



IoT Light Bulb Covert Channel

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



2018-06-11

IoT Light Bulb Attack

- Topic Relevance



IoT Light Bulb Covert Channel
Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater

22

IoT Security in General

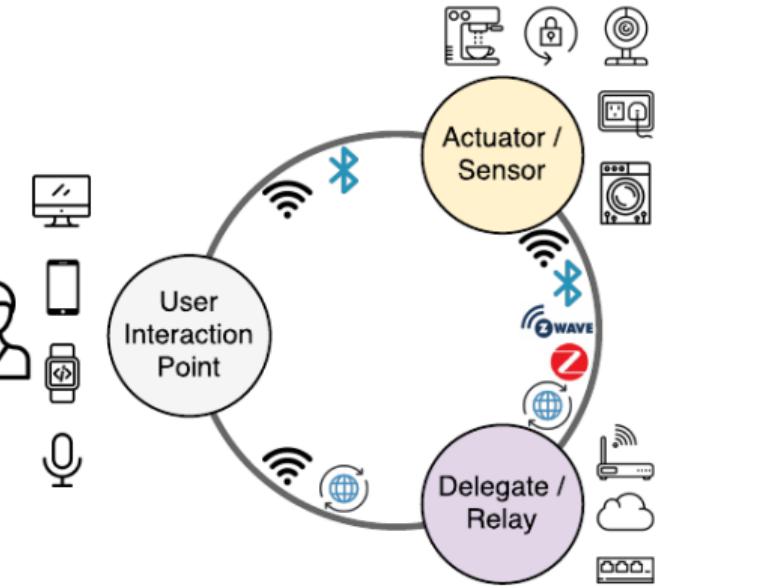


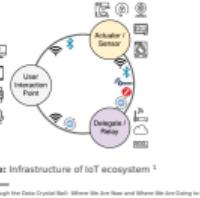
Figure: Infrastructure of IoT ecosystem¹

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

2018-06-11

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

IoT Security in General



IoT Security in General

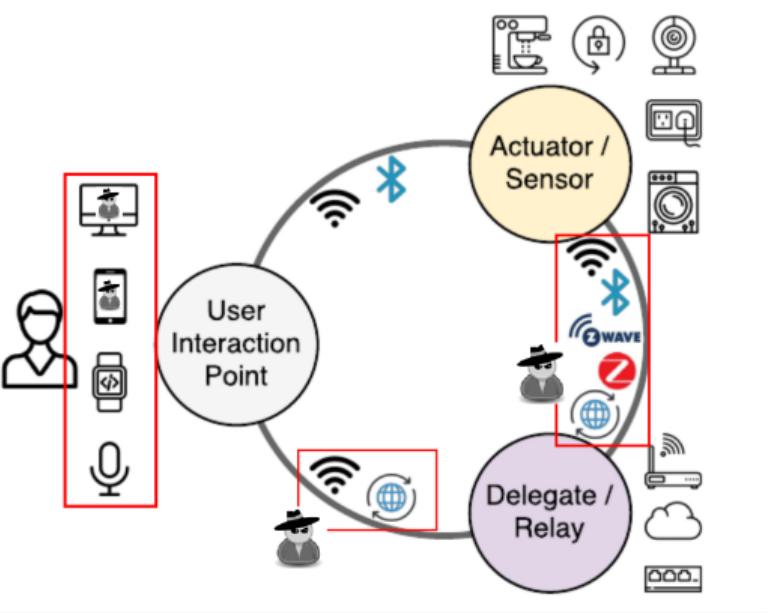
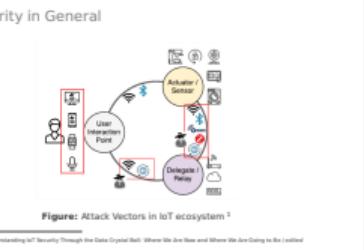


Figure: Attack Vectors in IoT ecosystem ¹

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

2018-06-11

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

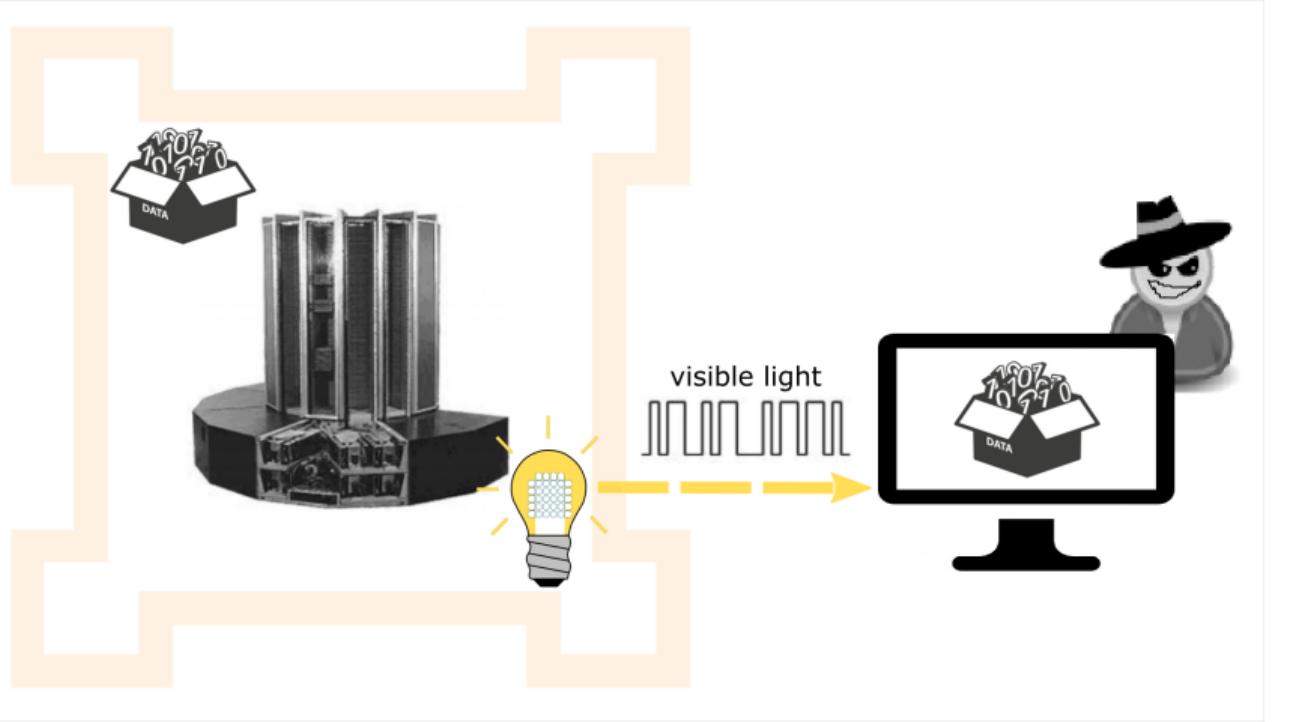
2018-06-11

Smart Light Security



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

Extending Functionality



3

2018-06-11
Topic Relevance
└ Topic Relevance
 └ Smart Light Security
 └ Extending Functionality

Extending Functionality





Topic Relevance

New Attack Vectors on IoT Devices

Julia Wanker, Bennett Piater



2018-06-11
Topic Relevance
└ Theoretical Background

Topic Relevance
New Attack Vectors on IoT Devices
Julia Wanker, Bennett Piater
2018-06-11

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
- **Lower leve** represents logical **0**
- **Higher level** represents logical **1**

4

Theoretical Background

Theoretical Background

(Covert) Communication With Lights

Communication With Lights

2018-06-11

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
- Lower leve 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

2018-06-11

(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

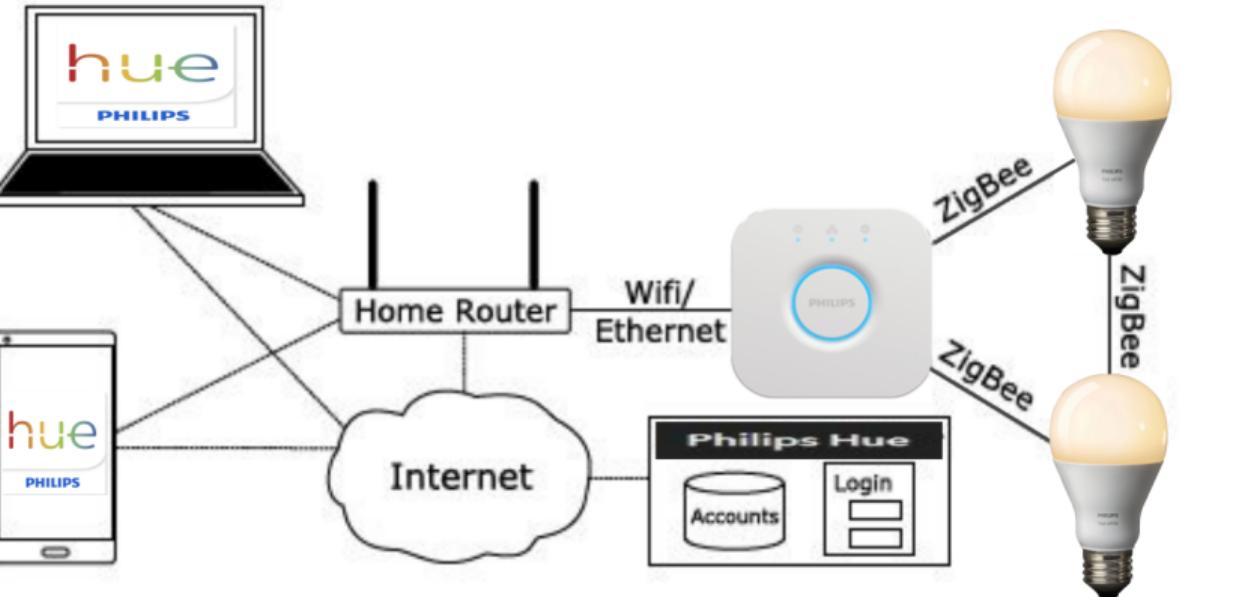
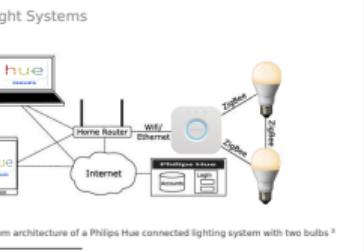


Figure: System architecture of a Philips Hue connected lighting system with two bulbs³

6

2018-06-11
Theoretical Background
└ Theoretical Background
└ Smart Light Systems
└ Smart Light Systems





Theoretical Background

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater



2018-06-11
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

2018-06-11

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

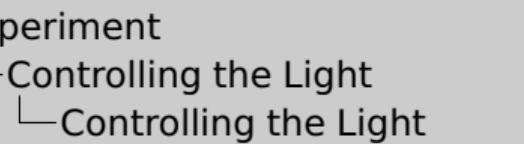
Limitations

- 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

Theoretical Background



2018-06-11

Controlling the Light

We use the Hue API for simplicity.

- Bridge controls light via ZLL

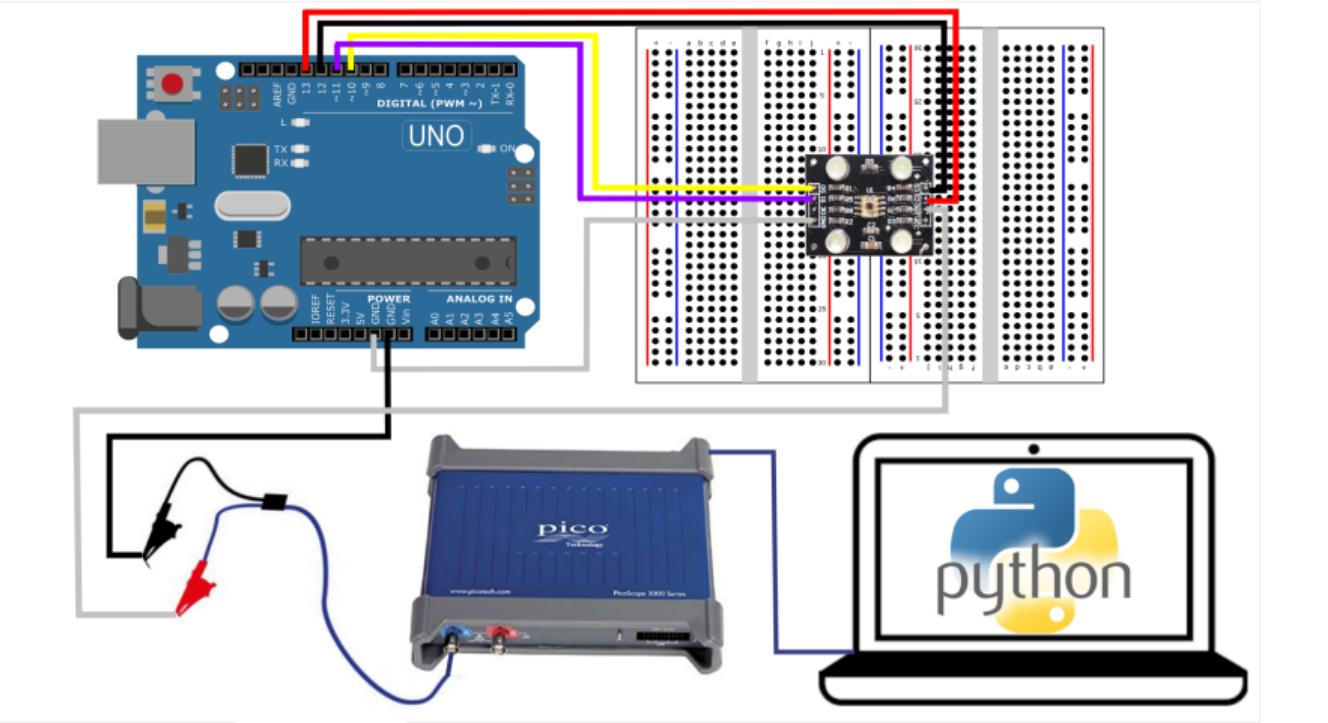
- We interface with REST-API on bridge

Limitations

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

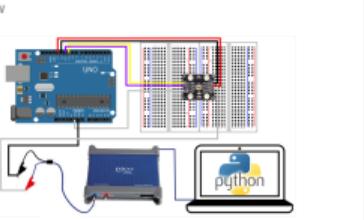
May be worked around some by speaking ZLL directly?

Overview

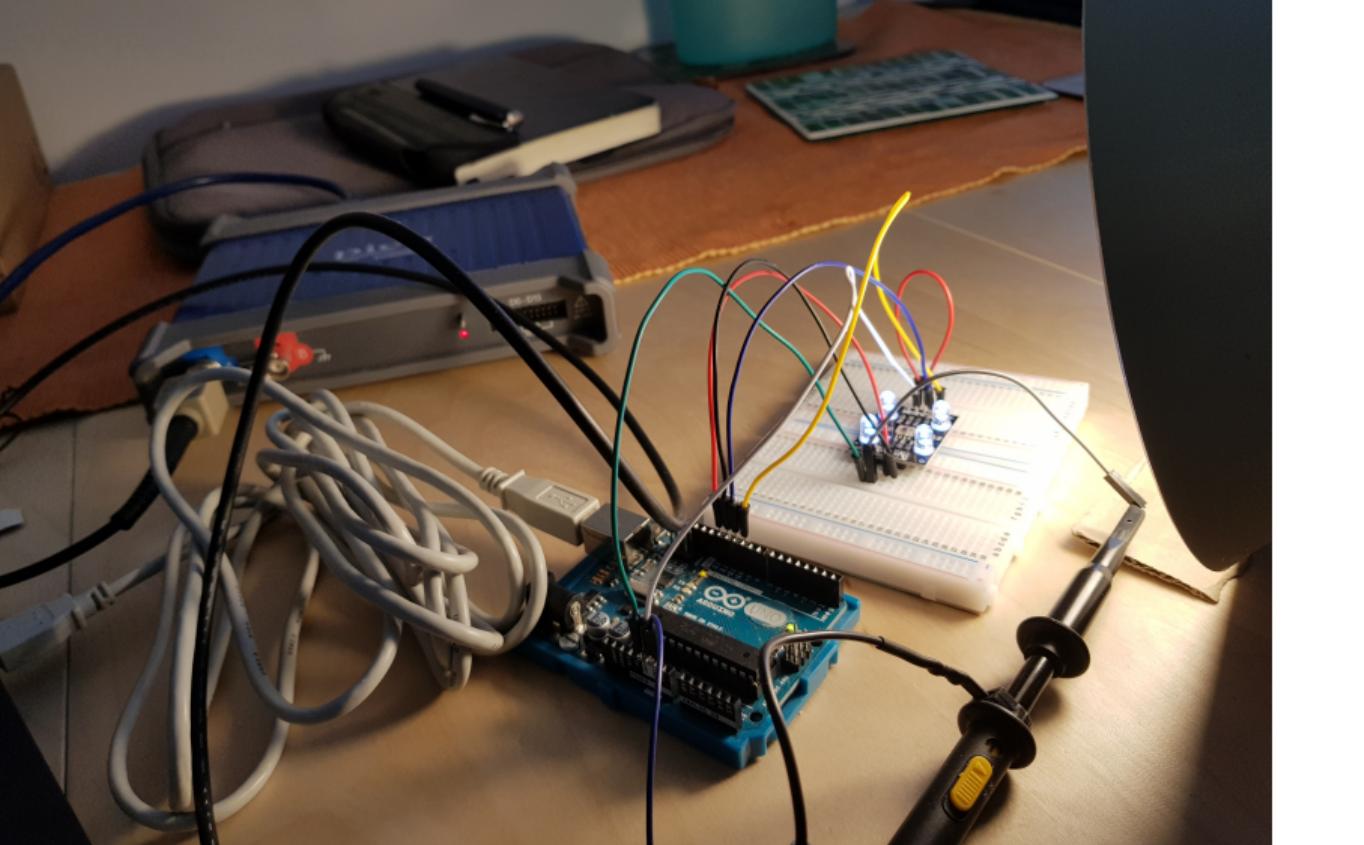


8

2018-06-11
Theoretical Background
└ Experiment
 └ Experimental Setup
 └ Overview



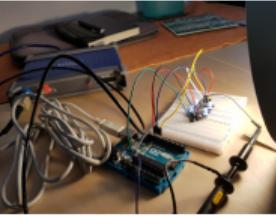
Experimental Setup



9

2018-06-11 Theoretical Background
└ Experiment
 └ Experimental Setup
 └ Experimental Setup

Experimental Setup



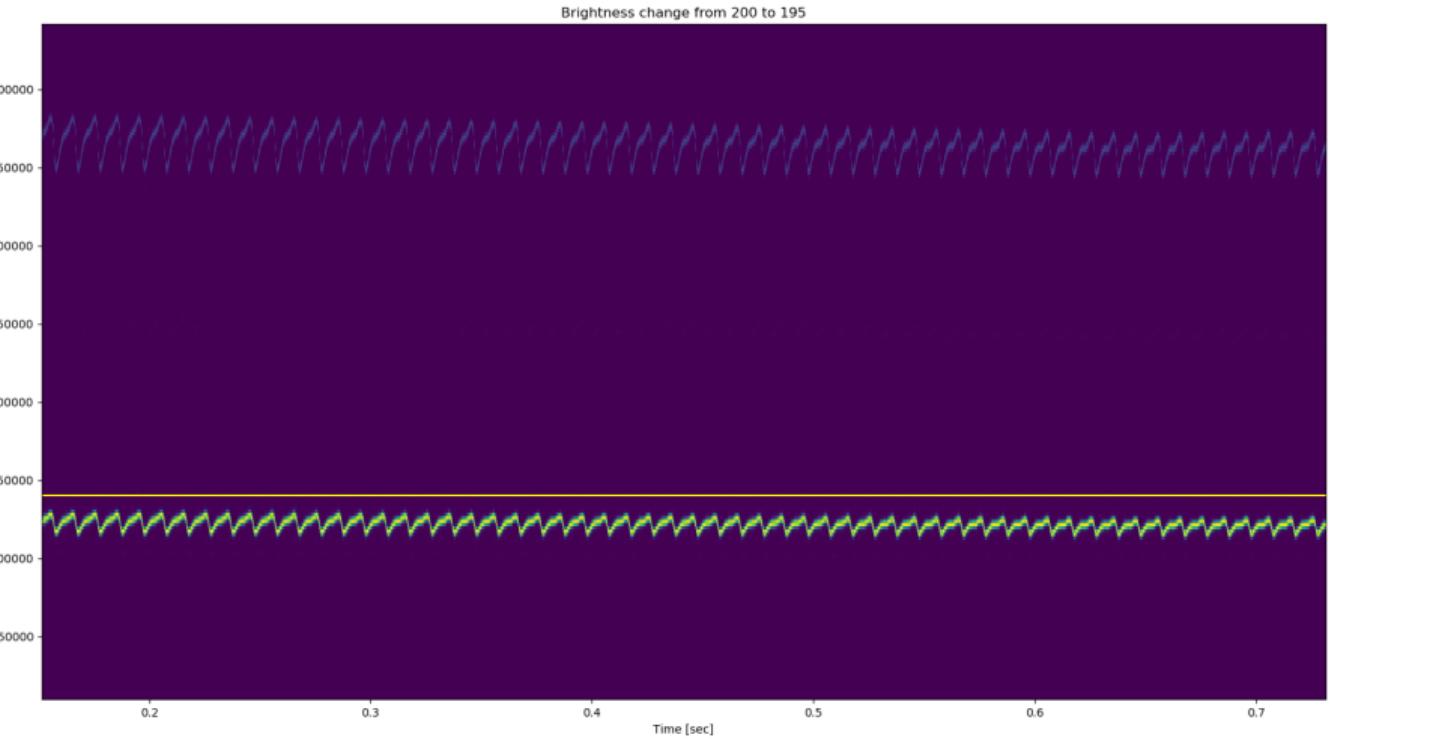
Some Results I

Theoretical Background
└ Experiment
└ Results
└ Some Results I

2018-06-11

Some Results I

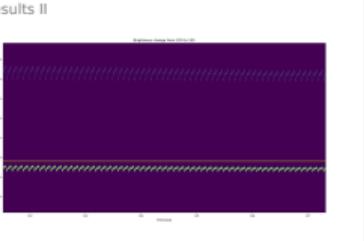
Some Results II



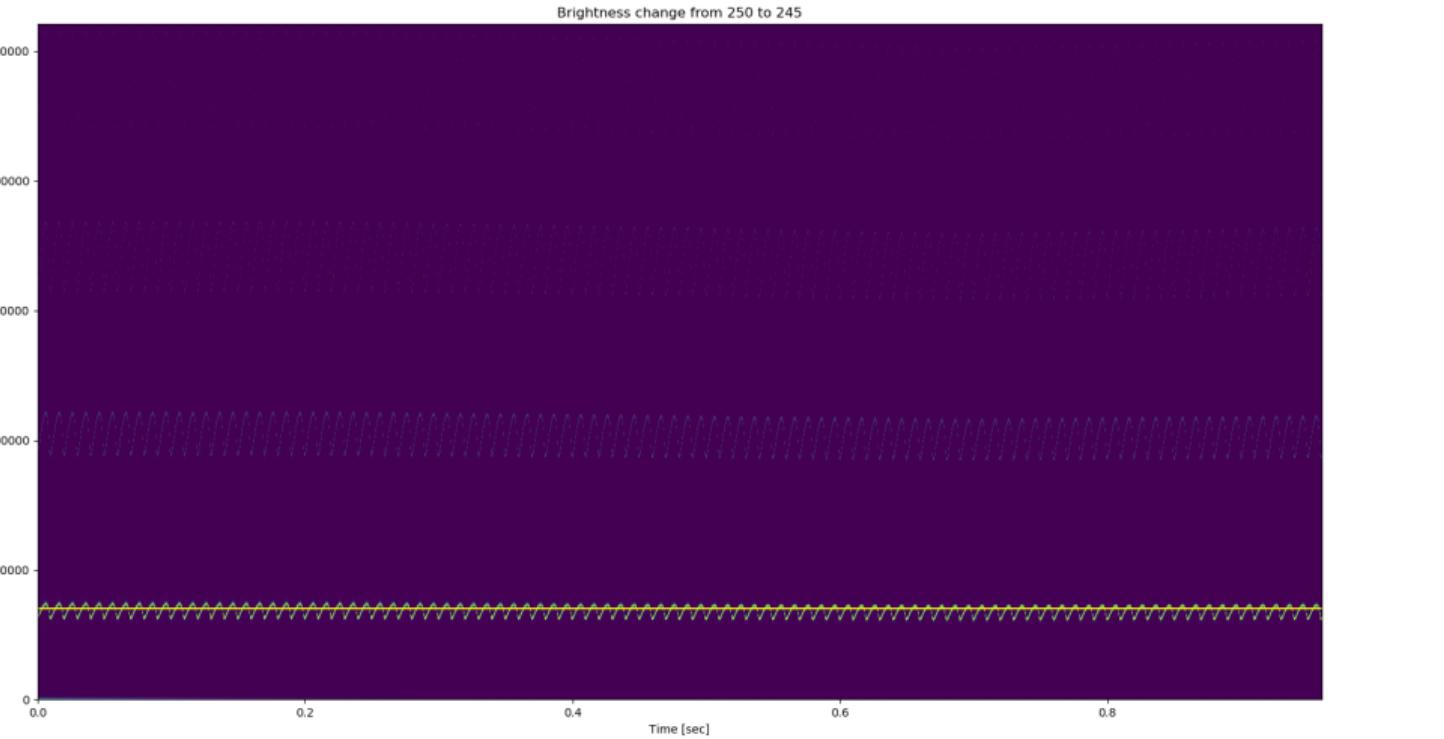
11

2018-06-11

- Theoretical Background
- └ Experiment
- └ Results
- └ Some Results II

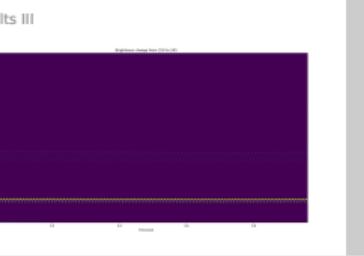


Some Results III



12

2018-06-11
Theoretical Background
└ Experiment
└ Results
└ Some Results III





Theoretical Background

Extended Functionality Attack on Smart Lights

Julia Wanker, Bennett Piater





Demonstration

Covert Communication Channel on Philips Hue White Smart Light

Julia Wanker, Bennett Piater



Demonstration
└ Conclusion

2018-06-11



Demonstration
Covert Communication Channel on Philips Hue White Smart Light

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
 - TODO: Automatically detect brightness changes
- Research from Ronen and Shamir [2016] reproduced in principle.

13

Conclusion └ Conclusion

└ Conclusion

13

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

2018-06-11

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 principal 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

2018-06-11

Outlook

An automated covert channel could in principal 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

2018-06-11



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?

2018-06-11

└ 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>.