00

SIDE CHANNEL ATTACKS

A look into exploiting security implementation

01

EXCERPT FROM "SECRETS AND LIES" BY BRUCE SCHNEIER

"Imagine the attack working against a stockroom; you want to know about its contents. You can’t look in the stockroom to see how things are arranged. However, you can ask the clerk to get stuff for you.”

EXCERPT FROM "SECRETS AND LIES" BY BRUCE SCHNEIER

01 "Imagine the attack working against a stockroom; you want to know about its contents. You can't look in the stockroom to see how things are arranged. However, you can ask the clerk to get stuff for you.By timing how long it takes him to get different things, you can learn a lot about the stockroom. Does he always take a long time to get toner cartridges? Then they must be in the back of the room. Does he take longer to get reams of paper every ten requests? Then they must come in boxes of ten. Does he take longer to get pencils if you've just asked him to get erasers? That tells you something about what boxes get stacked on top of each other."

WHAT ARE SIDE CHANNELS

Unintended information from a system as a result of implementation

Time

Power

EM Radiation

Thermals

Acoustics

SIDE CHANNEL ATTACK: POWER/EM/TIMING

Assumptions:

1. Constant with same input
2. Different with different inputs

PASSIVE AND NON-INVASIVE

- May require physical access to the system
- Does not damage the system
- Tools are relatively cheap (ChipWhisperer ~$250)
- multiple traces should be done to account for "noise"

RESULTS

- reverse engineering
- key extraction**

** you don't have to decipher the encryption algorithm to gain access!

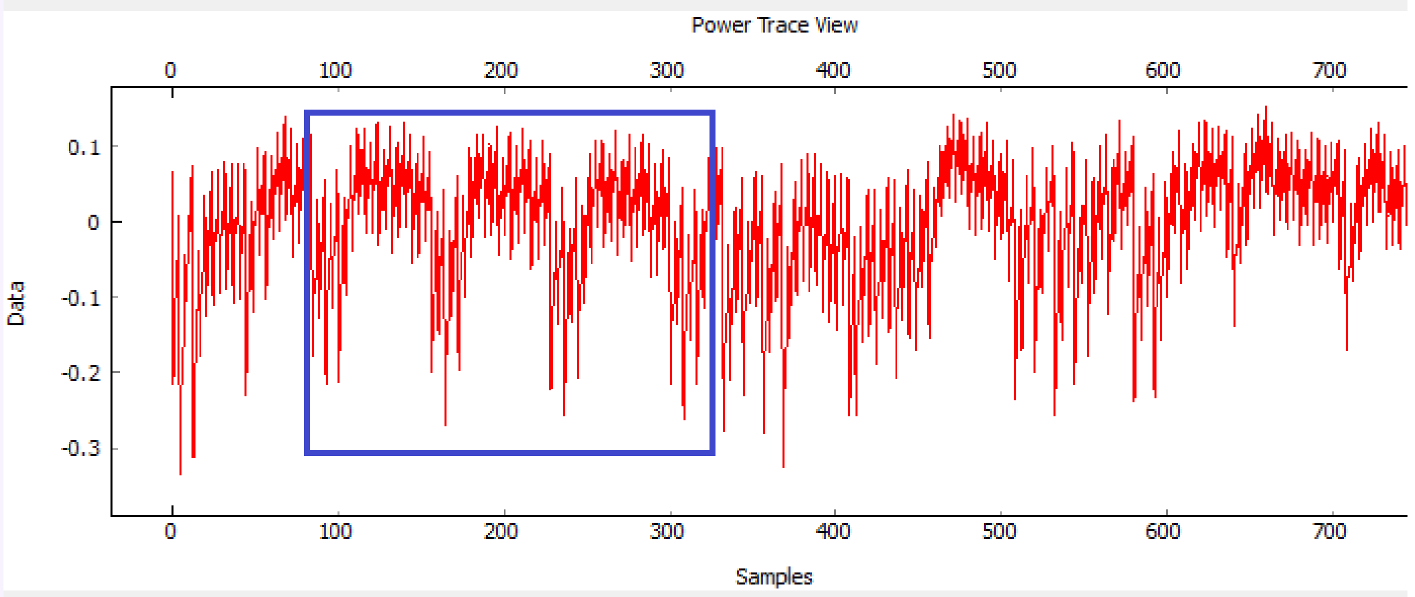
TARGETS

- remote OpenSSL server (2003)
- KeeLoq RFID (2008)
- DESFire Contactless Card (2011)
- TLS (2015)

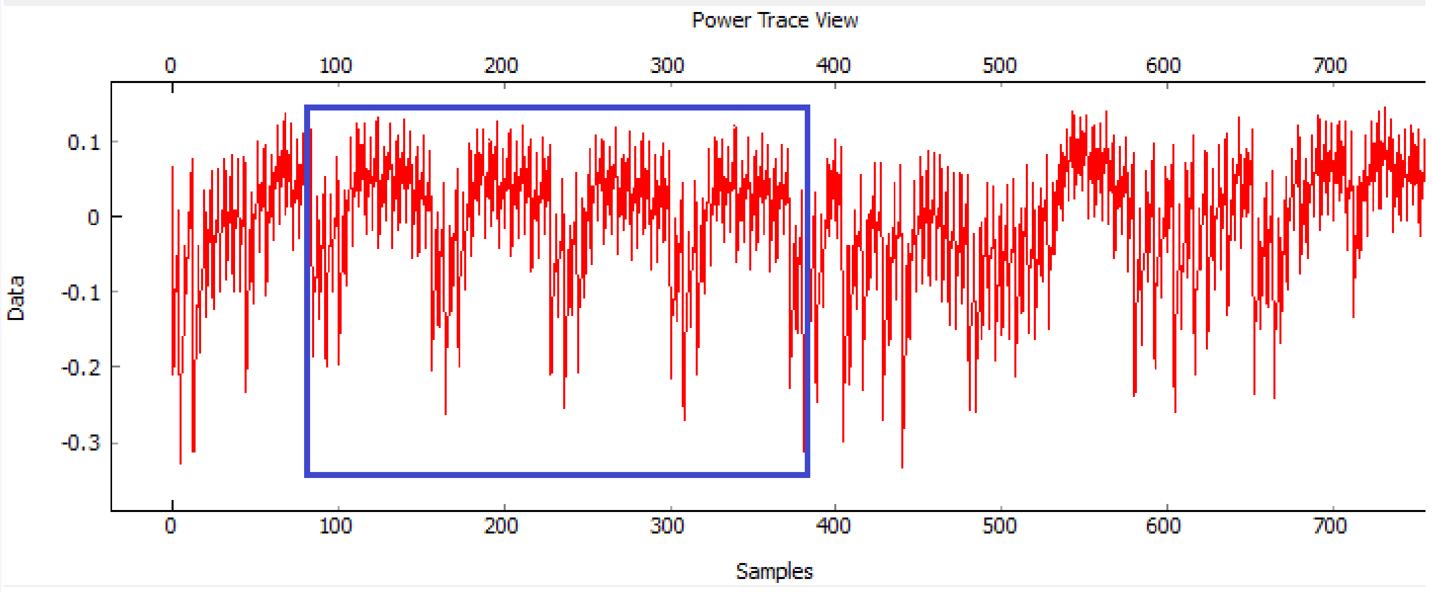
```
def password_checker(inp):
    password = "password"

    for i in range(len(password)):
        if (inp[i] != password[i]):
            return 0
    return 1
```

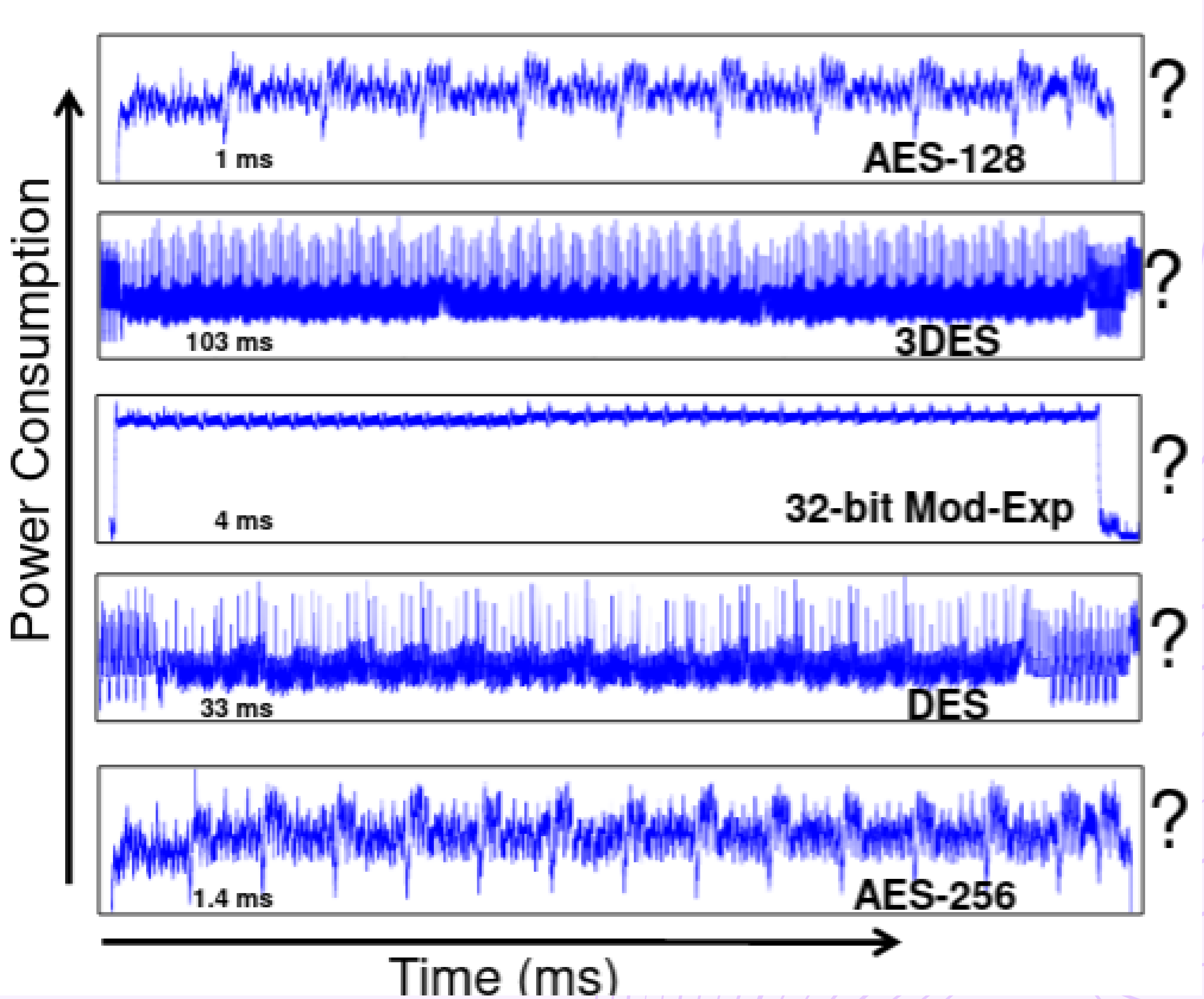
SPA ON CRPTOGRAPHY



3 correct



4 correct



IMAGES FROM NEWAE.COM

WORK CITED

- Bernard, D. (2018, July 23). Side Channel Attacks: The Cyber Security Attack You've Probably Never Heard Of. Retrieved January 14, 2021, from https://www.intellectiongroup.com/blog/side-channel-attacks-the-cyber-security-attack-youve-probably-never-heard-of
- Greenberg, A. (n.d.). What Is a Side Channel Attack? Retrieved January 14, 2021, from https://www.wired.com/story/what-is-side-channel-attack/
- Lakshminarasimhan, A. (2014). Electromagnetic Side-Channel Analysis for Hardware and Software Watermarking (Master's thesis, University of Massachusetts Amherst, 2011). Amherst: ScholarWorks@UMass Amherst.
- Randolph, M., & Diehl, W. (2020, May 19). Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. Retrieved January 14, 2021, from https://www.mdpi.com/2410-387X/4/2/15/htm
- Schneier, B. (2015). Secrets and lies: Digital security in a networked world. Indianapolis, IN: John Wiley & Sons.
- V3:Tutorial B3-1 Timing Analysis with Power for Password Bypass. (n.d.). Retrieved January 14, 2021, from http://wiki.newae.com/V3:Tutorial_B3-1_Timing_Analysis_with_Power_for_Password_Bypass

LAB!