



## A set of critical vulnerabilities in Smart-UPS devices

Yuval Sarel, Research Team Lead  
Gal Levy, Senior Researcher

Read more – [armis.com/TLStorm](https://armis.com/TLStorm)



# Who Are We?

---

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



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

# What is 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

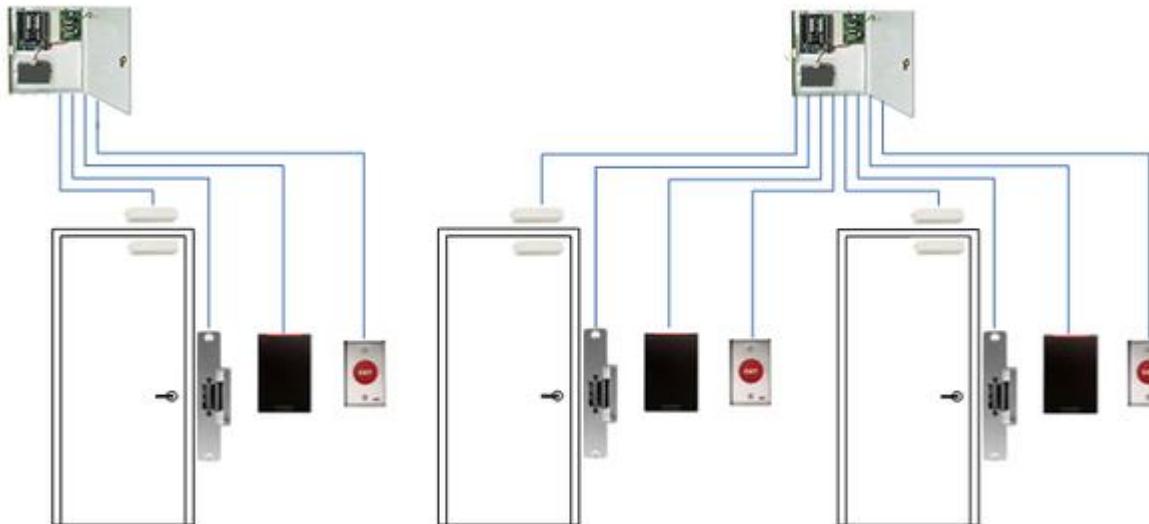


# Cyber Physical Systems

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



# Cyber Physical Systems



# Cyber Physical Systems



# Cyber Physical Systems



# Cyber Physical Systems



# Cyber Physical as an Attack Vector



## 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.

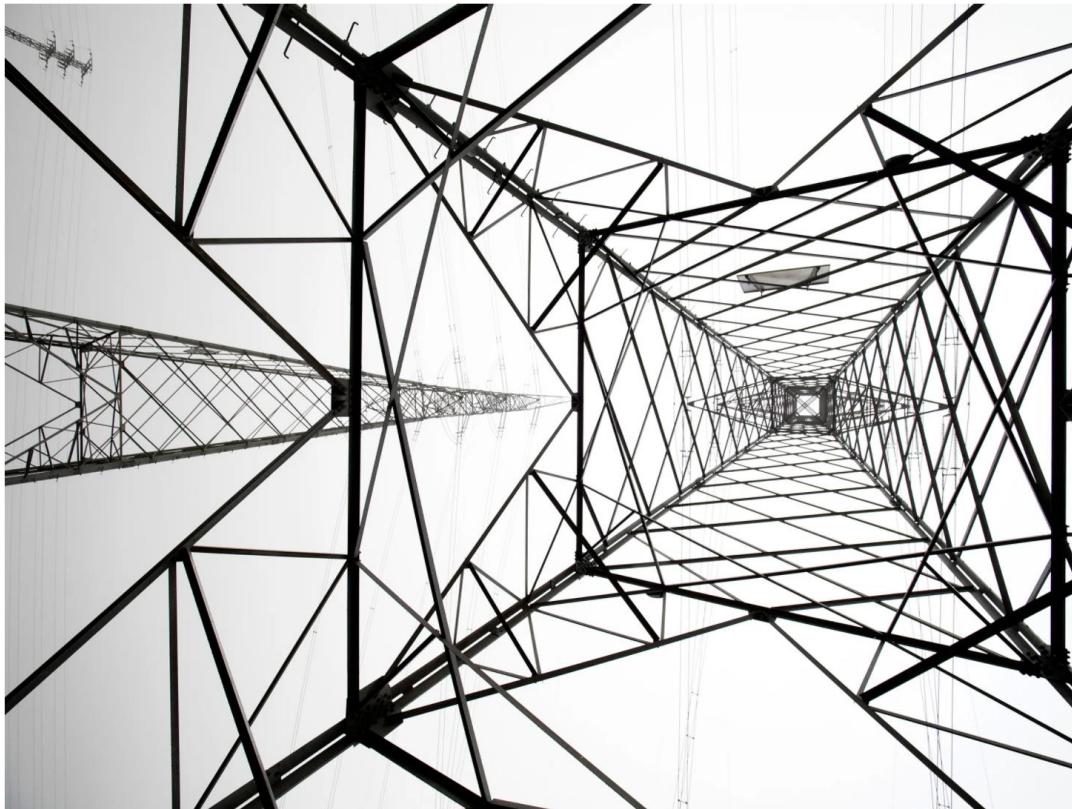
# Cyber Physical as an Attack Vector



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.



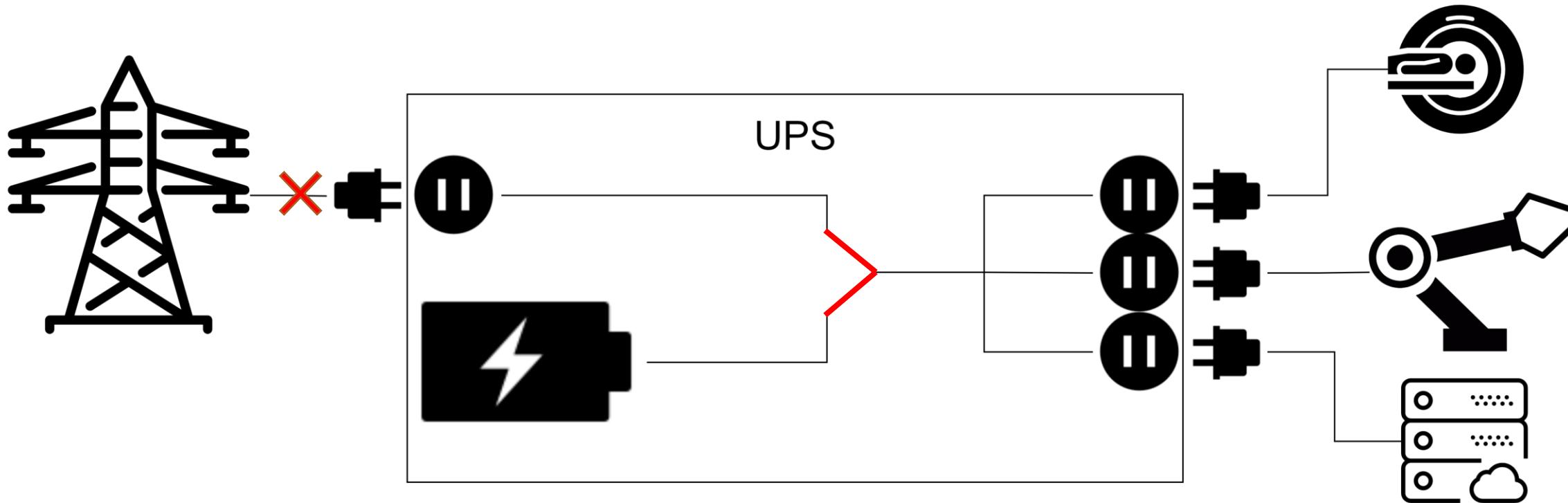
JOSE A. BERNAT BACET/GETTY IMAGES

- “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...”

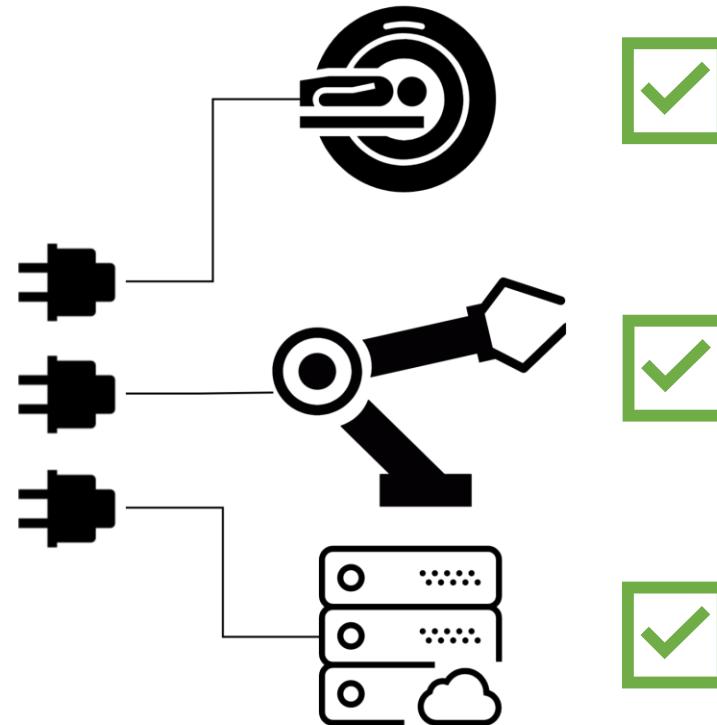
# UPS – ~~Un~~interruptible Power Supply



# UPS – Basic Operation



# UPS – Basic Operation



**UPS Vendor - APC**



---

**by Schneider Electric**

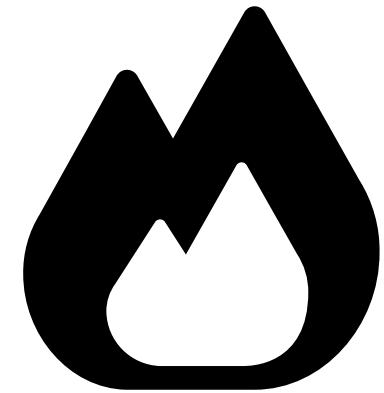
# Smart-UPS



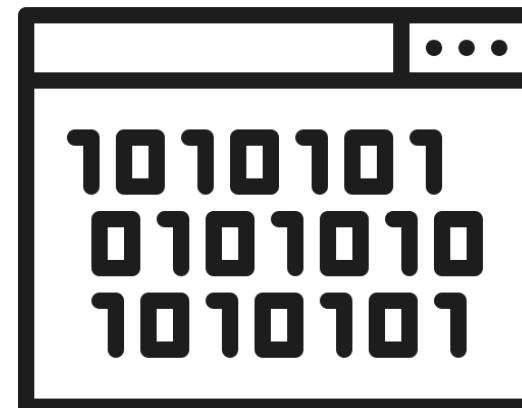
- Analog device turned digital
- “Over 20 million units sold” - APC
- “SmartConnect”



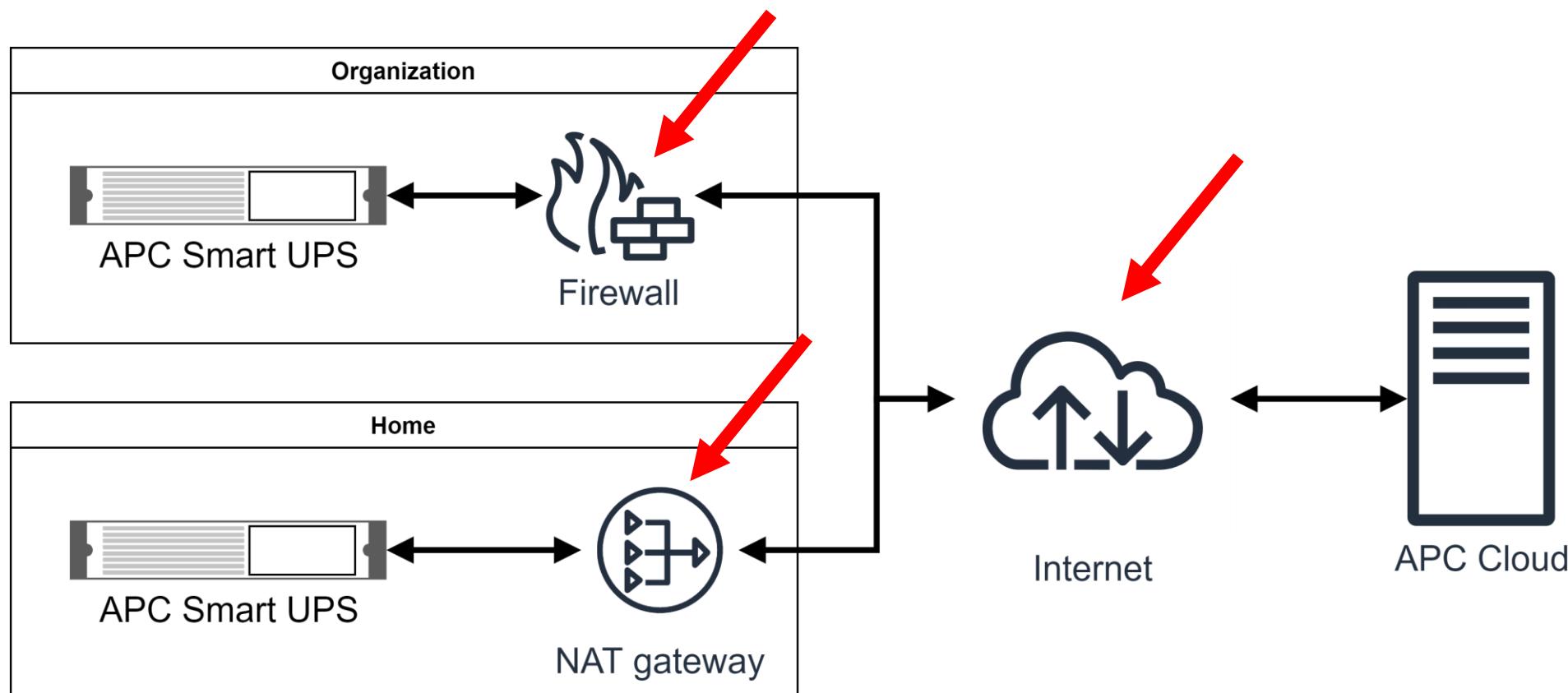
# SmartConnect Attack Surface



# Research Milestones



# SmartConnect - Overview



Internet  
Attack  
Vector

Remote  
Code  
Execution

Power  
Tampering

# SmartConnect - UI



Life Is On | APC by Schneider Electric

My Account | Help

DASHBOARD

EVENT LOGS

ADD DEVICE

NOTIFICATIONS

RENEWAL SUPPORT

## UPS Status

### ACTIVE EVENTS

- ! CRITICAL Battery Disconnected [VIEW LOGS](#) [VIEW HELP](#)
- ! WARNING UPS Firmware Version Out of Date [VIEW UPGRADE](#) [VIEW HELP](#)
- i INFO UPS Output Power Turned Off [VIEW HELP](#)

### STATUS

OPERATING MODE ! UPS Off  
Output power turned off

DEVICE HEALTH ! Error  
2 issues need attention

### BATTERY

### DEVICE

FIRMWARE ! v 04.1

INPUT ! 234 V

OUTPUT ! 0 V

LOAD ! 0%

### DIAGNOSTICS

### NETWORK

Internet Attack Vector → Remote Code Execution → Power Tampering

# SmartConnect – FW Update

**Important:** Connected load is not protected during upgrade

Interruption of UPS input power during this firmware upgrade will result in a loss of power supplied to connected devices. Learn more in the [Help Center](#).

 [RUN UPGRADE](#)

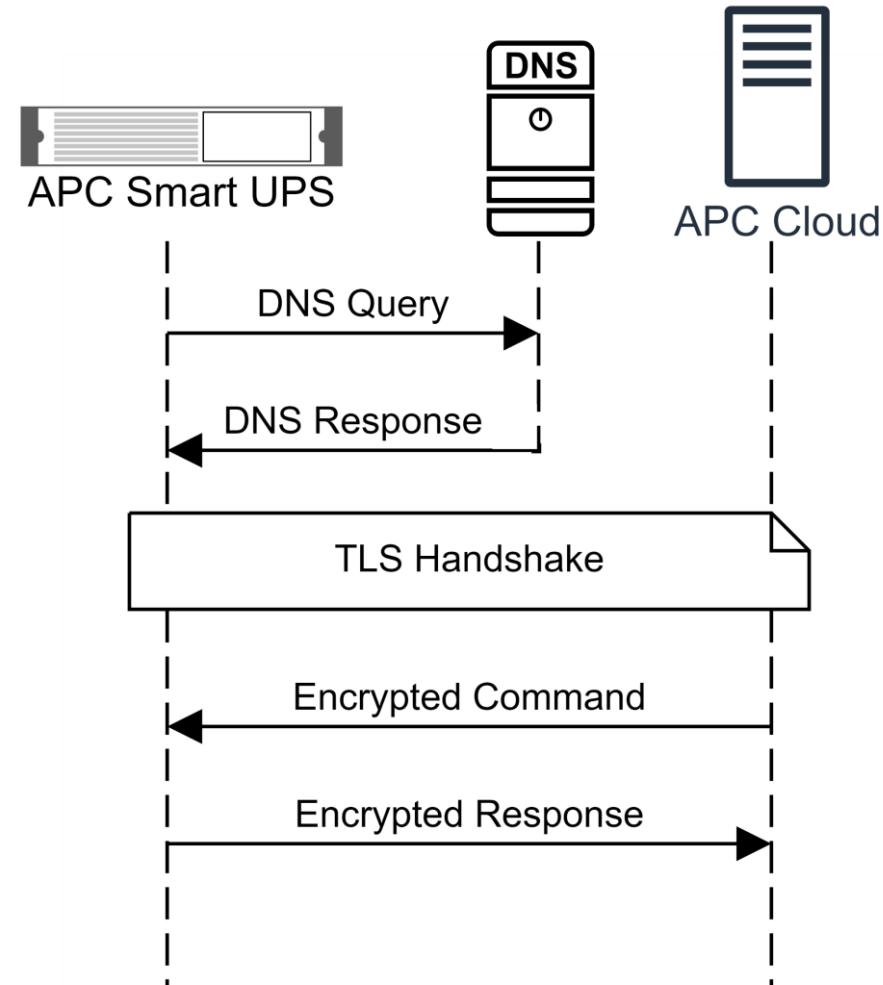
## Please note

The upgrade takes approximately 5-15 minutes. UPS network communications will be interrupted during this time.

If you are using PowerChute with this UPS, please see our configuration [recommendations](#) in the Help Center.

 [HELP CENTER](#)

# SmartConnect – Connection Scheme



# DNS Spoofing

KEEM 🎉 ✅ @KEEMSTAR · Aug 31, 2017  
100% confirmed #WikiLeaksHack !!!

KEEM 🎉 ✅ @KEEMSTAR · Aug 31, 2017  
BREAKING: OurMine claims to have HACKED @wikileaks! It's not showing up yet. But OurMine says it will soon. #DramaAlert

Done browserling.com

02:52 http://wikileaks.org Run Tools End Session

http://wikileaks.org/ Hacked By OurMine

[!] HACKED BY OURMINE[!]  
OURMINE  
Ä€" YOUR SECURITY IS LOW Ä€"

Hi, it's OurMine ( Security Group ), don't worry we are just testing your.... blablablab, Oh wait this is not a security test! Wikileaks, remember when you challenged us to hack you?

Anonymous, remember when you tried to dox us with fake information for attacking wikileaks?  
<https://twitter.com/YourAnonNews/status/679472812013301762>

There we go! One group beat you all! #WikiLeaksHack let's get it trending on twitter!

[Www.OurMine.Org](http://www.ourmine.org) | [contact@ourmine.org](mailto:contact@ourmine.org)

66 186 1.7K

Internet Attack Vector

Remote Code Execution

Power Tampering

# DNS Spoofing



## 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.

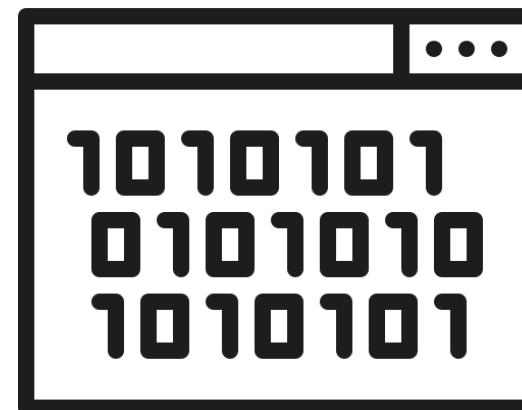
A screenshot of a Twitter post from the account @KEEMSTAR. The post includes two tweets. The first tweet from KEEMSTAR on Aug 31, 2017, says "BREAKING: OurMine claims to have HACKED @wikileaks! It's not showing up yet. But OurMine says it will soon. #DramaAlert". The second tweet from KEEMSTAR on Aug 31, 2017, shows a screenshot of a browser window titled "browserling.com" displaying a hacked WikiLeaks page. The page has a red banner at the top reading "!!I HACKED BY OURMINE!!" and "OURMINE". Below the banner, it says "YOUR SECURITY IS LOW". There is also some smaller text about testing and a link to their website. The post has 66 likes, 186 retweets, and 1.7K favorites.

Internet  
Attack  
Vector

Remote  
Code  
Execution

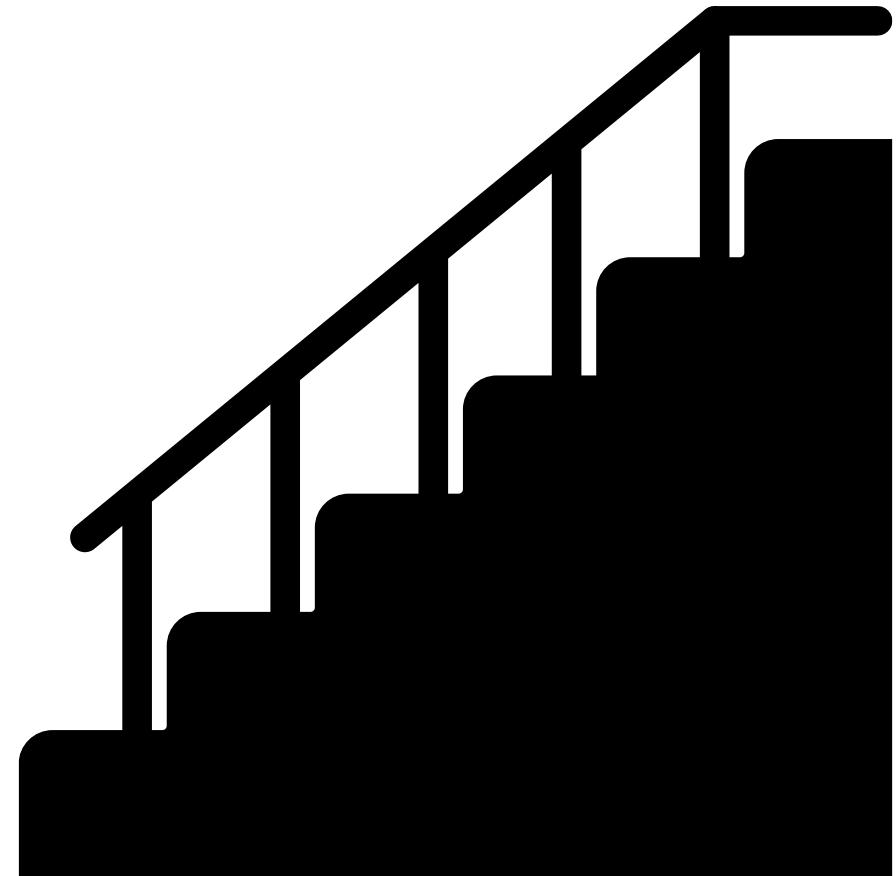
Power  
Tampering

# Research Milestones



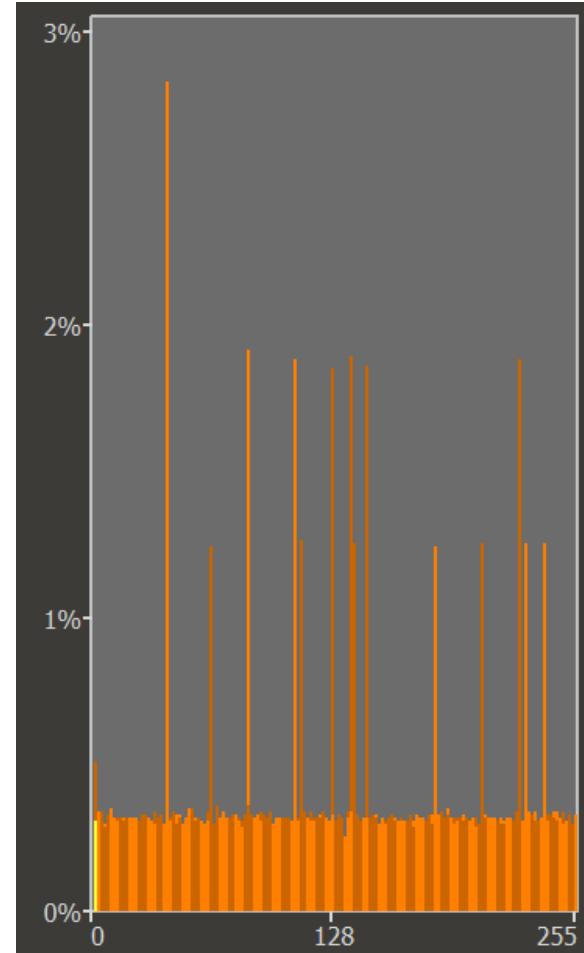
# RCE - Technical Steps

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



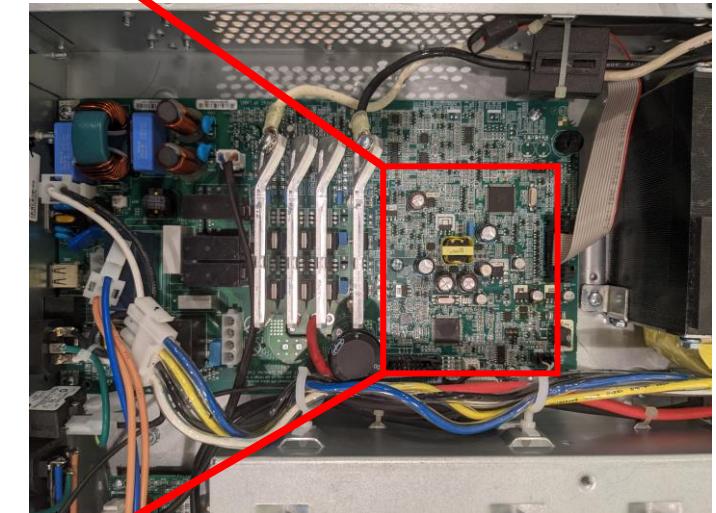
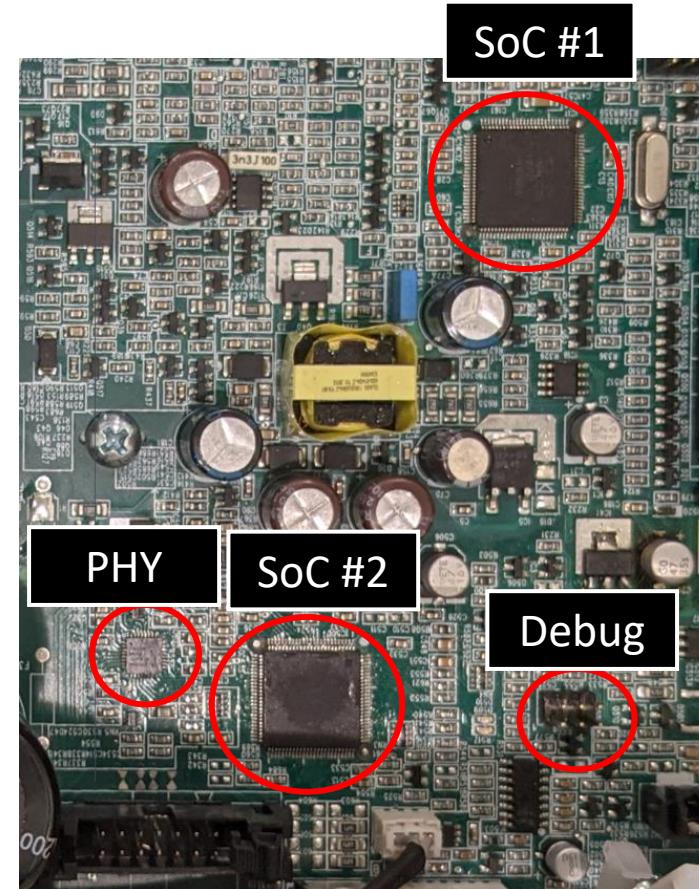
# Initial Review

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

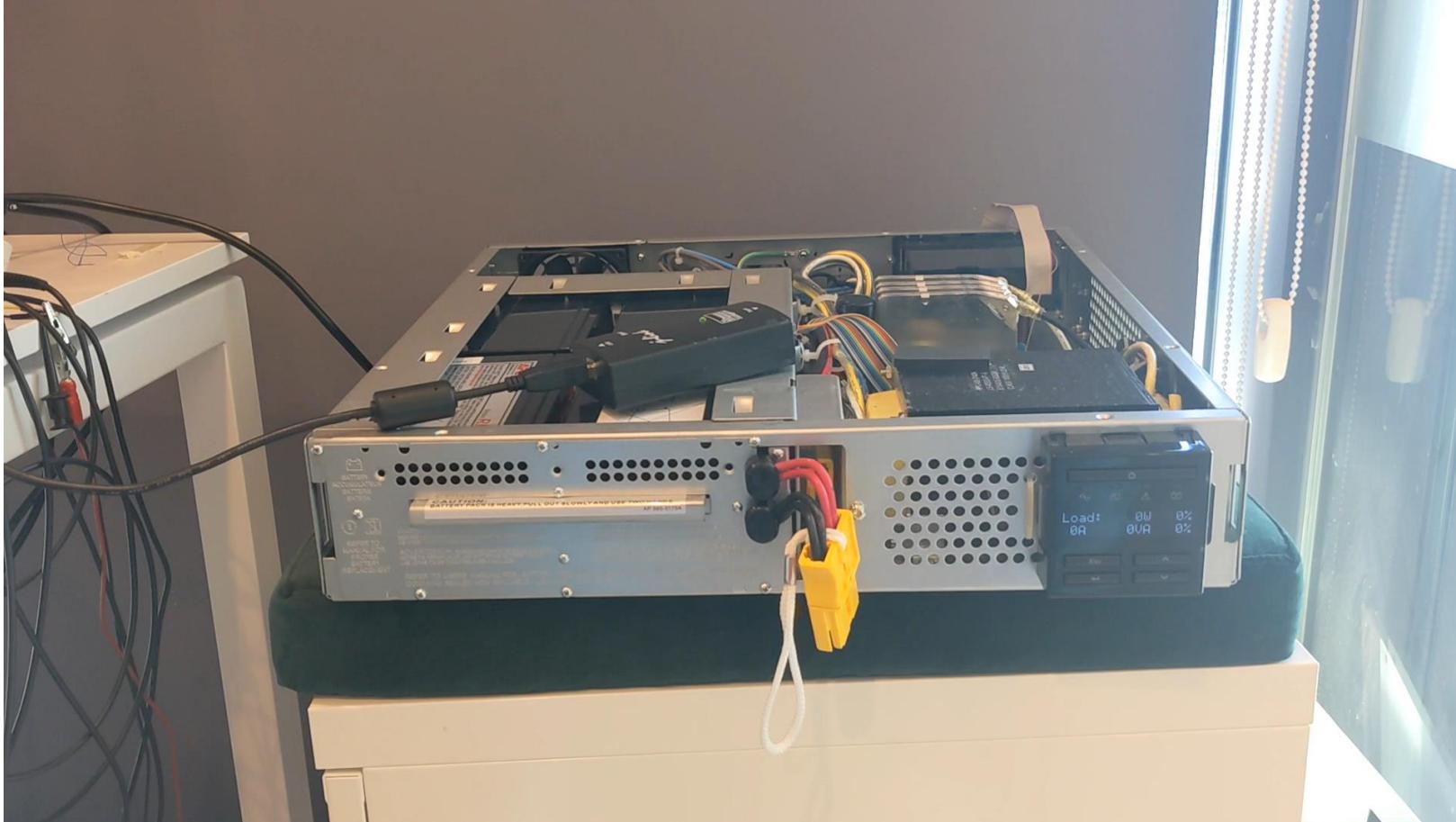


# FW Cracking

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

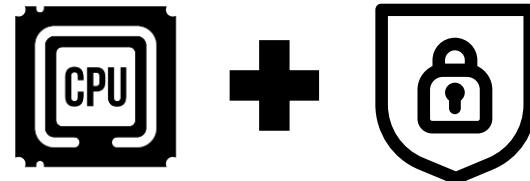


# Hardware Debugging



# Debugging Capabilities

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



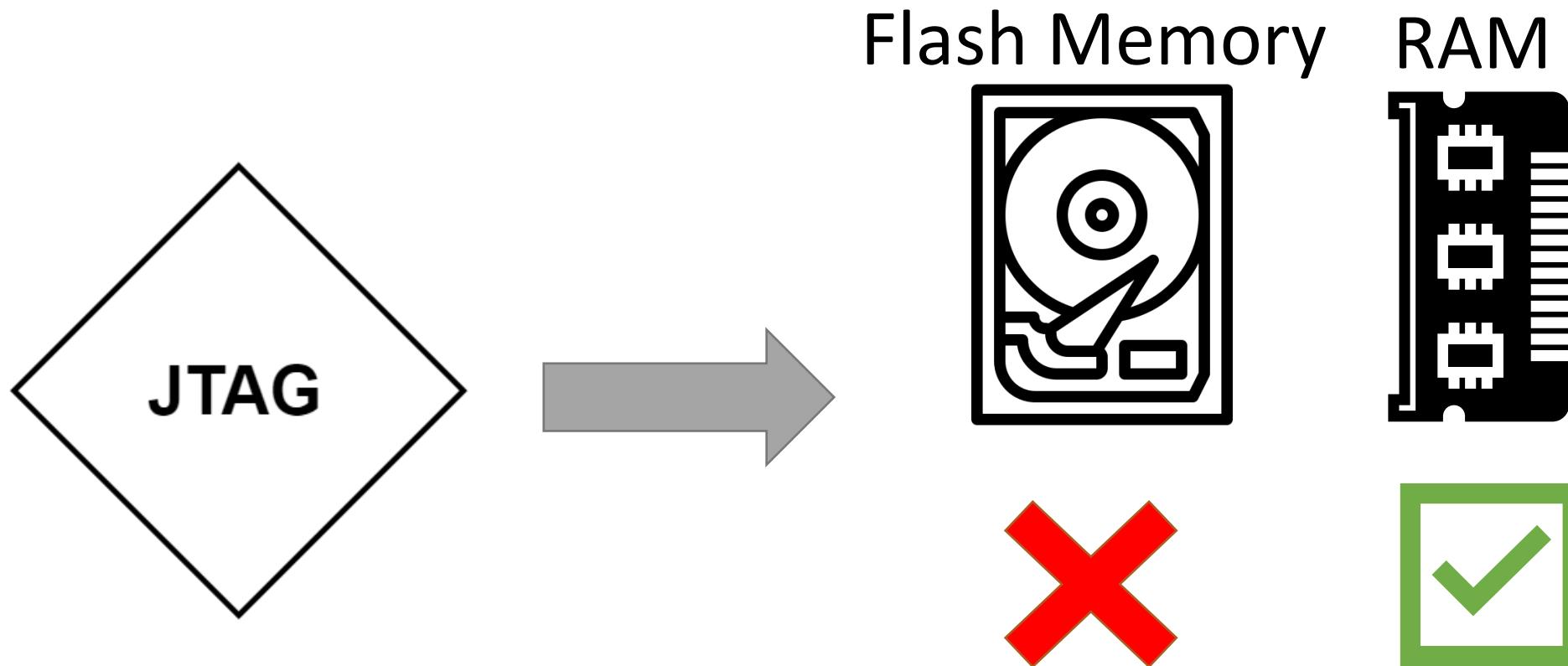
## 2.6.3 Read protection (RDP)

No access (read, erase, program) to Flash memory

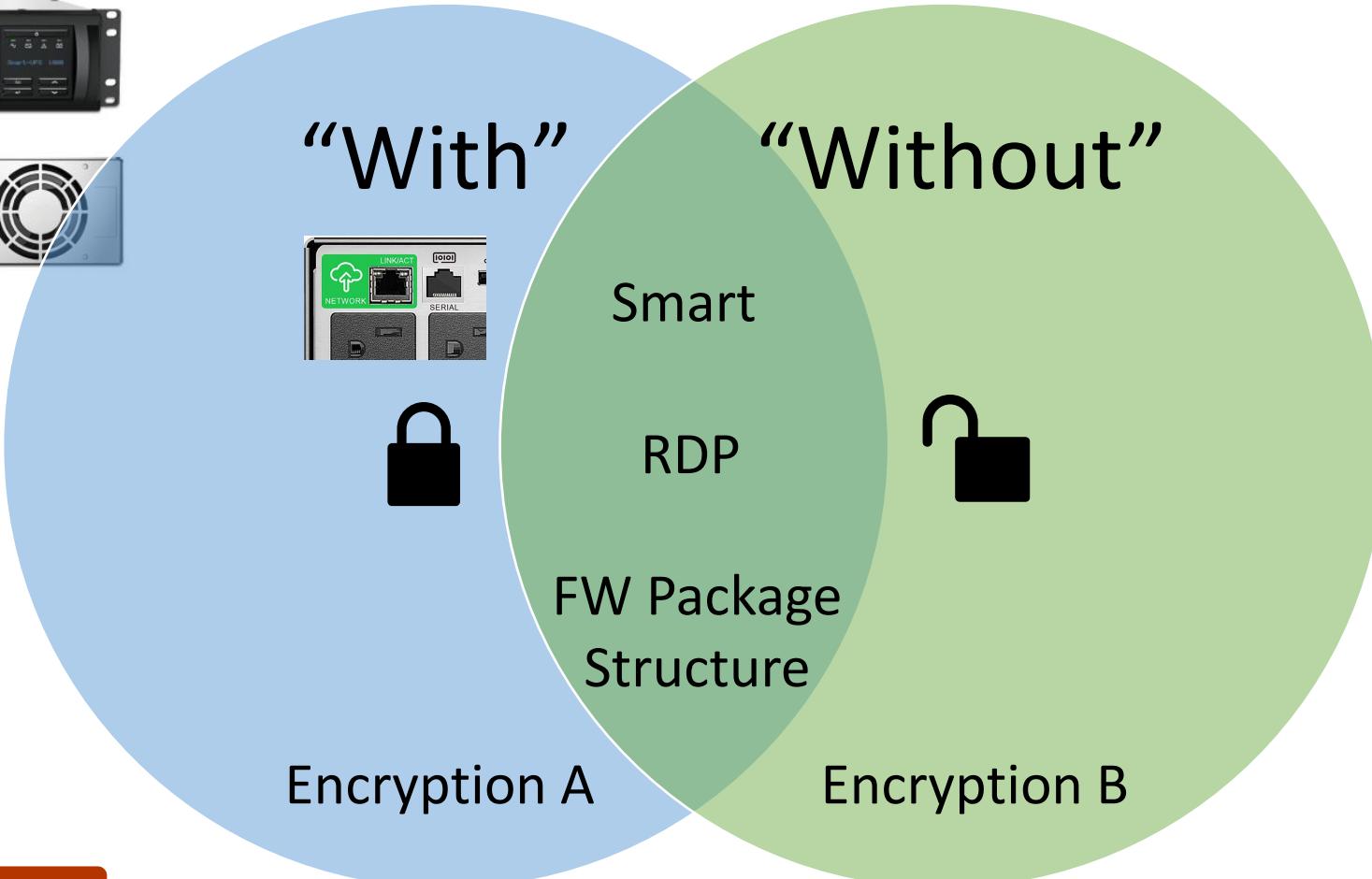
while the debug feature is connected

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

# RDP- Hardware Memory Protection

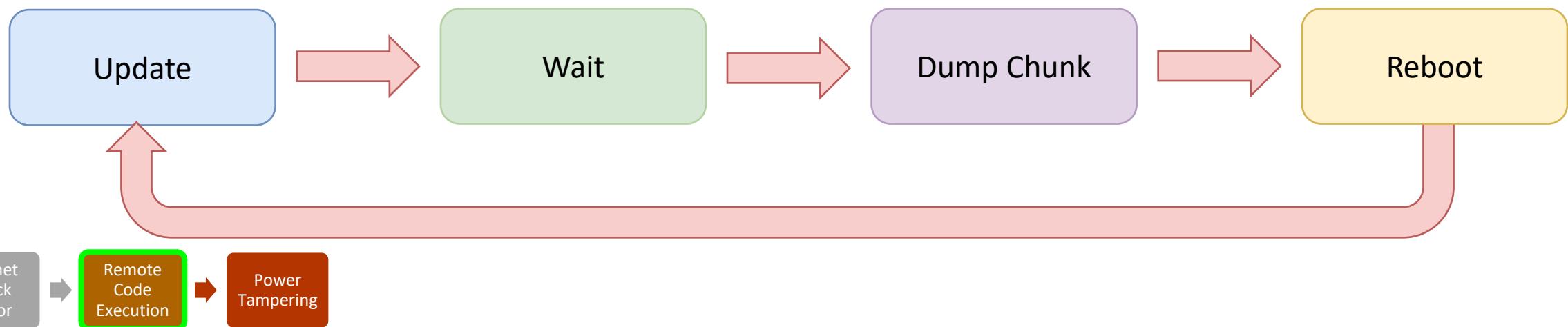


# Smart-UPS Sub-Family – W/O SmartConnect



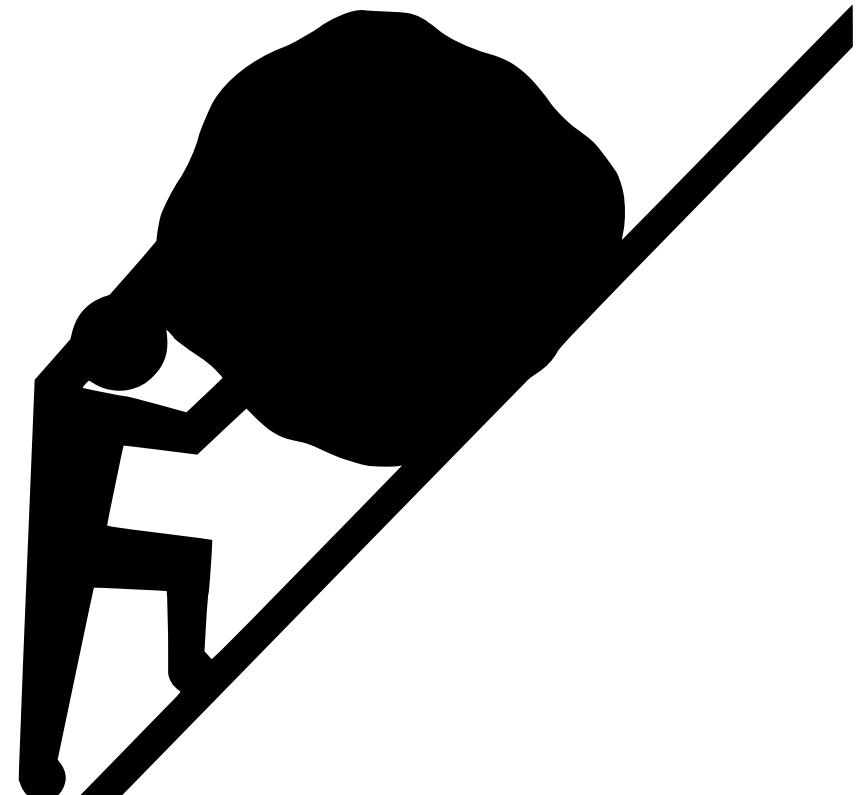
# Walking in The Dark

- 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



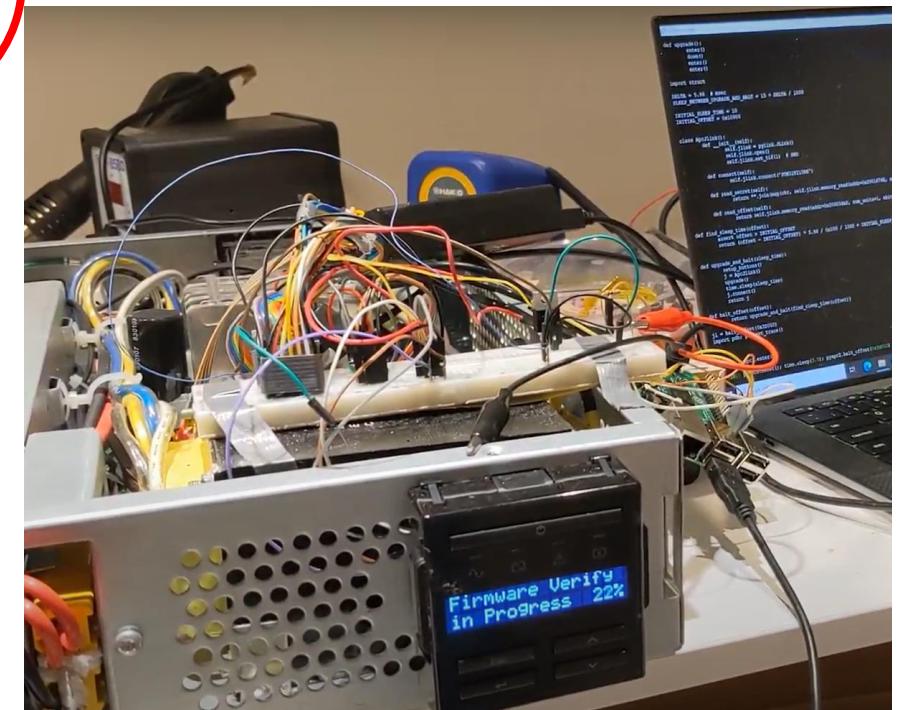
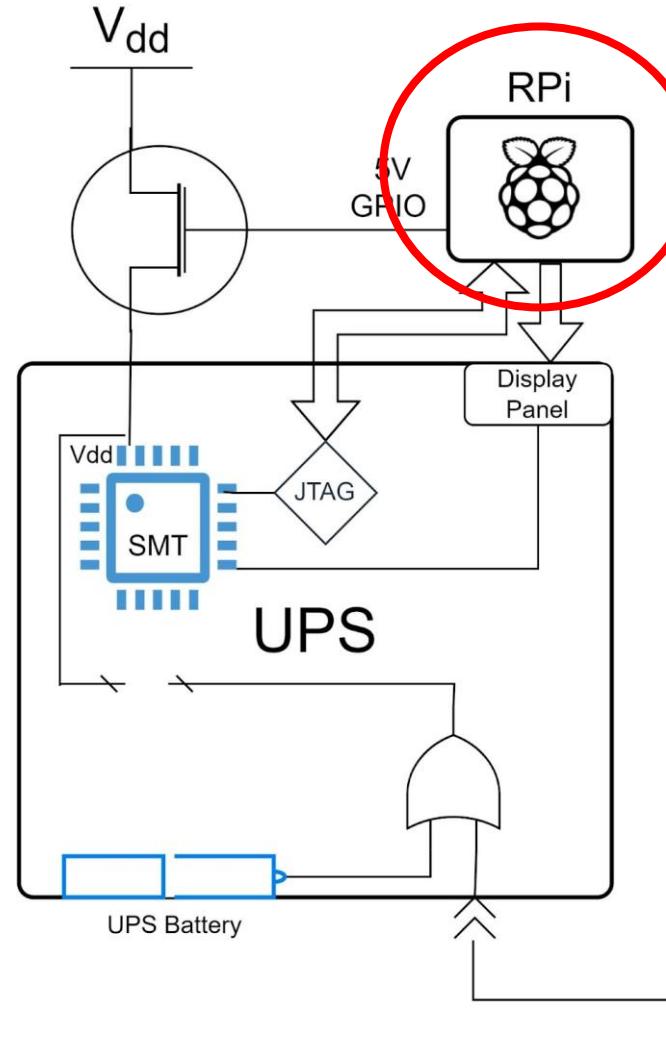
# Running the Numbers

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



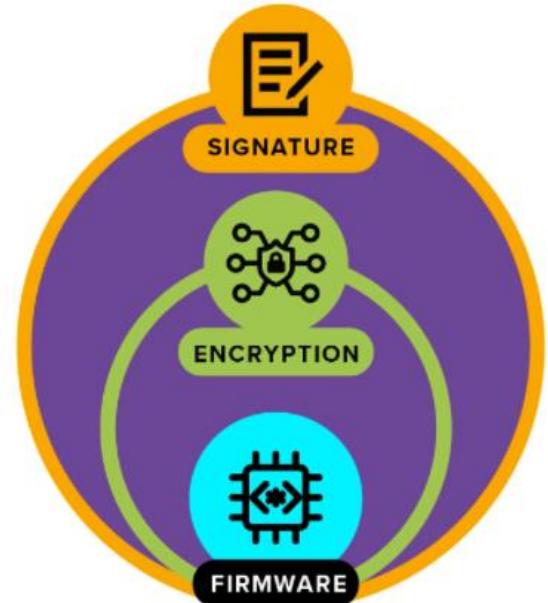
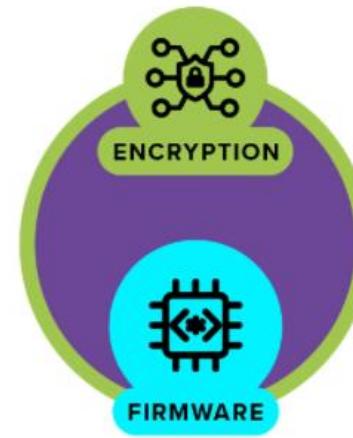
# Hardware Brute-Force

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



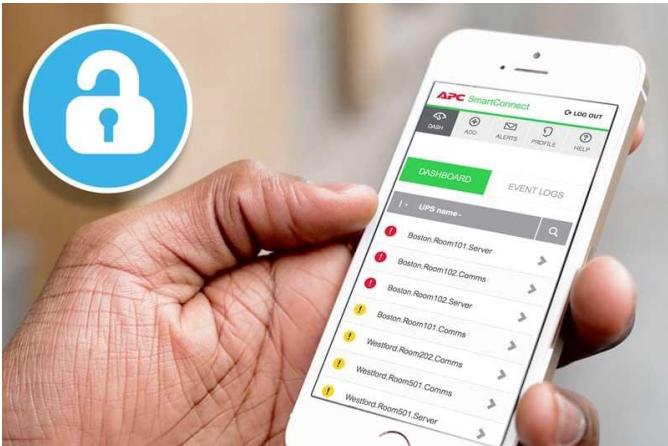
# Decrypted FW Findings

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

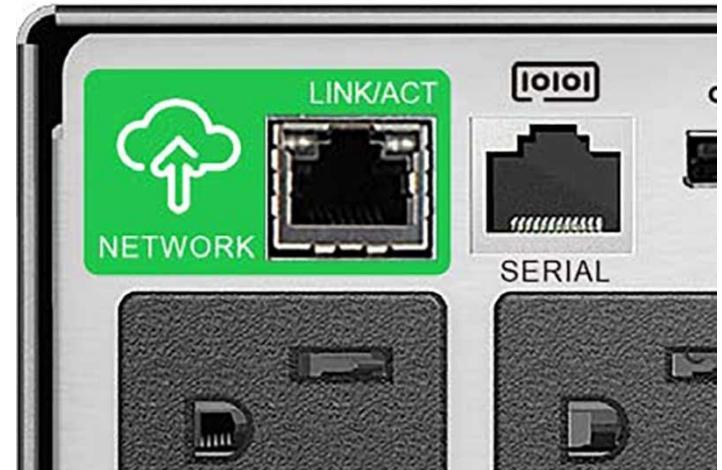


# SmartConnect Attack Surface

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



Internet  
Attack  
Vector



MOCANA®

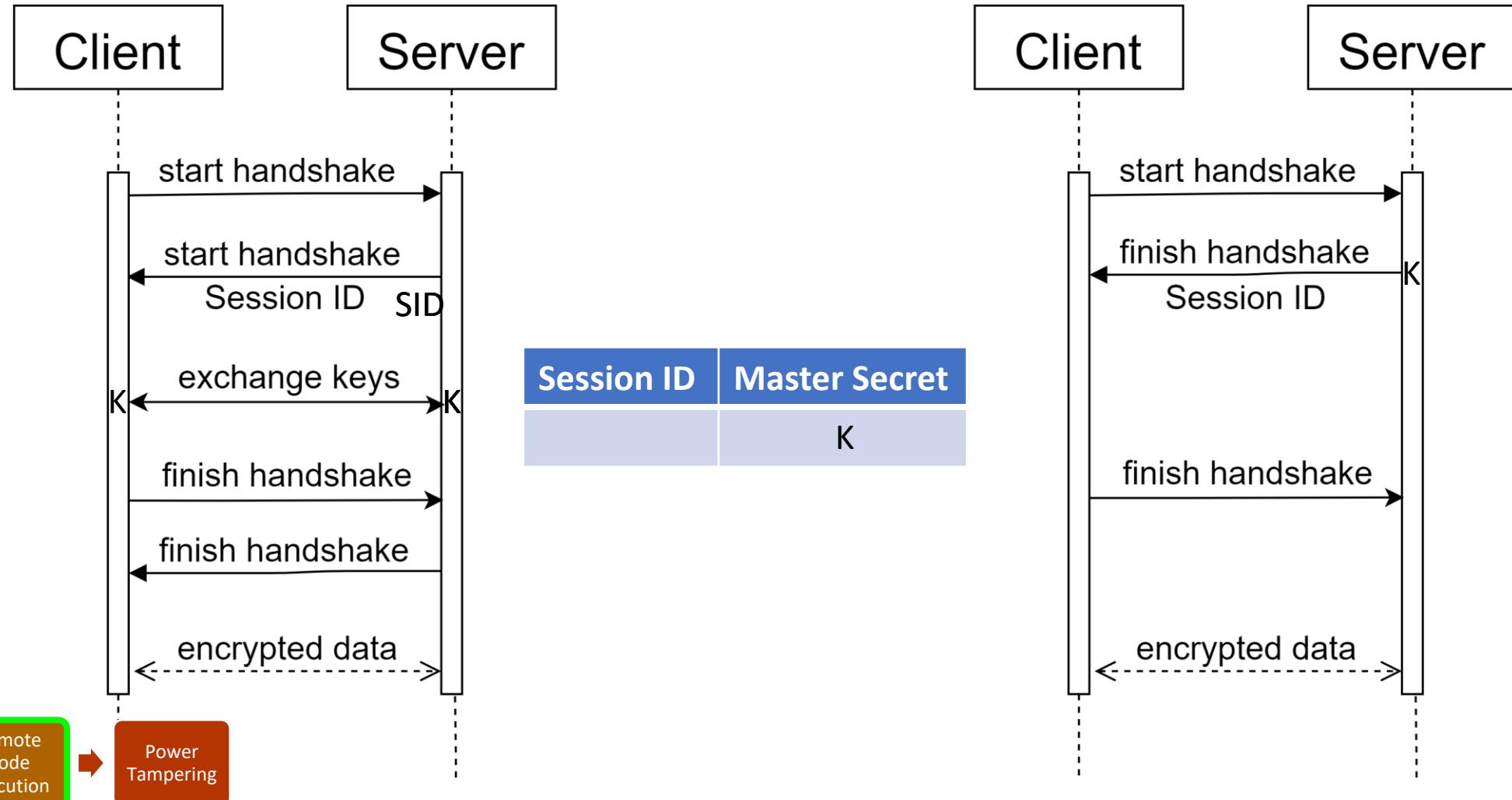
# External Risk

- 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

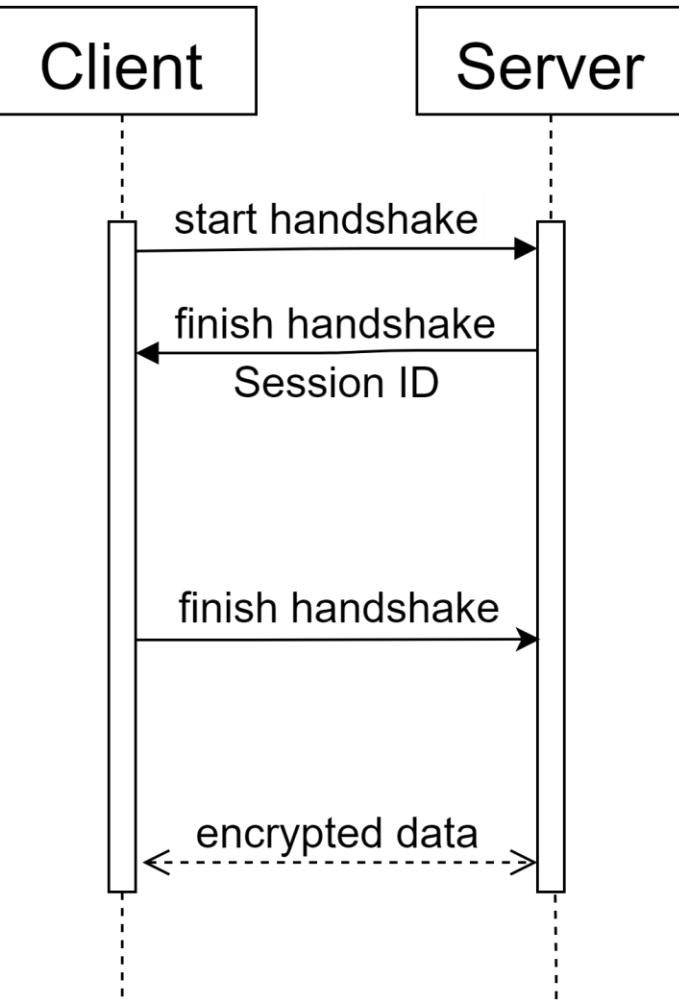
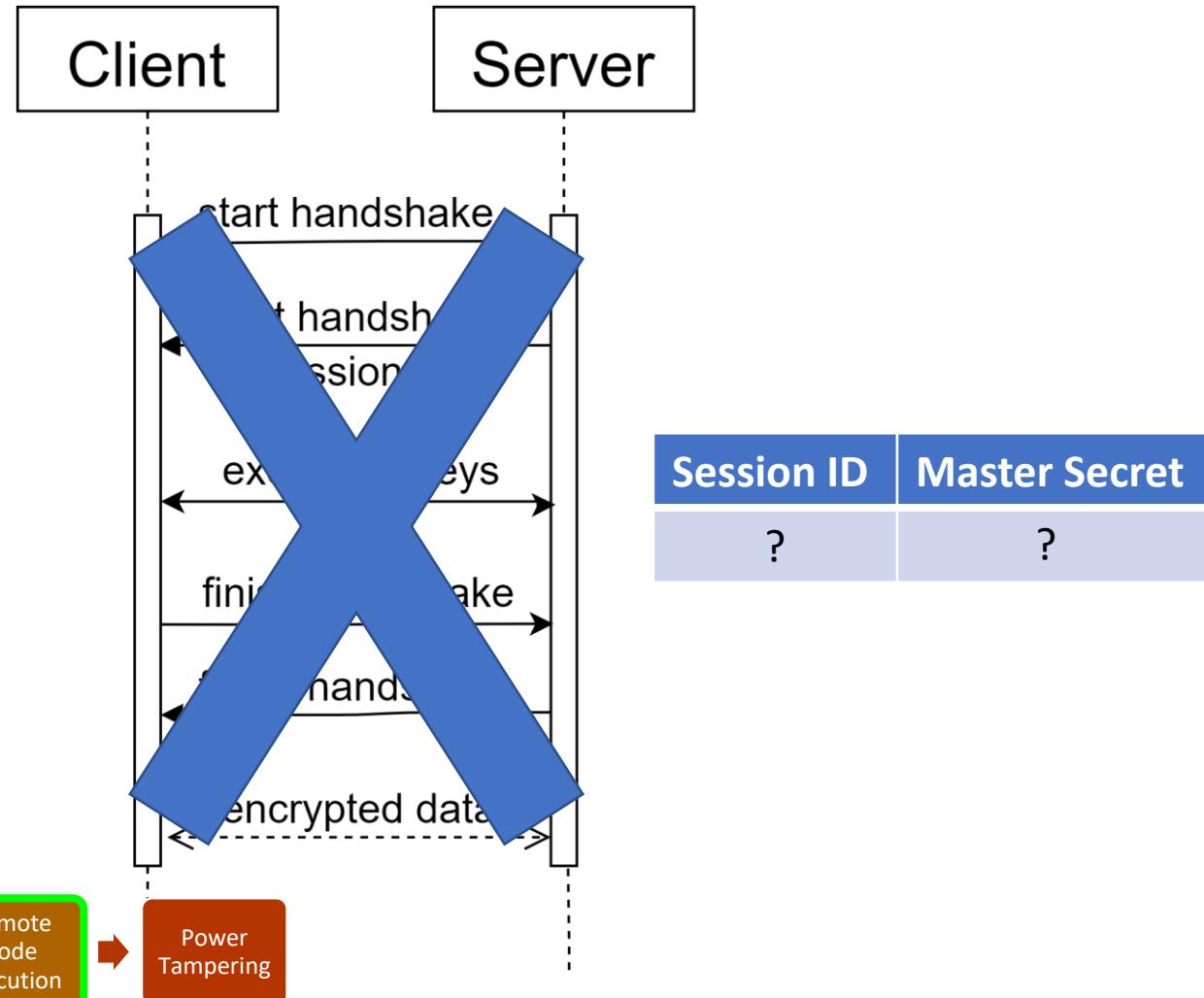
```
int recv_tls_async(ssl_t* ssl_sock)
{
    ...
    → func_tbl->mocana_ssl_recv(ssl_sock, pbuf);
    ...
    if (ssl_sock->state == COMPLETE)
        handle_payload(ssl_sock);
    pbuf_free(pbuf);
    ...
}
```



# TLS Resumption



# Pre-Auth-Resumption



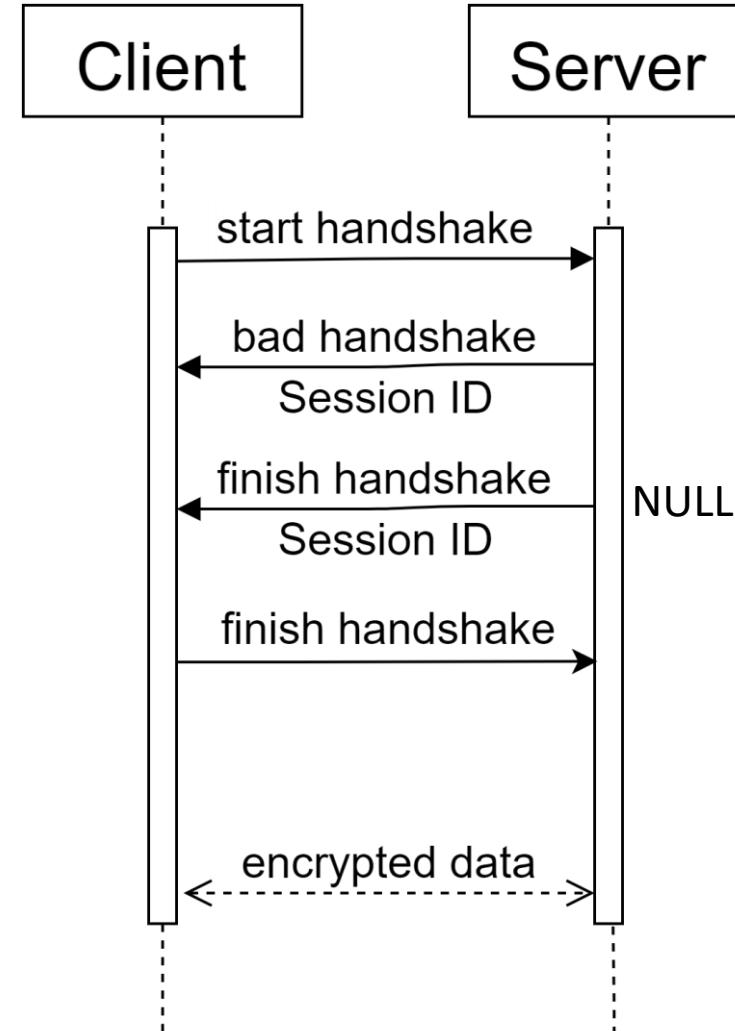
# Mocana Handshake

- 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
NSUDL	NULL



# Pre-Auth-Resumption Debug View



ssl\_sock

resumption  
cipher\_suite  
key  
id



packet #1

id  
cipher\_suite



packet #2

id  
cipher\_suite



```
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



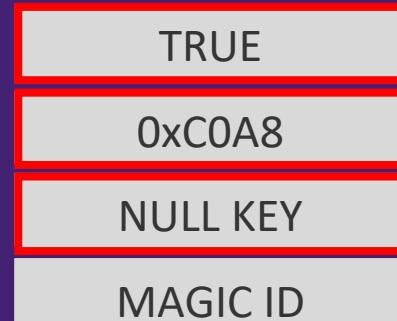
ssl\_sock

resumption

cipher\_suite

key

id



packet #1

id

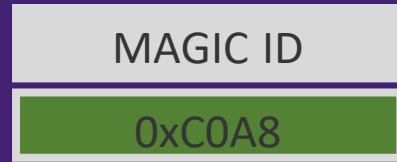
cipher\_suite



packet #2

id

cipher\_suite



```
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);  
    }  
    ...  
}
```

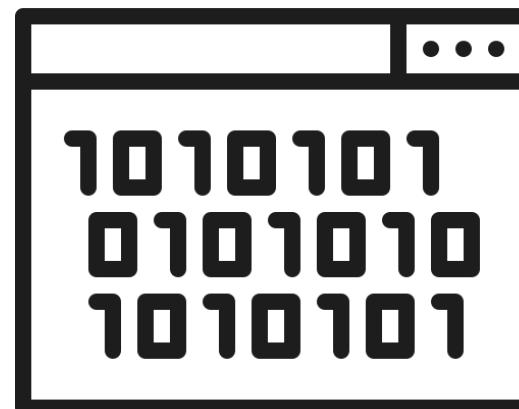
# What It Actually Looks Like

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 (0xffff)  
 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



# IMPACT CATEGORIES



Network

Internet Attack Vector



Persistency/Stronghold



Power Connected Devices

Shutdown



???



UPS

Brick



???

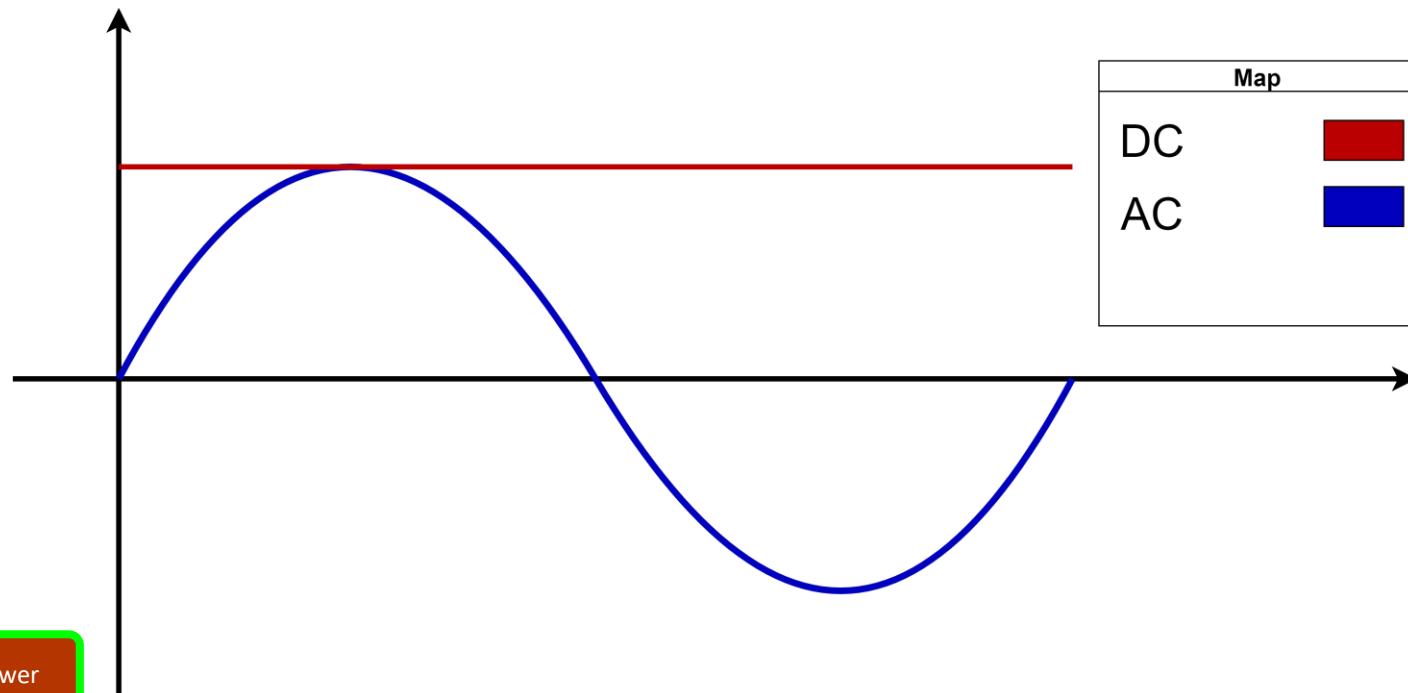
Internet  
Attack  
Vector

Remote  
Code  
Execution

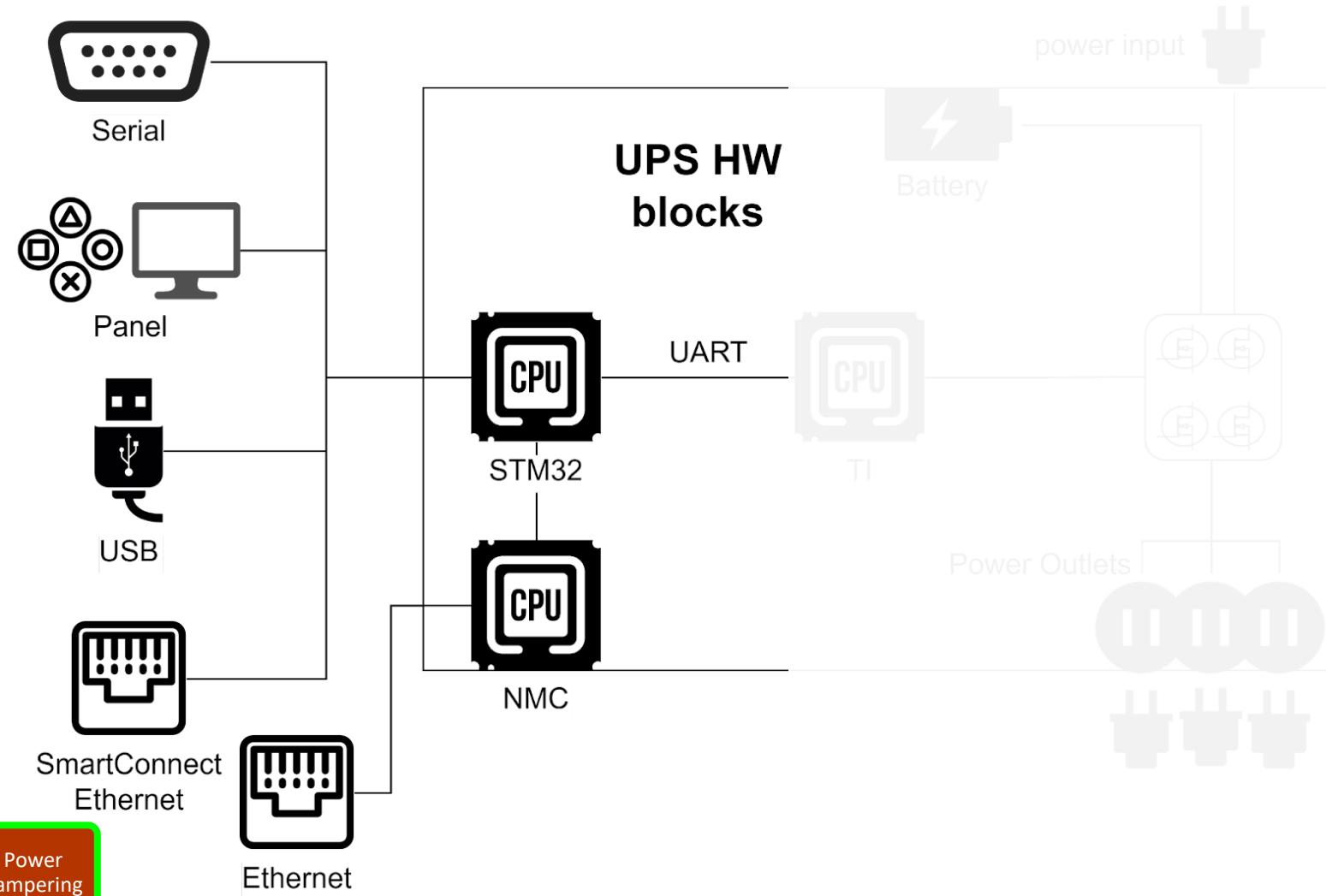
Power  
Tampering

# Maximizing Impact

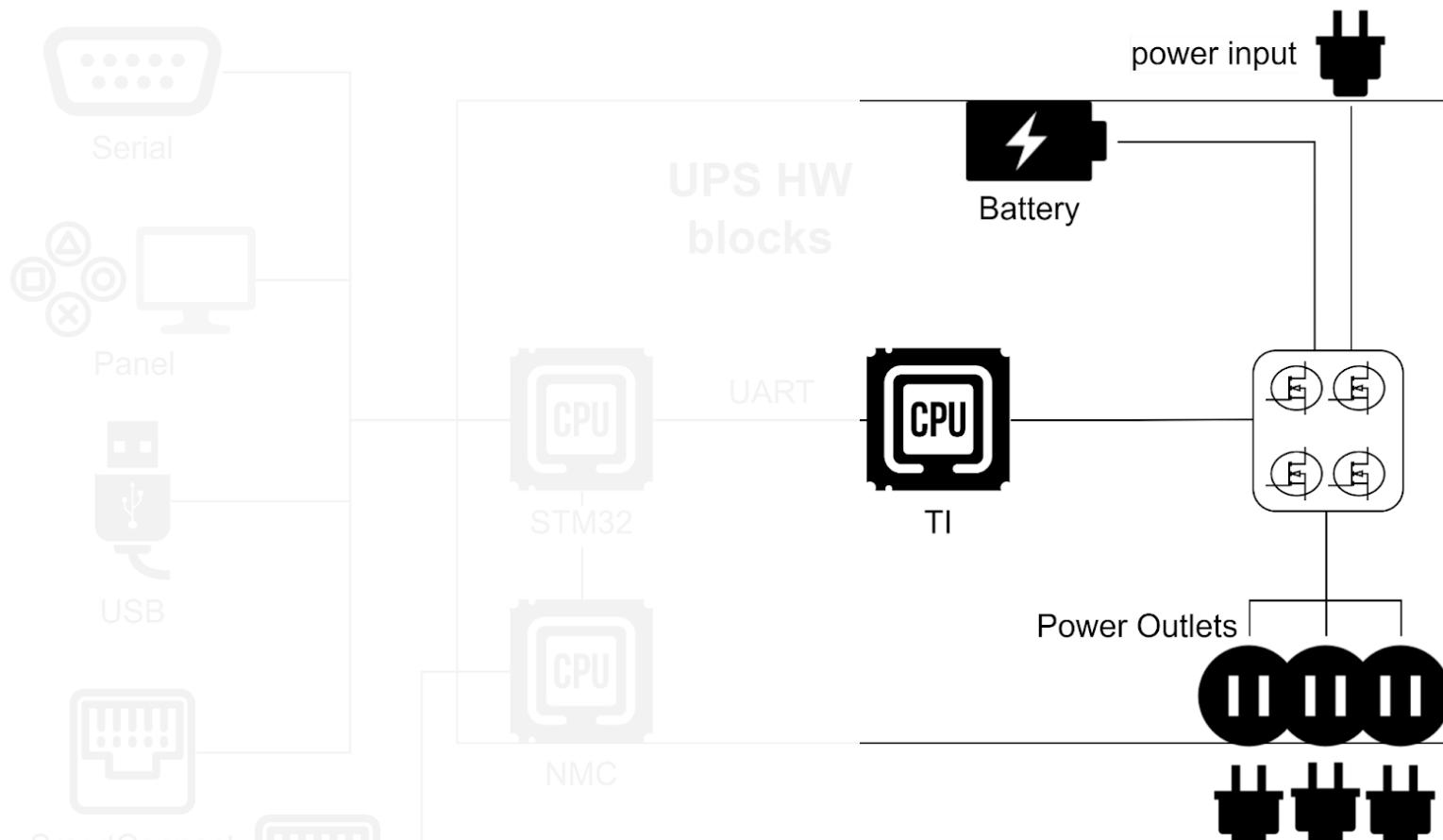
- Output via a battery meaning DC→AC converter
- Software is involved, but how much?



# Internal Architecture



# Internal Architecture



CH1

Vrms

336.0V

CH1

Vmax

424.0V

CH1

Vmin

-416.0V

CH1

Vpp

840.0V

CH1

Freq

50.00Hz



0.1sec/div

0.05 sec

0.5sec/div

0.1sec/div

0.05 sec

CH1

Vrms

112.0V

CH1

Vmax

168.0V

CH1

Vmin

-168.0V

CH1

Vpp

336.0V

CH1

Freq

200.0Hz



0-200V

0-199.999Hz

10.00ms

N Post 8.00ms

0-100V

# IMPACT CATEGORIES



Network

Internet Attack Vector



Persistency/Stronghold



Power Connected Devices

Shutdown



Power Tampering



UPS

Brick



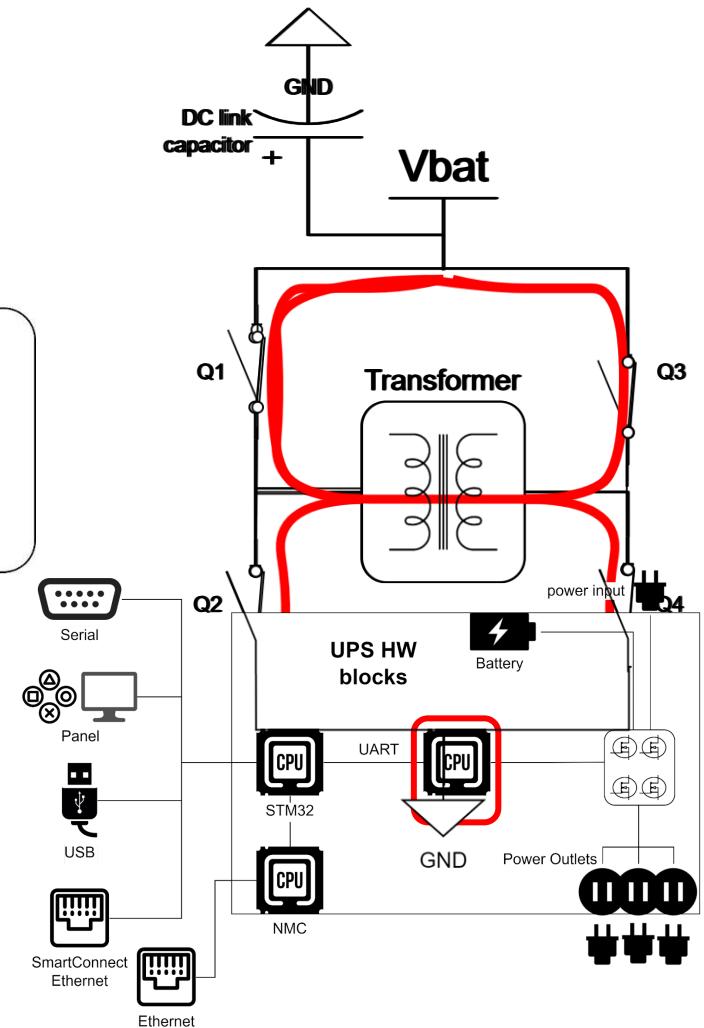
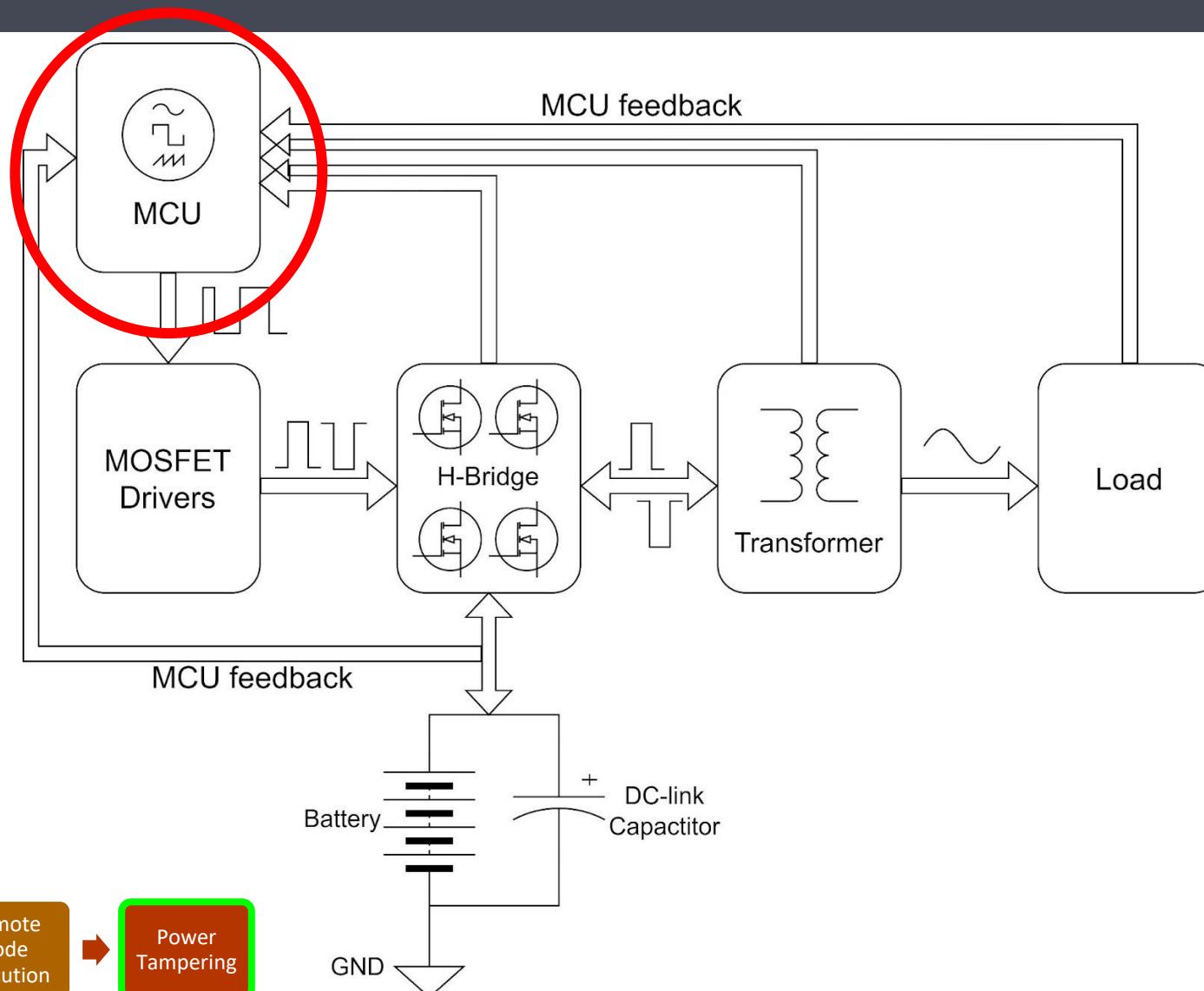
???

Internet  
Attack  
Vector

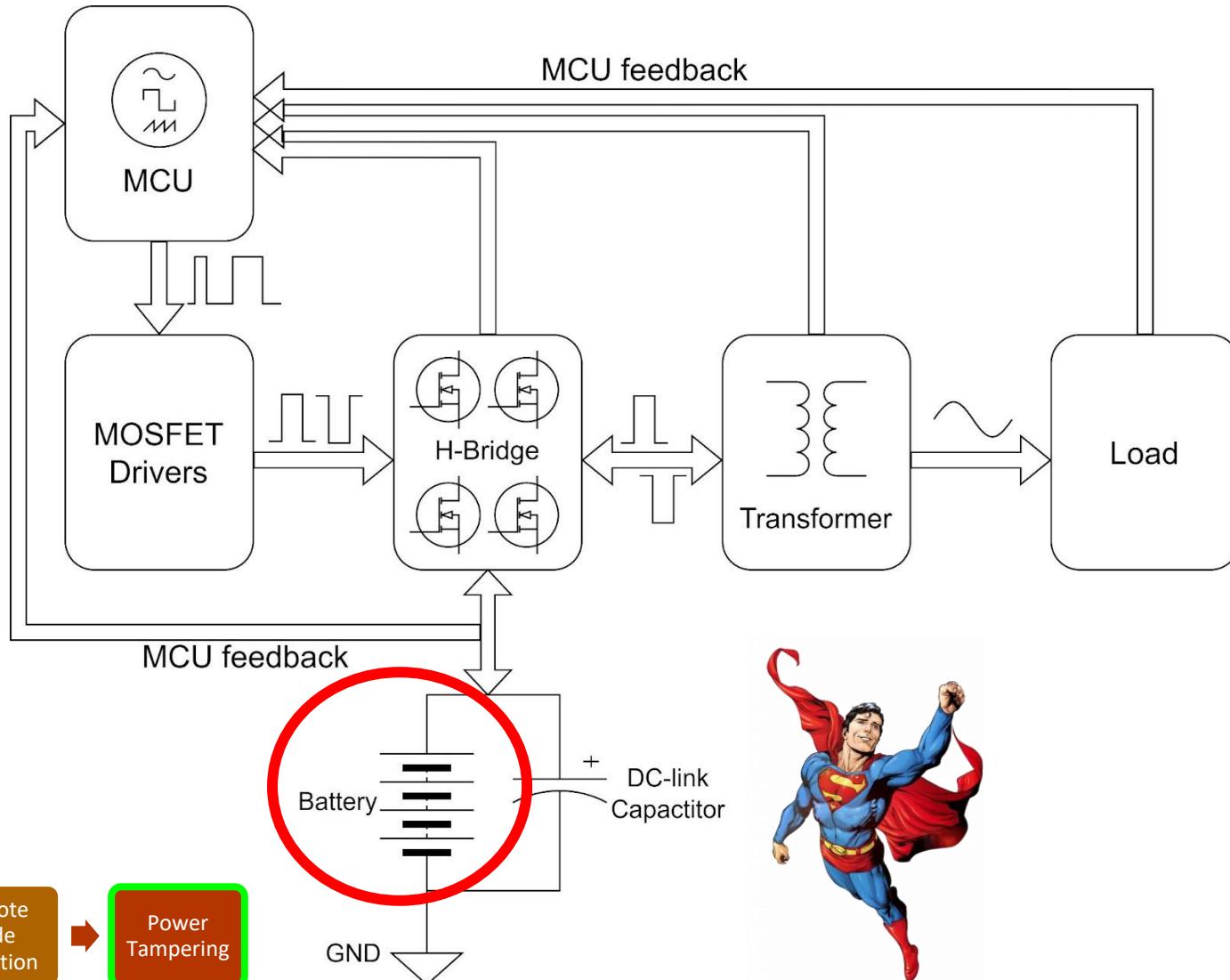
Remote  
Code  
Execution

Power  
Tampering

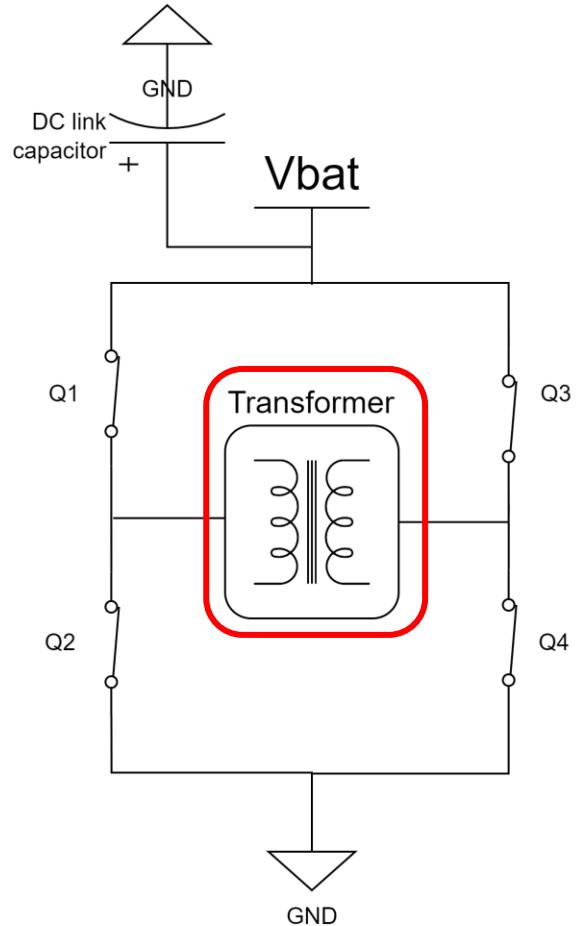
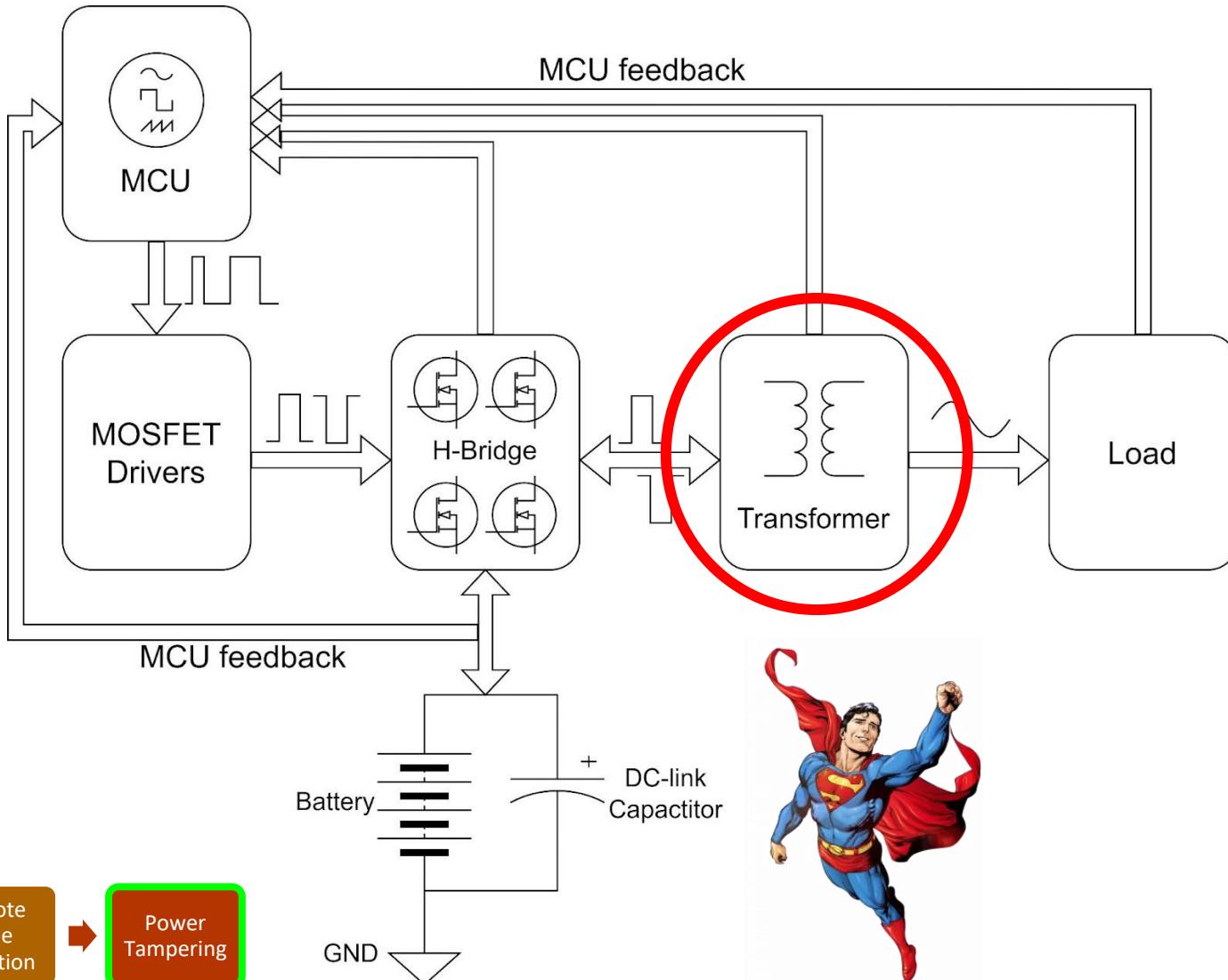
# Power Conversion Blocks



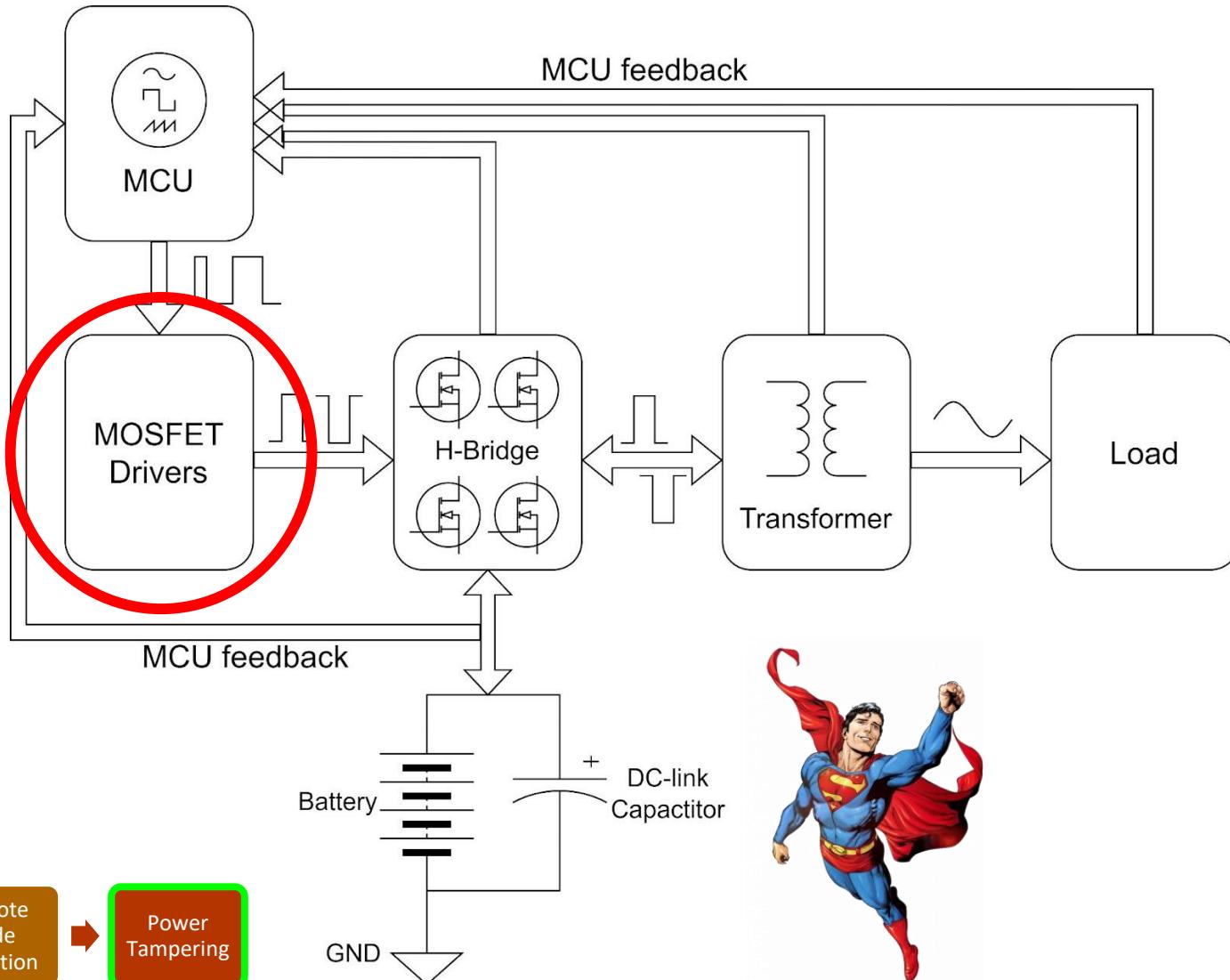
# Power Conversion Blocks



# Power Conversion Blocks



# Power Conversion Blocks



# Normal UPS On Battery

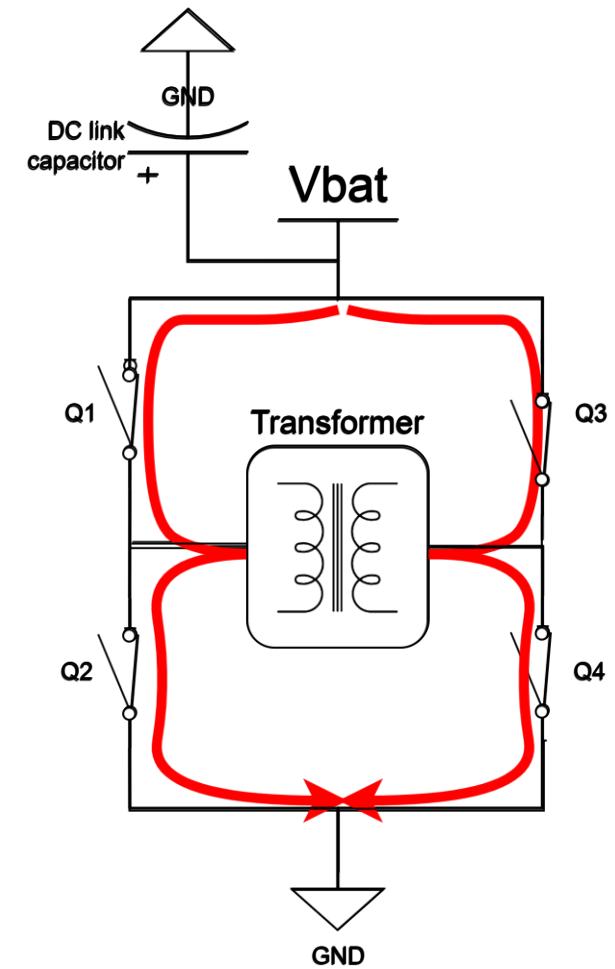


Internet  
Attack  
Vector

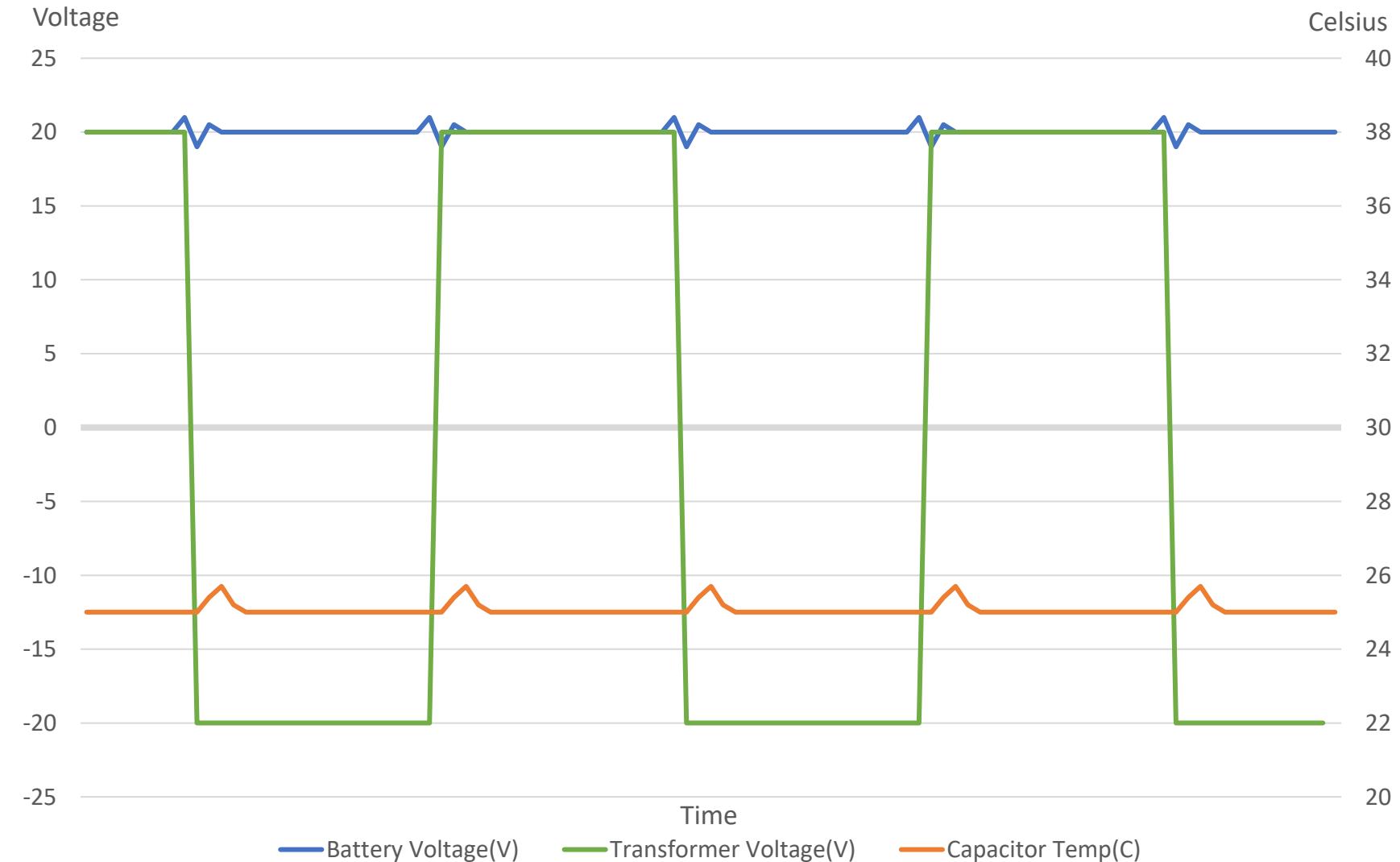
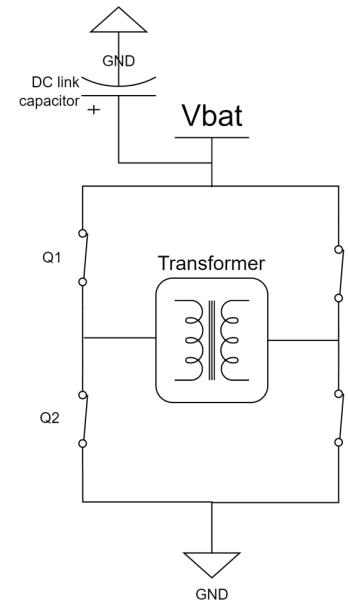
Remote  
Code  
Execution

Power  
Tampering

Transformer Voltage(V)

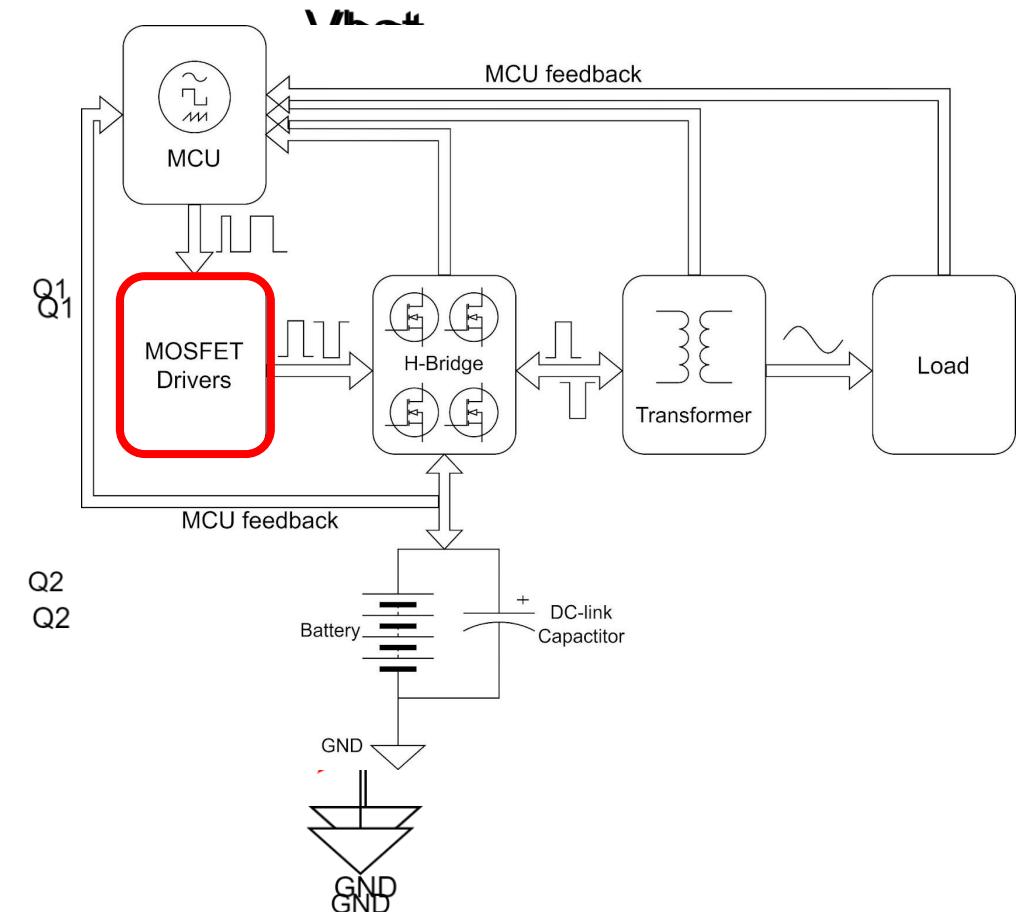


# Normal UPS On Battery



# 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?



# Open Circuit - Transformer

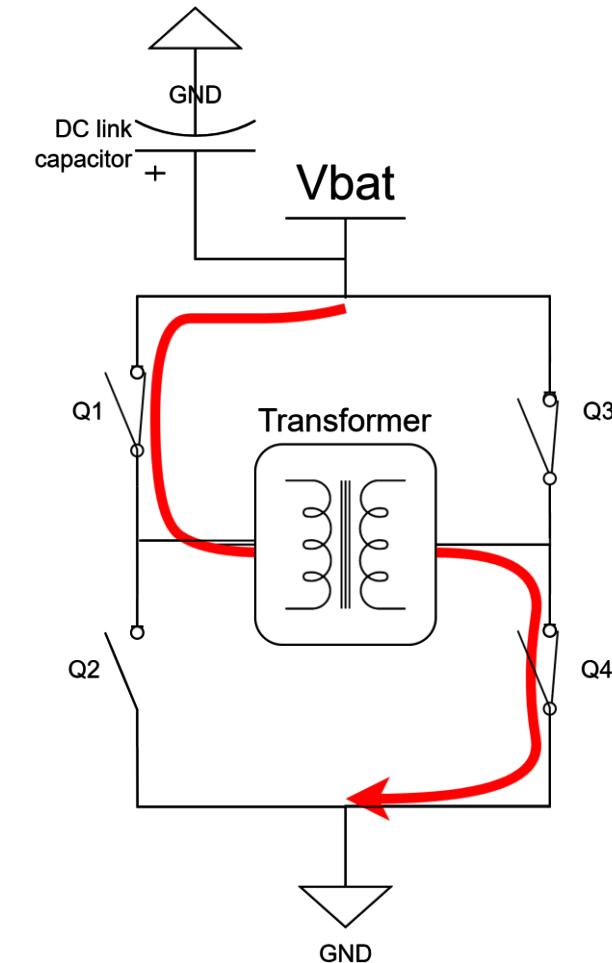
Open circuit Transformer state



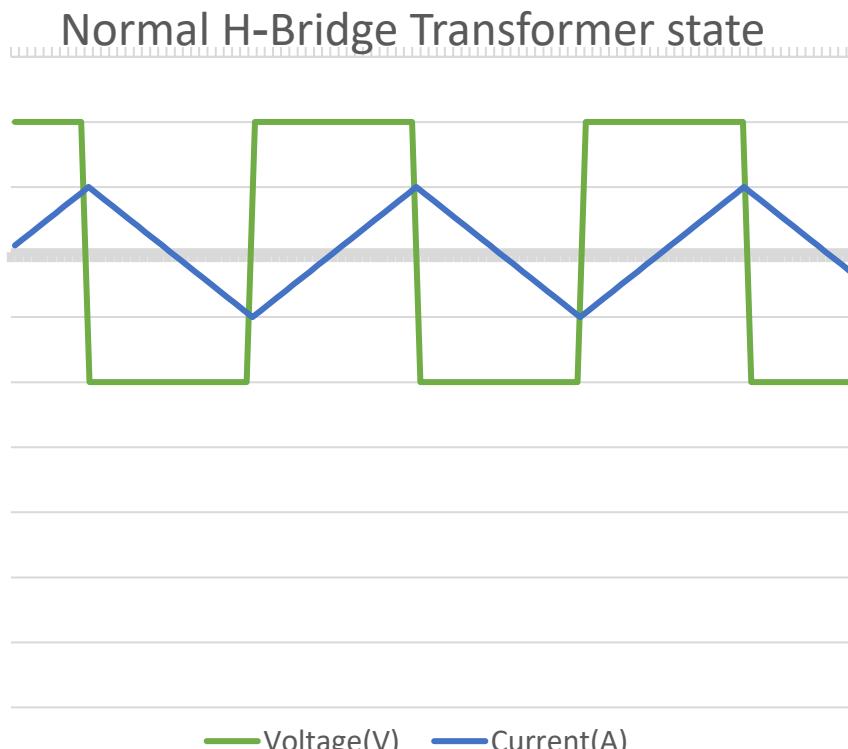
Internet  
Attack  
Vector

Remote  
Code  
Execution

Power  
Tampering

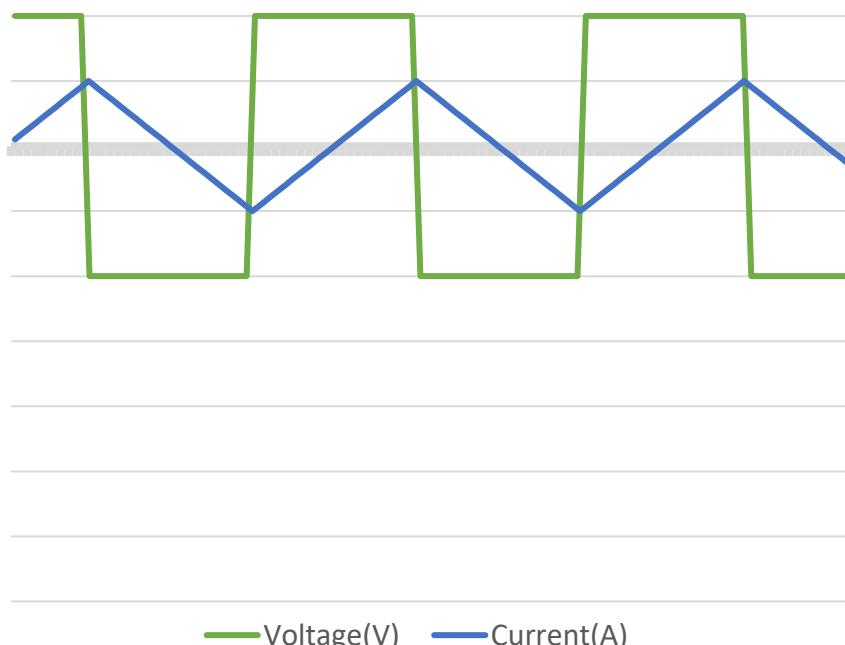


# Inductor's Characteristics

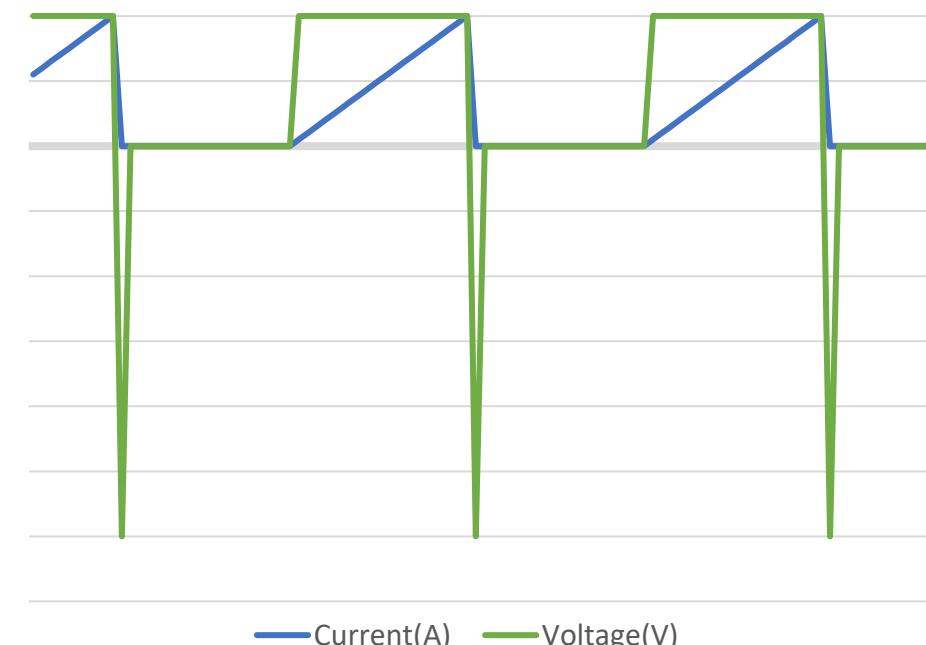


# Inductor's Characteristics

Normal H-Bridge Transformer state



Open circuit Transformer state

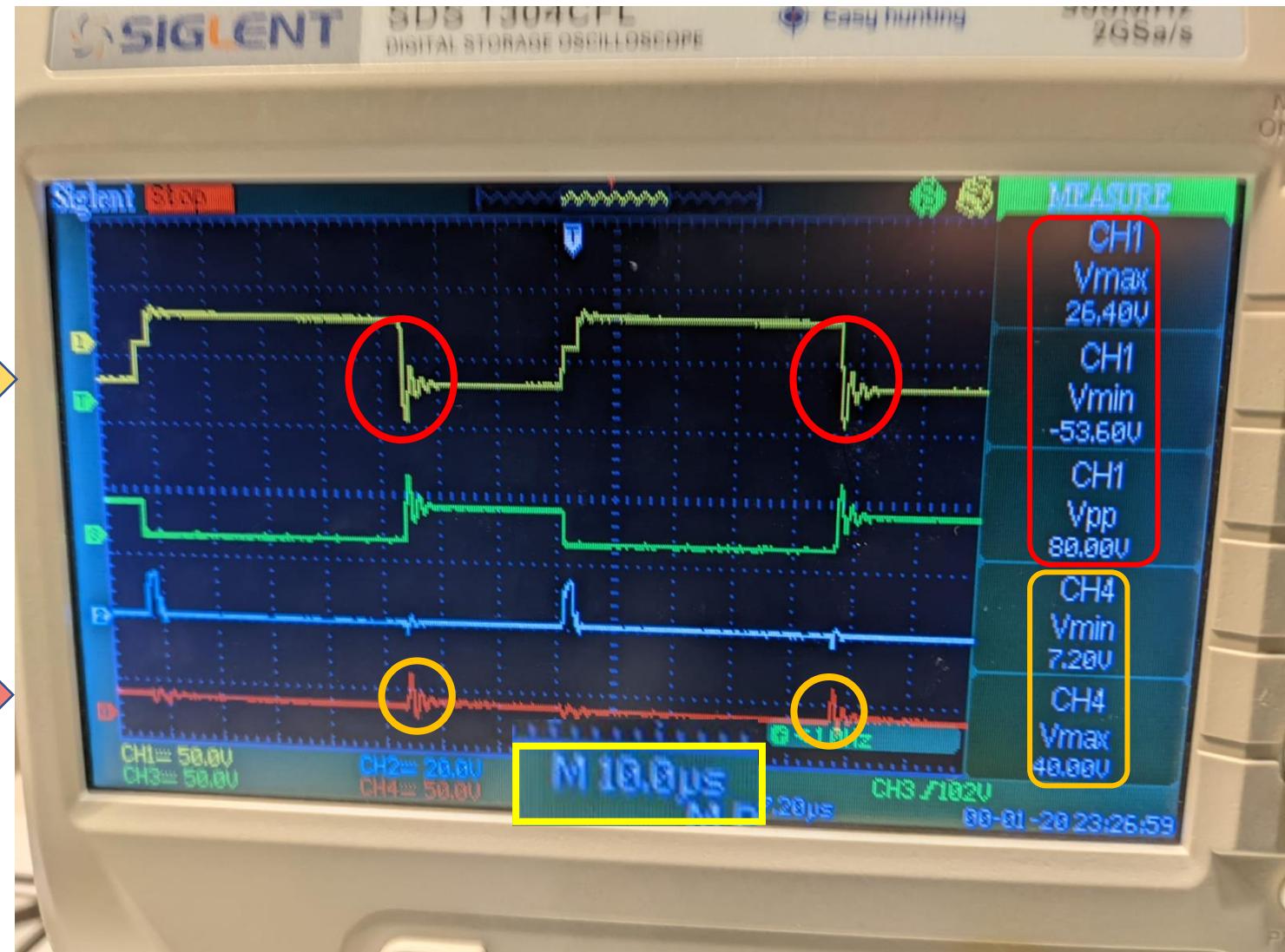


# Results

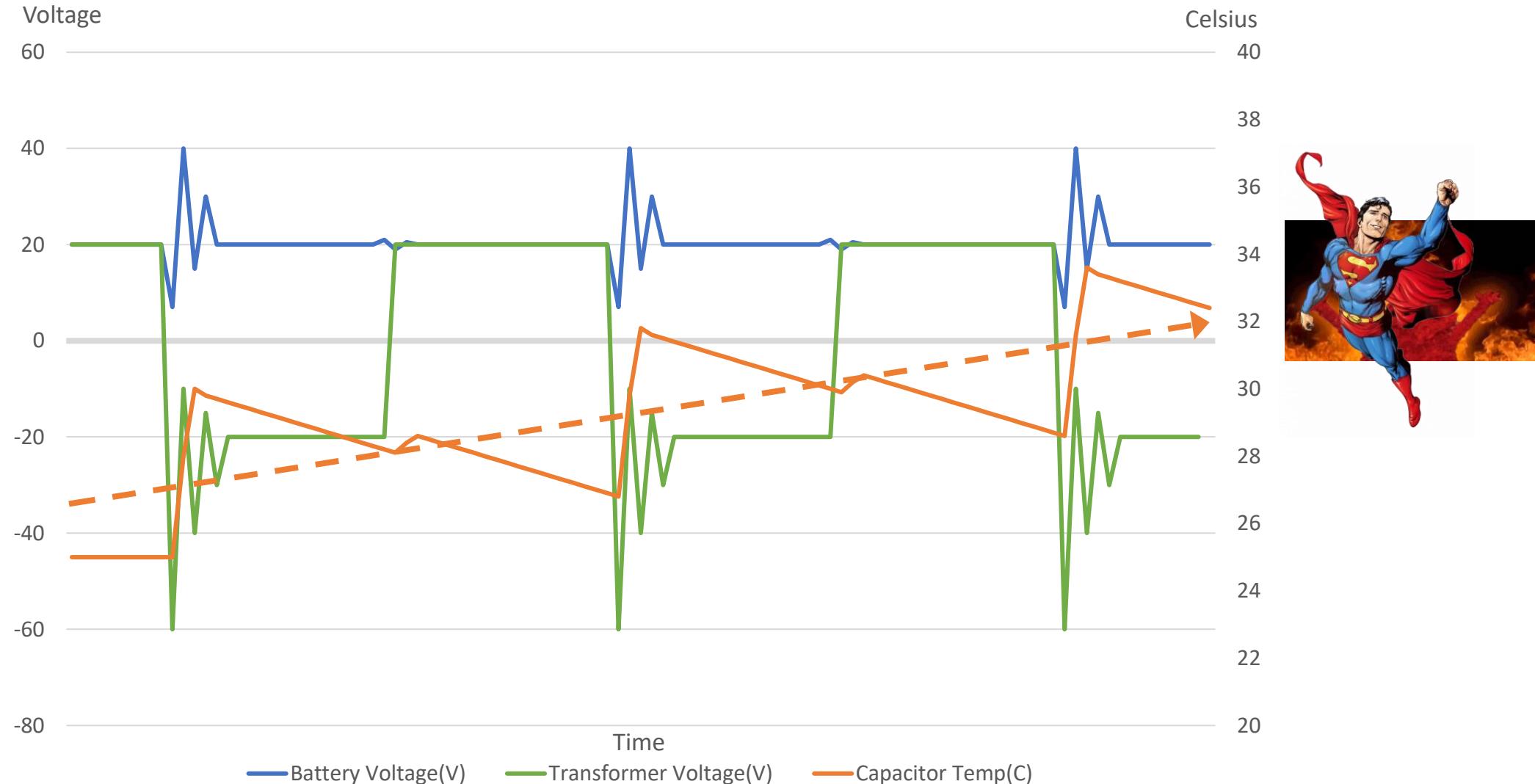
- $\Delta t = \sim 1\mu\text{sec}$
- $\Delta V_{\text{bat}} = 33\text{V}$
- $C = 2700\mu\text{F}$
- $I_C = \sim 100\text{KA!}$

Transformer voltage

Battery voltage



# Hazardous UPS On Battery



# IMPACT CATEGORIES



Persistency/Stronghold

Power Tampering

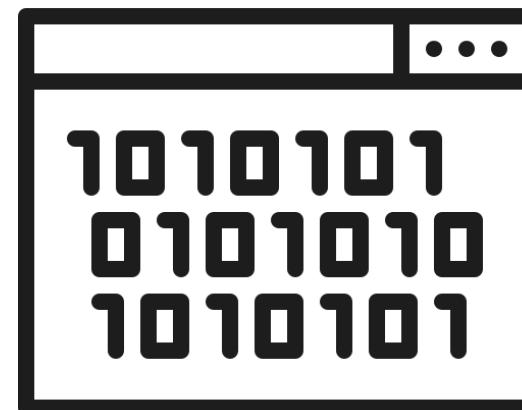
Toast

Internet  
Attack  
Vector

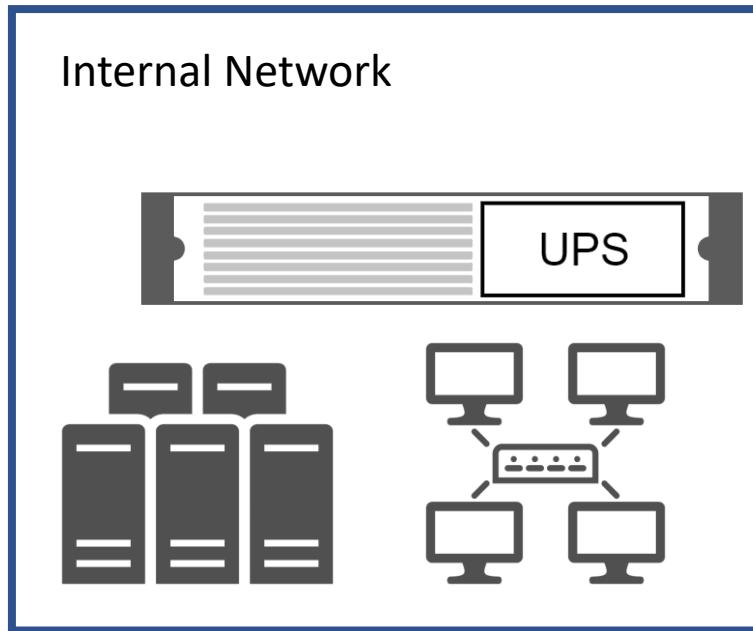
Remote  
Code  
Execution

Power  
Tampering

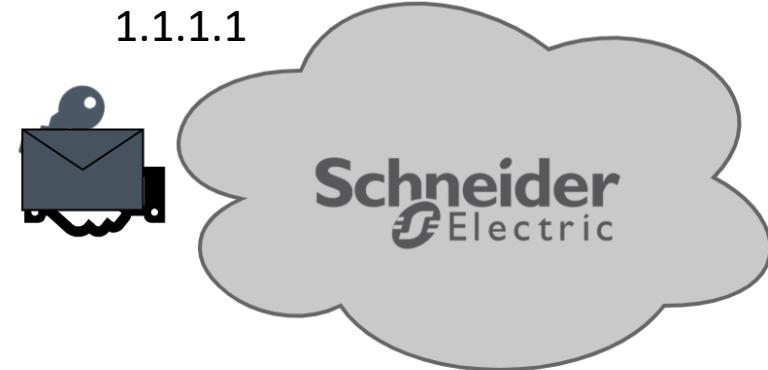
# Research Milestones



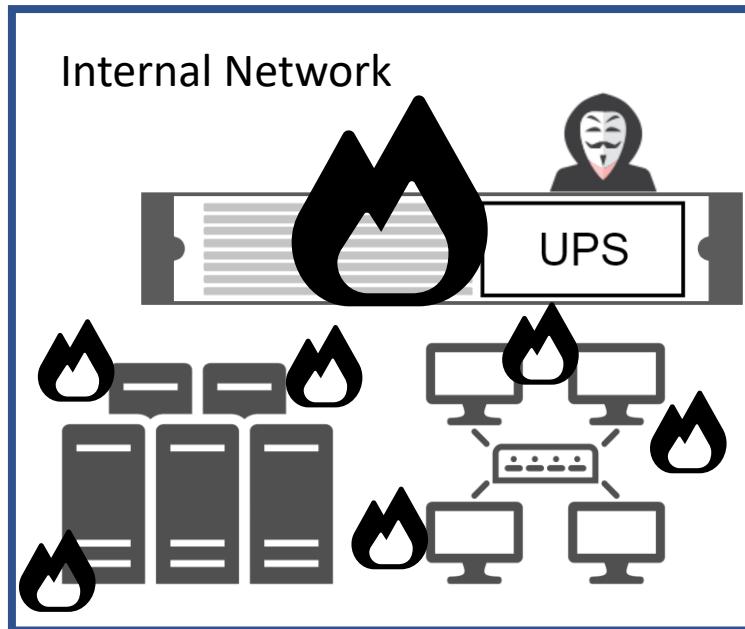
# Recap - Original Flow



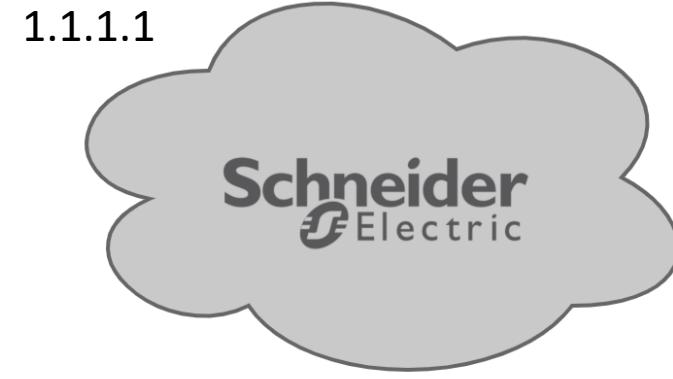
What's APC cloud IP?



# Recap - Attack Scenarios

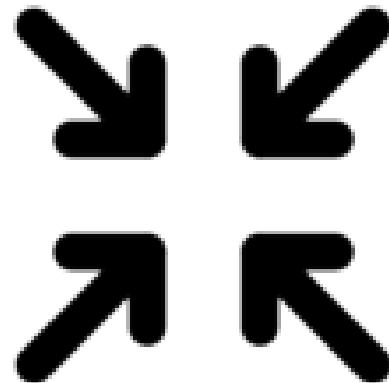


It's APC cloud IP?



# Mitigations

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





# TLStorm

The logo for TLStorm consists of the word "TLStorm" in a large, white, sans-serif font. Above the letter "T", there is a white cloud icon with a yellow lightning bolt striking through it.

Takeaways:

**External libraries could be a weak spot**

**Internet connectivity is an attack vector**

**Cyber physical is mean**



# Questions?

Read more – [armis.com/TLStorm](http://armis.com/TLStorm)

Yuval Sarel - @TheYuvalShow

Gal Levy - @Gal\_Levy92