Hardware Security

KAMILIMU COHORT 9: CYBER SECURITY

Why Hardware Security

1. Remember the Intro to Offensive and Defensive Technologies class... every technology matters

2. Smart watches... where are hardware technologies in use?

3. Impact of an attack on hardware security

4. It can also be a defensive measure!

Where?

ICS/SCADA Devices

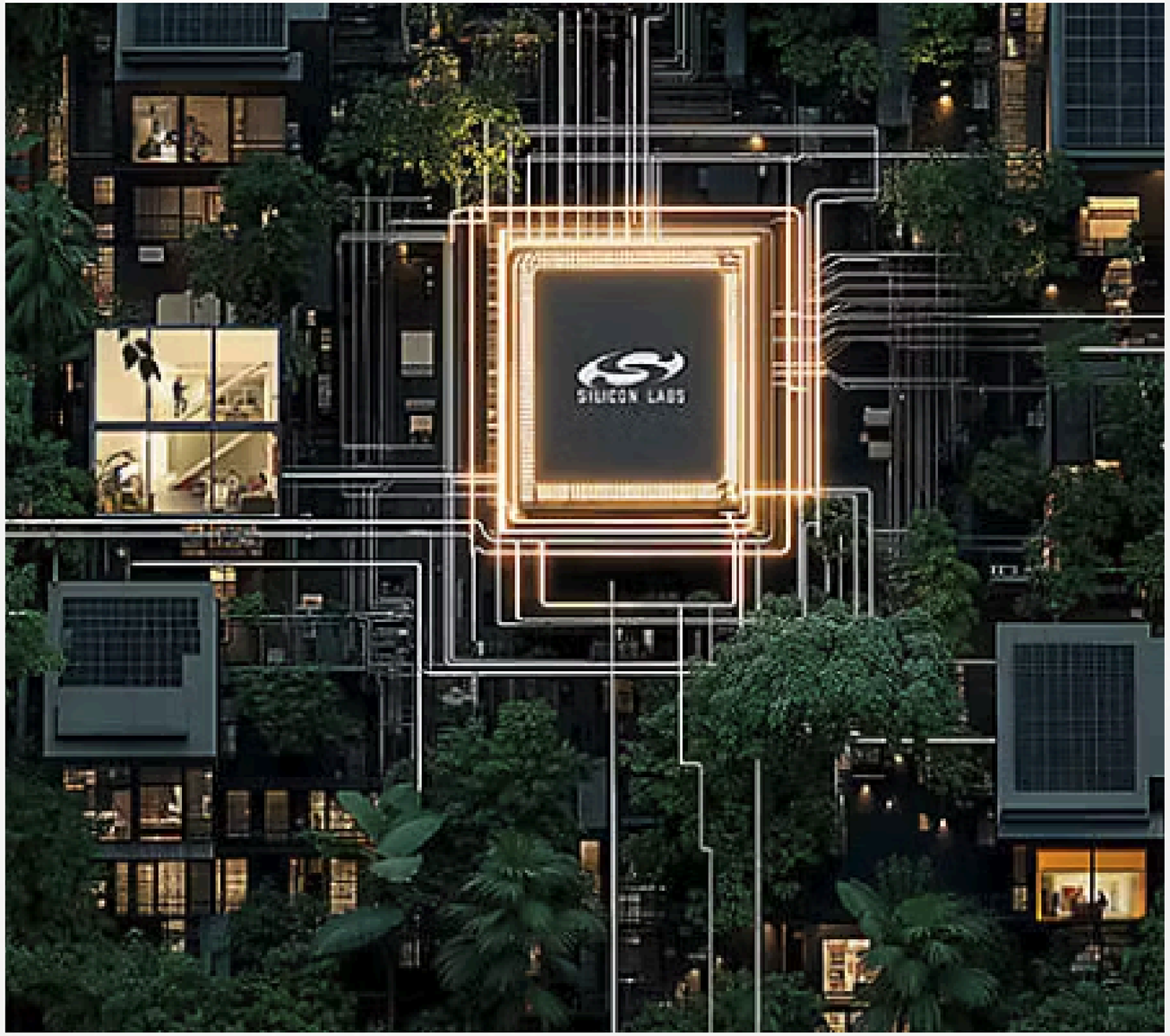
Internet of Things (IoT) devices

Embedded computing and others...

What could go wrong?

- Data disclosure
- Supply chain attacks
- Physical tampering
- Unpatched components
- Weak/Default credentials
- Side channel attacks e.g. eavesdropping

Example: Silicon Labs



Resources

Excellent places to learn more about hacking and securing hardware :)

Your favourite tool/retailer

Practice using tools you use often or that are available to you!

Many large brands have security disclosure programs for their hardware technologies including:

- Xiaomi
- OPPO
- Intel
- Amazon
- Google

Security Research blogs on the topic

There are many writeups on newly discovered vulenrabilities or how to prevent them in places such as:

- Unit 42 blog (under IoT)
- Siemens
- Kaspersky blog
- Hardware as a defense (here)
- so many more...

Pwn2own

Link: here

- Awesome global competition that brings top researchers to find vulnerabilities in various hardware from top organizations.

The end

QUESTIONS?