IoT Security 101:
Deep Dive Into Attack Surfaces & Vulnerabilities

•••

Sushant Mane
smmane_p22@el.vjti.ac.in
https://www.linkedin.com/in/sushantmmane/

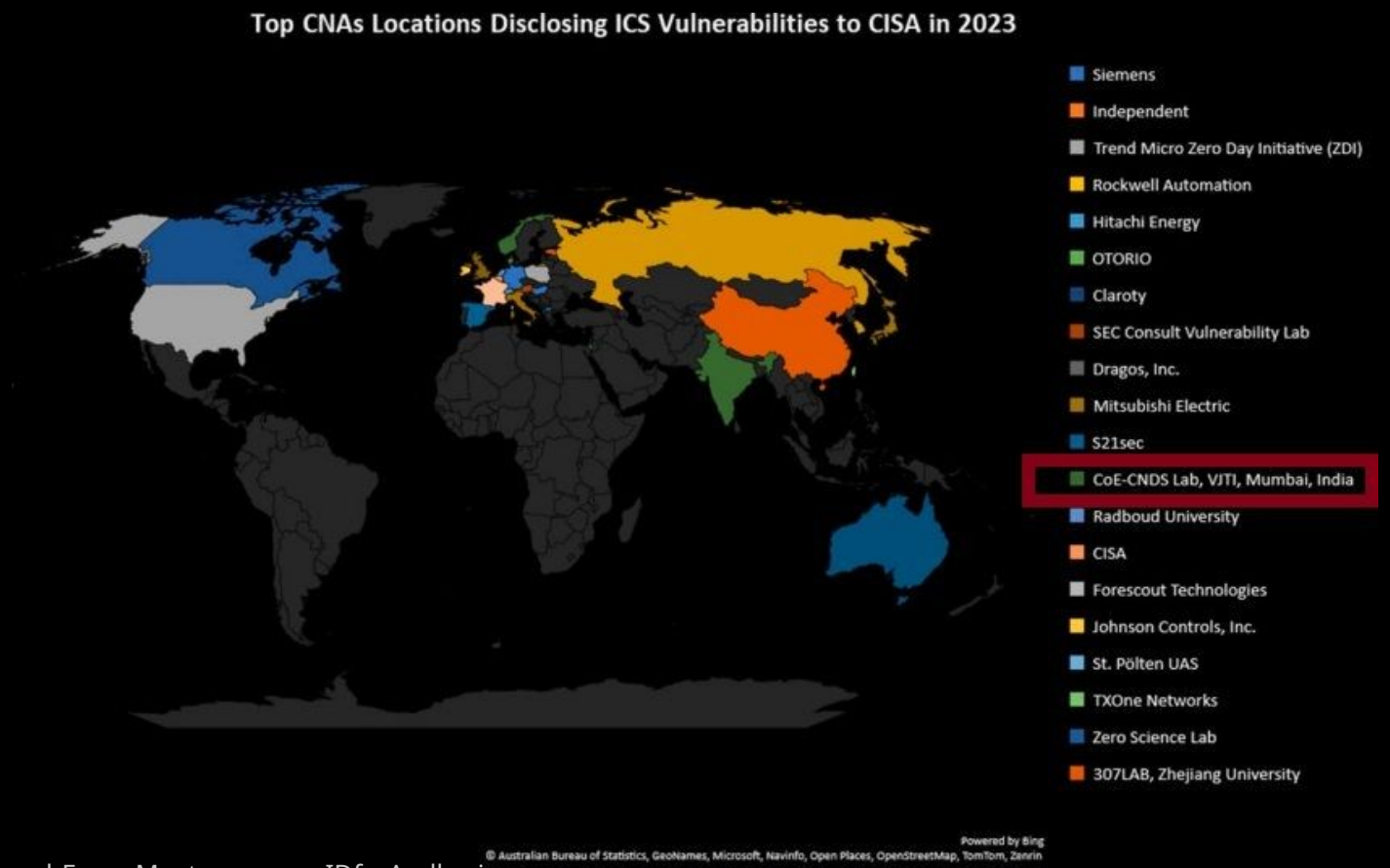
whoami

- Sushant Mane, soon to be Dr. Sushant Mane (Hopefully ;))
- Currently pursuing Ph.D, from VJTI, Mumbai.
- Working in CoE-CNDS, Lab, VJTI, Mumbai.
- Trying to “Make the World a Safer Place!”
- Vulnerability Researcher
- Hands on Experience in-
  - Web Application Pentesting
  - Hardware Hacking
  - SDR Exploitation
  - Side Channel Analysis
  - Reverse Engineering
  - Bug Bounty Hunter
  - Thick Client Pentesting
  - Malware Analysis
  - Hardware Trojan Detection

whoami - Some of my Achievements

- Smart India Hackathon 2023 Winner
- 30+ CVEs from multiple vendors in IoT, OT & IT domain.
  - CVE-2023-0898
  - CVE-2023-2264
  - CVE-2023-2265, ...
- Multiple Hall of Fames.
- Publications -
  - A Review of Drone Communication Protocols:Current Trends and Future Perspectives
  - Exploring Chip-Off Firmware Extraction Techniques and Challenges: Case Studies in Smart Plugs
  - Threat Modeling of Cube Orange Based Unmanned Aerial Vehicle System
- Speaker At -
  - VJTI-TBI: Drone Security
  - The Hacker’s Meetup: IoT Security
  - Rashtriya Raksha University, Kolkata: OT/ICS Security

Cited in the global list of Top ICS cyber security research teams



!!! WARNING !!!

During this session, we present different ways to “attack” IoT devices. This knowledge allows us to make the world a hell or a safer place. We definitely expect you to use this knowledge for the best, which means making the world a better and safer place.

When finding a vulnerability in an IoT device, it must be reported to the respective vendor in an ethical manner.

About Centre of Excellence (CoE) Lab:

- Centre of Excellence (CoE) was established under World Bank initiative of TEQIP (Technical Education Quality Improvement Program)
- Competitive funding from 163 shortlisted proposals across India including NITs.
- Industry support- Siemens, Emerson, L&T, CISCO, Claroty, Schneider
- Theme- CPS

Sushant Mane

SIEMENS - Smart Grid Cyber Security

2024 May Mumbai BreachForce Meetup IDfy, Andheri,

2024 May
Mumbai

BreachForce Meetup

IDfy, Andheri,


Sushant Mane
2024 May Mumbai
BreachForce Meetup
IDfy, Andheri,


HackRF One
HACKERS
ASUS
VOSTRO
Galaxy S23
2024 May
BreachForce Meetup

Agenda

- Introduction
- IoT Attack Surface
  - Device Level
    - Firmware
    - Hardware
    - Side Channel
  - Wireless Communication
  - Supply Chain
  - Web Interface
  - Network Communication

Agenda

- Introduction
- IoT Attack Surface
  - Device Level
    - Firmware
    - Hardware
    - Side Channel
  - Wireless Communication
  - Supply Chain
  - Web Interface
  - Network Communication

Introduction

- Internet of Things (IoT) or Internet of *Things to be hacked* or IoTS
- Most of the smaller IoT devices suffer from **limitations** that affect **security:**
  - Limited Memory
  - Processing Capacity
  - Power requirements -> This becomes direct threat to security controls such as **Encryption.**

Encryption - Deemed too e nd therefore left out of the design altoge

A short list of connected *things:*

- **Smart Things:** Smart homes, appliances, offices, cities, grids, etc.
- **Wearable Items:** Biomedical Wearables, fitness bands.
- **Automotive:** Car sensors, autonomous driving, telemetry, etc.
- **Energy Industry:** Power generation, storage, etc.

It’s a never ending list.

In 2008, the number of connected devices surpassed the number of humans on the planet at 8 billion.

According to Cisco’s report, the number of IoT devices exceed 50 billion by 2020.

A short list of connected *things:*

- **Smart Things:** Smart homes, appliances, offices, cities, grids, etc.
- **Wearable Items:** Biomedical Wearables, fitness bands.
- **Automotive:** Car sensors, autonomous driving, telemetry, etc.
- **Energy Industry:** Power generation, storage, etc.

It’s a never ending list.

In 2008, the number of connected devices surpassed the number of humans on the planet at 8 billion.

According to Cisco’s report, the number of IoT devices exceed 50 billion by 2020.

Just imagine, if misconfigured, poorly designed or just connected to the internet with defau[illegible]als... What will happen?

A short list of

- **Smart Thi**
- **Wearable**
- **Automoti**
- **Energy In**

It’s a never en

In 2008, the nu
humans on th

According to G on by 2020.

Just imagine, i the internet with

Security Concerns

- Traditionally → Confidentiality, Integrity & Availability.
- When it comes to connected devices, the order is often **reversed**.

- Eg. Embedded Medical Device that is connected via Bluetooth to the User's phone and thereby the internet. The primary concern in Availability, Integrity & then Confidentiality.

- What's the point of the device being used if it cannot be reached or trusted?

Traditional View of CIA

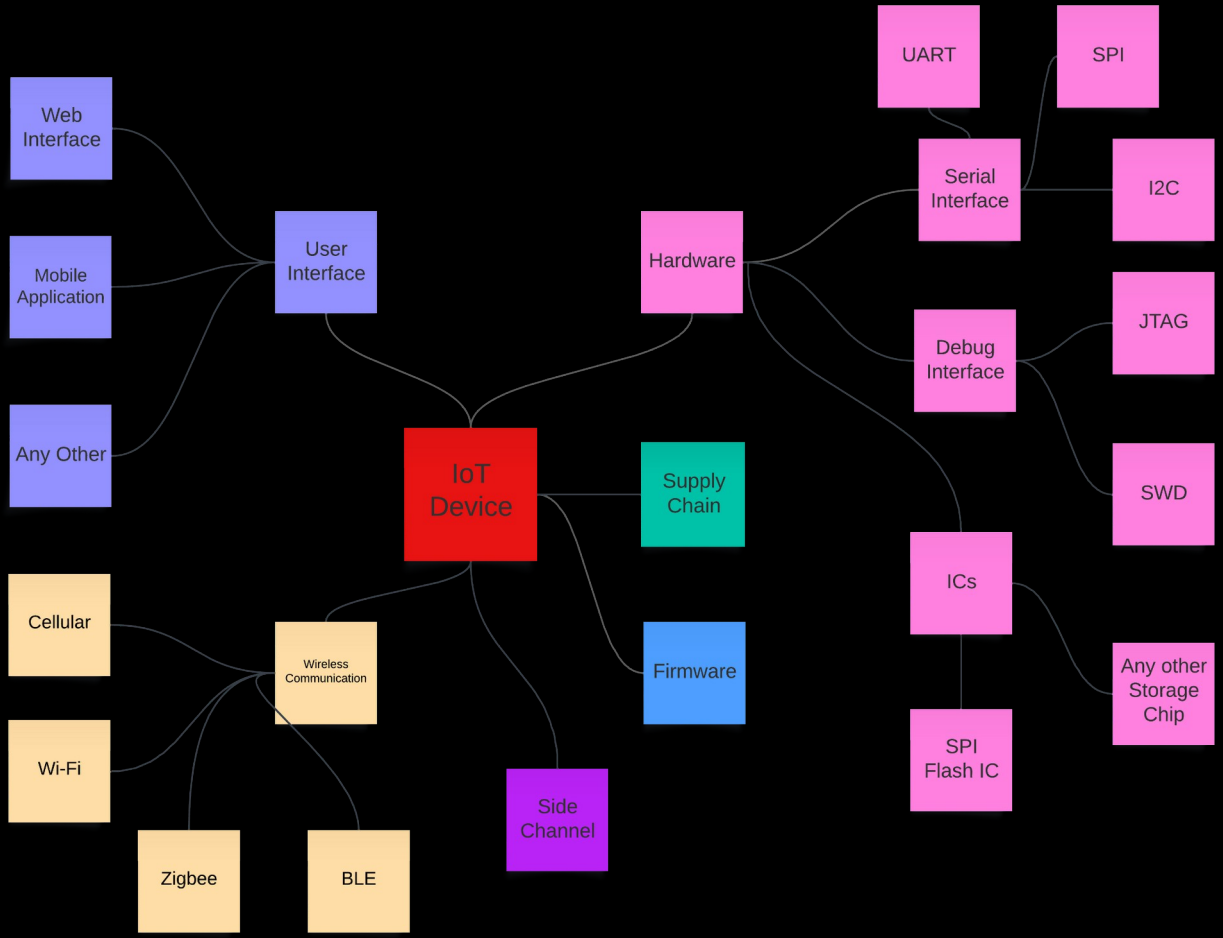
Security Concerns

- Limited resources and power constraints, often preventing security controls such as **Encryption.**
- **“Out of sight, out of mind”** situation. Eg. Routers.

- Protocols have limitations, including no encryption or no authentication, etc.

IoT Attack Surface

Sushant Mane



Hardware - Serial Interfaces

- A serial interface refers to a communication interface that transmits data as a sequence of bits sent one after the other over a single wire or channel.
- Serial interfaces are used for various purposes, such as connecting devices, transmitting data between computers and peripherals, and for communication between microcontrollers and sensors.
- Several serial protocols are used in embedded systems like:
  - Universal Asynchronous Receiver Transmitter (UART)
  - Serial Peripheral Interface (SPI)
  - Inter-Integrated Circuit (I2C)

We'll only discuss about **UART**.

UART Exploitation

Steps:

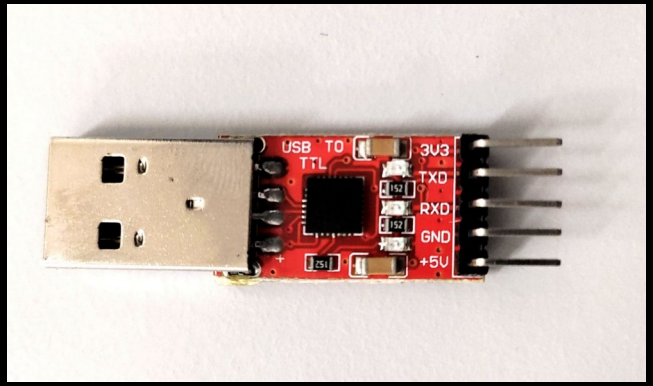
1. Identify/Locate UART headers or pins or pads by inspecting the PCB.
2. Identify GND and VCC pins using multimeter or seeing the datasheet.
3. Identify Rx and Tx pins using multimeter or datasheet or JTAGULATOR.
4. Connect the identified pins to your JTAGULATOR or USB2TTL
5. Identify the baudrate.
6. Get the interactive serial console.

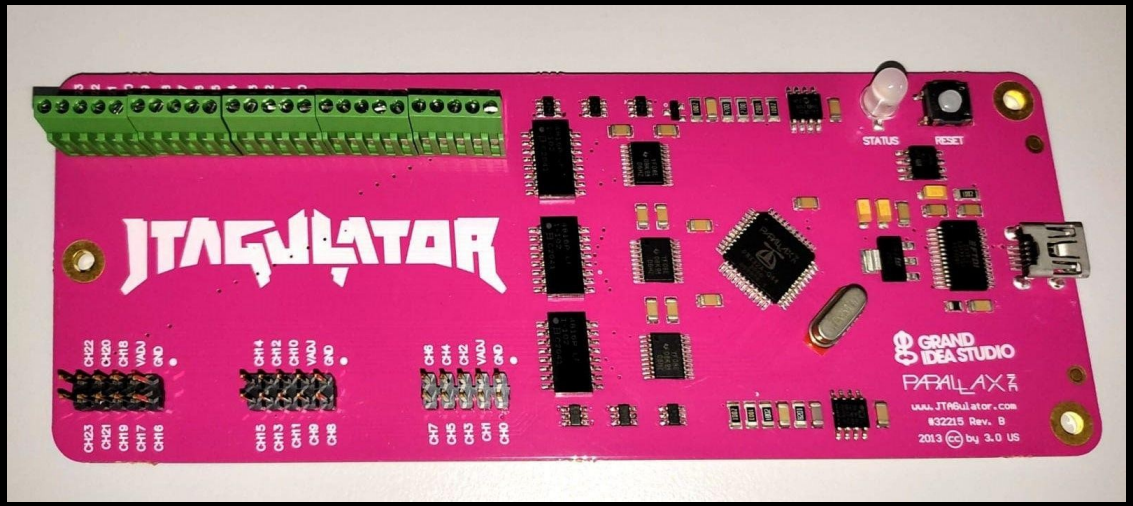
Findings:

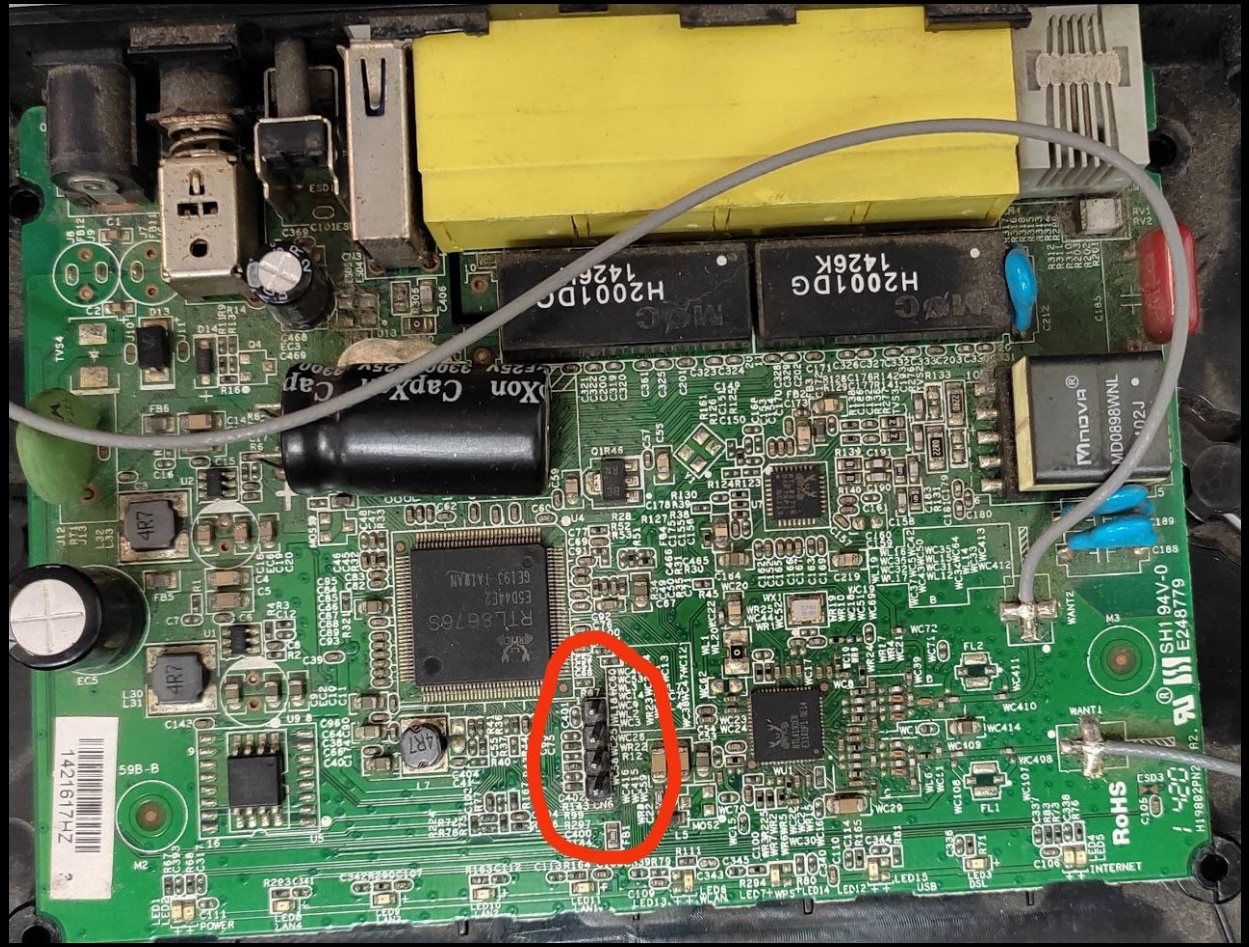
UART Port Exposing Serial Logs
Getting Root Shell Access

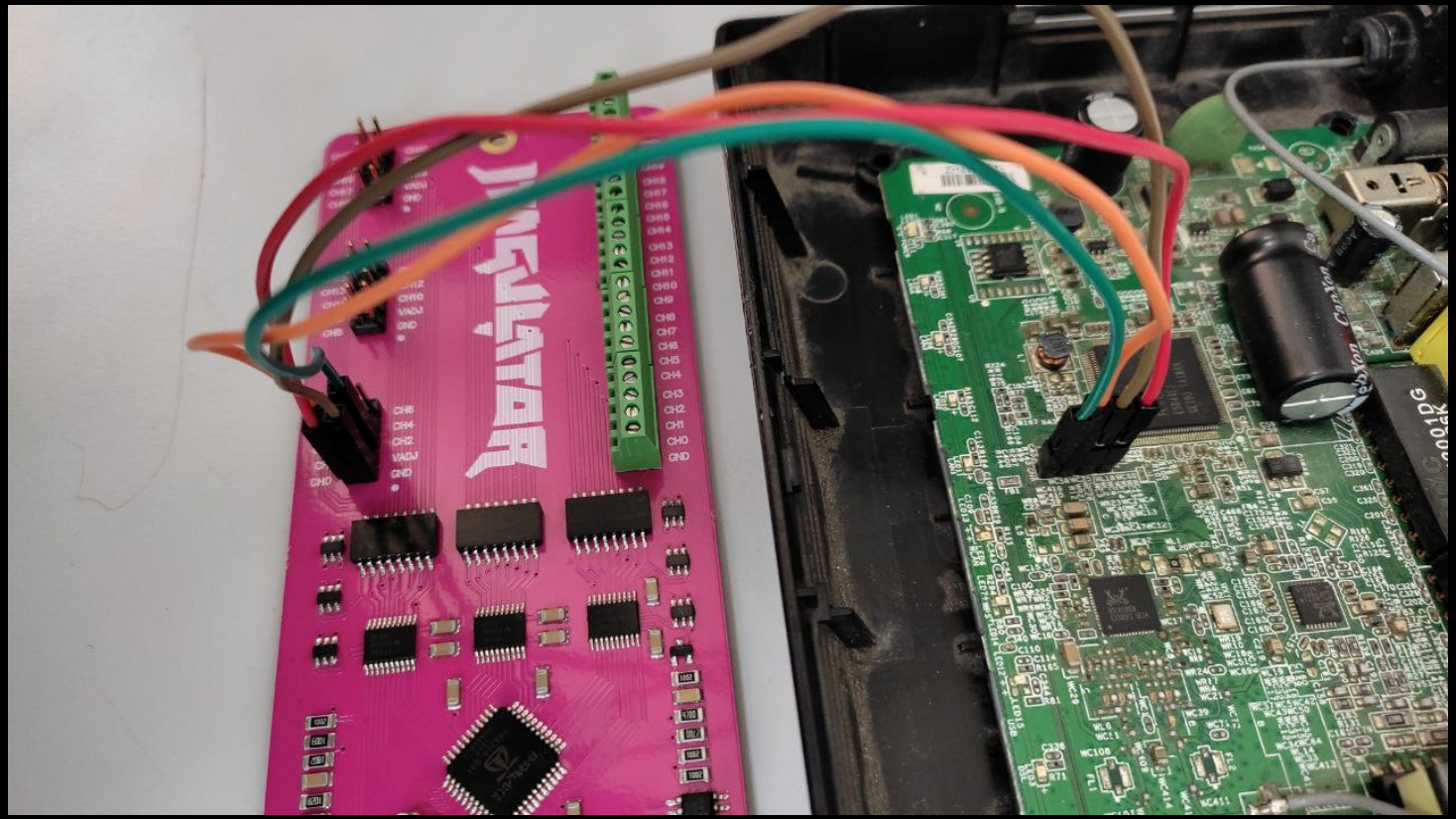
Tools Required

Suchant Mane






H2001DG
1426K
RTL8676S
SH1194V-0
E248779
RoHS
INTERNET
59B-B
1421617HZ


CH6
CH4
CH2
VADJ
GND
CH0
CH1
CH3
CH5
CH7
GND

```
┌──(kali㉿kali)-[~]
└─$ sudo picocom /dev/ttyUSB0 -b 115200
picocom v3.1

port is        : /dev/ttyUSB0
flowcontrol    : none
baudrate is    : 115200
parity is      : none
databits are   : 8
stopbits are   : 1
escape is      : C-a
local echo is  : no
noinit is      : no
noreset is     : no
hangup is      : no
nolock is      : no
send_cmd is    : sz -vv
receive_cmd is : rz -vv -E
imap is        :
omap is        :
emap is        : crcrlf,delbs,
logfile is     : none
initstring     : none
exit_after is  : not set
exit is        : no

Type [C-a] [C-h] to see available commands
Terminal ready
```

```
:h
JTAG Commands:
I   Identify JTAG pinout (IDCODE Scan)
B   Identify JTAG pinout (BYPASS Scan)
D   Get Device ID(s)
T   Test BYPASS (TDI to TDO)

UART Commands:
U   Identify UART pinout
P   UART passthrough

General Commands:
V   Set target I/O voltage (1.2V to 3.3V)
R   Read all channels (input)
W   Write all channels (output)
J   Display version information
H   Display available commands
```

```
:V
Current target I/O voltage: Undefined
Enter new target I/O voltage (1.2 - 3.3, 0 for off): 3.3
New target I/O voltage set: 3.3
Ensure VADJ is NOT connected to target!
```

```
:u
Enter text string to output (prefix with \x for hex) [CR]:
Enter number of channels to use (2 - 24): 3
Ensure connections are on CH2..CH0.
Possible permutations: 6
Press spacebar to begin (any other key to abort)...
JTAGulating! Press any key to abort......
```

```
TXD: 1
RXD: 2
Baud: 38400
Data: <.............. [ 3C 87 CE 19 06 FE 98 06 BC 0E E3 0D F8 8D C3 87 ]

TXD: 1
RXD: 2
Baud: 57600
Data: .JAJ...T....(7.. [ B1 4A 41 4A 94 B3 EA 54 B2 1B 94 BB 28 37 BB EA ]

TXD: 1
RXD: 2
Baud: 76800
Data: . [ FF ]

TXD: 1
RXD: 2
Baud: 115200
Data: ..-sh: ......... [ 0D 0A 2D 73 68 3A 20 C6 F9 F9 FD 80 E0 FE FF 80 ]
```

```
UART scan complete!
:p
Enter new TXD pin [0]: 1
Enter new RXD pin [0]: 2
Enter new baud rate [0]: 115200
Enable local echo? [y/N]:
Entering UART passthrough! Press Ctrl-X to abort...
```

Sushant Mane

```
usbcore: registered new interface driver 3g_modem
[USB MODEM SERIAL modem_usb_id_proc_write:211] Do attach...

/ $ ls
bin      etc      linuxrc  pool     root     sys      usr      wps
dev      lib      mnt      proc     sbin     tmp      var
```

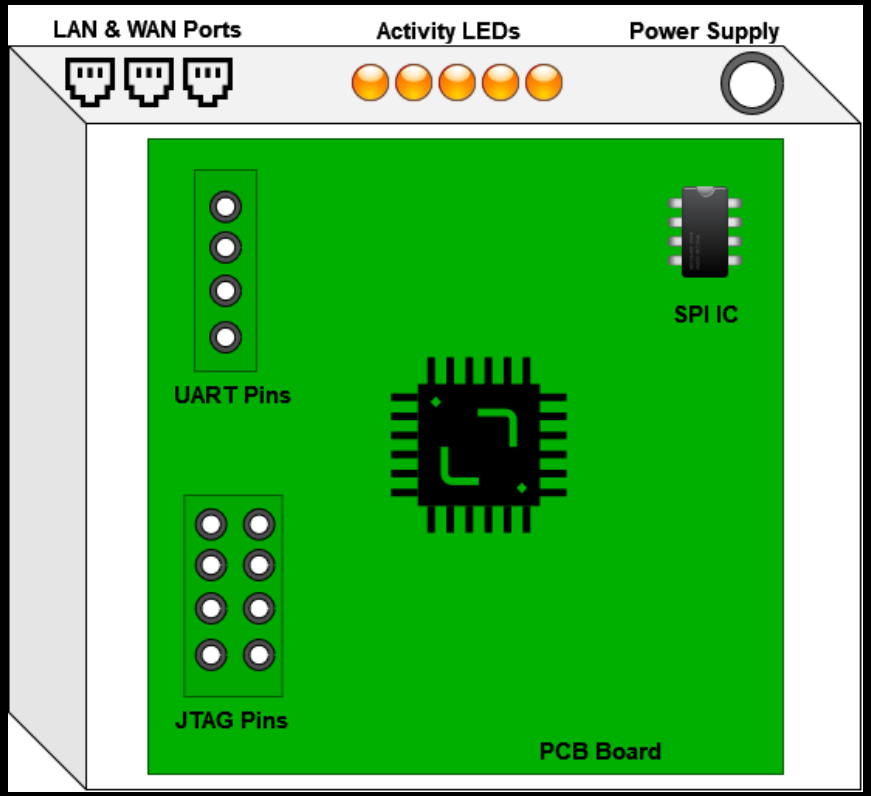
For more information- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=UART

Search Results

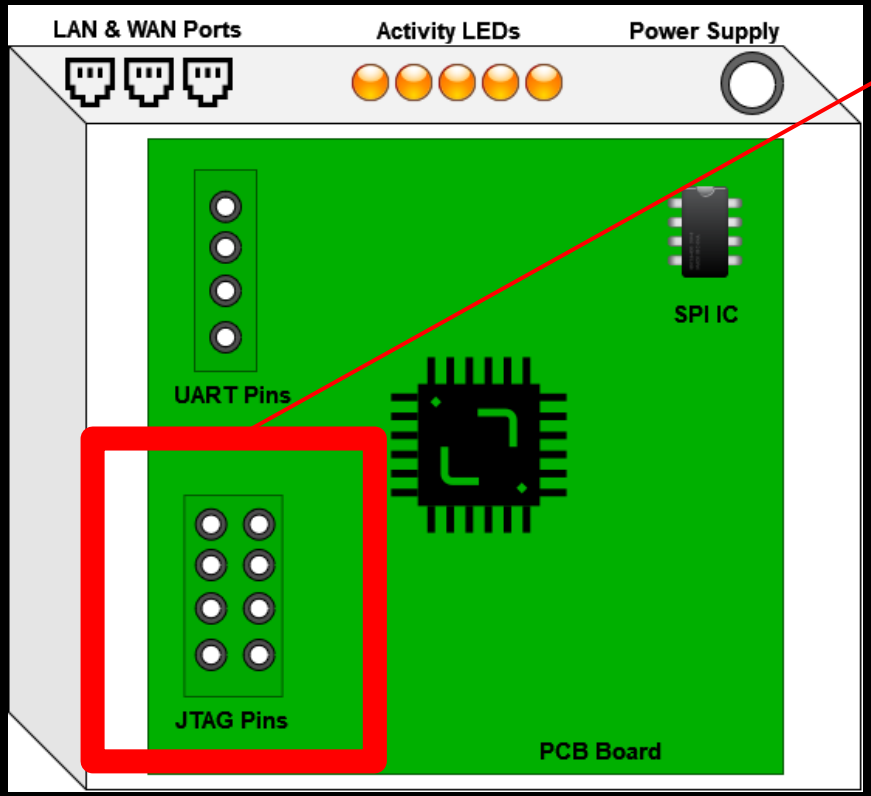
There are **48** CVE Records that match your search.

Name	Description
CVE-2023-36160	An issue was discovered in Qubo Smart Plug10A version HSP02_01_01_14_SYSTEM-10 A, allows local attackers to gain sensitive information and other unspecified impact via UART console.
CVE-2023-34724	An issue was discovered in TECHView LA5570 Wireless Gateway 1.0.19_T53, allows physical attackers to gain escalated privileges via the UART interface.
CVE-2023-33921	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05), CP-8050 MASTER MODULE (All versions < CPCI85 V05). The affected devices contain an exposed UART console login interface. An attacker with direct physical access could try to bruteforce or crack the root password to login to the device.
CVE-2023-33920	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05), CP-8050 MASTER MODULE (All versions < CPCI85 V05). The affected devices contain the hash of the root password in a hard-coded form, which could be exploited for UART console login to the device. An attacker with direct physical access could exploit this vulnerability.
CVE-2023-31083	An issue was discovered in drivers/bluetooth/hci_ldisc.c in the Linux kernel 6.2. In hci_uart_tty_ioctl, there is a race condition between HCIUARTSETPROTO and HCIUARTGETPROTO. HCI_UART_PROTO_SET is set before hu->proto is set. A NULL pointer dereference may occur.
CVE-2023-30354	Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 does not defend against physical access to U-Boot via the UART: the Wi-Fi password is shown, and the hardcoded boot password can be inserted for console access.
CVE-2023-30351	Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 was discovered to contain a hard-coded default password for root which is stored using weak encryption. This vulnerability allows attackers to connect to the TELNET service (or UART) by using the exposed credentials.
CVE-2022-45553	An issue discovered in Shenzhen Zhibotong Electronics WBT WE1626 Router v 21.06.18 allows attacker to execute arbitrary commands via serial connection to the UART port.
CVE-2022-43096	Mediatrix 4102 before v48.5.2718 allows local attackers to gain root access via the UART port.

Debugging Interfaces - JTAG



Debugging Interfaces - JTAG



For security researchers, the following capabilities are commonly used:

- Reading and Writing Flash (Firmware modification or extraction)
- Modifying the program flow to bypass functionality to gain restricted access.

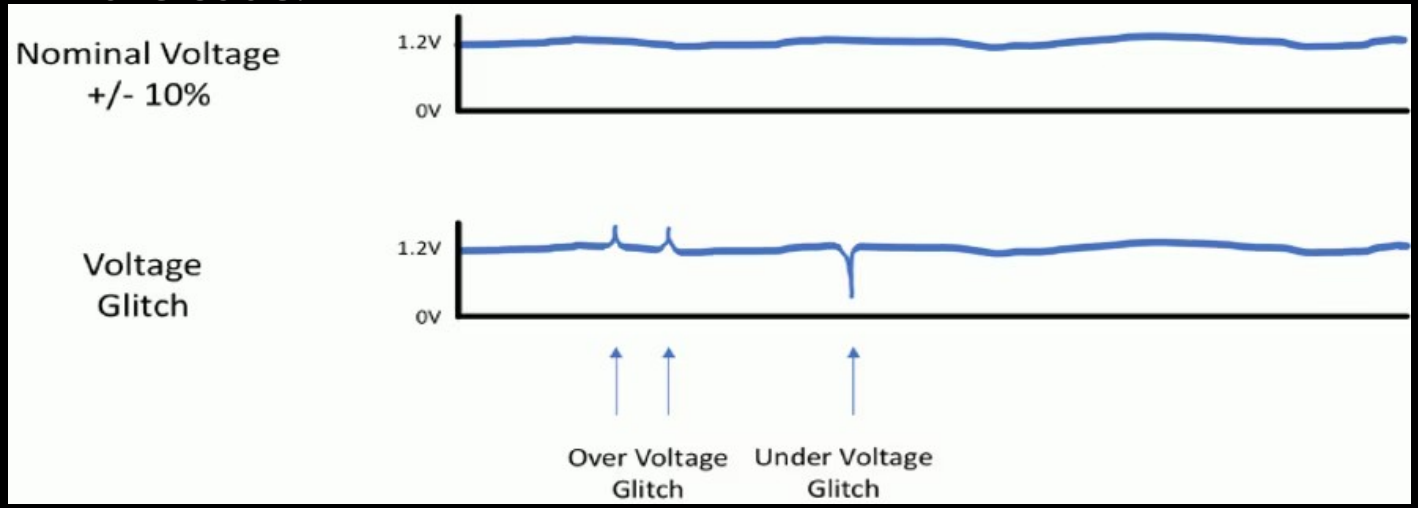
RDP Bypass!!!

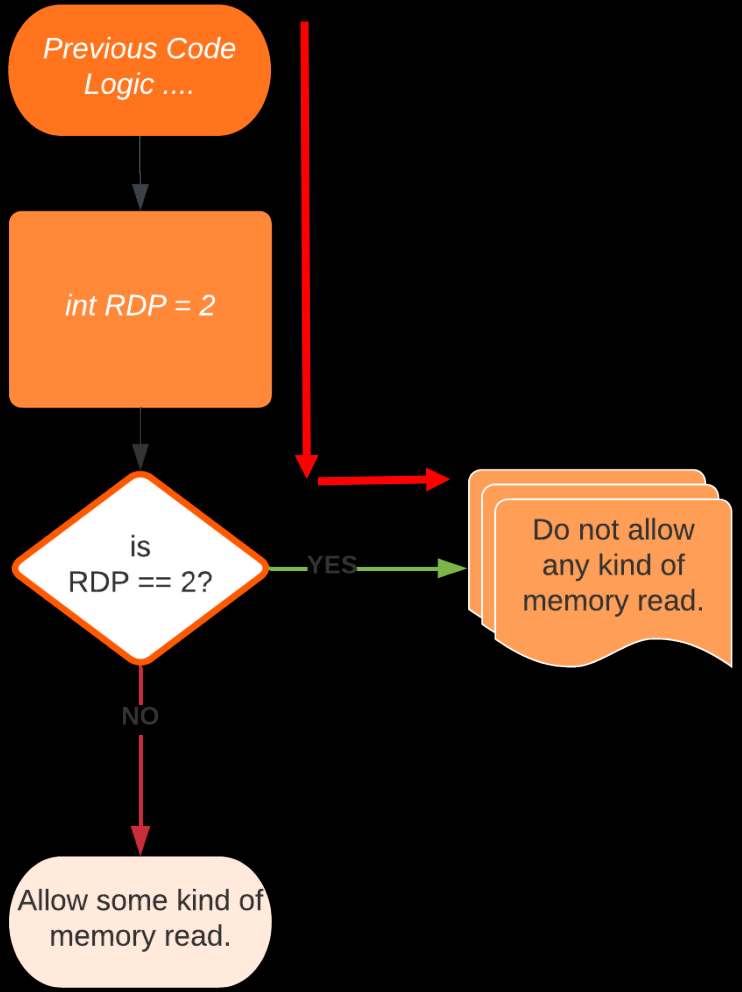
Side Channel Analysis/Attacks

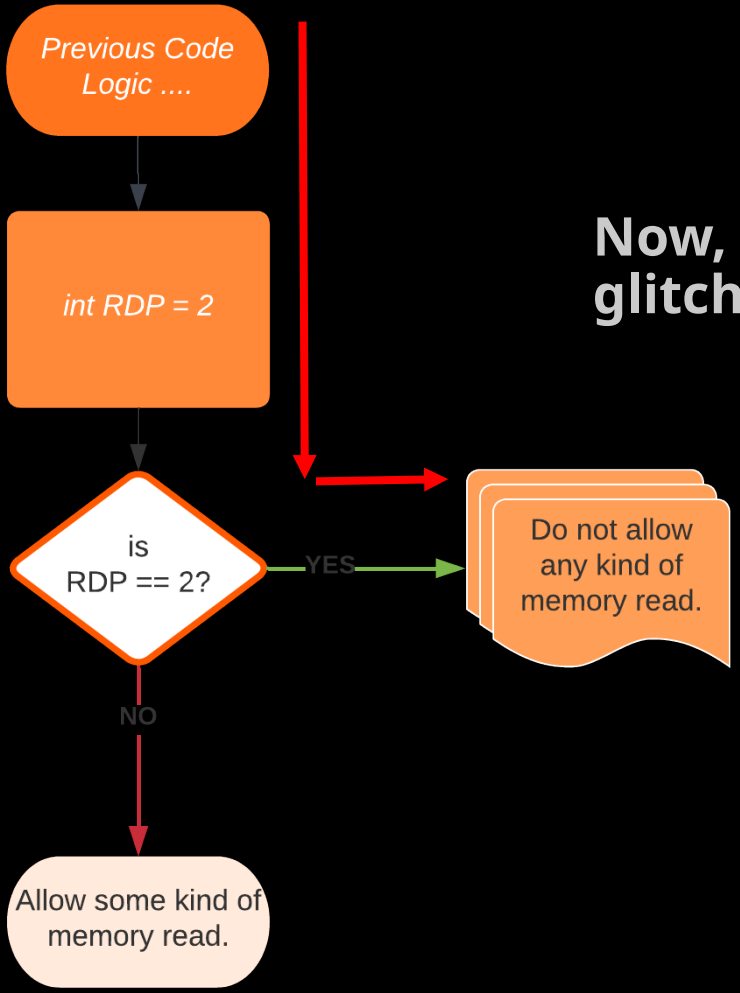
- Side-channel analysis (SCA) refers to a class of attacks in cryptography and computer security that focuses on exploiting information unintentionally leaked by a cryptographic device or system through various "side channels."
- These side channels are not part of the primary communication channel, but they inadvertently leak information about the system's internal operations. Side-channel attacks can be used to extract secret keys, cryptographic algorithms, or other sensitive information.
- Power Analysis, Electromagnetic Analysis (EMA), Timing Analysis, Fault Injection Attacks, etc.

Voltage Glitching

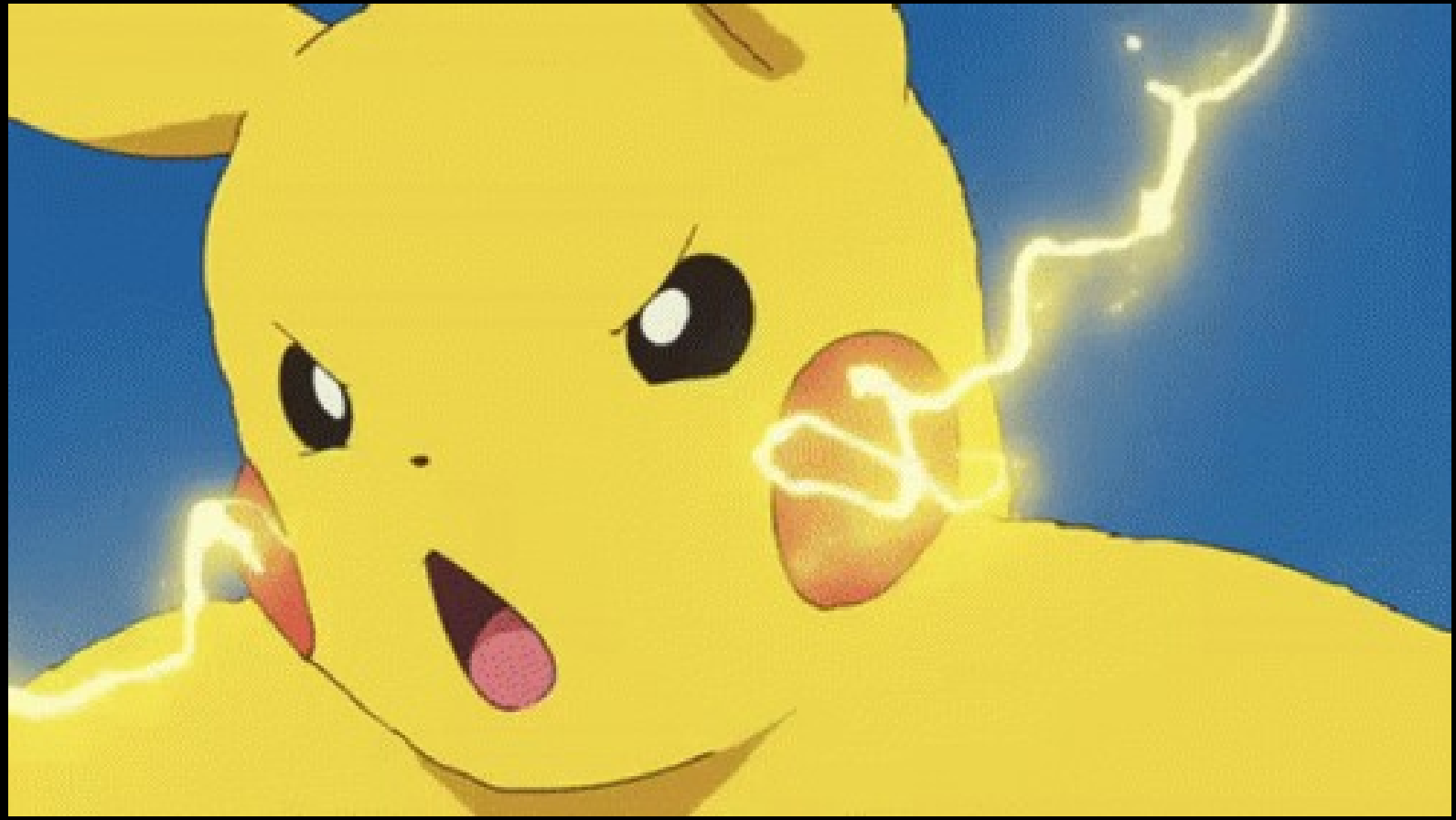
Voltage fault injection is a powerful active side channel attack that modifies the execution-flow of a device by creating disturbances on the power supply line. The attack typically aims at skipping security checks or generating side-channels that gradually leak sensitive data, including the firmware code.

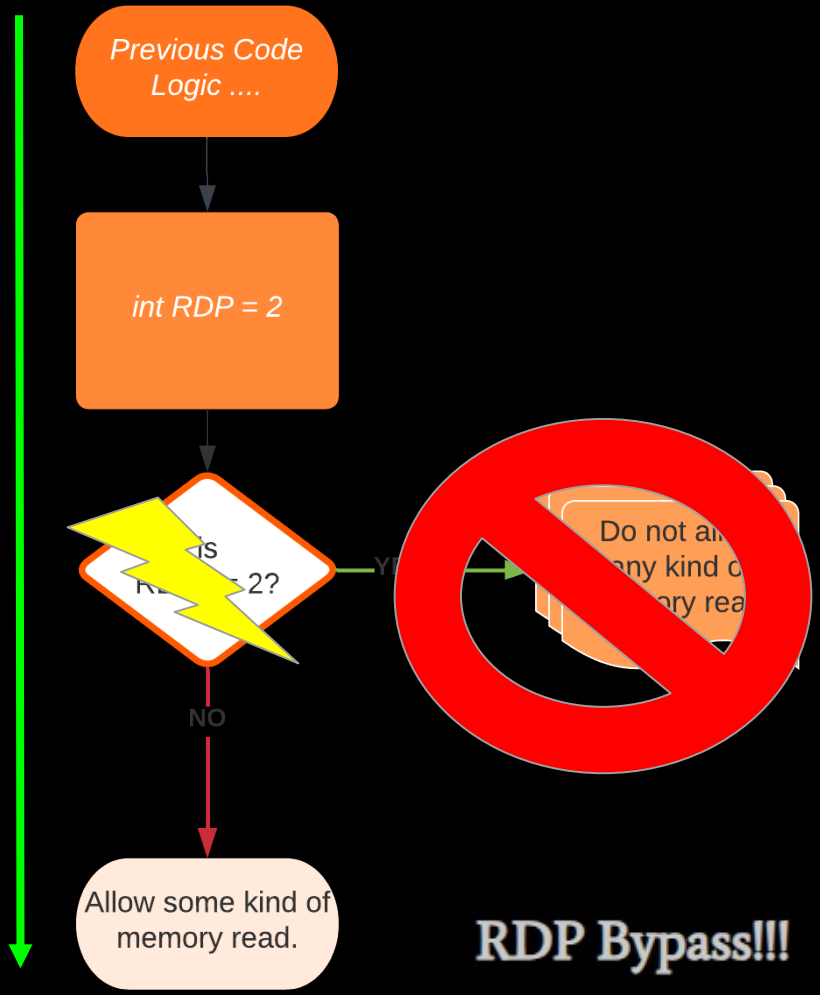



Previous Code Logic ....
int RDP = 2
is RDP == 2?
YES
Do not allow any kind of memory read.
NO
Allow some kind of memory read.



Now, let's do a voltage glitch!




Previous Code Logic ....
int RDP = 2
NO
Allow some kind of memory read.

RDP Bypass!!!

Firmware

Firmware can be obtained from the vendor’s website, dumped from the target device or captured during OTA updates.

Things to look in the firmware:

- Hardcoded Credentials
- Locate Executable Files
- Look for an executable file’s version for checking against any known vulnerabilities.
- Inside the executables or libraries look for unsafe functions using Disassembler like Ghidra, IDA or Binary Ninja.
- Look for HTML, JavaScript, CGI and config files.

Sushant
Mane

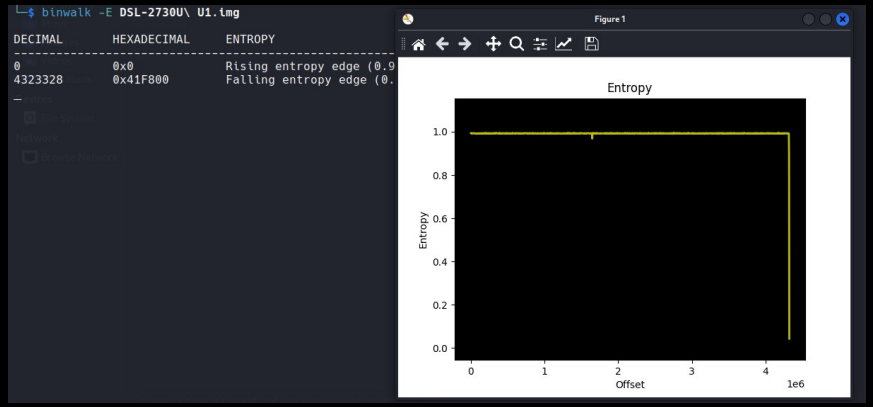
Firmware Analysis

- Using **binwalk** to study about the compression method, Filesystem, Endianness, etc.

```
└─$ binwalk DSL-2730U\ U1.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 5200744 bytes
1649920       0x192D00        Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2672919 bytes, 1106 inodes, blocksize: 524288 bytes, created: 2014-09-30 04:17:08
```

- Checking **Entropy**,

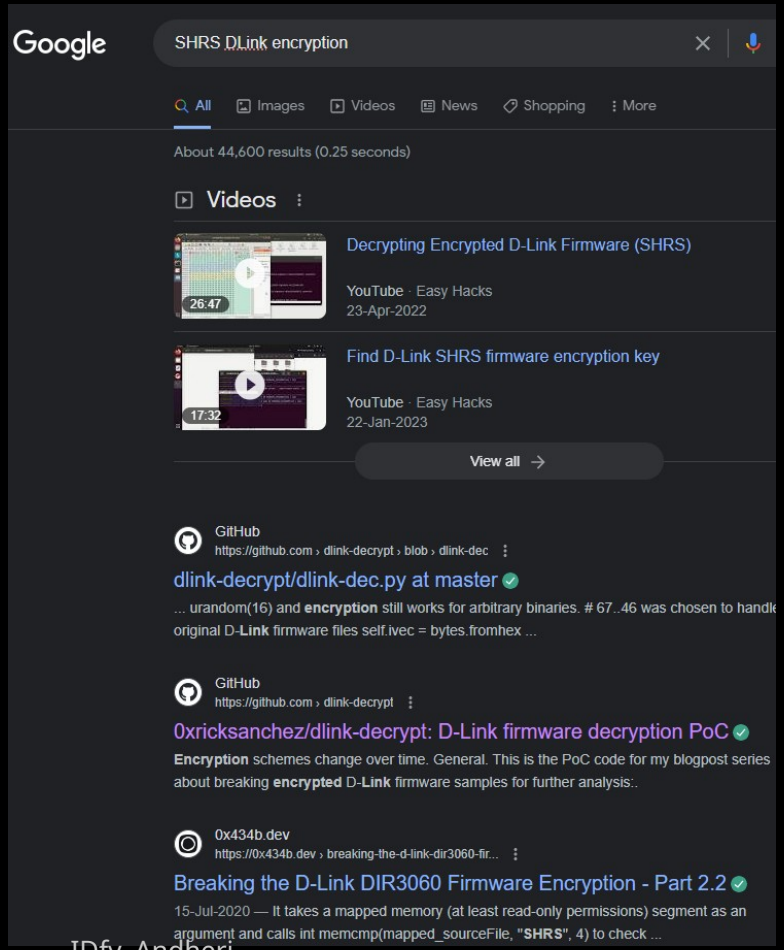


- Extracting the firmware, “binwalk -e firmware.ext”, we can see a new folder created in the same directory. The folder contains the File System.

- But what if the firmware is **Encrypted?** Binwalk is not working on that and Entropy shows that it is encrypted. Then.....

- Using any hex editor, check the magic number or the first 4 bytes of the binary. It may have the encryption type used, Google about it to get more details.

- Eg. First 4 bytes- “SHRS”.



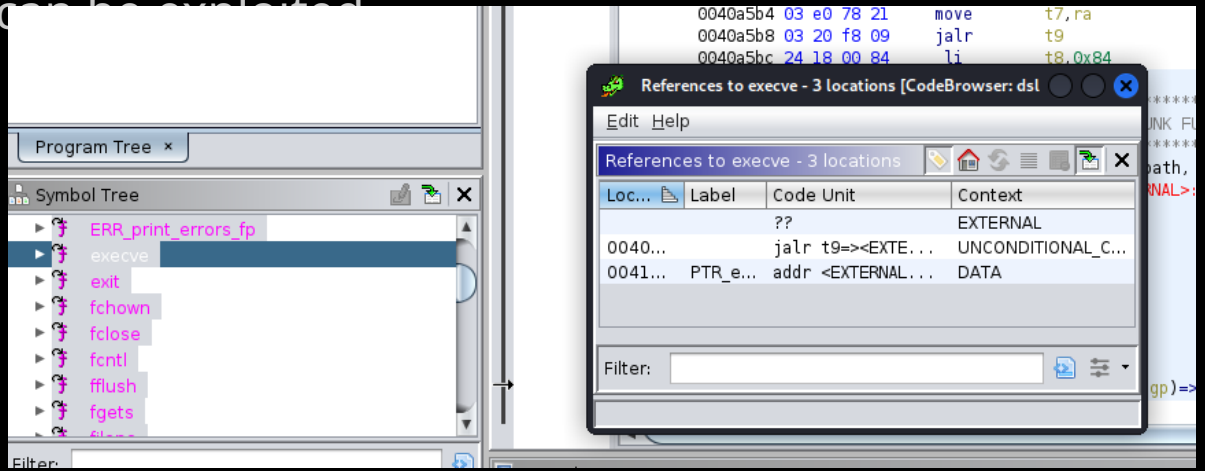
- Once, extracted the firmware, look for squashfs-root (in our case)

```
└─$ ls squashfs-root
bin  dev  etc  lib  linuxrc  mnt  pool  proc  root  sbin  sys  tmp  usr  var  wps
```

- Let's find and analyse some binaries in Ghidra,

```
└─$ ls
chat  dhcp6c  dhcp6s  dproxy  dropbear  inetd  ip  iwconfig  iwcontrol  iwlist  iwpriv  mini_httpd  mini_upnpd  pppd  radvd  radvdump  tc  telnetd
```

- In the Symbol Tree, we can see Imported and Exported Functions. Look for unsafe functions, check the cross references and see if they can be exploited



Wireless Communication - SDR Exploitation

Software-defined radio (SDR) is a versatile technology that allows attackers to intercept, decode, and manipulate wireless signals, making it a potential threat to IoT wireless communication.

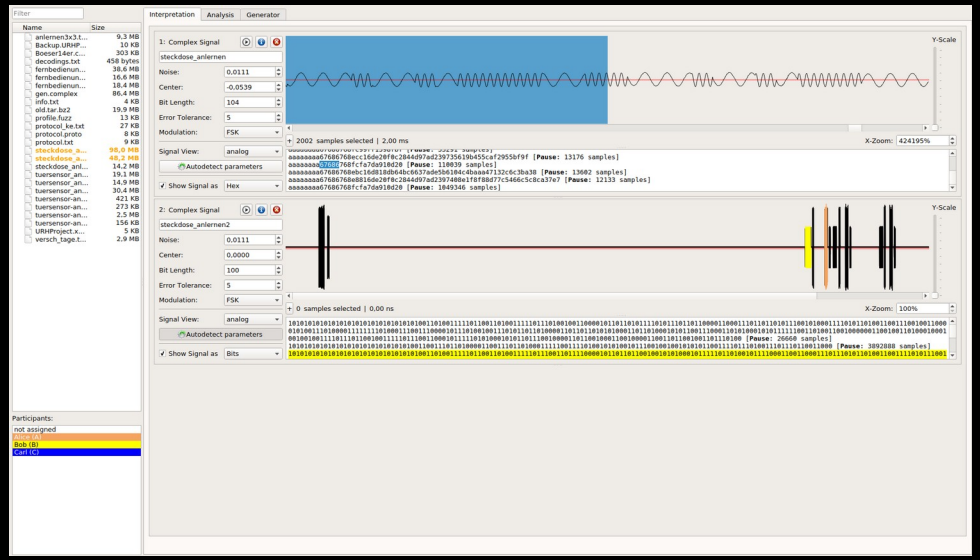
The general process followed for SDR Exploitation is SCRAPE, which stands for:

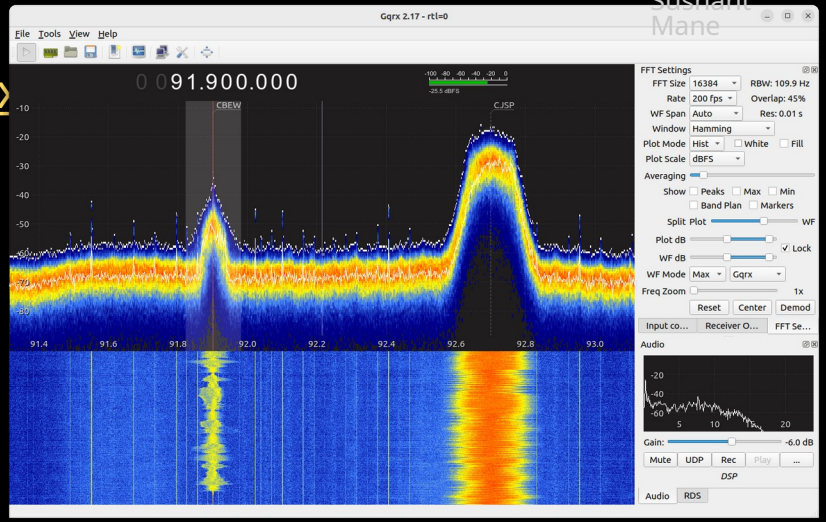
- S - Search
- C - Capture
- R - Replay
- A - Analyze
- P - Preview
- E - Execute

Tools Required-

Sushant Mane

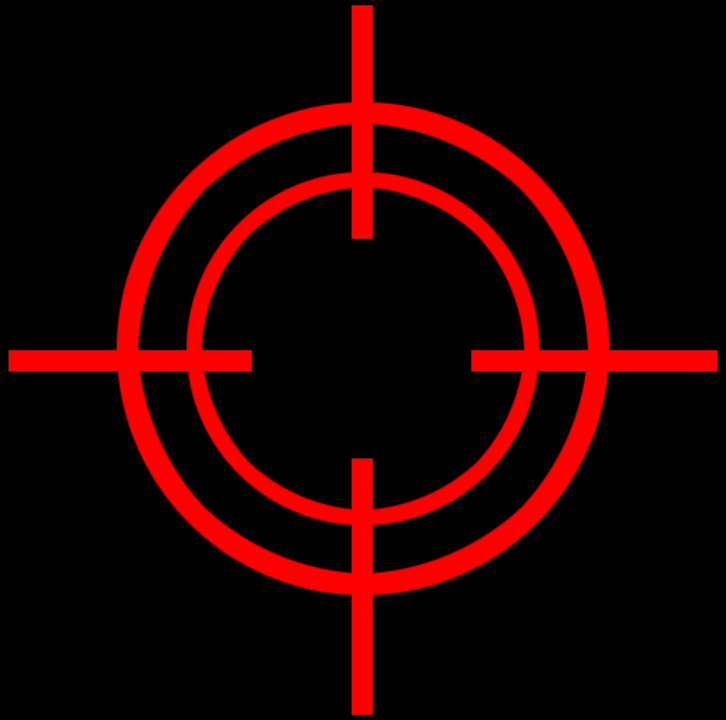
1. **Gqrx** → For receiving the signal. https://gqrx
2. **Universal Radio Hacker**





3. 

HackRF One or Any other SDR.....



Sushant Mane

2024 May Mumbai

BreachForce Meetup

IDfy, Andheri,

Sushant
Mane

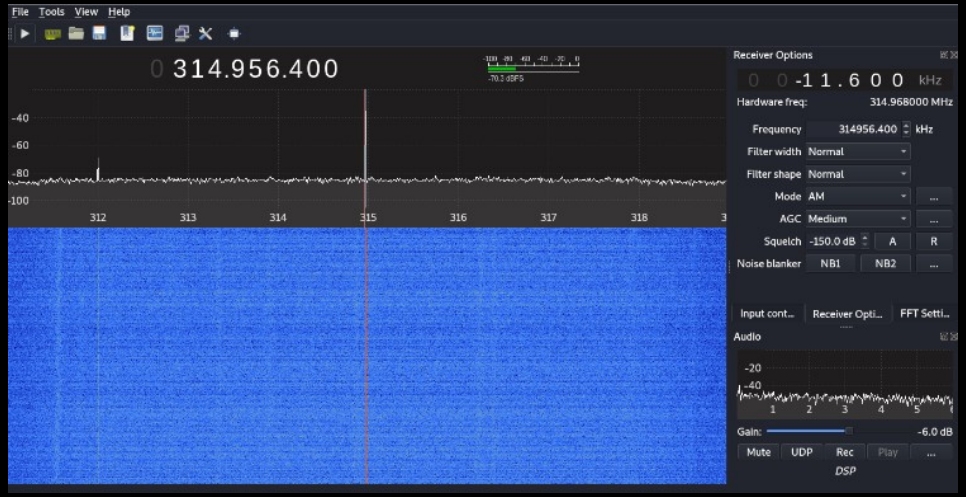
Wireless Bell

Capture & Replay Attack

Sushant Mane

Capturing The Signal

- Find the operating frequency of our wireless
- Rough Value: 315MHz
- Connect HackRF and run gqrx.
- Configuration.....
- Keep the frequency as 315MHz and START.

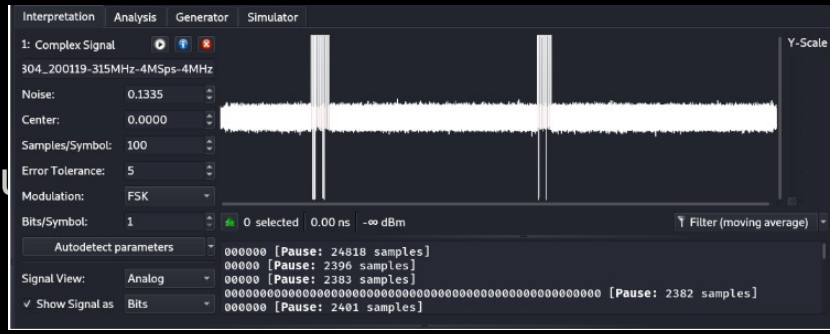


Record & Transmit

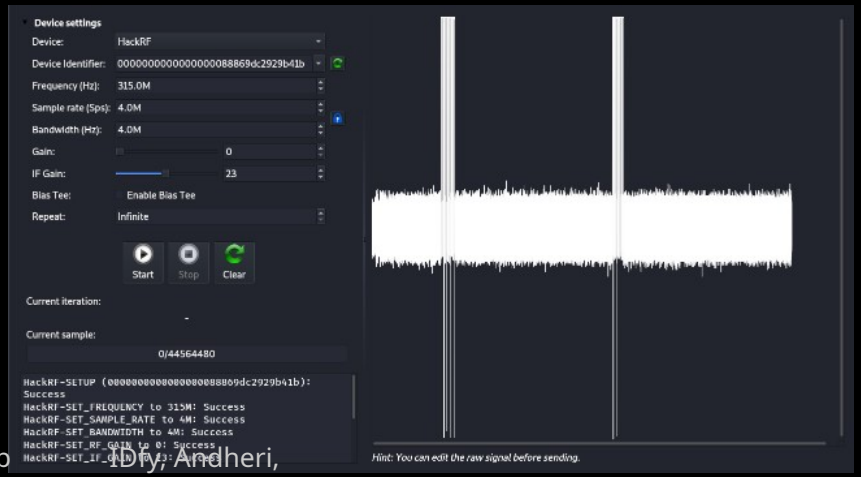
Sushant Mane

Tool- URH.

- Set the frequency as seen in gqrx.
- Capture the signal.
- Play with Gain, IF Gain & Baseband Gain valu
- Record the signal.



- Analyze the signal & then replay the signal.



Search Results

There are **259** CVE Records that match your search.

Name	Description
CVE-2023-4299	Digi RealPort Protocol is vulnerable to a replay attack that may allow an attacker to bypass authentication to access connected equipment.
CVE-2023-42138	Out-of-bounds read vulnerability exists in KV STUDIO Ver. 11.62 and earlier and KV REPLAY VIEWER Ver. 2.62 and earlier. If this vulnerability is exploited, information may be disclosed or arbitrary code may be executed by having a user of KV STUDIO PLAYER open a specially crafted file.
CVE-2023-39373	A Hyundai model (2017) - CWE-294: Authentication Bypass by Capture-replay.

Search Results

There are **259** CVE Records that match your search.

Name	Description
CVE-2023-4299	Digi RealPort Protocol is vulnerable to a replay attack that may allow an attacker to bypass authentication to access connected equipment.
CVE-2023-42138	Out-of-bounds read vulnerability exists in KV STUDIO Ver. 11.62 and earlier and KV REPLAY VIEWER Ver. 2.62 and earlier. If this vulnerability is exploited, information may be disclosed or arbitrary code may be executed by having a user of KV STUDIO PLAYER open a specially crafted file.
CVE-2023-39373	A Hyundai model (2017) - CWE-294: Authentication Bypass by Capture-replay.

Search Results

There are **259** CVE Records that match your search.

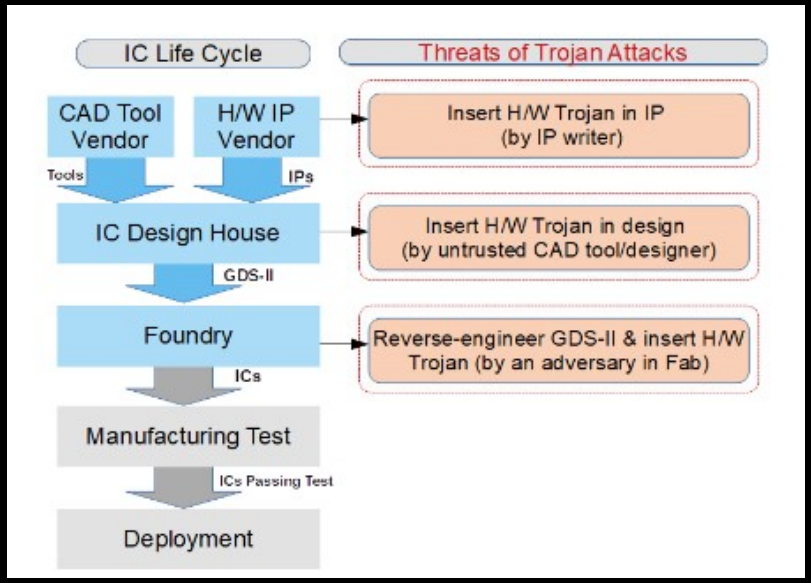
Name	Description
CVE-2023-4299	Digi RealPort Protocol is vulnerable to a replay attack that may allow an attacker to bypass authentication to access connected equipment.
CVE-2023-42138	Out-of-bounds read vulnerability exists in KV STUDIO Ver. 11.62 and earlier and KV REPLAY VIEWER Ver. 2.62 and earlier. If this vulnerability is exploited, information may be disclosed or arbitrary code may be executed by having a user of KV STUDIO PLAYER open a specially crafted file.
CVE-2023-39373	A Hyundai model (2017) - CWE-294: Authentication Bypass by Capture-replay.

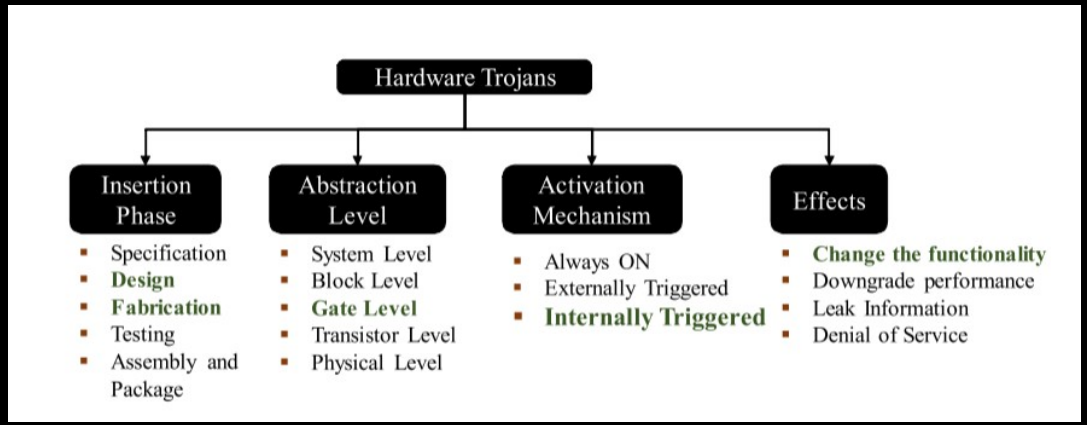
Unveiling the Vulnerabilities: CAN bus Injection Remote Attacks on E-Scooters

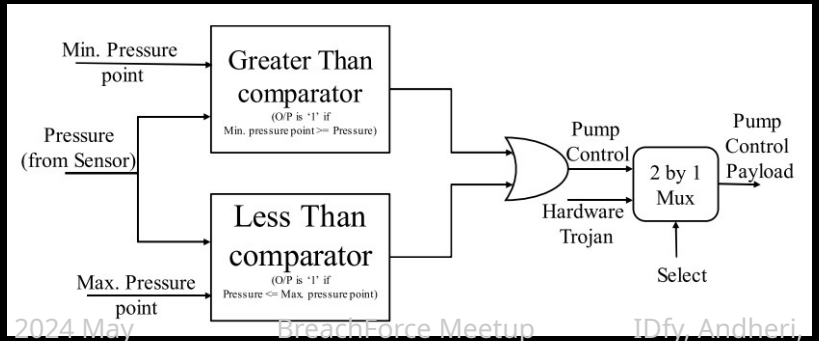
https://www.linkedin.com/feed/update/urn:li:activity:7187541783726174208/

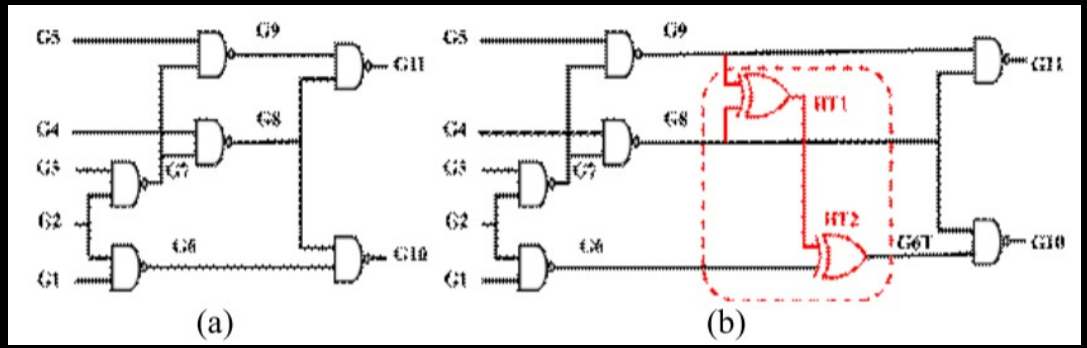
Supply Chain - Hardware Trojan

Sushant Mane









References:

- Study of Hardware Trojans Based Security Vulnerabilities in CPS by K.L, Ranveer K, Nagendra B.G and Thomas M
- Hardware trojan detection based on SCA using power traces and ML by Van-Phuc Hoang

I fear time is running out.....

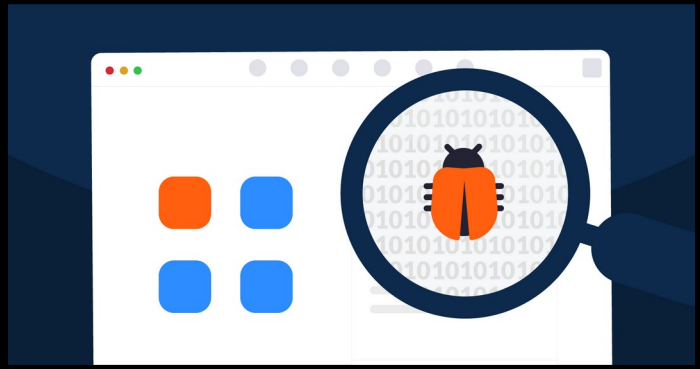
Network Communication

- Using Wireshark perform the packet inspection.
- Look for weak encryptions or plaintext transmission of sensitive information.

Sushant Mane

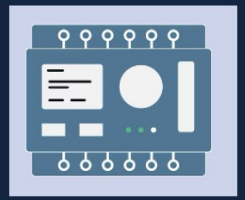
Web Interface

- Using tools like Burp suite, check for web based vulnerabilities like XSS, CSRF, OS Command Injection, etc.



The MITRE EMB3D™ Threat Model

Sushant Mane



Identify Device Properties

Application Software

- Runtime
- App Logic
- Web Srv
- Users DB

System Software

- System Calls
- Memory Mgmt
- Drivers
- Network Stack

Hardware

- CPU
- RAM
- JTAG
- I/O

Networking

EMB3D™ Threat Heat Map

Networking	Hardware	System Software	Application Software	
TID-001	TID-101	TID-201	TID-301	TID-318
TID-002	TID-102	TID-202	TID-302	TID-319
TID-003	TID-103	TID-203	TID-303	TID-320
TID-004	TID-104	TID-204	TID-304	TID-321
TID-005	TID-105	TID-205	TID-305	TID-322
TID-006	TID-106	TID-206	TID-306	TID-323
TID-007	TID-107	TID-207	TID-307	TID-324
TID-008	TID-108	TID-208	TID-308	TID-325
TID-010	TID-109	TID-209	TID-309	TID-326
TID-011	TID-110	TID-210	TID-310	TID-327
TID-012	TID-111	TID-211	TID-311	
	TID-113	TID-212	TID-312	
	TID-114	TID-213	TID-313	
	TID-115	TID-214	TID-314	
	TID-116	TID-215	TID-315	
	TID-117	TID-216	TID-316	
		TID-217	TID-317	

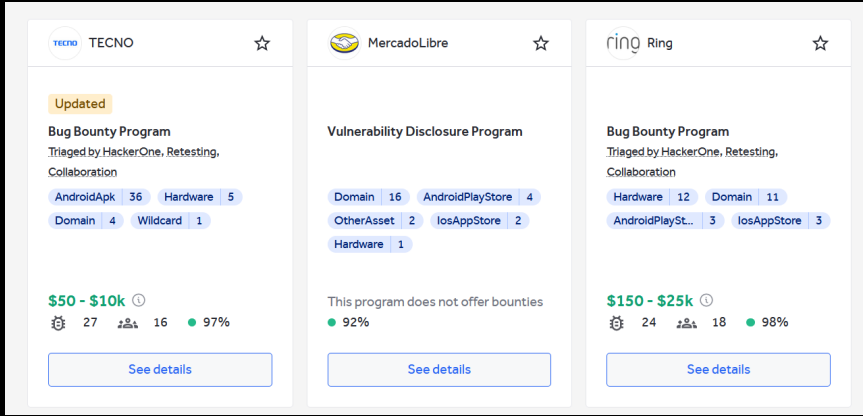
TID-XXX	Not Applicable	TID-XXX	Mitigated
TID-XXX	Conditionally Mitigated	TID-XXX	Vulnerable

https://emb3d.mitre.org/

Conclusion....

Sushant Mane

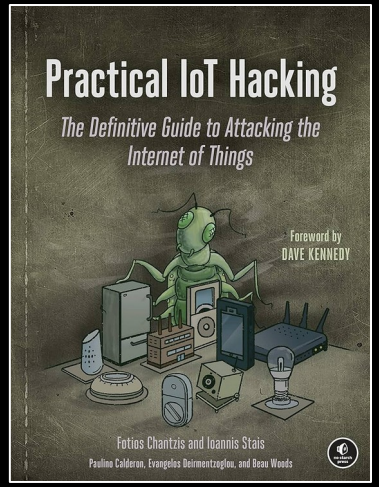
- Use the knowledge you gained to find some bugs in IoT devices.
  - Platform- Hackerone → Asset Type: Hardware

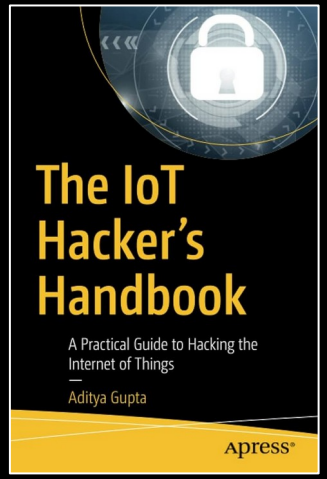


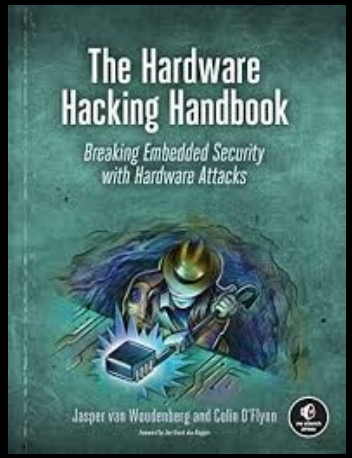
- Be Safe & Make The World A Safer Place....
- Take Slide Number 3 Seriously!
- Some good Telegram Groups to join- https://t.me/iotsecur 1
- https://t.me/iotsecuritygroup

Good References to Read-

- Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things
- The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things
- Payatu IoT Security Blogs - https://payatu.com/blog/







Some Amazing Researchers you can follow-

- https://www.linkedin.com/in/shakir-zari/
- https://www.linkedin.com/in/arun-mane-272456166/
- https://www.linkedin.com/in/veeraiot/

Thank You...

Sushant Mane
smmane_p22@el.vjti.ac.in
https://www.linkedin.com/in/sushantmmane/