How Simple IoT Device Firmware Updates Can Be Dangerous

By Chontele Coleman

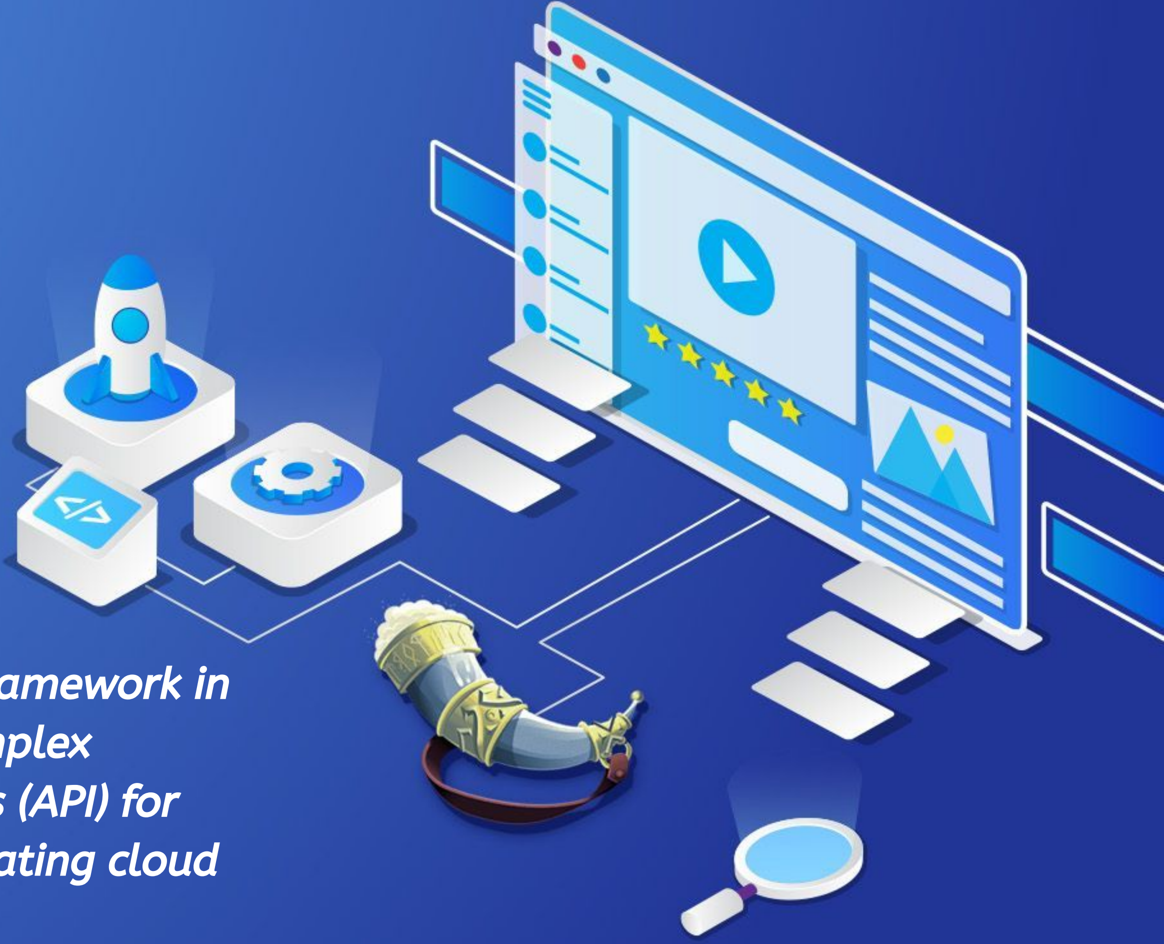
Perfect Timing

Furnaces should be replaced every 20-25 years, mine was 21 yrs. Old. The Lennox S40 Smart Thermostat came with the new furnace and AC Unit. Shortly after that Project 4 was announced. I said to myself, “well there’s my project.” And Immediately started doing research.

Research & Planning

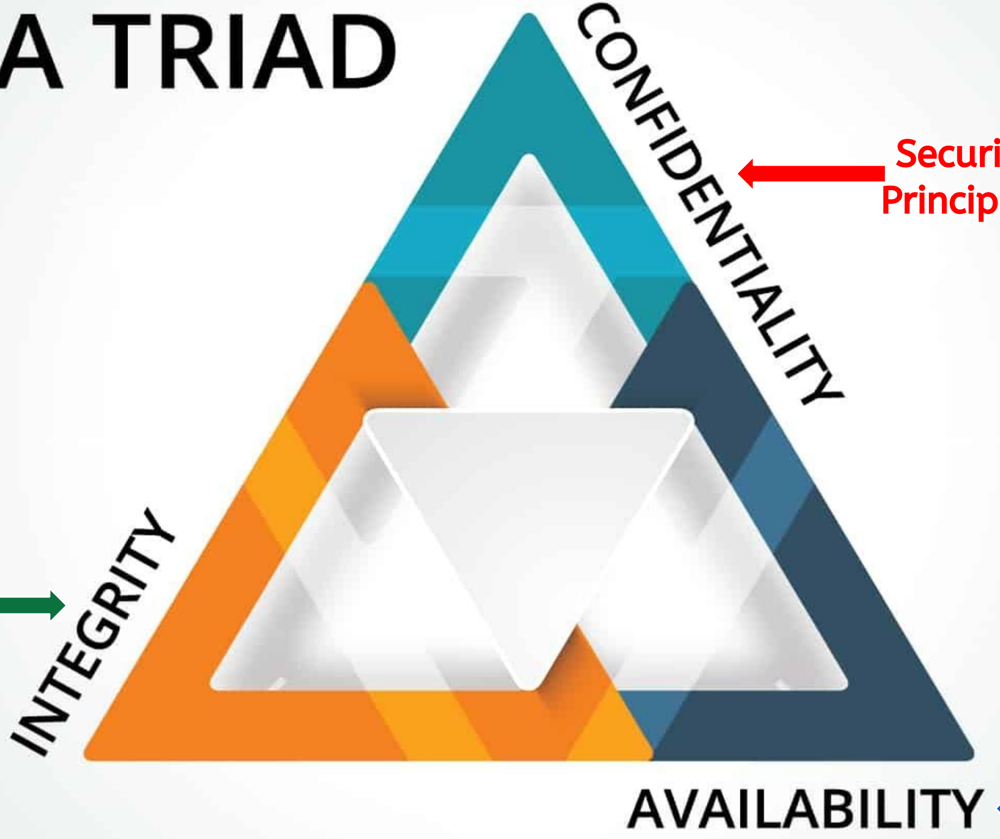
- ➔ Analyzed IoT vulnerabilities in smart thermostats.
- ➔ Studied CVE Records.
- ➔ Reviewed past attacks and failures like the 2021 Facebook DNS outage and Mirai (mee-rye) botnet in 2016.
- ➔ Learned how firmware updates and signature checks work.
- ➔ Researched simulation tools like curl, Docker, Flask, and Python.

BUILDING A PYTHON APP IN FLASK



- ★ *Lightweight web application framework in Python used to create non complex Application Program Interfaces (API) for uploading firmware and simulating cloud behavior*

CIA TRIAD



CONFIDENTIALITY

Security Principles

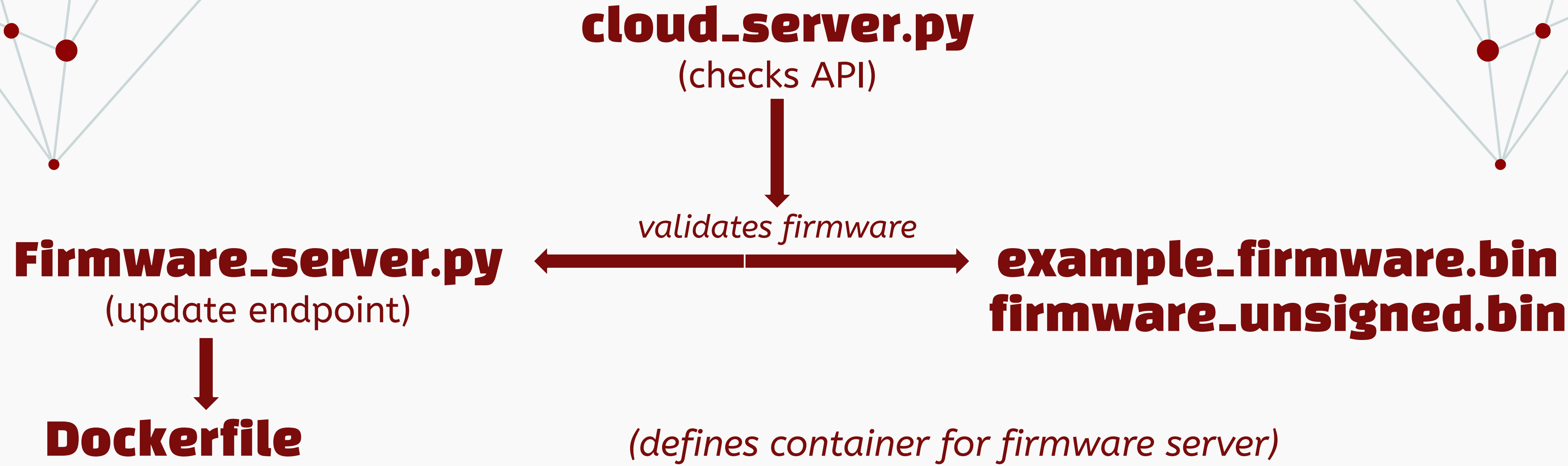
INTEGRITY

Cryptographic Concepts

AVAILABILITY

Networking Concepts

File Structure



cloud_server.py

(checks API)

validates firmware

Firmware_server.py

(update endpoint)

example_firmware.bin

firmware_unsigned.bin

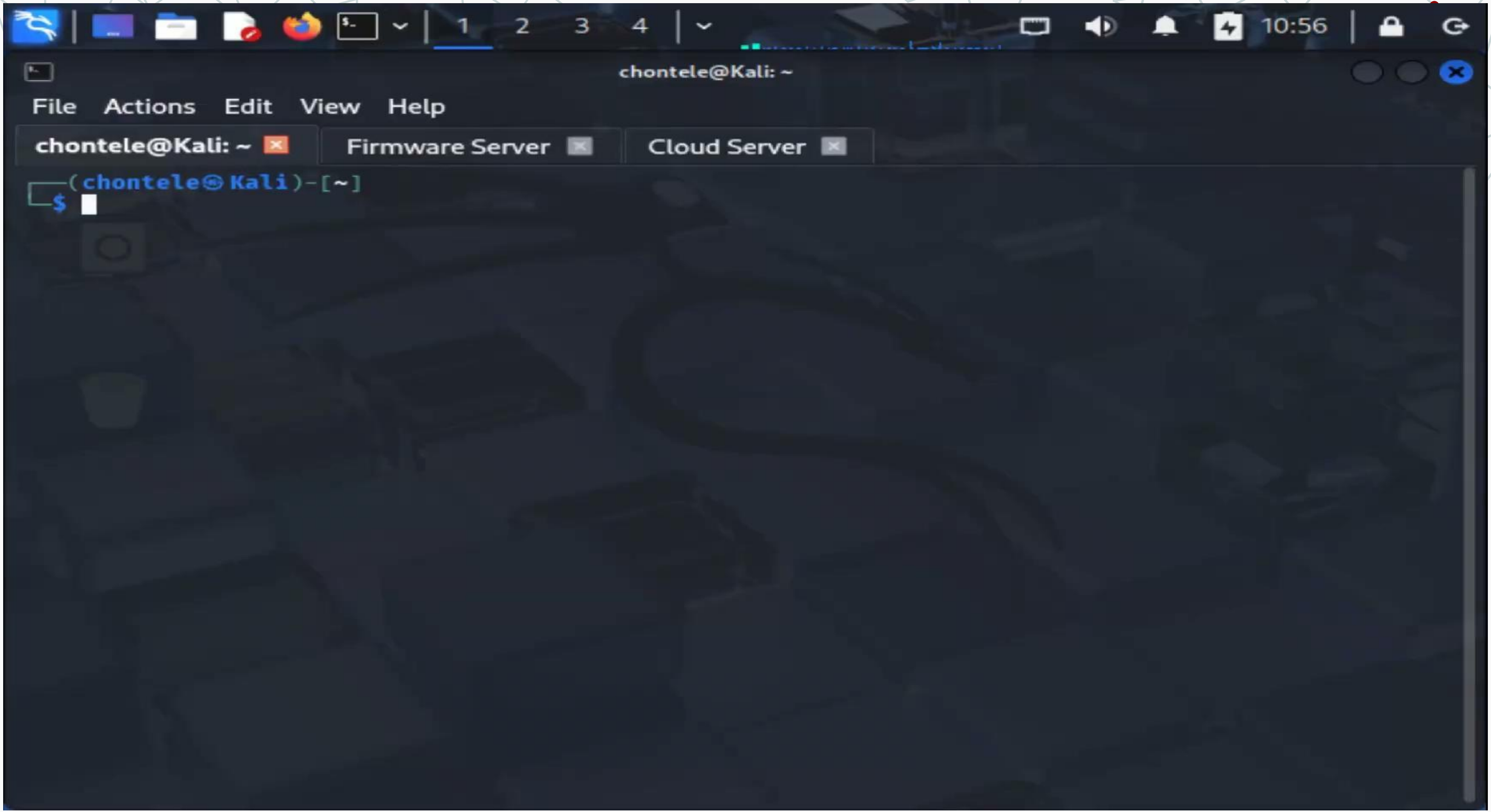
Dockerfile

(defines container for firmware server)

docker-compose.yml

(Connects firmware & cloud server)

Demo



```
┌──(chontele㉿Kali)-[~]
└─$ 
```

Breakdown

Install Now, Breach Later

- **Command:**
  - *curl -F "firmware=@example_firmware.bin" http://localhost:8080/update*
- **Outcome:**
  - *{"message":"Firmware example_firmware.bin uploaded and installed"}*
- **Why It's Insecure:**
  - *No signature check, the device blindly trust and installs any firmware*
  - *Opens the door for attackers to easily upload malicious firmware.*
- **Real-World Example:**
  - *In 2016 a malware called Mirai hijacked insecure IoT devices to create botnets. The botnets were used in a DDos attacks that took down Twitter, Netflix, Reddit.*

Weak Signature Validation

- **Commands:**

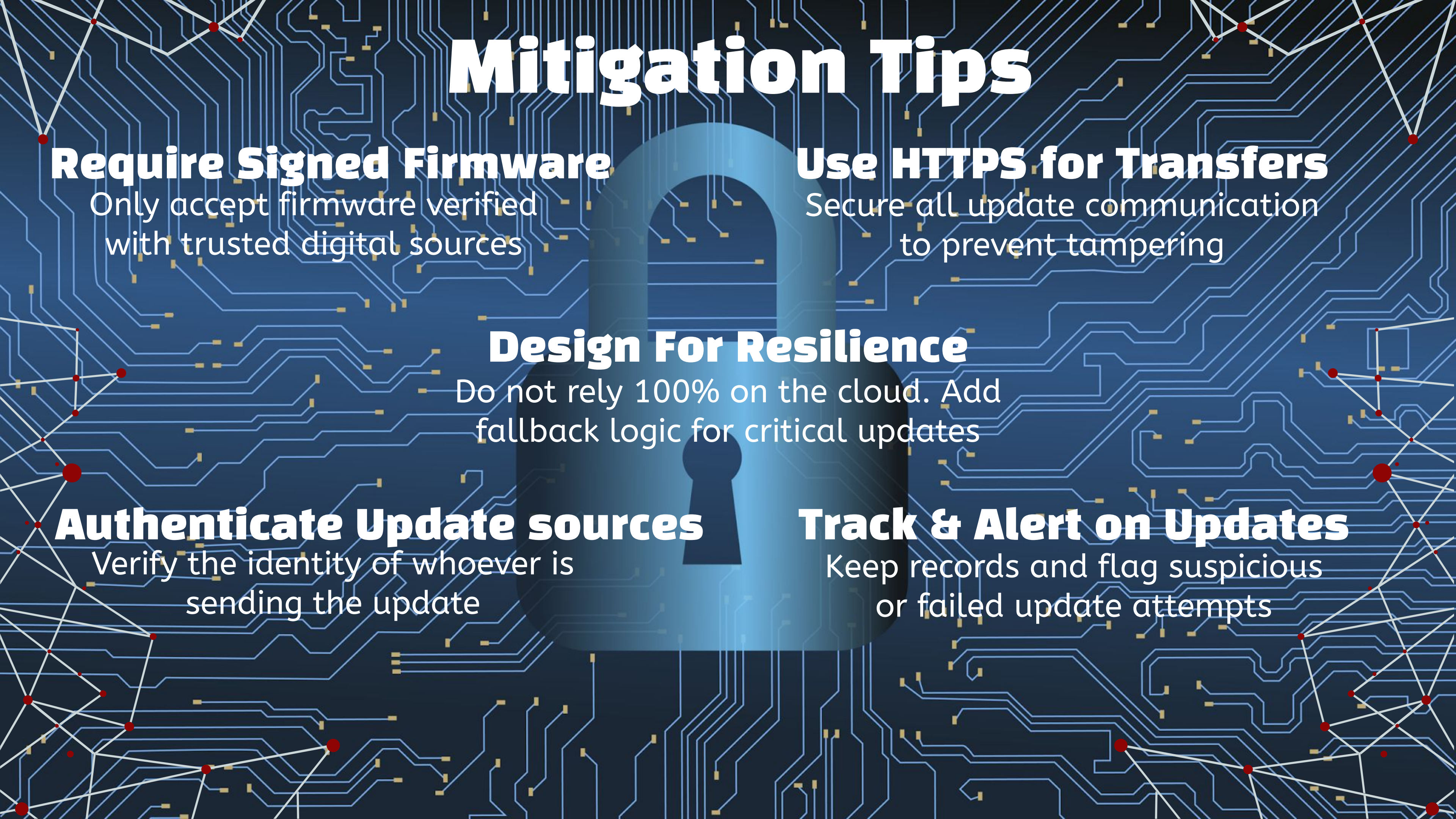
  -
    ```
    cp example_firmware.bin firmware_unsigned.bin
    ```

  -
    ```
    curl -F "firmware=@firmware_unsigned.bin" http://localhost:8080/update
    ```
- **Outcome:**

  -
    ```
    {"warning":"Firmware is unsigned but accepted (vulnerable behavior)"}
    ```
- **Why It’s Insecure:**
  - *Device accepts unsigned files without verification.*
  - *Shows how attackers exploit weak or missing signature checks.*
- **What Should have happened:**
  - *The firmware would include a type of digital signature that the device would verify using a public key.*

One Cloud, One Failure Point

- **Command:**
  - *docker-stop cloud server*
- **Outcome:**
  - *{"error":"Cloud service unreachable"}*
- **Why It’s a Risk:**
  - *Even locally the device will not update without cloud access*
  - *Outages can block firmware updates*
  - *Attackers can serve malicious firmware updates*
  - *Single Point of Failure (SPoF)*
- **Real-World Example:**
  - *Facebook outage in 2021. A misconfiguration of their routers caused DNS and BGP to go offline. This was possible because all services relied on a single internal network configuration.*



Mitigation Tips

Require Signed Firmware

Only accept firmware verified with trusted digital sources

Use HTTPS for Transfers

Secure all update communication to prevent tampering

Design For Resilience

Do not rely 100% on the cloud. Add fallback logic for critical updates

Authenticate Update sources

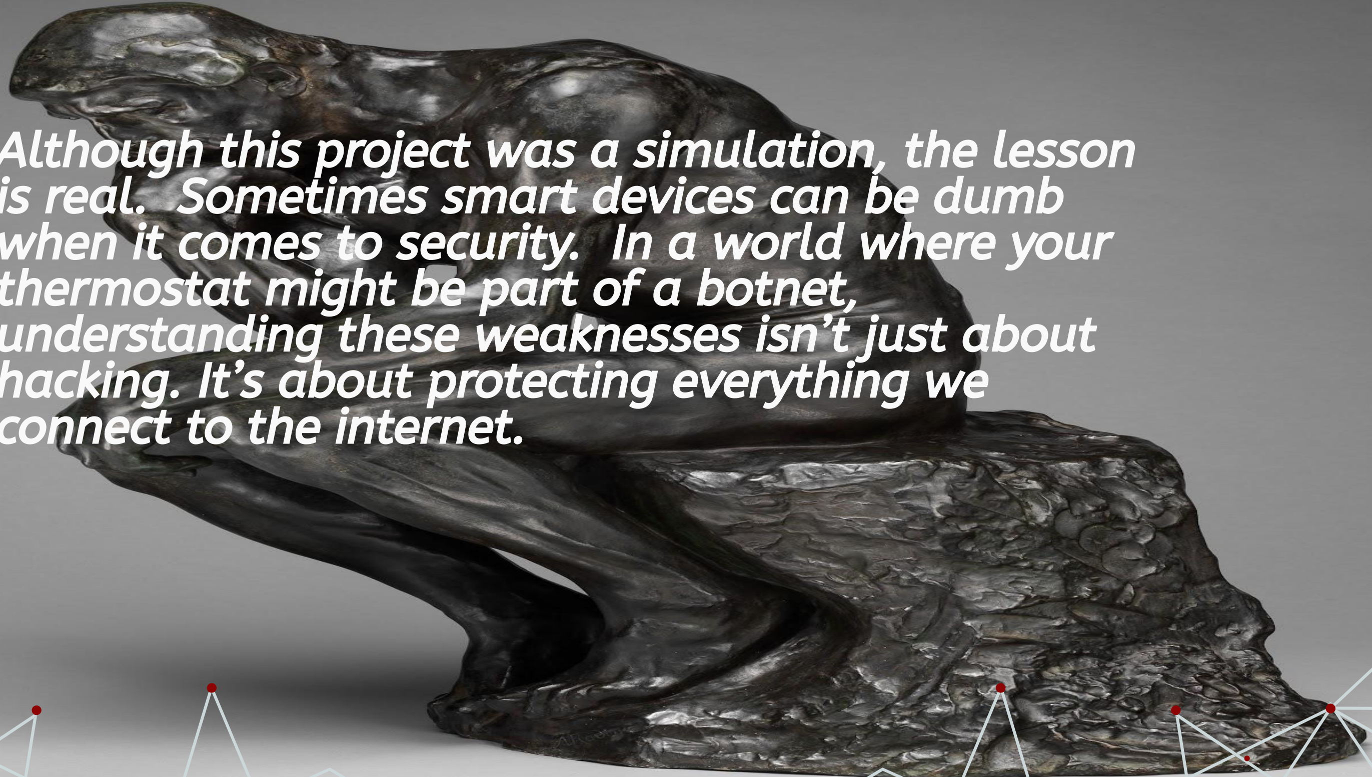
Verify the identity of whoever is sending the update

Track & Alert on Updates

Keep records and flag suspicious or failed update attempts

WRAP UP NOW
SECONDS
00

Final Thought



Although this project was a simulation, the lesson is real. Sometimes smart devices can be dumb when it comes to security. In a world where your thermostat might be part of a botnet, understanding these weaknesses isn't just about hacking. It's about protecting everything we connect to the internet.

Project References

https://flask.palletsprojects.com, For basic server setup, routing, and handling request

https://realpython.com

Wu, Y., & Yuhao, L. (2023). A Study of Firmware Update Vulnerabilities. USENIX

Bakhshi, T., Ghita, B.V., & Kuzminykh, I. (2024). Vulnerability Detection in IoT Firmware: A Survey. Sensors-Basel.

DEF CON 22 (2014), “Owning a Building” – research by @speakeasysecurity

Pen Test Partners – “Smart thermostats and building management fail” (2018)

Cloudflare. (2021). Inside the infamous Mirai IoT Botnet: A Retrospective Analysis. Cloudflare Blog.

SEGGER. (2022, May 24). Securing embedded systems with digital signatures: The Basics. SEGGER Blog.

The Guardian. (2021, October 5). Facebook outage: what went wrong and why did it take so long to fix.

Thank you