introduction to embedded system hacking

(maybe)

https://ruz.fi/

disclaimer

- i don't have much experience (just a little 🤏) especially about this
- don't expect too much
- just wanna share & let's discuss

what is embedded system?

embedded system = specialized computer system

a combination of a computer processor, computer memory, and input/output peripheral devices that has a dedicated function within a larger mechanical or electronic system.

e.g.

- router
- game console
- smart TVs
- security cameras
- smart homes (smart lights, smart locks)
- microwave
- washing machines
- ECUs (Engine Control Units)
- car navigation systems
- industrial robots
- PLCs (Programmable Logic Controllers)
- etc

related cases (unconfirmed)

https://www.tomshardware.com/networking/your-washing-machine-could-be-sending-37-gb-of-data-a-day

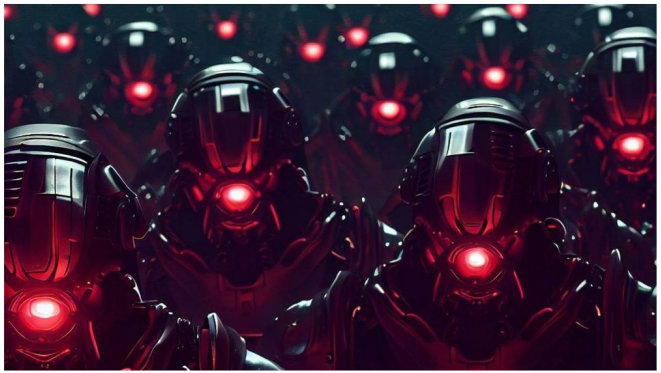
related cases

https://arstechnica.com/security/2024/01/network-connected-wrenches-used-in-factories-can-be-hacked-for-sabotage-or-ransomware/

related cases

Mirai botnet targets 22 flaws in D-Link, Zyxel, Netgear devices

By **Bill Toulas** June 22, 2023 01:53 PM 1



A variant of the Mirai botnet is targeting almost two dozen vulnerabilities aiming to take control of D-Link, Arris, Zyxel, TP-Link, Tenda, Netgear, and MediaTek devices to use them for distributed denial-of-service (DDoS) attacks.

https://www.bleepingcomputer.com/news/security/mirai-botnet-targets-22-flaws-in-d-link-zyxel-netgear-devices/

related cases

Tesla hacked again, 24 more zero-days exploited at Pwn2Own Tokyo

By **Sergiu Gatlan** January 25, 2024 10:49 AM 2

Security researchers hacked the Tesla infotainment system and demoed 24 more zero-days on the second day of the Pwn2Own Automotive 2024 hacking competition.

https://www.bleepingcomputer.com/news/security/tesla-hacked-again-24-more-zero-days-exploited-at-pwn2own-tokyo/

related cases

The story of the great Polish train hack

Polish rolling stock company Newag has alleged its train systems were illegally hacked, making four of its trains unsafe.

Patrick Rhys Atack | December 15, 2023

Share

The rolling stock affected all belongs to the Lower Silesia Railways provider in South West Poland. Credit: Dziajda/Shutterstock

https://www.railway-technology.com/news/the-story-of-the-great-polish-train-hack/

https://media.ccc.de/v/37c3-12142-breaking_drm_in_polish_trains

and many more

how to do?

- static analysis
  - analyze firmware file (binwalk, Firmware-Mod-Kit, strings, dd)
  - code review a.k.a. reverse engineering (ghidra, IDA Pro, Radare2)
- dynamic analysis
  - interface testing (logic analyzers, oscilloscopes, UART, JTAG)
  - runtime debugging (gdb w/wo OpenOCD)
  - analyze network/protocol communication (wireshark, tcpdump)

static analysis (some case examples)

- Linksys WAP54Gv3 Remote Debug Root Shell (CVE-2010-1573)

  https://www.icysilence.org/?p=268

- Unprotected Root Access via UART Using Default Password (CVE-2021-35033)

  https://www.tenable.com/security/research/tra-2022-06

static analysis (some case examples)

- Hardcoded Credentials on Action Camera Mobile App

  https://nikko.id/read.php?id=38

```
public static boolean a() {
    u.a("[Normal] -- SDKSession: ", "start prepareSession()");
    a = new com.icatch.wificam.a.h();
    if (a.a("192.168.1.1", "anonymous", "anonymous@icatchtek.com")) {
        try {
            b = a.h();
            c = a.f();
            e = a.e();
            d = a.i();
            g = a.g();
            f = a.c();
            h = a.d();
        } catch (com.icatch.wificam.a.a.i e2) {
            u.a("[Error] -- SDKSession: ", "IchInvalidSessionException");
            i = false;
            e2.printStackTrace();
        }
    } else {
        u.a("[Error] -- SDKSession: ", "failed to prepareSession");
        i = false;
    }
    u.a("[Normal] -- SDKSession: ", "end prepareSession() sessionPrepared");
    return i;
}
```

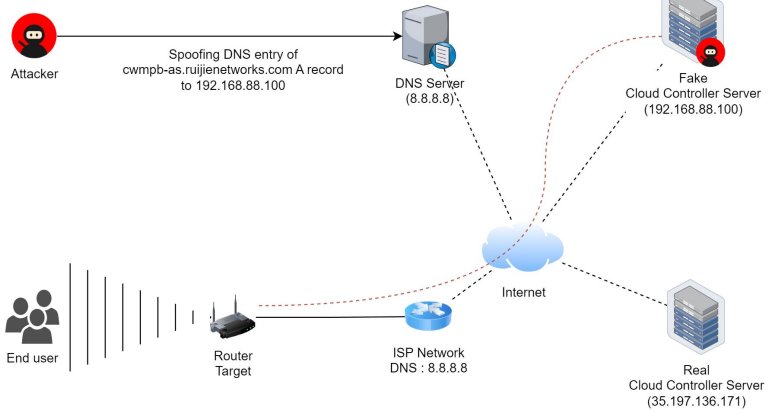
dynamic analysis (some case examples)

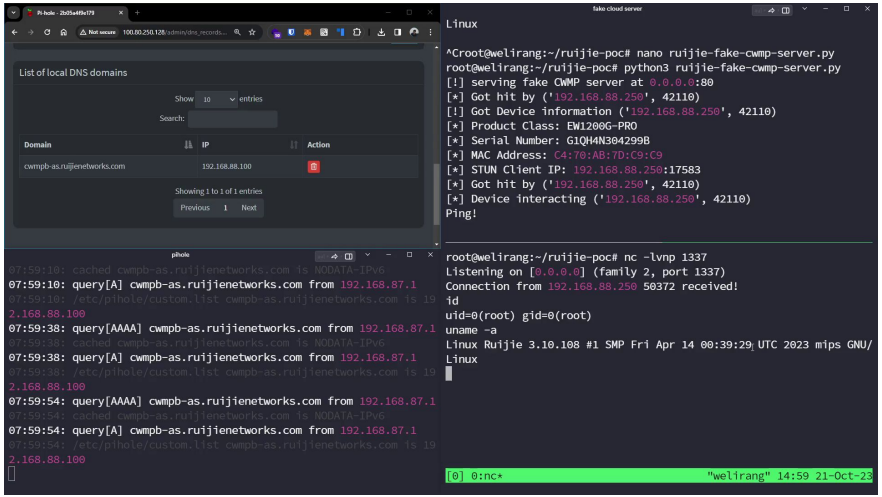
- Takeover Cloud Managed Router via CWMP Communication using MITM Scenario

  https://www.slideshare.net/slideshow/mochammad-riyan-firmansyah-takeover-cloud-managed-router-via-cwmp-communication-using-mitm-scenariopdf-0740/263331528

dynamic analysis (some case examples)

- Takeover Cloud Managed Router via CWMP Communication using MITM Scenario





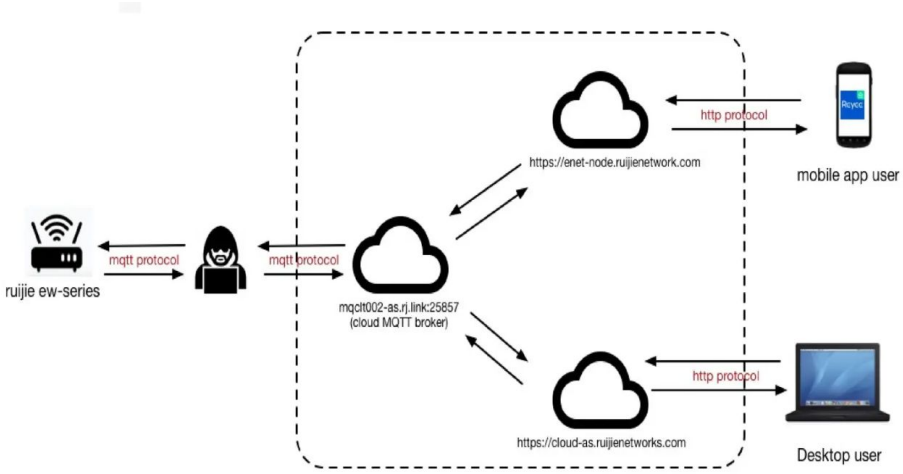
dynamic analysis (some case examples)

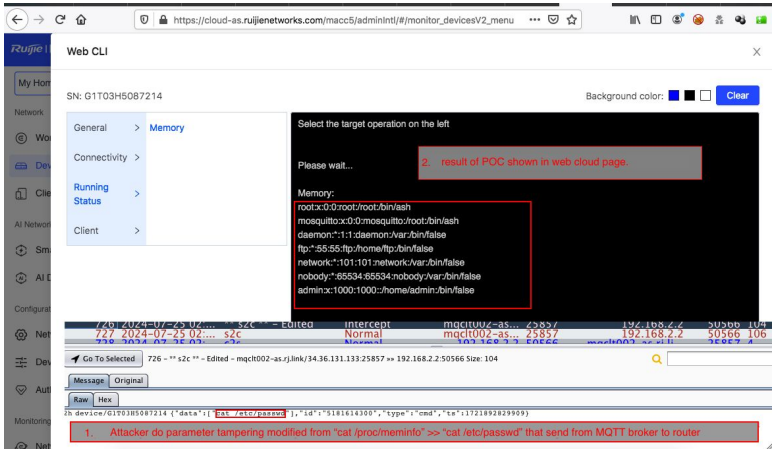
- MQTT hacking, RCE in Smart Router

  https://www.slideshare.net/slideshow/rama-tri-nanda-mqtt-hacking-rce-in-smart-router-pdf/272867902

dynamic analysis (some case examples)

- MQTT hacking, RCE in Smart Router





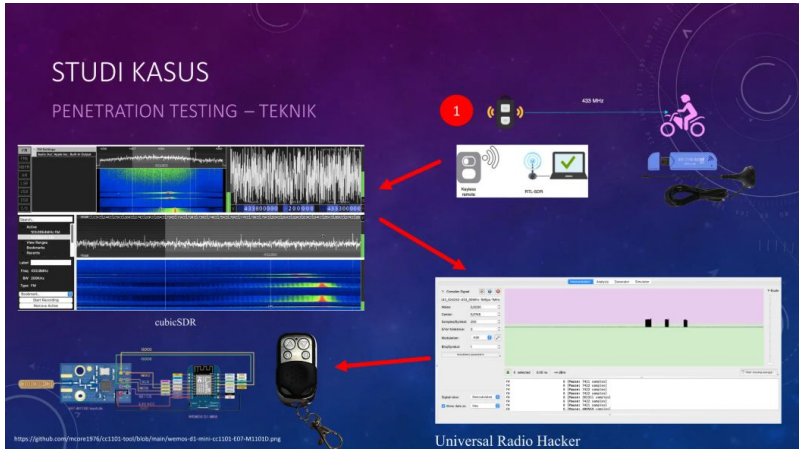
dynamic analysis (some case examples)

- Analyzing and Attacking Wireless Protocols

  https://www.slideshare.net/slideshow/ryan-fabella-daniel-dhaniswara-keamanan-siber-pada-kendaraan-listrik-studi-kasus-motor-listrik-di-indonesia-pdf/272867918

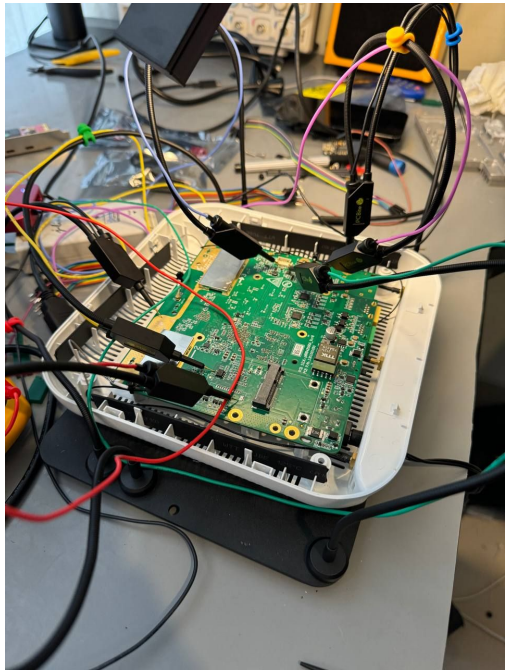
dynamic analysis (some case examples)

- Analyzing and Attacking Wireless Protocols



dynamic analysis (some case examples)

- interface testing on Femtocell (small BTS) device

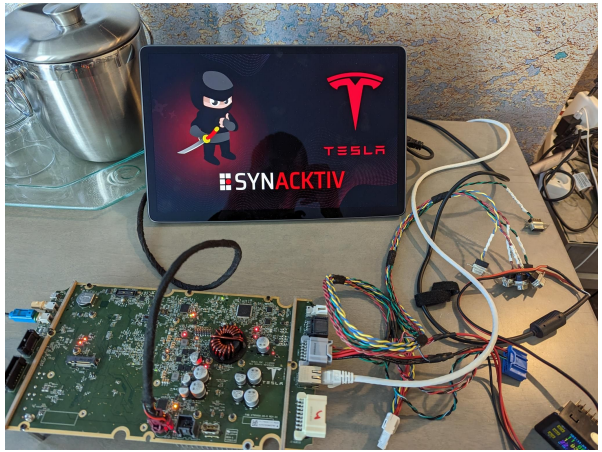


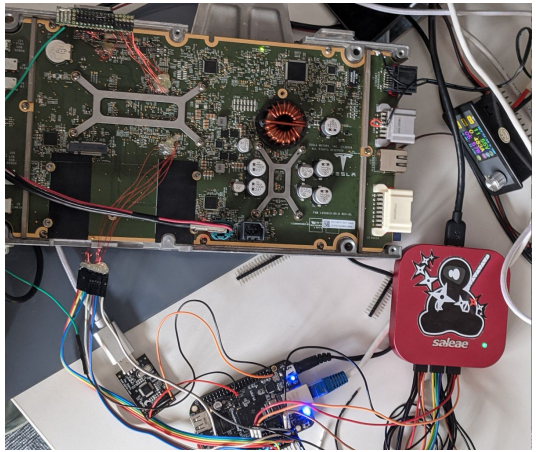
dynamic analysis (some case examples)

- interface testing on Tesla device

  https://x.com/Synacktiv/status/1638996681260781574

  https://x.com/Synacktiv/status/1526116912945586177





dynamic analysis (some case examples)

- Voltage Glitching in so many device (kinda cool but very hard to do)

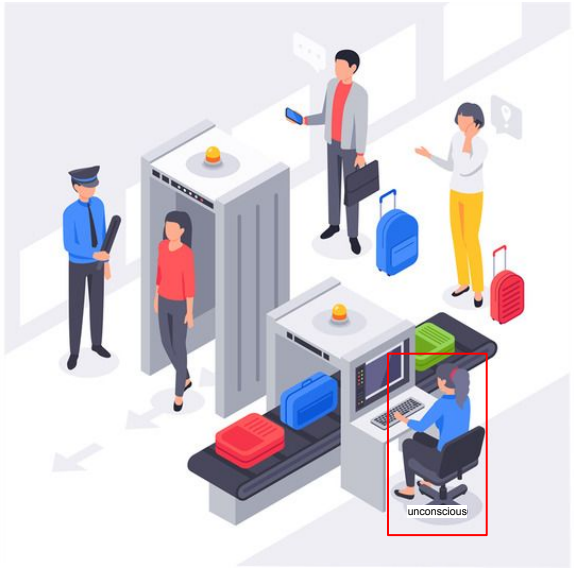
  https://youtu.be/6boKvdoTu2w?si=Q6w1rsHCMyAQ409z - Power glitch attacks

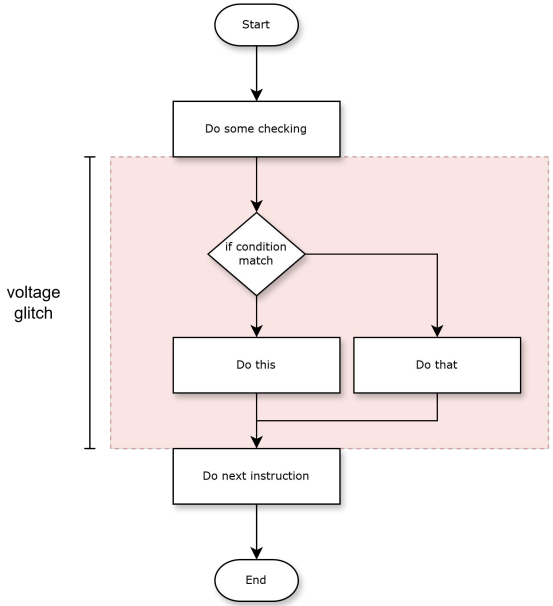
  https://youtu.be/NXqLMmGwJm0?si=kISvPNsyXZVlkrfN - Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal

  https://media.ccc.de/v/35c3-9364-viva_la_vita_vida - Viva la Vita Vida - Hacking the most secure handheld console

dynamic analysis (some case examples)

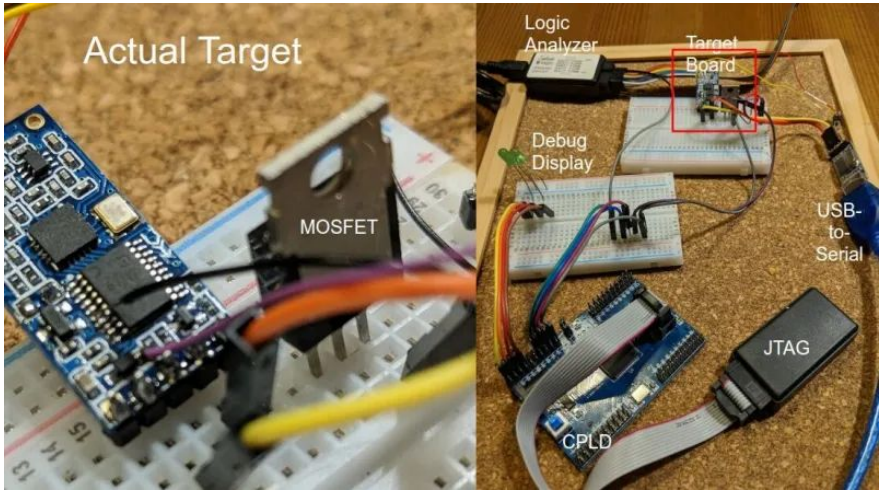
- Voltage Glitching in simple terms

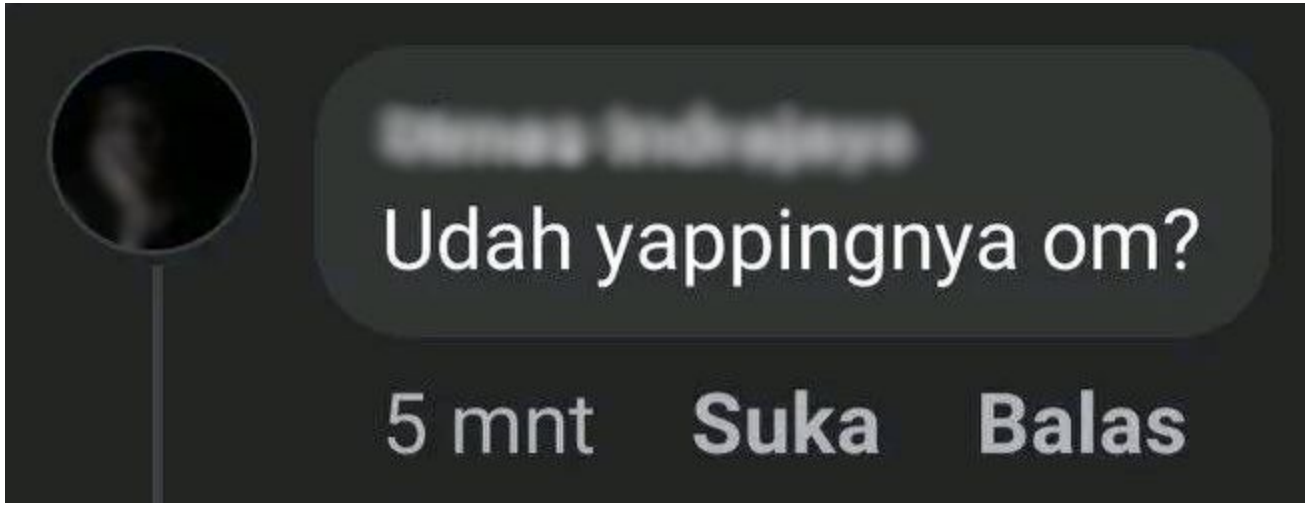




dynamic analysis (some case examples)

- Voltage Glitching in implementation
  - identifying the board
  - finding the test point
  - finding some information
  - setup device for voltage glitching
  - and many more




Udah yappingnya om?
5 mnt
Suka
Balas

let's try a little

what we can do after that?

if you are a bad person

- create mass exploits and sell them to the darkweb
- establish or join to an APT 😈

if you are a good person

- report to the vendor
- disclose to public (if permitted by the vendor or even if your report is not responded to)
- sharing is caring

faq

- learning path?

  i don't know how to start and what needs to be done to learn this, because I am learning very randomly and unstructured, but this topic might be related:

  - Microcontrollers, firmware, and hardware architecture.
  - Communication protocols (UART, JTAG, SPI, I2C, CAN).
  - TCP/IP, DNS, HTTP/HTTPS.
  - Wireless protocols (Wi-Fi, Zigbee, Bluetooth).
  - Firmware extraction (Binwalk, dd).
  - Static analysis (Reverse engineering) with Ghidra/IDA Pro.

  I just found a hidden gem
  OWASP IoT Security Testing Guide - https://owasp.org/owasp-istg/index.html

reference

- ChatGPT (of course)
- Wikipedia
- YouTube
- media.ccc.de
- hackaday.com
- research.seclab.id
- idsecconf conference archives
- Black Hat conference archives
- some sources from google search

* some images used in this presentation are under Creative Commons license or maybe not but credit is given to their respective authors