universität innsbruck

IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

Practical Relevance

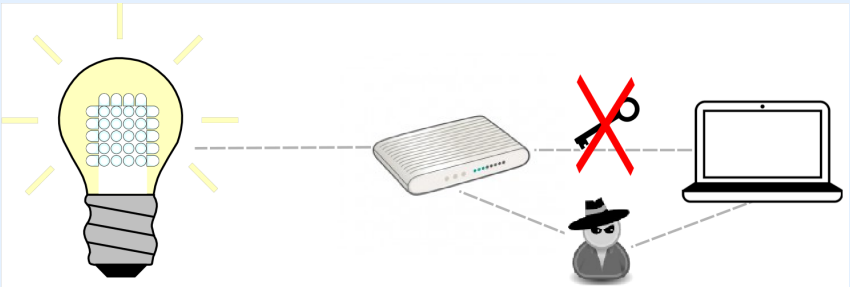
Market size

New vulnerabilities

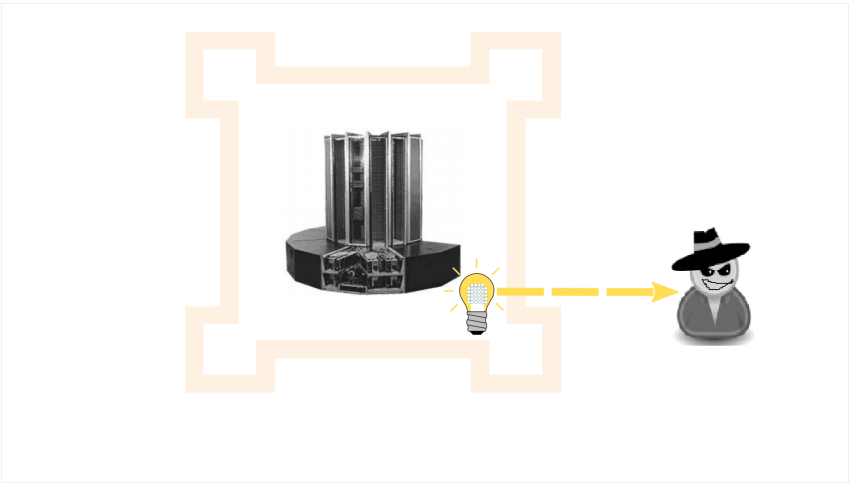
- Security is only an afterthought
- Patches rarely get shipped, let alone installed

Practical Relevance (cont.)

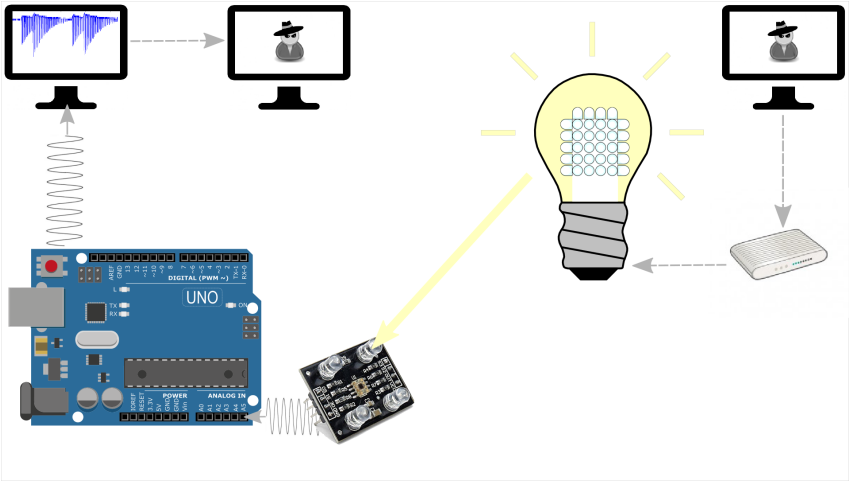
Hits close to home (literally)



Lights in Particular



Expected Outcome



Questions?

Julia Wanker, Bennett Piater

Details

Classification of Attacks on IoT Devices

We will present a taxonomy of the possible attacks against IoT devices.
We will then attempt to demonstrate the most interesting kind, namely extending the functionality of a device to make it useful for an attacker:

Our Goals

- Create a smart light that we can make flicker above $\sim$ 60 Hz
- Even cooler: Abuse API or vulnerabilities of a commercial smart light system
- Build a sensor that can capture our high-speed signals
- Encode, transmit and decode information over this channel