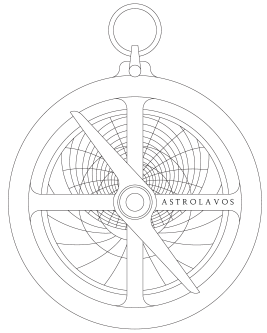
Where the insecure “things” are?

ELECTRICAL [+] COMPUTER

ENGINEERING



NIST ISPAB, 10/27/2016

Georgia Tech School of Electrical and Computer Engineering

About

- Manos Antonakakis, PhD.
  - Assistant Professor, ECE, Georgia Tech
  - Co-Chair of the Academic Committee at MAAWG
  - Co-founder of Netrisk (netrisk.io)

- Bio
  - PhD from Georgia Institute of Technology, CoC
  - Engineering Diploma from University of Aegean, GR
  - Past work experience;
    - Chief Scientist at Damballa (2010-2013)
    - Researcher at IBM/ISS (2008)
    - Researcher at the National Institute of Standards and Technology (NIST) (2004-2006)

Full disclosure

- Whatever you see next is joint work with the following researchers:
  - Chaz Level, GT
  - Dr. Yacin Nadji, GT
  - Dr. Fabian Monrose, UNC
  - David Dagon, GT

- This work would not be possible without our sponsors:
  - NIST (David Ferraiolo and Tim Grance)
  - DARPA (Angelos Keromytis)
  - Comcast (Michael O'Reirdan)

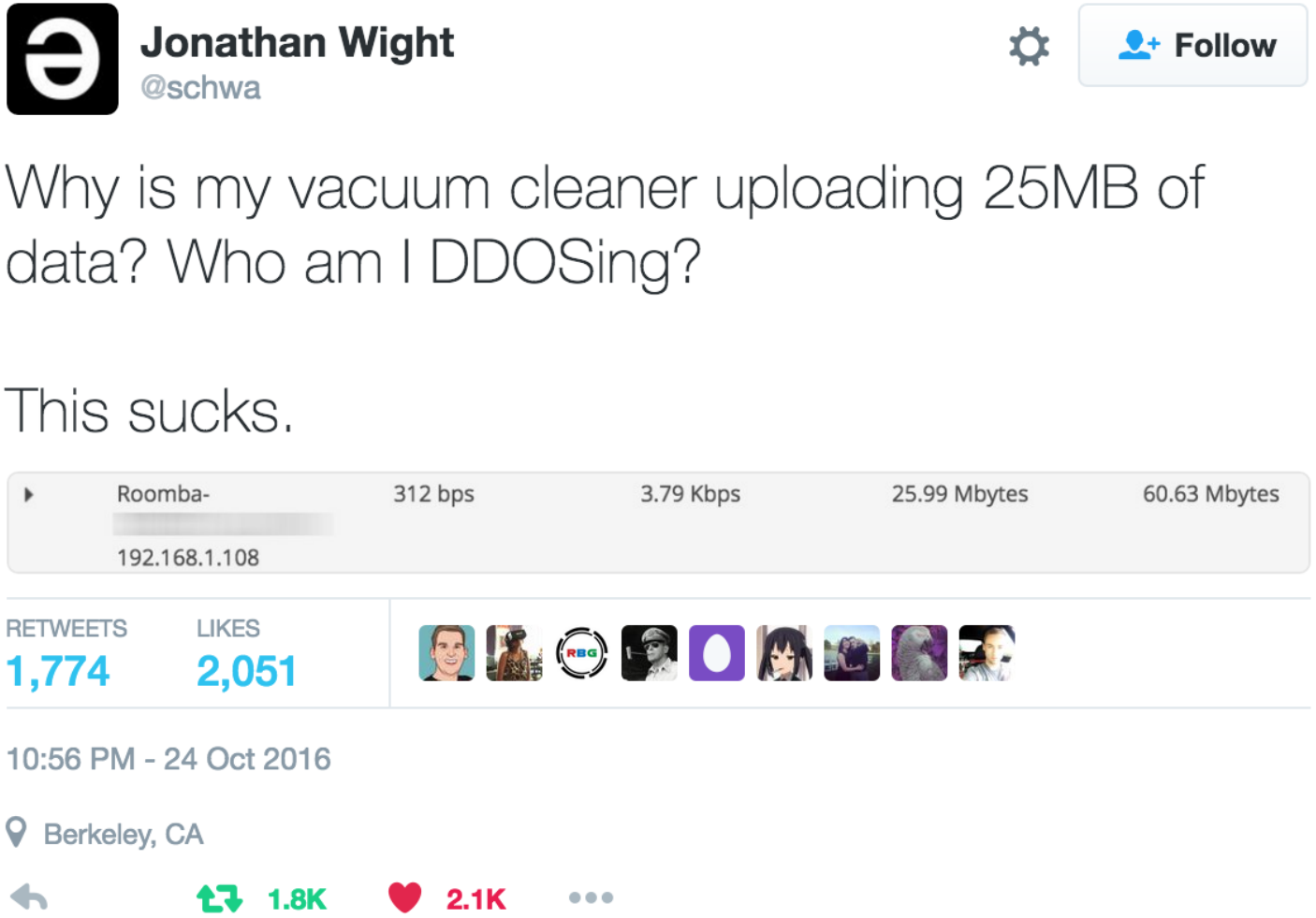
What we consider as IoT in our measurements?

IoT Definition

- Numerous definitions have been proposed by government, industry and academia.
- For our measurements **we do** consider as IoT;
  - Consumer devices (i.e., light bulbs, door locks, cameras, thermostat, etc.), and
  - Home automation devices (HVAC system controllers, building access controls, automated blinds, etc.)

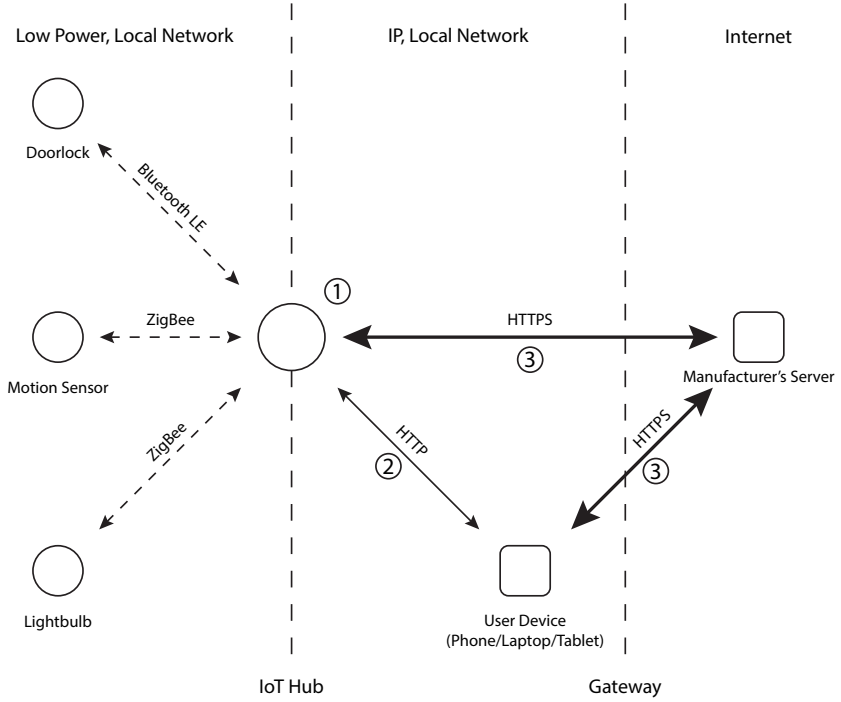
  that use the network to reach out to the rest of the Internet.
- For this presentation **we do not** consider as IoT devices laptops, mobile devices and industrial control sensors.

What is the problem with IoT?



What is the problem with IoT?

- They are “trusted” devices in our networks.
  - Increases the attack profile of our networks.
- They have less than good understanding of how network protocols and crypto should be used.
  - Opens holes to both end user’s security and privacy.

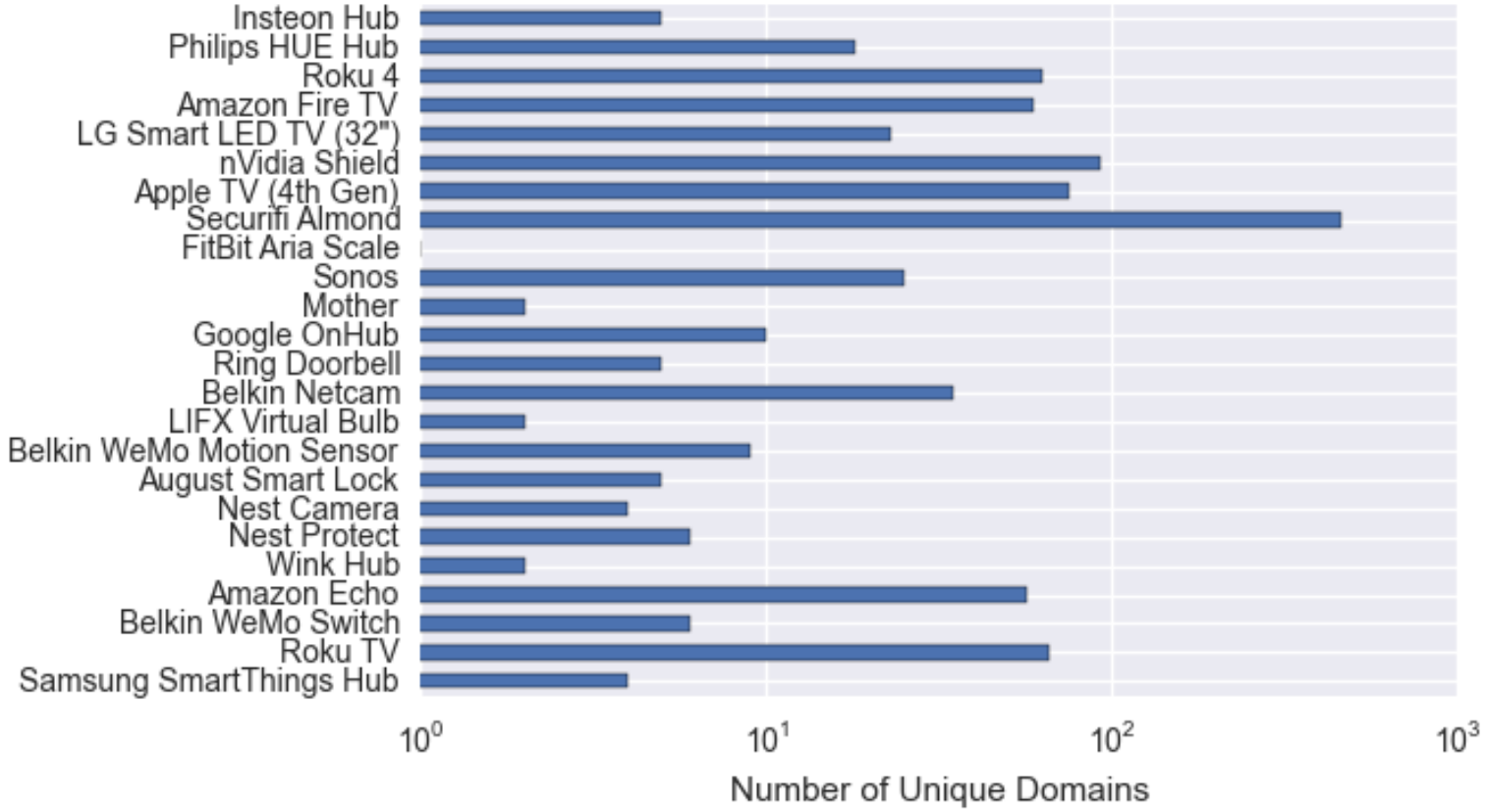


- Really hard to track the growth of these IoT devices.
  - Very important to measure.
  - Helps the community to anticipate events.

How to measure the IoT growth?

- We need an IoT lab!
  - Set up the network in a way where networking events can be clearly attributed to devices.
  - Run the devices for a long period of time. This is critical for measuring their behavior in real networks.
  - Collect IoT network indicators that can uniquely attributed to certain classes of IoT devices.
- We are ready for passive measurements!

IoT Network Indicators



- IoT devices are extremely “chatty”.
- They tend to connect to tenths of different locations in the Internet.

What kind of protocols they use?

- Using the devices in the IoT lab we can see the by-volume communication patterns from the IoT devices.
  - Surprisingly, they speak more UDP (DNS) than TCP.
  - Large numbers of ICMP and IGMP traffic too.
  - Many custom protocols on top of UDP.

What is the attack surface for IoTs?

			Encryption (TLS/SSL)		
Device	**Category**	**MITM**	**Device-to-Cloud**	**App-to-Device**	**App-to-Cloud**
Google OnHub	Hub	No	✓✓	--	✓✓
Mother	Sensors				
Samsung SmartThings Hub	Hub	No	✓✓	--	✓✓
Philips HUE Hub	Hub	Unclear	✓✗	--	✓✗
Insteon Hub	Hub		TBD	TBD	TBD
Sonos	Speaker	Local	--	✗✗	--
Securifi Almond	Hub	Local	--	✗✗	TBD
FitBit Aria Scale	Scale		TBD	TBD	TBD
Nest Camera	Security Camera				
August Smart Lock	Door Lock	No	✓✓	--	TBD
Belkin WeMo Motion Sensor	Sensors	NA	--	--	--
LIFX Virtual Bulb	Light Bulb	Unclear	--	--	??
Belkin WeMo Switch	Power Switch	App	✓✓	--	✓✗
Amazon Echo	Voice Control	None	✓✓	--	✓✓
Wink Hub	Hub		TBD	TBD	TBD
Nest Protect	Smoke Alarm		TBD	TBD	TBD
Belkin Netcam	Security Camera	Unclear	✗✗	--	✓✓
Ring Doorbell	Doorbell	Cloud	✗✗	--	✓✓
LG Smart LED TV (32")	Smart TV	Unclear	--	??	--
Roku TV	Smart TV	Partial on Cloud	✓✗	??	✓✓
Roku 4	Media Hub	Partial on Cloud	✓✗	??	✓✓
Amazon Fire TV	Media Hub	Partial on Cloud	✓✗	??	✓✓
nVidia Shield	Media Hub	No	✓✓	--	--
Apple TV (4th Gen)	Media Hub	Partial on Cloud	✓✗	--	--
Belkin WeMo Link	Hub	No	--	--	--
Negear Arlo Camera	Security Camera	No	✓✓	--	✓✓
D-Link DCS-5009L Camera	Security Camera	App	--	✗✗	--
Logitech Logi Circle	Security Camera	No	✓✓	--	✓✓
Canary	Security Camera	No	✓✓	--	✓✓
Piper NV	Security Camera	Cloud	✗✗	--	✓✓
Withings Home	Security Camera	Unclear	✓✗	--	✓✓

✓✓	Full Encryption
✓✗	Partial Encryption
✗✗	No Encryption
--	No communication

IoT HTTP and HTTPS? (I)

	SmartThings Hub			Nest Camera	August Lock	LG Smart TV	Roku TV						
	dc-na02-useast1.connect.smartthings.com	dc.connect.smartthings.com	fw-update.smartthings.com	files.dropcam.com	connect-ota.august.com	us.info.lgsmartad.com	api.roku.com	api.rokutime.com	liberty.ib.roku.com	liberty.logs.roku.com	liberty.sb.roku.com	liberty.sw.roku.com	ntp.rokutime.com
Grade	T(C)	T(C)	T(B)	T(C)	T(A-)	T(B)	T(B)	T(B)	T(A)	T(B)	T(A)	T(A)	T(B)
Weak Ciphers	yes	yes	no	no	no	yes	yes	no	no	no	no	no	no
TLSv1	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2
SSLv2	no	no	no	no	no	no	no	no	no	no	no	no	no
SSLv3	yes	yes	no	yes	no	no	no	no	no	no	no	no	no
Domain Mismatch	yes	yes	yes	no	yes	yes	no	no	no	no	no	no	no
Certificate Chain Issues	yes	yes	no	yes	no	no	yes	yes	yes	yes	yes	yes	yes
Uses HPKP				no	no	no	no	no	no	no	no	no	no
Uses HSTS				no	no	no	no	no	no	no	no	no	no
Forward Secrecy	yes	yes	yes	yes	yes	yes	no	yes	yes	yes	yes	yes	yes
BEAST	no	no	no	yes	no	no	no	no	no	no	no	no	no
CRIME	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
FREAK	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Heartbleed	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Lucky 13	no	no	no	yes	no	no	no	no	no	no	no	no	no
POODLE	no	no	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes
RC4 Bias	no	no	yes	yes	yes	no	no	yes	yes	yes	yes	yes	yes
Logjam	yes	yes	yes	no	yes	yes	no	yes	yes	yes	yes	yes	yes
DROWN	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

IoT HTTP and HTTPS? (II)

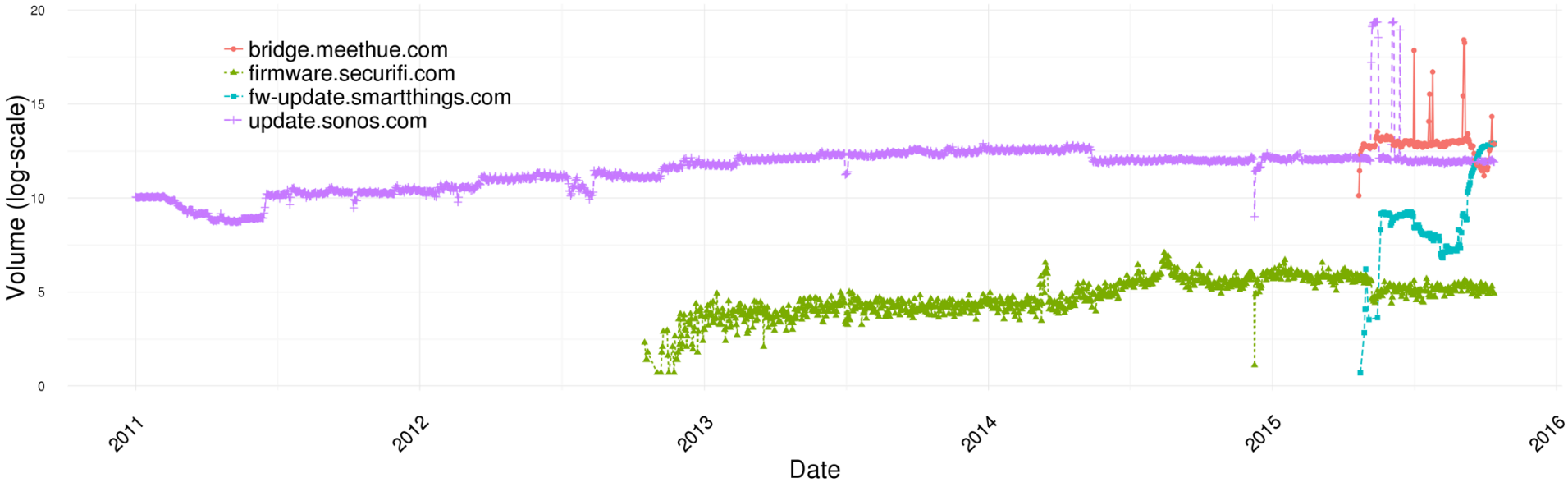
	Sonos								
	service-catalog.ws.sonos.com	static.sonos.com	system-api-tracking.sonos.com.out	system-api.sonos.com	**update-firmware.sonos.com**	update-services.sonos.com	update-timezone.sonos.com	**update.sonos.com**	www.sonos.com
Grade	C	F	F	F	F	F	F	F	F
Weak Ciphers	yes	yes	yes	yes	yes	yes	yes	yes	yes
TLSv1	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2	0/1/2
SSLv2	no	no	no	no	no	no	no	no	no
SSLv3	yes	no	no	no	no	no	no	no	no
Domain Mismatch	no	no	no	no	no	no	no	no	no
Certificate Chain Issues	no	no	no	no	no	no	no	no	no
Uses HPKP	no	no	no	no	no	no	no	no	no
Uses HSTS	no	no	no	no	no	no	no	no	no
Forward Secrecy	yes	no	no	no	no	no	no	no	no
BEAST	no	no	no	no	no	no	no	no	no
CRIME	yes	yes	yes	yes	yes	yes	yes	yes	yes
FREAK	yes	yes	yes	yes	yes	yes	yes	yes	yes
Heartbleed	yes	yes	yes	yes	yes	yes	yes	yes	yes
Lucky 13	no	no	no	no	no	no	no	no	no
POODLE	no	yes	yes	yes	yes	yes	yes	yes	yes
RC4 Bias	no	no	no	no	no	no	no	no	no
Logjam	no	no	no	no	no	no	no	no	no
DROWN	yes	no	no	no	no	no	no	no	no

Summarizing, can IoT encrypt?

	Amazon Echo			August Smart Lock	LG Smart LED TV	Nest Camera				Roku TV						SmartThings Hub			Securifi Almond	Sonos
	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_{11}	D_{12}	D_{13}	D_{14}	D_{15}	D_{16}	D_{17}	D_{18}	D_{19}	D_{20}
Grade	C	C	C	F	T (B)	T (C)	T (B)	T (B)	T (C)	T (B)	T (A)	T (B)	T (A)	T (A)	T (B)	T (C)	T (C)	T (B)	F	C
TLSv	1.0	1.0	1.0	1.2	1.2	1.2	1.2	1.2	1.0	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.0
SSLv3	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y
Domain Mismatch	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	N	N
Certificate Chain Issues	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Forward Secrecy	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	Y	N	Y
Weak Signature	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
RC4	N	N	N	N	Y	N	N	N	N	Y	N	N	N	N	Y	Y	Y	N	N	Y
POODLE	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	Y	N	N	Y

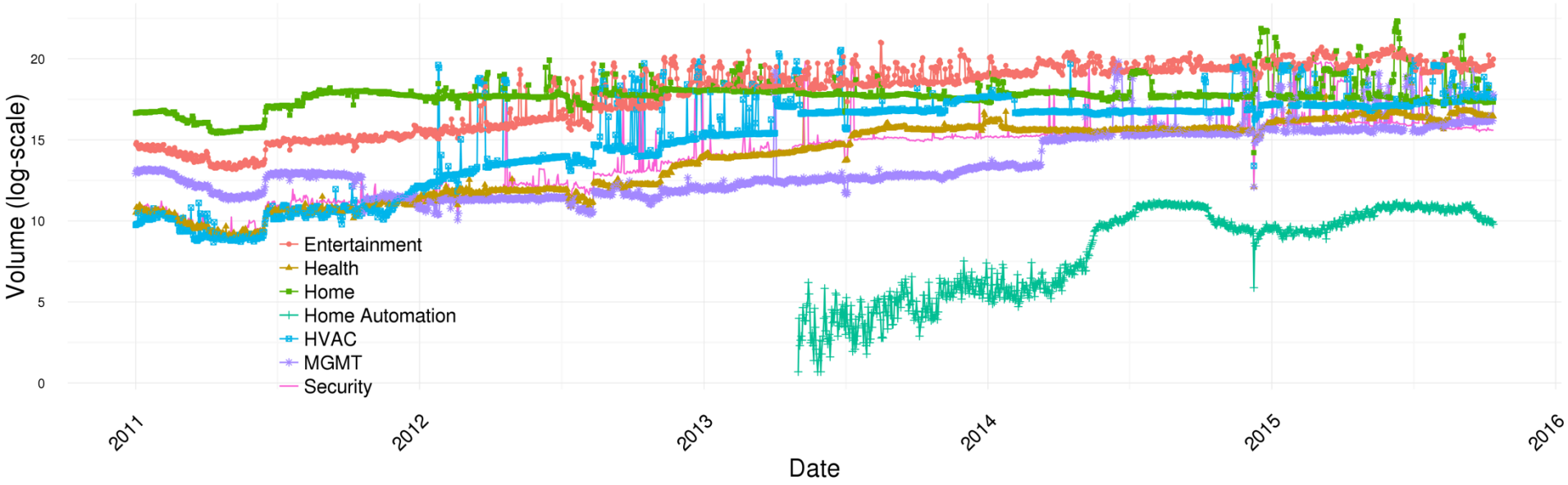
- Food for thought: Will these **known** security issues will ever be fixed (i.e., through patching)?

IoT device growth in the US (I)



- Using DNS data from one of the largest Telcos in the US, we can see the clear growth of certain very popular IoT devices over the last 5 years.

IoT device growth in the US (II)



- Note the home automation growth over the last 3 years.
- The rest of the groups of IoT devices have been steadily growing over the last half a decade.
- IoT are clearly growing in US Telcos.

IoT device growth in the US (III)

- What can we see from a week's worth of full DNS traffic?

DOW	Date	Daily DNS Lookups	Unique IPs
Thu	10/6/16	560,028,803	153,769
Fri	10/7/16	585,327,840	160,803
Sat	10/8/16	552,157,350	156,138
Sun	10/9/16	530,898,186	155,836
Mon	10/5/16	548,243,844	141,429
Tue	10/6/16	581,421,503	174,348
Wed	10/7/16	559,714,577	161,295

Policy Recommendations (I)

- By now we should all agree that this is a problem.
- There are some key points we need to consider (ordered from more basic to more sophisticated):
  - How can we ensure that devices are shipped with default password off?
  - How can we ensure that devices are able to facilitate unique passwords?
  - How can we “grade” the devices with the respect of the pen-testing they have been through? (think PCI-IoT)
  - How can we ensure that IoT devices can be tracked uniquely? **(Note: There is no hope for remediation without that.)**
  - How can we ensure that IoT devices can be patched?

Policy Recommendations (II)

- It is only mater of time for the US government to issue massive recalls on IoT devices due to security issues.
  - How can we do this in a way that is reasonable and objective?
- Food for thought:
  - Voluntary certification of IoT devices. Do we need for an UL certification mark for IoT devices?
    - **We are in desperate need of an IoT lab that would act as an early warning platform for security issues.**
  - US telecommunication companies own part of this problem. Instead of regulating the space, I suggest MAAWG-like initiatives to increase awareness and come up with practical solutions.
  - Who else have a stake in this game?
    - US and International manufacturing companies.
    - Retail chains.

    How can the DoC and the US government incentivize them to promote certified IoT devices?

The IoT things at your environment!

- Visit https://www.findyourthings.info/ from your local network and you will find out if you have a IoT-based trust violation problem. ☺

Back To Sessions

Details

24.72.227.139	192.168.1	27 Oct 01:07
IP	Subnet	Observation Date

Hosts

IP	Port/Path	HTTP Code	Annotation	
205	1400/xml/device_description.xml	200	SONOS Sonos PLAYBAR (B8-E9-37-7C-6D-46:1)	Details
144	1400/xml/device_description.xml	200	SONOS Sonos PLAY:1 (B8-E9-37-EC-C6-A8:B)	Details
39	1400/xml/device_description.xml	200	SONOS Sonos PLAY:1 (B8-E9-37-BF-18-BC:G)	Details
5	1400/xml/device_description.xml	200	SONOS Sonos SUB (B8-E9-37-64-61-78:F)	Details
2	80/description.xml	404		Details
2	80/api/v1/status	404		Details
2	80/	200		Details
2	80/api/config	404		Details

Thanks, questions?

manos@gatech.edu

http://astrolavos.gatech.edu/