



IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



2018-06-14

IoT Light Bulb Attack

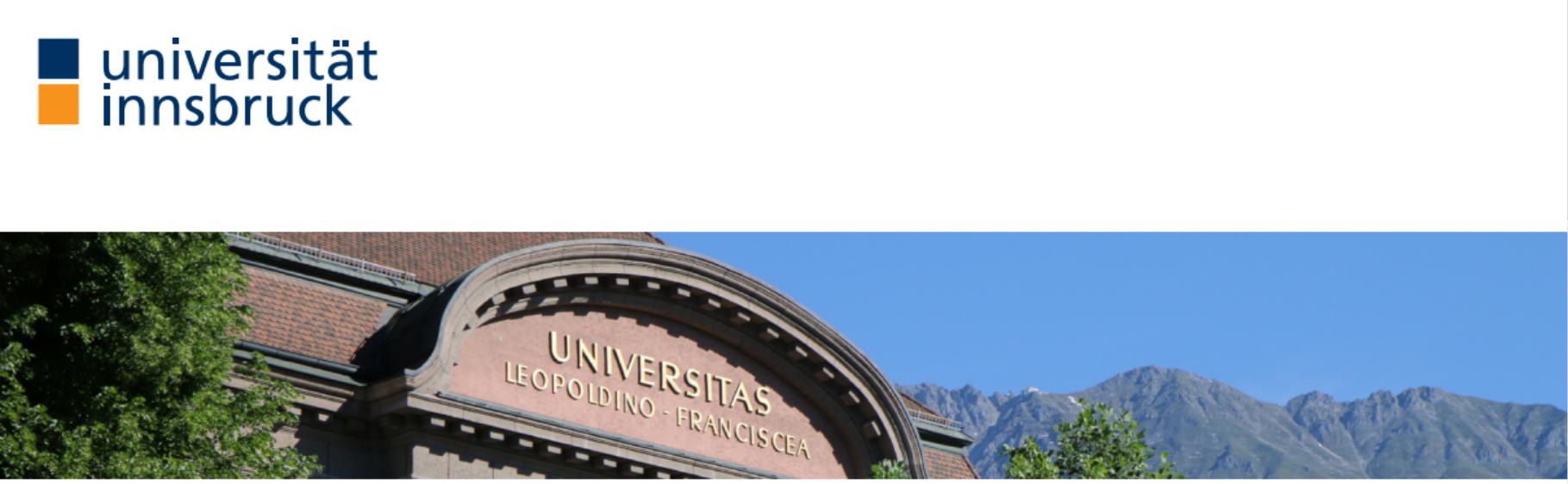
- title



IoT Light Bulb Covert Channel
Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

ee



Topic Relevance

New Attack Vectors on IoT Devices

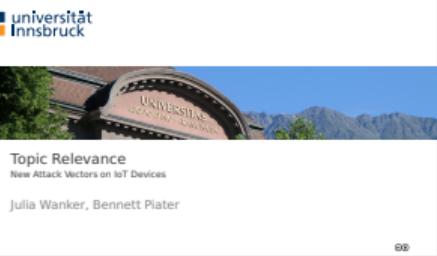
Julia Wanker, Bennett Piater



2018-06-14

Topic Relevance
└ Topic Relevance

universität
Innsbruck



IoT Security in General

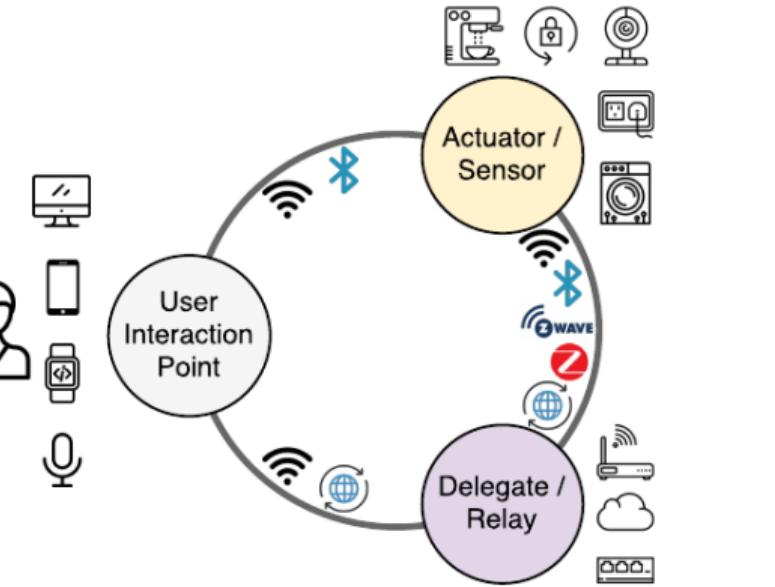
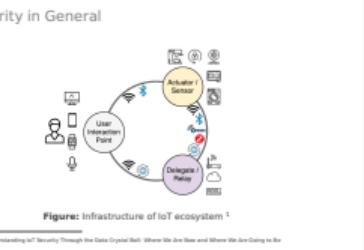


Figure: Infrastructure of IoT ecosystem ¹

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

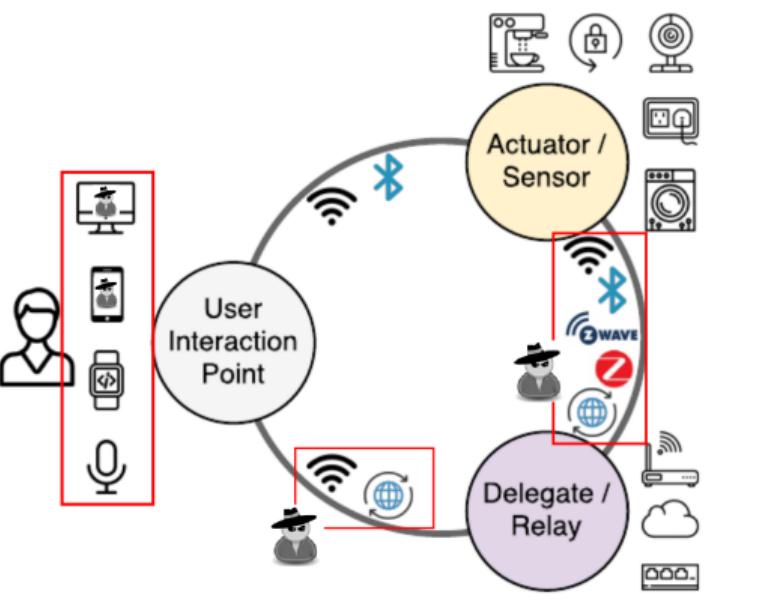


Figure: Attack Vectors in IoT ecosystem²

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

2018-06-14

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

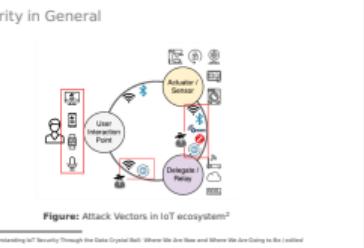


Figure: Attack Vectors in IoT ecosystem²

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
HETEROGENITY -> bulk of protocols co-exist -> need overall valid
solution]

Smart Light Security



Figure: NYC Blackout of 1977³

³Allan Tannenbaum/Getty Images

2

Topic Relevance
└ Topic Relevance
 └ Smart Light Security
 └ Smart Light Security

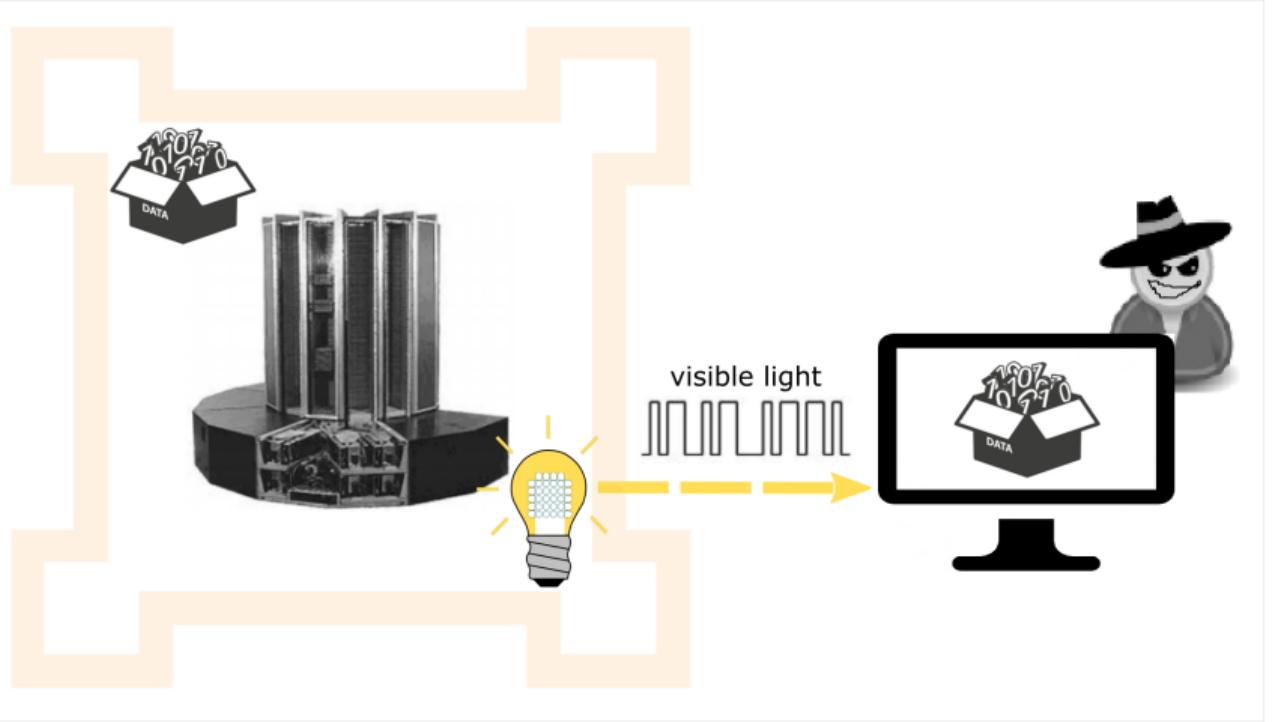
ubiquity

reminder: spread malware over whole city

Smart Light Security



Extending Functionality



2018-06-14

Topic Relevance
└ Topic Relevance
 └ Smart Light Security
 └ Extending Functionality

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

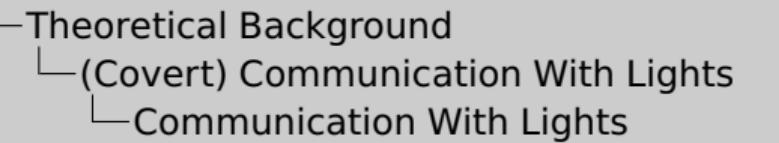
- Change PWM signal
- **Off** period represents logical **0**
- **On** period represents logical **1**

Smart Light Communication

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

4

Theoretical Background



2018-06-14

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

2018-06-14

Theoretical Background

Theoretical Background

(Covert) Communication With Lights

(Covert) Communication With Lights

(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

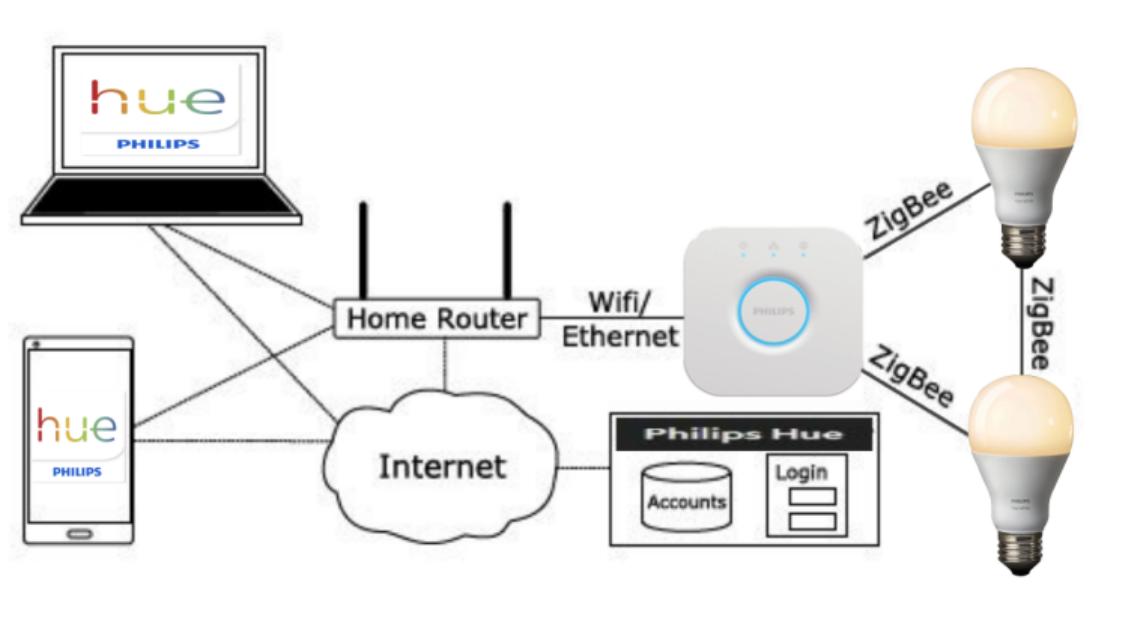
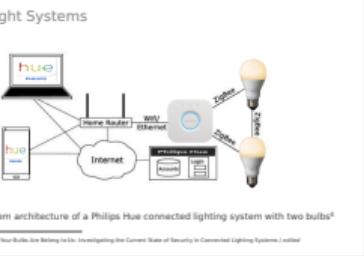


Figure: System architecture of a Philips Hue connected lighting system with two bulbs⁴

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

2018-06-14

Theoretical Background
└ Theoretical Background
└ Smart Light Systems
└ Smart Light Systems





Experiment

Covert Communication Channel on Philips Hue White

Julia Wanker, Bennett Piater



Experiment
└ Experiment

2018-06-14



Experiment
Covert Communication Channel on Philips Hue White

Julia Wanker, Bennett Piater

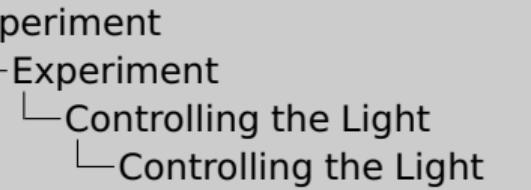
ee

Controlling the Light

We use the Hue API for simplicity.

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

2018-06-14



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 due 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.

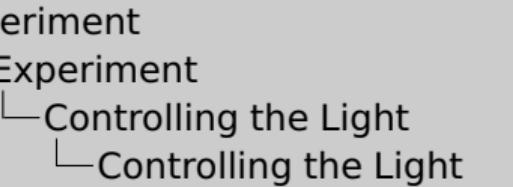
- Bridge controls light via ZLL
- We interface with REST-API on bridge

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?

2018-06-14



limits we met due 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

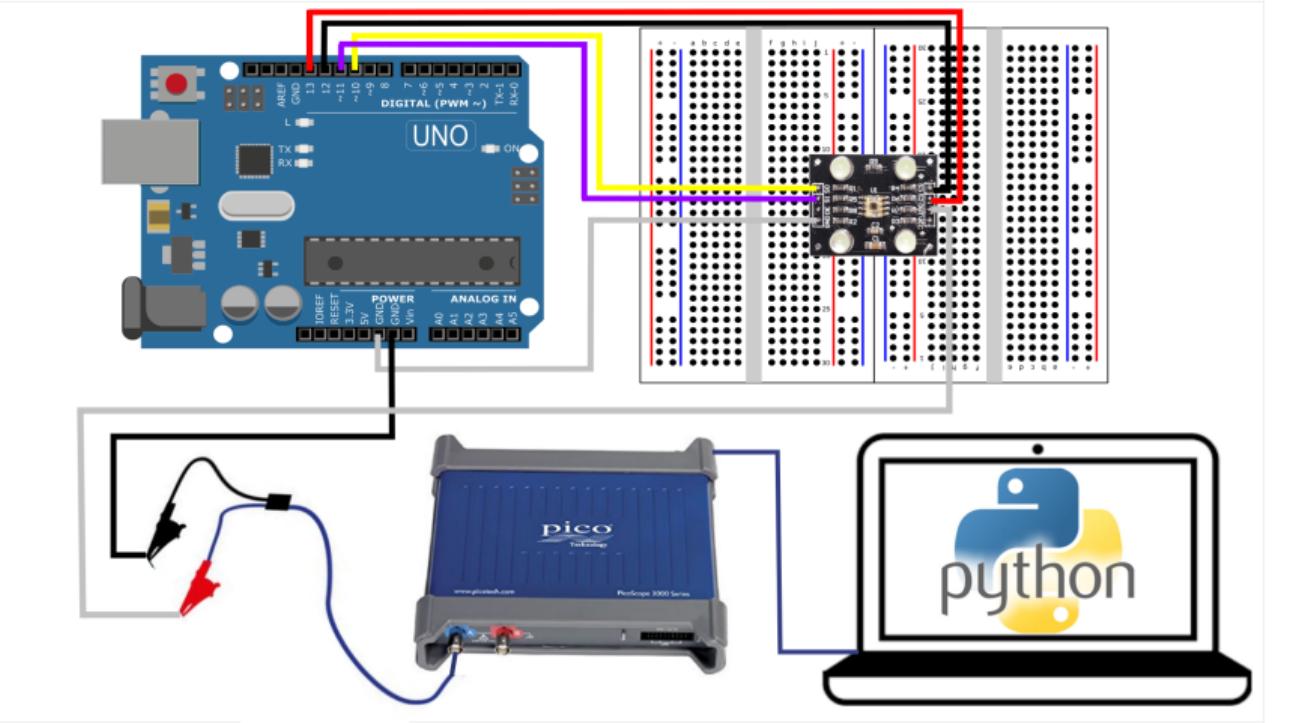
We use the Hue API for simplicity.

- * 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?

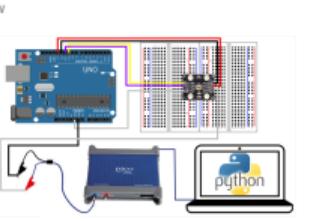
Overview



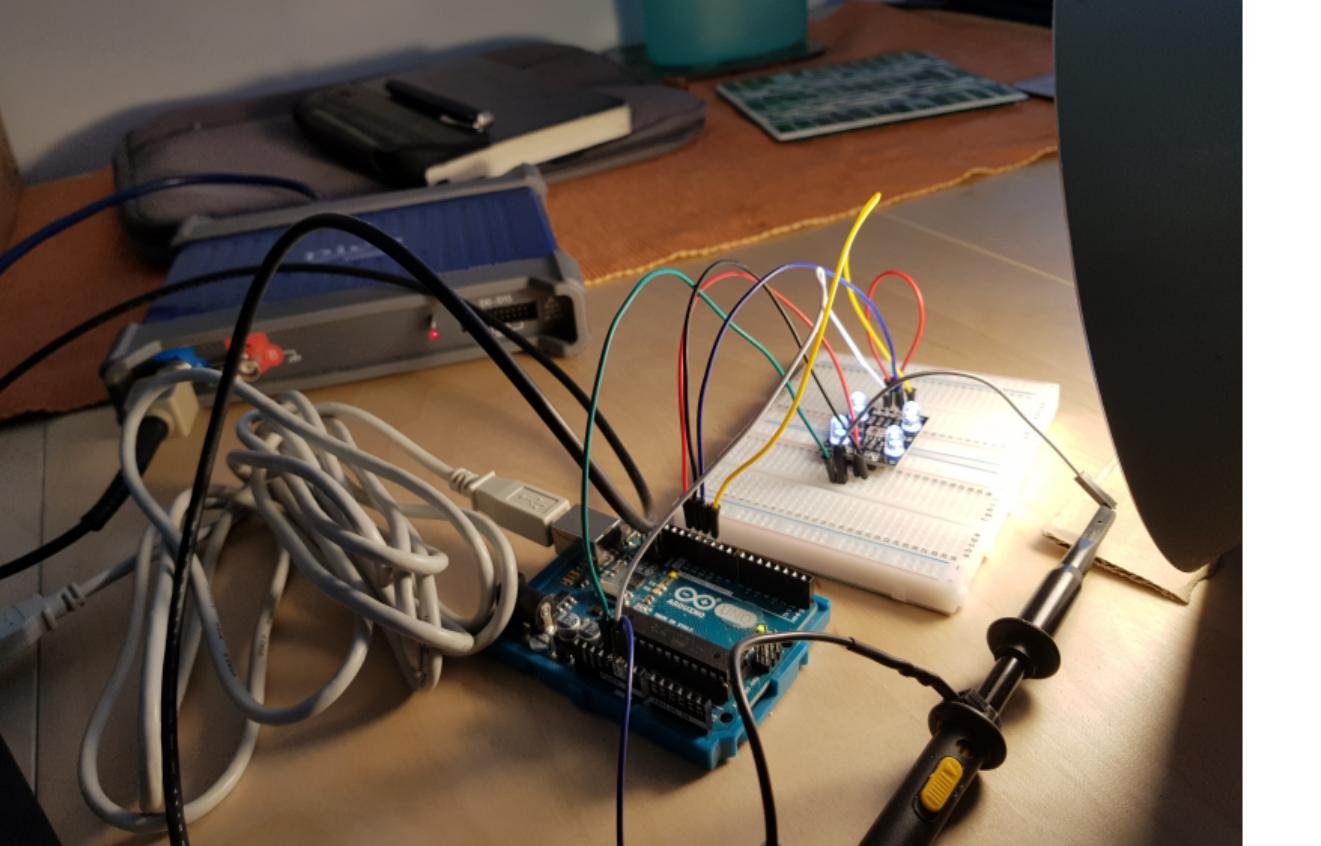
2018-06-14

Experiment
└ Experiment
 └ Experimental Setup
 └ Overview

Arduino serves as power supply + setup light sensor
sensor frequency output sent to picoscope
sensor 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



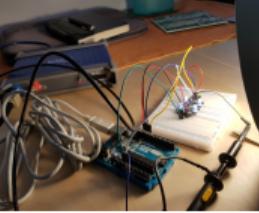
Experimental Setup



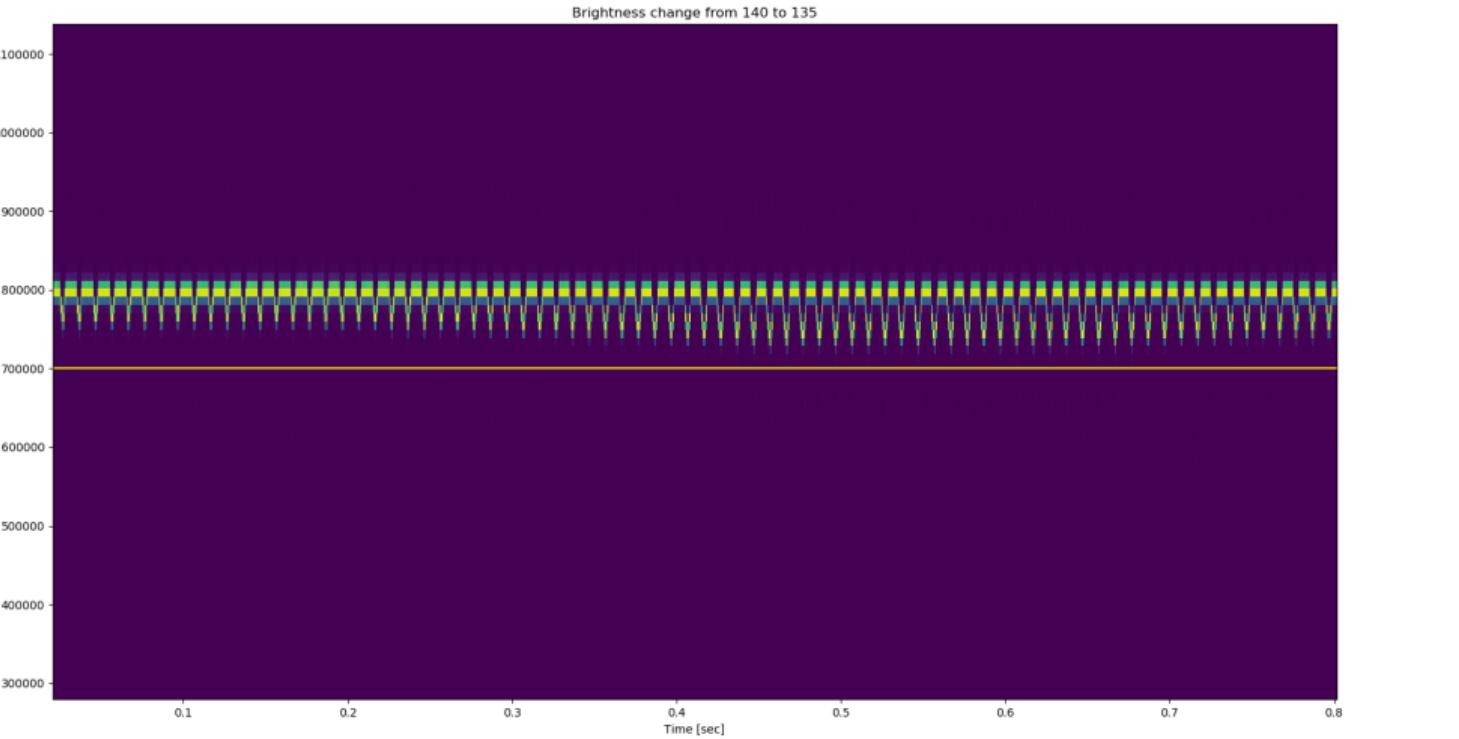
9

2018-06-14
Experiment
└ Experiment
 └ Experimental Setup
 └ Experimental Setup

Experimental Setup



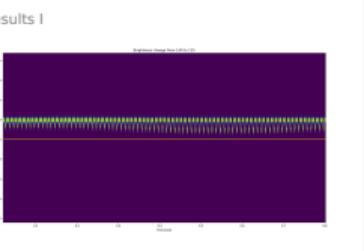
Some Results I



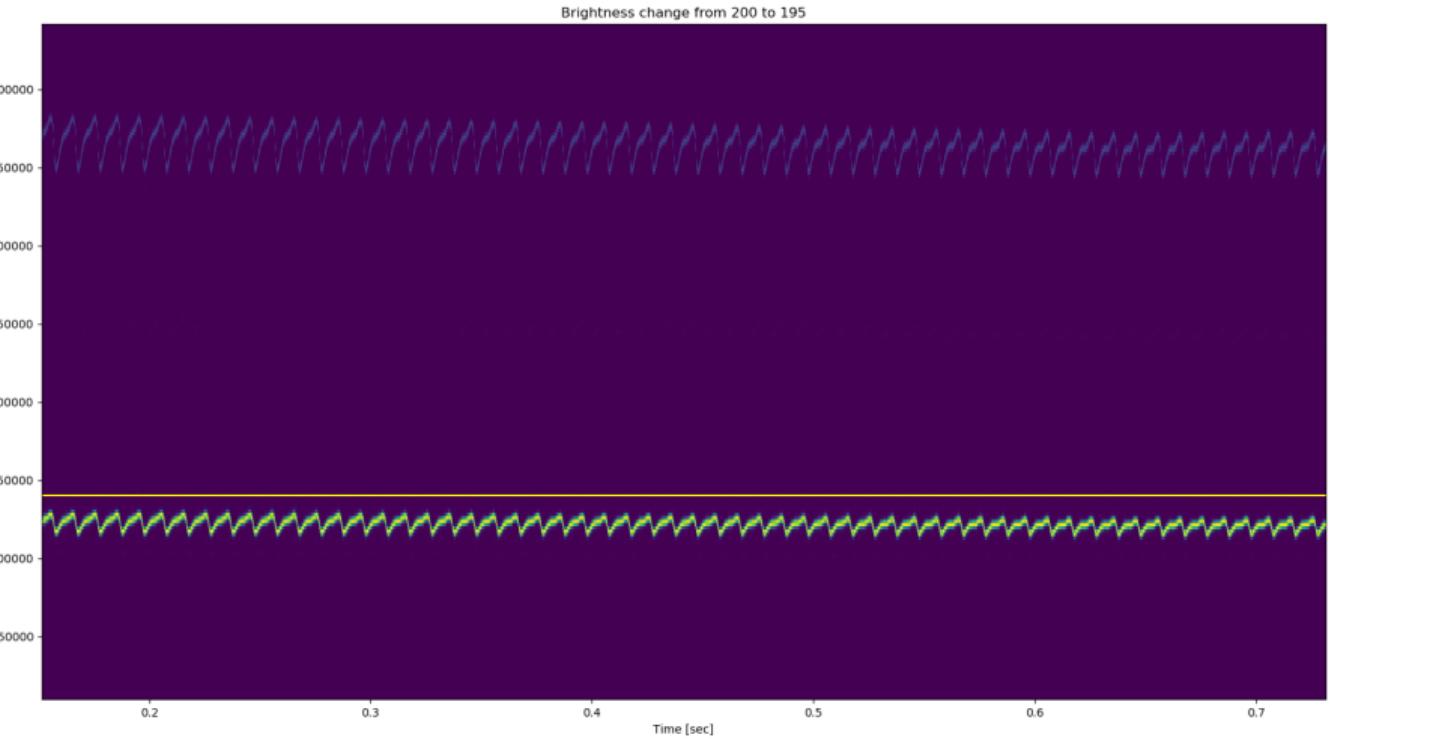
10

2018-06-14
Experiment
└ Experiment
 └ Results
 └ Some Results I

2m for the 3 images



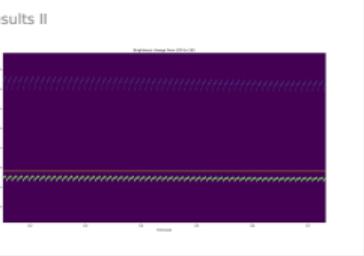
Some Results II



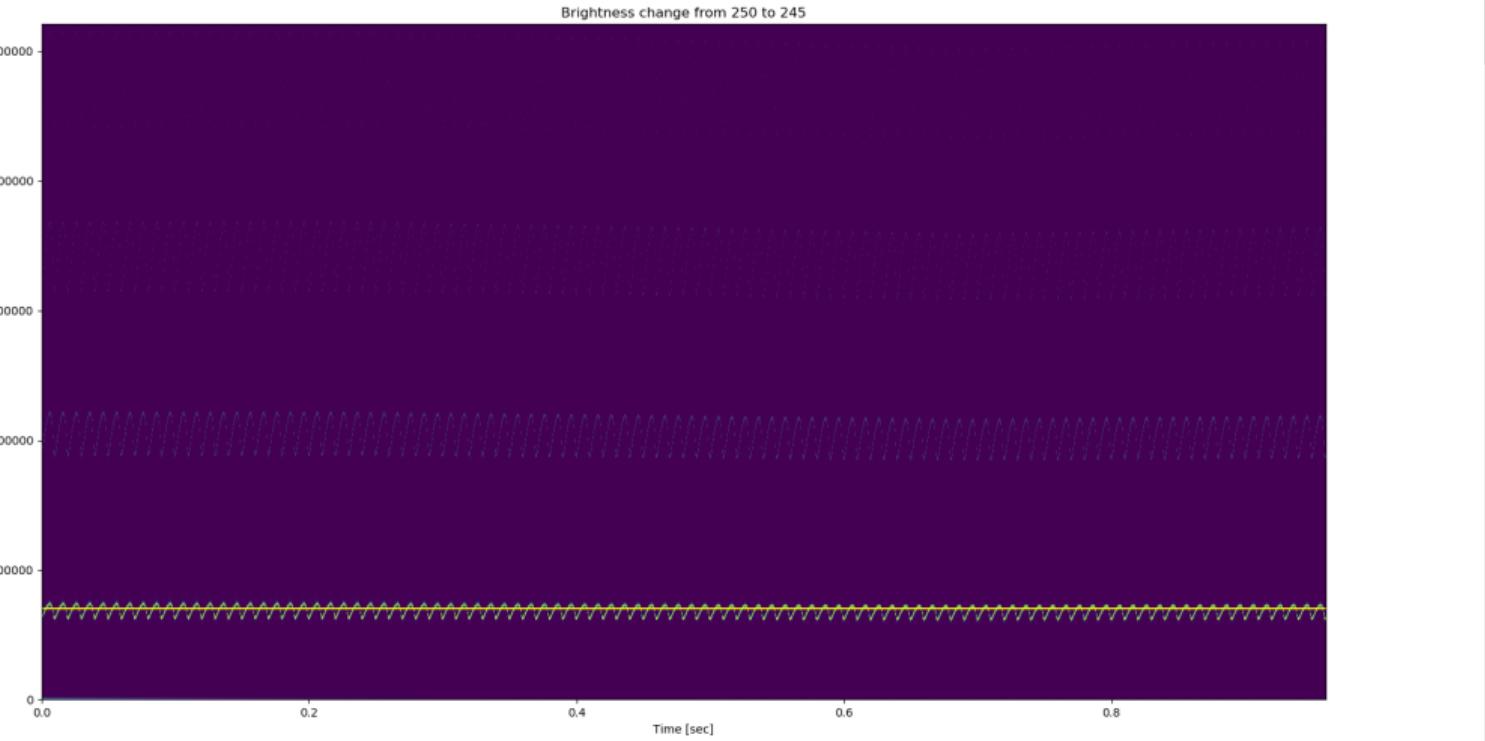
11

2018-06-14
Experiment
└ Experiment
└ Results
└ Some Results II

2m for the 3 images



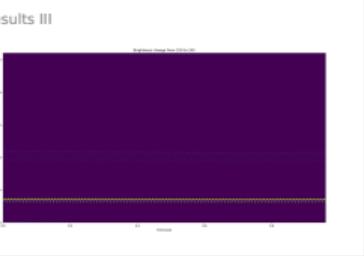
Some Results III



12

2018-06-14
Experiment
└ Experiment
└ Results
└ Some Results III

2m for the 3 images





Demonstration

Covert Communication Channel on Philips Hue White

Julia Wanker, Bennett Piater



2018-06-14

Demonstration
└ Demonstration



Demonstration
Covert Communication Channel on Philips Hue White

Julia Wanker, Bennett Piater

ee



Conclusion

Summary and Outlook

Julia Wanker, Bennett Piater



2018-06-14

Conclusion
└ Conclusion



Conclusion
Summary and Outlook
Julia Wanker, Bennett Piater

22

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.

2018-06-14

Conclusion └ Conclusion

└ Conclusion

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.

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

2018-06-14

Conclusion └ Conclusion

└ Conclusion

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

Outlook

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

Important Lessons

- 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.
- Connected LEDs should not be trusted in secure areas
- Alternatively, if you must use smart lights, isolate and secure them as much as possible.

14

Conclusion

Conclusion

Outlook

1m

Outlook

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

Important Lessons

- 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.
- Connected LEDs should not be trusted in secure areas
- Alternatively, if you must use smart lights, isolate and secure them as much as possible.



Questions?

Julia Wanker, Bennett Piater



2018-06-14

Questions?
└ Questions



Questions?
Julia Wanker, Bennett Piater

ee

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>.

1

Questions?

└ Bibliography

2018-06-14

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>.