Internet of Things

Security, Best Practices, AWS IoT

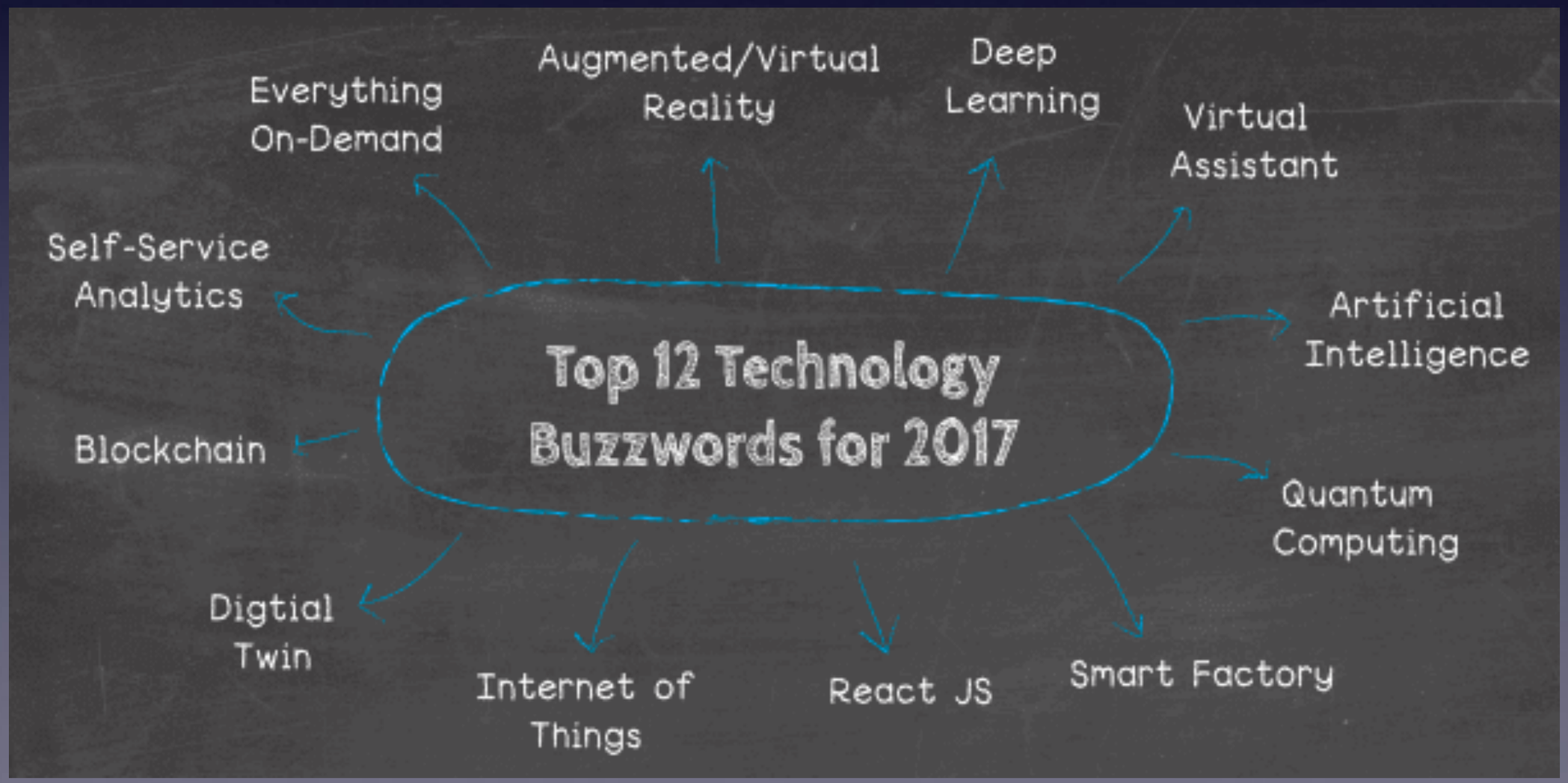
Who The Heck Am I?

- From Berkeley, California
- Work in San Francisco
- Co-Founder and Entrepreneur
- SF Internet Society IoT Working Group Chair
- Make Experimental Electronic Music

What the heck is IoT?

What the heck is IoT?

- Buzzword?



My definition

- Billions of internet-connected devices
- Form-factor convergence
- Interoperability nightmare
- Security nightmare
- Potential!

More stuff on the internet

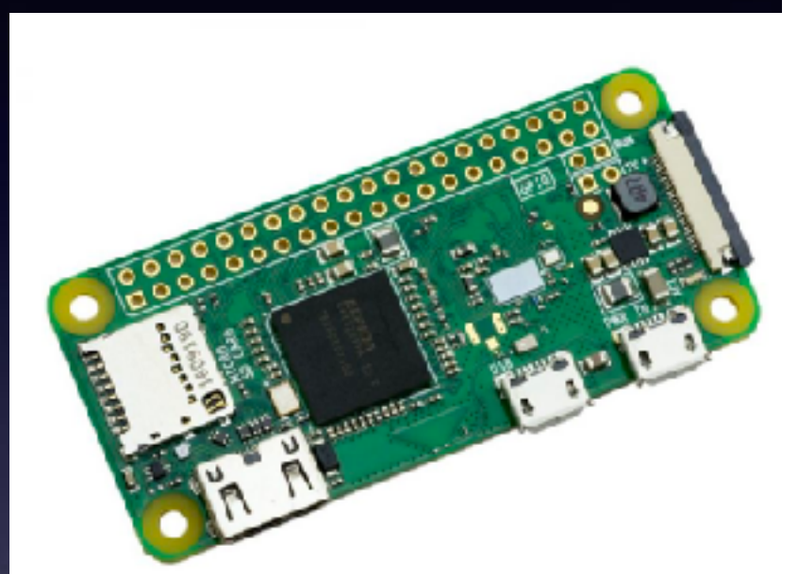
- 2.3 billion smart phone users in 2017
- 8 billion mobile subscriptions in 2017
- 20 billion IoT devices in 2017
- 30 billion IoT devices predicted in 2020

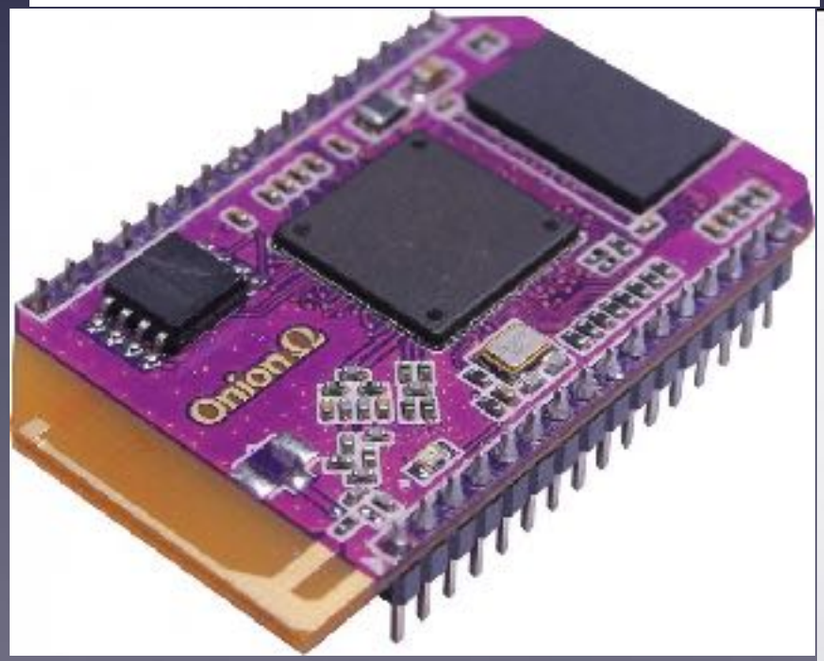
Source: Statista 2017

More stuff on the internet

- IPv4 addresses
- IPv6 addresses
- NAT (Network address translation)
- Massive botnets
- Critical infrastructure

Device convergence

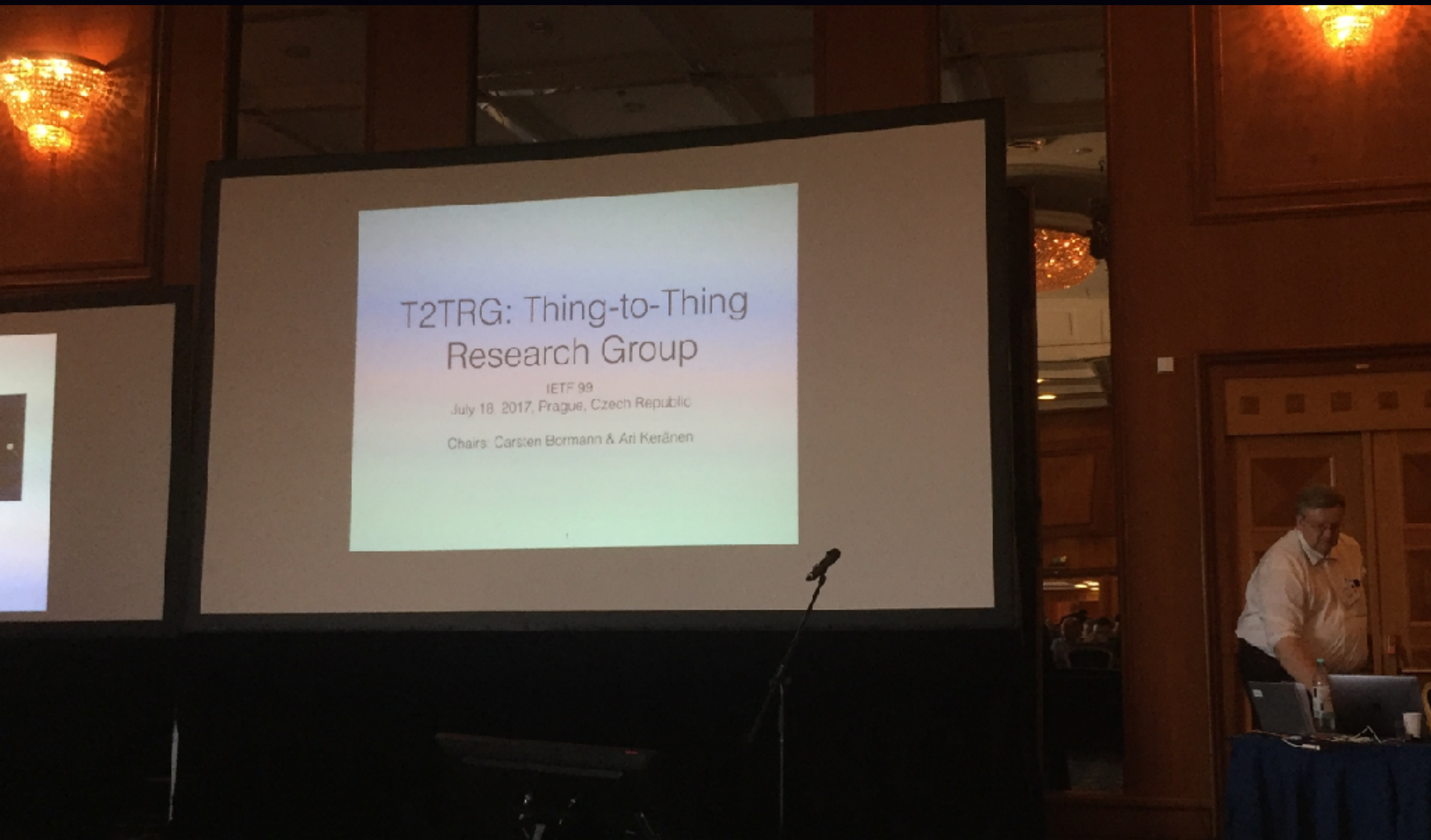




Interoperability

- Service advertisement and discovery
- Share resources (IP address, network)
- Conflicts (DHCP server, multicast)
- Unsolved problems

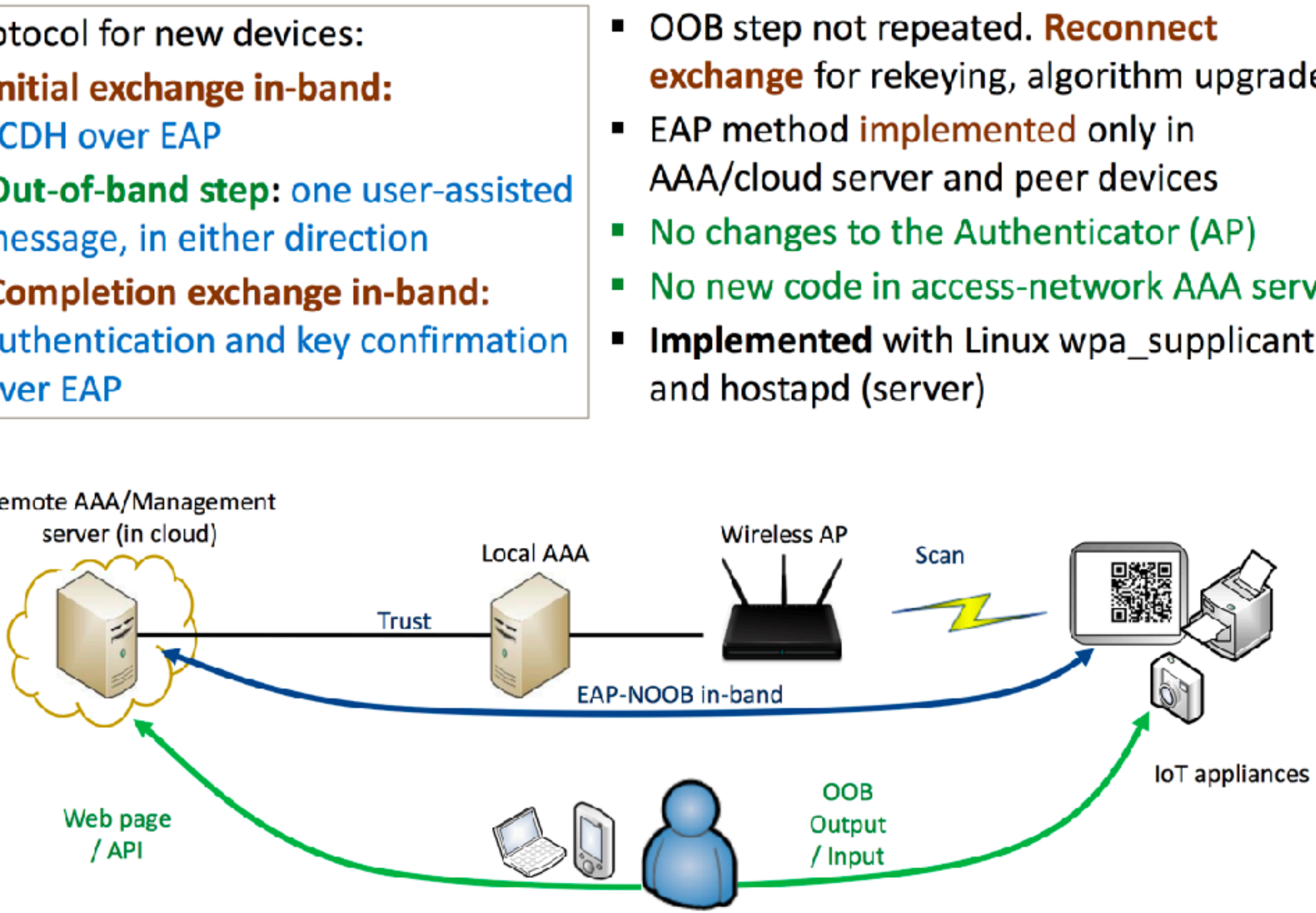
Standardization



Protocol for new devices:

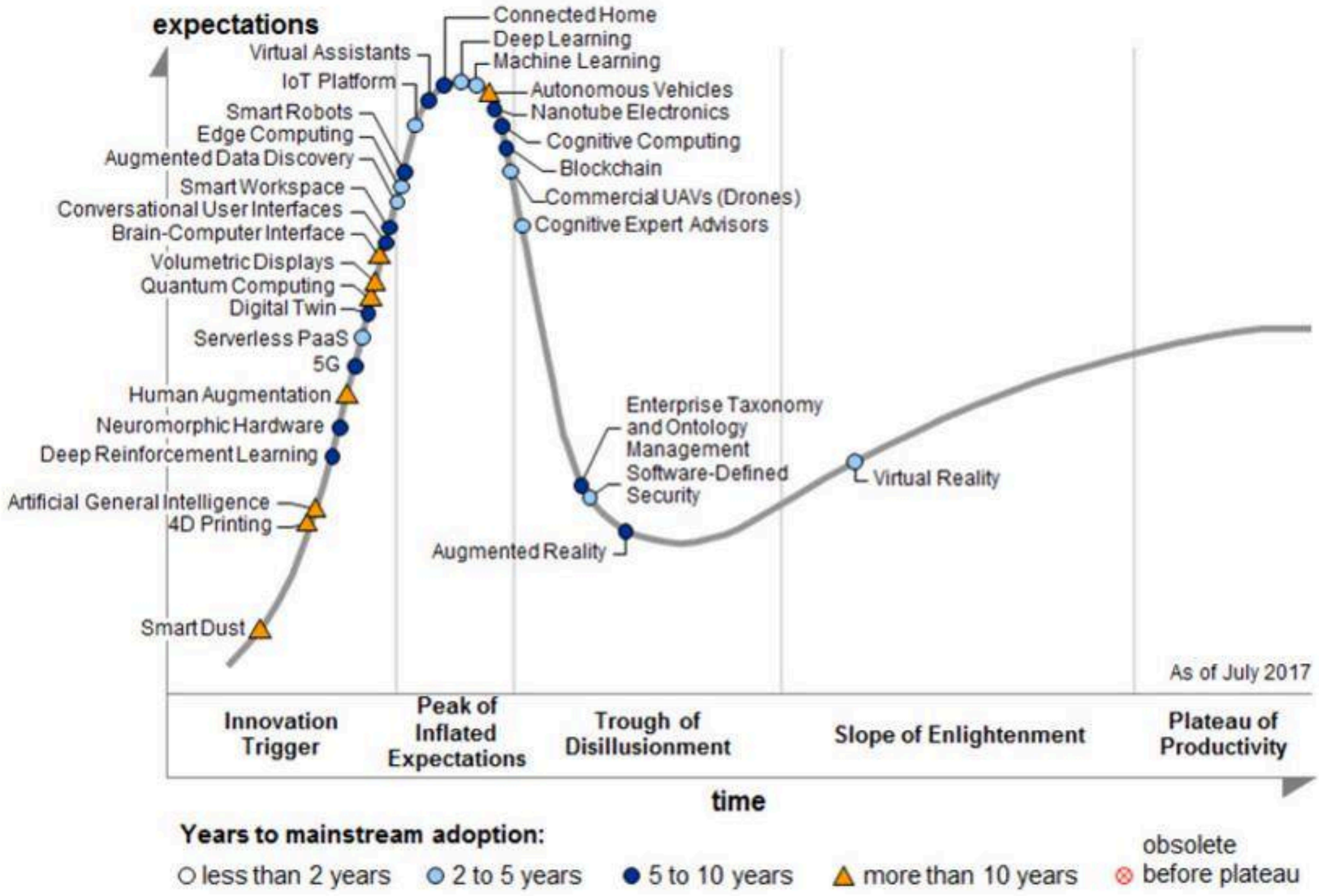
1. **Initial exchange in-band:**
   ECDH over EAP
2. **Out-of-band step:** one user-assisted message, in either direction
3. **Completion exchange in-band:**
   authentication and key confirmation over EAP

- OOB step not repeated. **Reconnect exchange** for rekeying, algorithm upgrade
- EAP method implemented only in AAA/cloud server and peer devices
- No changes to the Authenticator (AP)
- No new code in access-network AAA server
- **Implemented** with Linux wpa_supplicant and hostapd (server)



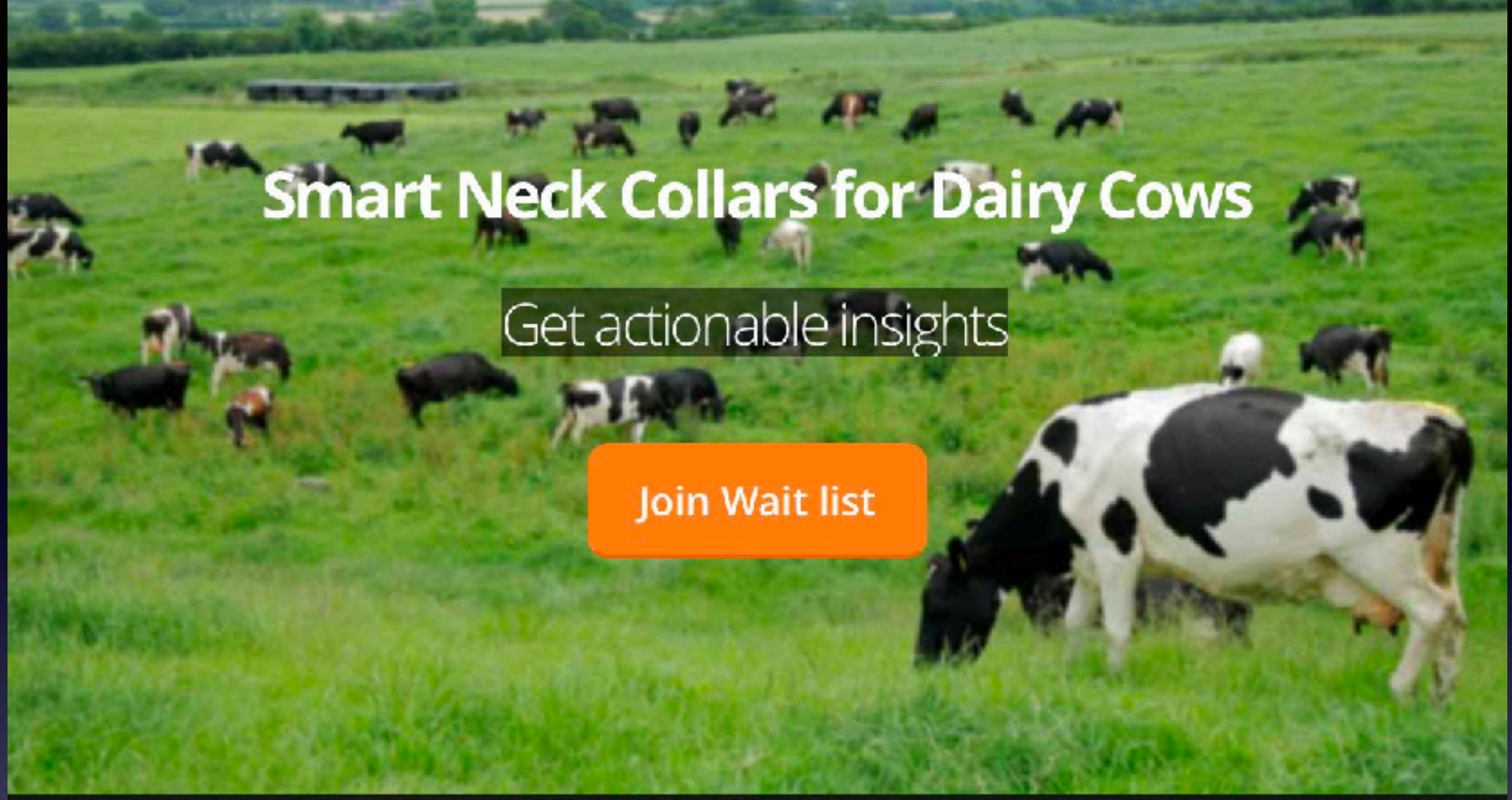
https://datatracker.ietf.org/doc/draft-aura-eap-noob

Hype Cycle for Emerging Technologies, 2017



Note: PaaS = platform as a service; UAVs = unmanned aerial vehicles

Source: Gartner (July 2017)

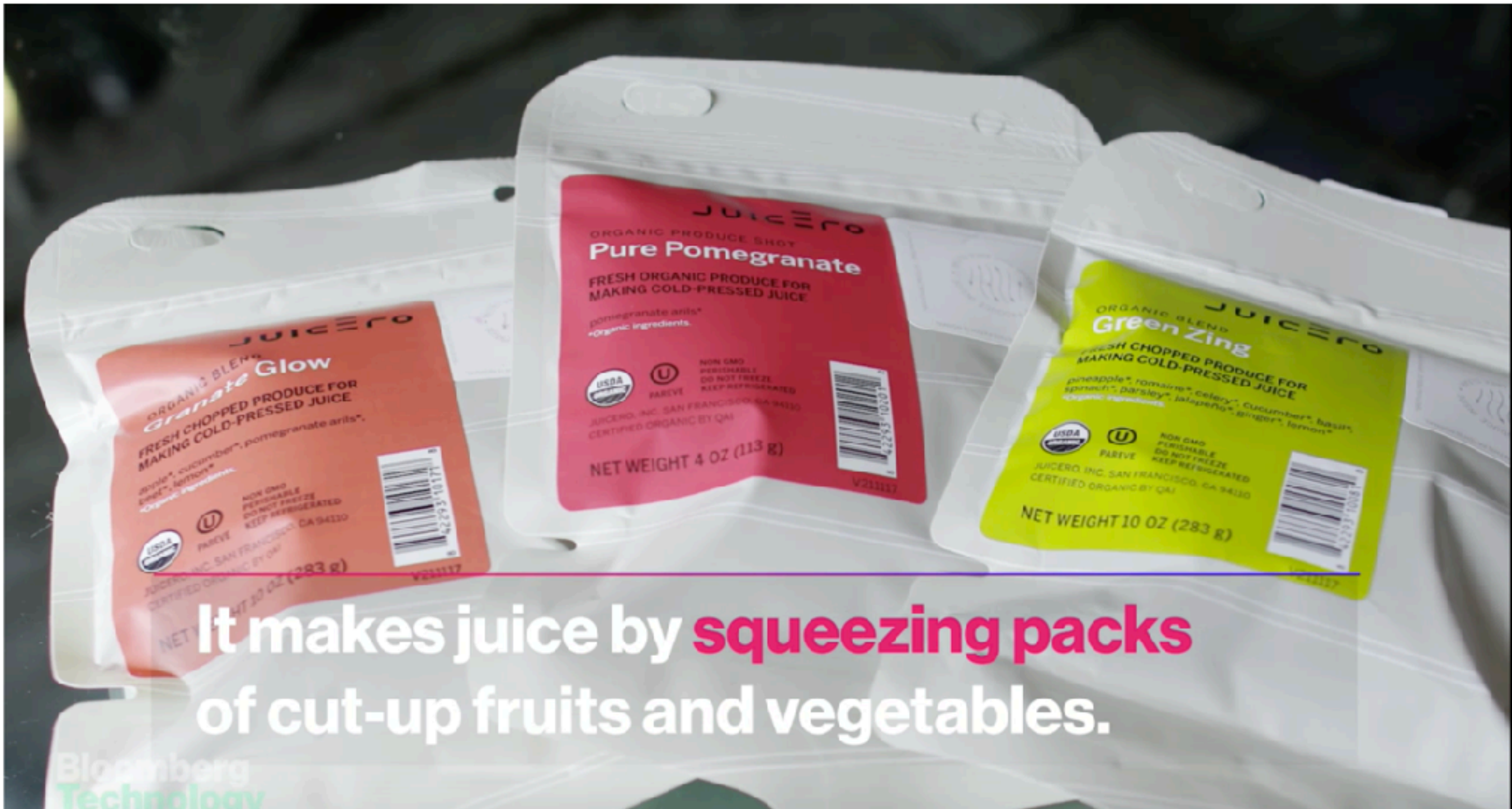


Streamline your dairy business!

Reduce labor, make good decisions & relax while we

Silicon Valley's $400 Juicer May Be Feeling the Squeeze

Two investors in Juicero were surprised to learn the startup's juice packs could be squeezed by hand without using its high-tech machine.



Bloomberg Technology

Wi-Fi Connectivity

Remotely monitor your cooktop and oven for peace of mind. Remotely turn on/off, preheat, and adjust temperature or time on your oven for ultimate cooking experience.

**As a safety precaution, remote start function only available on the Electric range.*

Powerful Cooktop

Enjoy the flexibility to cook on 5 specialized burners simultaneously. For added convenience, the oval burner can be used for oversized pots and pans.


[8028.420066] 0000000000000000 0000000000000019 0000000000000000 ffff88001a045
c00
[8028.420066] ffff88001a4c34c8 ffff88001f3f8000 ffff88001f3f8000 0000000000000
041
[8028.420066] Call Trace:
[8028.420066] [<ffffffff8107e9ca>] lg_local_lock+0x1a/0x20
[8028.420066] [<ffffffff811907f6>] path_init+0x1e6/0x400
[8028.420066] [<ffffffff81190973>] path_lookupat+0x33/0x720
[8028.420066] [<ffffffff81194af0>] ? __pollwait+0xf0/0xf0
[8028.420066] [<ffffffff81194af0>] ? __pollwait+0xf0/0xf0
[8028.420066] [<ffffffff8116df17>] ? kmem_cache_alloc+0x67/0x130
[8028.420066] [<ffffffff81191091>] do_path_lookup+0x31/0xc0
[8028.420066] [<ffffffff818cc933>] ? getname_flags+0x53/0xf0
[8028.420066] [<ffffffff81191bfd>] user_path_at_empty+0x5d/0xa0
[8028.420066] [<ffffffff8119c75c>] ? destroy_inode+0x3c/0x70
[8028.420066] [<ffffffff816046f5>] ? _raw_spin_lock_irq+0x15/0x20
[8028.420066] [<ffffffff811c9224>] ? eventfd_ctx_read+0xa4/0x1e0
[8028.420066] [<ffffffff81191e51>] user_path_at+0x11/0x20
[8028.420066] [<ffffffff81186ce5>] vfs_fstatat+0x35/0x70
[8028.420066] [<ffffffff81186d5b>] vfs_stat+0x1b/0x20
[8028.420066] [<ffffffff81186f8a>] sys_newstat+0x1a/0x40
[8028.420066] [<ffffffff811826ZZ>] ? vfs_read+0x182/0x180
[8028.420066] [<ffffffff811826ea>] ? sys_read+0x4a/0x90
[8028.420066] [<ffffffff8119621b>] ? sys_poll+0x6b/0x100
[8028.420066] [<ffffffff8160c969>] system_call_fastpath+0x16/0x1b
[8028.420066] Code: 84 00 00 00 00 00 0f 1f 00 55 b8 00 00 01 00 48 89 e5 3e 0f
c1 07 89 c1 c1 e9 10 66 39 c1 89 ca 74 11 0f 1f 80 00 00 00 00 f3 90 <0f> b7 07
66 39 d0 75 f6 5d c3 0f 1f 40 00 8b 17 55 31 c0 48 89
For more information about owning your own networ
VODKA3.com


130
110
90
70
50
30
10
MPH

Update gone wrong leaves 500 smart locks inoperable

Fatal error leaves customers scrambling for fixes that can take a week or longer.

DAN GOODIN - 8/15/2017, 1:07 AM

NEWS

Parents warned over exploding fidget spinners powered by Bluetooth

Fidget spinners burst on to the scene earlier this year and rapidly gained popularity amongst children

COMMENTS

BY JAMES RODGER

Ahead | Turn Any Helmet Into A Smart Helmet

56%
funded

$28,327
pledged

33
days to go

HAPIFORK 2013

Jérôme Lepine
Quantified-self device

The HAPIfork is an electronic fork that monitors your eating habits and alerts you with the help of lights and gentle vibrations when you eat too fast, with

WHISTLE 2014

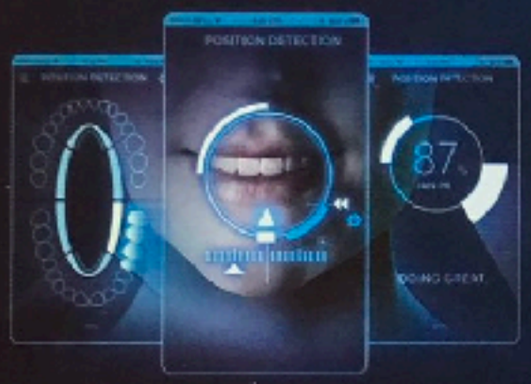
Ben Jacobs, Whistle Labs, Inc.
Monitor activity

BRAUN

Oral-B

GENIUS

9000A



ポジション検知機能付き

歯科医が推奨する磨き方を実現する
インテリジェントな電動歯ブラシ

USB充電機能付きトラベルケース

Bluetooth
SMART

充電式
RECHARGEABLE TOOTHBRUSH

*P&G調べ。世界の歯科医師を対象にした継続的サンプル調査に基づく。

Security

Security

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2015

Alert Number
I-091015-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights

Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Topics: Internet Policy | Internet Policy Task Force | Cybersecurity

Date:

June 08, 2017

Docket Number:

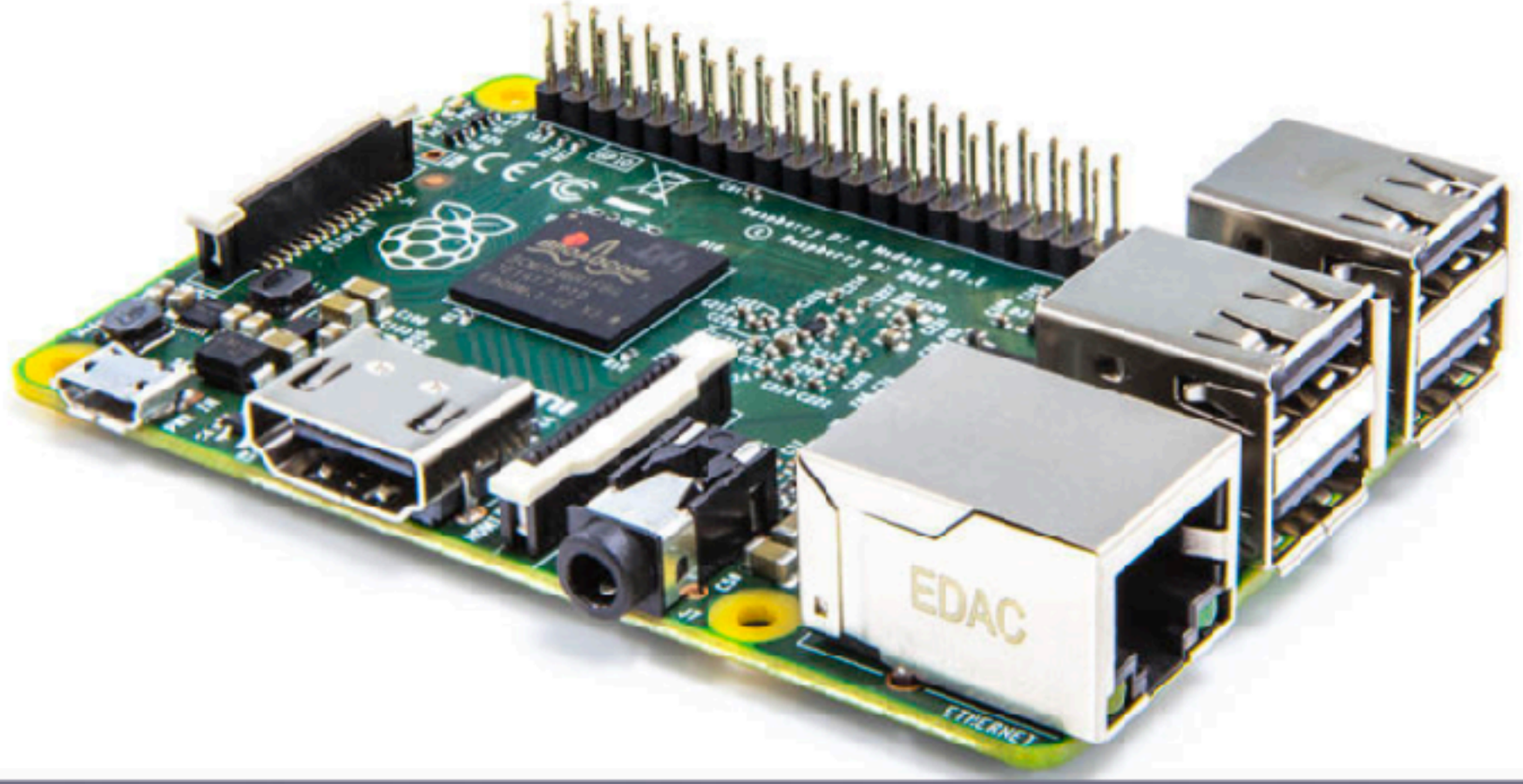
170602536-7536-01

NTIA, on behalf of the Department of Commerce, is requesting comment on actions that can be taken to address automated and distributed threats to the digital ecosystem as part of the activity directed by the President in Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Through this Request for Comments, NTIA seeks broad input from all interested stakeholders - including private industry, academia, civil society, and other security experts - on ways to improve industry's ability to reduce threats perpetuated by automated distributed attacks, such as botnets, and what role, if any, the U.S. Government should play in this area.

Linux malware enslaves Raspberry Pi to mine cryptocurrency

It's time to update your Raspberry Pi devices or risk them being infected with cryptocurrency mining malwa

By Liam Tung | June 8, 2017 -- 12:23 GMT (05:23 PDT) | Topic: Security



RELATED STORIES

Security
Google Chrome under atta you used one of these hija extensions?

Security
Petya ransomware: Cyber costs could hit $300m for giant Maersk

Security
ShadowPad: Backdoor in e server software exposed

Security
Google awards student $1 discovery of App Engine d flaw

NEWSLETTERS

ZDNet Security

Your weekly update on security around

Mirai Botnet

- Japanese for “future”

Mirai Botnet

- Has 60 common factory default logins
- Infected security cameras, routers
- September and October 2016
- Took most of the internet offline

Mirai Botnet

- Krebs On Security: 620Gbit/s
- OVH French web host: 1Tbit/s
- Dyn offline: taking down GitHub, Twitter, Reddit, Netflix, Airbnb, etc
- 900,000 Deutsche Telekom routers crashed

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00E
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Agent **183-scottlinux** Location **US - Fremont** Network **Abovenet Comm ... (AS17025)**	208.67.222.222	OpenDNS, LLC ... (AS36692)	✔	14 ms	199.16.156.70 199.16.156.230 199.16.156.198 199.16.156.102 expand
	74.207.242.5	Linode, LLC ... (AS63949)	✖	64 ms	expand
	45.33.58.84	Linode, LLC ... (AS63949)	✖	66 ms	expand
	8.8.8.8	Google Inc. ... (AS15169)	✖	2 ms	expand
Agent **187-TWCRR-AS10796** Location **US - Cleveland** Network **Time Warner C ... (AS10796)**	209.18.47.62	Time Warner C ... (AS7843)	✖	13 ms	expand
	208.67.222.222	OpenDNS, LLC ... (AS36692)	✔	26 ms	199.16.156.102 199.16.156.198 199.16.156.70 199.16.156.230 expand
	209.18.47.61	Time Warner C ... (AS7843)	✖	22 ms	expand
	8.8.8.8	Google Inc. ... (AS15169)	✖	37 ms	expand
	8.8.8.8	Google Inc. ... (AS15169)	✖	26 ms	expand
Agent **188-STLMO** Location **US - St. Louis** Network **Charter Commu ... (AS20115)**	208.67.222.222	OpenDNS, LLC ... (AS36692)	✔	40 ms	199.59.150.7 199.59.148.10 199.59.149.198 199.59.148.82 expand
	24.196.64.53	Charter Commu ... (AS20115)	✖	42 ms	expand
Agent **190-ATT-AS7018** Location **US - Cleveland** Network **AT&T Services ... (AS7018)**	208.67.222.222	OpenDNS, LLC ... (AS36692)	✔	28 ms	199.16.156.230 199.16.156.198 199.16.156.102 199.16.156.70 expand
	8.8.8.8	Google Inc. ... (AS15169)	✖	37 ms	expand
	68.94.157.1	AT&T Services ... (AS7018)	✖	21 ms	expand
	68.94.156.1	AT&T Services ... (AS7018)	✖	960 ms	expand
	8.8.8.8	Google Inc. ... (AS15169)	✖	2 ms	expand

Do security right

- Problem: time to market incentives
- Solution: open certification

OTA
Online Trust Alliance
an Internet Society initiative

IoT Security & Privacy Trust Framework v2.0

The IoT Trust Working group has developed the IoT Trust Framework® including a set of required and recommended strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, key criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines requirements including the need for comprehensive disclosures which must be provided prior to product purchase articulating policies regarding data collection, usage and sharing, as well as the terms and condition of security patching post warranty.

Why a certification?

Do security right

- No passwords! Mutual TLS authentication ONLY
- No passwords!
- Remote (signed) updates OR expiration date
- Closed source = more liability

Potential

- Medical devices
- Smart cars/homes/cities
- Cheap distributed sensors
- Security locks/surveillance/alarms
- Easy checkout while shopping
- Lots more!

Building an IoT system

- Concepts
- Client
- Cloud services

Concepts

Concepts

- “Thing” & “Registry”

Concepts

- MQTT (Message Queue Telemetry Transport)
- ISO standard
- Real-time only

Shadow

AWS IoT Shadow - Simple Yet Powerful

Report its current state to one or multiple shadows
Retrieve its desired state from shadow

Thing

Shadow reports delta, desired and reported states along with metadata and version

Shadow

Set the desired state of a device
Get the last reported state of the device
Delete the shadow

Mobile App

```
{
"state" : {
    "desired" : {
        "lights": { "color": "RED" },
        "engine" : "ON"

    },
    "reported" : {
        "lights" : { "color": "GREEN"  },
        "engine" : "ON"
    },
    "delta" : {
        "lights" : { "color": "RED"  }
    } },
"version" : 10

}
```

Backend (λ)

- Serverless
- AWS Lambda is great
- IoT messages can trigger lambdas

Client

- Node.js
- Python
- Java
- C

AWS IoT Demo

- Create thing
- IoT client
- Create rule to invoke lambda
- Send message from IoT client to Lambda
- Lambda sends SMS

https://www.youtube.com/watch?v=a26LskU5FJ8

AWS IoT Tips

- Device state = **Partition** from CAP Theorem
- Encode desired state with device shadow
- Messages may arrive out of order
- Device shadow uses latest version only

What should I use?

- AWS IoT?
- C/Python 3/Lambda?
- Depends what you are doing

Questions?