universität innsbruck


# IoT Light Bulb Covert Channel

## Extended Functionality Attack on Smart Lights

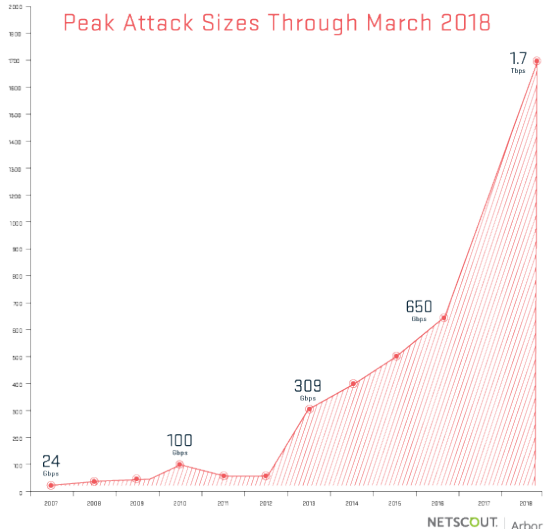
Julia Wanker, Bennett Piater

# Taxonomy of IoT Attacks

1. Ignoring Functionality
2. Reducing Functionality
3. Misusing Functionality
4. Extending Functionality

# Ignoring Functionality

# Ignoring Functionality



# Reducing Functionality

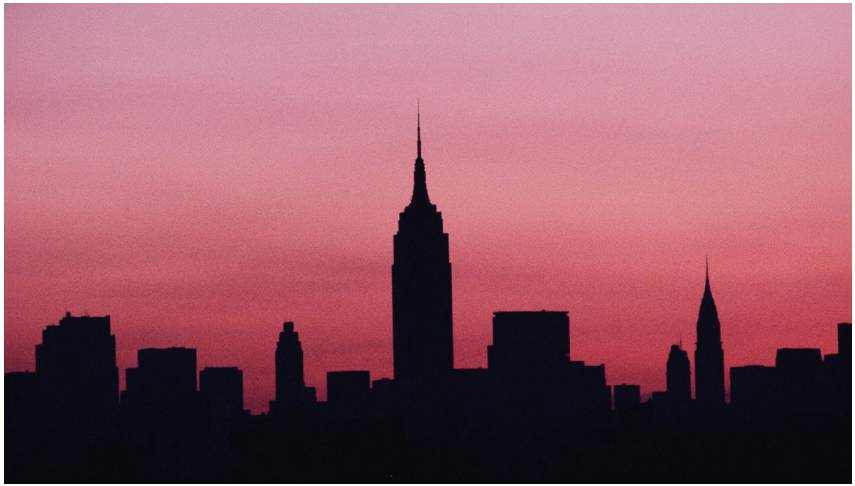


**Figure:** NYC Blackout of 1977 (Allan Tannenbaum/Getty Images)

# Misusing Functionality

## Create Discomfort

- Heat in summer, AC in winter
- Flash bedroom lights at night
- Turn on AC in bathroom in the morning

## Generally be Annoying

- Turn on lights
- Open Faucets
- Run Washing Machine

# Misusing Functionality

## Create Discomfort

- Heat in summer, AC in winter
- Flash bedroom lights at night
- Turn on AC in bathroom in the morning

## Generally be Annoying

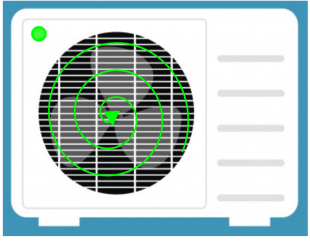
- Turn on lights
- Open Faucets
- Run Washing Machine

. . . when the owners leave for vacation.

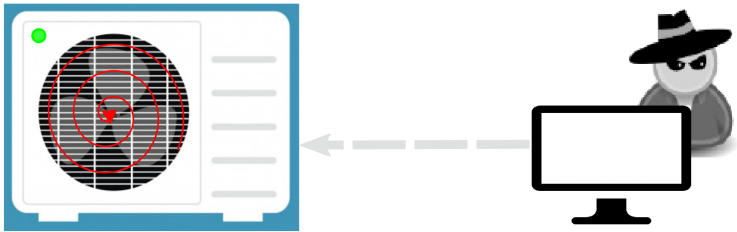
# Extending Functionality

## Possible Extending Functionality Attacks

- Open front door with smart household robots
- Start a fire with an AC

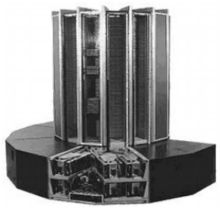


# Extending Functionality

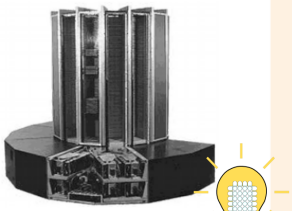


# Extending Functionality

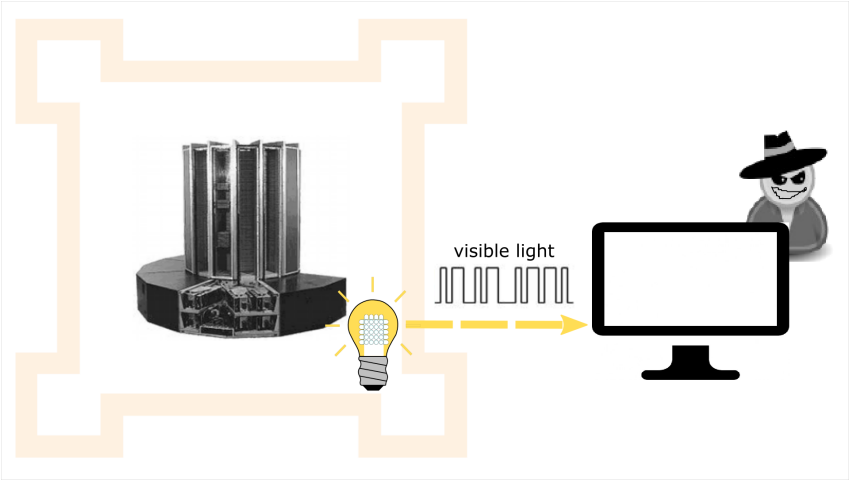
# Extending Functionality - The Case of Smart Lights



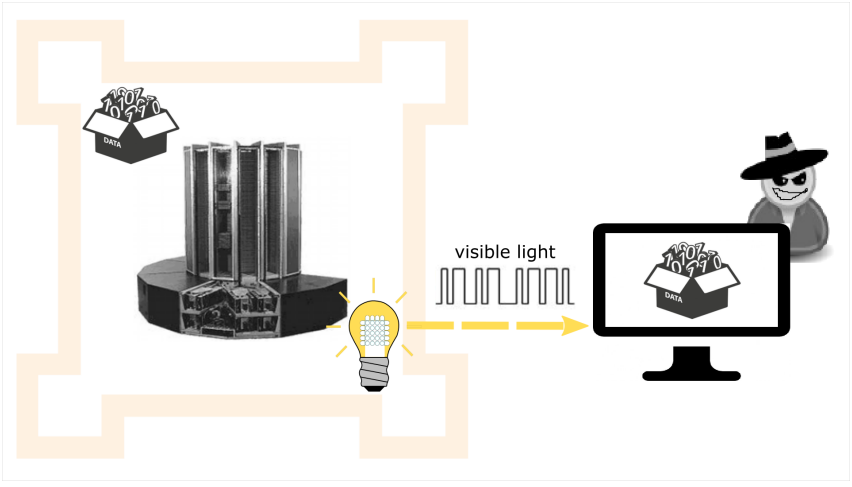
# Extending Functionality - The Case of Smart Lights



# Extending Functionality - The Case of Smart Lights



# Extending Functionality - The Case of Smart Lights




# E. Ronen and A. Shamir Paper

Extended Functionality Attacks on IoT Devices: The Case of Smart Lights

Julia Wanker, Bennett Piater

# Requirements for Covert Channel

**Correctness**

Switch between 2 brightnesses that can be robustly distinguished by a sensor.

**Covertness**

Use brightnesses so similar or switch so fast that a human cannot distinguish them.

# How (smart) LEDs Work

## RF Receiver (and transmitter)

- For communication with controller
- Communicate with ZigBee Light Link (ZLL)

# How (smart) LEDs Work

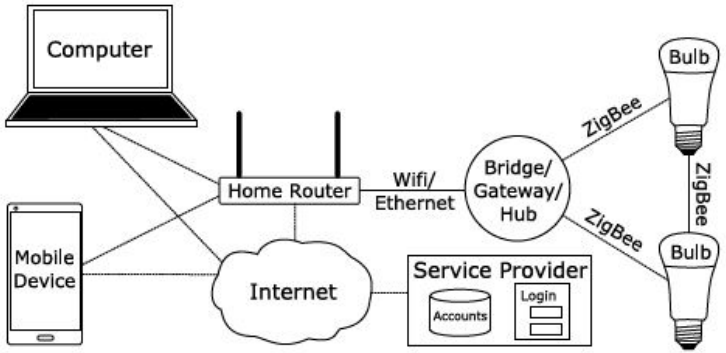



**Figure:** System architecture of a ZLL-based connected lighting system with two bulbs [1]

[1] Morgner et al. All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems

# How (smart) LEDs Work

## Processing Unit

- For processing commands received from controller
- LEDs are controlled using pulse width modulation (PWM) signals

## Drivers and LEDs

- Driver controls LED on and off states
- Determine brightness level of bulb

# How (smart) LEDs Work

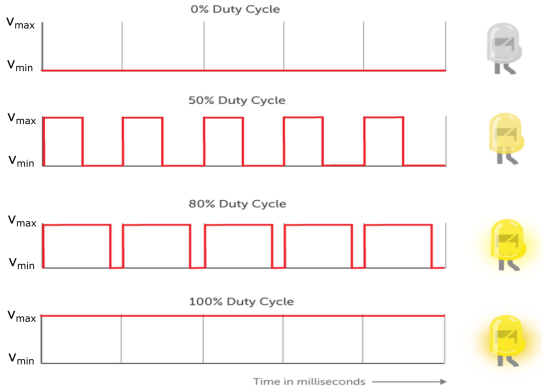
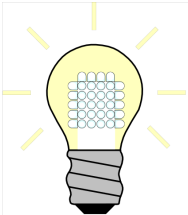


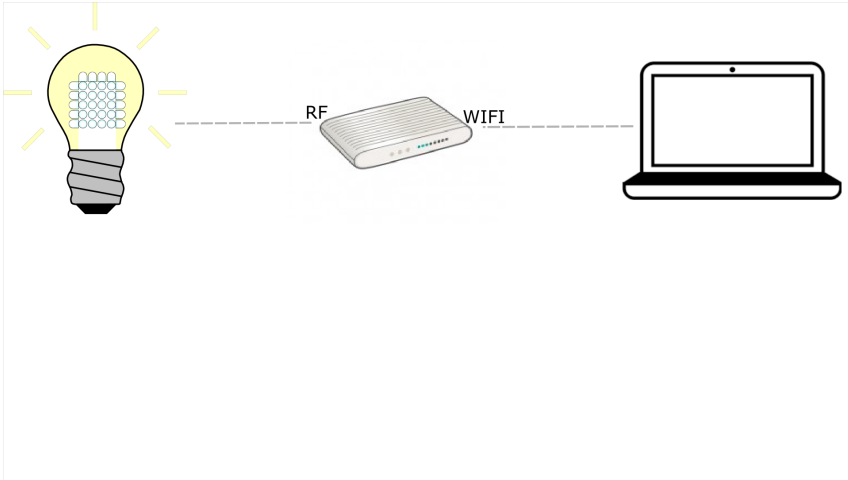

**Figure:** Brightness control on LEDs [1]

[1] PubNub - Building the Raspberry Pi Smart House: Controlling Lights with PWM

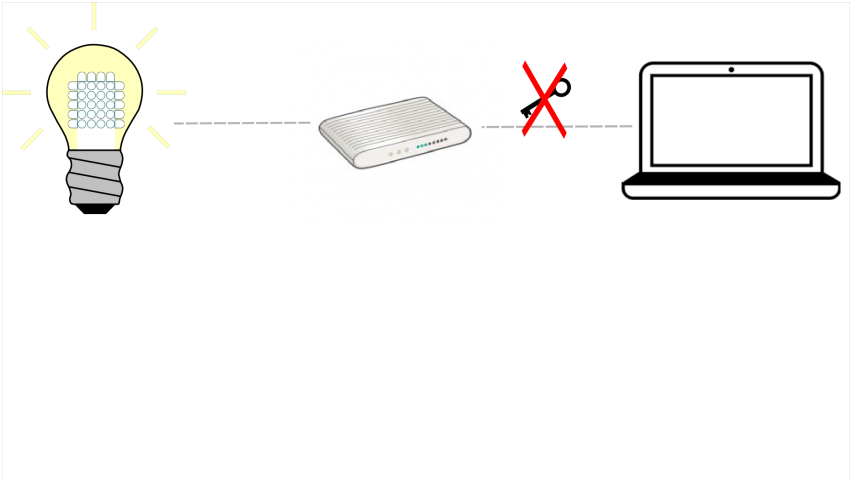
# Encoding: Access Controller



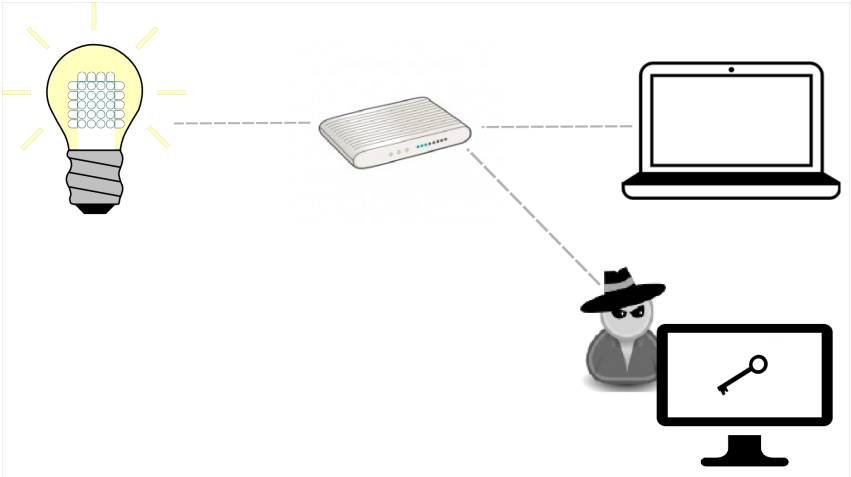
# Encoding: Access Controller



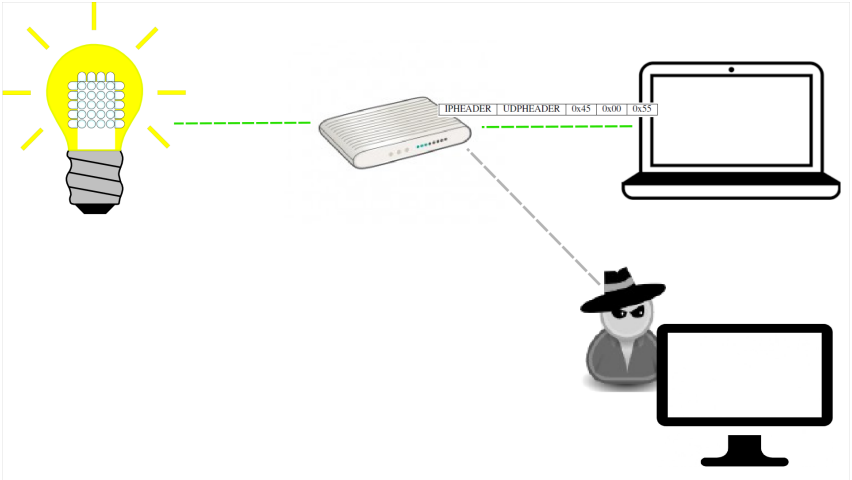
# Encoding: Access Controller



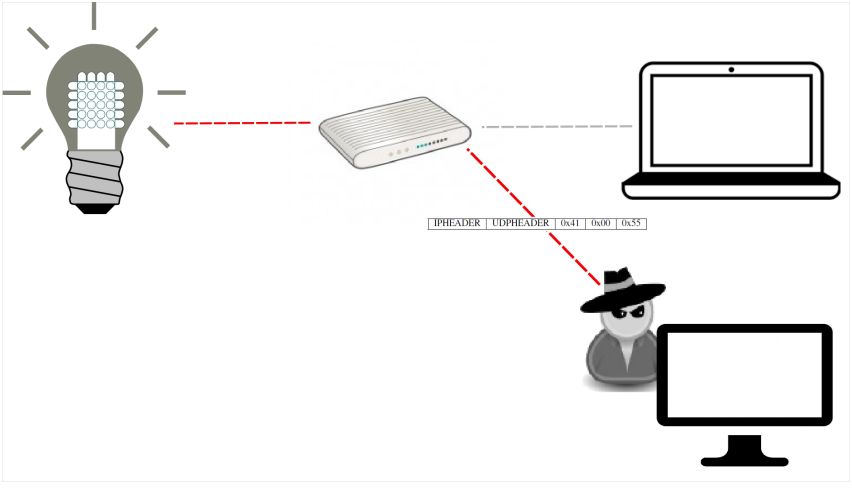
# Encoding: Access Controller



# Encoding: Access Controller

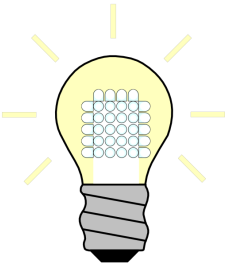


# Encoding: Access Controller

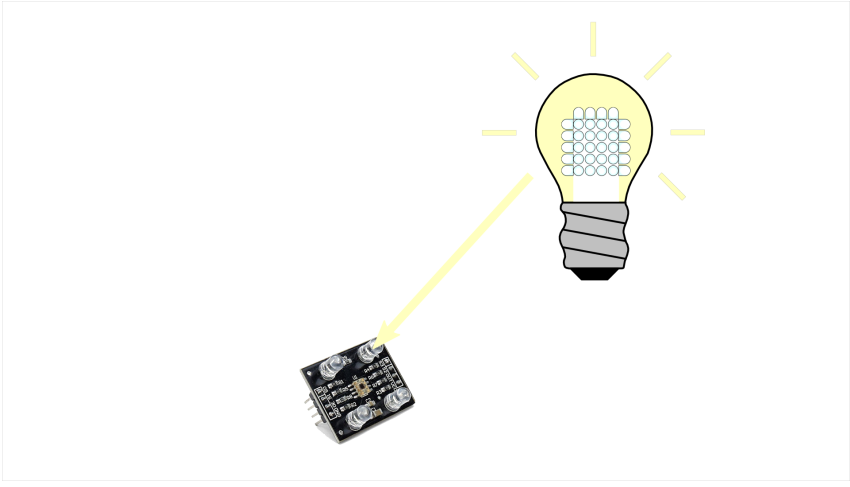


# Encoding: Crafting of PWM Signals

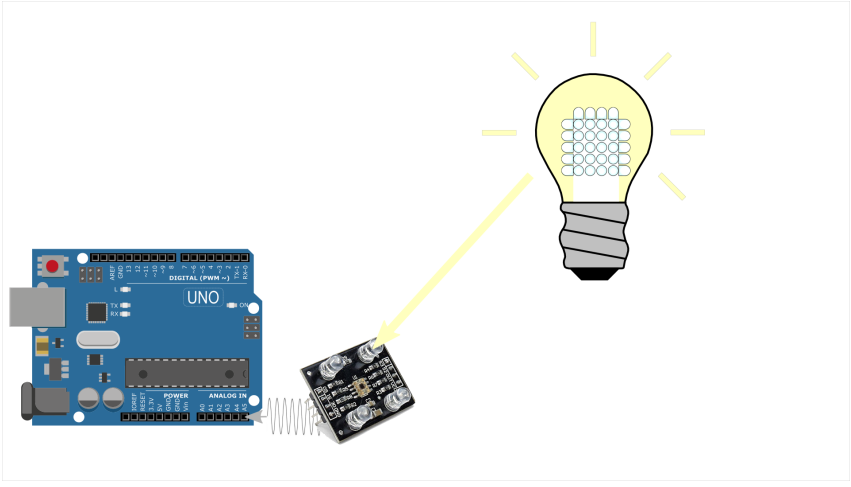
# Decoding: Light Sensor Signal Analysis



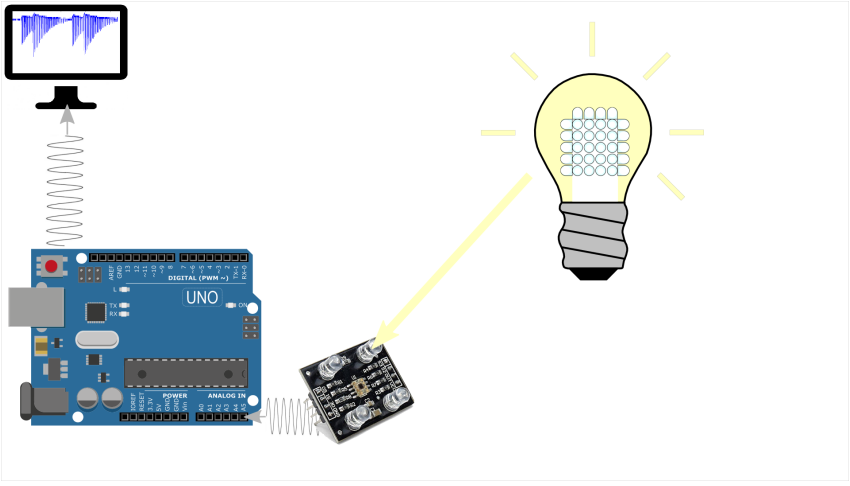
# Decoding: Light Sensor Signal Analysis



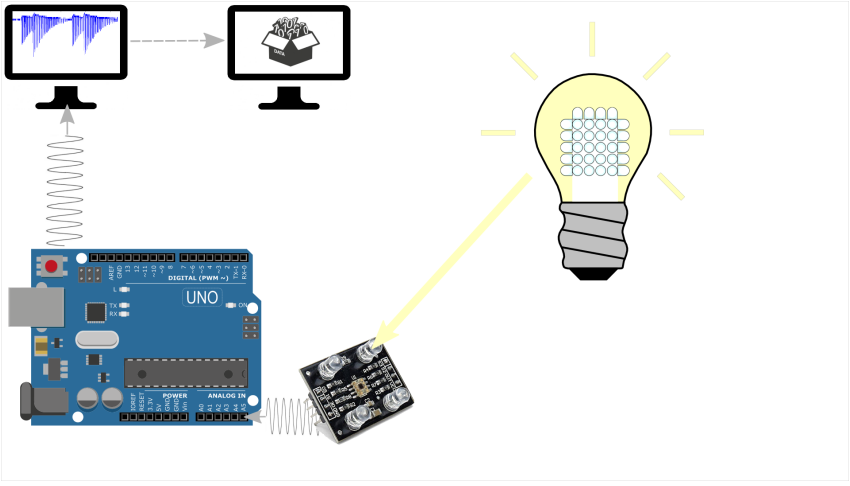
# Decoding: Light Sensor Signal Analysis



# Decoding: Light Sensor Signal Analysis



# Decoding: Light Sensor Signal Analysis




# Questions?

Julia Wanker, Bennett Piater