

### SharkFest '18 US



### Packet Monitoring in the IoT and Cloud Days

### Luca Deri <deri@ntop.org> @lucaderi



### About Me



 (1997) Founder of the <u>ntop.org</u> project with purpose of creating a simple, and open source web-based traffic monitoring application.
 Lecturer at the University of Pisa, Italy.



							10 -	Filter Hosts+	IP Ver
	IP Accress	Location	Flows	Alerts	Nome	Seen Since	Ereakdown	Throughput♥	Total I
Picers	192.103.2.20 🗯 🖨 💭	LocalPost	111	0	Lucas-Mac	01:21:14	Sent Rovd	1.15 Mb//s 🕈	790.7
Fires	72.947.178.76 🚍	Remarks Head	1		72.247.178.74	49:37	Sent 📴	1.09 Mb/9's 4	388.8
Fires	192.103.2.42	LocalPost	4		192.193.2.42 [1099752-01-DT1720002963]	01:20:55	Rovd	26.40 KDIV's 💠	105.00
Fires	192.108.2.46	Local Post	15	0	192.193.2.46	01:20:56	Sert 🔤	6.44 kb///s 💠	1.73
Fices	0.0.0	Broadcast	8		NoIP	01:20:14	Dent	604.57 bit/s +	26.64
Fires	255.255.255.255	Broadcast	3	•	Broadcast	01:21:10	Rox	634.57 bit/s 🛧	70.3
Picers	35.171.220.249 🗯	Rende Host	0	•	35.171.220.249	01:33	Sert Nex	0 bit/s	8.7
Trees	52.203.218.154 🛤	Renate Heat	1	•	52.203.219.154	00:04		0 bps	0.8
Fices	210.56.211.99 🗯	Rende Hoel	1	•	216.53.211.99	01:27	Sect	0 bit/s -	30.3
Fires	54.230.93.34 🛤	Rameta Heat	7	•	54.230.95.34	01:52	Sert Rost	0 bit/is =	34.0



- ntop contributed to wireshark in various components such as the NetFlow dissector, and high-speed packet filtering extcap modules (see Sharkfest Restrospective).
- Recently we have contributed with a Lua-based sFlow collector presented yesterday at sf18us.

#### 

11:15am - 12:30pm

21: sFlow: Theory & practice of a sampling technology and its analysis with Wireshark Instructor: Simone Mainardi



### Packet Traces



• This talk is a <u>tutorial</u> about networking focusing mostly on cloud and IoT.

• You can find packet traces of the various topics at: <u>http://luca.ntop.org/Sharkfest2018/</u>



# Part 1: (Tutorial on) Network and Traffic Trends

### Motivation



- Networks have changed significantly in the past decade due to many advances in computing:
  - Protocols (peer to peer).
  - CDN (Content Delivery Networks) and Cloud Computing.
  - User (from PC to smartphones).
- These have been <u>major</u> changes that had an impact on traffic and thus on our daily activities.

# Network Protocols [1/11]



- When the Internet was created each service had its own custom protocol designed to serve at best the needs of a specific application.
  - Email: SMTP, POP3, IMAP...
  - Name Resolution: DNS
  - Host Connectivity: telnet, SSH
  - Time: time, ntp...
  - VoIP: SIP, H.323...

### Network Protocols [2/11]

+OK Hello there. USER +OK Password required. PASS +OK logged in. STAT +0K 7 32932 LIST +OK POP3 clients that break here, they violate STD53. 1 5826 2 4602 3 7521 4 2587 5 4616 6 3335 7 4445 UIDL 1 +0K 1 UID146-1145365523 UIDL +0K 1 UID146-1145365523 2 UID147-1145365523 3 UID148-1145365523 4 UID149-1145365523 5 UID150-1145365523 6 UID151-1145365523 7 UID152-1145365523 RETR 6 +OK 3335 octets follow. Return-Path: <emailbusiness@email.it> Delivered-To: emailbusiness@email.it Received: from localhost (smtp-in06.email.it [127.0.0.1]) by smtp-in06.email.it (Postfix) with ESMTP id 2DB4944008; Thu, 26 Oct 2006 01:07:00 +0200 (CEST) X-Virus-Scanned: amavisd-new at email.it

Received: from smtp-in06.email.it ([127.0.0.1]) by localhost (smtp-in06.email.it [127.0.0.1]) (amavisd-new, port 10024) with LMTP id 32mPd3yTMBW; Thu, 26 Oct 2006 01:06:59 +0200 (CEST) Received: from localhost.localdomain (unknown [80.247.77.99]) by smtp-in06.email.it (Postfix) with ESMTP id 229DE4400C; Thu, 26 Oct 2006 01:06:59 +0200 (CEST) Date: Thu, 26 Oct 2006 01:07:15 +0200 From: emailbusinessgemail.it Subject: Ponti in Beauty Farm da 156 euro! Mine-Version: 1.0 Content-Type: multipart/alternative; boundary=ABCD Message\_Id: <20061025230659.229DE4400Cgsmtp-in06.email.it> To: undisclosed-recipients:;

....INVITE sip:0239777289@sip.messagenet.it SIP/2.0 Via: SIP/2.0/udp 81.116.18.30:5060:branch=z9hG4bK816A42BEFF629368D009F9814DD16 Route: <sip:sip.messagenet.it:5061:lr> From: <sip:5319921@sip.messagenet.it>;tag=C881DF084C6CE08915B3DC41EFFC3 To: <sip:0239777289@sip.messagenet.it> Call-ID: 2C2C591F0B4E77E8FD433C24A7D37@81.116.18.30 CSeq: 7 INVITE Contact: <sip:5319921@81.116.18.30;unig=6C8E2C86C13E942742D9C4DB95BDF> Max-Forwards: 70 Expires: 120 User-Agent: AVM FRITZ!Box Fon ata 1020 11.04.01 (Jan 25 2006) Supported: 100rel, replaces Allow-Events: telephone-event, refer Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, UPDATE, PRACK, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE Content-Type: application/sdp Accept: application/sdp. multipart/mixed Accept-Encoding: identity Content-Length: 380

#### v=0

POP3

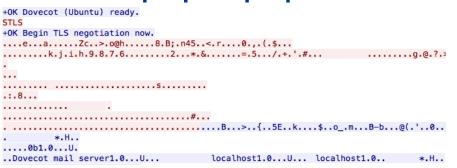
o=user 10296005 10296005 IN IP4 81.116.18.30 s=call c=IN IP4 81.116.18.30 t=1157359145 1157362745 m=audio 7078 RTP/AVP 8 0 2 102 100 99 97 18 101 a=sendrecv a=rtpmap:2 G726-32/8000 a=rtpmap:102 G726-32/8000 a=rtpmap:100 G726-40/8000 a=rtpmap:99 G726-24/8000 a=rtpmap:97 iLBC/8000 a=fmtp:97 mode=30 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-11 a=rtcp:7079 INVITE sip:0239777289@sip.messagenet.it SIP/2.0 Via: STP/2 0/udp 81 116 18 30:5060:branch=z9b64bK8160428EEE629368D009E9814DD16

SIP

# Network Protocols [3/11]



- All protocols were in clear text, and only later they have been replaced with an encrypted/ secure version. Two options:
  - Extend existing protocols: pop->pops
  - Encapsulation on a secure channel: telnet->SSH.



## Network Protocols [4/11]



- Binary protocols such as Radius/DHCP were not that popular.
- Instead it was <u>privileged portability</u> across systems and CPU types, instead of ad-hoc compression/ encoding.
- The ASN.1 (Abstract Syntax Notation 1) is still serving the needs of data serialisation and portability: SNMP and 3G/UMTS, 4G/LTE use it.

## Network Protocols [5/11]



- This model worked for a while until HTTP was created.
- HTTP stands for HyperText Transfer Protocol and it was initially designed for transferring hypertext (HTML, images....) but it has been transformed into a protocol used for mostly everything.
- One of reasons behind this success is that firewall/ proxy/etc allow it to flow through them: why look for trouble with a custom protocol if there is HTTP?

## Network Protocols [6/11]



• The jeopardisation is not over, in particular with the upcoming HTTP/2.0....

### DNS over HTTPS

From Wikipedia, the free encyclopedia

**DNS over HTTPS (DoH)** is an experimental protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol. The goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-themiddle attacks.<sup>[1]</sup> As of March 2018, Google and the Mozilla Foundation are testing versions of DNS over HTTPS.<sup>[2][3]</sup>

# Network Protocols [7/11]

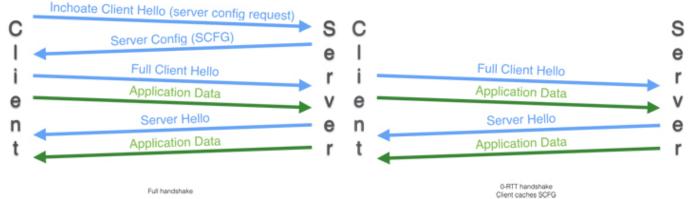


- The widespread "misuse" of HTTP has implications in traffic analysis as it makes it challenging to figure out what is the "real" protocol transported via HTTP(S), and what are the interactions between two peers.
- Today Netflix, Amazon Video, or your accounting software use HTTP(S) to transport video or data. It is the <u>new TCP/IP</u> in essence.

# Network Protocols [8/11]

#### With some exceptions... (FaceBook Zero)

- TCP over port 443 (SSL)
- QUIC Derivative
- Performance improvement over TLS1.2
- Used in iOS and Android Facebook Messenger apps (but not on the browser version)



https://code.facebook.com/posts/608854979307125/building-zero-protocol-for-fast-secure-mobile-connections/ https://code.facebook.com/posts/557147474482256/this-browser-tweak-saved-60-of-requests-to-facebook/

### Network Protocols [9/11]

## With some exceptions...

1	( 📕 🥂 🛞 🚞 🗋 🖄	रे 🖸 🔍 🔶 🏓 警	🔶 👱 💶 🗄	•	Q 🖳			
	fb_zero						Expres	sion +
No	Time	Source	Destination	Protocol	Length I	nFlight	Info	
T	66 17.895647	192.168.137.10	31.13.86.2	FB_ZER0	125	59	Client Hello	
Т	68 17.899655	31.13.86.2	192.168.137.10	FB_ZER0	1314	1248	Payload (Encrypte	d)
	69 17.899753	31.13.86.2	192.168.137.10	FB_ZER0	1314		Payload (Encrypte	
	70 17.899831	31.13.86.2	192.168.137.10	FB_ZER0	804		Payload (Encrypte	d)
	73 17.913282	192.168.137.10	31.13.86.2	FB_ZER0	329		Client Hello	
	74 17.914373	192.168.137.10	31.13.86.2	FB_ZER0	613		Payload (Encrypte	d)
	75 17.915921	31.13.86.2	192.168.137.10	FB_ZER0	204		Server NOM??	
	77 17.939730	192.168.137.10	31.13.86.2	FB_ZER0	112		Payload (Encrypte	
	79 17.954603	192.168.137.10	31.13.86.2	FB_ZER0	112		Payload (Encrypte	
	80 17.957644	192.168.137.10	31.13.86.2	FB_ZER0	286		Payload (Encrypte	
	82 18.020457	31.13.86.2	192.168.137.10	FB_ZER0	95		Payload (Encrypte	
-	Frame 66: 125 bytes on wire (1	000 bits), 125 bytes captu	red (1000 bits)	ED 7ED0	115	16	Pauload (Encrunte	d1)
	Ethernet II, Src: Apple e7:90:			8 (bc+85+56	c1.f7.08)			
	Internet Protocol Version 4, S			0 (00.05.50)				
	Transmission Control Protocol,			181. Ack: 1	74677318. Len:	59		
	(Facebook) Zero Protocol	51010101010100	acdi Erooraa	LOLY MENT IN		55		
	Public Flags: 0x31							
	Version: OTV							
	Unknown: 30							
	Length: 50							
	Tag: CHLO, Type: CHLO (Clier	nt Hello)						
	Tag Number: 2							
	Padding: 0000							
	Tag/value: SNI (Server Name)	Indication) (l=22): edge-r	gtt.facebook.com					
	Tag Type: SNI (Server Nam							
	Tag offset end: 22							
	[Tag length: 22]							
		74742e66616365626f6f6b2e63	6 <b>f6</b> d					
0	00 bc 85 56 c1 f7 08 9c fc	01 e7 90 87 08 00 45 00	· · V · · · · · · · · · · · E ·					
0		7b c7 c0 a8 89 0a 1f 0d	· o · · @ · @ · { · · · · · ·					
			V····· [··i]F··					
		08 0a 0f a0 b8 e1 7a 08	Oe Z					
		00 00 00 43 48 4c 4f 02 00 00 00 56 45 52 53 1a	10TV02 CHL0 SNI VERS					
		6d 71 74 74 2e 66 61 63	edge- mgtt.fac					
	70 65 62 6f 6f 6b 2e 63 6f		ebook.co mQTV1					
G	The fully qualified DNS name of the	server, canonicalised to lowercase with	no trailing period (fb zero.ta	o.sni). 22 bytes	Packets: 3854 · D	splayed: 268	(7.0%) Pr	ofile: Classic
_	The rany quantee bits halfe of the s	server, canonicanaca to lowercase with	the training period (ro_zero.te	grow), 22 bytes	Fucheta: 3004 - D	aprayed: 200	(A.V.A) PI	ormen endestic

iPhoneMessenger.pcap

Note: Wireshark 2.6+

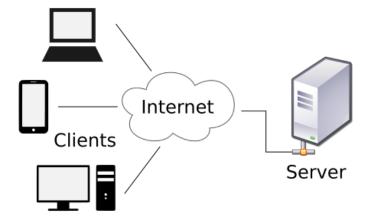
## Network Protocols [10/11]

- Internet protocols have been originally designed on two main paradigms:
  - Store and forward (e.g. email): information is not delivered directly but through an intermediate station.
  - Client-Server: the server usually operates as a centralised system that serves multiple clients. Communications can be direct or decentralised based on the peer-to-peer paradigm.

# Network Protocols [11/11]



Source: Wikipedia



- Direct communications.
- Easy to monitor (ip.src==xxx).



- Mix: direct and peer-communications depending on the IP address (NAT prevents some communications patterns).
- Difficult to track communications end-to-end (Wireshark filters help partially).
- More peers other than the client and server (many IPs make packet traces difficult to understand).
- Custom data encryption (no SSL)





- The advent of cloud computing and CDN (Content Delivery Network), contributed to create dynamic decentralised architectures whose topology, number of peers and their IP address can change overtime based on current usage needs.
- From a business perspective this has shifted the focus from hardware/software to services that are often rented based on the current needs.

### Cloud and CDN [2/19]



- From a traffic analysis perspective:
  - Cloud services often use application/network balancers: not simple to predict where your traffic will flow.
  - Nodes can serve multiple customers: filters on IP addresses won't necessarily restrict the traffic to the right target.
  - If you want to monitor <u>cloud components</u> traffic you are often forced to move monitoring tools to the cloud.
  - If you want to monitor <u>customer access</u> to cloud-based services, you need to sit at the customer premises in order to impersonate that real user experience.

### Cloud and CDN [3/19]



- Using cloud services also means that IP addresses are no longer relevant, in particular when leveraging on large providers such as Amazon or Google. The (cloud) server:
  - Based on your network/location/service load you access a different server pool.
  - Symbolic name might be the same but associated to different IP addresses, or names.
    - Corollary: IP address is not persistent.
    - Sub-Corollary: Wireshark filtering is more complex than "ip.addr==www.facebook.com"

### Cloud and CDN [4/19]

deri@ntop-digitaocean 204> host www.facebook.com www.facebook.com is an alias for star-mini.c10r.facebook.com. star-mini.c10r.facebook.com has address 31.13.64.35 star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f106:83:face:b00c:0:25de

defiginedp=uigitaocean 200> traceroute www.tacebook.com

traceroute to www.facebook.com (31.13.64.35), 30 hops max, 60 byte packets

128.199.32.254 (128.199.32.254) 1.216 ms 1.186 ms 1.183 ms

2 138.197.250.102 (138.197.250.102) 0.964 ms 138.197.250.98 (138.197.250.98) 0.971 ms 138.197.250.80 (138.197.250.80) 0.990 ms

ae37.pr02.ams2.tfbnw.net (157.240.67.244) 2.140 ms 0.903 ms ae37.pr01.ams2.tfbnw.net (157.240.67.242) 0.865 ms

po111.asw01.ams3.tfbnw.net (157.240.35.54) 1.050 ms po121.asw02.ams3.tfbnw.net (157.240.35.58) 1.039 ms po111.asw01.ams2.tfbnw.net (31.13.31.36) 1.275 ms

po241.psw02.ams2.tfbnw.net (157.240.35.181) 1.257 ms po212.psw01.ams2.tfbnw.net (157.240.32.13) 0.926 ms po231.psw01.ams2.tfbnw.net (157.240.35.163) 1.084 ms

6 173.252.67.1 (173.252.67.1) 1.180 ms 173.252.67.173 (173.252.67.173) 0.668 ms 173.252.67.3 (173.252.67.3) 1.085 ms edge-star-mini-shv-01-amt2.facebook.com (31.13.64.35) 0.879 ms 0.865 ms 0.847 ms

#### deri@ntop-digitaocean 206> ping6 www.facebook.com

PING www.facebook.com(edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de)) 56 data bytes 64 bytes from edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de): icmp seg=1 ttl=58 time=1.23 ms 64 bytes from edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de): icmp seg=2 ttl=58 time=0.939 ms 64 bytes from edge-star-mini6-shv-01-ams3.facebook.com (2a03:2880:f11b:83:face:b00c:0:25de): icmp seg=3 ttl=58 time=0.635 ms ^

--- www.facebook.com ping statistics ---

3 packets transmitted and received to packet lossy time 2003ms

rtt min/avg/max/mdev = 0.635/0.935/1.232/0.245 ms

deri@ntop-digitaocean 20/> ping -4 www.tacebook.com

PING star-mini.c10r.facebook.com (31.13.91.36) 56(84) bytes of data.

64 bytes from edge-star-mini-shv-01-ams3.facebook.com (31.13.91.36): icmp seg=1 ttl=58 time=1.03 ms

64 bytes from edge-star-mini-shv-01-ams3.facebook.com (31.13.91.36): icmp seg=2 ttl=58 time=0.668 ms ^

--- star-mini.c10r.facebook.com ping statistics ---

2 packets transmitted *and the packet descry* time 1001ms rtt min/avg/max/mdev 🚽 0.668/0.853/1.039/0.187 ms

### Cloud and CDN [5/19]

deri@Lucas-MacBookPro.local 201> host www.facebook.com www.facebook.com is an alias for star-mini.c10r.facebook.com. star-mini.c10r.facebook.com has address 31.13.86.36 star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f108:83:face:b00c::25de deri@Lucas-MacDookPro.tocal 202> ping 31.13.86.30 PING 31.13.86.36 (31.13.86.36): 56 data bytes 64 bytes from 31.13.86.36: icmp seq=0 ttl=51 time=78.956 ms 64 bytes from 31.13.86.36: icmp seg=1 ttl=51 time=66.536 ms <u>^</u> --- 31.13.86.36 ping statistics ---2 packets transmitted, 2 packets received 0.0% packet loss round-trip min/avg/max/stddev = 66.536/72.746/78.956/6.210 ms deri@Lucas-MacBookPro.local 203> traceroute www.facebook.com traceroute to star-mini.c10r.facebook.com (31.13.86.36), 64 hops max, 52 byte packets 172.20.10.1 (172.20.10.1) 1.209 ms 0.598 ms 0.455 ms 2 \* \* \* 3 10.133.16.37 (10.133.16.37) 68.925 ms 26.025 ms 33.354 ms 4 10.133.16.14 (10.133.16.14) 24.278 ms 23.648 ms 25.263 ms 5 10.133.16.236 (10.133.16.236) 24.370 ms 26.927 ms 24.421 ms <u>^C</u>

2/3

### Cloud and CDN [6/19]

deri@builder 201> host www.facebook.com www.facebook.com is an alias for star-mini.c10r.facebook.com. star-mini.c10r.facebook.com has address 31.13.86.36 star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f108:83:face:b00c:0:25de deri@builder 202> ping 31.13.86.36 PING 31.13.86.36 (31.13.86.36) 56(84) bytes of data. 64 bytes from 31.13.86.36: icmp\_seq=1 ttl=55 time=5.98 ms 64 bytes from 31.13.86.36: icmp\_seq=2 ttl=55 time=6.02 ms **^**C --- 31.13.86.36 ping statistics ---2 packets transmitted, 2 received, 0% packet loss, time 1001ms rtt min/avg/max/mdev  $\frac{4}{5}$  5.986/6.006/6.027/0.080 ms deri@builder 203> traceroute www.facebook.com traceroute to www.facebook.com (31.13.86.36), 30 hops max, 60 byte packets \* \* \* \* \* \* 3 \* \* \* \* \* \*

#sf18us • Computer History Museum, Mountain View, CA • June 25-28

3/3

### Cloud and CDN [7/19]



- In essence
  - Same symbolic <u>and</u> numeric IP (in this case Wireshark filtering will still work)
  - Different server(s) locations (traceroute)
  - Different latencies

    - ~ 60 msec

### Cloud and CDN [8/19]

1



Gerald Combs

Follow

 $\sim$ 

My **#Wireshark #Lua** skills were getting rusty so I wrote a postdissector that adds distance fields based on frame.time\_delta\_displayed.

#### gist.github.com/geraldcombs/d3...

No.		Time	Prev ∆	Cat 6 km	Length	Source
Г	1	0.000000	0.000000000	0	1454	200.121.1.13
	2	0.000011	0.000011000	2.14351	54	172.16.0.122
	3	0.025738	0.025727000	5013.29	1454	200.121.1.13
	4	0.025749	0.000011000	2.14351	54	172.16.0.122
	5	0.076967	0.051218000	9980.58	1454	200.121.1.13
	6	0.076978	0.000011000	2.14351	54	172.16.0.122
	7	0.102939	0.025961000	5058.89	1454	200.121.1.13
	8	0.102946	0.000007000	1.36405	54	172.16.0.122
	9	0.128285	0.025339000	4937.68	1454	200.121.1.13
1	.0	0.128319	0.000034000	6.6254	54	172.16.0.122
1	1	0.154162	0.025843000	5035.89	1454	200.121.1.13
1	2	0.154169	0.000007000	1.36405	54	172.16.0.122

6:44 PM - 11 Apr 2018

_	combs / delta_d		
<> Code	Revisions 1	🛧 Stars 2	Embe

Wireshark Lua postdissector that converts frame.time\_delta\_displayed to distance values.

#### 

#sf18us • Computer History Museum, Mountain View, CA • June 25-28

<scrip

### Cloud and CDN [9/19]



### Velocity factor

From Wikipedia, the free encyclopedia

The velocity factor (VF),<sup>[1]</sup> also called wave propagation speed or velocity of propagation (VoP or  $v_P$ ),<sup>[2]</sup> of a transmission medium is the ratio of the speed at which a wavefront (of an electromagnetic signal, a radio signal, a light pulse in an optical fibre or a change of the electrical voltage on a copper wire) passes through the medium, to the speed of light in a vacuum. For optical signals, the velocity factor is the reciprocal of the refractive index.

The speed of radio signals in a vacuum, for example, is the speed of light, and so the velocity factor of a radio wave in a vacuum is unity, or 100%. In electrical cables, the velocity factor mainly depends on the insulating material (see table below).

The use of the terms *velocity of propagation* and *wave propagation speed* to mean a ratio of speeds is confined to the computer networking and cable industries. In a general science and engineering context, these terms would be understood to mean a true speed or velocity in units of distance per time,<sup>[3]</sup> while *velocity factor* is used for the ratio.

#### Contents [hide]

- 1 Typical velocity factors
- 2 Calculating velocity factor
  - 2.1 Electric wave
  - 2.2 Optical wave
- 3 See also
- 4 References

### ~300k KM/s - ~190k Miles/s

https://en.wikipedia.org/wiki/Velocity\_factor

### Cloud and CDN [10/19]



	Minimum velocity factors for network cables			
VF (%)	Cable	Ethernet physical layer		
74–79	Cat-7 twisted pair			
77	RG-8/U	Minimum for 10BASE5 <sup>[4]</sup>		
67	Optical fiber	Minimum for 10BASE-FL, <sup>[5]</sup> 100BASE-FX,		
65	RG-58A/U	Minimum for 10BASE2 <sup>[6]</sup>		
65	Cat-6A twisted pair	10GBASE-T		
64	Cat-5e twisted pair	100BASE-TX, 1000BASE-T		
58.5	Cat-3 twisted pair	Minimum for 10BASE-T <sup>[7]</sup>		
-		·		

- Note: this is the pure network speed based on propagation. Add latency due to packet processing, queueing... to compute realistic distances. Typical RTT:
  - LAN: < 5 msec
  - Continent: < 25 msec
  - Across Atlantic: 100+ msec

### Cloud and CDN [11/19]



function formatValue(amount) local formatted = amount if(formatted == nil) then return(0) end while true do formatted, k = string.gsub(formatted, "^(-?%d+)(%d%d%d)", '%1,%2') if(k==0) then break end end return formatted end function distance(label, delta t) local c vacuum km s = 299792local c vacuum mi s = 186000 local fiber vf = .67 local dd\_fiber\_km local dd fiber mi delta t = delta t / 1000 -- msec -> sec dd fiber km = delta t \* c vacuum km s \* fiber vf dd fiber mi = delta t \* c vacuum mi s \* fiber vf print("\t"..label..": "..formatValue(dd\_fiber\_km).." Km / "..formatValue(dd\_fiber\_mi).." Miles ["..delta\_t.." sec]") end

```
print("Distance to www.facebook.com")
distance("Wind IT", 0.935)
distance("DigitalOcean", 1.232)
distance("Vodafone 3G", 78.956)
```

#### deri@Lucas-MacBookPro.local 235> lua distance.lua

Distance to www.facebook.com Wind IT: 187.8046984 Km / 116.5197 Miles [0.000935 sec] DigitalOcean: 247.46030848 Km / 153.53184 Miles [0.001232 sec] Vodafone 3G: 15,859.15269184 Km / 9,839.49672 Miles [0.078956 sec]

### Cloud and CDN [12/19]

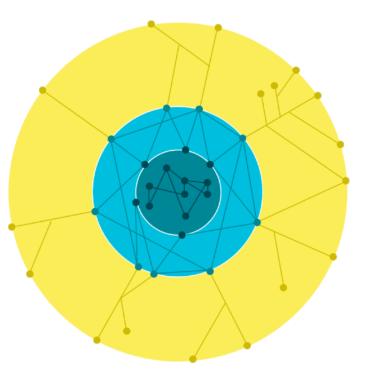


or and a second	B Hosts - Interfaces - Devices -	Search Host				
Flow: pc-deri:45614 == 164.132.198.64:143	Overview					
Flow Peers [ Client / Server ]	pc-deri I=:45614 [ 64:00:6A:63:35:CC ] 🚔 164.132.198.64:143 [ F4:B5:2F:FC:AF:F0 ]					
Protocol	TCP / IMAPS (51)					
First / Last Seen	15/05/2018 03:07:45 [21:20:02 ago]	16/05/2018 00:27:42 [00:05 ago]				
Total Traffic	Total: 3.55 MB -	Goodput: 2.49 MB (70.1 %) -				
	Client -> Server: 7,674 Pkts / 642.00 KB	Client 🗲 Server: 9,343 Pkts / 2.92 MB -				
	192.12.193.11:45614	164.132.198.64:143				
Round-Trip Time Breakdown	10.65 m	15 (server)				
Client/Server Estimated Distance	2,143 Km	1,329 Miles				
	21.296 ms	annar the second standard the second standard standard standard standard standard standard standard standard st				
Application Latency	21.200 116					
Application Latency Packet Inter-Arrival Time [ Min / Avg / Max ]	Client -> Server: < 1 ms / 00:10 / 00:32	Cilent <b>{</b> Server: < 1 ms / 00:08 / 00:32				
Packet Inter-Arrival Time		Client & Server: < 1 ms / 00:08 / 00:32				
Packet Inter-Arrival Time [ Min / Avg / Max ]						

https://github.com/ntop/ntopng

## Cloud and CDN [13/19]





Google aims to deliver its services with high performance, high reliability, and low latency for users, in a manner that respects open internet principles.

We have invested in network infrastructure that is aligned with this goal and that also allows us to work with network operators to exchange traffic efficiently and cost-effectively.

Google's network infrastructure has three distinct elements:

Core data centers

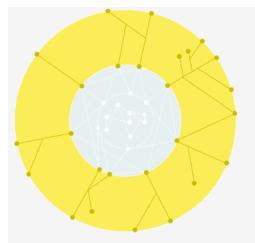
Edge Points of Presence (PoPs)

Edge caching and services nodes (Google Global Cache, or GGC)

#### Source: https://peering.google.com/

### Cloud and CDN [14/19]





#### Edge nodes (Google Global Cache, or GGC)

Our edge nodes (called Google Global Cache, or GGC) represent the tier of Google's infrastructure closest to our users. With our edge nodes, network operators and internet service providers deploy Google-supplied servers inside their network.

Static content that is very popular with the local host's user base, including YouTube and Google Play, is temporarily cached on edge nodes. Google's traffic management systems direct user requests to an edge node that will provide the best experience.

In some locations, we also use our edge nodes to support the delivery of other Google services, such as Google Search, by proxying traffic where it will deliver improved end-toend performance for the end user.



## Cloud and CDN [15/19]

- Anycast is a popular addressing and routing technology pioneered in DNS, that provides multiple route paths to two or more destinations.
- In essence the principle that (public) IP addresses are unique (i.e. each server must have a unique IP) is gone, as it is now possible to have IP address 1.2.3.4 multiple times on the Internet.

## Cloud and CDN [16/19]

10110 01101 1010 1010

- Through anycast it is now possible to
  - Announce the same IP network multiple times (reliability through replication).
  - Let routing protocols select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or least congested route.

## Cloud and CDN [17/19]

- CDNs heavily use anycast routing to bring (static) content close to their users.
- This on a reliable fashion as:
  - If the best node is unreachable (e.g. due to maintenance) another node can be used.
  - DDoS attacks will affect only regional servers as routing will protect "sub-optimal" routes

## Cloud and CDN [18/19]



- In summary cloud and CDNs make traffic analysis a bit more <u>challenging</u>.
  - The same numeric IP might be on different locations (one IP one host no longer holds).
  - Latency is crucial: providers place nodes as close as possible to users but this deceives consolidated technologies such as geo-location.
  - Packet-based analysis must be aware of all this, as service transparency and data caching might make troubleshooting more tricky.

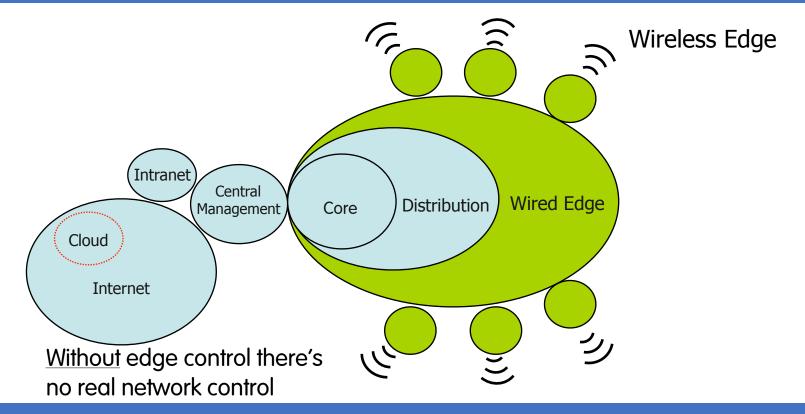


Packet analysis with CDNs and cloud-based services is not special but:

- You need to <u>be able to interpret the results</u> Wireshark will report you (including geolocation).
- During a troubleshooting session be ready to see the same service provided by different servers so adapt your filtering rules as necessary.

#### Networks Have Changed [1/2]







Traffic analysis implications:

- Packet capture location might be challenging with mobile users. If you analyse:
  - Internet traffic: being close to the gateway will be enough.
  - LAN traffic: the gateway will be too far away, in particular if you want to inspect traffic for security purposes. Being closed to the edge might help.

## A Middle Age Approach

- For years security was tackled with as a middle age problem:
  - Bad guys are outside of my network
  - Good guys are in
  - If I have an internal service to expose to the Internet I need to place it on a DMZ where the firewall can enforce selected traffic policies
- This approach was good until devices/users where easy to partition in groups but with the advent of BYOD (Bring Your Own Device), IoT and cloud computing things became more difficult.

## A Broken Security Model [1/3]

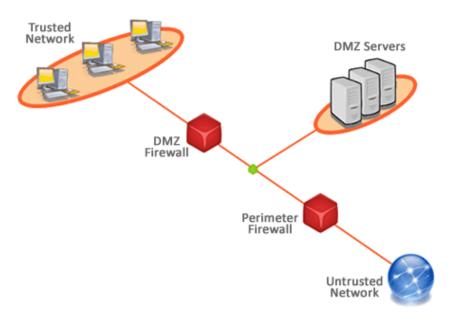


"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job." - Jerome Saltzer

• Procedural Security

• Logical Security

• Physical Security



Denning's Least Privilege Principle

#### A Broken Security Model [2/3]

- The Low-voltage Environment:
  - Wide-spread use of IoT devices.

- <u>Increasing interconnection</u> between edge devices and corporate networks: an edge device has <u>important topological privileges</u>.
- Edge devices <u>lack built-in security features</u>: too simple, yes easy to attack or replace with "trojan" devices.
- Physical location makes networks <u>vulnerable</u> <u>to external attack</u> – even without Internet connection

## A Broken Security Model [3/3]



- Unsecured low-voltage devices:
  - Access control
    - Unauthorised opening of gates/doors, false attendance information.
  - Video surveillance cameras
    - Manipulation of video camera streams, unauthorised viewing or disabling video edge-device elements.
  - Building-management/Fire-alarm systems
    - False readings, disabling or blinding.
  - Perimeter IP-based sensors
    - False readings, disabling or blinding.
  - DDoS (Distributed Denial of Service) attacks, can disrupt network operations and thus break a complex system/factory.



#### Part 2: Practical Traffic Analysis

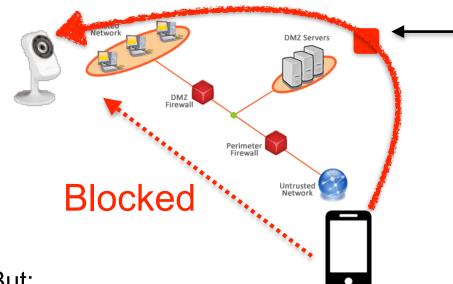
## Cloud-Managed Devices [1/6]



- The current trend in consumer device is the following:
  - Install the device in the designated network, usually behind a firewall or at least a NAT.
  - Configure the device from the designated network usually connecting to the device through a web browser and/or (optional) a mobile application connected to the WiFi network.
  - Access your device on-the-go using the mobile app.

## Cloud-Managed Devices [2/6]





This is where the camera was supposed to be ideally located:

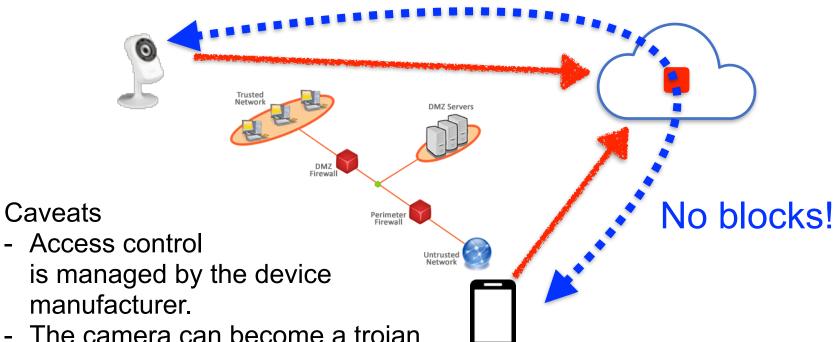
- Open a fixed TCP port
- Use it as a pivot to reach the Internal network

But:

- Most home networks have no DMZ nor static IP
- People do not like to configure anything, just unbox the camera and plug it to electricity

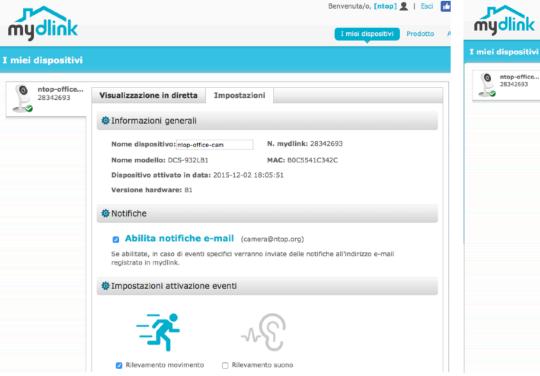
## Cloud-Managed Devices [3/6]

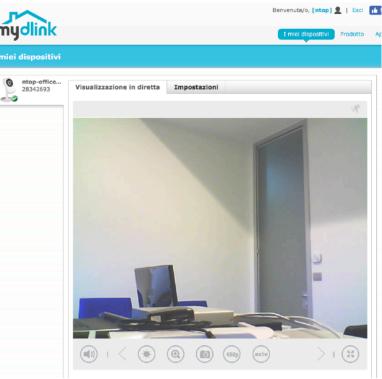




- The camera can become a trojan horse if not properly protected.

#### Cloud-Managed Devices [4/6]





#### Cloud-Managed Devices [5/6]



•	•							Wiresha	rk · Conversations	camera.pcap					
								Ethernet · 1	IPv4 · 2 IPv6	TCP · 4 UDP					
	Address A	A Port A		Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
	192.168.2.13	6	4927	54.194.162.25	443	12	2084	6	970	(	6 11	0.000000	25.1503	308	35
	192.168.2.13	6	3800	54.194.162.98	80	10	1023	6	687	4	4 33	0.059867	20.2254	271	13
	192.168.2.13	6	3720	54.194.162.98	2047	15	1098	9	672	(	6 4:	0.060684	0.9185	5852	37
	192.168.2.13	6	4501	54.194.162.98	2048	2,246	2070 k	1,516	1893 k	730	0 177	k 0.276662	53.6841	282 k	26
	Name resol	ution		Limit to display f	ilter	Absolute star	t time							Cor	oversation Types
	Help	ору 🔻	Fc	ollow Stream	Graph.										Clo

#### Camera view

- 1.Open a permanent connection camera <-> cloud and wait for commands sent from the cloud
- 2.Communications are encrypted, local sysadmins cannot pass/deny commands based on stream content

## Cloud-Managed Devices [6/6]



					Wiresh	iark · Cor	iversations - cam	era_client.p	capng						
					Ethernet	-1 IP	v4 · 9 IPv6	TCP · 15	UDP						
ddress A 🔺	Port A	Address B	Port B	Packets	Byte		Packets A → B	Bytes A		ckets B → A Bytes B		Rel Start	Duration	Bits/s A → B	Bits/s B → A
92.168.2.20		ec2-50-16-213-39.compute-1.amazonaws.com	htt		2	120		1	54	1	66	0.000000	0.1297	3330	4
92.168.2.20	61796	ec2-52-16-97-42.eu-west-1.compute.amazonaws.com	htt	ps	106	72 k		53	14 k	53	57 k	0.408464	21.9988	5198	
92.168.2.20	61797	ec2-52-16-97-42.eu-west-1.compute.amazonaws.com	htt	ps	161	135 k		68	7108	93	128 k	0.540518	12.4395	4571	
92.168.2.20	61798	ec2-52-16-97-42.eu-west-1.compute.amazonaws.com	htt	ps	15	3627		9	2087	6	1540	0.540764	2.4216	6894	5
92.168.2.20	61799	ec2-52-16-97-42.eu-west-1.compute.amazonaws.com	htt	ps	12	2110		7	1379	5	731	0.541196	1.0863	10 k	5
92.168.2.20	61520	151.101.14.2	htt	ps	2	120		1	54	1	66	0.632403	0.0364	11 k	
92.168.2.20	60501	162.125.18.133	htt	ps	4	1537		2	1148	2	389	3.137485	0.1385	66 k	
92.168.2.20	61802	ec2-52-204-250-205.compute-1.amazonaws.com	htt	ps	21	3299		13	2444	8	855	3.148964	10.6063	1843	
92.168.2.20	61807	ec2-54-194-162-61.eu-west-1.compute.amazonaws.com	ı ht	tp	11	1130		6	526	5	604	7.455747	0.1856	22 k	
92.168.2.20	61808	ec2-54-194-162-25.eu-west-1.compute.amazonaws.com	n ht	tp	11	1844		6	528	5	1316	7.628724	0.1833	23 k	
92.168.2.20	61833	ec2-54-229-64-81.eu-west-1.compute.amazonaws.com	ht	tp	11	1178		6	550	5	628	12.996878	0.1816	24 k	
92.168.2.20	61834	ec2-54-194-162-25.eu-west-1.compute.amazonaws.com	n ht	tp	11	1144		6	552	5	592	13.119850	0.1850	23 k	
92.168.2.20	61835	ec2-54-194-162-98.eu-west-1.compute.amazonaws.com	n (	dis	17	1234		10	742	7	492	13.245206	1.1721	5064	3
92.168.2.20	61836	ec2-54-229-64-81.eu-west-1.compute.amazonaws.com	ht	tp	11	1009		6	526	5	483	13.246308	0.1839	22 k	
92.168.2.20		ec2-54-194-162-98.eu-west-1.compute.amazonaws.com		or	1,429	966 k	(	87	105 k	742	860 k	13.999324	20.3467	41 k	3
Name resolutio	n 🗆	Limit to display filter 📃 Absolute start time					a de	<b>N</b> .						Con	versation Types
									Came	era video	stre	am			_

#### **Client view**

- 1. The communications camera <-> client do not use the same cloud host for displaying camera info or configuration
- 2.Camera <-> client talk with the same cloud host only for camera video stream

## IoT Devices in Cloud [1/10]



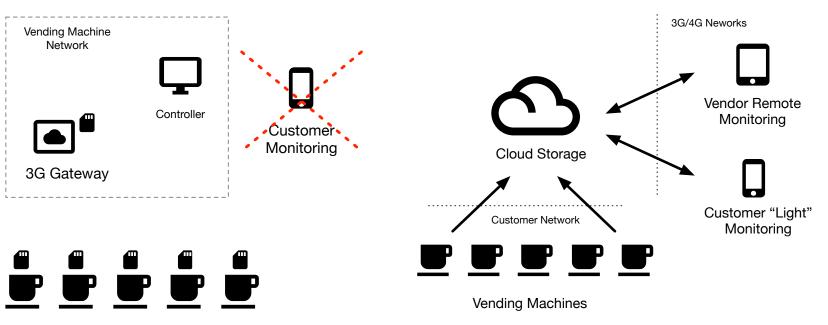
- "Modern" programmers use technologies such as the cloud, Web services, containers pretty extensively as they simplify application development.
- Platforms like <u>Thingspeak</u> for IoT analytics. Assumptions:
  - Devices are all Internet connected (if not a backup 3G connection will be installed).
  - Metrics storage is on the cloud, with no local persistency.
  - All devices interaction is not direct but through cloudbased services.

## IoT Devices in Cloud [2/10]



Today

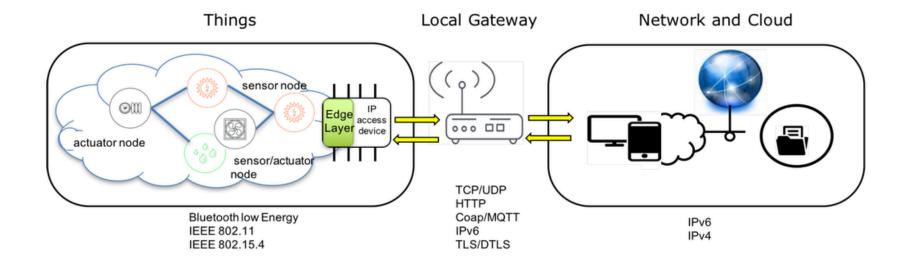
Before the Cloud



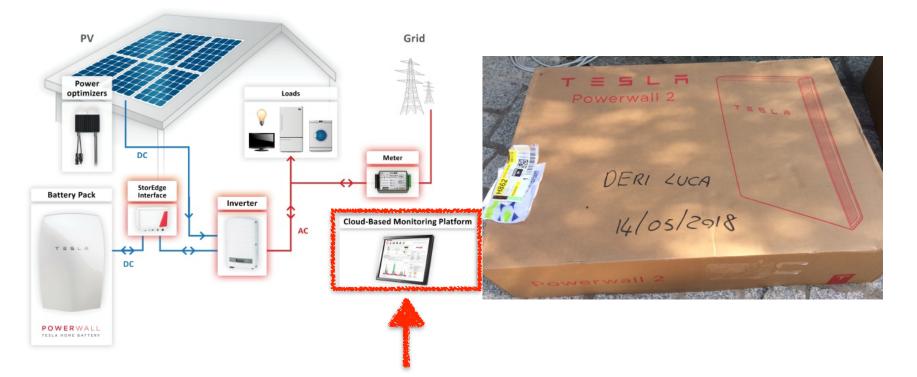
Vending Machines

## IoT Devices in Cloud [3/10]



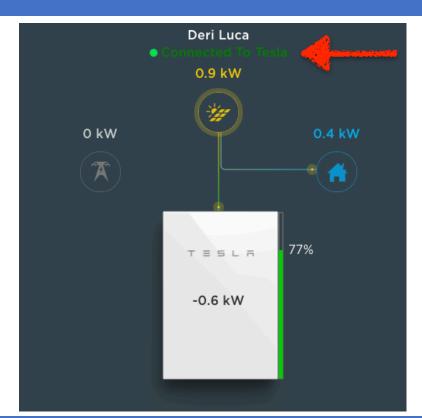


## IoT Devices in Cloud [4/10]



## IoT Devices in Cloud [5/10]





		1/11
Net	twork	
Conne	ect to the internet to ensure the system stays up to d	late.
• Eth	Beensiewy and sons in a start and in a st	
Not	connected	>
• Wi-	Fi	
Not	connected	>
• Cell	ular	
IP: 1	0.44.121.70	
CHECK		
	amener and the second	successive successive and
	E Cellular bypas	scas my han

< BACK

CONTINUE >

## IoT Devices in Cloud [6/10]



#!/bin/bash
watch 'curl -s http://192.168.2.36/api/meters/aggregates | jq
"{battery:.battery.instant\_power,solar:.solar.instant\_power,grid:.site.instant\_p
ower,house:.load.instant power}"'

Every 2.0s: curl -s http://192.168.2.36/api/meters/aggregates |... Sat Jun 9 11:22:56 2018

```
{
    "battery": -530,
    "solar": 845.3064575195312,
    "grid": -11.2249755859375,
    "house": 304.08148193359375
}
```

## IoT Devices in Cloud [7/10]



- Cellular connectivity does not allow a customer to analyse what is the device reporting to the cloud (local security devices are bypassed).
- Disabling cellular allows Wireshark to analyse the network traffic produced by the Powerwall.
- See tesla.pcap: capture of Powerwall traffic to the Internet

## IoT Devices in Cloud [8/10]

tesla.pcap 1 🙆 💼 🖹 🕅 🏹 🖓 🗭 🗯 🖉 🛃 🜉 0,0,0, 👎 Expression... Time Source Destination Protocol Length Info 41 111,010721 192,168,2,36 ns-389.awsdns-38.com 91 Standard query 0x7c2b AA. DNS 42 111.012840 192.168.2.36 ns-1121.awsdns-12.org DN5 91 Standard query 0x57d1 A ... 43 111.040420 ns-1121, avsdns-12, org 192, 168, 2, 36 DNS 272 Standard query response ... 44 111.041866 192.168.2.36 ns-309.awsdns-38.com DNS 95 Standard guery Øxbled A . 45 111.062580 ns-309.avsdns-38.com 192.168.2.36 DNS 272 Standard guery response ... 46 111.064052 192.168.2.36 ns-309.awsdns-38.com DNS 95 Standard guery 0x049d AA. DNS 47 111.094536 ns-309.awsdns-38.com 192.168.2.36 315 Standard query response ... 48 111,896648 192,168,2,36 ns-1475, awsdns-56, org DN5 129 Standard query exefeb A ... ns-309.awsdns-38.com 49 111, 116268 192.168.2.36 DNS 315 Standard query response ... 192,168,2,36 ns-332.awsdns-41.com DNS 129 Standard query 0x7273 AA. 50 111,117959 51 111.126146 ns-1475.awsdns-56.org 192.168.2.36 DNS 314 Standard query response ... ns-332.awsdns-41.com 192.168.2.36 52 111.170695 DNS 207 Standard query response ... 330 204.260463 192.168.2.36 ns4.p31.dynect.net DNS 86 Standard query 0x846b PT... 331 204.300726 ns4.p31.dynect.net 192,168,2,36 DNS 262 Standard query response ... 332 284, 387929 192.168.2.36 ns3.p31.dynect.net DNS 87 Standard guery 0xdef6 PT... 333 284, 368575 ns3.p31.dynect.net 192, 168, 2, 36 DNS 264 Standard guery response ... 825 431,709492 192.168.2.36 ns-309.awsdns-38.com DNS 89 Standard guery 0x85f8 AA. 826 431.710801 192.168.2.36 ns-1757.avsdns-27.co.uk DNS 89 Standard guery 0xe89c A ... 827 431.757798 ns-1757.awsdns-27.co.uk 192.168.2.36 DNS 301 Standard query response ... 828 431,758788 192.168.2.36 ns-1769.awsdns-29.co.uk DN5 121 Standard query ByBbcc A ▶ Frame 41: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) Ethernet II, Src: Winsyste\_07:d5:ac (00:01:45:07:d5:ac), Dst: AvnAudio\_75:4e:6a (5c:49:79:75:4e:6a) Internet Protocol Version 4, Src: 192.168.2.36 (192.168.2.36), Dst: ns-309.avsdns-38.con (205.251.193.53) ▶ User Datagram Protocol, Src Port: 53413 (53413), Dst Port: domain (53) y Donain Name System (query) Transaction ID: 0x7c2b Flags: 0x0000 Standard query 0... .... = Response: Message is a query .000 0... .... - Opcode: Standard query (0) ..... ..0. .... = Truncated: Message is not truncated .... ...8 .... = Recursion desired: Don't do query recursively ..... .0.. .... = Z: reserved (0) .... ....0 .... = Non-authenticated data: Unacceptable Questions: 1 Answer BRs: 0 Authority BBs: 0 Additional BBs: 0 ▶ Oueries (Response In: 45) 5c 49 79 75 4c 6a 00 21 45 07 d5 ac 28 00 45 00 VIVONI-- E----2010 00 4d 8b a3 40 00 40 11 5c ff c8 a8 02 24 cd fb M-0.0. \----5-2020 c1 35 d0 a5 00 35 00 39 2d 6c 7c 2b 20 00 20 01 -5---5-9 -11+---2030 CO 02 CO 02 CO 02 CO 73 79 6c 65 72 67 79 22 73 ·····s ynergy s 8848 6c 0b 74 65 73 6c 61 65 6c 65 72 67 79 08 73 65 n-teslae nergy-se 72 76 69 63 65 73 00 20 lc 00 01 rvices..... O Z Do query requisively? (dos flags recidesired), 2 bytes. Packets: 1905 - Displayed: NS (3,053) Reafile: Default

#### DNS

#### See tesla.pcap

#### IoT Devices in Cloud [9/10]

deri@ntop-digitalocean 201> dig +norecurse synergy.sn.teslaenergy.services

- ; <<>> DiG 9.11.3-1ubuntu1-Ubuntu <<>> +norecurse synergy.sn.teslaenergy.services
- ;; global options: +cmd
- ;; Got answer:
- ;; ->>HEADER<<- opcode: QUERY, status: **REFUSED**, id: 58690
- ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;synergy.sn.teslaenergy.services. IN A
```

;; Query time: 0 msec ;; SERVER: 127.0.0.53#53(127.0.0.53) ;; WHEN: Sat Jun 09 11:49:35 CEST 2018 ;; MSG SIZE rcvd: 60

# IoT Devices in Cloud [10/10]

deri@ntop-digitalocean 202> dig +norecurse @205.251.193.53 synergy.sn.teslaenergy.services

; <<>> DiG 9.11.3-1ubuntu1-Ubuntu <<>> +norecurse @205.251.193.53 synergy.sn.teslaenergy.services : (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39134 :: flags: gr aa: OUERY: 1. ANSWER: 1. AUTHORITY: 4. ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;synergy.sn.teslaenergy.services. IN A ;; ANSWER SECTION: synergy.sn.teslaenergy.services. 60 IN CNAME hermes-stream-prd.sn.tesla.services. ;; AUTHORITY SECTION: sn.teslaenergy.services. 172800 IN NS ns-1121.awsdns-12.org. sn.teslaenergy.services. 172800 IN NS ns-1757.awsdns-27.co.uk. sn.teslaenergy.services. 172800 IN NS ns-309.awsdns-38.com. sn.teslaenergy.services. 172800 IN NS ns-914.awsdns-50.net. ;; Query time: 1 msec ;; SERVER: 205.251.193.53#53(205.251.193.53) ;; WHEN: Sat Jun 09 11:52:39 CEST 2018 ;; MSG SIZE rcvd: 241

# Home IoT Devices [1/11]



## Home IoT Devices [2/11]





### Home IoT Devices [3/11]

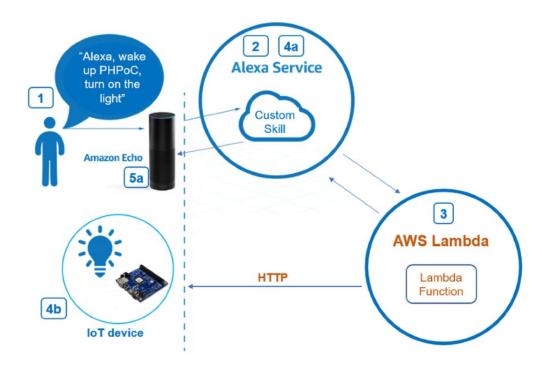
	0		0
0	L,	0	
	0		0
		2	I.

Alexa Skills	5 ¥	Q Deals for Father's Day
Deliver to Departm	nents - Your Amazon.com Today's Deals Gift Cards Registr	try ⊕ - Account & Lists - Orders Try Prime - VCa
Alexa Skills For Your Smart Home G	Sames and Trivia Lifestyle Your Skills Getting Started Help	
Alexa Skills > Smart Home	Atmo by fourteenislands.io Rated: Guidance Suggested ★★★☆☆ 12 Free to Enable *Alexa, ask atmo what's the *Alexa, ask atmo to give m	Get this Skill         Sign In         By enabling, this skill can be accessed on all your available Alexa devices.
Description Atmo helps you retrieve measuremer for the sensors (also known as modul Available measurements: - carbon dioxide level - humidity - noise level - oressure		personal weather station. Atmo can leverage on the names you have specified

A Netatmo account is required and the account linking process must be completed in order to retrieve measurements.

# Home IoT Devices [3/11]





#### Home IoT Devices [4/11]

	RealtekS_69:8e:eb			Packets A → B	Bytes $A \rightarrow B$	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s $A \rightarrow B$	Bits/s $B \rightarrow A$
limDevi_f8:f7:cf		1,075	190 k	541	66 k	534	124 k	6.780849	1558.5546	339	
	Broadcast	8	480	8	480	0	0	114.274522	1321.1559	2	
limDevi_f8:f7:cf	IPv4mcast_7f:ff:fa	4	652	4	652	0	0	232.155622	0.6043	8630	
&MHoldi_5a:85:23	Broadcast	1	60	1	60	0	0	591.577673	0.0000	_	
onos_68:54:44	Broadcast	1	60	1	60	0	0	543.903936	0.0000	_	
onos_83:7a:44	Broadcast	1	60	1	60	0	0	599.861517	0.0000	_	
onos000E58C683A4.local	RealtekS_69:8e:eb	1,159	758 k	608	64 k	551	694 k	13.198110	1560.6807	328	3
onos000E58C683A4.local	IPv4mcast_7f:ff:fa	30	17 k	30	17 k	0	0	423.559342	1131.0916	124	
onos000E58C683A4.local	Broadcast	13	6536	13	6536	0	0	423.560607	1131.0916	46	
onos000E58C683A4.local	IPv4mcast_fb	4	1688	4	1688	0	0	655.555058	734.7355	18	
ynology_37:dc:df	Broadcast	1	60	1	60	0	0	725.302726	0.0000	_	
ealtekS_69:8e:eb	Android.local	5,887	2072 k	2,877	686 k	3,010	1385 k	0.000000	1552.0649	3537	7
ealtekS_69:8e:eb	Azurewav_65:36:67	532	65 k	268	25 k	264	40 k	0.912947	1566.2723	128	
ealtekS_69:8e:eb	Broadcast	1	60	1	60	0	0	6.806581	0.0000	_	
ealtekS_69:8e:eb	Netatmo_00:fe:24	85	11 k	50	7009	35	4383	290.137804	1220.5116	45	
Pv4mcast_16	Android.local	4	224	0	0	4	224	590.060264	0.7599	0	2
Pv4mcast_fb	Android.local	65	10 k	0	0	65	10 k	232.591680	1062.1002	0	
zurewav_65:36:67	Broadcast	9	540	9	540	0	0	581.680506	3.8684	1116	
ndroid.local	Broadcast	1	60	1	60	0	0	590.403074	0.0000	_	
ndroid.local	4e:af:23:b3:2d:7e	2	158	1	60	1	98	681.292528	0.0001	_	
e:af:23:b3:2d:7e	Broadcast	2	84	2	84	0	0	680.034648	1.0011	671	
lphaNet_fc:f9:f2	Broadcast	1	60	1	60	0	0	583.696996	0.0000	_	
letatmo_00:fe:24	Broadcast	16	960	16	960	0	0	292.758838	1215.8748	6	
pple_a5:0c:93	Broadcast	64	3840	64	3840	0	0	5.011088	1543.8964	19	

#### Home IoT Devices [5/11]

Source Mac Addresses

Manufacturer-

Mac Address	Manufacturer A	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
5C:33:8E:FC:F9:F2	Alpha Networks Inc.	Computer 🖵	5C:33:8E:FC:F9:F2	0	1	70 days, 01:17:08	Sent	0 bit/s	60 Bytes
40:B4:CD:2B:4C:9E	Amazon Technologies Inc.	Multimedia 🞜	amazon-bd974b201	1	81	70 days, 01:26:52	Sent Rcvd	0 bit/s	1.99 MB
98:01:A7:A5:0C:93	Apple, Inc.	Multimedia 🞜	98:01:A7:A5:0C:93	0	64	70 days, 01:26:47	Sent	0 bit/s	3.75 KB
40:9F:38:65:36:67 4	AzureWave Technology Inc.	IoT 🖟	Roomba	1	93	70 days, 01:26:51	Sent Rcvd	0 bit/s	64.49 KB
00:05:CD:5A:85:23	D&M Holdings Inc.	Unknown	00:05:CD:5A:85:23	0	1	70 days, 01:17:00	Sent	0 bit/s	60 Bytes
70:EE:50:00:FE:24 4	Netatmo	IoT 🖟	Netatmo-Personal-Weather-Station	1	23	70 days, 01:22:02	Sent Rcvd	0 bit/s	12.06 KB
00:E0:4C:69:8E:EB	Realtek Semiconductor Corp.	Router/Switch	00:E0:4C:69:8E:EB	36	312	70 days, 01:26:52	Sent Rcvd	0 bit/s	2.95 MB
00:04:20:F8:F7:CF 🟠 🗲 💩	Slim Devices, Inc.	IoT 🕼	HarmonyHub	1	103	70 days, 01:26:45	Sent Rcvd	0 bit/s	187.25 KB
00:0E:58:68:54:44	Sonos, Inc.	Multimedia 🞜	SonosZB	0	1	70 days, 01:17:48	Sent	0 bit/s	60 Bytes
00:0E:58:83:7A:44	Sonos, Inc.	Multimedia 🞜	00:0E:58:83:7A:44	0	1	70 days, 01:16:52	Sent	0 bit/s	60 Bytes
00:0E:58:C6:83:A4 🟠 🐓	Sonos, Inc.	Multimedia 🞜	SonosZP	1	48	70 days, 01:26:39	S Rovd	0 bit/s	765.94 KB
00:11:32:37:DC:DF	Synology Incorporated	NAS	00:11:32:37:DC:DF	0	1	70 days, 01:14:46	Sent	0 bit/s	60 Bytes
4E:AF:23:B3:2D:7E	n/a	Computer 🖵	rock64	1	3	70 days, 01:15:32	Sent Rcv	0 bit/s	242 Bytes

#### #sf18us • Computer History Museum, Mountain View, CA • June 25-28

Filter Macs T - Device Type-

20 -

## IoT Devices in Cloud [6/11]

- smart\_home.pcap interactions include:
  - Alexa (.172) turns on music on Sonos (.122)
    - Alexa checks the temperature
      - Alexa starts turns on the robot cleaner



#### No direct communication between devices

### IoT Devices in Cloud [7/11]

sonos ----



#### Select traffic with "(ip.addr==192.168.177.122 or ip.addr==192.168.179.172) and ssl" or see alexa\_sonos\_only.pcap

• •		Wireshark ·	Conversatio	ns · alex	xa_sonos_onl	y.pcap						
		Ethernet · 2	IPv4 · 11	IPv6	TCP · 13	UDP						
Address A	Address B	Packets	Bytes	Pac	kets A → B	Byte	es A → B	Packets B → A	Bytes B → A	Rel Start	Duration	
ec2-34-243-113-114.eu-west-1.compute.amazonaws.c	om 192.168.177.122	1	89 5	0 k		61	19 k	12	8 31 k	13.198110	1560.6789	,
ec2-35-171-252-96.compute-1.amazonaws.com	192.168.179.172		27 90	94		14	5886	1	3 3208	591.594802	910.3486	1
52.46.128.105	192.168.179.172		14 1	5 k		6	4049		8 11 k	906.174398	6.4771	
52.46.132.96	192.168.179.172		14 2	3 k		6	4049		8 19 k	1206.276985	6.5832	
52.94.219.213	192.168.179.172	2,7	44 165	Bk	:	381	390 k	2,36	3 1268 k	0.000000	1548.7505	6
52.94.228.52	192.168.179.172		13 1	5 k		5	3995		8 12 k	606.147843	299.8981	
52.94.228.85	192.168.179.172		3 7	36		1	146		2 590	376.599880	1.2223	
52.94.232.230	192.168.179.172		11 83	57		6	4611		5 3746	590.732688	0.9168	
ec2-54-83-96-78.compute-1.amazonaws.com	192.168.179.172		15 14	73		6	582		9 891	26.550450	460.1042	
54.239.27.116	192.168.179.172		7 68	29		3	3898		4 2931	591.127147	0.6163	
192.168.177.122	mil04s26-in-f106.1e100.n	et	20 98	62		13	4532		7 5330	824.538056	1.6344	l i
										-		
Name resolution     Limit to display filter     Help     Copy     Follow Stream     Grap	Absolute start time									Conver	sation Types	

### IoT Devices in Cloud [8/11]



### IoT Devices in Cloud [9/11]





## IoT Devices in Cloud [10/11]



- Alexa/Sonos do not talk directly but only through the cloud even though they are sitting on the same network.
- Cloud-based interactions are encrypted. The only options are: pass or drop with no restrictions on actions performed by the devices.
- As cloud communications are started from the local network (inside NAT), the cloud can <u>remotely</u> instruct <u>local</u> devices to do everything.

## IoT Devices in Cloud [11/11]

#### 2.5 Privacy Requirements

The skill must not:

- 1. Contain references to or include malicious hacking, such as phishing or Trojans. This includes rooting a device or circumventing Amazon's or any developer's digital rights management (DRM) software.
- 2. Contain references to or include malicious user spying or tracking, including stalking, in the skill or skill metadata.
- 3. Misuse customer personally identifiable information or sensitive personal information.
- 4. Collect personal information from end users without doing *all* of the following: (i) provide notice of that data collection to end users in your skill's detail page,
  (ii) use the information in a way that end users have consented to, and

(iii) ensure that your collection and use of that information complies with your privacy notice and all

applicable laws.

Prior to submitting a skill that collects personal information from end users, you are required to supply a privacy policy that will be displayed to end users on your skill's detail page in the Alexa App.

https://developer.amazon.com/docs/custom-skills/security-testing-for-an-alexa-skill.html



#### Final Remarks



- As shown with Tesla, there are some (limited) checks to make sure the device is running on a "free" network.
- HTTP public certificate pinning can definitively help to detect intruders but device owner still need to trust the device manufacturer (<u>https://en.wikipedia.org/wiki/</u> <u>HTTP\_Public\_Key\_Pinning</u>).
- SSL implements privacy/security (good) but on the other hand limits inspection (bad).
- Alternative connectivity (e.g. cellular network with Tesla) can further complicate all this.