universität
innsbruck

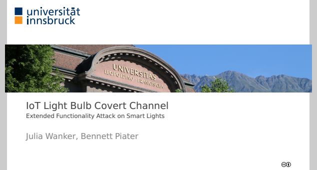
IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

2018-06-14

IoT Light Bulb Attack
└─title

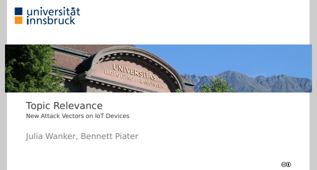


universität innsbruck

Topic Relevance

New Attack Vectors on IoT Devices

Julia Wanker, Bennett Piater



IoT Security in General

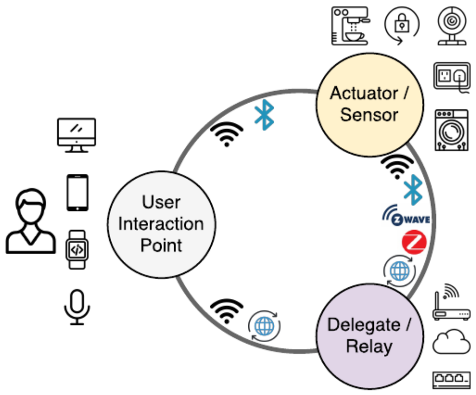
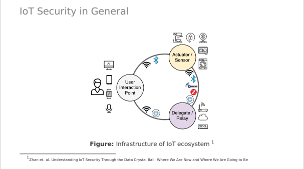


Figure: Infrastructure of IoT ecosystem [1]

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

2018-06-14

Topic Relevance
└Topic Relevance
 └IoT Security in General
  └IoT Security in General



IoT Security in General

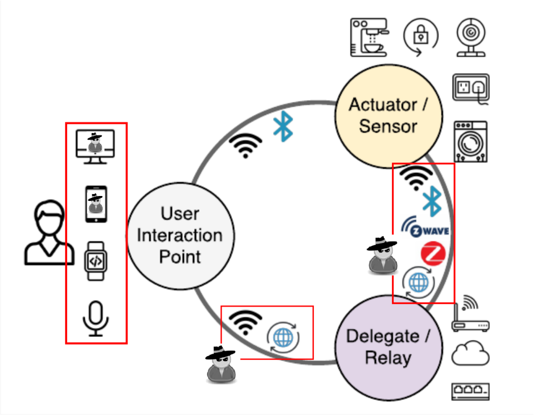
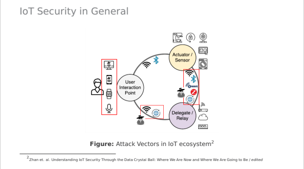


Figure: Attack Vectors in IoT ecosystem[2]

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



NETWORK SIZE -> limit in computation and energy capabilities –> skip authentication, encryption
[HUMANS tightly involved –> attacker can steal this sensitive info -> access control and privacy
HETEROGINITY -> bulk of protocols co-exist –> need overall valid solution]

Smart Light Security

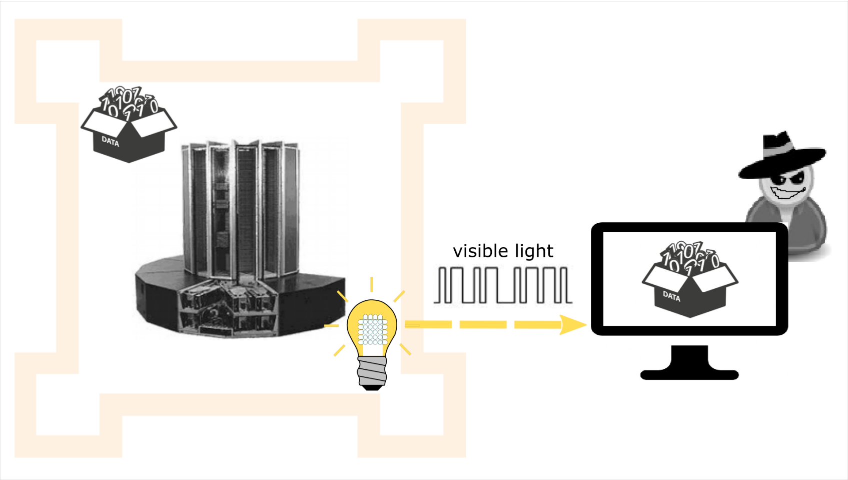
Figure: NYC Blackout of 1977[3]

[3] Allan Tannenbaum/Getty Images

ubiquity

reminder: spread malware over whole city

Extending Functionality



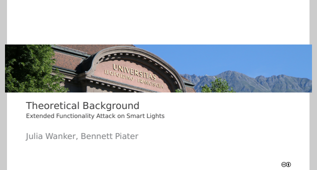
our focus

remember: steal info through light communication

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**

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**

based on LEDs turned on and off at high rate –> pulse width changed according to data

smart light: not directly change PWM –> indirectly through brightness commands

(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

(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

change between two brightnesses at high rate -> reminder: human eye threshold

cannot change PWM –> choose two close brightnesses

[Hue 255 levels]

Smart Light Systems

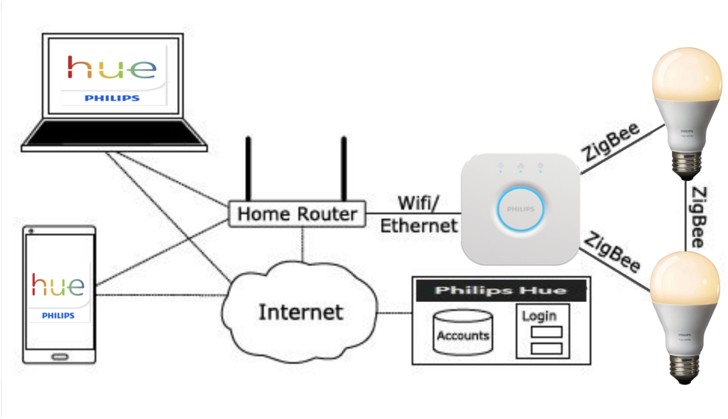
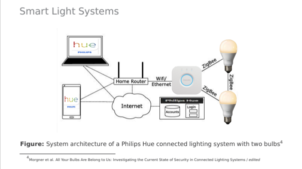


Figure: System architecture of a Philips Hue connected lighting system with two bulbs[4]

[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

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

limits we met du to communication over bridge:
(x) restrictions on rate of commands sent in system –> restricts our transmission speed

(x) brightness increased incrementally -> avoid sharp changes –>

thus cannot see phase shifts

Controlling the Light

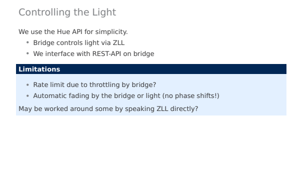
We use the Hue API for simplicity.

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

Limitations

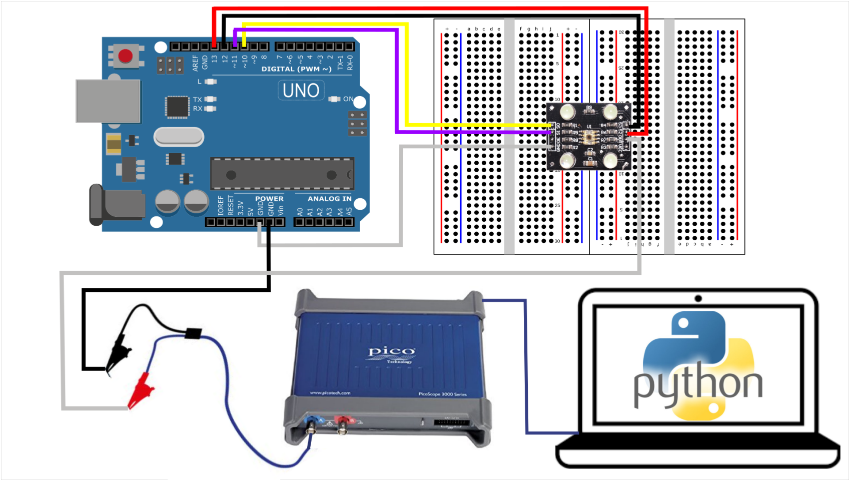
- Rate limit due to throttling by bridge?
- Automatic fading by the bridge or light (no phase shifts!)

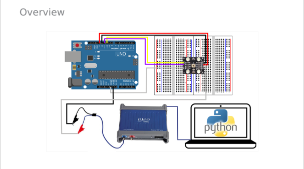
May be worked around some by speaking ZLL directly?



limits we met du to communication over bridge:
(x) restrictions on rate of commands sent in system –> restricts our transmission speed
(x) brightness increased incrementally -> avoid sharp changes –> thus cannot see phase shifts

Overview





Arduino serves as power supply + setup light sensor

sensor frequency output sent to picoscope

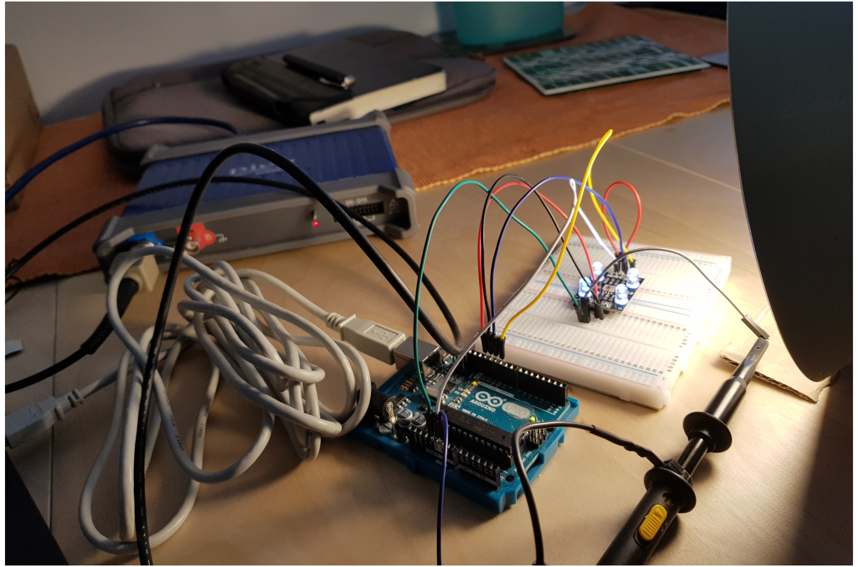
sennsor frequency: 800 kHz -> pico samples at 10 MHz

python read out frequency output from pico

do stft to get phase content of sections of signal since changes over time

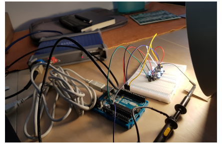
plot to check

Experimental Setup

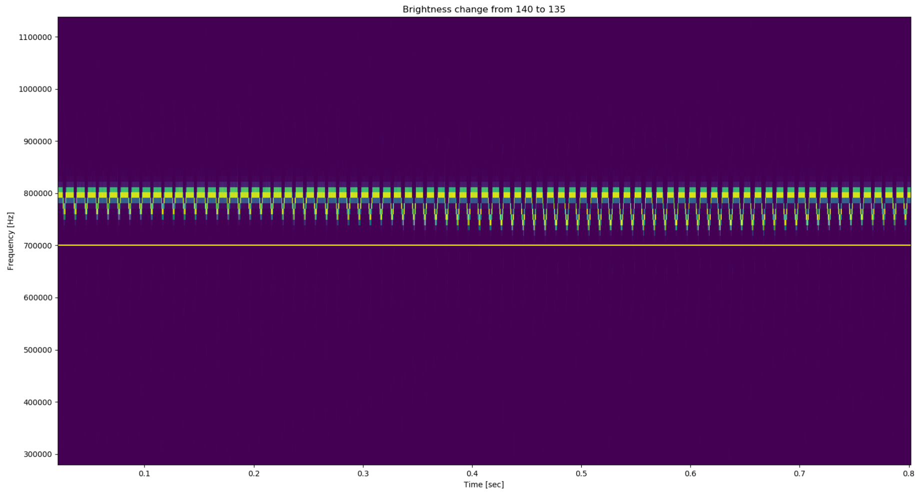


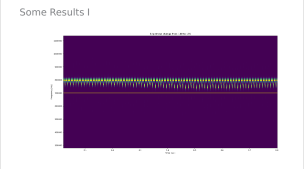
2018-06-14

Experimental Setup



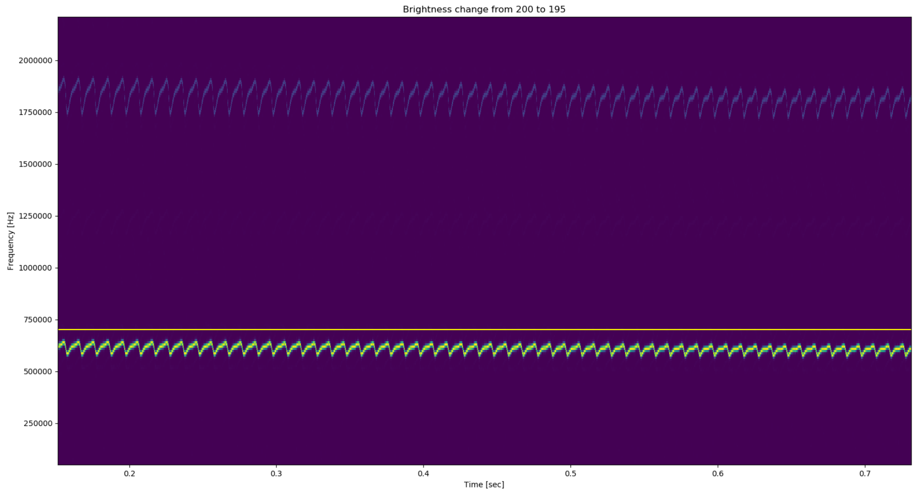
Some Results I

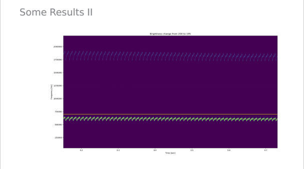




2m for the 3 images

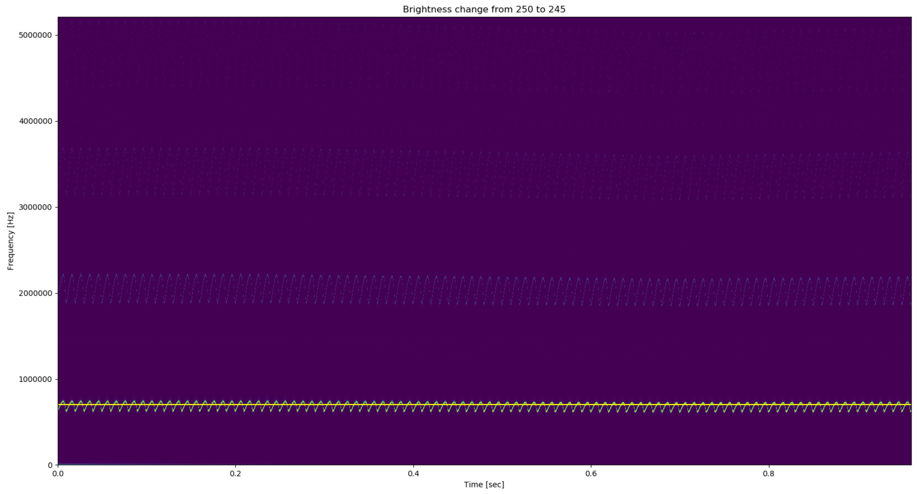
Some Results II

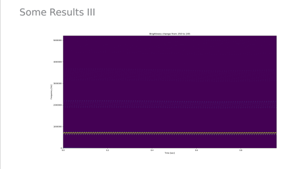




2m for the 3 images

Some Results III



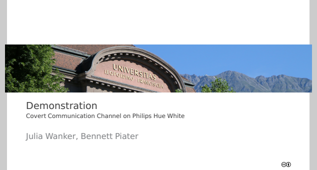


2m for the 3 images

Demonstration

Covert Communication Channel on Philips Hue White

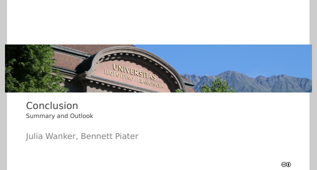
Julia Wanker, Bennett Piater



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

→ 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
→ Research from Ronen and Shamir [2016] reproduced in principle.

1.5–2m

Improvements for our project:

- Good channel encoding
- More robust PWM detection
- Higher range
- Automatic calibration

Conclusion

Successes

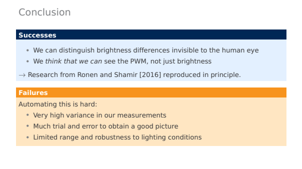
- We can distinguish brightness differences invisible to the human eye
- We *think that we can* see the PWM, not just brightness

→ 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



1.5–2m

Improvements for our project:

- Good channel encoding
- More robust PWM detection
- Higher range
- Automatic calibration

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.

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.

1m

Questions?

Julia Wanker, Bennett Piater

2018-06-14

Questions?
└─Questions

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`.

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`.