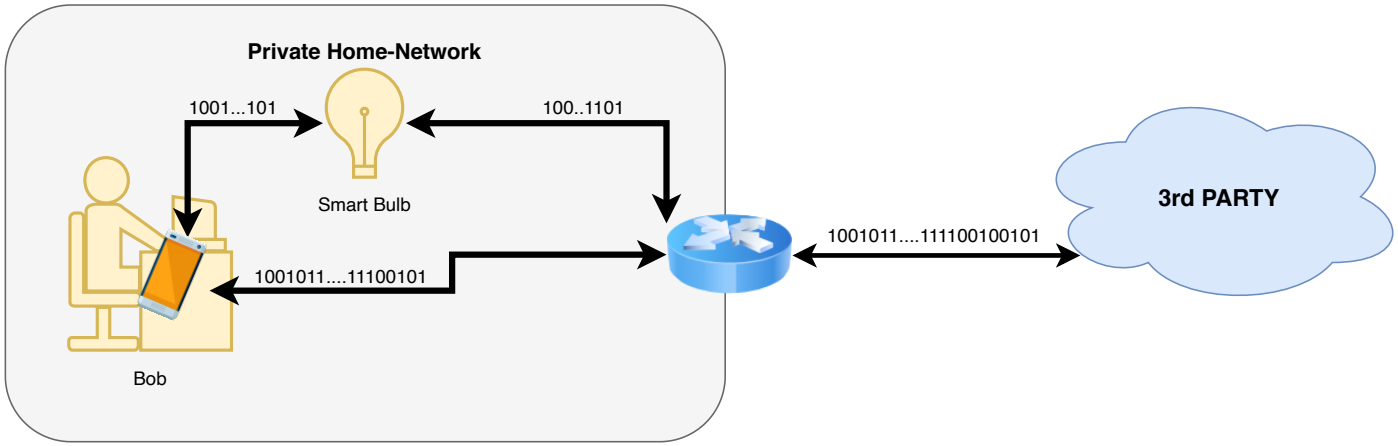
Towards Privacy-Preserving Local Monitoring and Evaluation of Network Traffic from IoT Devices and Corresponding Mobile Phone Applications

Felix Klement, Henrich C. Pöhls, Korbinian Spielvogel

Chair of IT-Security
University of Passau, Germany

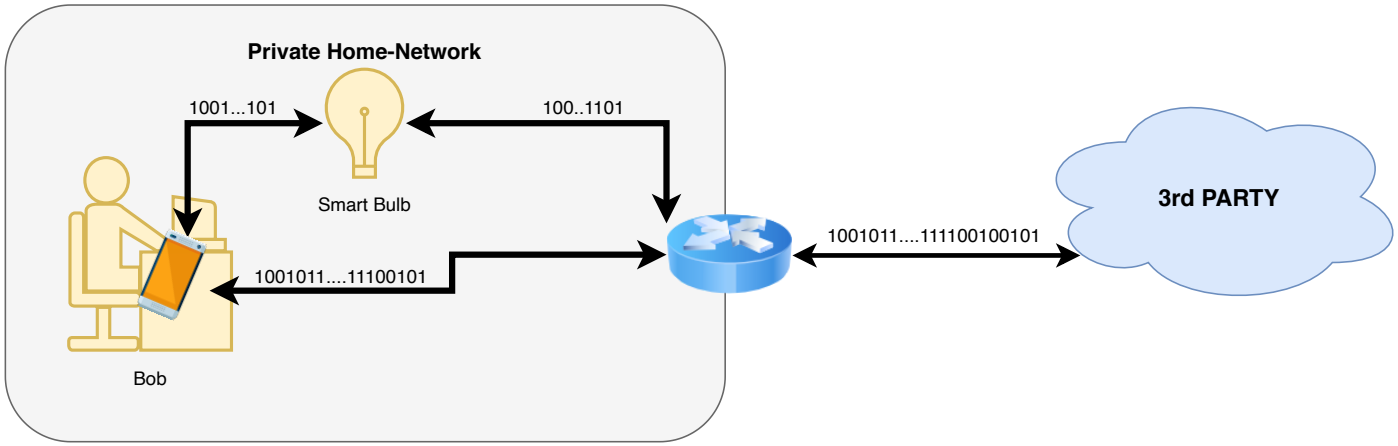
(funded by the European Union's H2020 grant n^o780315)

How to know what is being sent?



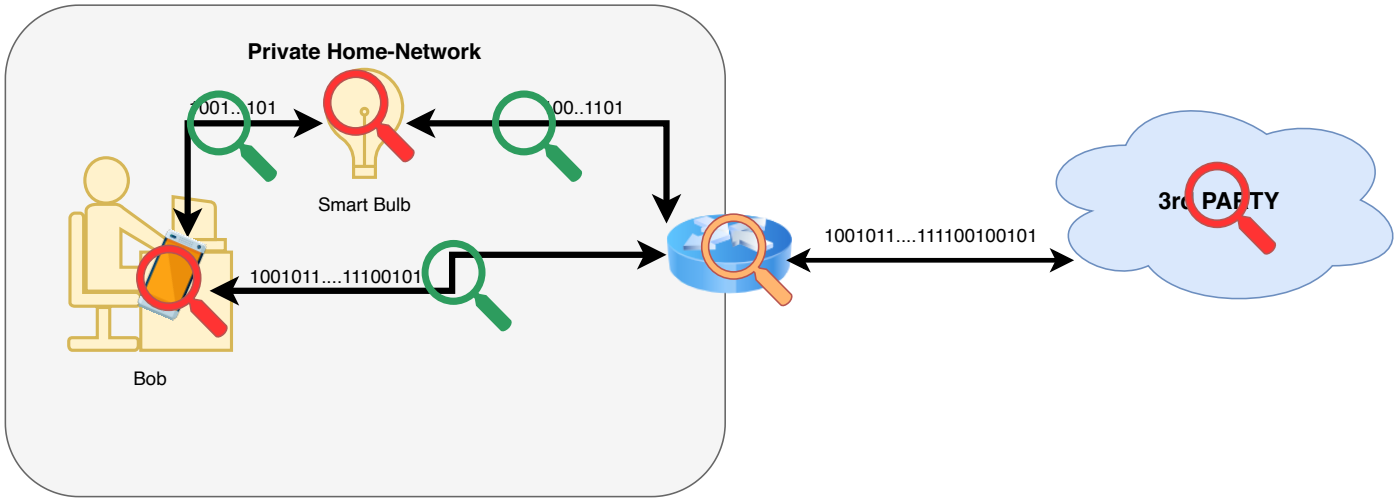
- Bob interacts with his smart bulb using the app on his mobilephone
- Bob does usually not inspect network traffic

How to know what is being sent?



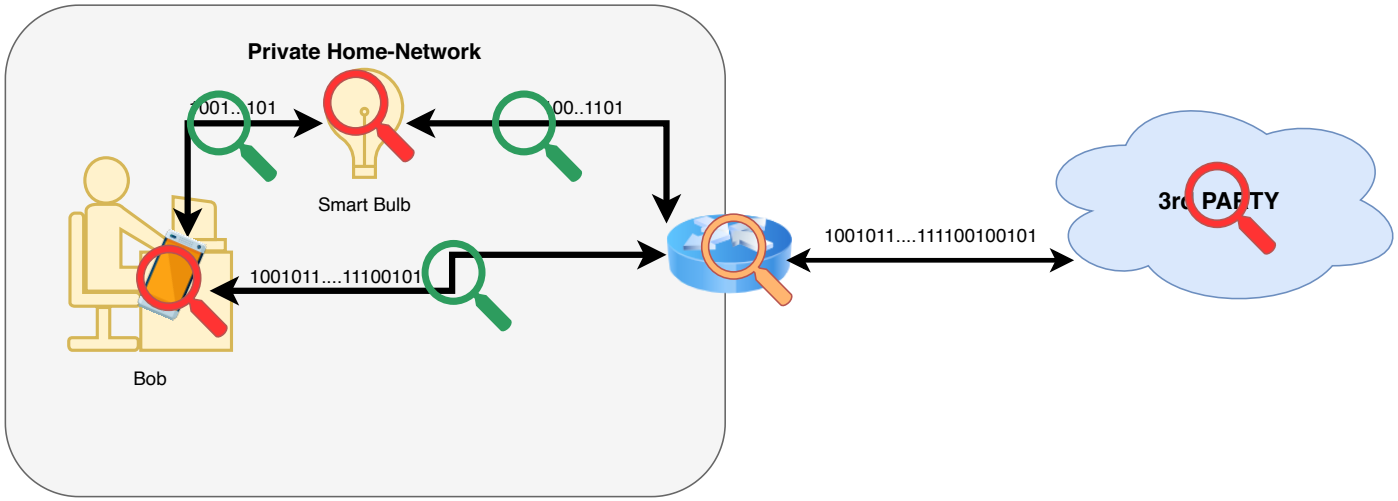
- Bob interacts with his smart bulb using the app on his mobilephone
- Bob does usually not inspect network traffic

How to know what is being sent?



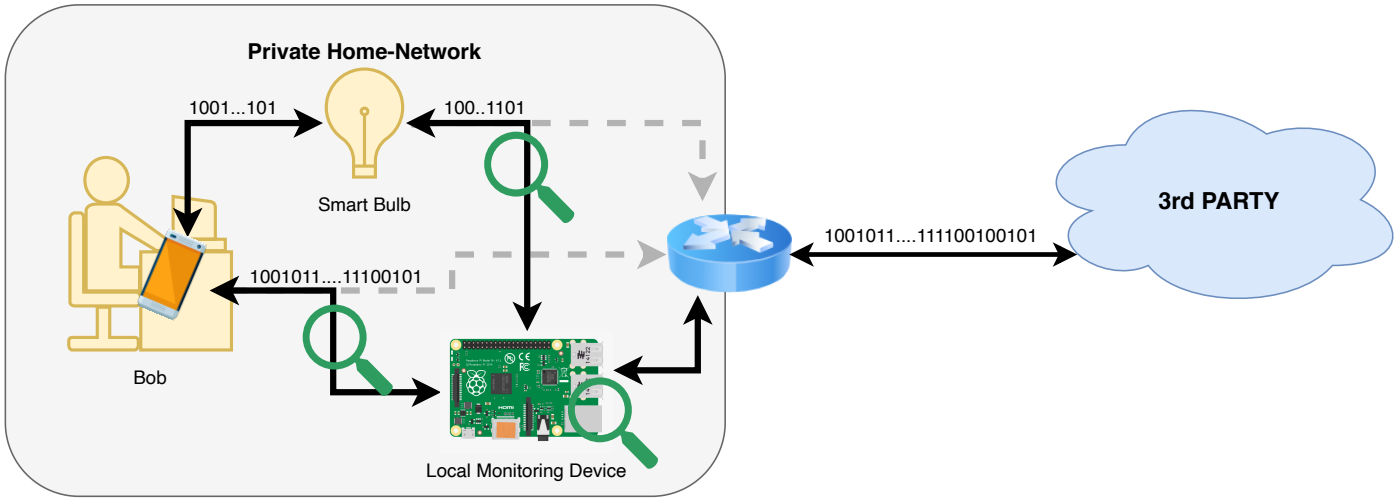
- Bob cannot reverse-engineer
  - the app
  - the smart bulb
  - the 3rd party server
- To see the network traffic, Bob needs to modify the router

How to know what is being sent?



- Bob cannot reverse-engineer
  - the app
  - the smart bulb
  - the 3rd party server
- To see the network traffic, Bob needs to modify the router

How to know what is being sent?



- Our local monitoring device allows Bob to observe traffic from the smart bulb and the mobile phone without modifying existing devices

Goals of our approaches

UNIVERSITÄT PASSAU

1. Provide local user insight into the actual communication of devices
   - 1.1 Enable a local-only aquisition/analysis of IoT devices
   - 1.2 Enable identification of potentially compromised devices
   - 1.3 Visualizations for user-friendly device analysis
2. Educate users what network traffic their devices generate
3. Allow to voluntarily report selected communication traces to a central collection point

Goals of our approaches

UNIVERSITÄT PASSAU

1. Provide local user insight into the actual communication of devices
   - 1.1 Enable a local-only aquisition/analysis of IoT devices
   - 1.2 Enable identification of potentially compromised devices
   - 1.3 Visualizations for user-friendly device analysis
2. Educate users what network traffic their devices generate
3. Allow to voluntarily report selected communication traces to a central collection point

Goals of our approaches

UNIVERSITÄT PASSAU

1. Provide local user insight into the actual communication of devices
   - 1.1 Enable a local-only aquisition/analysis of IoT devices
   - 1.2 Enable identification of potentially compromised devices
   - 1.3 Visualizations for user-friendly device analysis
2. Educate users what network traffic their devices generate
3. Allow to voluntarily report selected communication traces to a central collection point

Goals of our approaches

UNIVERSITÄT PASSAU

1. Provide local user insight into the actual communication of devices
   - 1.1 Enable a local-only aquisition/analysis of IoT devices
   - 1.2 Enable identification of potentially compromised devices
   - 1.3 Visualizations for user-friendly device analysis
2. Educate users what network traffic their devices generate
3. Allow to voluntarily report selected communication traces to a central collection point

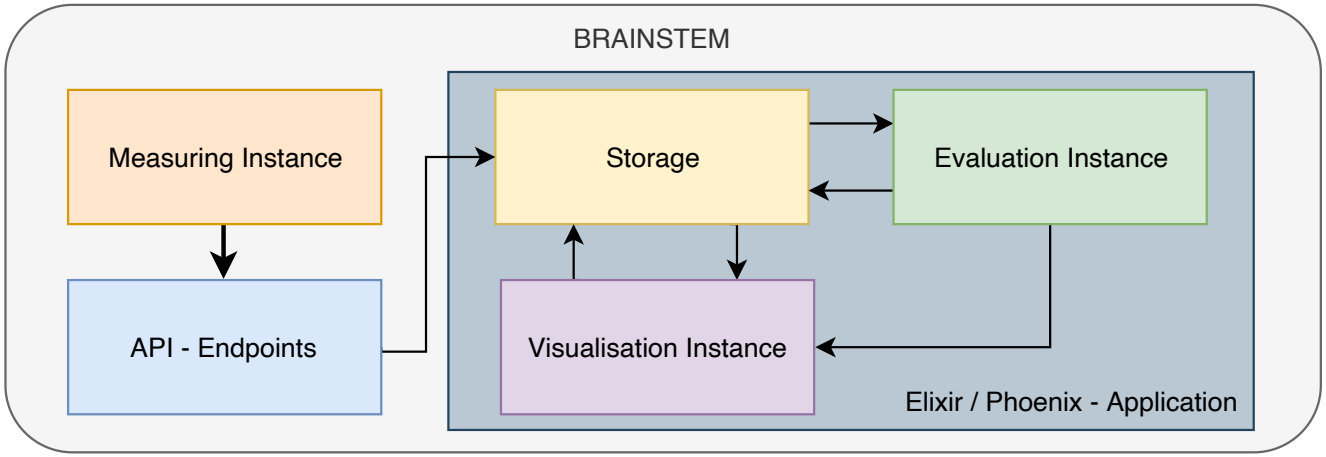
UNIVERSITÄT PASSAU

1. Introduction

2. Data Acquisition and Tools

3. Conclusion

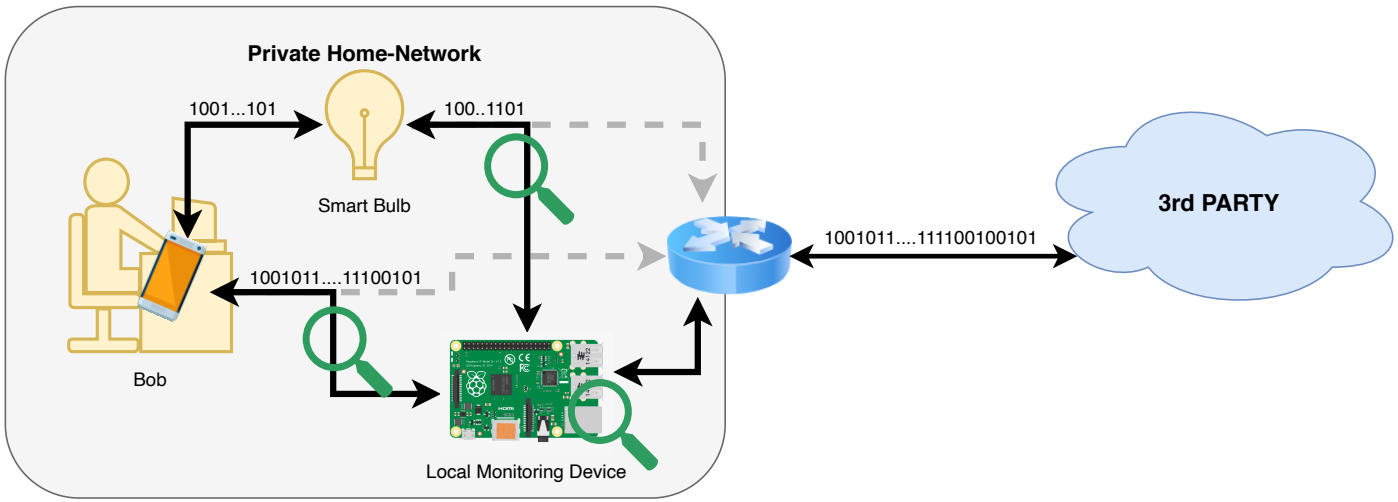
Modular architecture



- Modular architecture allows to add *Measuring Instances* for other communication technologies
  - Ethernet/Wifi
  - Zigbee
  - etc.
- Runs locally on an RaspberryPi 3b+
- Using Elixir in combination with Phoenix

ARP python library

- Used to detect new devices on the network
- ARP-Spoofing to redirect traffic over our raspberry pi



Toolset - 2/3

UNIVERSITÄT PASSAU

Netdisco

- Scans local network for devices using SSDP, mDNS and UPnP

NMAP

Used to identify open ports on devices e.g. insecure telnet ports used by bots to capture devices

UNIVERSITÄT PASSAU

Netdisco

- Scans local network for devices using SSDP, mDNS and UPnP

NMAP

Used to identify open ports on devices e.g. insecure telnet ports used by bots to capture devices

UNIVERSITÄT PASSAU

MITM Proxy

Open source interactive HTTPS proxy

- Used to intercept, inspect communication once it is redirected over our local monitoring device

Scapy

Collects information like:

- Vendor of network chipset
- DNS requests and responses
- Remote IP-Addresses/ports

UNIVERSITÄT PASSAU

MITM Proxy

Open source interactive HTTPS proxy

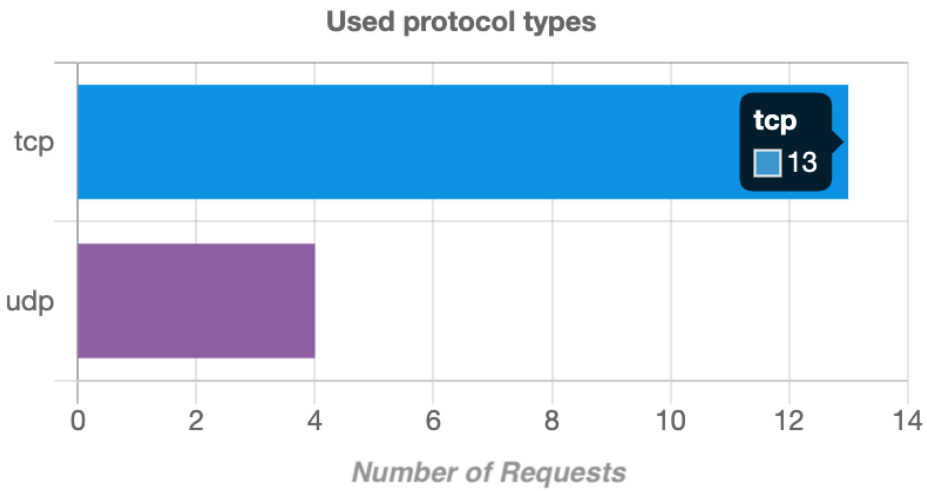
- Used to intercept, inspect communication once it is redirected over our local monitoring device

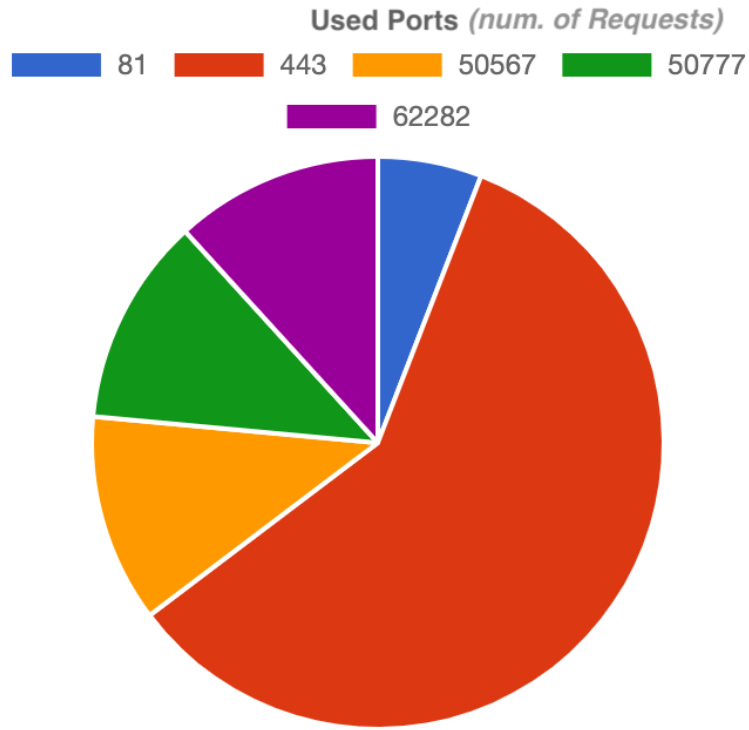
Scapy

Collects information like:

- Vendor of network chipset
- DNS requests and responses
- Remote IP-Addresses/ports

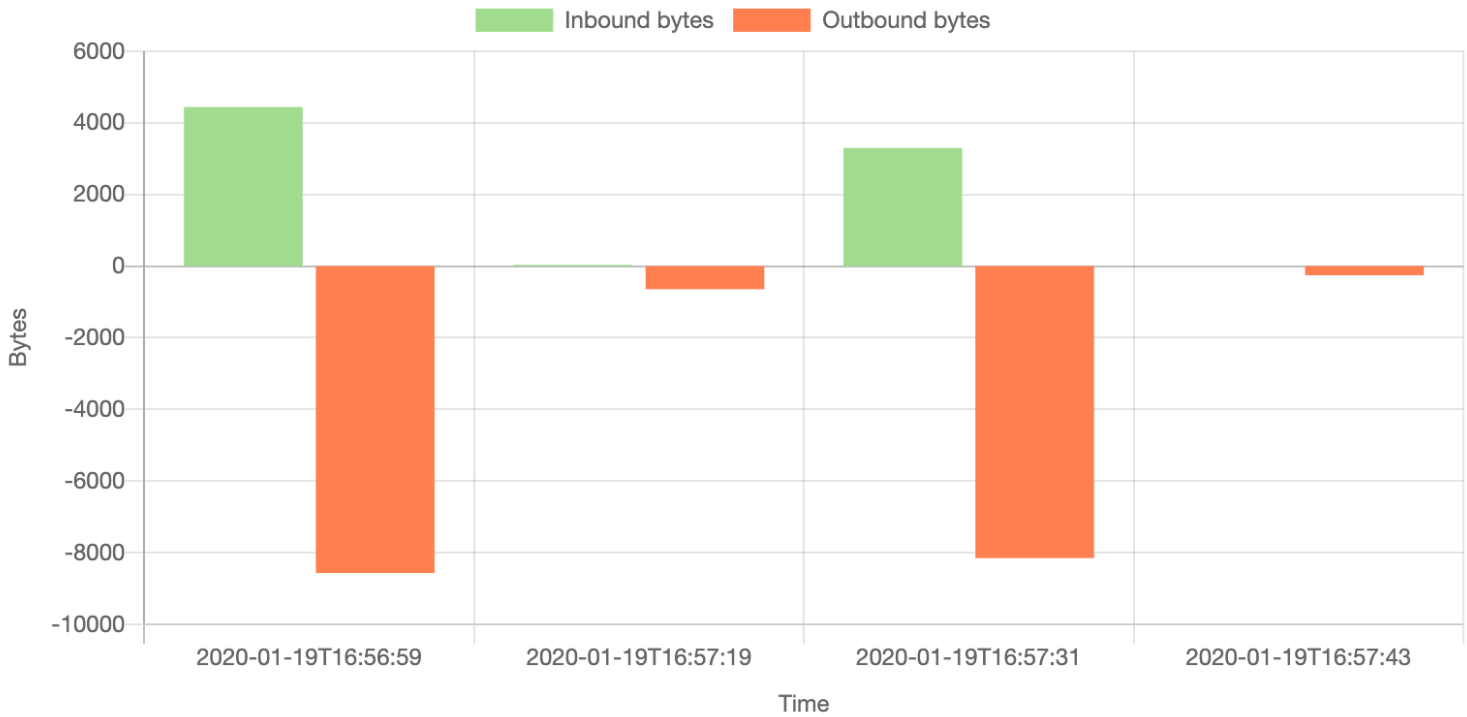
Example of observed Protocol / Port usage





- With our local analysis and visualisation the local users gain an insight into services that are used by their devices.

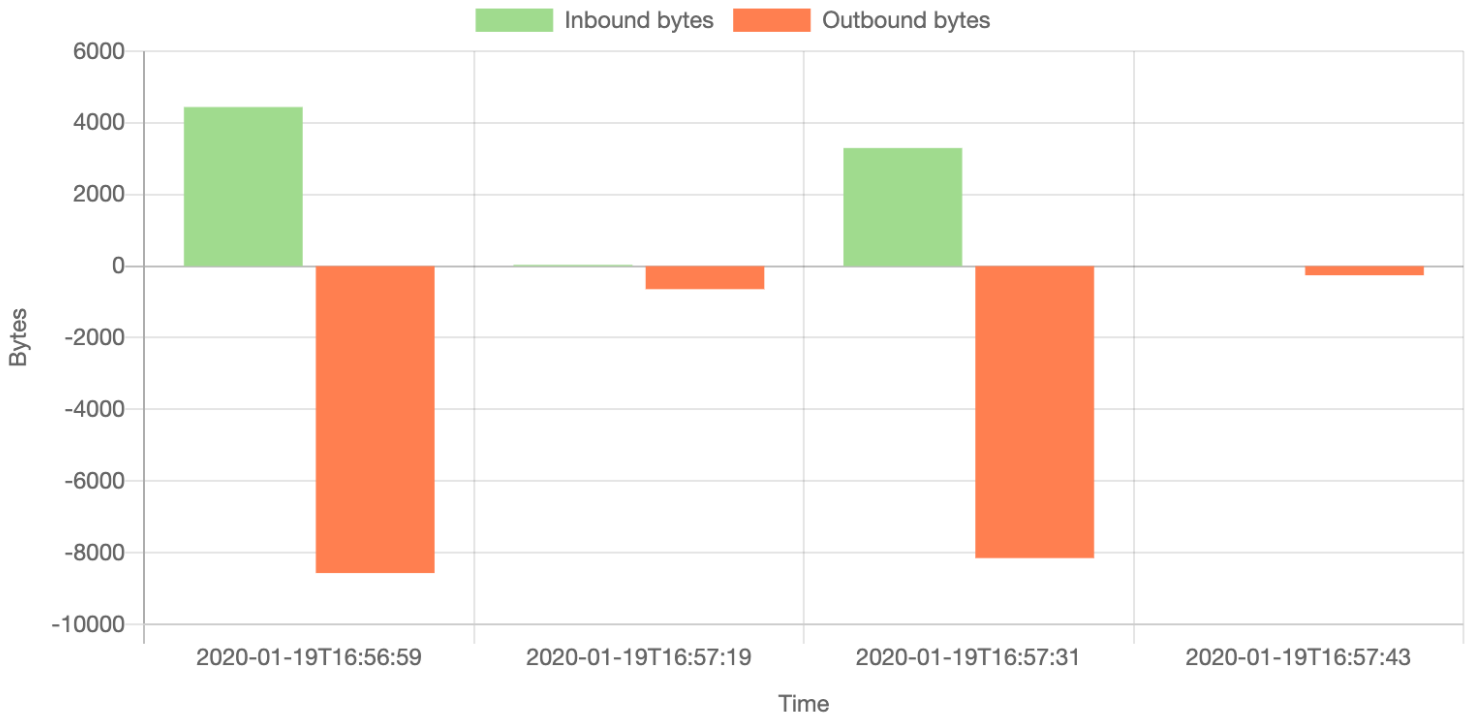
Inbound- Outbound Traffic



Our local analysis and visualisation allows to:

- Identify on a timeline unusually high or low data traffic
- Detect potentially unwanted traffic

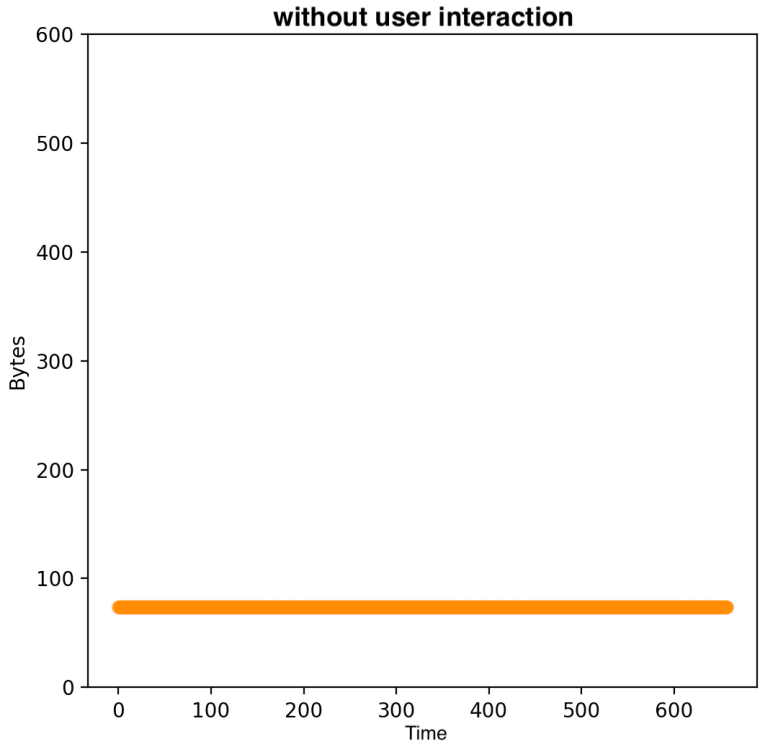
Inbound- Outbound Traffic

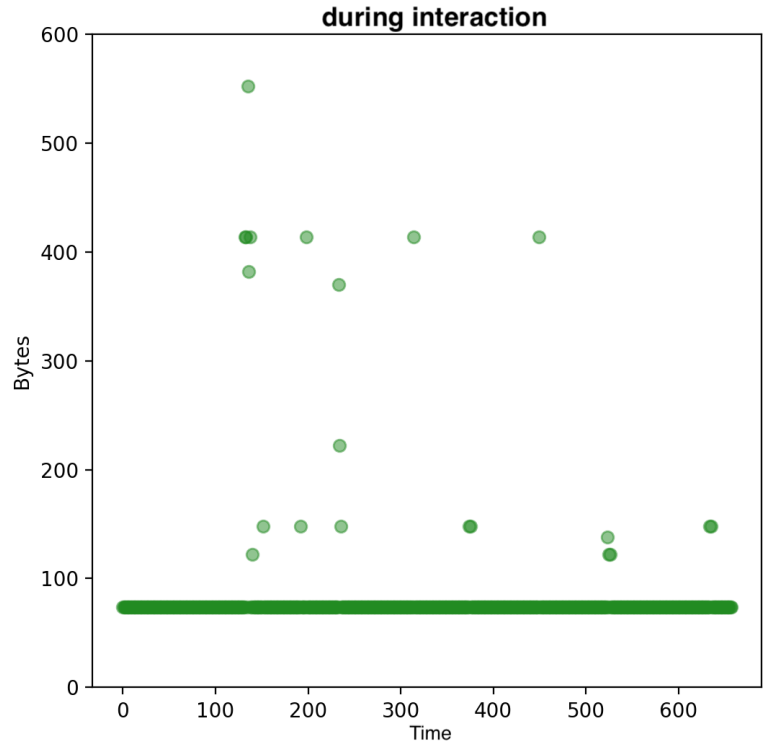


Our local analysis and visualisation allows to:

- Identify on a timeline unusually high or low data traffic
- Detect potentially unwanted traffic

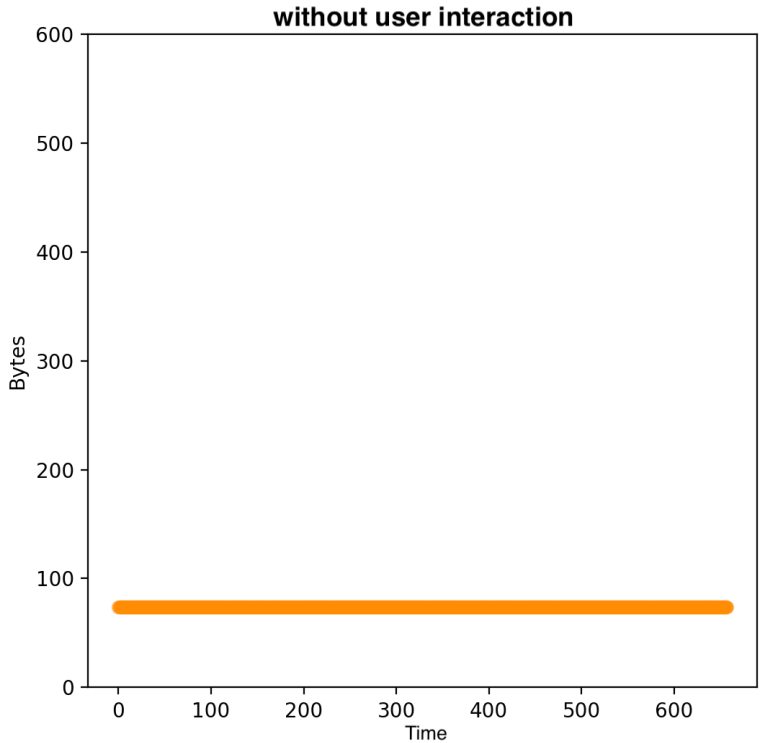
Example Inbound-Traffic analysis

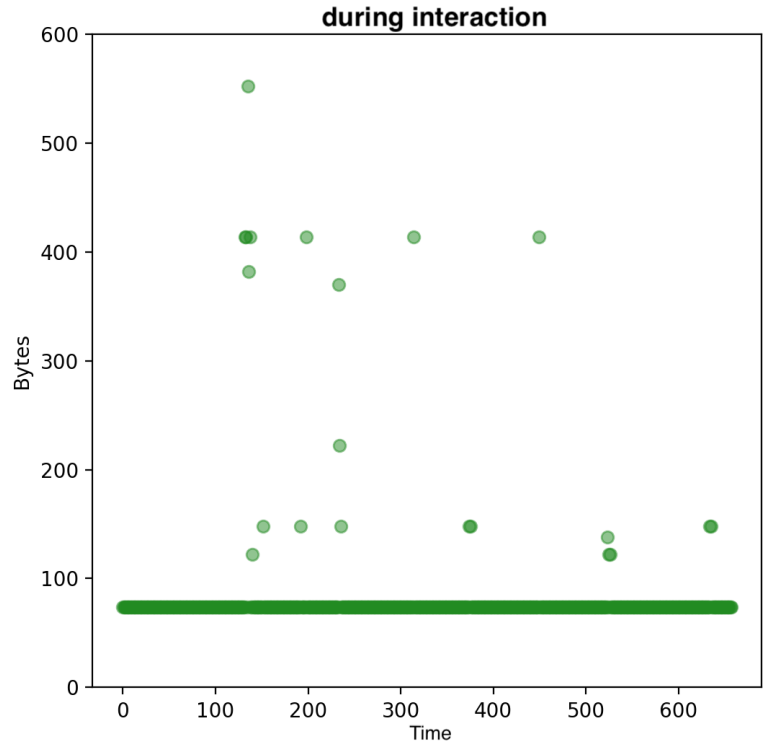




- Measurements of bytes per timeslot: *YEELIGHT Smart LED*
- Metainformation of communication (i.e. number of inbound bytes) leaks information about user interaction
- Communication analysis needs to happen locally so that privacy-sensitive data stays local

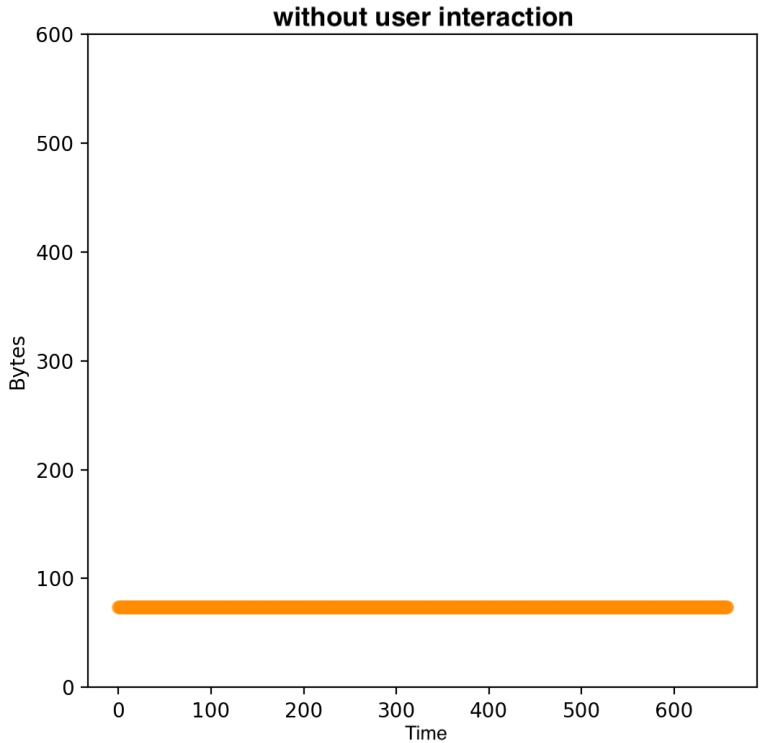
Example Inbound-Traffic analysis

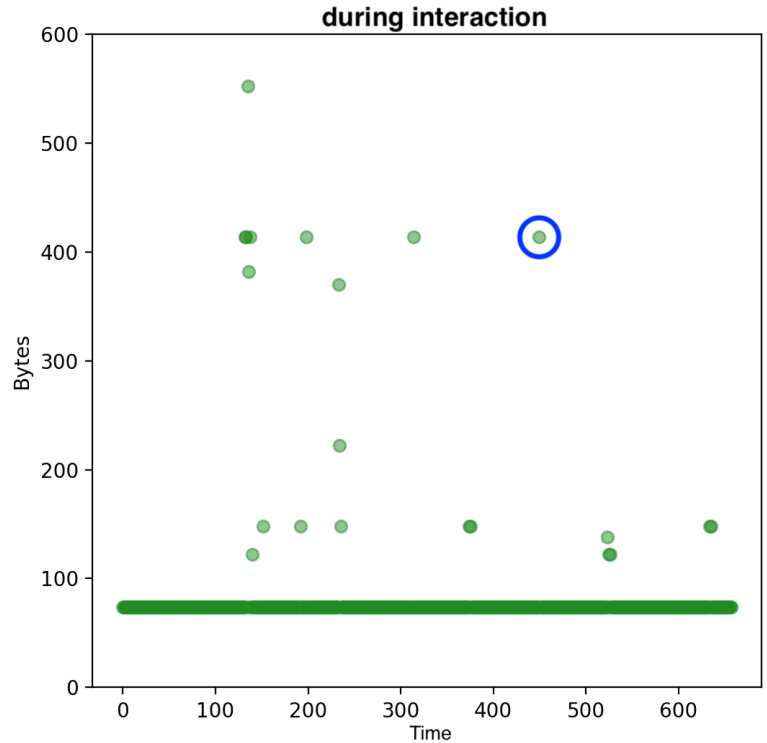




- Measurements of bytes per timeslot: *YEELIGHT Smart LED*
- Metainformation of communication (i.e. number of inbound bytes) leaks information about user interaction
- Communication analysis needs to happen locally so that privacy-sensitive data stays local

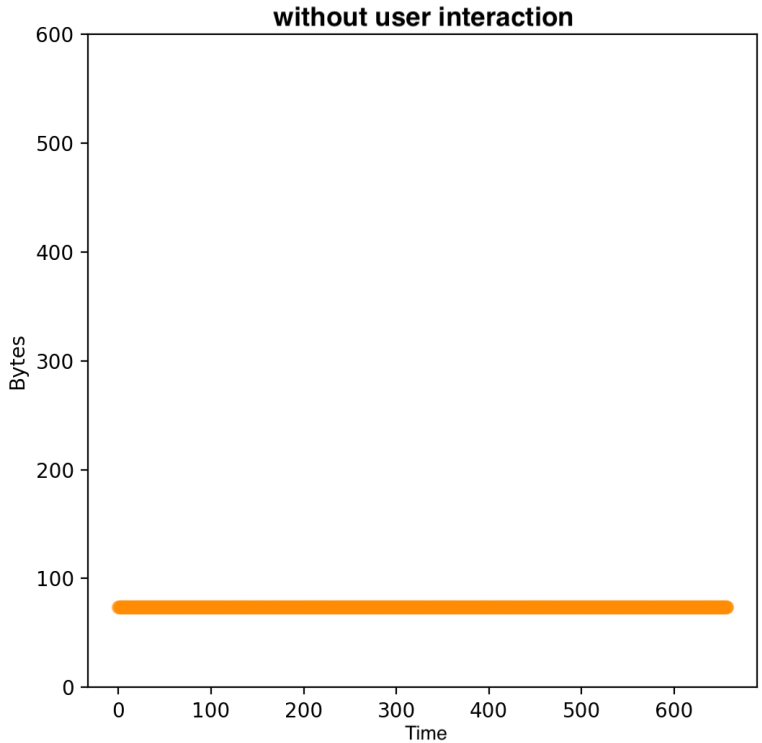
Example Inbound-Traffic analysis

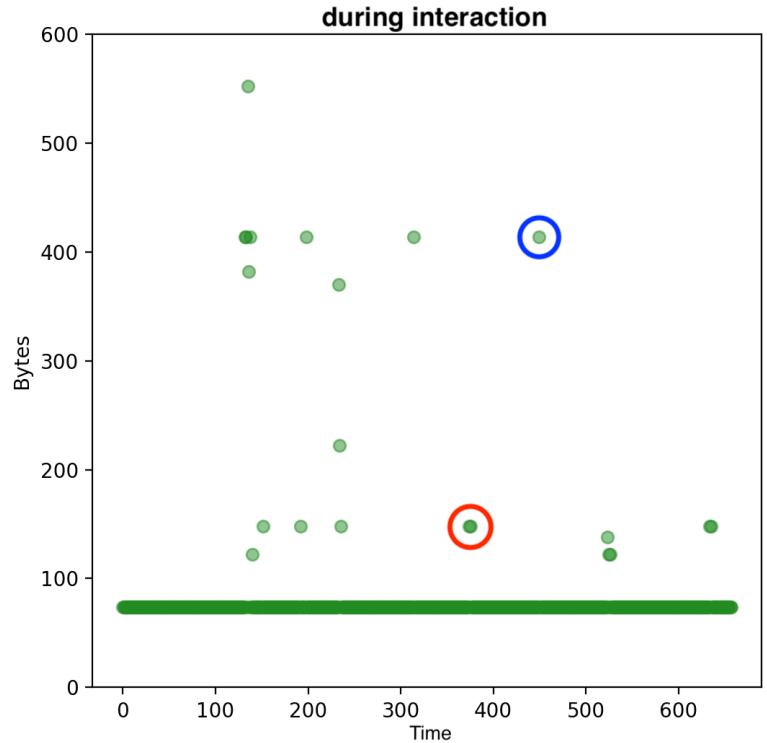




- Measurements of bytes per timeslot: *YEELIGHT Smart LED*
- Metainformation of communication (i.e. number of inbound bytes) leaks information about user interaction
- Communication analysis needs to happen locally so that privacy-sensitive data stays local

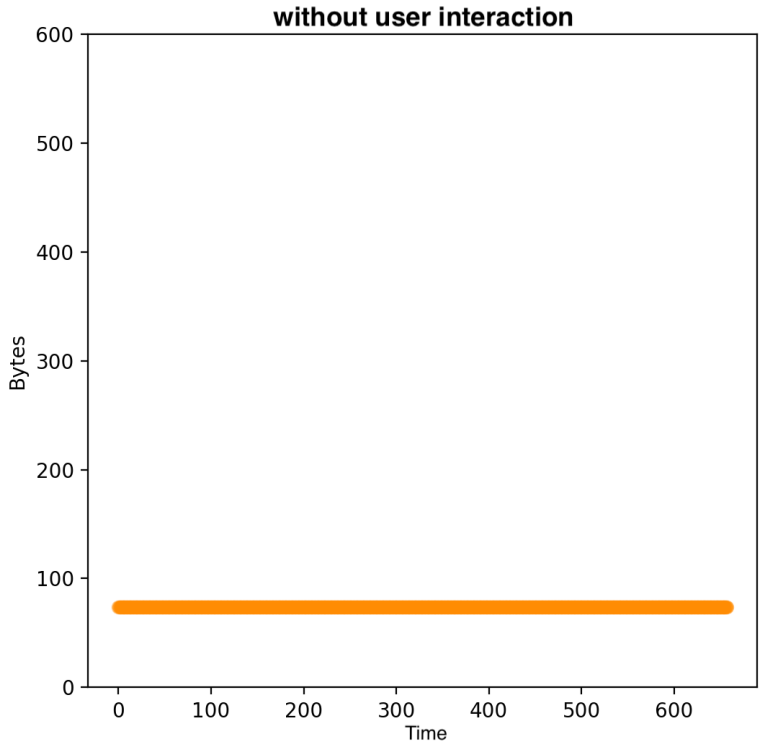
Example Inbound-Traffic analysis

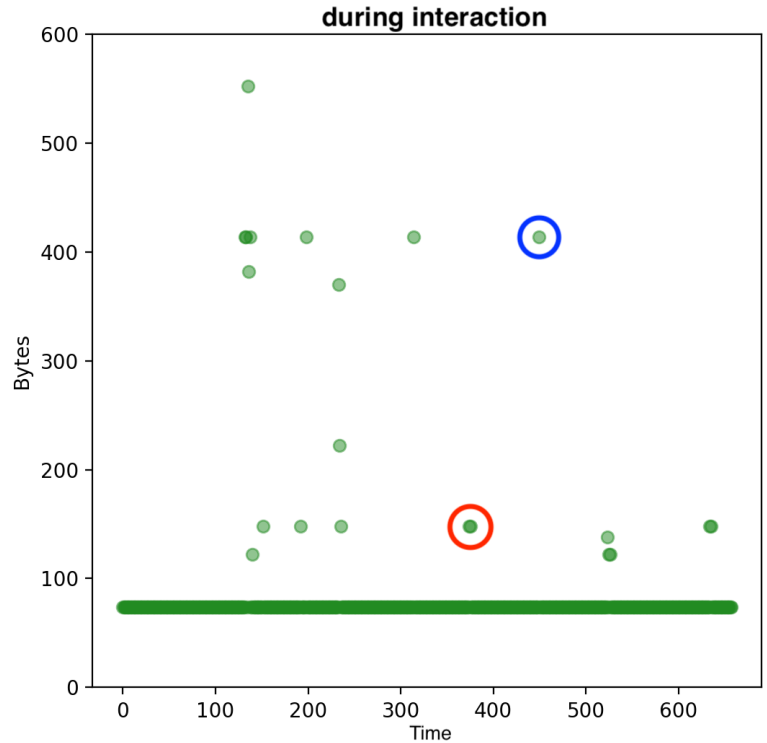




- Measurements of bytes per timeslot: *YEELIGHT Smart LED*
- Metainformation of communication (i.e. number of inbound bytes) leaks information about user interaction
- Communication analysis needs to happen locally so that privacy-sensitive data stays local

Example Inbound-Traffic analysis





- Measurements of bytes per timeslot: *YEELIGHT Smart LED*
- Metainformation of communication (i.e. number of inbound bytes) leaks information about user interaction
- Communication analysis needs to happen locally so that privacy-sensitive data stays local

UNIVERSITÄT PASSAU

NMAP - Command

nmap -sV -version-all -script vulners -oX /my/path/file.xml

- Vulners = Vulnerability Assesment Platform
- Request to API to learn whether any known vulnerabilities exist for a CPE
- Make use of NSE-Scripting Engine

Side Development

Open Source wrapper of NMAP for Elixir (`https://github.com/fklement/hades`)

UNIVERSITÄT PASSAU

1. Introduction

2. Data Acquisition and Tools

3. Conclusion

Conclusion

UNIVERSITÄT PASSAU

- Local-only acquisition and user-friendly representation of network communication data gives the local user an insight into the actual communication of his local IoT devices
- Gathered data is highly sensitive and must be kept local
  - Already metadata-information is privacy-sensitive (see our Light Bulb example)
  - Locally gathered data contains metainformation + actual content
- We developed a framework and a first prototype will be available as an open-source tool
- Our solution helps the users becoming aware of the information contained in communication traces
  - Users can make a more informed decision to share selected traces with professionals or semi-professionals
- Contact: fk@sec.uni-passau.de

Conclusion

UNIVERSITÄT PASSAU

- Local-only acquisition and user-friendly representation of network communication data gives the local user an insight into the actual communication of his local IoT devices
- Gathered data is highly sensitive and must be kept local
  - Already metadata-information is privacy-sensitive (see our Light Bulb example)
  - Locally gathered data contains metainformation + actual content
- We developed a framework and a first prototype will be available as an open-source tool
- Our solution helps the users becoming aware of the information contained in communication traces
  - Users can make a more informed decision to share selected traces with professionals or semi-professionals
- Contact: fk@sec.uni-passau.de

Conclusion

UNIVERSITÄT PASSAU

- Local-only acquisition and user-friendly representation of network communication data gives the local user an insight into the actual communication of his local IoT devices
- Gathered data is highly sensitive and must be kept local
  - Already metadata-information is privacy-sensitive (see our Light Bulb example)
  - Locally gathered data contains metainformation + actual content
- We developed a framework and a first prototype will be available as an open-source tool
- Our solution helps the users becoming aware of the information contained in communication traces
  - Users can make a more informed decision to share selected traces with professionals or semi-professionals
- Contact: fk@sec.uni-passau.de

Conclusion

UNIVERSITÄT PASSAU

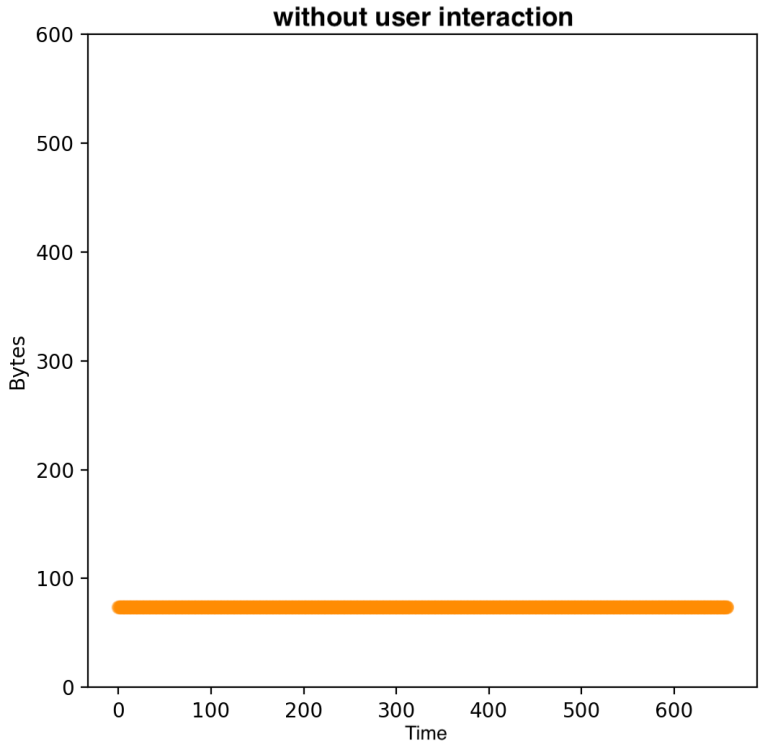
- Local-only acquisition and user-friendly representation of network communication data gives the local user an insight into the actual communication of his local IoT devices
- Gathered data is highly sensitive and must be kept local
  - Already metadata-information is privacy-sensitive (see our Light Bulb example)
  - Locally gathered data contains metainformation + actual content
- We developed a framework and a first prototype will be available as an open-source tool
- Our solution helps the users becoming aware of the information contained in communication traces
  - Users can make a more informed decision to share selected traces with professionals or semi-professionals
- Contact: fk@sec.uni-passau.de

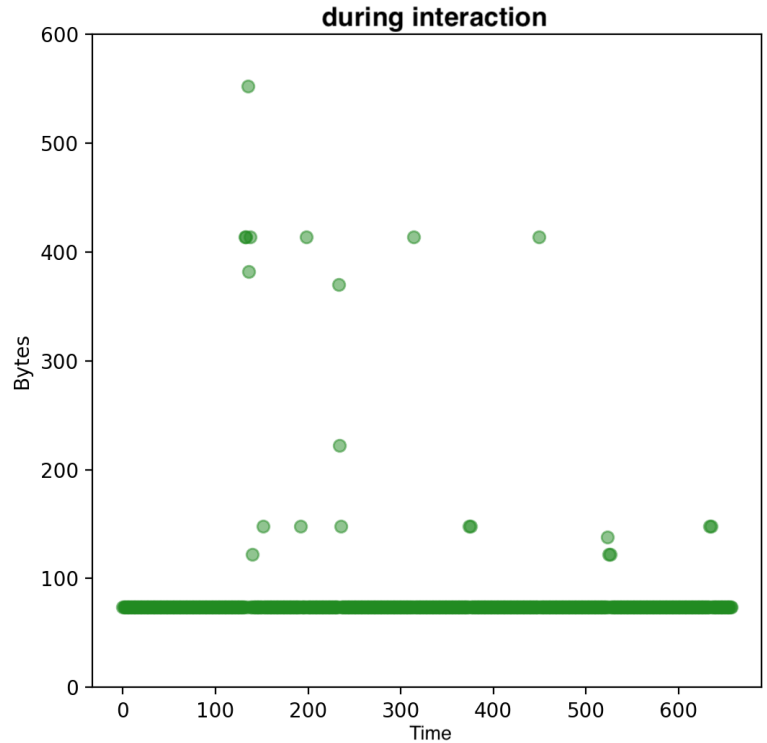
Conclusion

UNIVERSITÄT PASSAU

- Local-only acquisition and user-friendly representation of network communication data gives the local user an insight into the actual communication of his local IoT devices
- Gathered data is highly sensitive and must be kept local
  - Already metadata-information is privacy-sensitive (see our Light Bulb example)
  - Locally gathered data contains metainformation + actual content
- We developed a framework and a first prototype will be available as an open-source tool
- Our solution helps the users becoming aware of the information contained in communication traces
  - Users can make a more informed decision to share selected traces with professionals or semi-professionals
- Contact: fk@sec.uni-passau.de

Example Inbound-Traffic analysis





- Measurements of bytes per timeslot: *YEELIGHT Smart LED*
- Metainformation of communication (i.e. number of inbound bytes) leaks information about user interaction
- Communication analysis needs to happen locally so that privacy-sensitive data stays local

UNIVERSITÄT PASSAU