



IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



2018-06-12

IoT Light Bulb Attack

- Topic Relevance



IoT Light Bulb Covert Channel
Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

ee

IoT Security in General

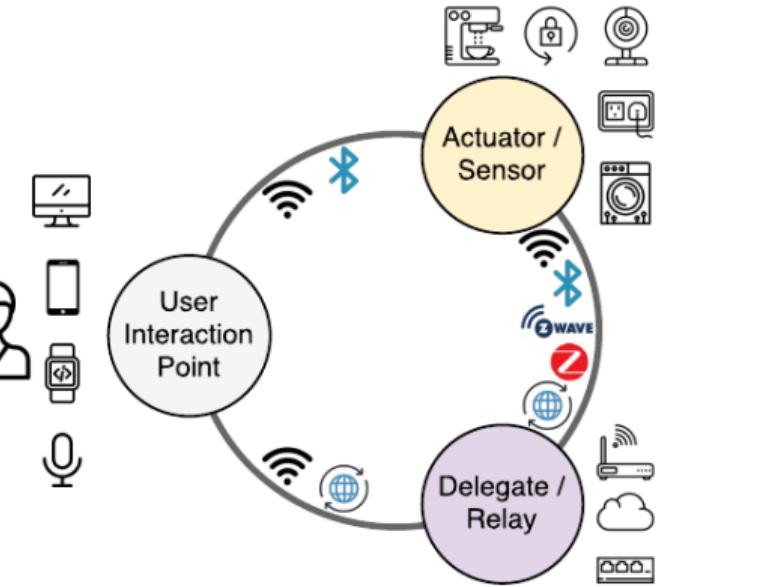


Figure: Infrastructure of IoT ecosystem¹

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

2018-06-12

Topic Relevance

└ Topic Relevance

└ IoT Security in General

└ IoT Security in General

IoT Security in General



Figure: Infrastructure of IoT ecosystem¹

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

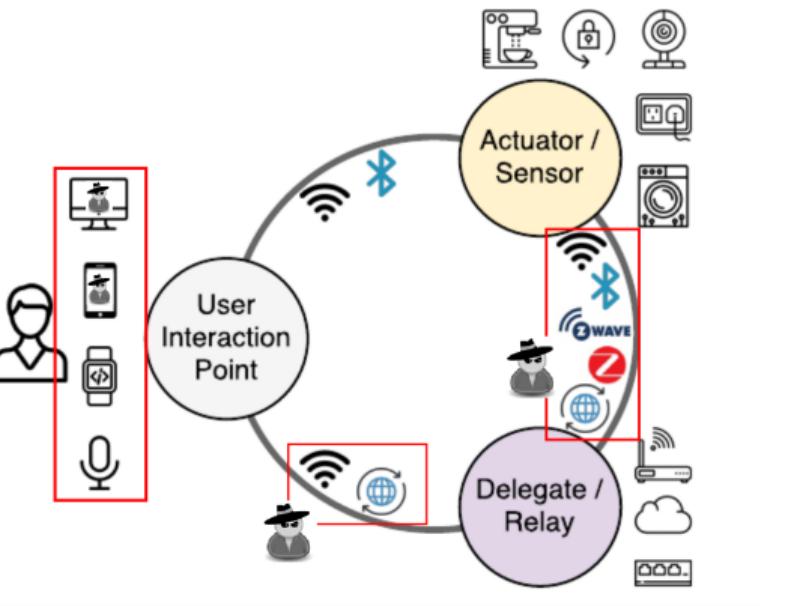
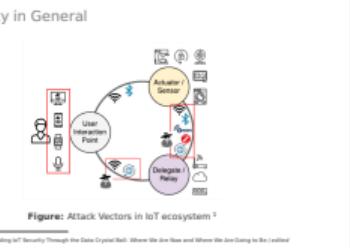


Figure: Attack Vectors in IoT ecosystem ¹

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

2018-06-12

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



Smart Light Security



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

2

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

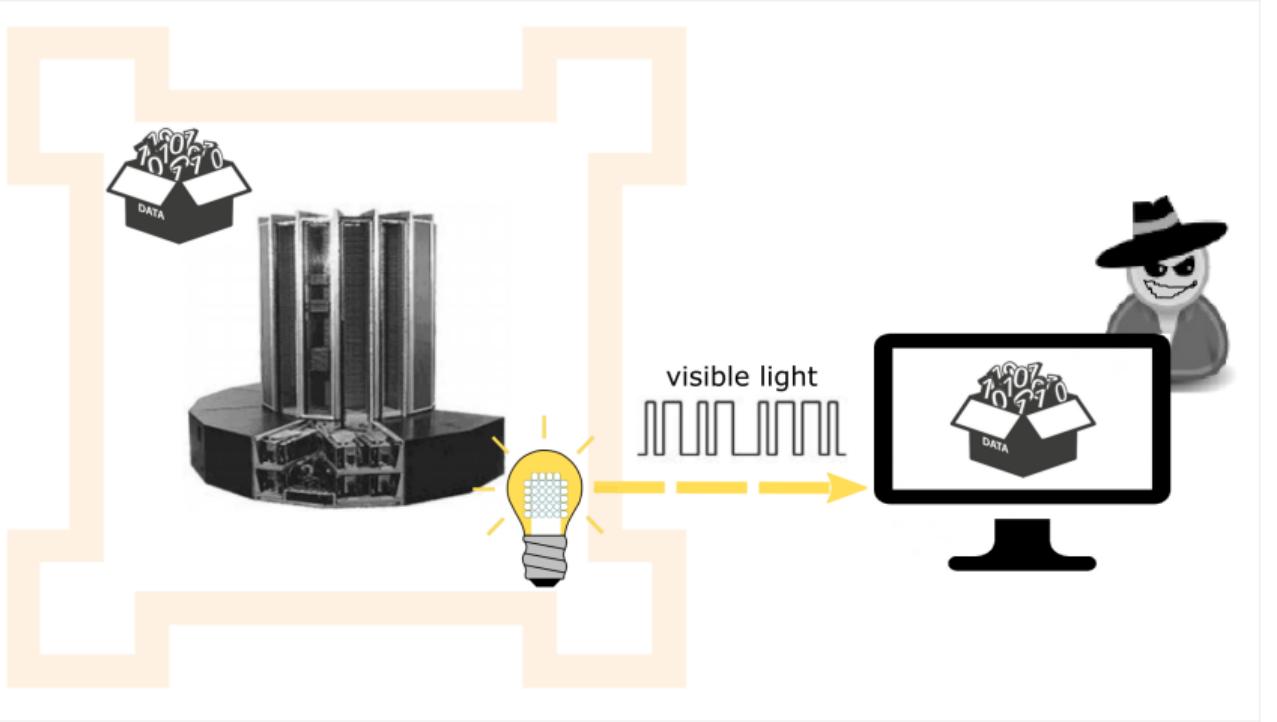
2018-06-12

Smart Light Security



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

Extending Functionality



3

2018-06-12
Topic Relevance
└ Topic Relevance
└ Smart Light Security
└ Extending Functionality





Topic Relevance

New Attack Vectors on IoT Devices

Julia Wanker, Bennett Piater



Topic Relevance
└ Theoretical Background

2018-06-12



Topic Relevance
New Attack Vectors on IoT Devices

Julia Wanker, Bennett Piater

88

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

Theoretical Background

(Covert) Communication With Lights

Communication With Lights

2018-06-12

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

5

Theoretical Background

Theoretical Background

(Covert) Communication With Lights

(Covert) Communication With Lights

2018-06-12

(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

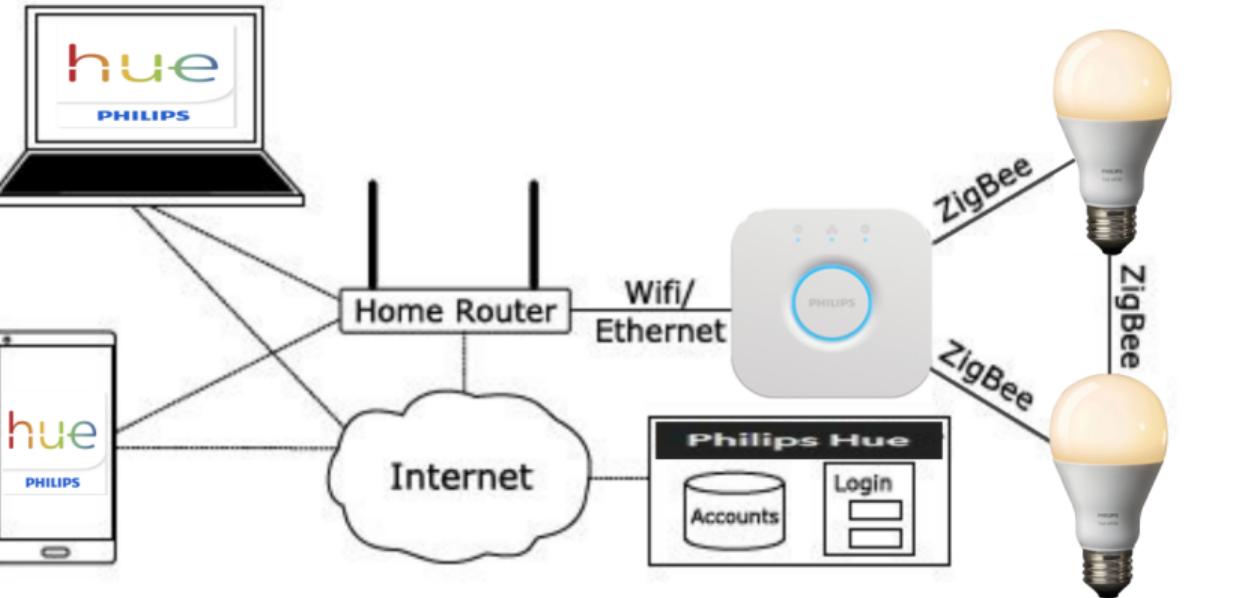
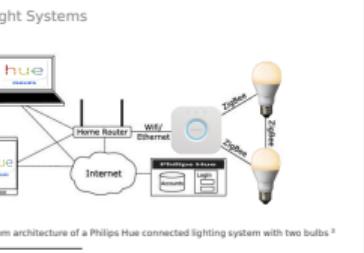


Figure: System architecture of a Philips Hue connected lighting system with two bulbs³

6

2018-06-12
Theoretical Background
└ Theoretical Background
└ Smart Light Systems
└ Smart Light Systems





Theoretical Background

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



2018-06-12
Theoretical Background
└ Experiment



Theoretical Background
Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

22

Controlling the Light

We use the Hue API for simplicity.

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

7

Theoretical Background
└ Experiment
 └ Controlling the Light
 └ Controlling the Light

1m

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.

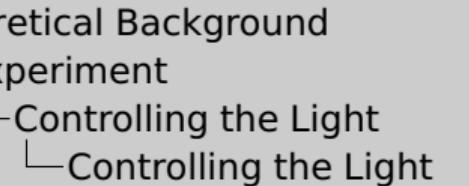
- Bridge controls light via ZLL
- We interface with REST-API on bridge

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?

7



1m

Controlling the Light

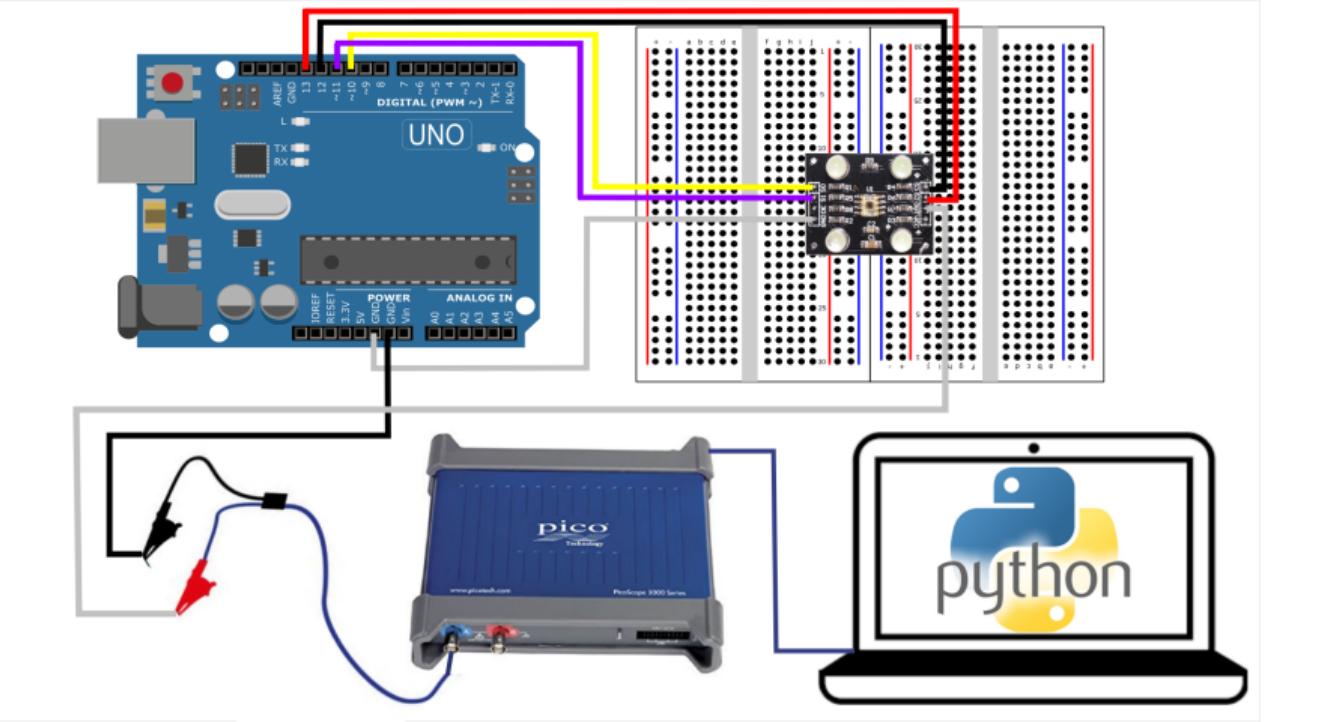
We use the Hue API for simplicity.

- * 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?

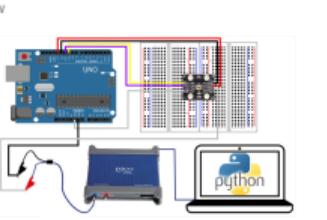
Overview



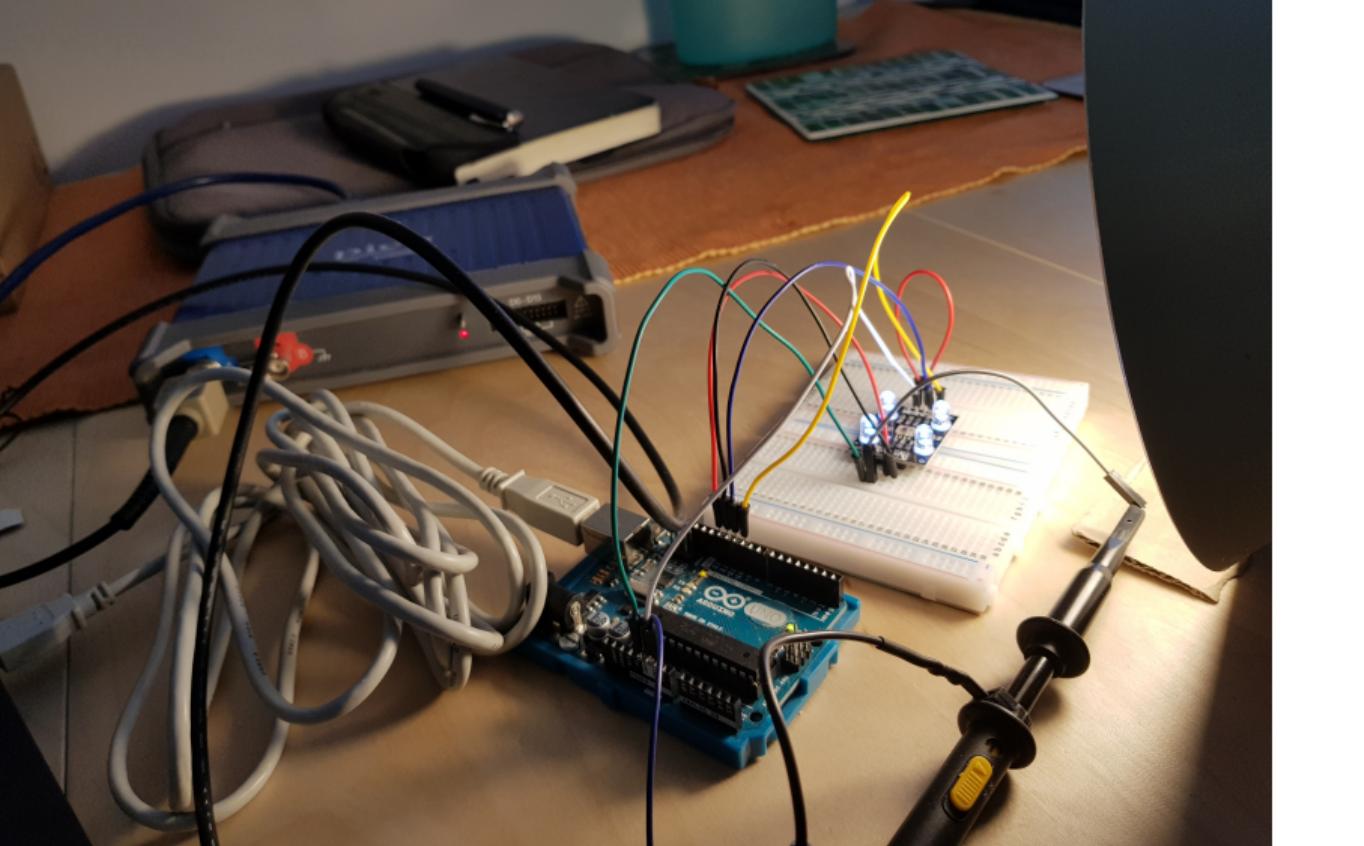
8

2018-06-12
Theoretical Background
└ Experiment
 └ Experimental Setup
 └ Overview

40s



Experimental Setup

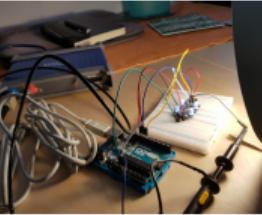


9

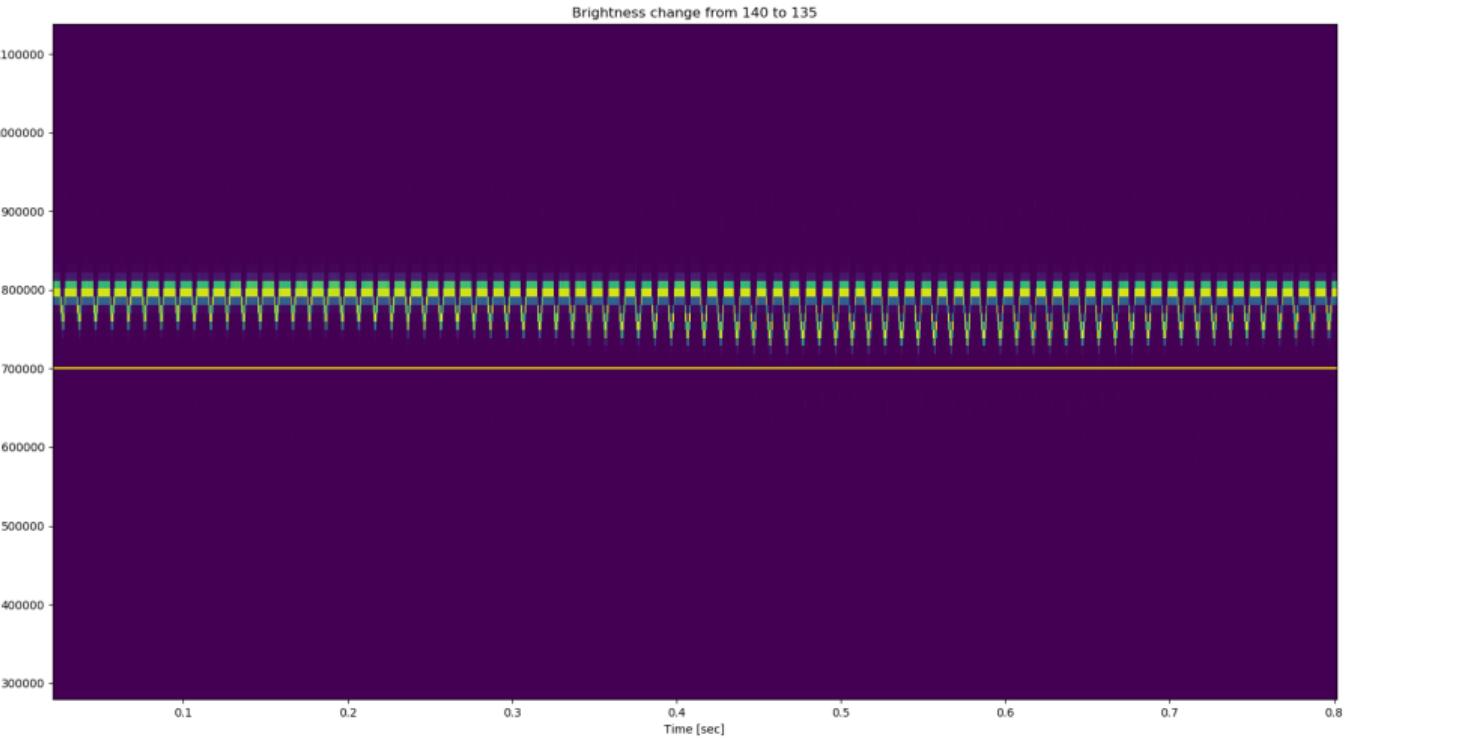
2018-06-12 Theoretical Background
└ Experiment
 └ Experimental Setup
 └ Experimental Setup

20s

Experimental Setup



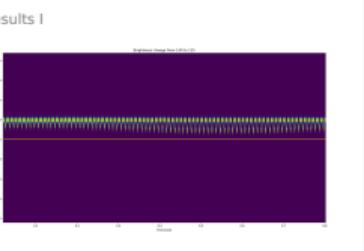
Some Results I



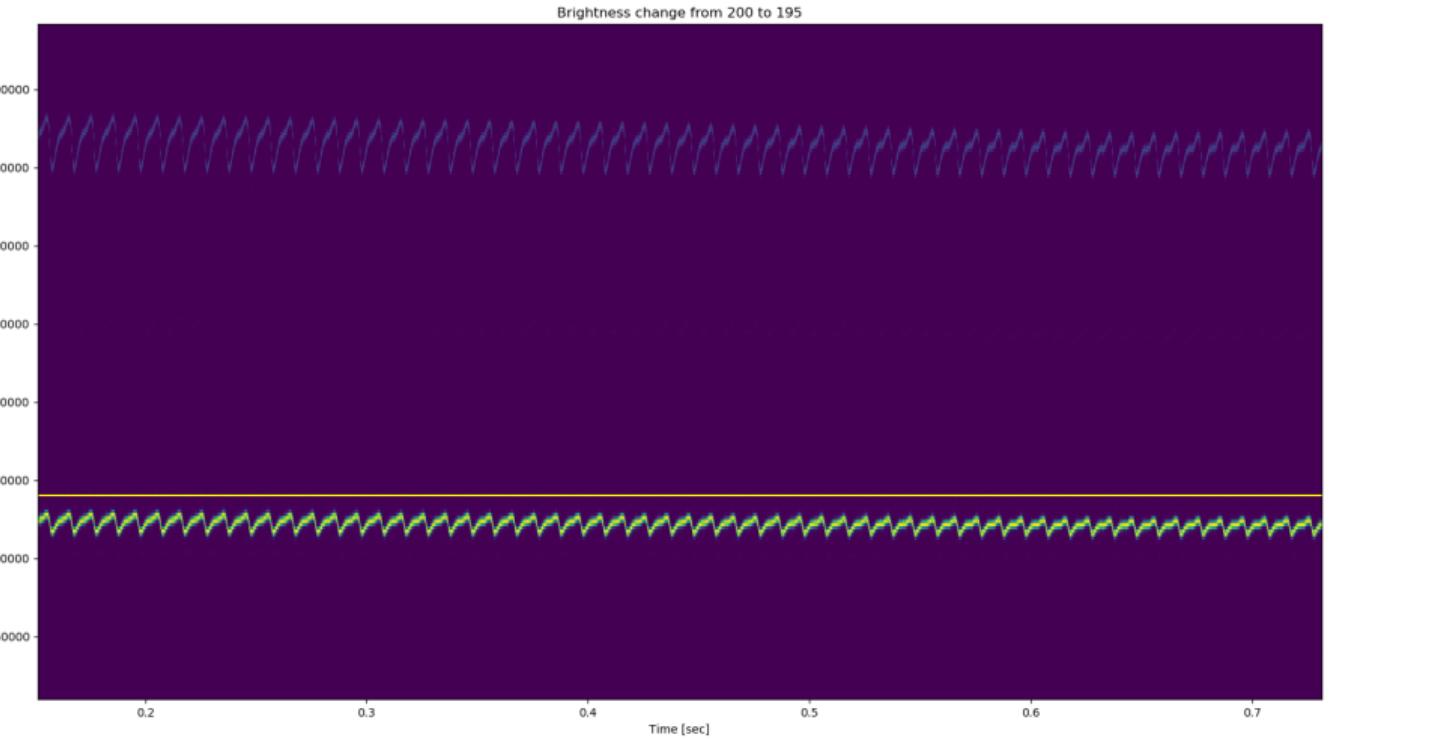
10

2018-06-12
Theoretical Background
└ Experiment
└ Results
└ Some Results I

2m for the 3 images



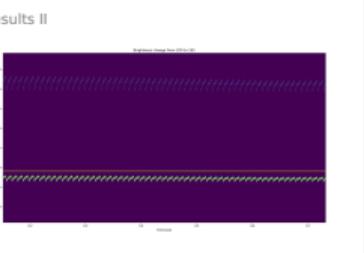
Some Results II



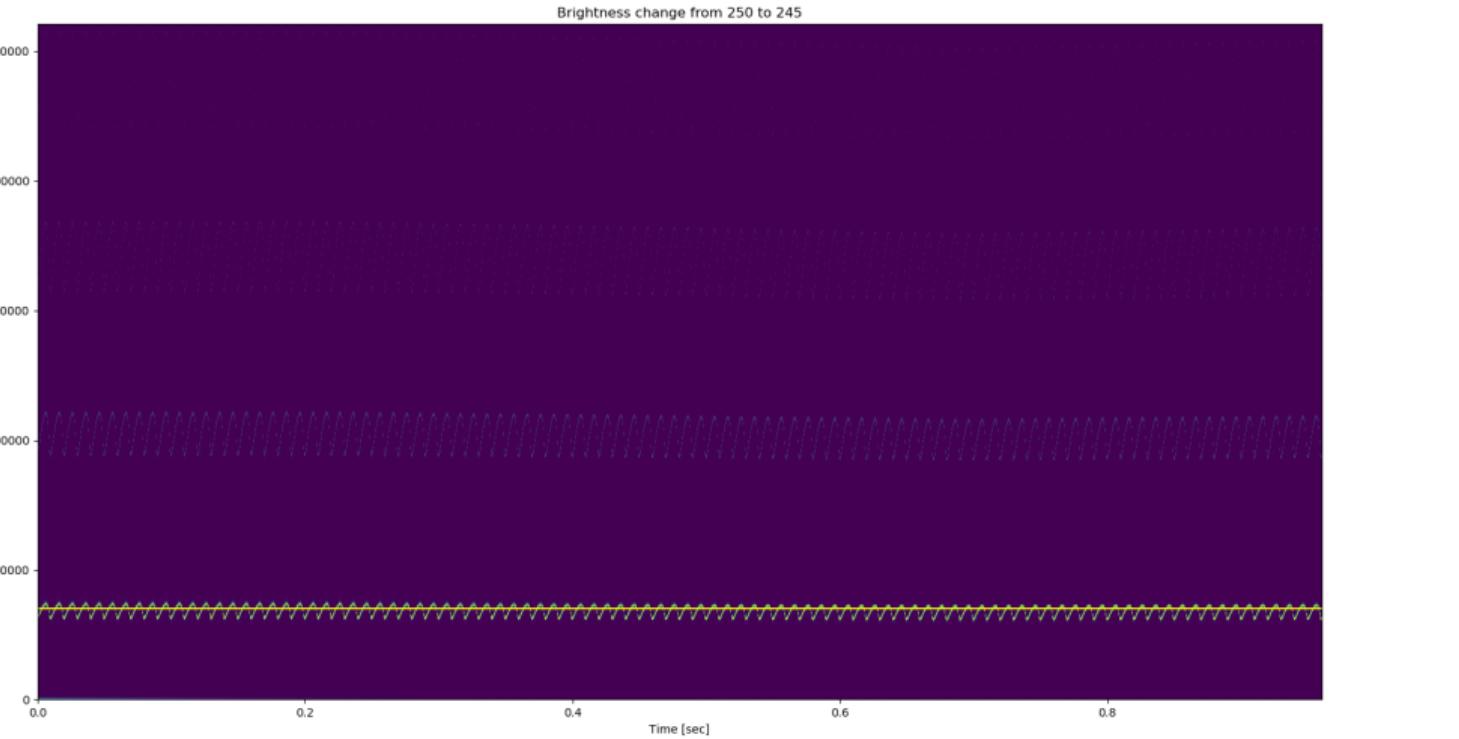
11

2018-06-12
Theoretical Background
└ Experiment
└ Results
└ Some Results II

2m for the 3 images



Some Results III

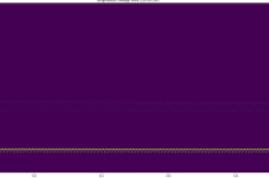


12

Theoretical Background
└ Experiment
└ Results
└ Some Results III

2m for the 3 images

Some Results III





Theoretical Background

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



2018-06-12
Theoretical Background
└ Demonstration



Theoretical Background
Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

22



Demonstration

Covert Communication Channel on Philips Hue White Smart Light

Julia Wanker, Bennett Piater



Demonstration
└ Conclusion

2018-06-12



Demonstration
Covert Communication Channel on Philips Hue White Smart Light

Julia Wanker, Bennett Piater

88

Conclusion

Successes

- We can distinguish brightness differences invisible to the human eye
 - We *think that we can* see the PWM, not just brightness
 - TODO: Automatically detect brightness changes
- Research from Ronen and Shamir [2016] reproduced in principle.

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
 - TODO: Automatically detect brightness changes
- 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
 - TODO: Automatically detect brightness changes
- 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

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
 - TODO: Automatically detect brightness changes
- 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.

14

Conclusion

Conclusion

Outlook

1m

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



Questions?
└ Questions

2018-06-12



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>.

Questions?

2018-06-12

└ Bibliography

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>.