universität innsbruck

IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

universität innsbruck

Topic Relevance

New Attack Vectors on IoT Devices

Julia Wanker, Bennett Piater

IoT Security in General

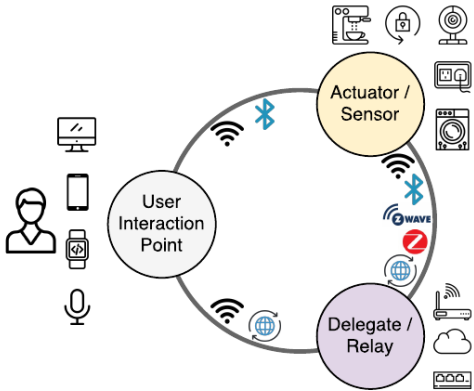


Figure: Infrastructure of IoT ecosystem [1]

[1] Zhan et. al. Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be

IoT Security in General

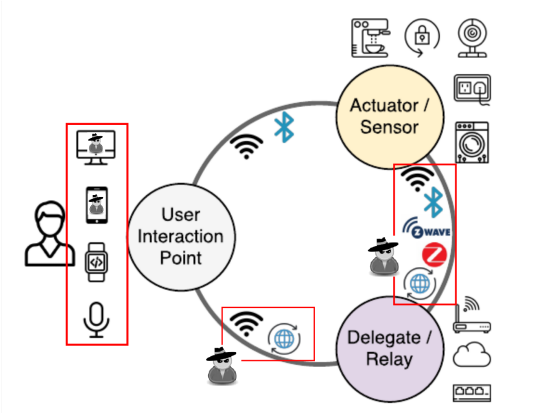


Figure: Attack Vectors in IoT ecosystem[2]

[2] Zhan et. al. Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be / *edited*

Smart Light Security

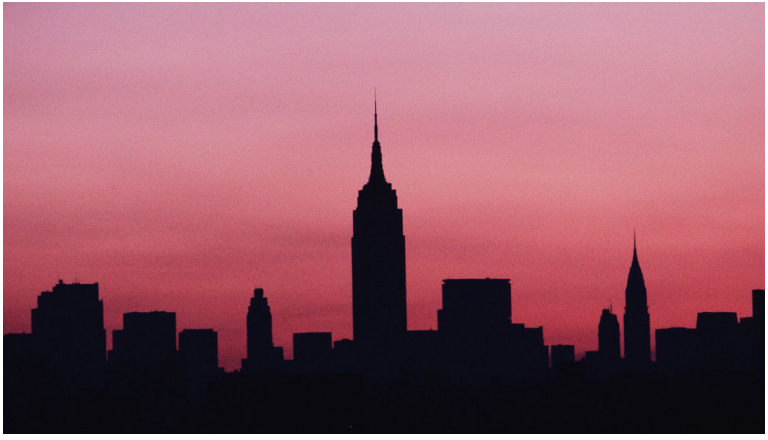
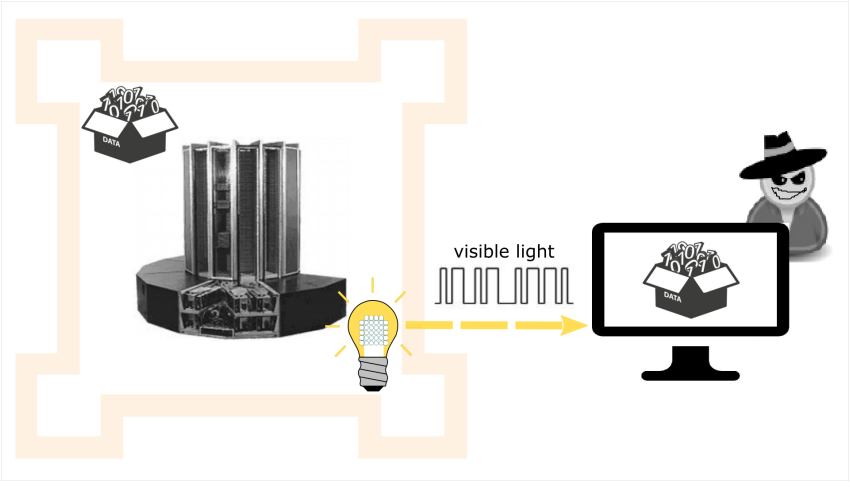


Figure: NYC Blackout of 1977[3]

[3] Allan Tannenbaum/Getty Images

Extending Functionality



Theoretical Background

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

Communication With Lights

General Light Communication

- Change PWM signal
- **Off** period represents logical **0**
- **On** period represents logical **1**

Smart Light Communication

- Send close brightness change commands, distinguish using PWM
- **Lower level** represents logical **0**
- **Higher level** represents logical **1**

(Covert) Communication With Lights

Covertness

- Flicker at a rate above 60 Hz or use close brightness commands
- Detectable by sensor but not seen by human eye

Smart Light Systems

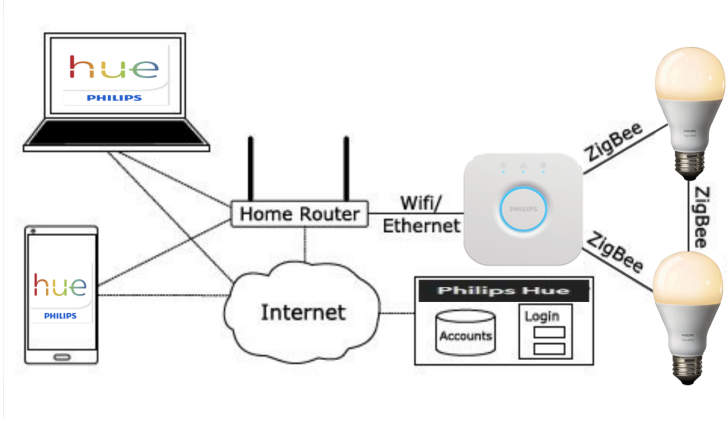


Figure: System architecture of a Philips Hue connected lighting system with two bulbs[4]

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

Experiment

Covert Communication Channel on Philips Hue White

Julia Wanker, Bennett Piater

Controlling the Light

We use the Hue API for simplicity.

- Bridge controls light via ZLL
- We interface with REST-API on bridge

Controlling the Light

We use the Hue API for simplicity.

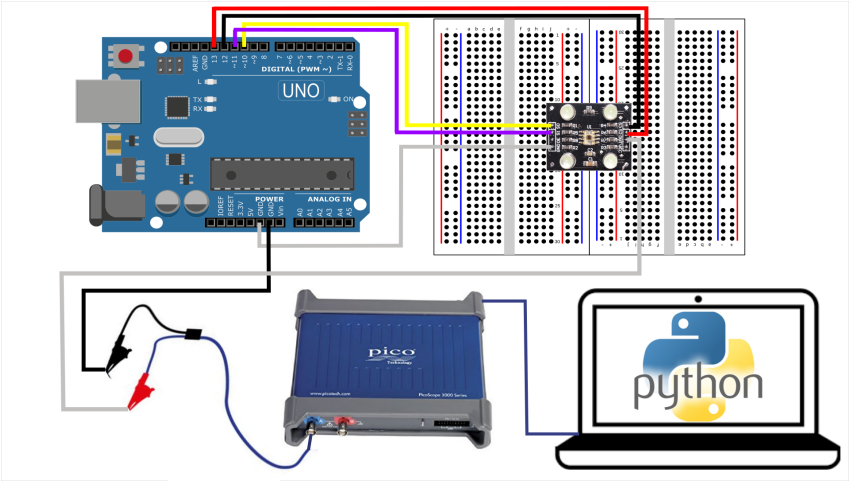
- Bridge controls light via ZLL
- We interface with REST-API on bridge

Limitations

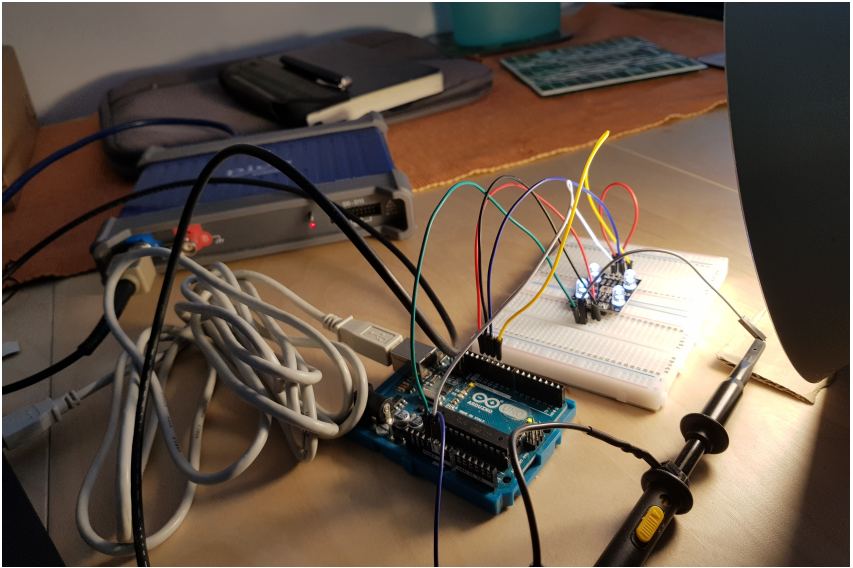
- Rate limit due to throttling by bridge?
- Automatic fading by the bridge or light (no phase shifts!)

May be worked around some by speaking ZLL directly?

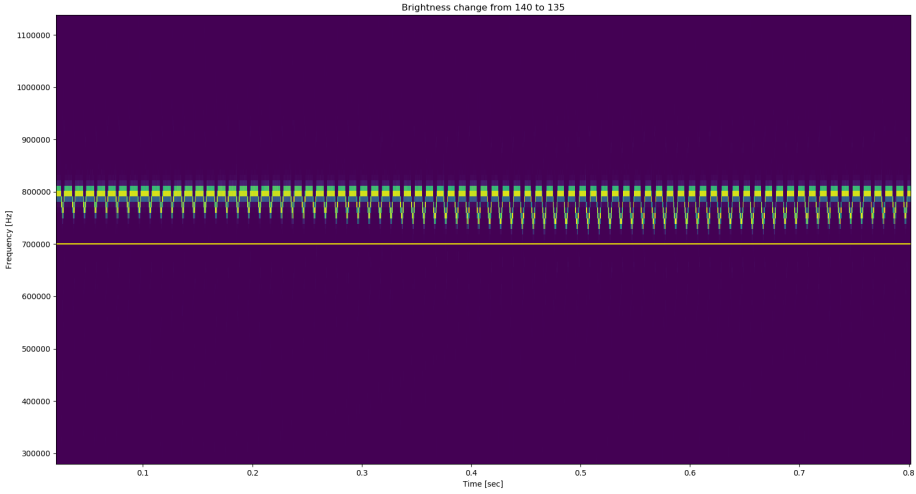
Overview



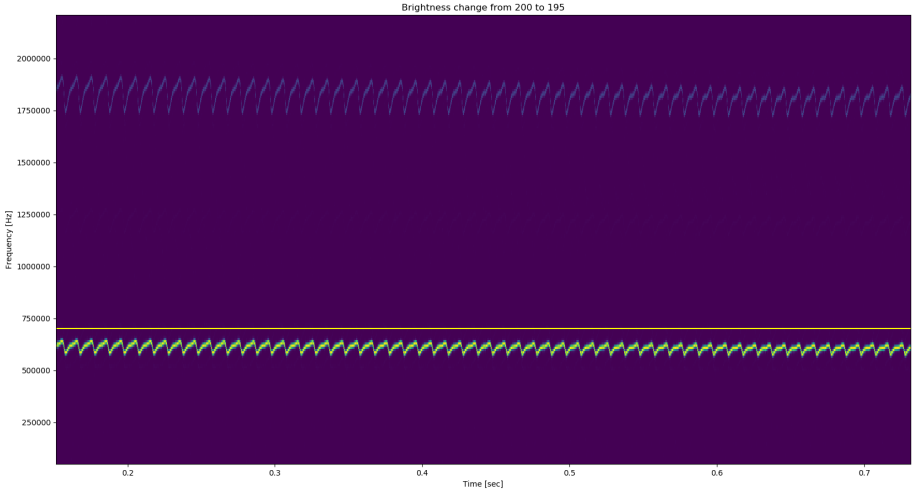
Experimental Setup



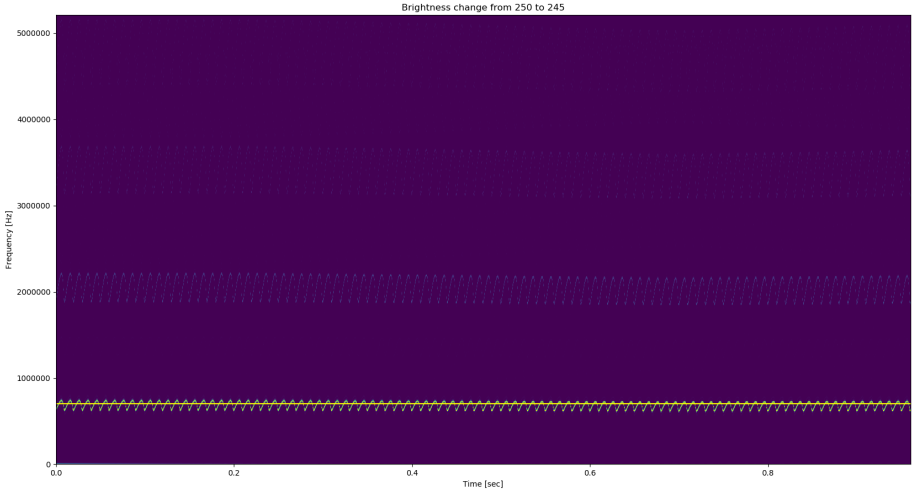
Some Results I



Some Results II



Some Results III



Demonstration

Covert Communication Channel on Philips Hue White

Julia Wanker, Bennett Piater

Conclusion

Summary and Outlook

Julia Wanker, Bennett Piater

Conclusion

Successes

- We can distinguish brightness differences invisible to the human eye
- We *think that we can* see the PWM, not just brightness

$\rightarrow$ Research from Ronen and Shamir [2016] reproduced in principle.

Conclusion

Successes

- We can distinguish brightness differences invisible to the human eye
- We *think that we can* see the PWM, not just brightness

$\rightarrow$ Research from Ronen and Shamir [2016] reproduced in principle.

Failures

Automating this is hard:

- Very high variance in our measurements
- Much trial and error to obtain a good picture
- Limited range and robustness to lighting conditions

Outlook

An automated covert channel could in principle be built using this technique.

Important Lessons

- Connected LEDs should not be trusted in secure areas
- Smart lights should not have this many brightness levels. Fading and throttling improve their security a little though.
- . . . combine this demo with the insecurity of IoT devices for maximum effect.
- Alternatively, if you must use smart lights, isolate and secure them as much as possible.

Questions?

Julia Wanker, Bennett Piater

Bibliography I

E. Ronen and A. Shamir. Extended functionality attacks on iot devices: The case of smart lights. In *EuroS&P*, pages 3–12. IEEE, 2016. ISBN 978-1-5090-1752-2. URL http://dblp.uni-trier.de/db/conf/eurosp/eurosp2016.html#RonenS16;http://dx.doi.org/10.1109/EuroSP.2016.13;http://www.bibsonomy.org/bibtex/21ec9f74336617b4511304c4b35818c79/dblp.