



AN ANALYSIS OF TRUST IN SMART HOME DEVICES

Davide Ferraris

PhD Student @ University of Malaga, NICS lab

Daniel Bastos

Senior Researcher @ British Telecom

Co-Authors: Dr. Carmen Fernandez Gago, Dr. Fadi El-Moussa, Prof. Javier Lopez



Outline



- ☐ Introduction
- ☐ Motivation
- ☐ Use Case
- ☐ Findings
- ☐ Trust Model
- ☐ Conclusion

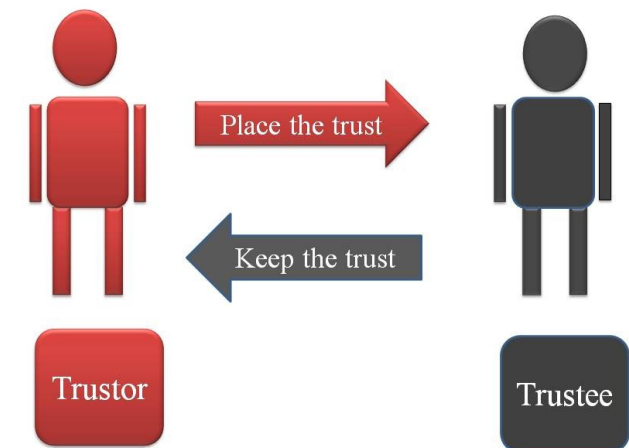


Introduction (Trust)



Trust is difficult to define because:

- ❑ “Trust is a multidimensional, multidisciplinary and multifaceted concept” (Yan et al., 2008)
- ❑ “The personal, unique and temporal expectation that a trustor places on a trustee regarding the outcome of an interaction between them” (Moyano et al., 2012)





Introduction (IoT)



IoT

- Connection “everywhere”
- Remote Control
- Protocols (Many)
- Low protection
- Low computation power



Smart Home security enhanced by Trust





Motivation



VS

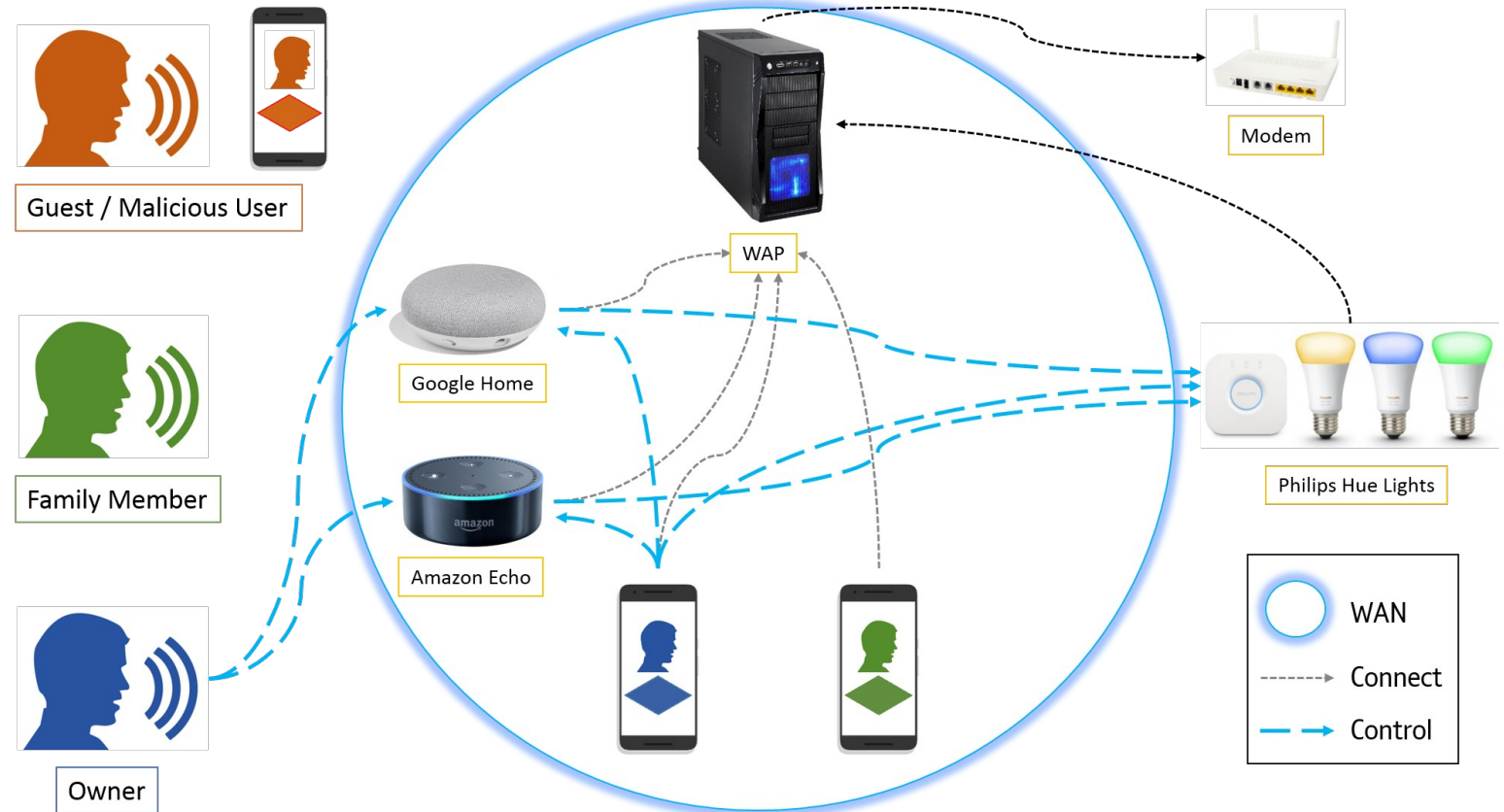




Use Case



- Smart Home Scenario
- Users
- IoT Devices





Findings



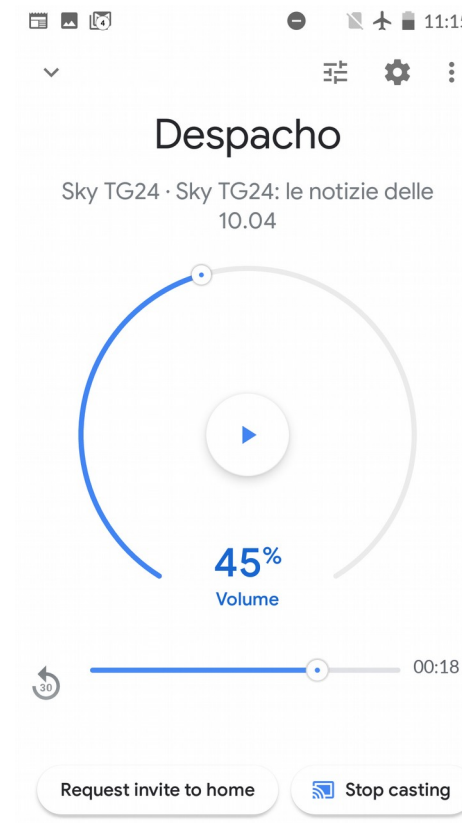
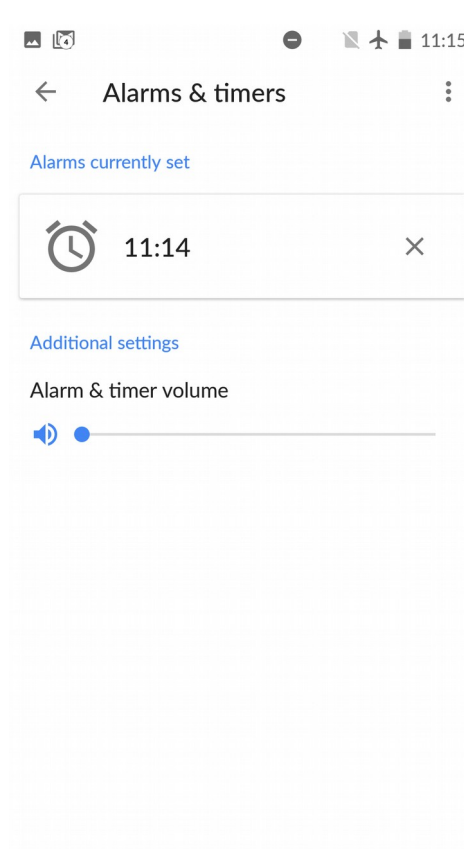
- ❑ Alexa (Only the owner can see what is going on through the smartphone app)
- ❑ Google (Too much trust for the connected users, every connected user can see what is going on and can cast commands)
- ❑ Google (Wi-Fi steal) Anytime the Wi-Fi is not available the device creates a WAP that allow any user to configure it. (Not ownership)
- ❑ Hue (Some details are revealed in clear: Bridge ID, IP, commands)



Findings



Google





Findings



UNIVERSIDAD DE MÁLAGA



TECHNISCHE UNIVERSITÄT DARMSTADT



University of Kent



Atos

Alexa & Hue

*wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.13.200 && ip.dst == 192.168.13.36

No.	Time	Source	Destination	Protocol	Length	Info
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	74	33753 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33753 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	HTTP	246	PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33753 → http(80) [ACK] Seq=193 Ack=516 Win=8704
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33753 → http(80) [FIN, ACK] Seq=193 Ack=516 Win=8
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	66	[TCP Dup ACK 489554#1] 33753 → http(80) [ACK] Seq=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	74	33754 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33754 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	HTTP	159	GET /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33754 → http(80) [ACK] Seq=106 Ack=1178 Win=89984
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33754 → http(80) [FIN, ACK] Seq=106 Ack=1179 Win=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	74	33755 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33755 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	HTTP	247	PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33755 → http(80) [ACK] Seq=194 Ack=516 Win=8704
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33755 → http(80) [FIN, ACK] Seq=194 Ack=517 Win=8
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	66	[TCP Dup ACK 489554#1] 33755 → http(80) [ACK] Seq=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	74	33756 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33756 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	HTTP	159	GET /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33756 → http(80) [ACK] Seq=106 Ack=1179 Win=89984
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33756 → http(80) [FIN, ACK] Seq=106 Ack=1180 Win=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	66	[TCP Dup ACK 489554#1] 33756 → http(80) [ACK] Seq=

TCP payload (192 bytes)

▼ Hypertext Transfer Protocol

PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state HTTP/1.1\r\n

[Expert Info (Chat/Sequence): PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state HTTP/1.1\r\n]

[PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: PUT

Request URI: /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state

Request Version: HTTP/1.1

Host: 192.168.13.36\r\n

Accept: */*\r\n

Content-type: application/x-www-form-urlencoded\r\n

Content-Length: 12\r\n

\r\n

[Full request URI: http://192.168.13.36/api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state]

[HTTP request 1/1]

[Response in frame: 489551]

File Data: 12 bytes

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: ("on": true) = ""

Key: ("on": true)

Value:

0050 49 4e 4a 57 59 6e 57 57 52 4f 56 54 4e 47 73 51 INjWmM ROVtNgS

0060 74 69 4d 44 35 2d 79 2f 6c 69 67 68 74 73 2f 31 tIMDS-y/ lights/1

0070 2f 73 74 61 74 65 20 48 54 54 50 2f 31 2e 31 0d /state H TTP/1.1

0080 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 31 Host: 1 92.168.1

0090 33 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 3.36: Ac cept: */

00a0 2a 0d 0a 43 6f 6e 74 65 6e 74 2d 74 79 70 65 3a * Conte nt-type:

00b0 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 applica tion/x-w

00c0 77 77 2d 66 6f 72 6d 2d 75 72 6c 6e 6e 63 6f 64 ww-form- urlencod

00d0 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 ed- Cont ent-Leng

00e0 74 68 3a 20 31 33 0d 0a 0d 0a 7d 22 6f 6e 22 30 th: 12 -["on"]

00f0 20 74 72 75 65 7d true

Key (urlencoded-form.key), 12 bytes

Packets: 490802 · Displayed: 109 (0.0%) Profile: Default

*wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.13.200 && ip.dst == 192.168.13.36

No.	Time	Source	Destination	Protocol	Length	Info
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	74	33753 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33753 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	HTTP	246	PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33753 → http(80) [ACK] Seq=193 Ack=516 Win=8704
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33753 → http(80) [FIN, ACK] Seq=193 Ack=516 Win=8
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	66	[TCP Dup ACK 489554#1] 33753 → http(80) [ACK] Seq=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	74	33754 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33754 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	HTTP	159	GET /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33754 → http(80) [ACK] Seq=106 Ack=1178 Win=89984
48.	2019-03-06 10:15:28.	Android.local	Philips-hue.local	TCP	54	33754 → http(80) [FIN, ACK] Seq=106 Ack=1179 Win=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	74	33755 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33755 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	HTTP	247	PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33755 → http(80) [ACK] Seq=194 Ack=516 Win=8704
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33755 → http(80) [FIN, ACK] Seq=194 Ack=517 Win=8
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	66	[TCP Dup ACK 489554#1] 33755 → http(80) [ACK] Seq=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	74	33756 → http(80) [SYN] Seq=0 Win=65535 Len=0 MSS=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33756 → http(80) [ACK] Seq=1 Ack=1 Win=87616 Len=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	HTTP	159	GET /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33756 → http(80) [ACK] Seq=106 Ack=1179 Win=89984
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	54	33756 → http(80) [FIN, ACK] Seq=106 Ack=1180 Win=
48.	2019-03-06 10:15:41.	Android.local	Philips-hue.local	TCP	66	[TCP Dup ACK 489554#1] 33756 → http(80) [ACK] Seq=

▼ Hypertext Transfer Protocol

PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state HTTP/1.1\r\n

[Expert Info (Chat/Sequence): PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state HTTP/1.1\r\n]

[PUT /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: PUT

Request URI: /api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state

Request Version: HTTP/1.1

Host: 192.168.13.36\r\n

Accept: */*\r\n

Content-type: application/x-www-form-urlencoded\r\n

Content-Length: 13\r\n

\r\n

[Full request URI: http://192.168.13.36/api/7-00kj1DrIjWlCXvDlNjWmMROVtNgSQtIMDS-y/lights/1/state]

[HTTP request 1/1]

[Response in frame: 489129]

File Data: 13 bytes

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: ("on": false) = ""

Key: ("on": false)

Value:

0050 49 4e 4a 57 59 6e 57 57 52 4f 56 54 4e 47 73 51 INjWmM ROVtNgS

0060 74 69 4d 44 35 2d 79 2f 6c 69 67 68 74 73 2f 31 tIMDS-y/ lights/1

0070 2f 73 74 61 74 65 20 48 54 54 50 2f 31 2e 31 0d /state H TTP/1.1

0080 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 31 Host: 1 92.168.1

0090 33 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 3.36: Ac cept: */

00a0 2a 0d 0a 43 6f 6e 74 65 6e 74 2d 74 79 70 65 3a * Conte nt-type:

00b0 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 applica tion/x-w

00c0 77 77 2d 66 6f 72 6d 2d 75 72 6c 6e 6e 63 6f 64 ww-form- urlencod

00d0 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 ed- Cont ent-Leng

00e0 74 68 3a 20 31 33 0d 0a 0d 0a 7d 22 6f 6e 22 30 th: 13 -["on"]

00f0 20 74 72 75 65 7d false

Key (urlencoded-form.key), 13 bytes

Packets: 490648 · Displayed: 109 (0.0%) Profile: Default



Findings



Google & Hue



UNIVERSIDAD
DE MÁLAGA



TECHNISCHE
UNIVERSITÄT
DARMSTADT



University of
Kent



Atos

*enp17s0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 192.168.13.36

No.	Time	Source	Destination	Protocol	Length	Info
158	2019-03-06 12:50:28...	diagnostics.meethue.com	Philips-hue.local	TCP	54	http(80) → 50670 [FIN, ACK] Seq=328 Ack=1143 Win=0
161	2019-03-06 12:50:31...	time2.google.com	Philips-hue.local	NTP	90	NTP Version 4, server
165	2019-03-06 12:50:37...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TLSv1.2	232	Application Data
168	2019-03-06 12:50:37...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	https(443) → 54909 [ACK] Seq=1091 Ack=1294 Win=19
178	2019-03-06 12:51:07...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	[TCP Keep-Alive ACK] https(443) → 54909 [ACK] Seq=...
191	2019-03-06 12:51:28...	diagnostics.meethue.com	Philips-hue.local	TCP	54	http(80) → 50670 [RST] Seq=329 Win=0 Len=0
194	2019-03-06 12:51:29...	time1.google.com	Philips-hue.local	NTP	90	NTP Version 4, server
195	2019-03-06 12:51:29...	time4.google.com	Philips-hue.local	NTP	90	NTP Version 4, server
197	2019-03-06 12:51:30...	time3.google.com	Philips-hue.local	NTP	90	NTP Version 4, server
201	2019-03-06 12:51:35...	time2.google.com	Philips-hue.local	NTP	90	NTP Version 4, server
203	2019-03-06 12:51:37...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	[TCP Keep-Alive ACK] https(443) → 54909 [ACK] Seq=...
225	2019-03-06 12:52:04...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TLSv1.2	229	Application Data
227	2019-03-06 12:52:04...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	https(443) → 54909 [ACK] Seq=1266 Ack=1502 Win=19
230	2019-03-06 12:52:10...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TLSv1.2	229	Application Data
232	2019-03-06 12:52:10...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	https(443) → 54909 [ACK] Seq=1441 Ack=1710 Win=20
238	2019-03-06 12:52:17...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	https(443) → 54909 [ACK] Seq=1441 Ack=1749 Win=20
239	2019-03-06 12:52:17...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TLSv1.2	89	Application Data
241	2019-03-06 12:52:18...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TLSv1.2	230	Application Data
244	2019-03-06 12:52:18...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	https(443) → 54909 [ACK] Seq=1652 Ack=1958 Win=21
249	2019-03-06 12:52:23...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TLSv1.2	232	Application Data
252	2019-03-06 12:52:23...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	https(443) → 54909 [ACK] Seq=1830 Ack=2169 Win=22
260	2019-03-06 12:52:34...	time1.google.com	Philips-hue.local	NTP	90	NTP Version 4, server
265	2019-03-06 12:52:53...	91.18.155.104.bc.googleusercontent...	Philips-hue.local	TCP	54	[TCP Keep-Alive ACK] https(443) → 54909 [ACK] Seq=...

Acknowledgment number: 1958 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 215
[Calculated window size: 215]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xae61 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Bytes in flight: 178]
[Bytes sent since last PSH flag: 178]
[Timestamps]
[Time since first frame in this TCP stream: 216.748443000 seconds]
[Time since previous frame in this TCP stream: 4.247012000 seconds]
TCP payload (178 bytes)
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 173
Encrypted Application Data: f079c29c43580b9d5a98b2d0ae4f757f2d339a6ce49bf231....

0030 00 d7 ae 61 00 00 17 03 03 00 ad f0 70 c2 9c 43 ...a... p...C
0040 58 0b 9d 5a 98 b2 d0 ae 4f 75 7f 2d 33 9a 6c e4 X..Z... Ou..3..1
0050 3b f2 31 27 09 76 47 b5 67 85 f0 b8 08 43 8f 08 .1.vG. g...C
0060 3e 1a be aa 67 57 04 2a bf 87 f2 fe ca 5c aa ad >...W* ...X
0070 45 15 e4 71 9d b9 cb 61 ed 73 bc df 58 43 ef b3 ...q..a..s..XC..
0080 52 7b 64 65 a6 38 bf 24 b7 e2 1d 61 4e ce 16 99 R(de.8.S...aN..
0090 ce 1f 92 b8 15 3d 74 71 bc b8 35 f2 a1 a0 3a 8ftq...5...
00a0 83 8f 33 38 f1 16 58 e8 30 b4 f5 d8 69 db 14 c3 ...38.X. 0...1..
00b0 45 8f 41 bb 2e 4c 11 64 d4 ba b1 72 79 ea 3e a0 E.A..L.d...ry>
00c0 34 19 2a 75 a8 a5 a7 d5 88 f8 40 a5 2e 5d 0b f8 4*u... .0..].
00d0 79 13 51 02 35 e6 79 af 6a 2e c9 3d 4d 0b 0b 6c y.Q.5.y. j..=Mk.1

Payload is encrypted application data (ssl.app_data), 173 bytes

Packets: 354 · Displayed: 71 (20.1%)

Profile: Default



Trust model



How the system is? Improvements?

- ☐ Google: Trust in the users, (set-up) security must be improved
- ☐ Alexa: Less trust in the other users, (set-up) security can be improved
- ☐ Hue: “Physical” trust, (set-up) good security measure



Trust Model



- ❑ Role: HO, HM, HG, MU
- ❑ Context: {1,2,3,4}
- ❑ Score: {0,1,2,3,4,5}

- ❑ Trust Metric : $TM(\text{Role}, \text{Context}, \text{Score})$

How it works? Subtraction of Score and Context to decide if a user is allowed to do something.



Trust Model



Trust Metric : $TM(\text{Role}, \text{Context}, \text{Score})$

Possible values (Negative, Zero, Positive)

Negative (No actions are allowed for the particular context)

Zero (You can only check what is going on)

Positive (You are trusted enough to cast commands)



Conclusion



- ❑ Different trust models related to Alexa, Google and Hue
- ❑ Improvement is needed
- ❑ Improvement proposed

- ❑ Contact: ferraris@uma.es



Questions?



Thanks to the European Commission, NeCS Project and to the university of Malaga for the opportunity given to me.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675320.

This work reflects only the author's view and the Research Executive Agency is not responsible for any use that may be made of the information it contains.