VENABLE

Identity and the Internet of Things

Jeremy Grant

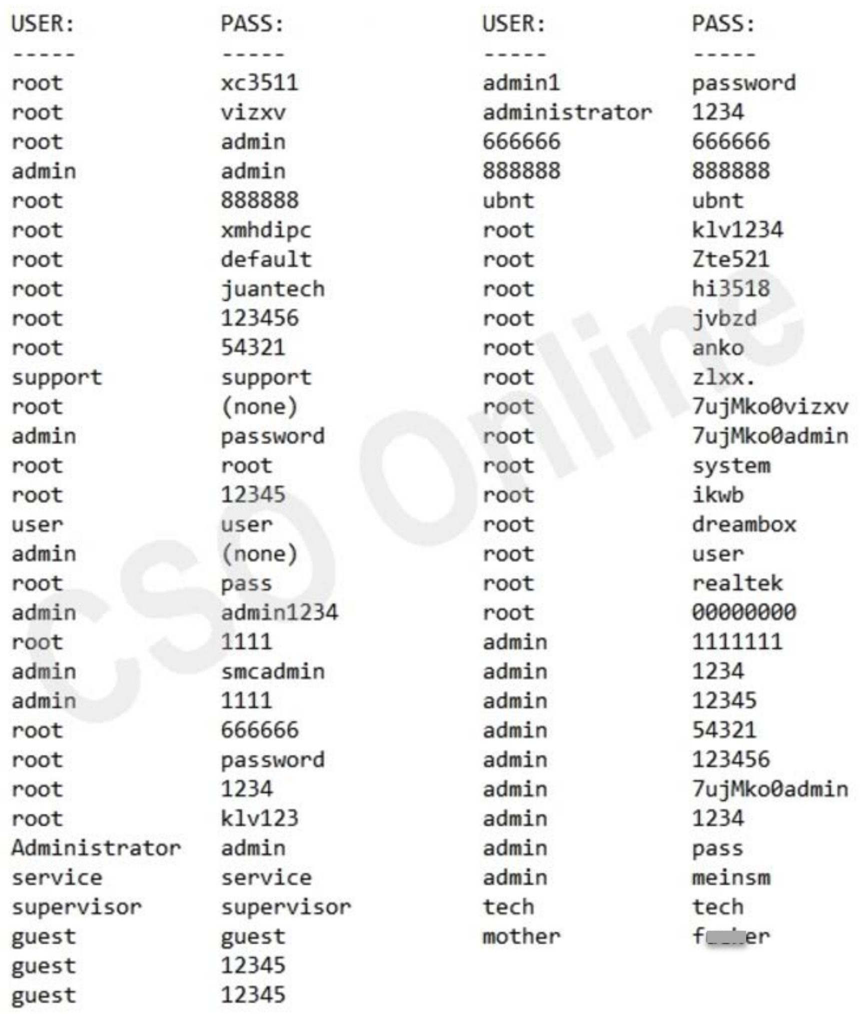
Managing Director, Technology Business Strategy

jeremy.grant@Venable.com

@jgrantindc

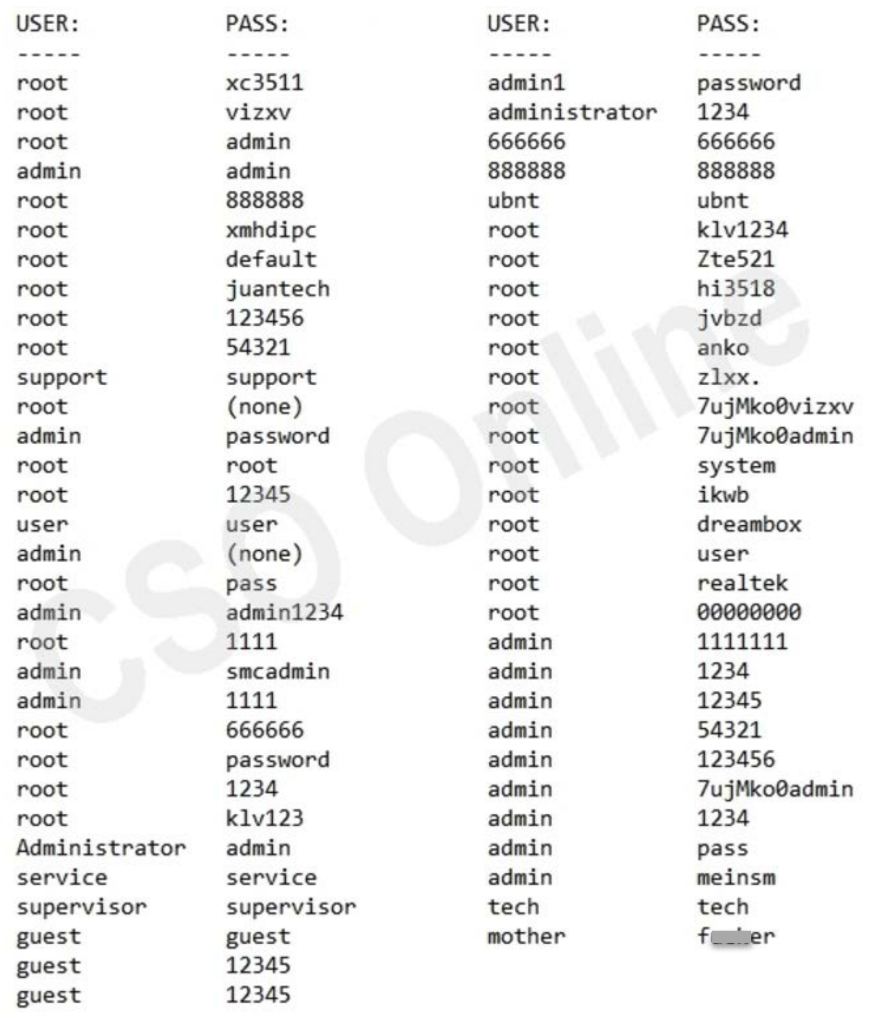
NIST IOT Cybersecurity Colloquium - October 19, 2017

IOT: Why identity matters

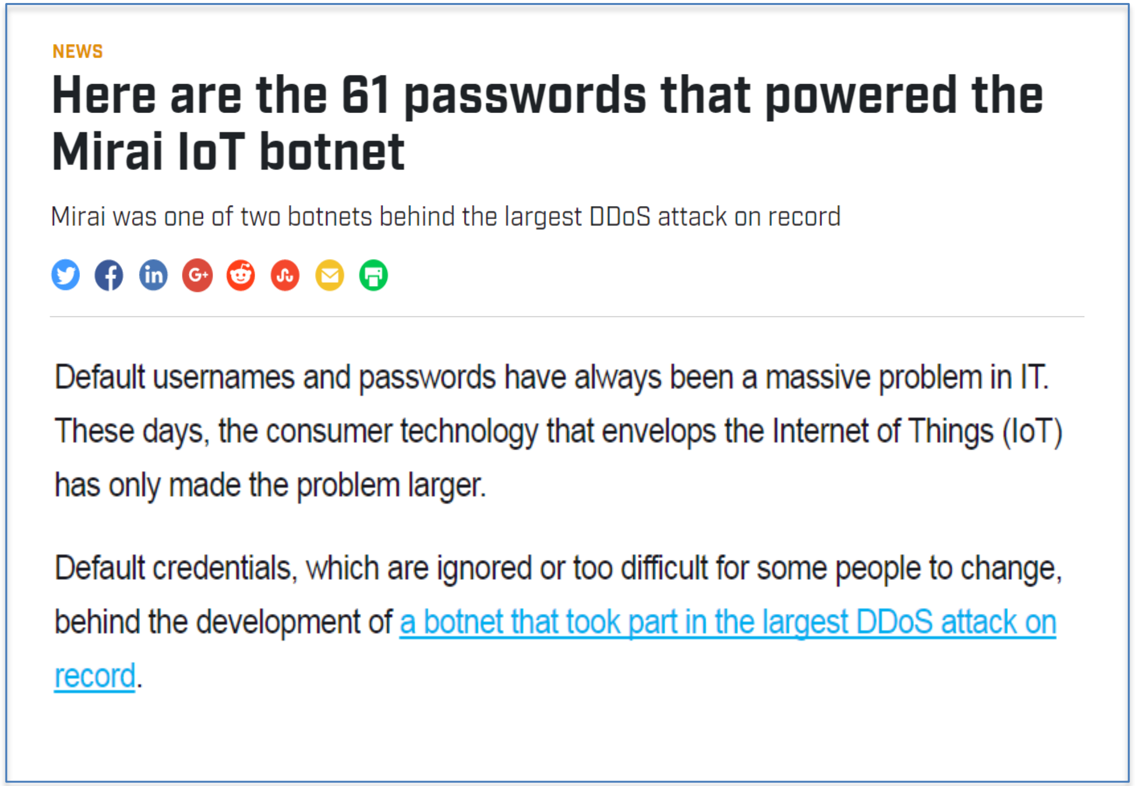


USER:	PASS:
-----	-----
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345
USER:	PASS:
-----	-----
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	00000000
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	f[redacted]er

IOT: Why identity matters



```
USER:          PASS:          USER:          PASS:
-----          -----          -----          -----
root           xc3511         admin1         password
root           vizxv          administrator  1234
root           admin          666666         666666
admin          admin          888888         888888
root           888888         ubnt           ubnt
root           xmhdipc        root           klv1234
root           default        root           Zte521
root           juantech       root           hi3518
root           123456         root           jvbzd
root           54321          root           anko
support        support        root           zlxx.
root           (none)         root           7ujMko0vizxv
admin          password       root           7ujMko0admin
root           root           root           system
root           12345          root           ikwb
user           user           root           dreambox
admin          (none)         root           user
root           pass           root           realtek
admin          admin1234      root           00000000
root           1111           admin          1111111
admin          smcadmin       admin          1234
admin          1111           admin          12345
root           666666         admin          54321
root           password       admin          123456
root           1234           admin          7ujMko0admin
root           klv123         admin          1234
Administrator  admin          admin          pass
service        service        admin          meinsm
supervisor     supervisor     tech           tech
guest          guest          mother         f[redacted]er
guest          12345
guest          12345
```



NEWS

Here are the 61 passwords that powered the Mirai IoT botnet

Mirai was one of two botnets behind the largest DDoS attack on record

Default usernames and passwords have always been a massive problem in IT. These days, the consumer technology that envelops the Internet of Things (IoT) has only made the problem larger.

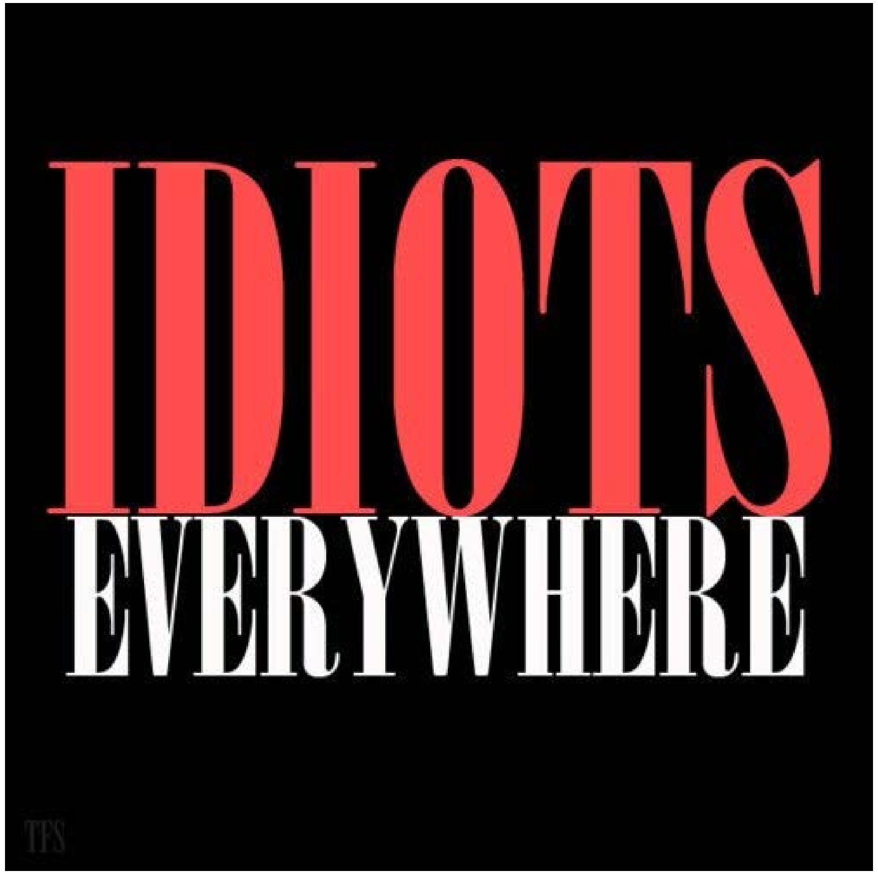
Default credentials, which are ignored or too difficult for some people to change, behind the development of a botnet that took part in the largest DDoS attack on record.

The relevant acronym

ID IOT

IDentity of Internet of Things

Let’s turn this into a good thing!

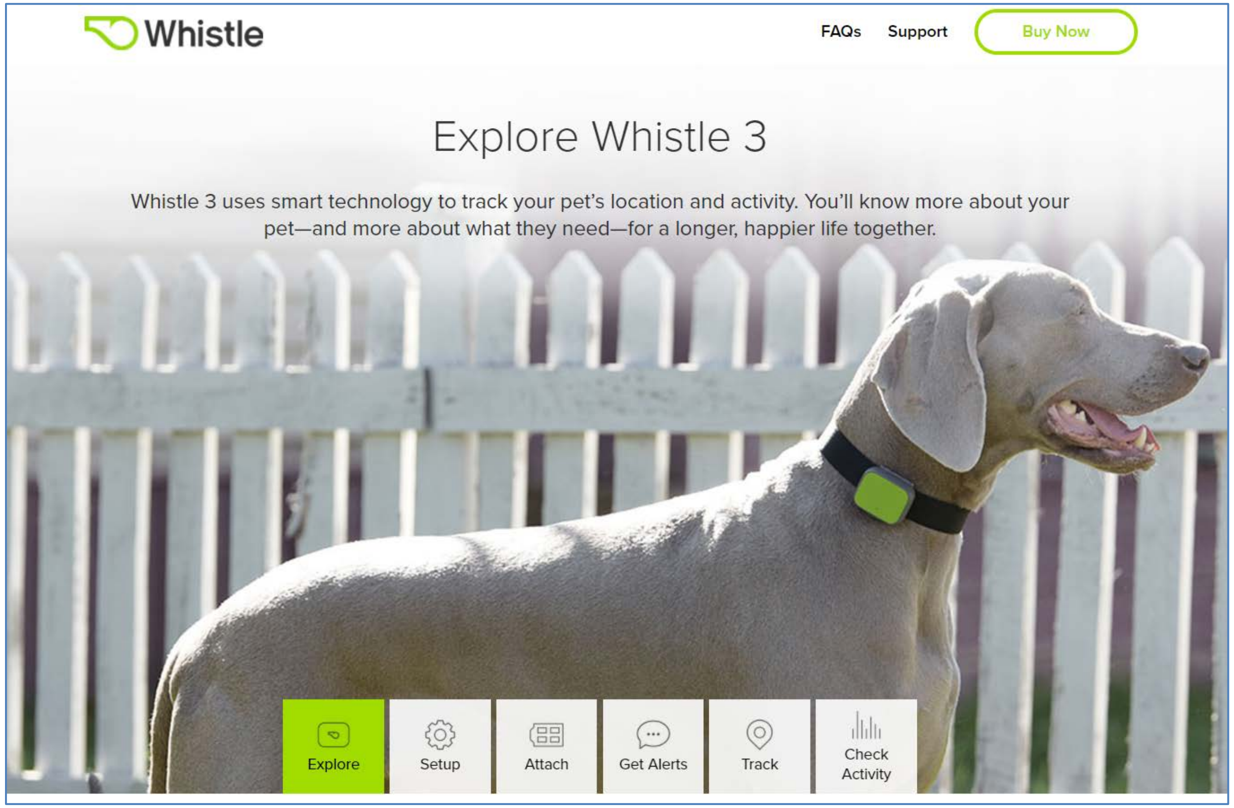


Evolution

1993

"On the Internet, nobody knows you're a dog."

2017

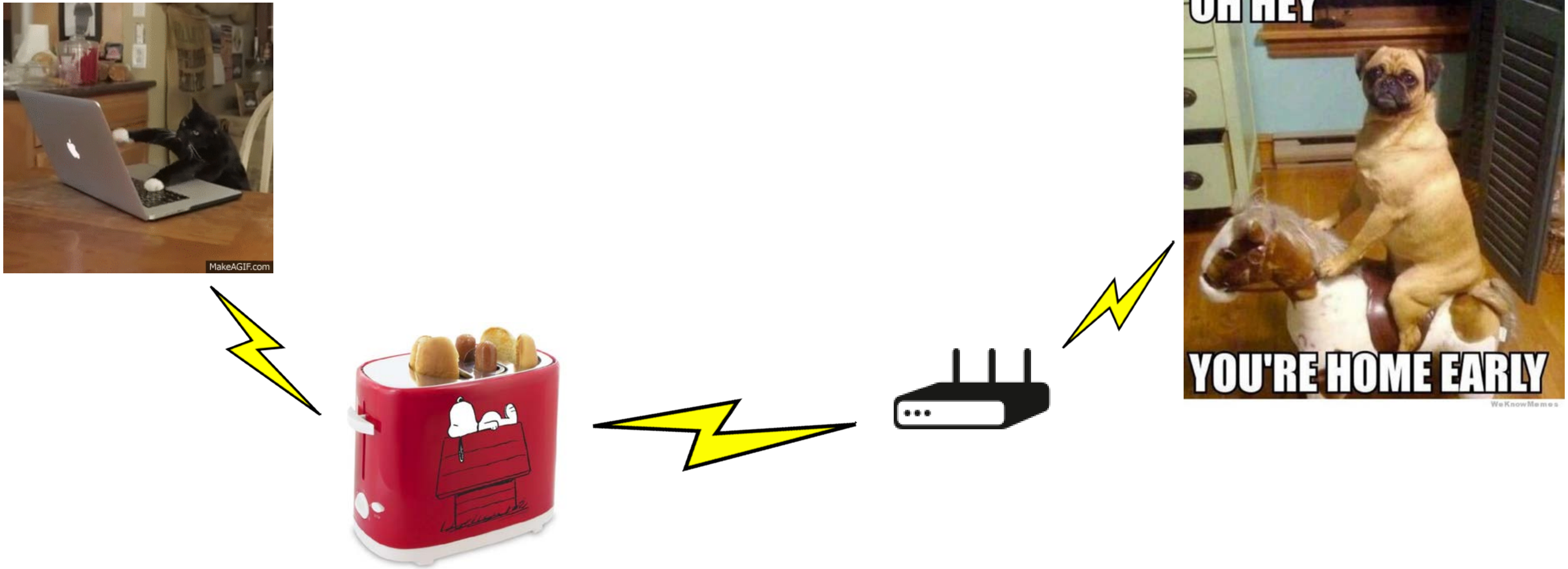


Explore Whistle 3

Whistle 3 uses smart technology to track your pet's location and activity. You'll know more about your pet—and more about what they need—for a longer, happier life together.

If your dog is on the Internet,
how do you know it's not a toaster?

Or – how do you make sure that someone can’t take hack into your toaster and use it to control your dog?



Authentication is important to ID-IOT

But it’s not the only thing

The “5 As” of Identity

Authentication

- The means by which a receiver of an electronic transaction or message makes a decision to accept or reject that transaction or message*
- Is a device what it claims to be?
- Is the entity seeking to control a device who or what it claims to be?

Authorization

- What actions is a device – or an entity seeking to control a device – authorized to perform?
- How are permissions or delegations granted or revoked?

Analytics

- Detecting whether identities are being used improperly or suspiciously – and triggering additional, appropriate controls

Audit

- Looking back to review events and confirm the identity system was being used properly
- Determining what happened if it was not

Administration

- How is the identity system governed?
- How are the policies and processes of the identity system managed?
- How are new devices and entities added or removed from the identity system?

*Asia-Pacific Economic Cooperation (APEC) Report, 2002

Why the "5 As" of Identity Matter

Authentication | Authorization | Analytics | Audit | Administration

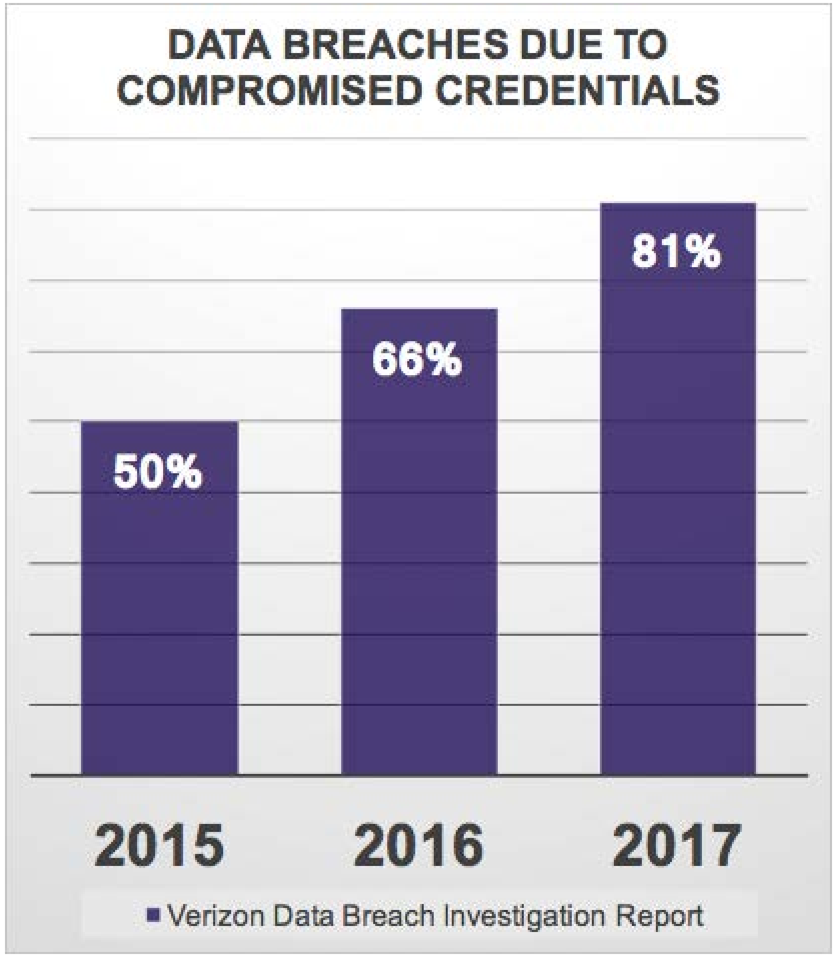
- Most IoT devices connect – at some point – to the cloud
- Human control of – and access to – these devices is generally controlled by traditional identity solutions
- A full-lifecycle approach to identity is needed to govern access to Things on the Internet

Let’s go back to Authentication

Default passwords are bad.

Let’s go back to Authentication

But…how much will changing passwords help?



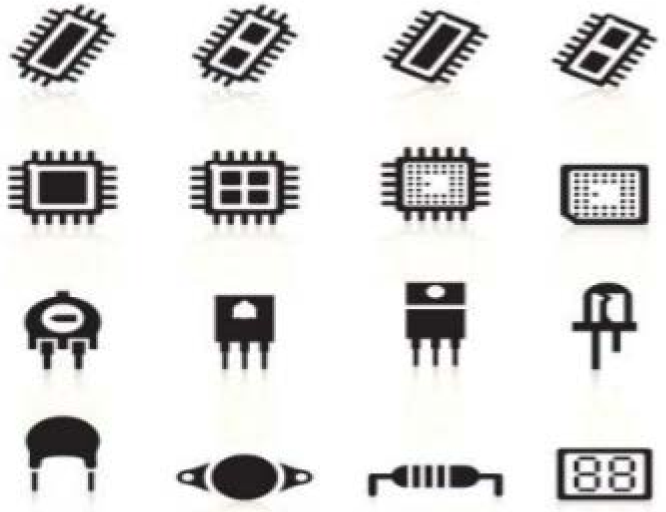
The security value of passwords

Authentication in IOT: What's Better?

The ideal (from a security perspective): cryptographic keys

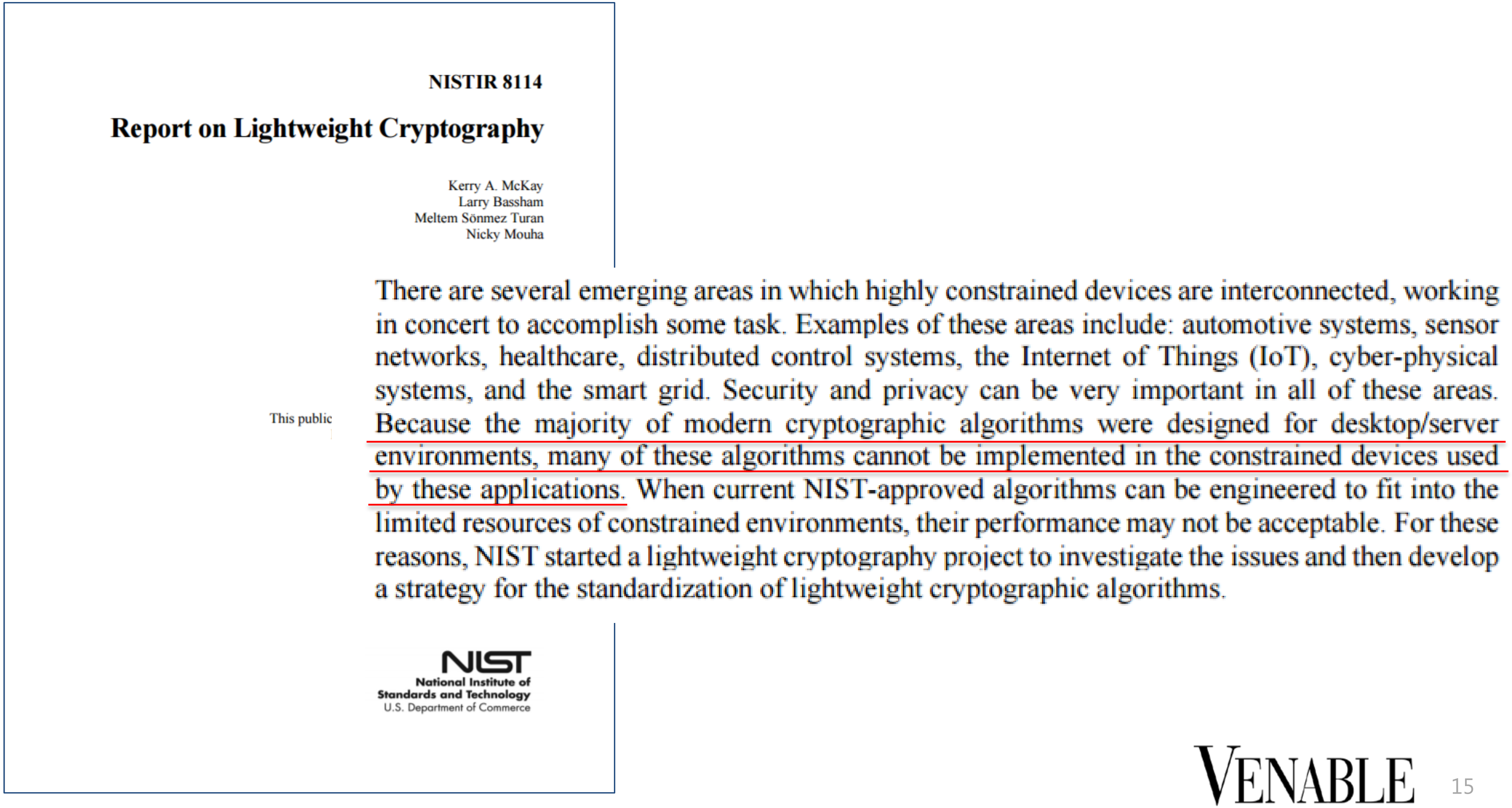
But in the IOT, not all the "T's" have the same capabilities.

- The "things" we are connecting to the Internet vary widely…
- …as do the chips within them



VENABLE

Not all crypto works in all things



NISTIR 8114

Report on Lightweight Cryptography

Kerry A. McKay
Larry Bassham
Meltem Sönmez Turan
Nicky Mouha

This public

There are several emerging areas in which highly constrained devices are interconnected, working in concert to accomplish some task. Examples of these areas include: automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. Security and privacy can be very important in all of these areas. Because the majority of modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in the constrained devices used by these applications. When current NIST-approved algorithms can be engineered to fit into the limited resources of constrained environments, their performance may not be acceptable. For these reasons, NIST started a lightweight cryptography project to investigate the issues and then develop a strategy for the standardization of lightweight cryptographic algorithms.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

So we’ll need different types of authentication

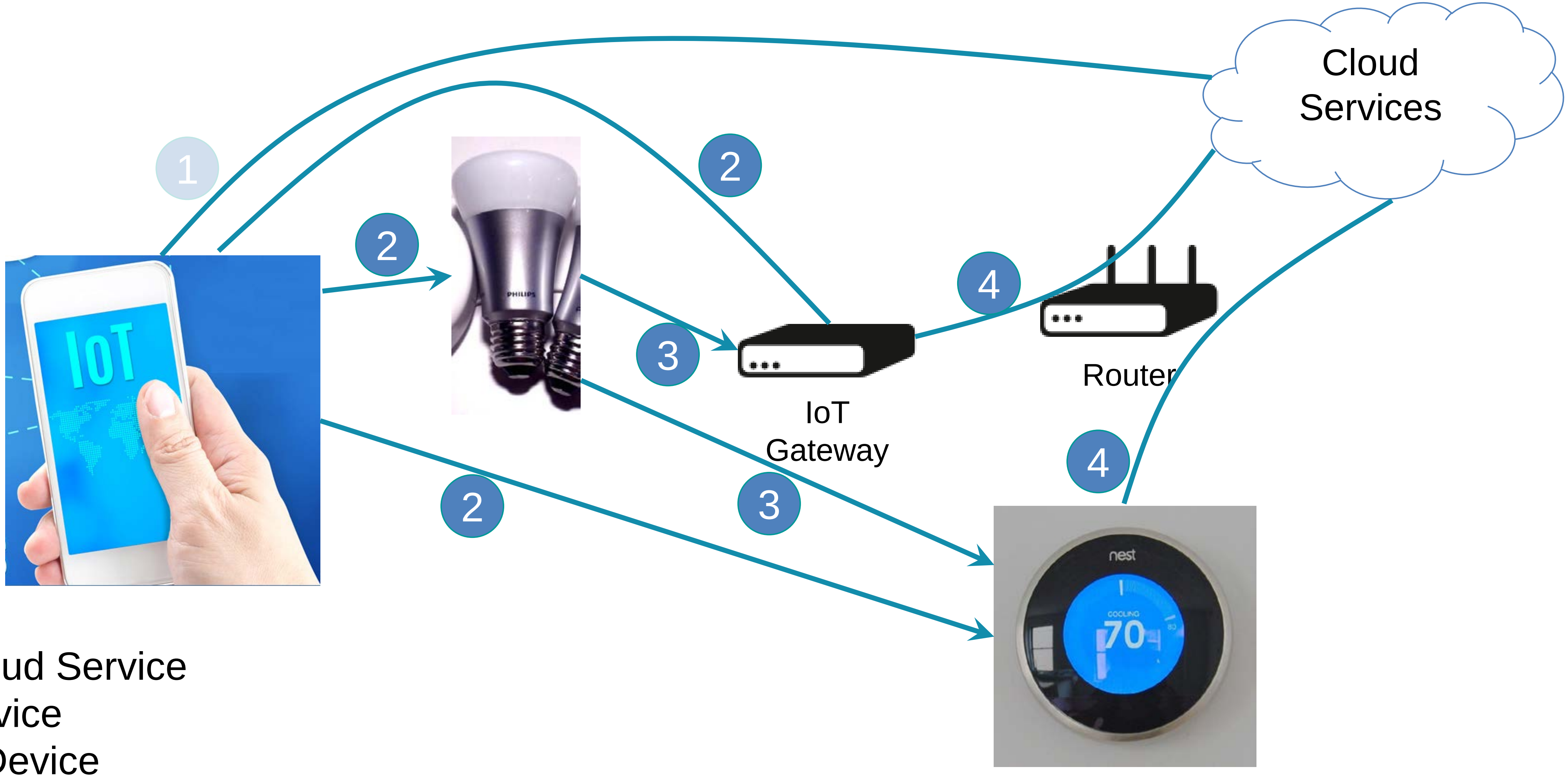
- PKI/X.509 certs are highly secure – but not feasible in many devices, and may be overkill
- FIDO standards (aka “PK without the I”) can deliver PK-based security with less overhead
- Constrained devices will likely need something else – more work needed here
- 2016 Cornell paper* declared there are 40+ authentication protocols which may apply – and noted many have shortcomings

*https://arxiv.org/pdf/1612.07206.pdf

Also: there are different authentication use cases.

Different authentication use cases

Thanks to NokNok Labs for Ideas and content here!



1. User to Cloud Service
2. User to Device
3. Device to Device
4. Device to Cloud Service

Keep in mind

- Some devices will be connected directly to the Internet
- Some won’t – but will be connected to other devices that are
- Any device could be an attack point

Secure identity for every connected device becomes very important

Summary: Where Work is Needed

1. Guidance on how to handle the “5 As” of the IOT Identity life cycle
   - Authentication
   - Authorization
   - Analytics
   - Audit
   - Administration

2. Specific work on Authentication for IOT
   - Passwords aren’t the only answer
   - Lightweight crypto – to enable strong ID-IOT authentication in devices of all shapes, sizes and capabilities
   - Focus on the 4 major use cases – and are there others?

One more thing…

We need to prevent a race to the bottom.

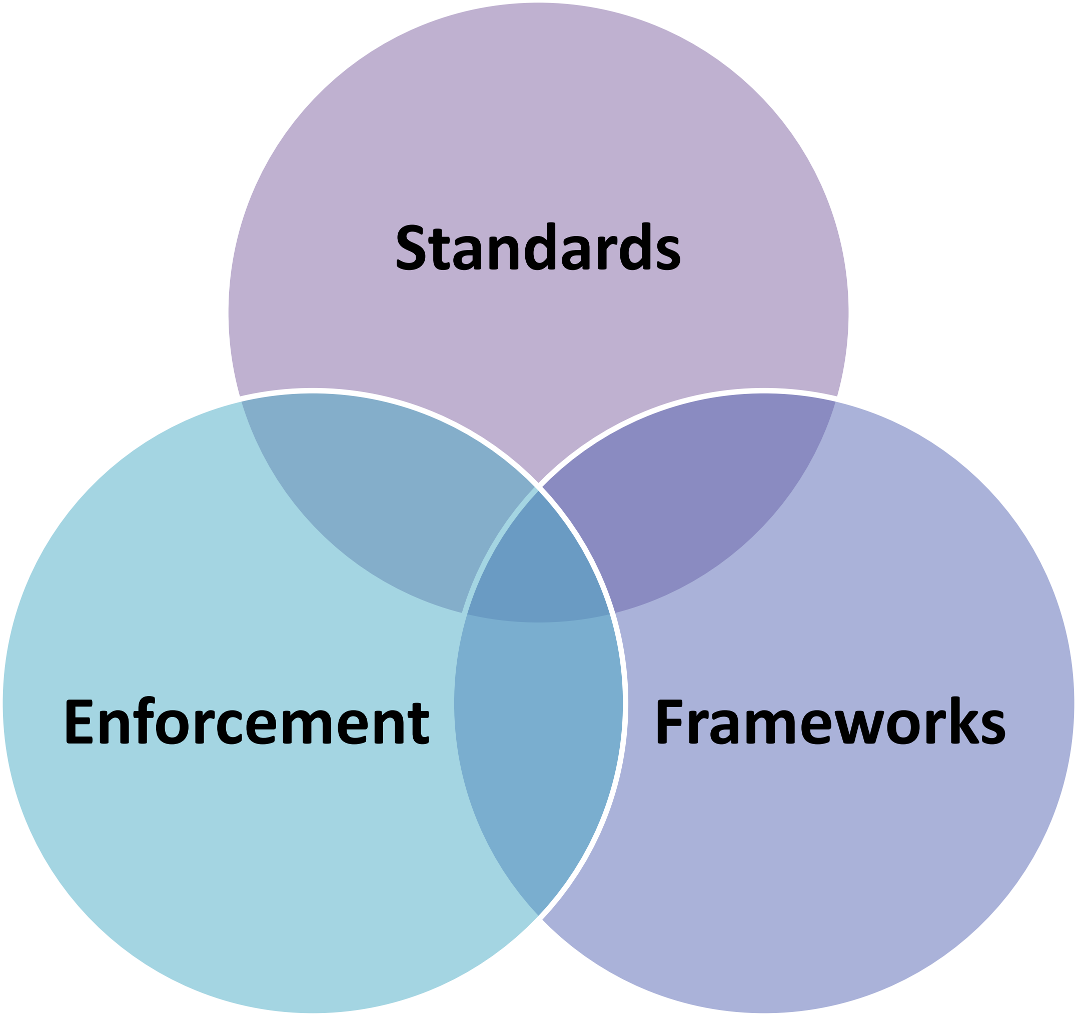
We need to prevent a race to the bottom

- Many IOT vendors – who want to do the right thing – are expressing concerns that the market won't

- Economics at play may disincentivize "good" security behavior if there is no forcing function
  - If building in security adds 10% to the cost, will anyone buy it?

Amidst concern that laws or regulations would be too heavy handed – and stifle innovation – what can government do?

What government can do



VENABLE

Questions?

Jeremy Grant

Managing Director, Technology Business Strategy

jeremy.grant@Venable.com