ThingPot: an interactive Internet-of-Things honeypot

Meng Wang, Javier Santillan, and Fernando Kuipers

Nov. 23, 2017

TUDelft

brightsight®

the number one
security lab
in the world

Motivation

Popularity

- IoT becomes more and more popular

Security challenges

- Limited resources of IoT devices
- Large number of diverse devices

Serious consequences

- IoT-related attacks (e.g. Mirai) have already emerged

Questions

What are the most common protocols used by IoT devices?

Which vulnerabilities and attacks on IoT protocols are known?

Can honeypots be harnessed to identify attack vectors w.r.t. IoT?

What can be done to prevent observed IoT attacks?

What is a honeypot?
What is XMPP?
What is an IoT platform?

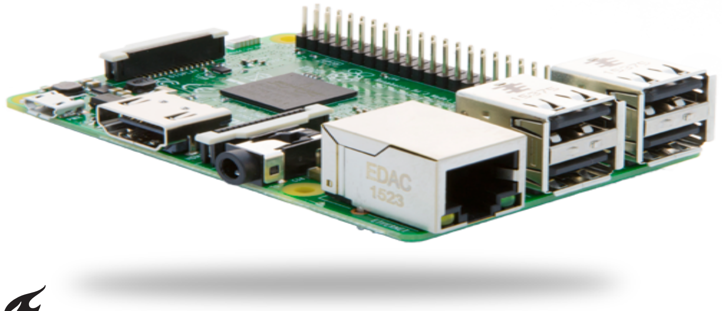
Honeypot: learn by deception!

- ➢ Emulation of a real device
- ➢ Detect, deflect or counteract

In XMPP/REST/… language

Hey! *"I'm a …"*

- SmartTV
- Home appliance
- Medical device
- Sensor system
- Automotive device



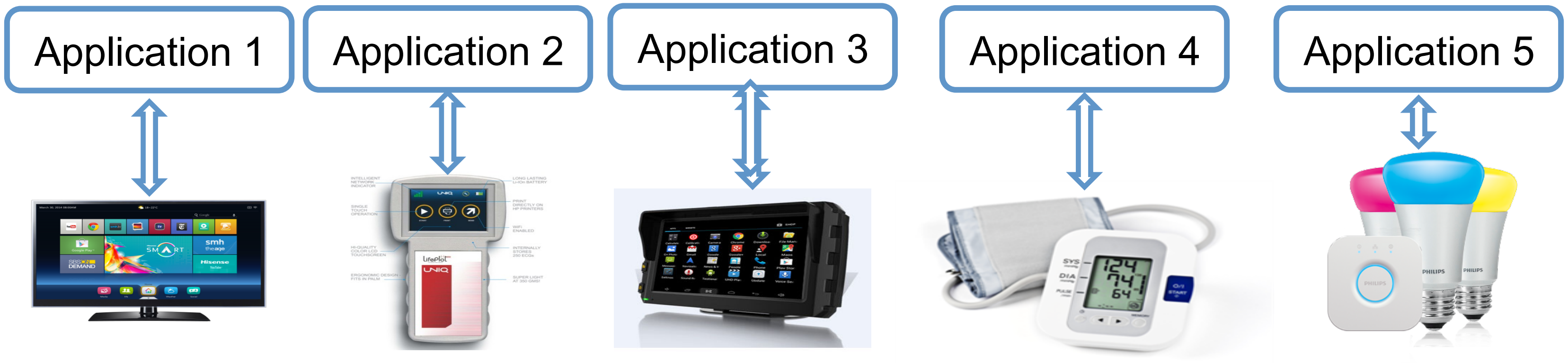
Honeypot: learn by deception!

- Advantages:
  - Collect data on actual attacks
  - Take advantage of emulation
  - Can help IoT security development

- Classification:
  - High Interaction Honeypot (HIH)
  - Low Interaction Honeypot (LIH)
  - Medium Interaction Honeypots (MIH)

XMPP: eXtensible Messaging and Presence Protocol

- Application-layer protocol for instant messaging
- Jabber ID (JID): XMPP account
- Extension for IoT (XEP-0323, 0324, 0325, 0326)



Application 1

Application 2

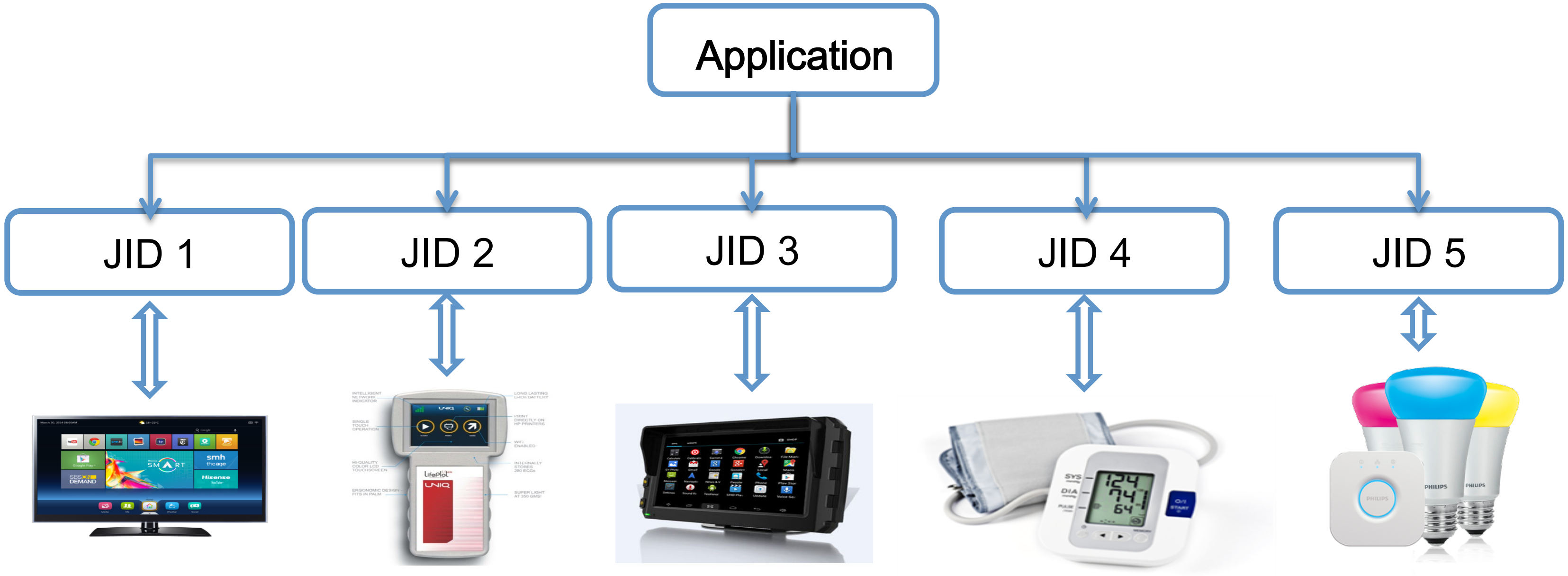
Application 3

Application 4

Application 5

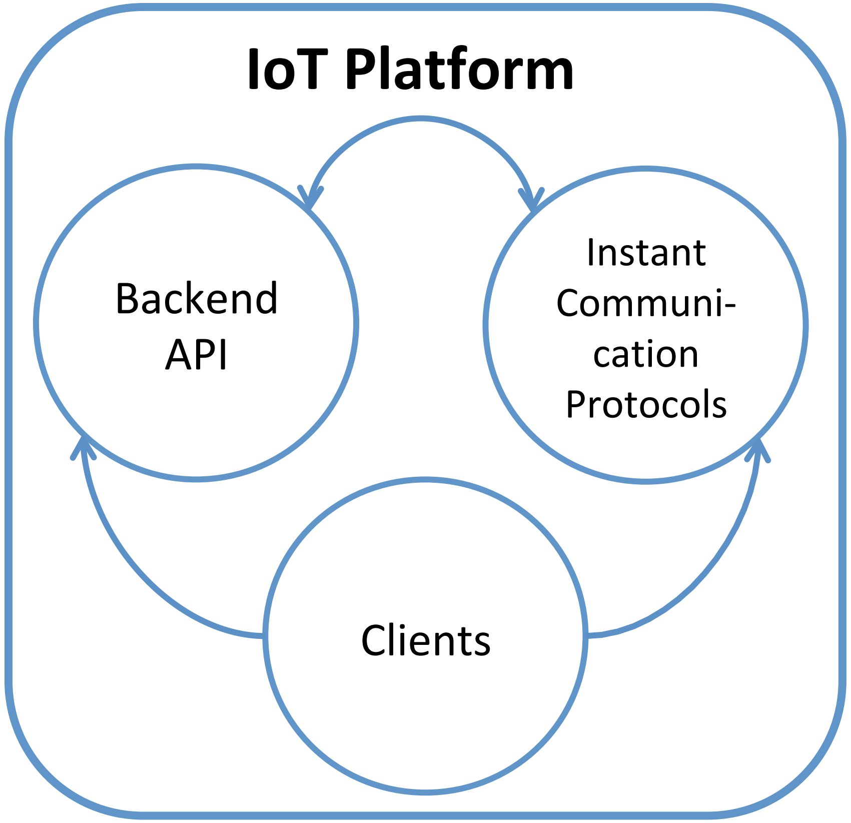
XMPP: eXtensible Messaging and Presence Protocol

- Application-layer protocol for instant messaging
- Jabber ID (JID): XMPP account
- Extension for IoT (XEP-0323, 0324, 0325, 0326)



IoT platform

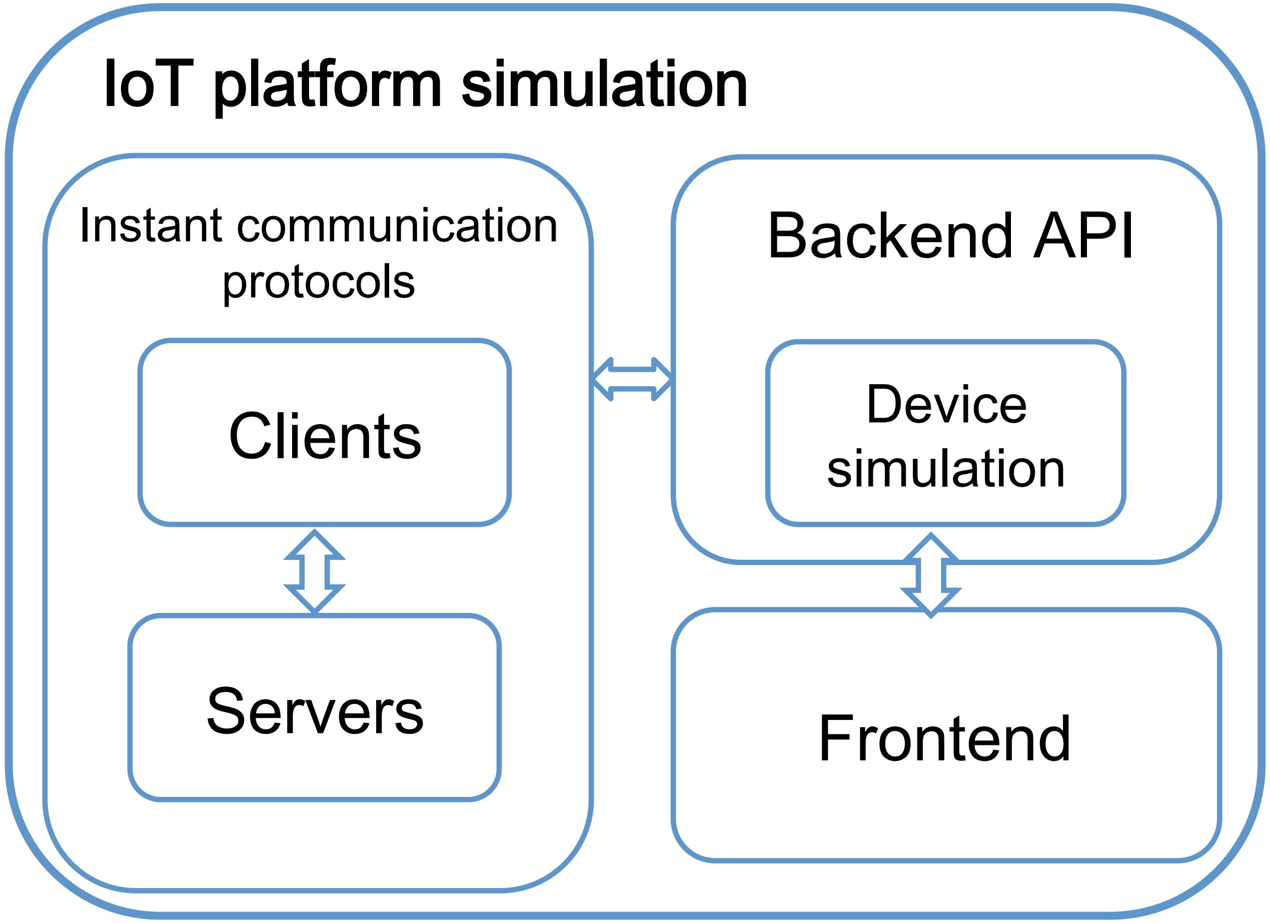
Work and communicate with the devices



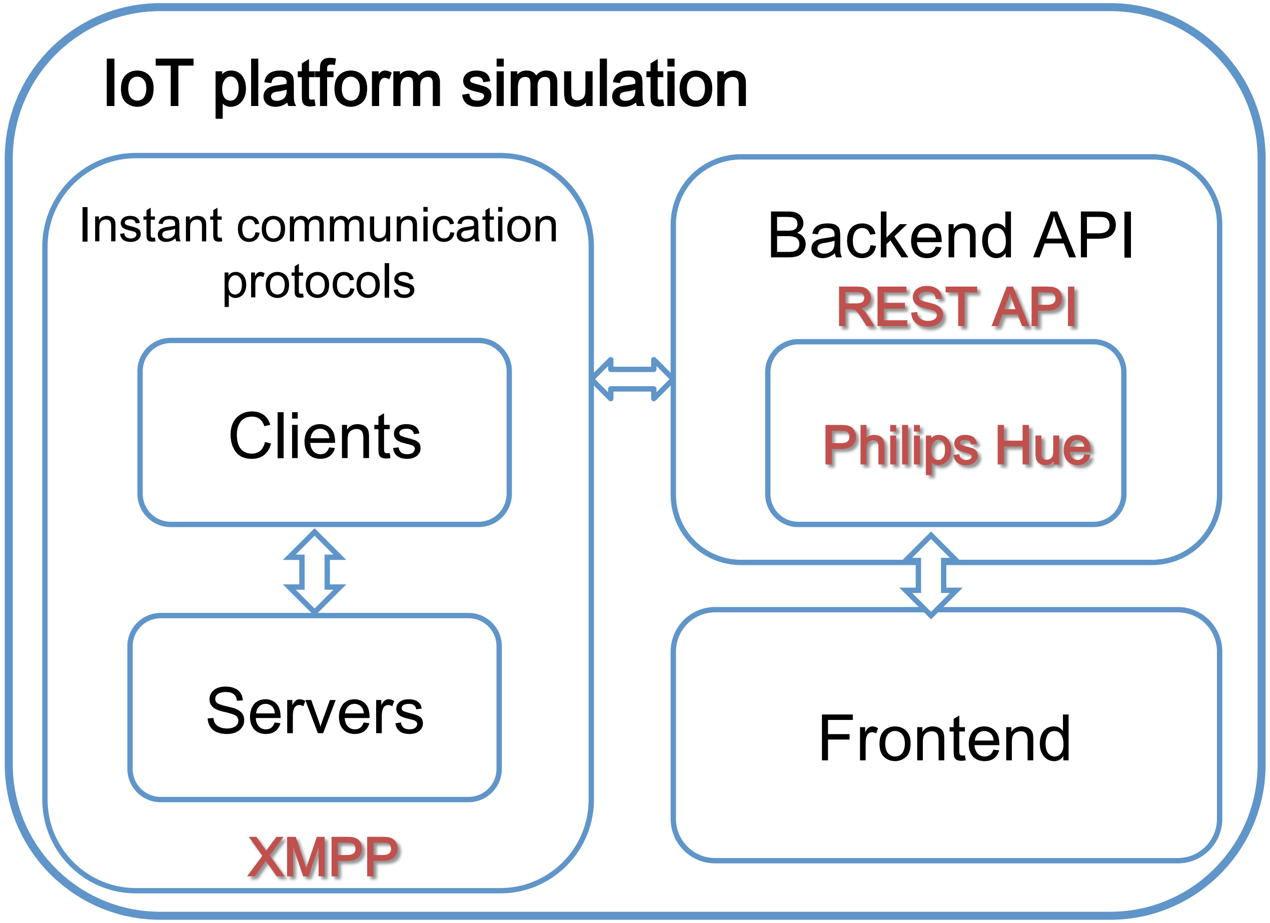
Communication between users and API

Users/developers

ThingPot PoC & use case

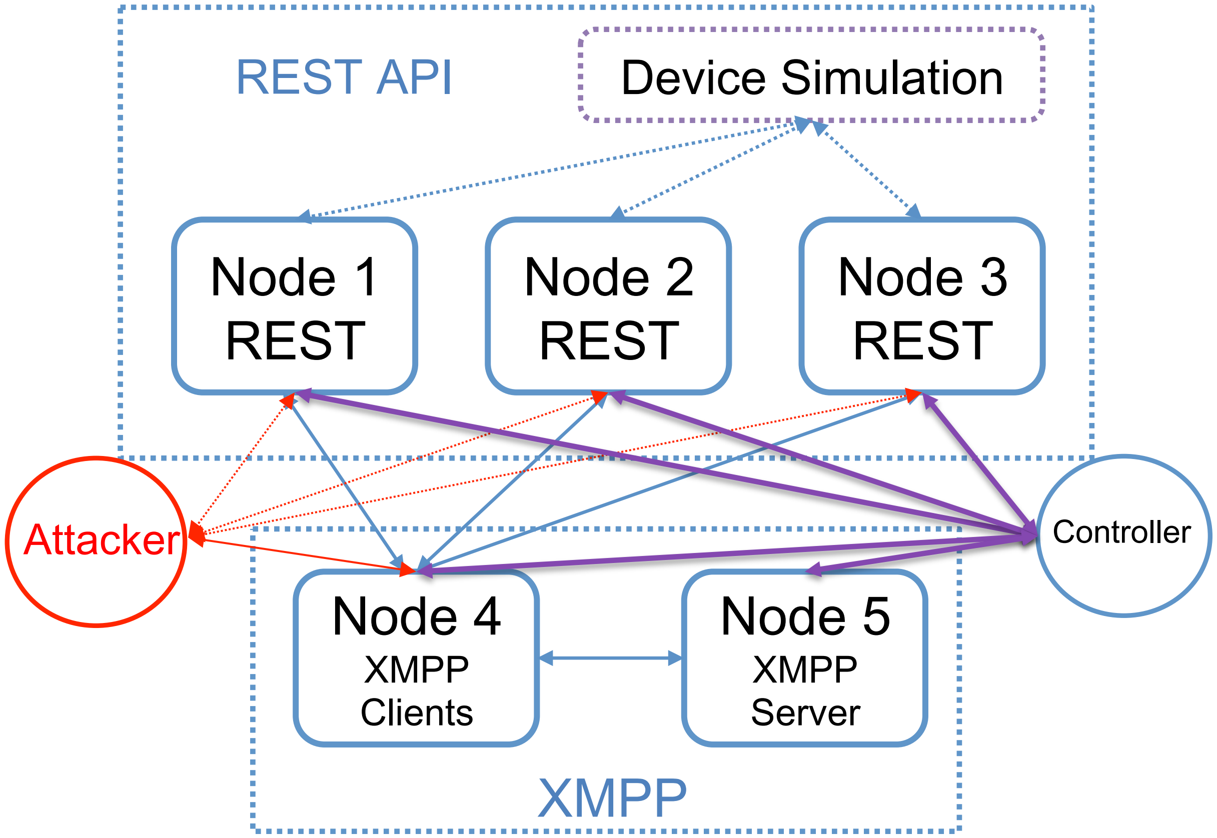


ThingPot PoC & use case



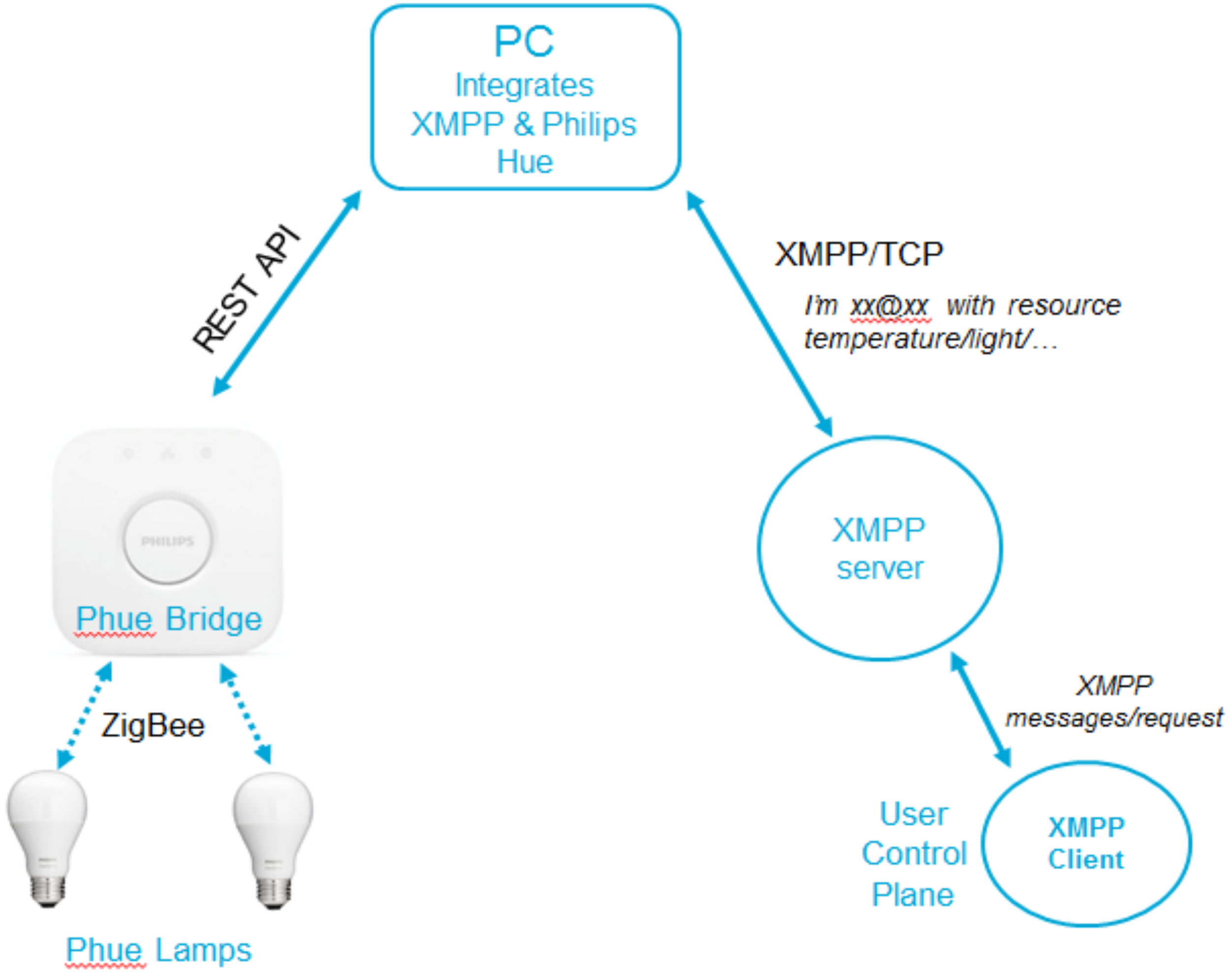
ThingPot PoC & use case

Physical topology



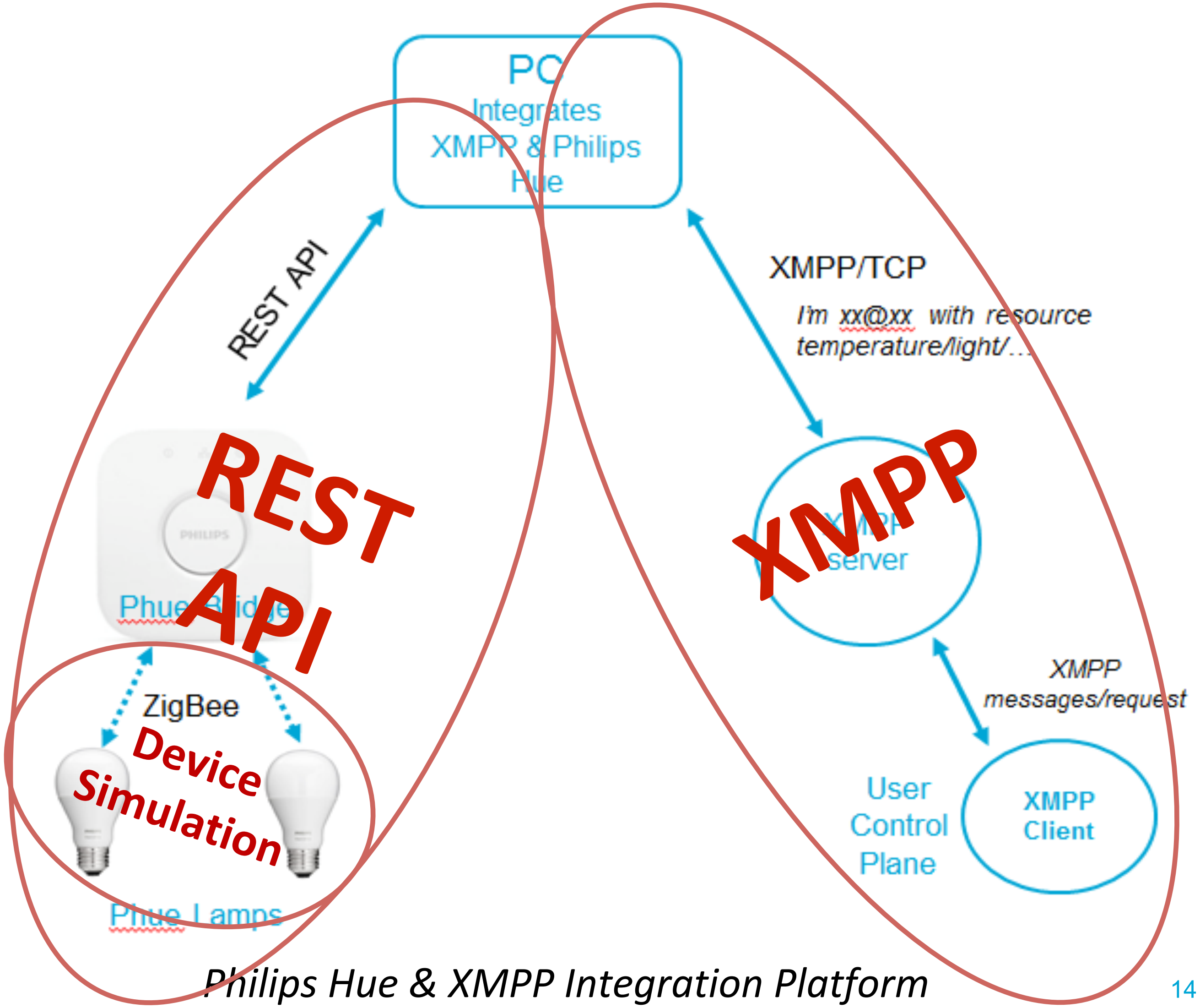
ThingPot implementation & use case

Philips Hue



ThingPot implementation & use case

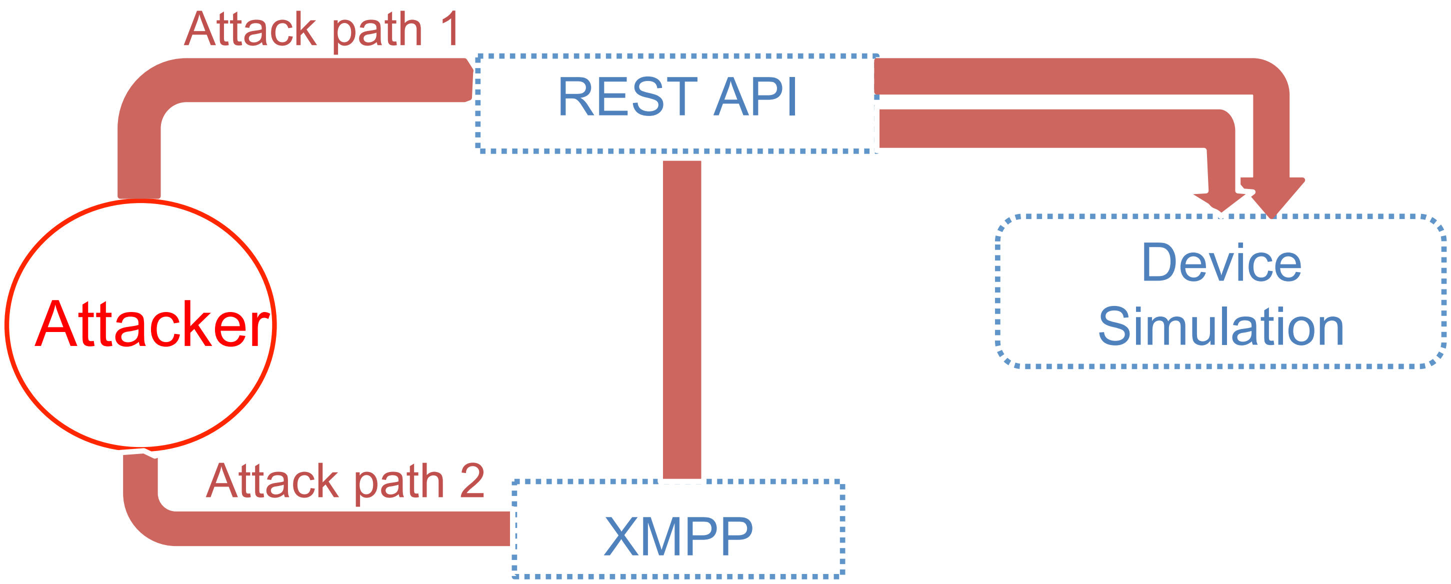
Philips Hue



Philips Hue & XMPP Integration Platform

ThingPot implementation & use case

Attack paths



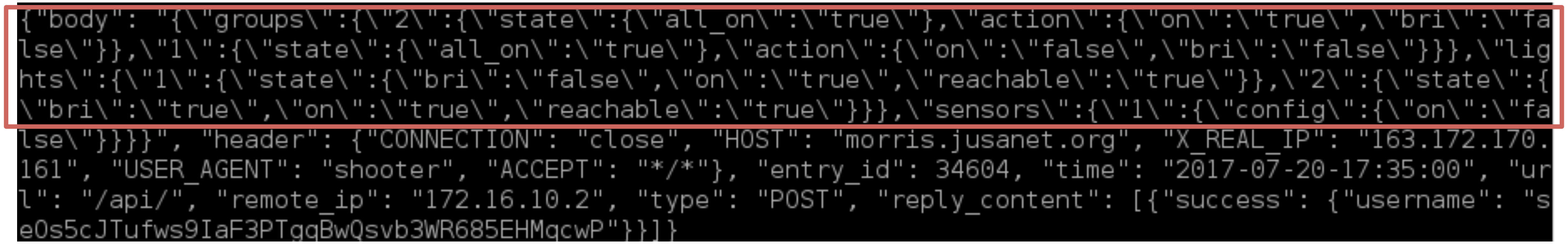
ThingPot in the wild!

Data

- **46** days (from June 22nd to August 7th, 2017)
- **113,741** backend requests in total
- **619** different IPs involved

Findings

1. Targeted attack trying to take control

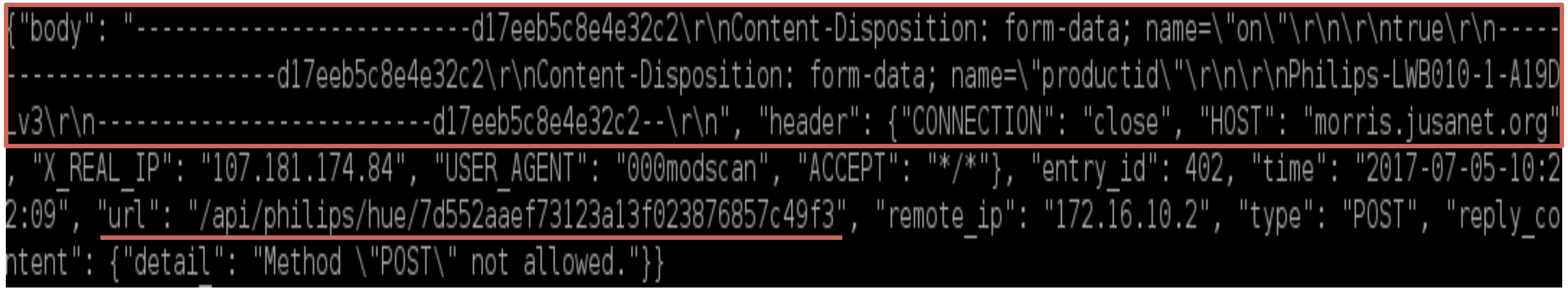


```
{"body": "{\"groups\":{\"2\":{\"state\":{\"all_on\":\"true\"},\"action\":{\"on\":\"true\",\"bri\":\"fa
lse\"}},\"1\":{\"state\":{\"all_on\":\"true\"},\"action\":{\"on\":\"false\",\"bri\":\"false\"}}},\"lig
hts\":{\"1\":{\"state\":{\"bri\":\"false\",\"on\":\"true\",\"reachable\":\"true\"}},\"2\":{\"state\":{
\"bri\":\"true\",\"on\":\"true\",\"reachable\":\"true\"}}},\"sensors\":{\"1\":{\"config\":{\"on\":\"fa
lse\"}}}}}", "header": {"CONNECTION": "close", "HOST": "morris.jusanet.org", "X_REAL_IP": "163.172.170.
161", "USER_AGENT": "shooter", "ACCEPT": "*/*"}, "entry_id": 34604, "time": "2017-07-20-17:35:00", "ur
l": "/api/", "remote_ip": "172.16.10.2", "type": "POST", "reply_content": [{"success": {"username": "s
e0s5cJTufws9IaF3PTgqBwQsvb3WR685EHMqcwP"}}]}
```

"shooter"
31567 requests on the honeypot
92 IPs involved
"/api/" with the POST method

Findings

1. Targeted attack trying to take control
2. Attack with the body following the *multipart/form-data* format



```
{"body": "--------------------------d17eeb5c8e4e32c2\r\nContent-Disposition: form-data; name=\"on\"\r\n\r\ntrue\r\n-----
--------------------d17eeb5c8e4e32c2\r\nContent-Disposition: form-data; name=\"productid\"\r\n\r\nPhilips-LWB010-1-A19D
_v3\r\n--------------------------d17eeb5c8e4e32c2--\r\n", "header": {"CONNECTION": "close", "HOST": "morris.jusanet.org"
, "X_REAL_IP": "107.181.174.84", "USER_AGENT": "000modscan", "ACCEPT": "*/*"}, "entry_id": 402, "time": "2017-07-05-10:2
2:09", "url": "/api/philips/hue/7d552aaef73123a13f023876857c49f3", "remote_ip": "172.16.10.2", "type": "POST", "reply_co
ntent": {"detail": "Method \"POST\" not allowed."}}
```

“000modscan”, “mass”, “botlight”
HTTP POST with interesting body
5392 requests on the honeypot
33 IPs involved
URL: with targeted keyword

Findings

1. Targeted attack trying to take control
2. Attack with the body following the *multipart/form-data* format
3. Attack with url

HTTP GET:
1. /api/philips/hue/{32_chars}
2. /api/phi/light/{32_chars}
3. /api/philips1/hue/{32_chars}
4. /api/philips2/hue-link/{32_chars}
5. /api/belkin/wemo/{32_chars}
6. /api/tplink/light/{32_chars}
7. /api/hue/{0-750}
8./api/phi/light/{32_chars}/tokens
9. /api/{32_chars}/tokens
10. /api/{32_chars}

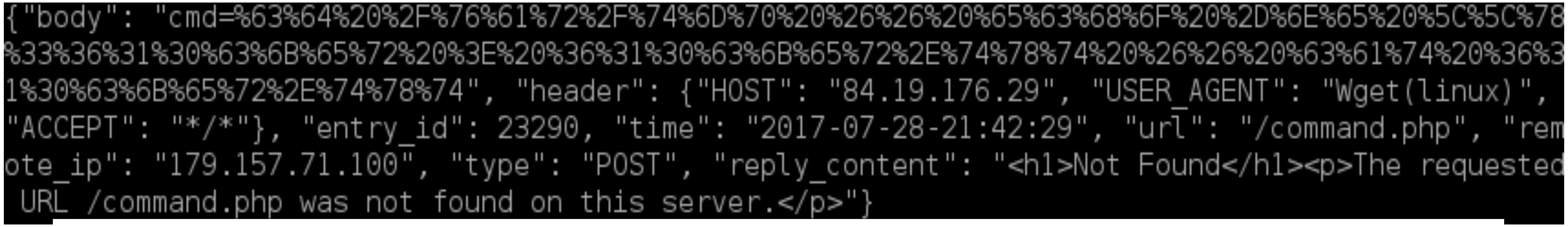
Findings

1. Targeted attack trying to take control
2. Attack with the body following the *multipart/form-data* format
3. Attack with url
4. General scanning tools or libraries

- skipfish
- Nikto
- Jorgee:
- masscan:
- Python library: urllib [9]
- /http:/testp3.pospr.waw.pl/testproxy.php
- Proxyradar: On *https://proxyradar.com/*

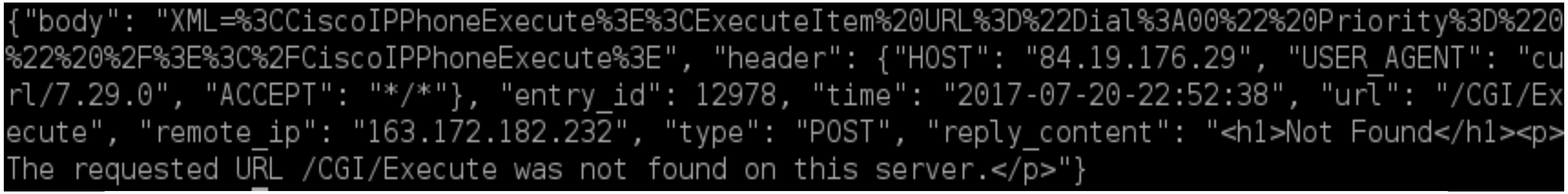
Findings

1. Targeted attack trying to take control
2. Attack with the body following the *multipart/form-data* format
3. Attack with url
4. General scanning tools or libraries
5. Other unrelated attacks



```
{"body": "cmd=%63%64%20%2F%76%61%72%2F%74%6D%70%20%26%26%20%65%63%68%6F%20%2D%6E%65%20%5C%5C%78
%33%36%31%30%63%6B%65%72%20%3E%20%36%31%30%63%6B%65%72%2E%74%78%74%20%26%26%20%63%61%74%20%36%3
1%30%63%6B%65%72%2E%74%78%74", "header": {"HOST": "84.19.176.29", "USER_AGENT": "Wget(linux)",
"ACCEPT": "*/*"}, "entry_id": 23290, "time": "2017-07-28-21:42:29", "url": "/command.php", "rem
ote_ip": "179.157.71.100", "type": "POST", "reply_content": "<h1>Not Found</h1><p>The requested
 URL /command.php was not found on this server.</p>"}
```

$$cd/var/tmpecho-ne\backslash\backslash x3610cker>610cker.txtcat610cker.txt$$



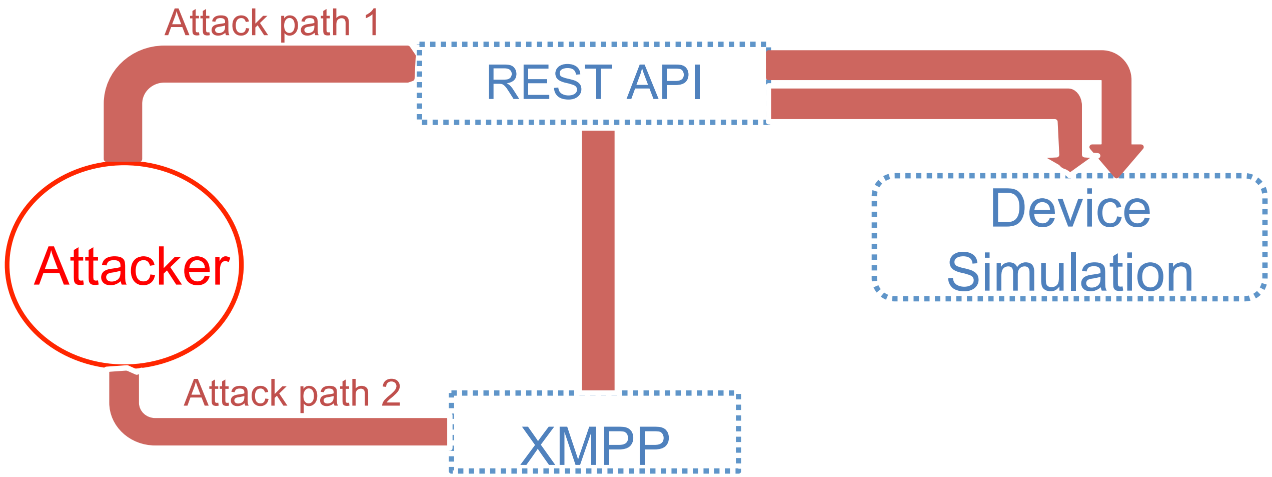
```
{"body": "XML=%3CCiscoIPPhoneExecute%3E%3CExecuteItem%20URL%3D%22Dial%3A00%22%20Priority%3D%220
%22%20%2F%3E%3C%2FCiscoIPPhoneExecute%3E", "header": {"HOST": "84.19.176.29", "USER_AGENT": "cu
rl/7.29.0", "ACCEPT": "*/*"}, "entry_id": 12978, "time": "2017-07-20-22:52:38", "url": "/CGI/Ex
ecute", "remote_ip": "163.172.182.232", "type": "POST", "reply_content": "<h1>Not Found</h1><p>
The requested URL /CGI/Execute was not found on this server.</p>"}
```

$$XML=\backslash<CiscoIPPhoneExecute\backslash>\backslash<ExecuteItem\backslash URL\backslash=\backslash"Dial$$

$$\backslash:00\backslash"\backslash Priority\backslash=\backslash"0\backslash"\backslash\backslash/\backslash>\backslash<\backslash/CiscoIPPhoneExecute\backslash>$$

Conclusion

- XMPP
  - ✓ Integration of different components in multi-node communications
  - ✓ May provide additional layers of security
  - ✓ Attacker activities are very limited
- REST
  - ✓ Large number of attacker activities



Conclusion

- **ThingPot:** First IoT platform honeypot (https://github.com/Mengmengada/ThingPot)

- **Five types of attacks were found:**
  - ✓ Attackers are looking (e.g. via Shodan.io) for devices like **Philips Hue, Belkin Wemo, TPlink**, etc.
  - ✓ Attackers are interested to obtain information about the smart devices and **to take control of them**
  - ✓ Attackers are using the **TOR network** to mask their real source address

Thank you for your attention!