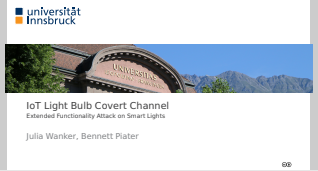
universität
innsbruck

IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



Taxonomy of IoT Attacks [RS16]

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

Taxonomy of IoT Attacks [RS16]
1. Ignoring Functionality
2. Reducing Functionality
3. Misusing Functionality
4. Extending Functionality

1m

Briefly introduce the taxonomy to give viewers an overview.

Ignoring Functionality [Ang17, AAB+17, DDGS17]

Ignoring Functionality [Ang17, AAB+17, DDGS17]

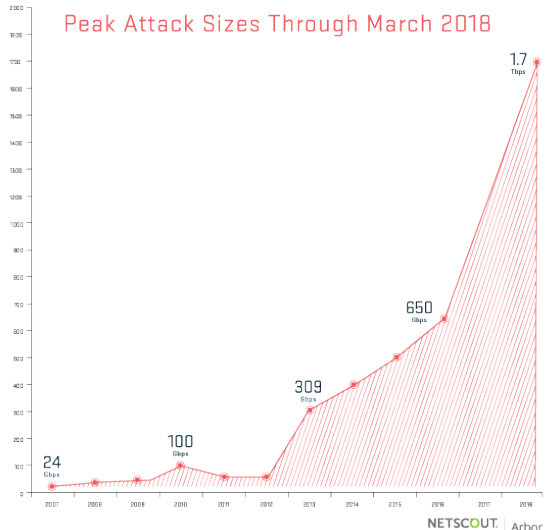
1m

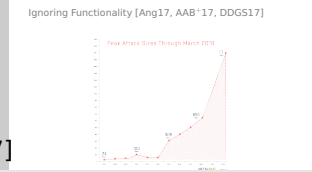
systematic insecurity, highly used for DDoS and spamming. [Angrishi]

Analysis of Mirai by [Antonakakis] showed massive vulnerabilities, weak default passwords etc. as the cause.

Many IoT devices will cause more problems, esp. DDoS (see 1.2TB/s DynDNS) [Donno]

Ignoring Functionality [Ang17, AAB^{+}17, DDGS17]





1m

systematic insecurity, highly used for DDoS and spamming. [Angrishi]

Analysis of Mirai by [Antonakakis] showed massive vulnerabilities, weak default passwords etc. as the cause.

Many IoT devices will cause more problems, esp. DDoS (see 1.2TB/s DynDNS) [Donno]

Reducing Functionality [Dha13, RSWO18, Bha17]

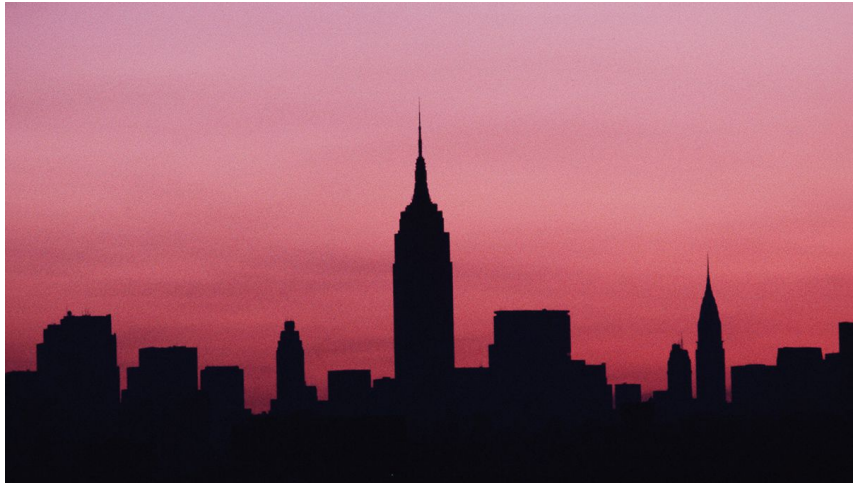


Figure: NYC Blackout of 1977 (Allan Tannenbaum/Getty Images)

Reducing Functionality [Dha13, RSWO18, Bha17]

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

1m

Disabling things can be very dangerous when more and more of them become connected.

e.g. blackout entire city with ZLL drive-by attack. (image was lightning strike)

Fridge murder story.

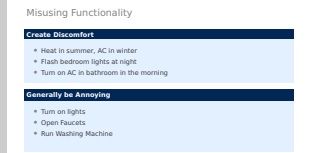
Misusing Functionality

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



30s
This is probably more annoying than dangerous.

Misusing Functionality

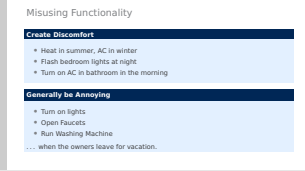
Create Discomfort

- 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.

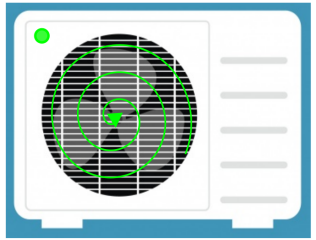


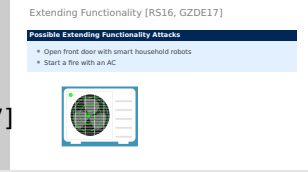
30s
This is probably more annoying than dangerous.

Extending Functionality [RS16, GZDE17]

Possible Extending Functionality Attacks

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

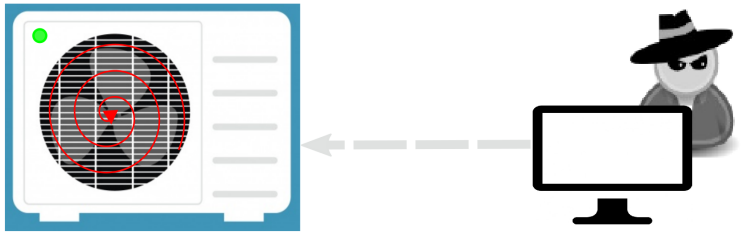




30s

- Most interesting
- Almost no reseach (Ronen, Guri (Router LEDs))

Extending Functionality [RS16, GZDE17]



Extending Functionality [RS16, GZDE17]

30s

- Most interesting
- Almost no reseach (Ronen, Guri (Router LEDs))

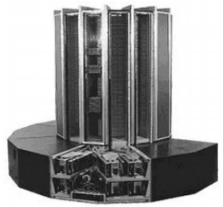
Extending Functionality [RS16, GZDE17]

Extending Functionality [RS16, GZDE17]

30s

- Most interesting
- Almost no reseach (Ronen, Guri (Router LEDs))

Extending Functionality — The Case of Smart Lights

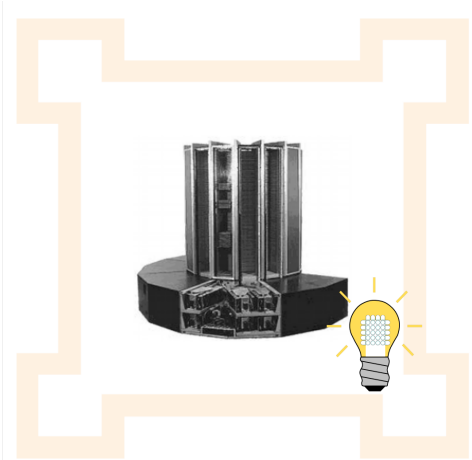


Extending Functionality — The Case of Smart Lights

30s

Interesting because light is often the only part of the EM-spectrum that is allowed to leave air-gapped systems.

Extending Functionality — The Case of Smart Lights

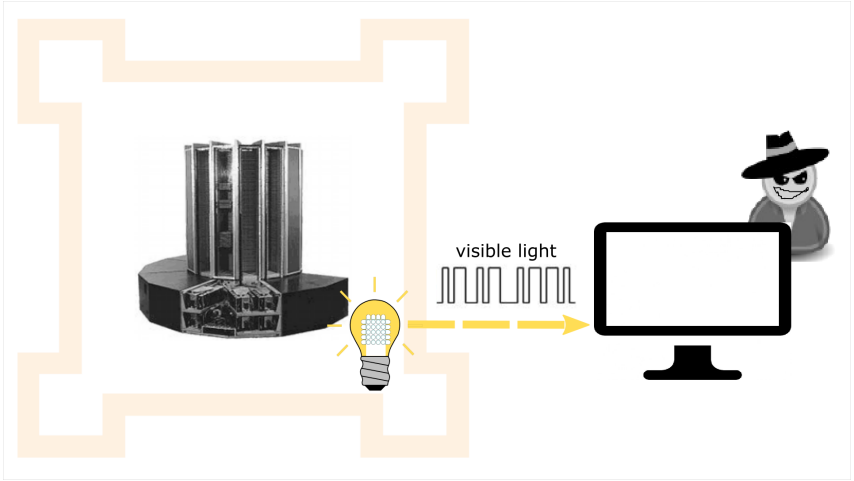


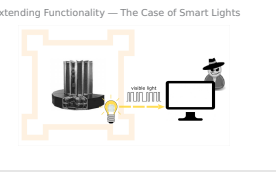
Extending Functionality — The Case of Smart Lights

30s

Interesting because light is often the only part of the EM-spectrum that is allowed to leave air-gapped systems.

Extending Functionality — The Case of Smart Lights

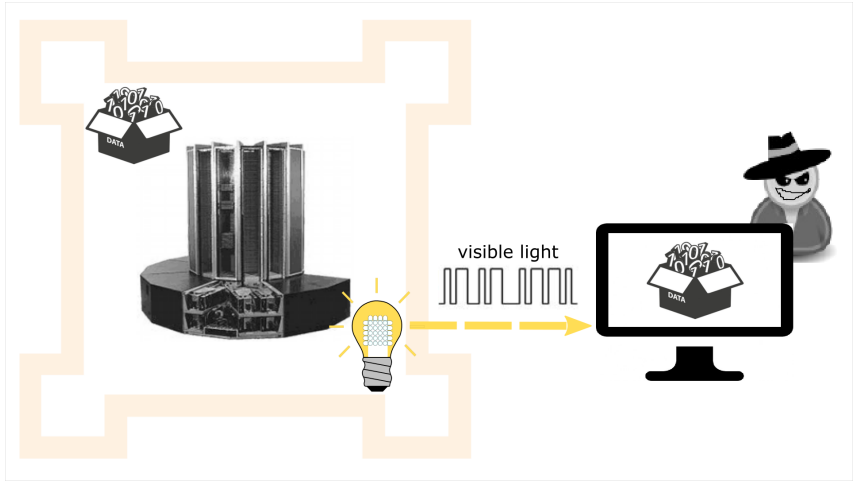


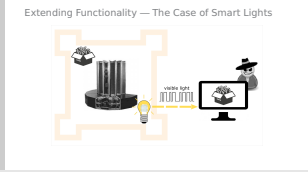


30s

Interesting because light is often the only part of the EM-spectrum that is allowed to leave air-gapped systems.

Extending Functionality — The Case of Smart Lights





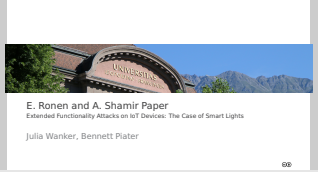
30s

Interesting because light is often the only part of the EM-spectrum that is allowed to leave air-gapped systems.

E. Ronen and A. Shamir Paper

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

Julia Wanker, Bennett Piater



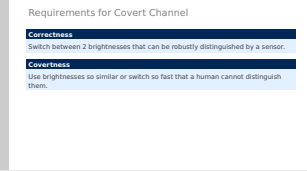
Requirements for Covert Channel

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) [RSWO18]

How (smart) LEDs Work

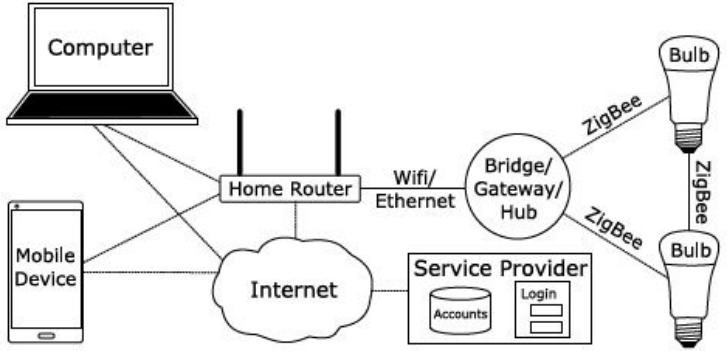


Figure: System architecture of a ZLL-based connected lighting system with two bulbs [1]

[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

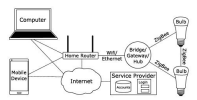


Figure: System architecture of a ZLL-based connected lighting system with two bulbs [1]

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

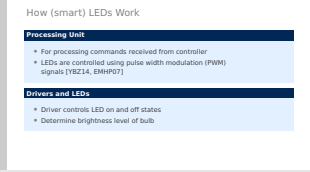
How (smart) LEDs Work

Processing Unit

- For processing commands received from controller
- LEDs are controlled using pulse width modulation (PWM) signals [YBZ14, EMHP07]

Drivers and LEDs

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



How (smart) LEDs Work

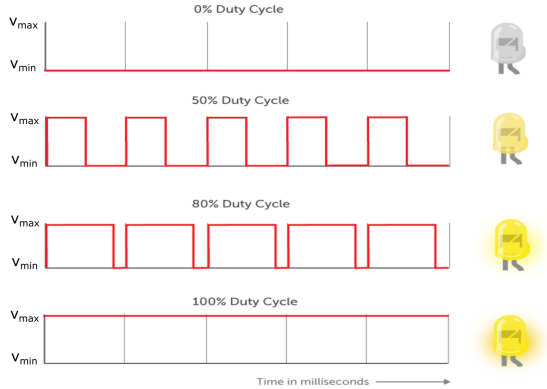
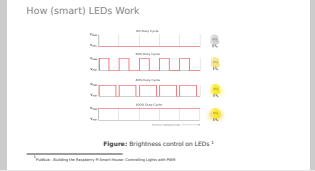
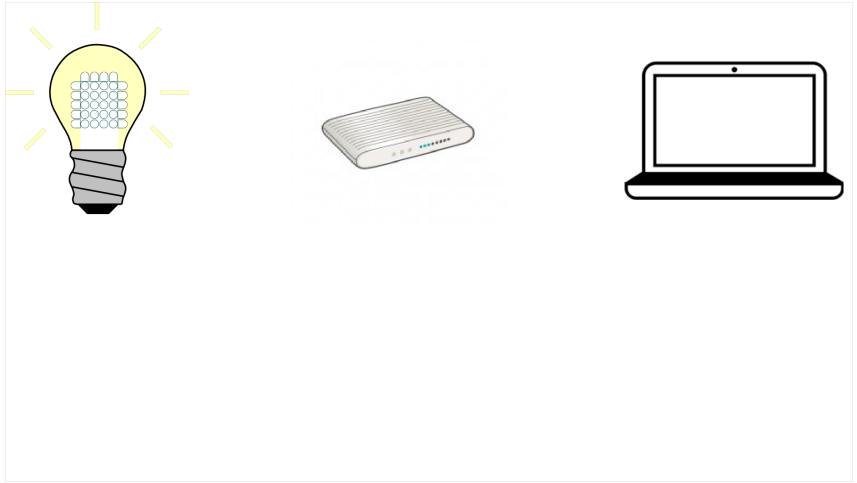


Figure: Brightness control on LEDs [1]

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

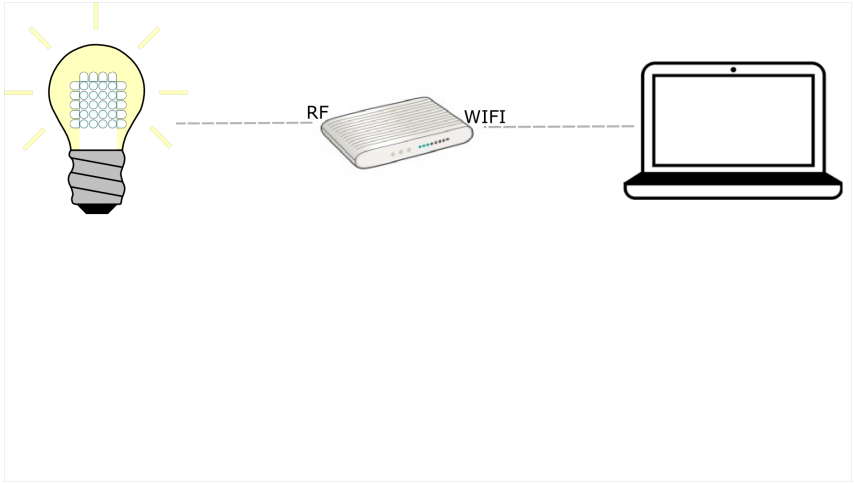


Encoding: Access Controller



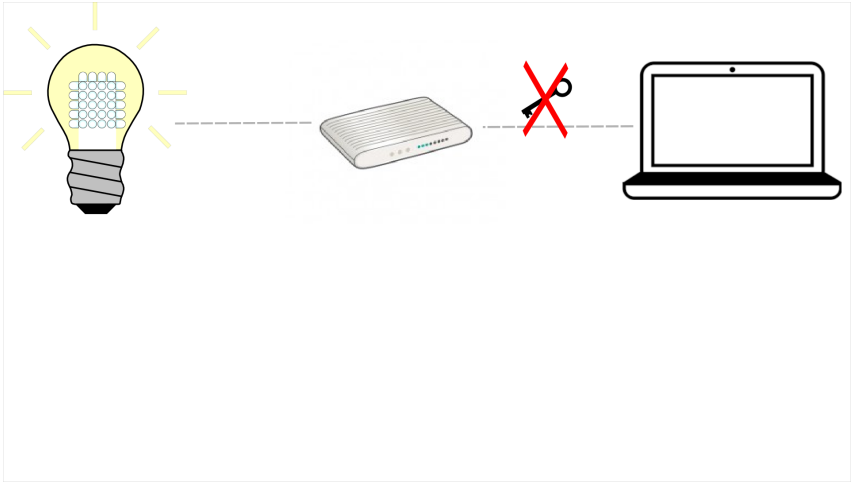
Encoding: Access Controller

Encoding: Access Controller



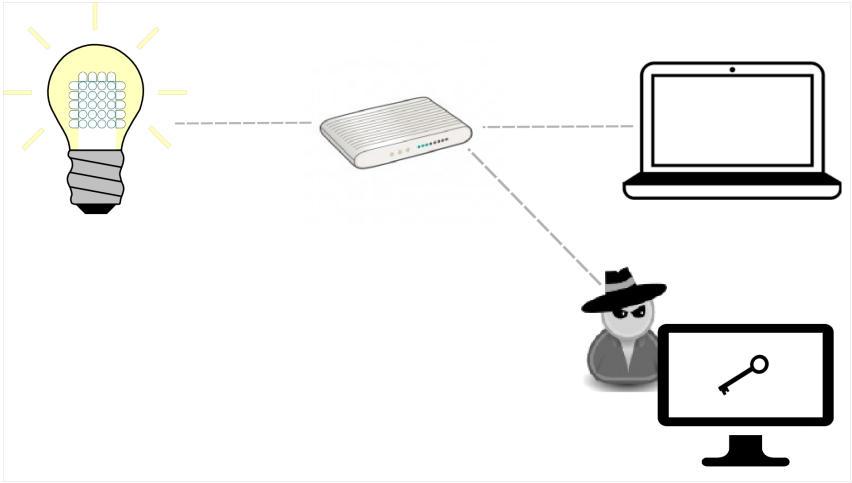
Encoding: Access Controller

Encoding: Access Controller

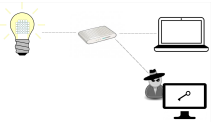


Encoding: Access Controller

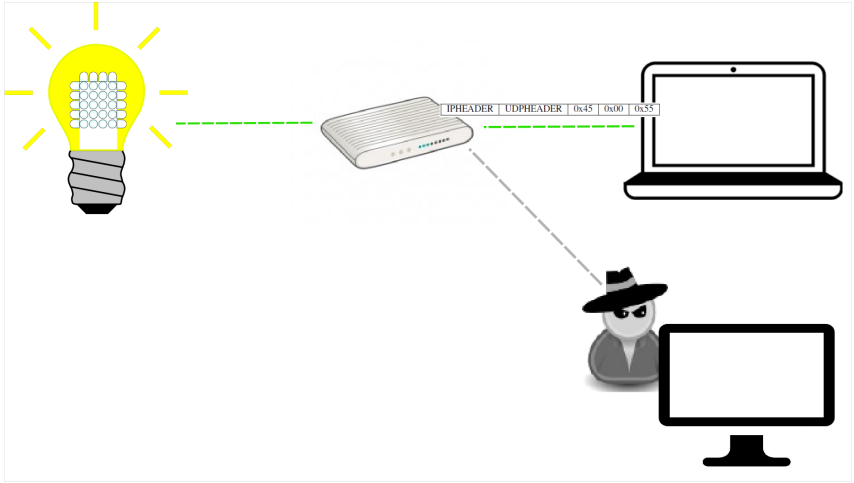
Encoding: Access Controller

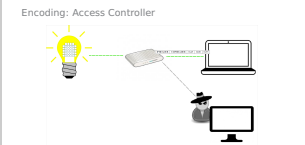


Encoding: Access Controller

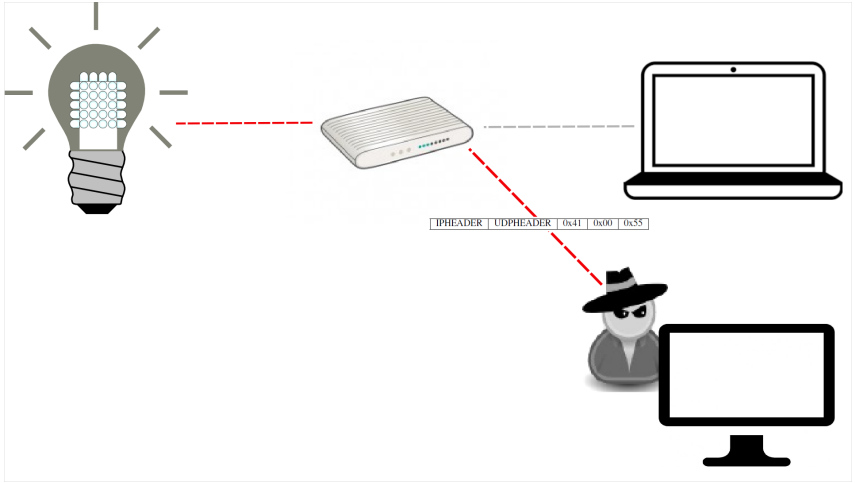


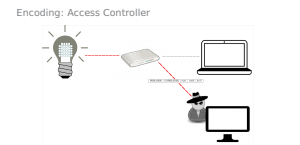
Encoding: Access Controller





Encoding: Access Controller





Encoding: Crafting of PWM Signals

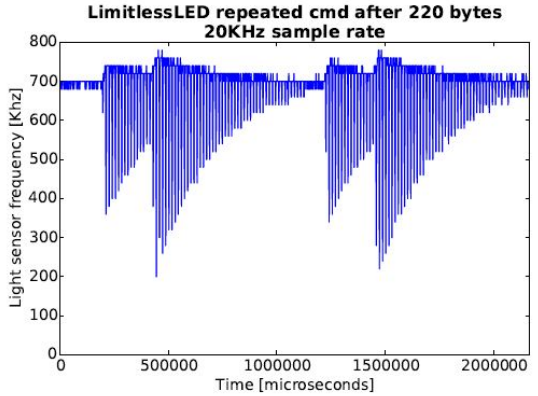
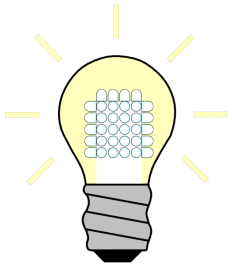


Figure: Smooth control of PWM duty cycle [2]

[2] Ronen and Shamir. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights

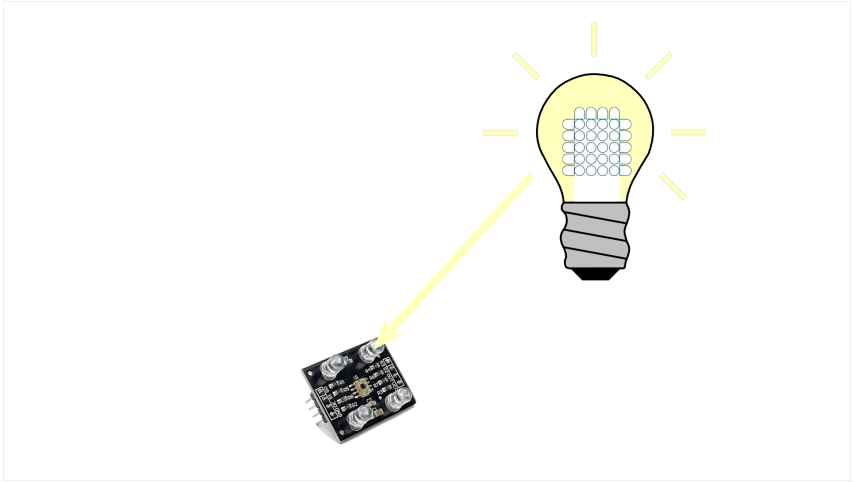
Encoding: Crafting of PWM Signals

Decoding: Light Sensor Signal Analysis



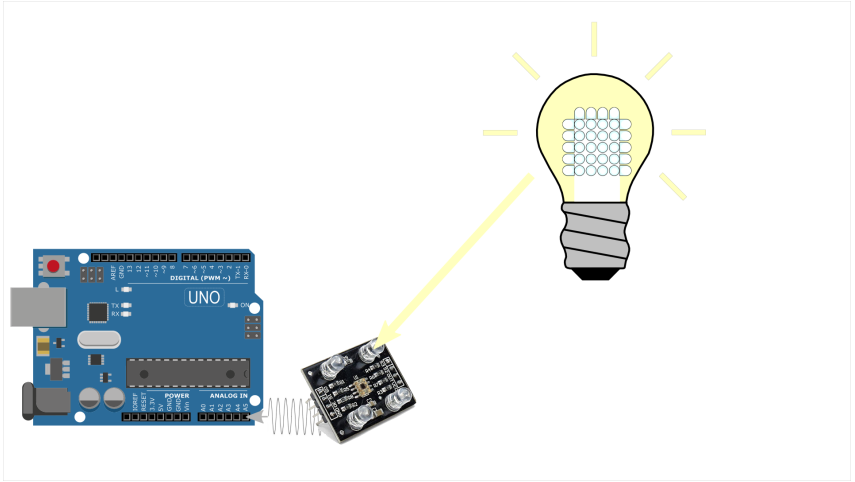
Decoding: Light Sensor Signal Analysis

Decoding: Light Sensor Signal Analysis

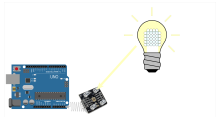


Decoding: Light Sensor Signal Analysis

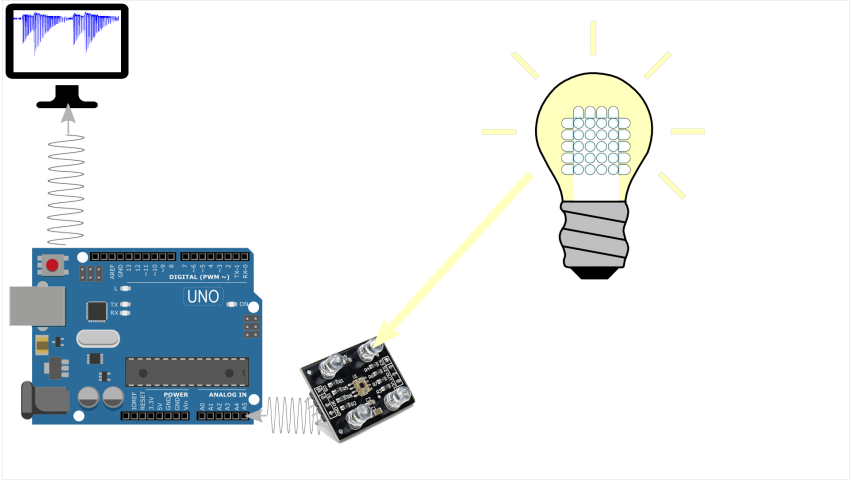
Decoding: Light Sensor Signal Analysis

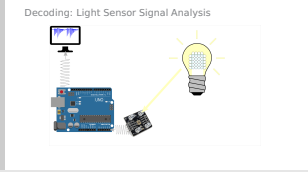


Decoding: Light Sensor Signal Analysis

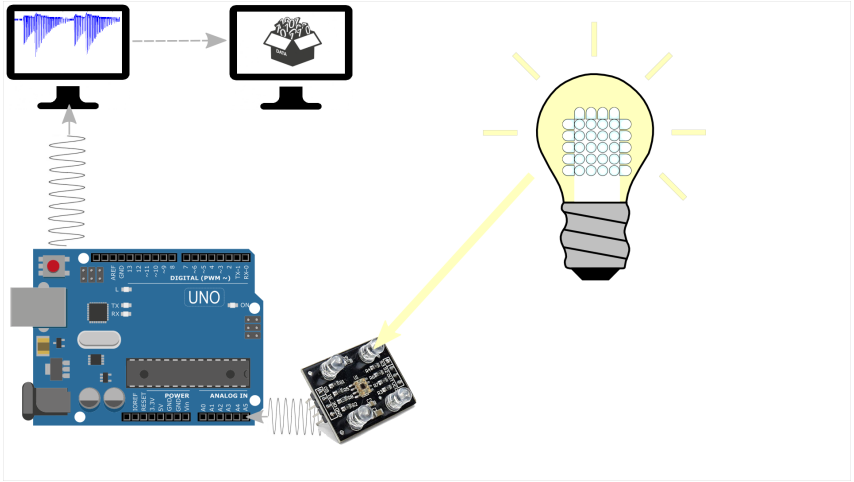


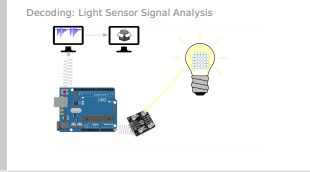
Decoding: Light Sensor Signal Analysis





Decoding: Light Sensor Signal Analysis





Why this Paper is Important for our Topic

The One and Only

- Cluster IoT attacks in presented fashion
- Functionality extension attack
- Covert Channel on IoT light bulb

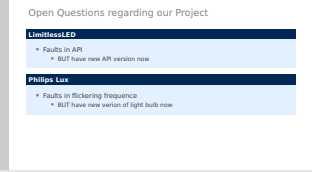
Open Questions regarding our Project

LimitlessLED

- Faults in API
  - BUT have new API version now

Philips Lux

- Faults in flickering frequence
  - BUT have new verion of light bulb now



Questions?

Julia Wanker, Bennett Piater

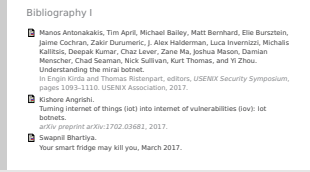
Questions?
Julia Wanker, Bennett Piater

Bibliography I

Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou.
Understanding the mirai botnet.
In Engin Kirda and Thomas Ristenpart, editors, *USENIX Security Symposium*, pages 1093–1110. USENIX Association, 2017.

Kishore Angrishi.
Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets.
arXiv preprint arXiv:1702.03681, 2017.

Swapnil Bhartiya.
Your smart fridge may kill you, March 2017.



Bibliography II

- Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi.
  Analysis of ddos-capable iot malwares.
  In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *FedCSIS*, pages 807–816, 2017.
- Nitesh Dhanjani.
  Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system.
  2013.
- H. Elgala, R. Mesleh, H. Haas, and B. Pricope.
  Ofdm visible light wireless communication based on white leds.
  In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pages 2185–2189, April 2007.

Bibliography II
Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. Analysis of ddos-capable iot malwares. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *FedCSIS*, pages 807–816, 2017.
Nitesh Dhanjani. Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system. 2013.
H. Elgala, R. Mesleh, H. Haas, and B. Pricope. Ofdm visible light wireless communication based on white leds. In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pages 2185–2189, April 2007.

Bibliography III

- Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici.
  xled: Covert data exfiltration from air-gapped networks via router leds, June 2017.
- Eyal Ronen and Adi Shamir.
  Extended functionality attacks on iot devices: The case of smart lights.
  In *EuroS&P*, pages 3–12. IEEE, 2016.
- Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn.
  Iot goes nuclear: Creating a zigbee chain reaction.
  IEEE Security & Privacy, 16(1):54–62, 2018.
- Z. Yu, R. J. Baxley, and G. T. Zhou.
  Brightness control in dynamic range constrained visible light ofdm systems, January 2014.

Bibliography III
Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. xled: Covert data exfiltration from air-gapped networks via router leds, June 2017.
Eyal Ronen and Adi Shamir. Extended functionality attacks on iot devices: The case of smart lights. In EuroS&P, pages 3–12. IEEE, 2016.
Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. Iot goes nuclear: Creating a zigbee chain reaction. IEEE Security & Privacy, 16(1):54–62, 2018.
Z. Yu, R. J. Baxley, and G. T. Zhou. Brightness control in dynamic range constrained visible light ofdm systems, January 2014.