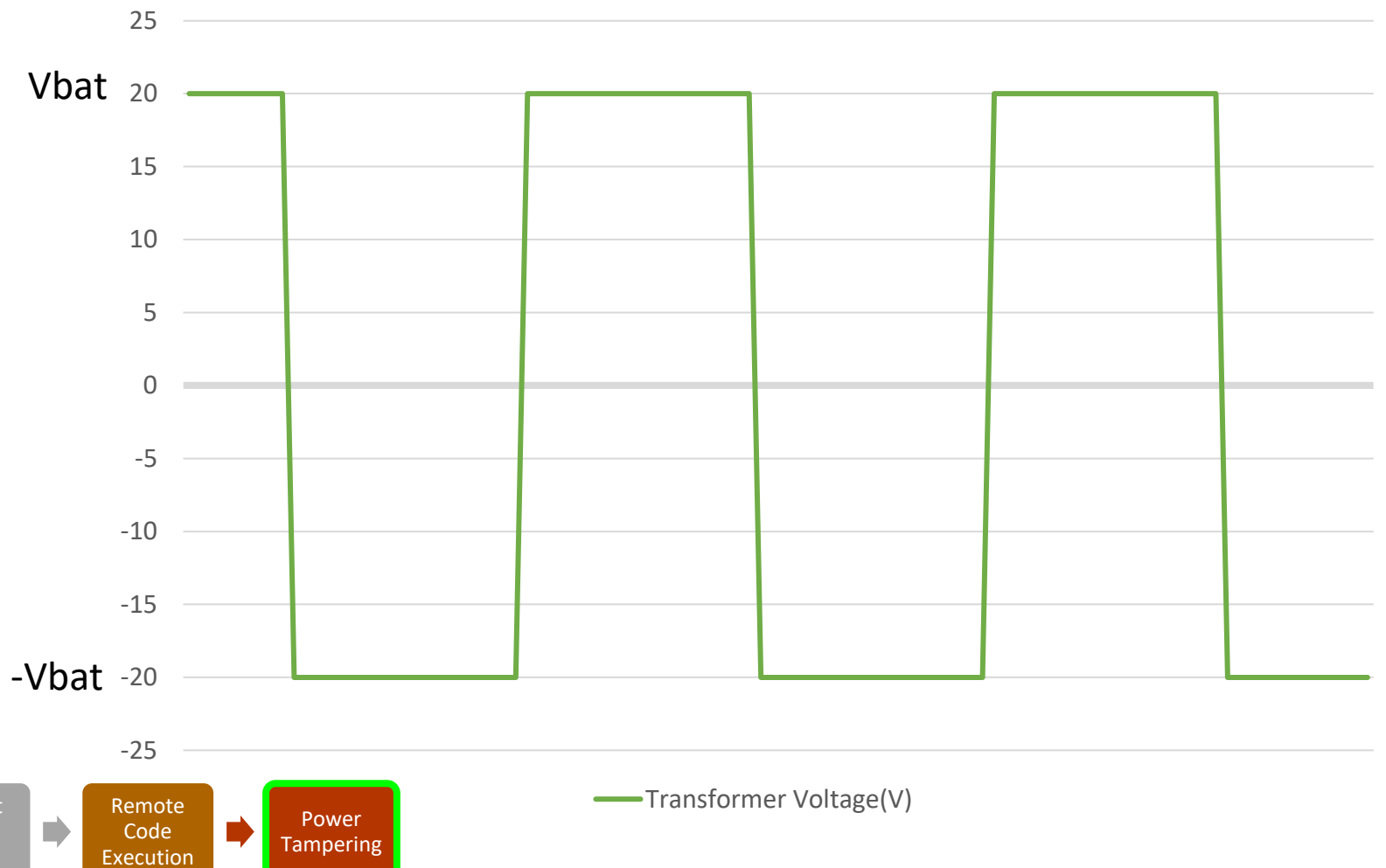

Internet Attack Vector → Remote Code Execution → Power Tampering

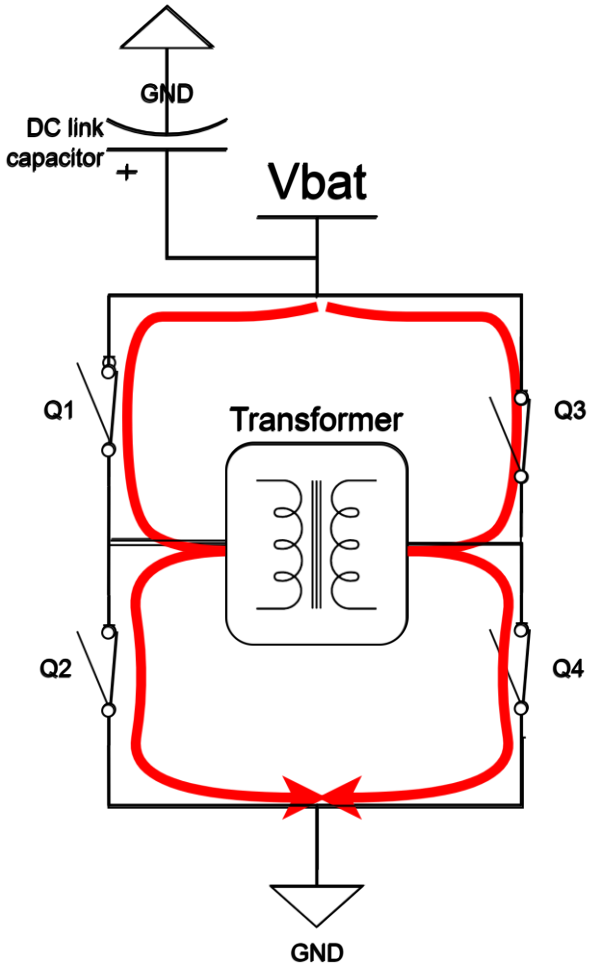
# Power Conversion Blocks




Internet Attack Vector → Remote Code Execution → Power Tampering

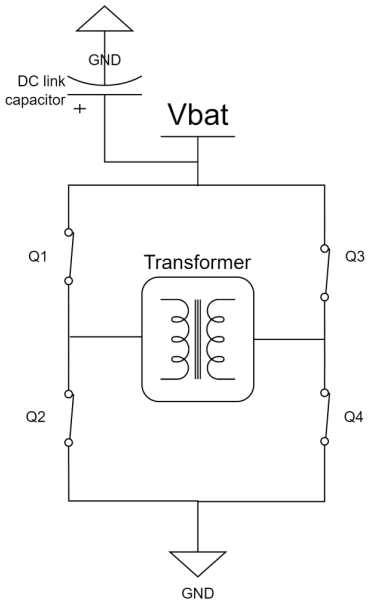
# Normal UPS On Battery

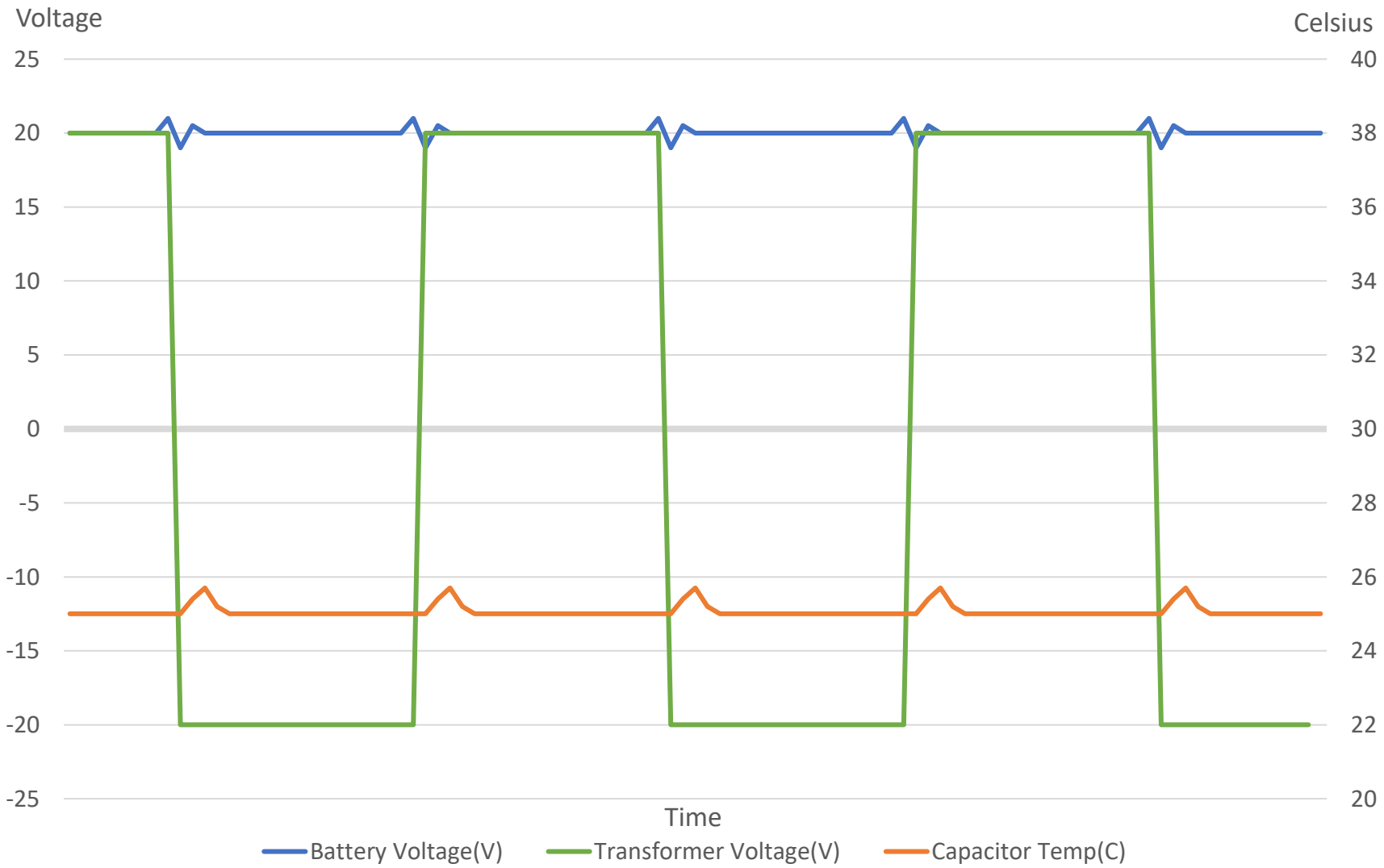



Internet Attack Vector → Remote Code Execution → Power Tampering

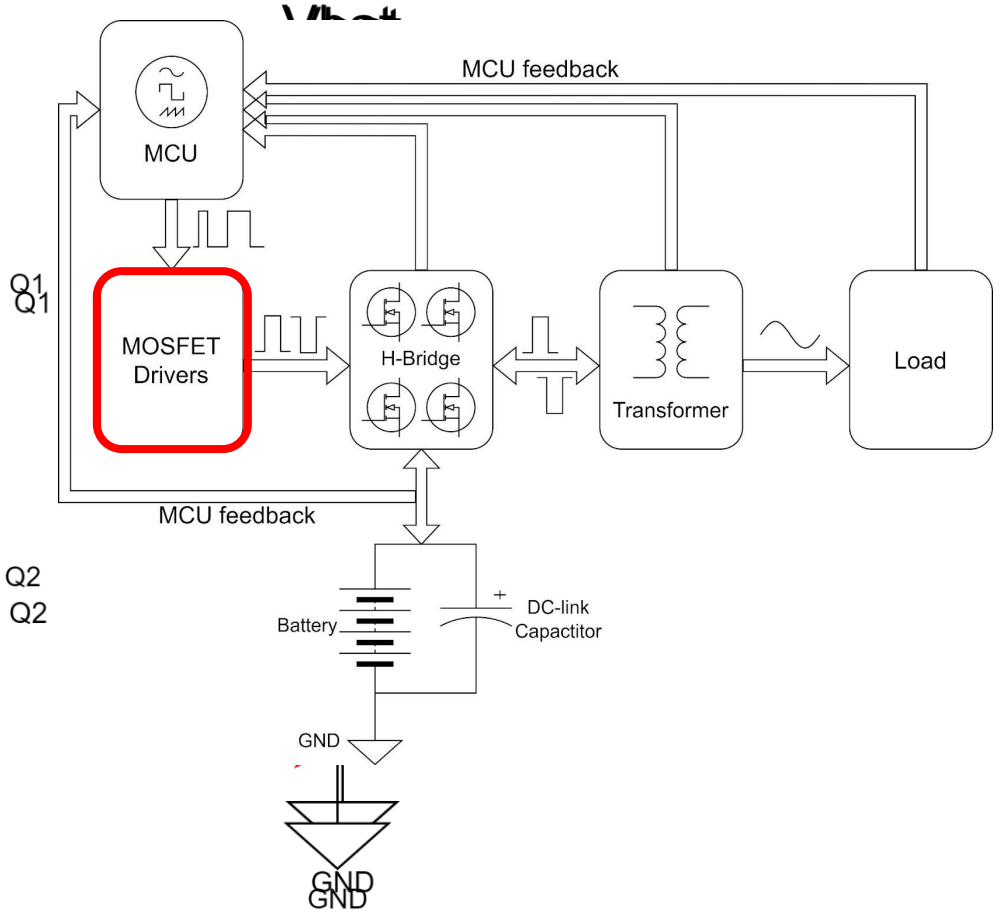
# Normal UPS On Battery



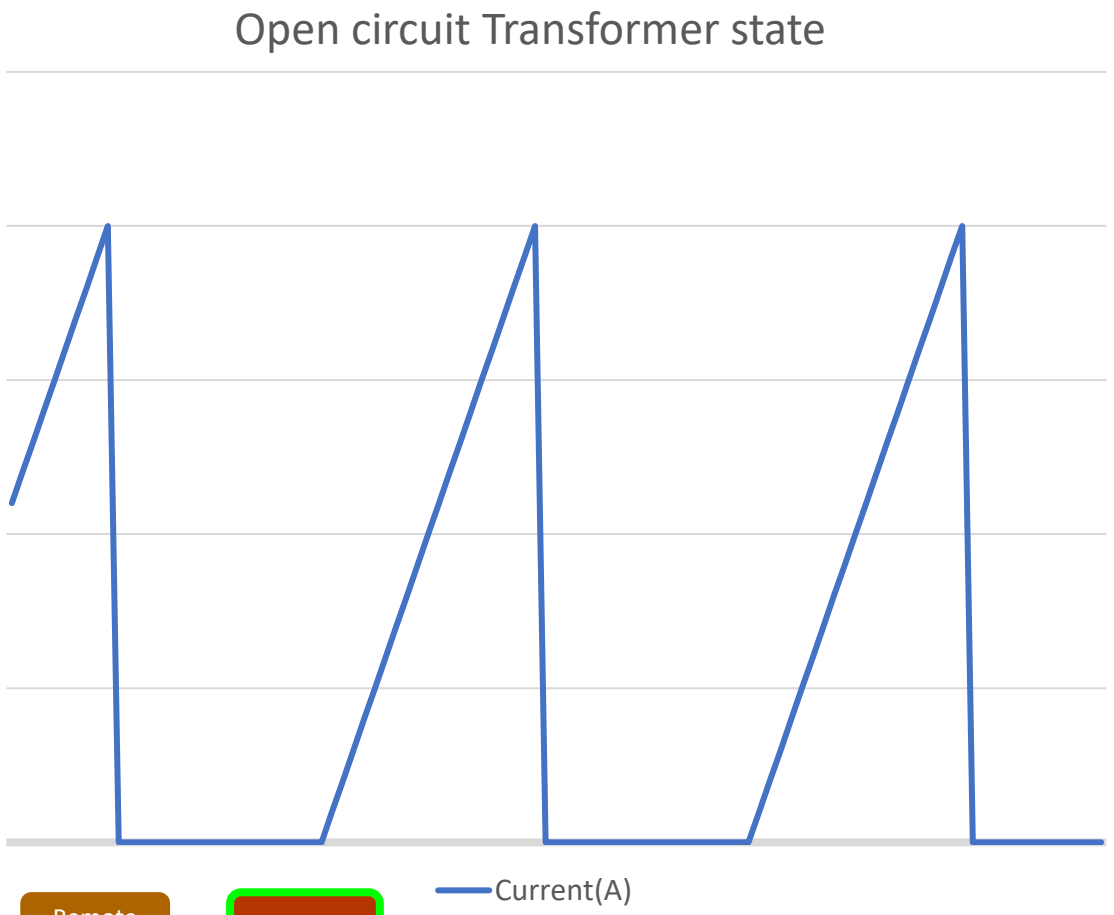
# Burning Bridges

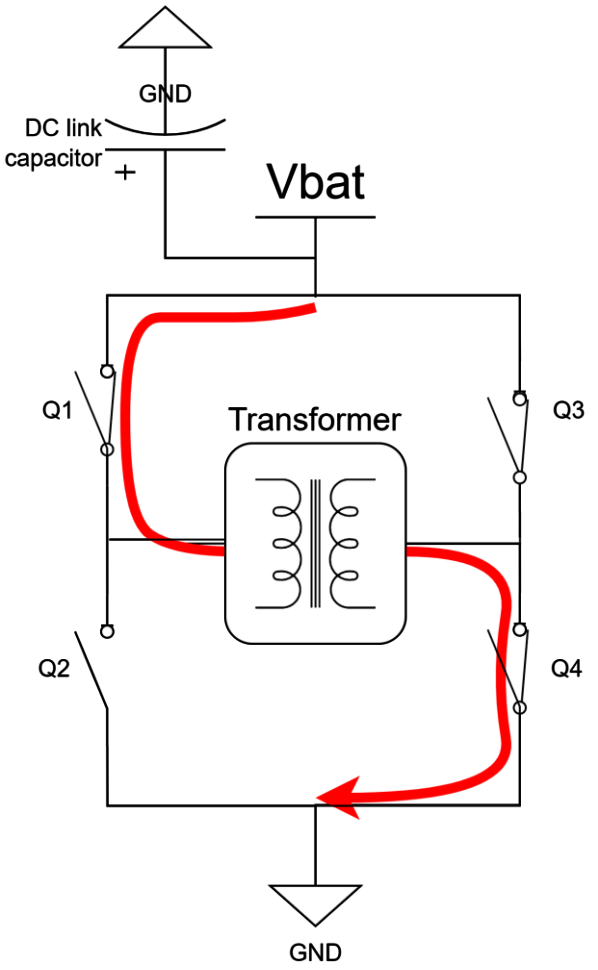
- The H-bridge can be orchestrated using the vulnerability
- Can the UPS be abused that way?
  - Battery connection directly to the ground!
  - Hardware protected
  - How about open circuit?




Internet Attack Vector → Remote Code Execution → Power Tampering

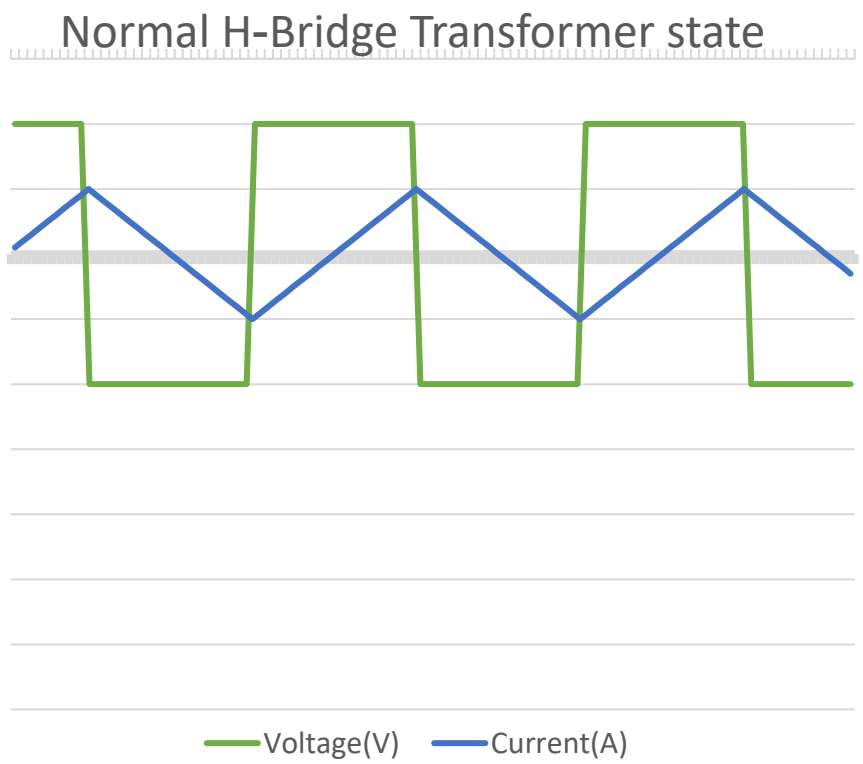
# Open Circuit - Transformer



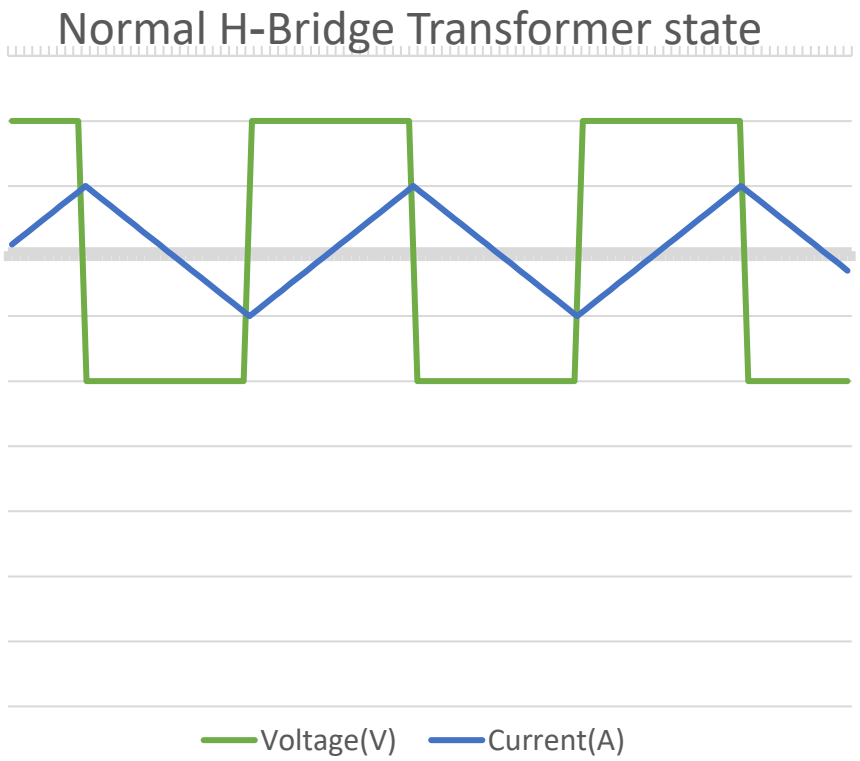

Internet Attack Vector → Remote Code Execution → Power Tampering

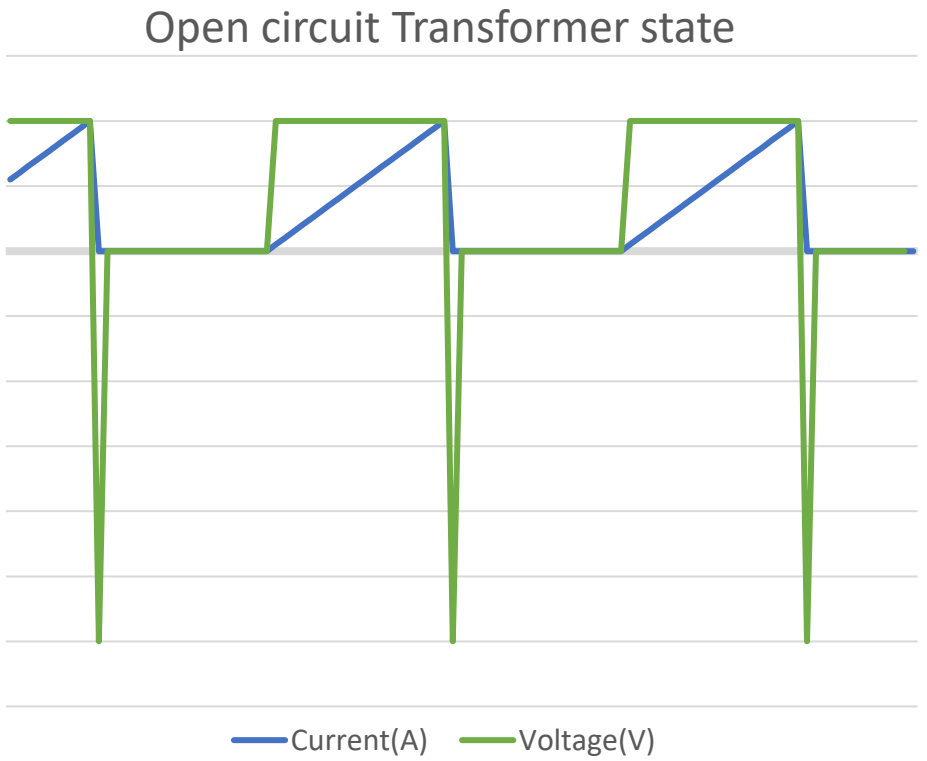
# Inductor’s Characteristics




# Inductor’s Characteristics

TLStorm



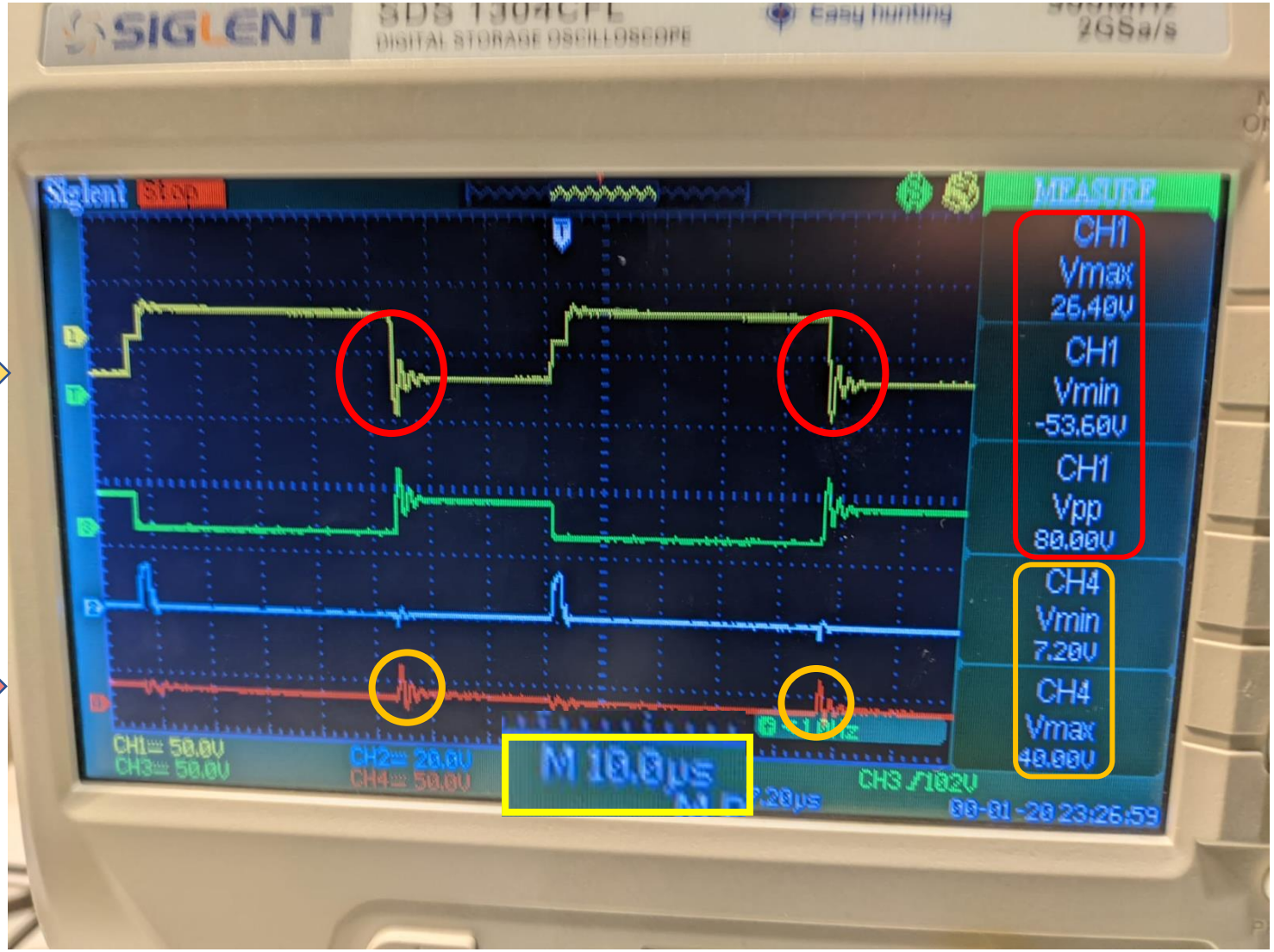




# Results

- $\Delta t$ = ~1µsec
- $\Delta V_{bat}$ = 33V
- C = 2700µF
- $I_C$ = ~100KA!

Transformer voltage

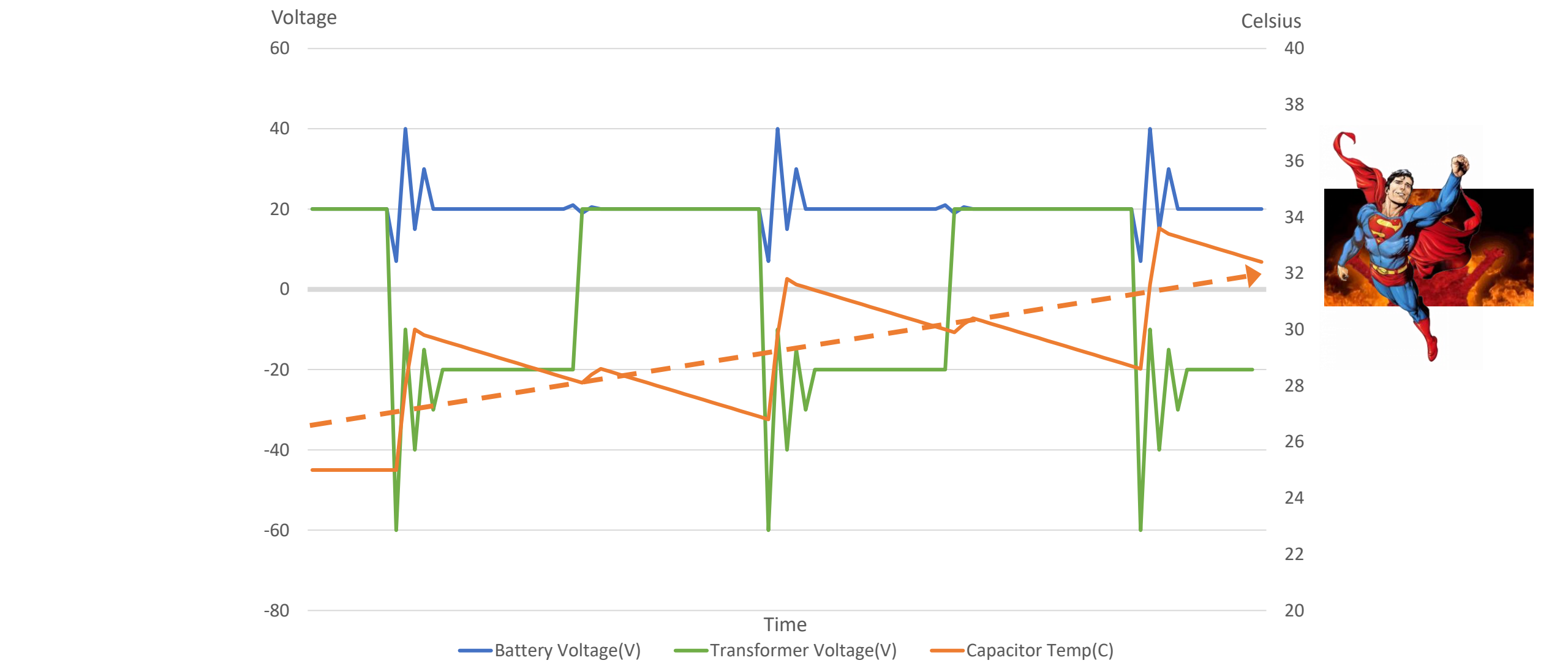
Battery voltage




Internet Attack Vector → Remote Code Execution → Power Tampering

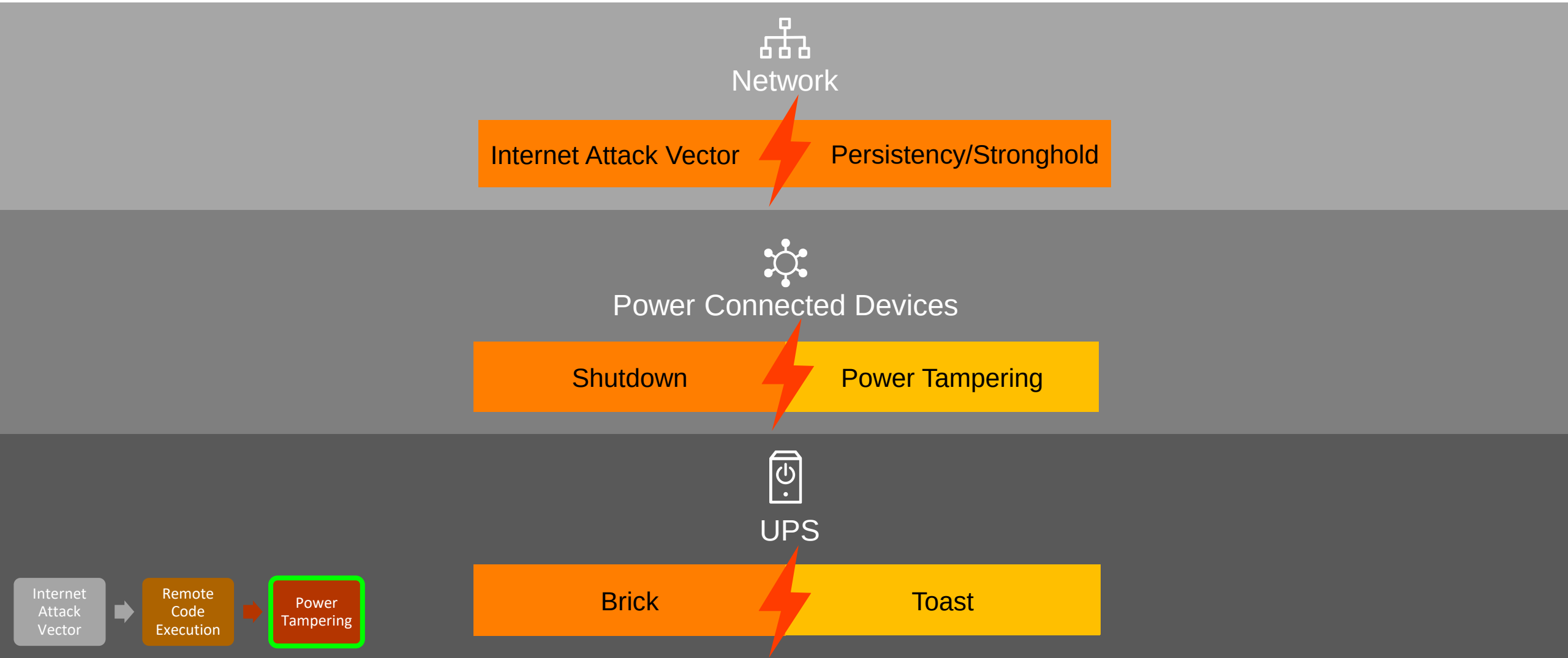
# Hazardous UPS On Battery

TLStorm



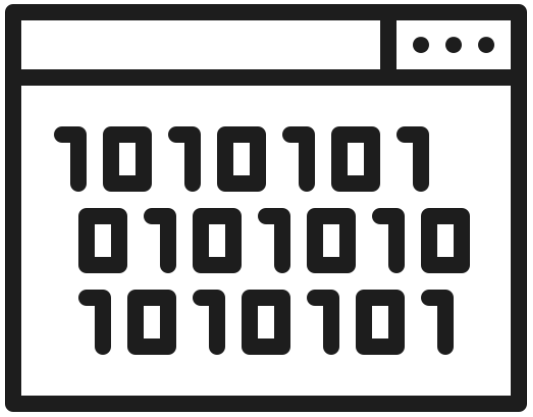
# IMPACT CATEGORIES

TLStorm



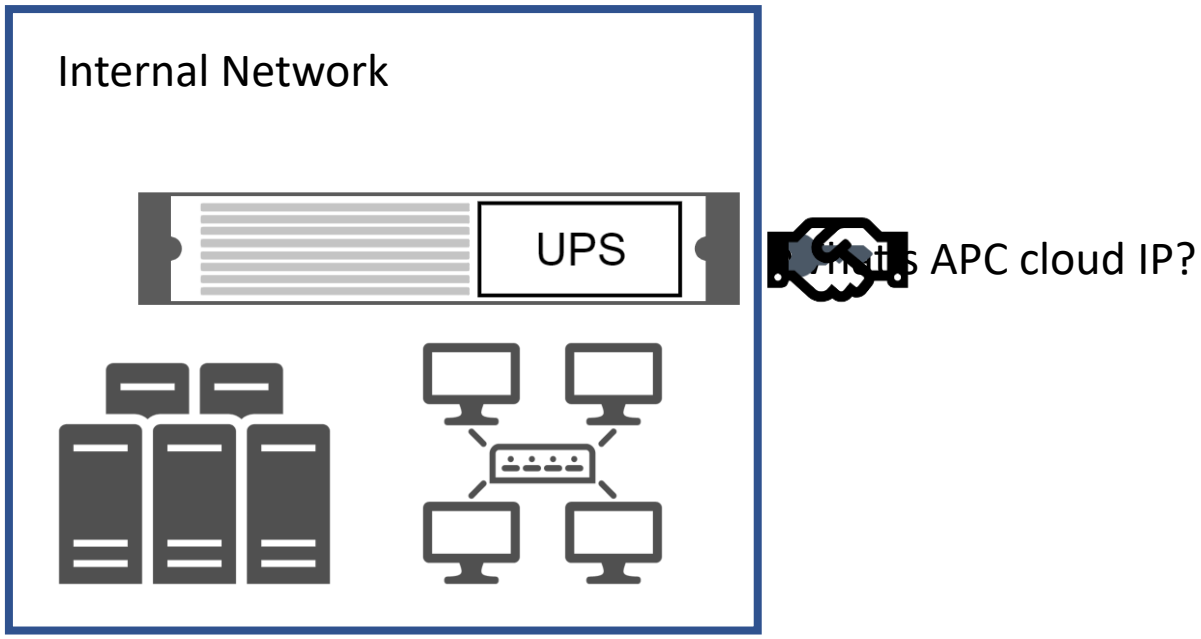
# Research Milestones

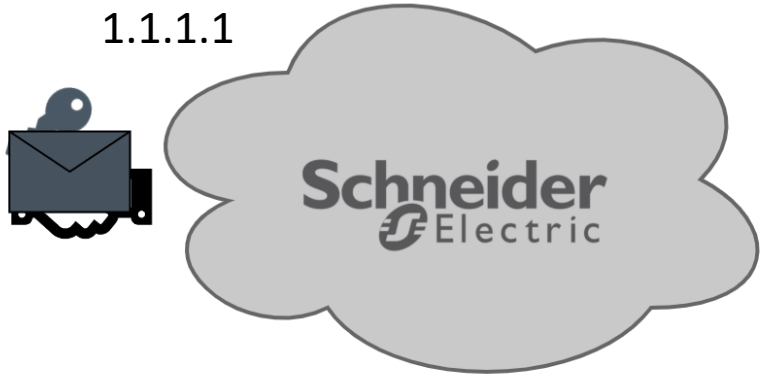
TLStorm

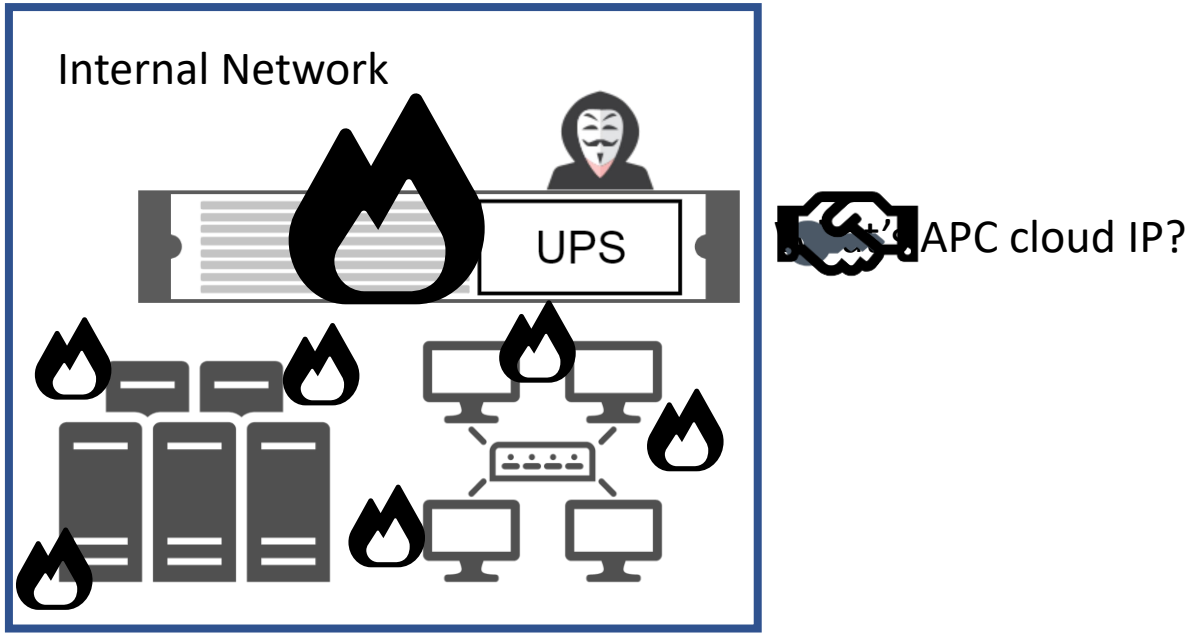

# Recap - Original Flow

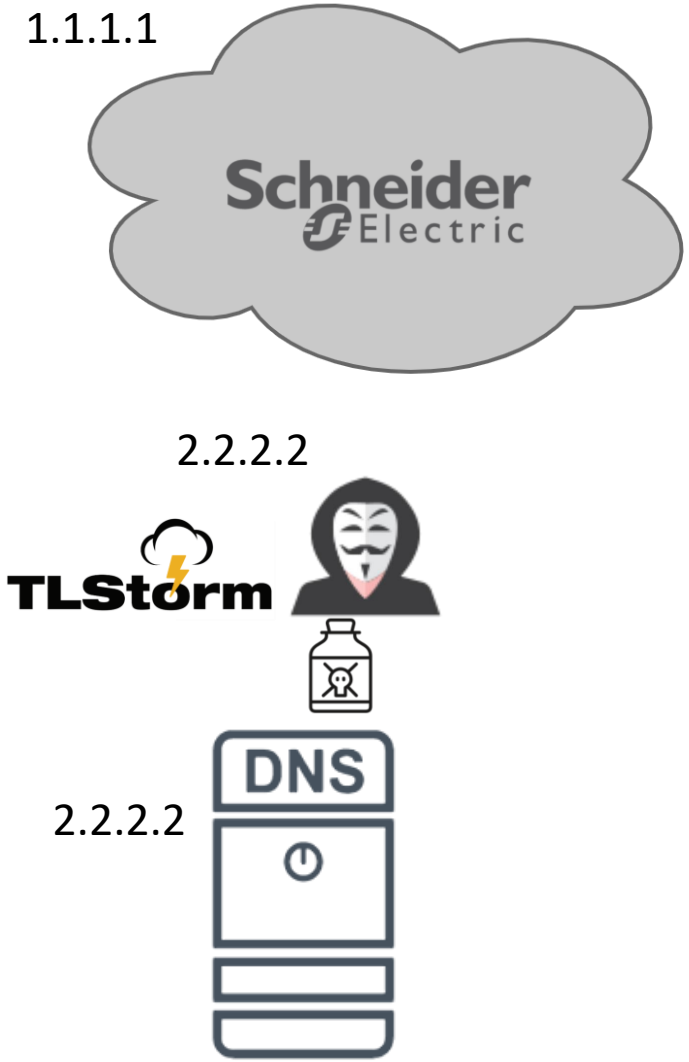
TLStorm




# Recap - Attack Scenarios

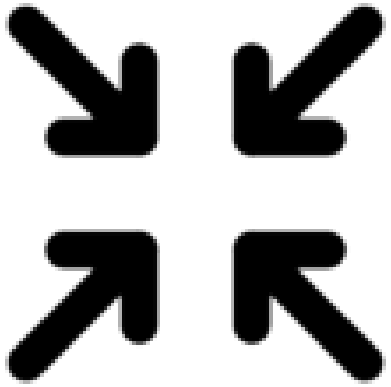


# Mitigations

TLStorm

- Apply patches where applicable
- Minimize attack surface
- Monitor communication




# TLStorm

Takeaways:

**External libraries could be a weak spot**

**Internet connectivity is an attack vector**

**Cyber physical is mean**



# Questions?

Read more – armis.com/TLStorm

Yuval Sarel - @TheYuvalShow

Gal Levy - @Gal_Levy92