RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

#RSAC

SESSION ID: IDY-W14

Identity and Access Management of Things

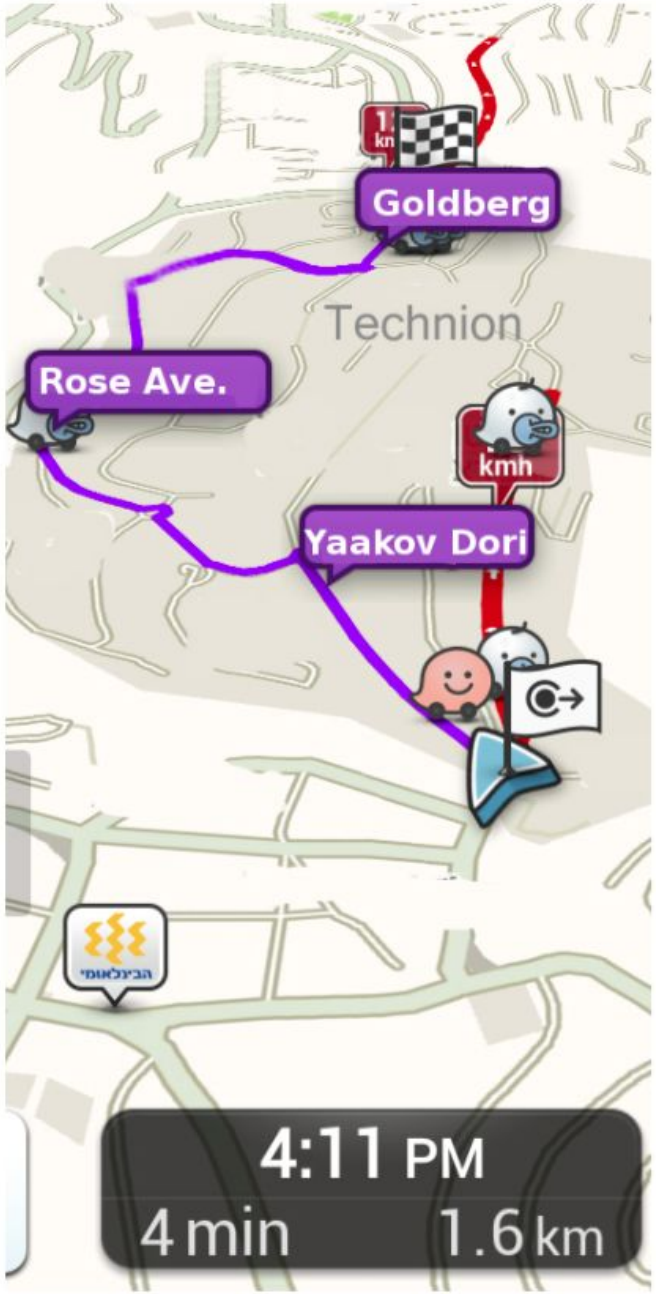
Ping Identity

Robert Brown

IoT consultant

1969

(a) Pre-attack route



(b) Post-attack route

2014

The IoTalian Job

“The plan is simple; we’ll gridlock Turin with a Waze hack, steal the gold and escape in three off-grid vintage Minis”.

- *Charlie Croker*

Content of this presentation

Defining Internet Things

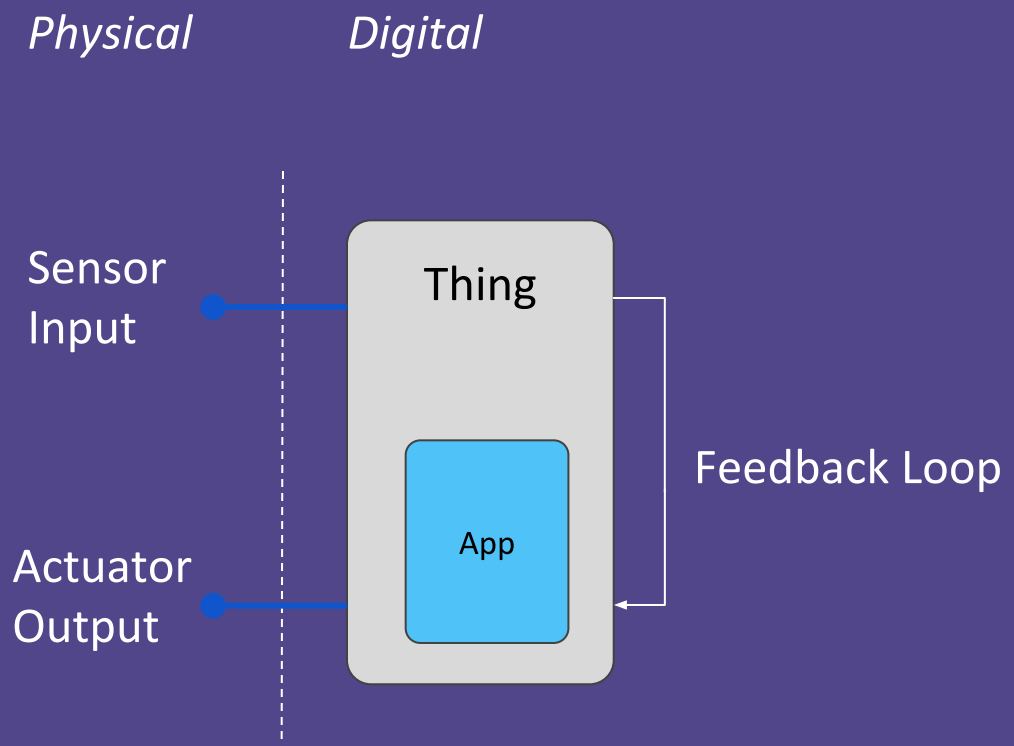
Chip-to-Cloud Layers

What we have learned so far

Identity and Access Management of Things

What you can do next

Simple Things



Outputs are a function of inputs

Thing processor executes a control app

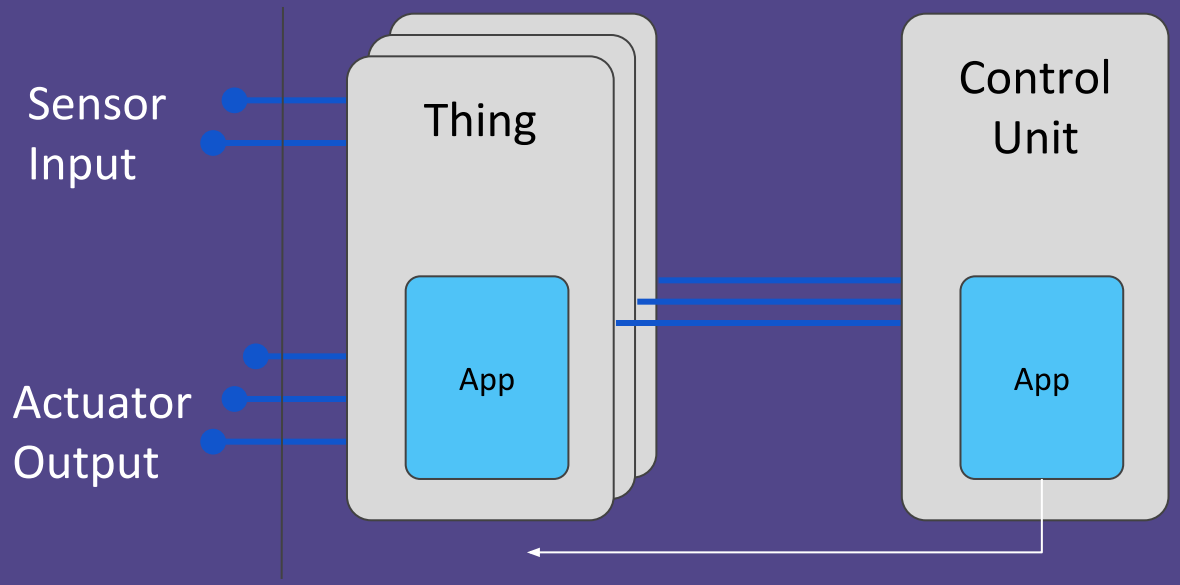
Things work in isolation

Anti Lock Brakes

Speed Sensor

Brake Force Modulator

Locally Networked Things



Outputs a function of many inputs

Centralized control app creates greater utility

Things implicitly trust central control

Parking Assist

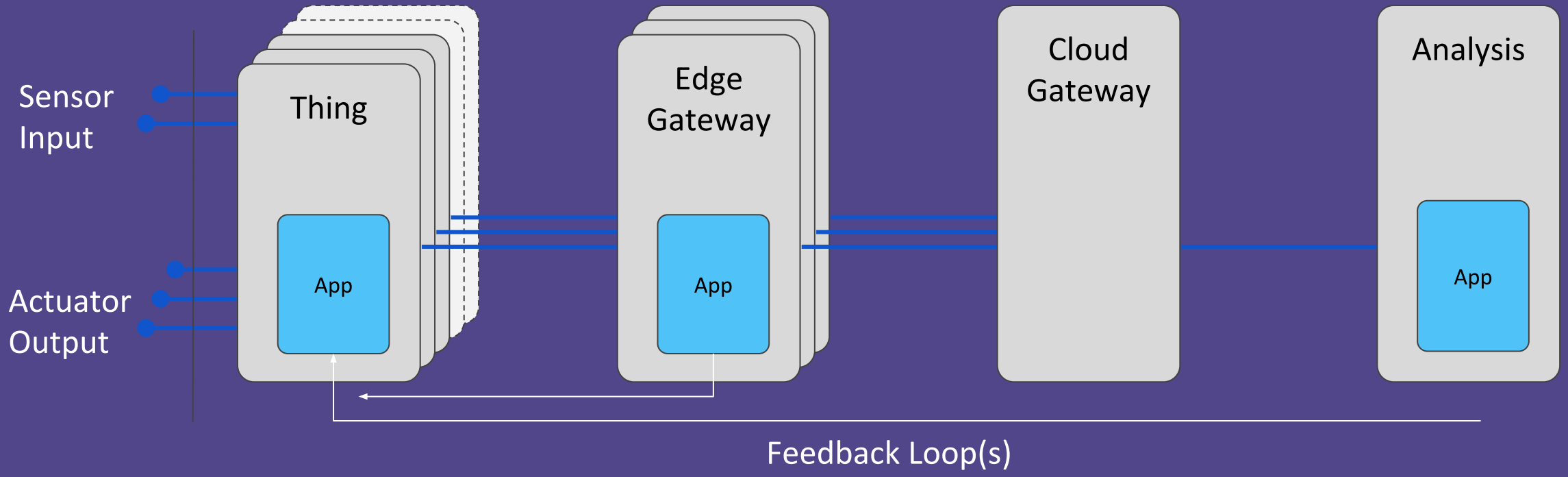
Cameras
Proximity sensors

Brakes
Accelerator
Steering

Internet Things

Inputs from external sources affect outputs

Local controllers optimized by peer performance

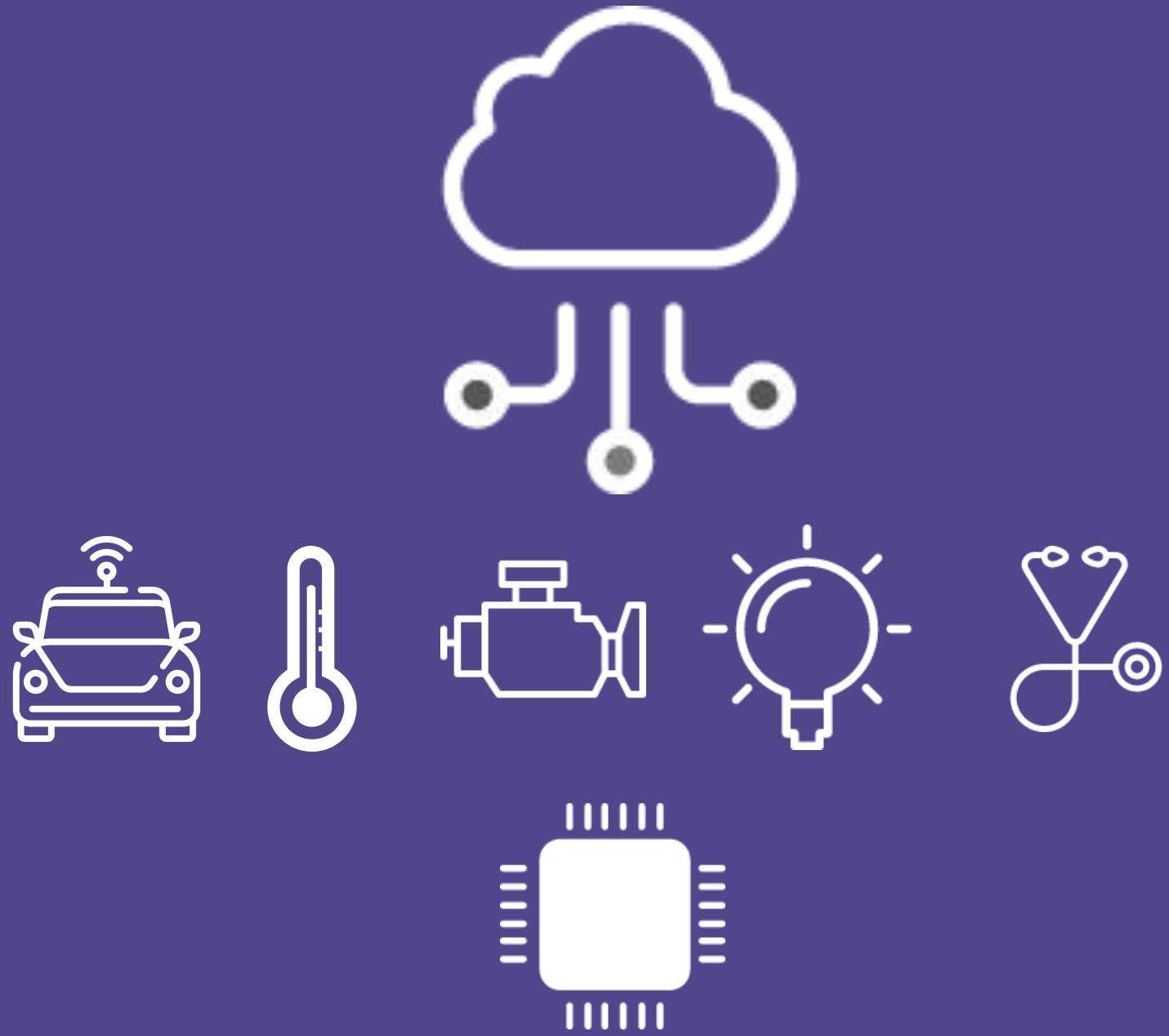


Fully Autonomous Vehicles

Cameras
Lidar
Radar
Proximity sensors
Traffic sensors
GPS
Gyroscope
Accelerometers
Temperature
Tyre pressure/wear
Weather forecast
Infrastructure alerts
Traffic history
Insurance
Destination
Passenger preferences
Passenger credit score
Driver intent (manual override)
....

Brakes
Accelerator
Steering
Lights
Turn signals
Horn
Wipers
Heating/Cooling
Door locks
...

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture



Business Intelligence
Rules / Analytics
Device Management
Directory / Registry
AuthN & AuthZ
Cloud Gateway
Edge Gateway
Thing Identity
Code Protection
Operating System
Comms Module
Embedded Firmware
Silicon Chip
Security Blocks
Processor Architecture

Business Intelligence

Cut costs
Create value

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Rules / Analytics

Find information in data then act

Business Intelligence	**Device Management**
Rules / Analytics	
Device Management	**Maintain Things**
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	
Security Blocks	
Processor Architecture	

- Business Intelligence
- Rules / Analytics
- Device Management
- **Directory / Registry**
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Directory / Registry

Enrol Authorized Users & Things

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- **AuthN & AuthZ**
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Authentication & Authorization

Set and Enforce Policy

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- **Cloud Gateway**
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Cloud Gateway

Ingest data from known sources

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- **Edge Gateway**
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Edge Gateway

Connect Local Things

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- **Thing Identity**
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Thing Identity

Secure Thing to Cloud Relationship

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- **Code Protection**
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Code Protection

Protect Application Secrets & Integrity


Business Intelligence
Rules / Analytics
Device Management
Directory / Registry
AuthN & AuthZ
Cloud Gateway
Edge Gateway
Thing Identity
Code Protection
Operating System
Comms Module
Embedded Firmware
Silicon Chip
Security Blocks
Processor Architecture
Operating System
Privilege Separation

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- **Comms Module**
- Embedded Firmware
- Silicon Chip
- Security Blocks
- Processor Architecture

Comms Module

Secure Communication

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- **Embedded Firmware**
- Silicon Chip
- Security Blocks
- Processor Architecture

Embedded Firmware

Secure Boot
Runtime Integrity

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- **Silicon Chip**
- Security Blocks
- Processor Architecture

Silicon Chip

Resist Tampering

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- **Security Blocks**
- Processor Architecture

Security Blocks

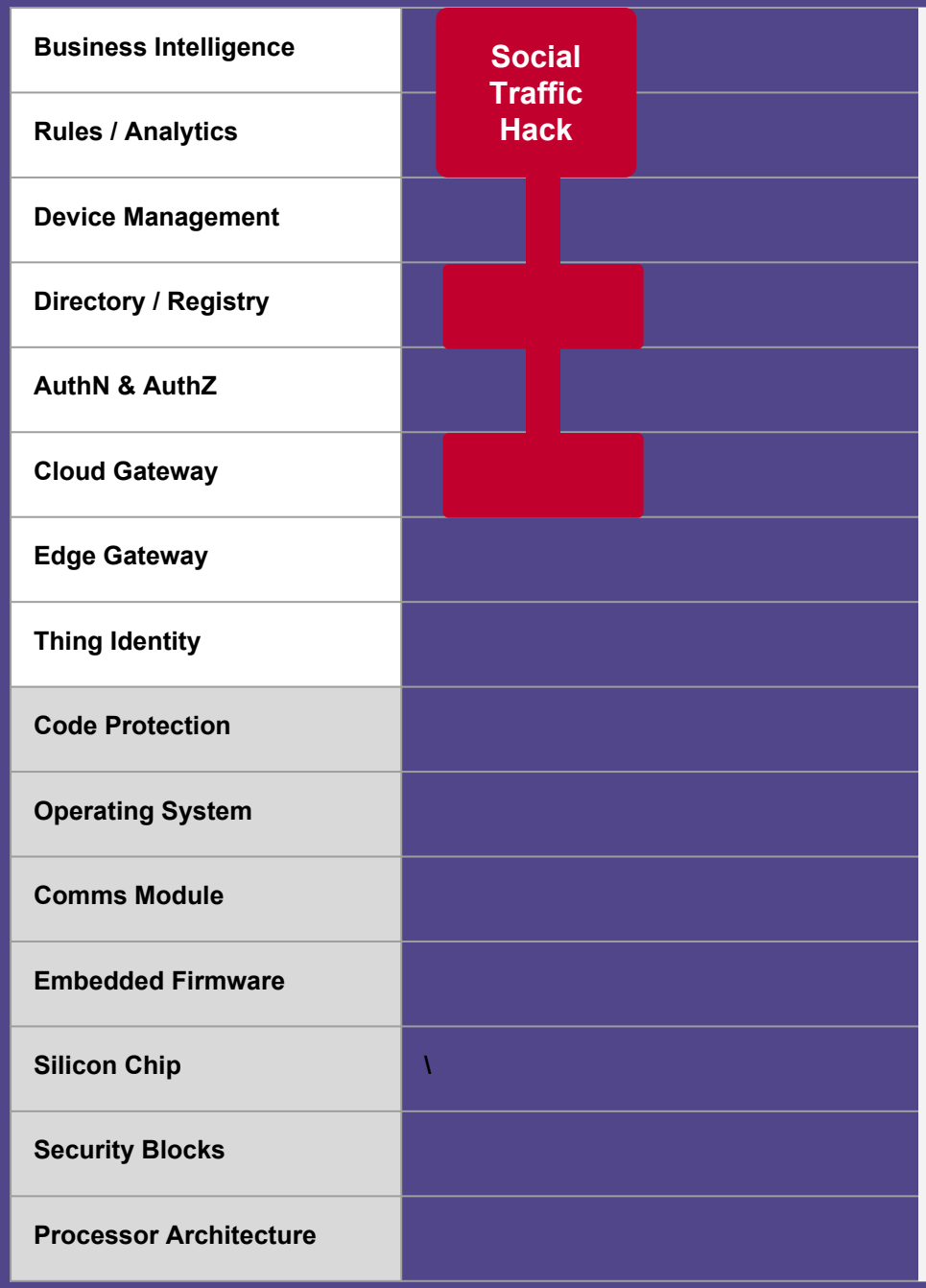
Embedded Cryptography

- Business Intelligence
- Rules / Analytics
- Device Management
- Directory / Registry
- AuthN & AuthZ
- Cloud Gateway
- Edge Gateway
- Thing Identity
- Code Protection
- Operating System
- Comms Module
- Embedded Firmware
- Silicon Chip
- Security Blocks
- **Processor Architecture**

Processor Architecture

Isolate Sensitive Assets

Where has IoT gone wrong?



No validation of user email

No MNO identity validation

No social login via Facebook

No checks that devices were real

No checks on network interfaces carrying data

No way to know GPS data came from a real sensor

Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	\
Security Blocks	
Processor Architecture	

Thermostat

No user authorization for updates

Nest Thermostat Glitch Leaves Users in the Cold

Disruptions
By NICK BILTON JAN. 13, 2016

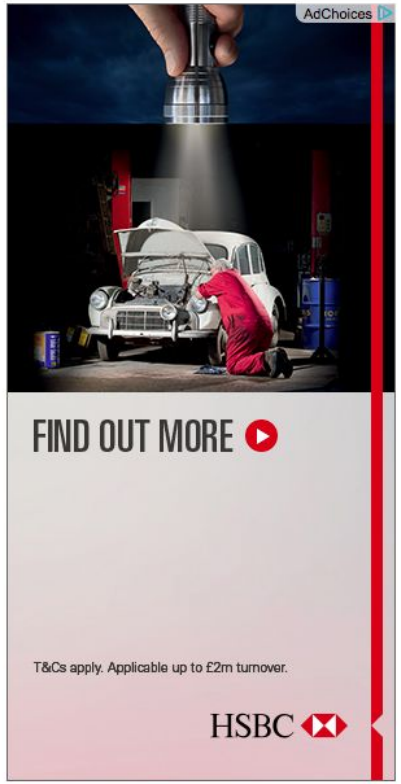
Photo illustration by Jim DeMaria/The New York Times and photo by Ben Margot/Associated Press.

The Nest Learning Thermostat is dead to me, literally. Last week, my once-beloved "smart" thermostat suffered from a mysterious software bug that drained its battery and sent our home into a chill in the middle of the night.

Although I had set the thermostat to 70 degrees overnight, my wife and I were woken by a crying baby at 4 a.m. The thermometer in his room read 64 degrees, and the Nest was off.

This didn't happen to just me. The problems with the much-hyped thermostat, which allows users to monitor and adjust their thermostats on their smartphones (Google purchased Nest Labs for $3.2 billion in 2014), affected an untold number of customers when the device went haywire across America.

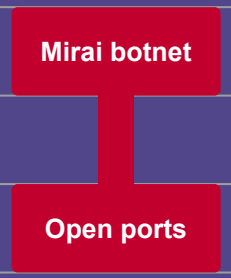
Users vented on the company's online forums and on social media. The glitch also coincided with plunging temperatures throughout much of the country.



Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	Stranded Driver
Thing Identity	
Code Protection	
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	\
Security Blocks	
Processor Architecture	

No resilience when cloud unavailable

Business Intelligence
Rules / Analytics
Device Management
Directory / Registry
AuthN & AuthZ
Cloud Gateway
Edge Gateway
Thing Identity
Code Protection
Operating System
Comms Module
Embedded Firmware
Silicon Chip
Security Blocks
Processor Architecture



\

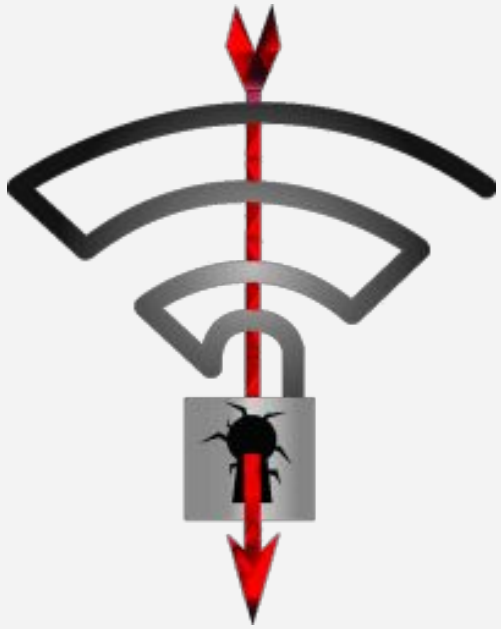
USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
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	fucker
guest	12345		
guest	12345		

Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	ZLL shared signing key
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	\
Security Blocks	
Processor Architecture	

Shared master signing key leaked in 2015

Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	
Operating System	
Comms Module	KRACK
Embedded Firmware	
Silicon Chip	\
Security Blocks	
Processor Architecture	

WPA2 protocol flaw



Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	\
Security Blocks	Debug
Processor Architecture	

HACKADAY

HOME BLOG HACKADAY.IO STORE HACKADAY PRIZE SUBMIT ABOUT

ECHO

THE AMAZON ECHO AS A LISTENING DEVICE

August 3, 2017 by Jenny List

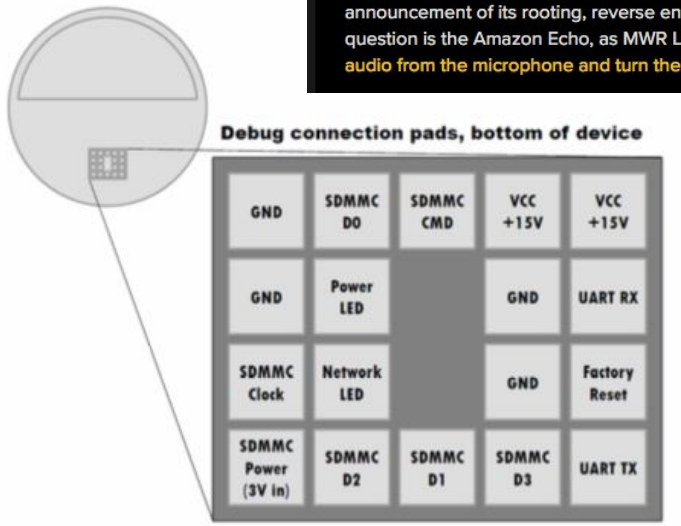
30 Comments

It is an inevitability that following swiftly on the heels of the release of a new device there will be an announcement of its rooting, reverse engineering, or other revealing of its hackability. Now the device in question is the Amazon Echo, as MWR Labs announce their work in persuading an Echo to yield the live audio from the microphone and turn the voice assistant device into a covert listening device.

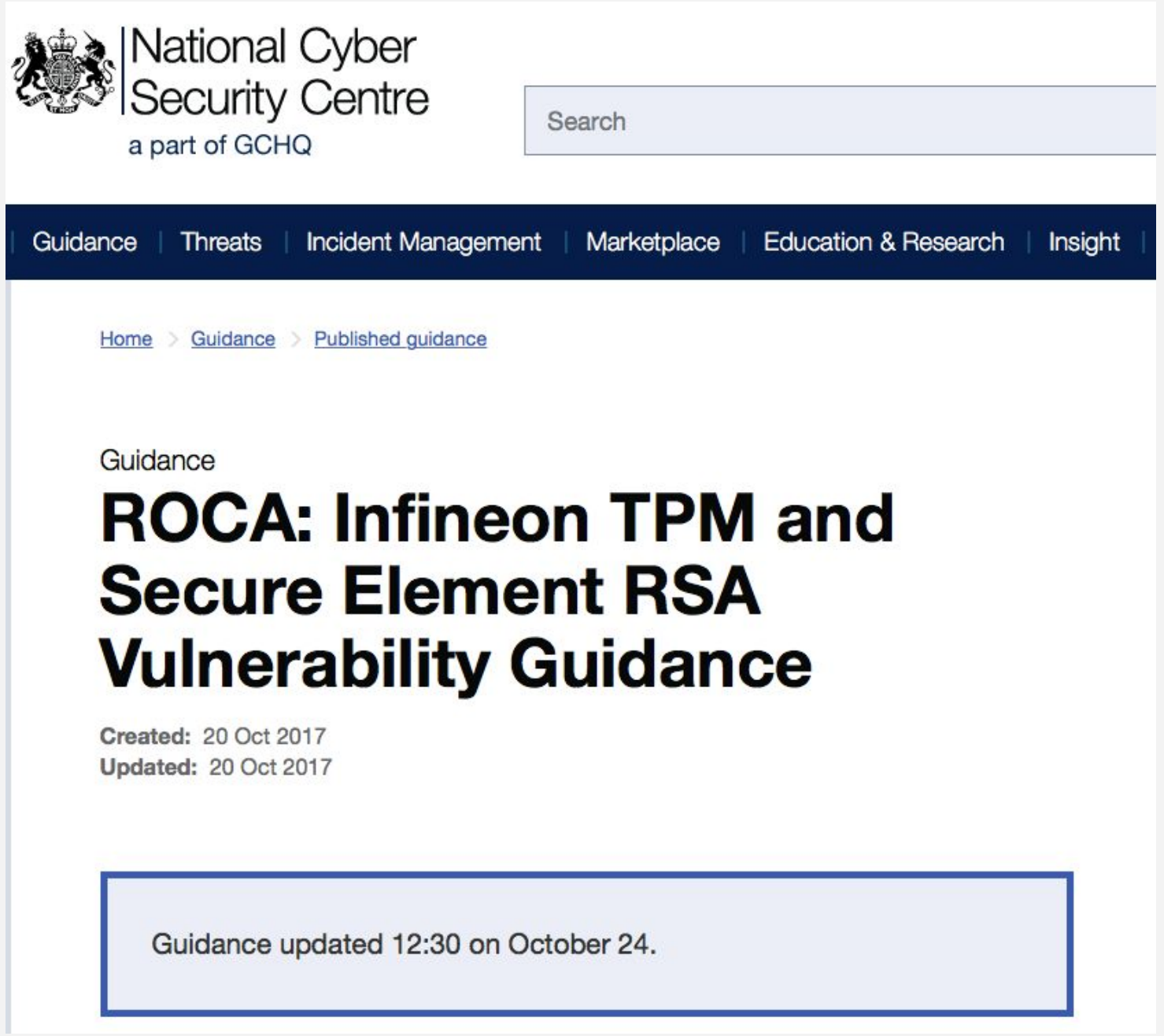
1 Million

Make t sourci

Data Scie of compa sourcing



Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	\ ROCA
Security Blocks	
Processor Architecture	



National Cyber Security Centre
a part of GCHQ

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight

Home > Guidance > Published guidance

Guidance

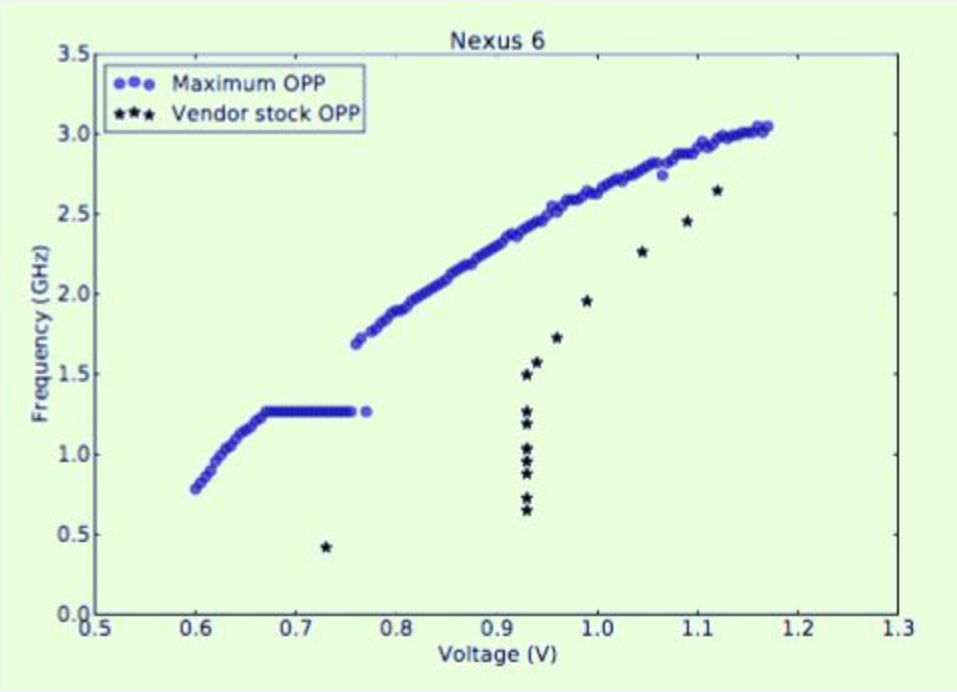
ROCA: Infineon TPM and Secure Element RSA Vulnerability Guidance

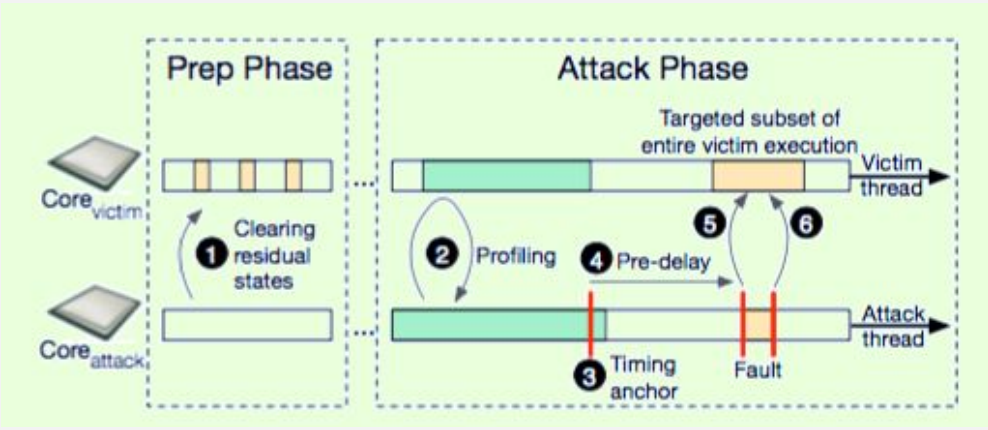
Created: 20 Oct 2017
Updated: 20 Oct 2017

Guidance updated 12:30 on October 24.

Business Intelligence	
Rules / Analytics	
Device Management	
Directory / Registry	
AuthN & AuthZ	
Cloud Gateway	
Edge Gateway	
Thing Identity	
Code Protection	
Operating System	
Comms Module	
Embedded Firmware	
Silicon Chip	\
Security Blocks	
Processor Architecture	CLKSCREW, SPECTRE

Side channel analysis or fault injection





secure

"Things are only ~~impossible~~ until they are not"

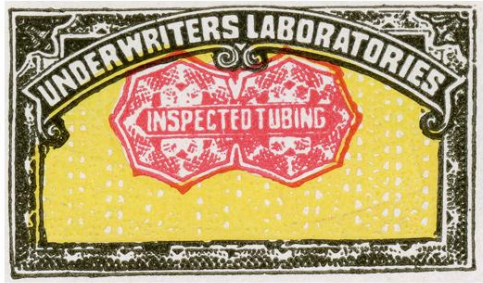
IMPROVED
INVIOLABLE
LOCK

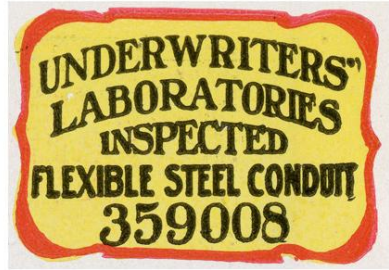
Safety = Safety(*Security*)


PHOENIX®
MARINE TYPE ELECTRIC FIXTURE
OUTSIDE TYPE (SALT WATER)
ALSO LISTED AS
H.I.D. FIXTURE
SUITABLE FOR WET LOCATIONS
MARINE
UL
LISTED
19M5
MODEL MS-120-1500LB
MAXIMUM
1500 WATTS
600 VOLTS
CAUTION: RISK OF FIRE USE E-25 OR BT56 LAMP WITH SUITABLE BALLAST: HIGH PRESSURE SODIUM 1000 WATT (S52), METAL HALIDE 1000 WATT (M47) OR 1500 WATT (M48)
PHOENIX PRODUCTS CO., INC. MILWAUKEE, WI. 53218 U.S.A.

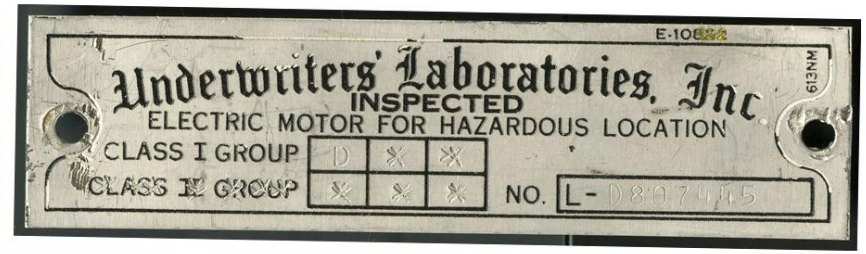

UNDERWRITERS LABORATORIES
INSPECTED SNAP SWITCH

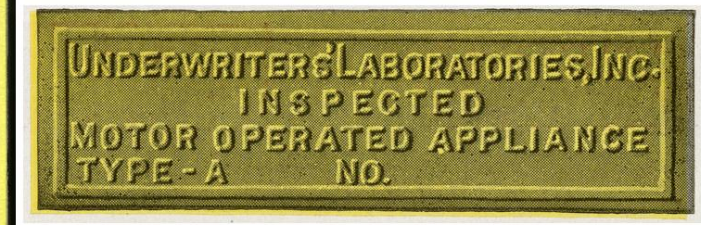

UNDERWRITERS' LABORATORIES, INC.
INSPECTED
12
INSULATING JOINT
12
Nº

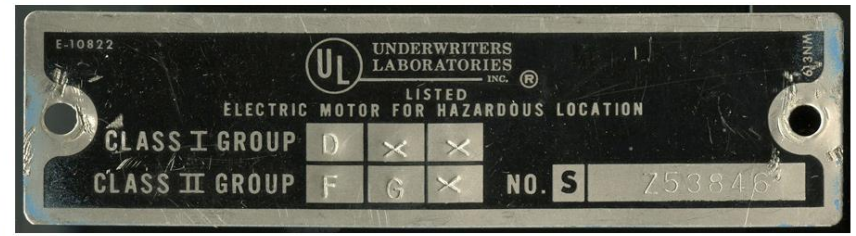

UNDERWRITERS LABORATORIES
INSPECTED TUBING


UNDERWRITERS'
LABORATORIES
INSPECTED
FLEXIBLE STEEL CONDUIT
359008


UNDERWRITERS
LABORATORIES
INC.®
CLASSIFIED
SWINGING TYPE
FIRE DOOR Nº.
B293624
FIRE
RATING:
3 HOUR (A)
MINIMUM
LATCH THROW
SINGLE 1/2"
PAIRS 5/8"
Steelcraft®
CINCINNATI, OHIO
31282


E-10824
Underwriters' Laboratories, Inc.
INSPECTED
ELECTRIC MOTOR FOR HAZARDOUS LOCATION
CLASS I GROUP D
CLASS II GROUP
NO. L-D807045
613NM


UNDERWRITERS' LABORATORIES, INC.
INSPECTED
MOTOR OPERATED APPLIANCE
TYPE-A NO.


E-10822
UL
UNDERWRITERS LABORATORIES INC.®
LISTED
ELECTRIC MOTOR FOR HAZARDOUS LOCATION
CLASS I GROUP D
CLASS II GROUP F G
NO. S Z53846
613NM

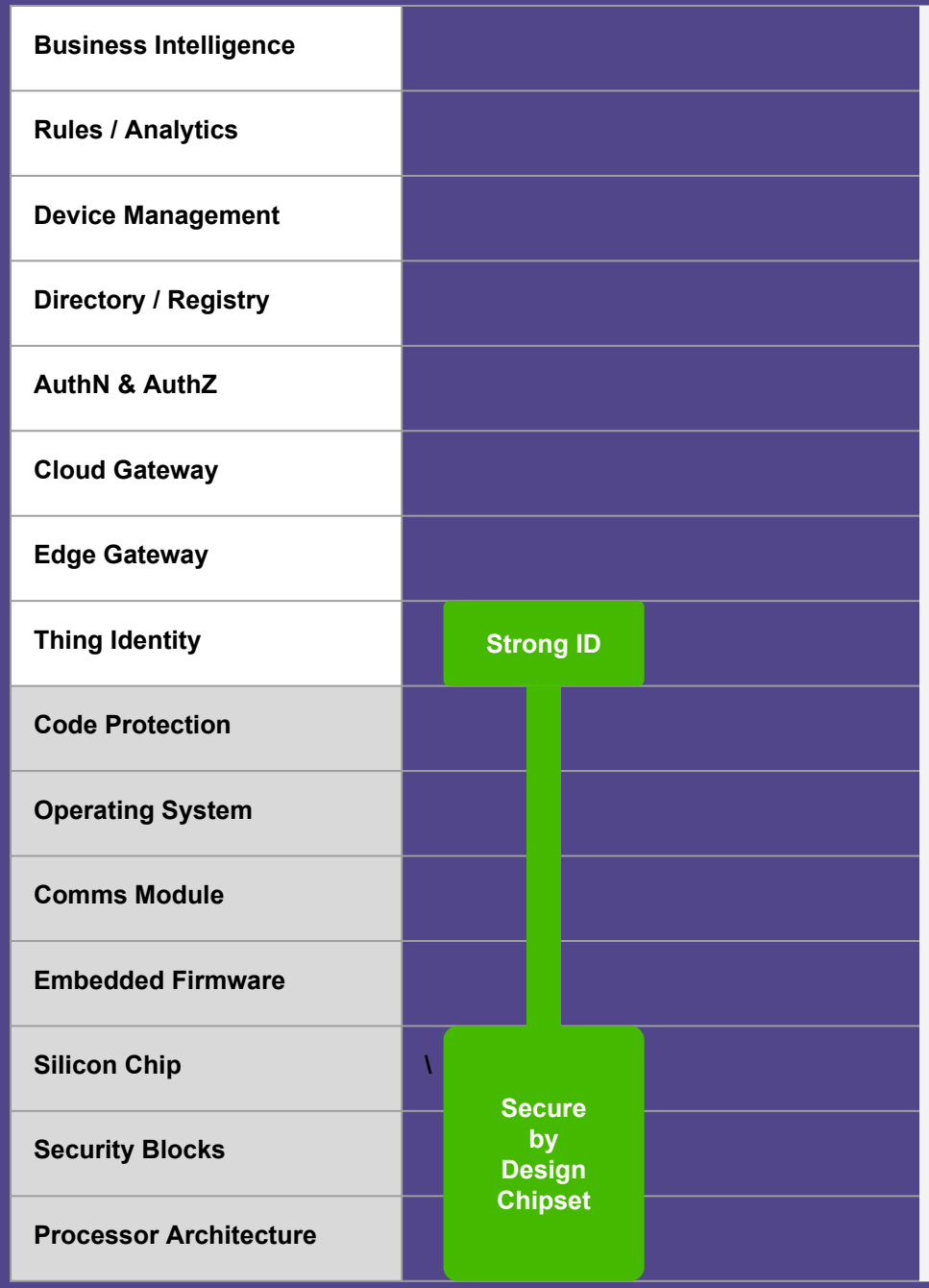

UNDERWRITERS' LABORATORIES
INSPECTED INSULATING JOINT

15 CIRCLES OF HELL

James Bridle - Autonomous Trap 001

It’s a matter of time

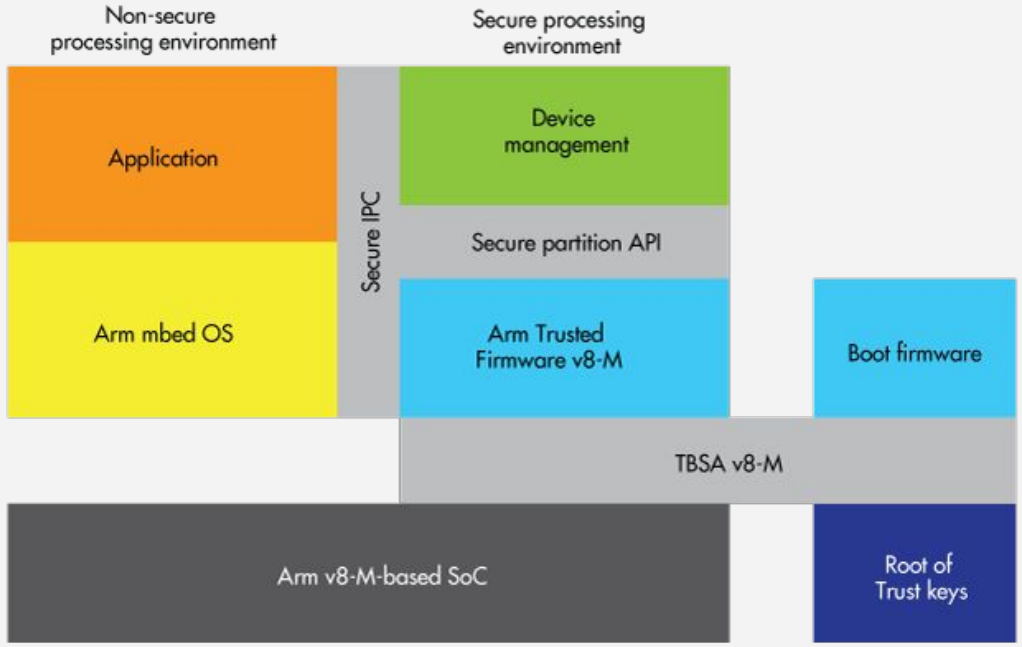
Identity & Access Management
How can it help IoT?

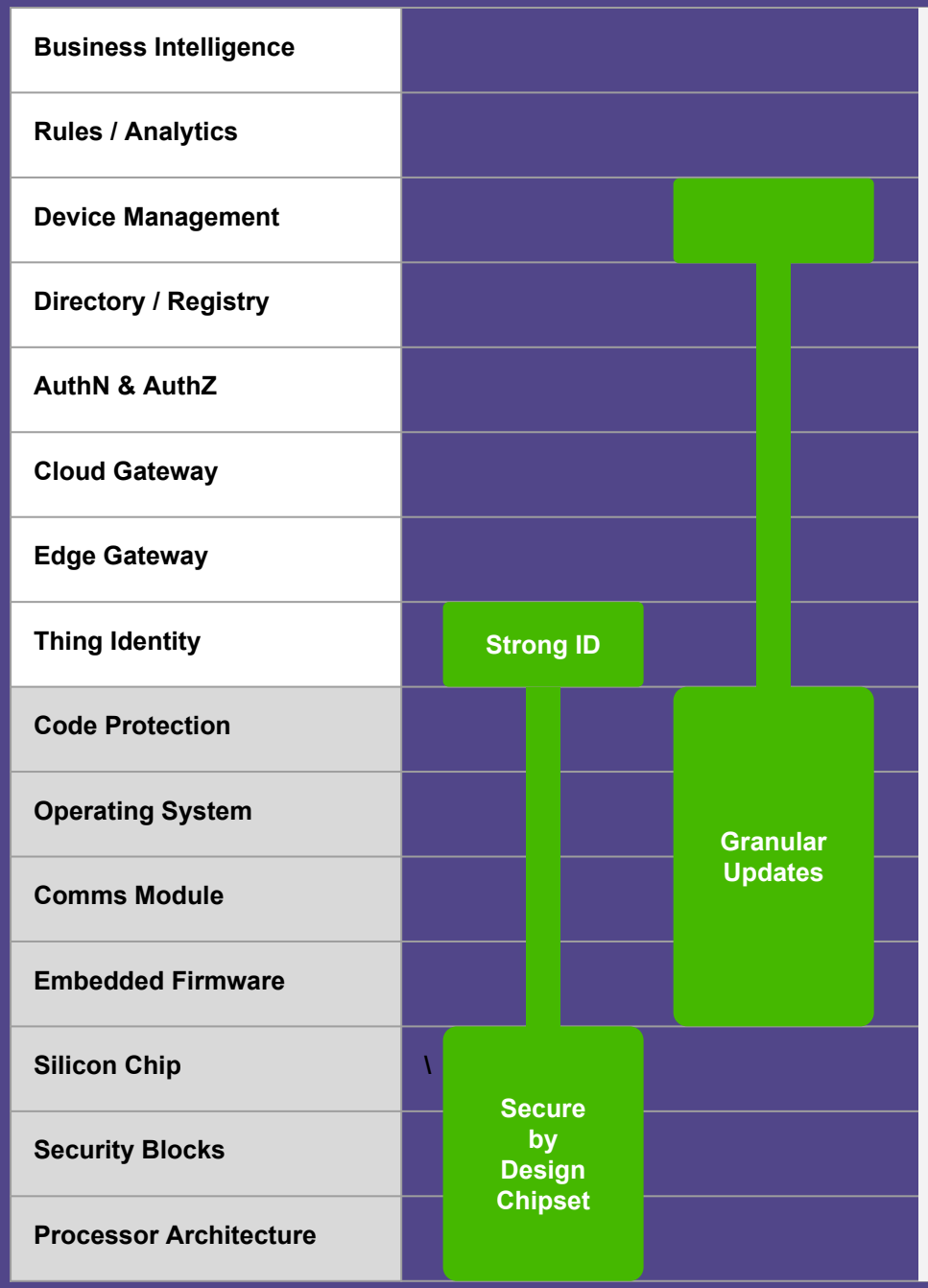


A Strong Start

Unique private key(s) per device
Chipsets that can protect root-of-trust identity
Attestation capability

Examples:
TCG Device Identifier Composition Engine (DICE)
ARM Platform Security Architecture (PSA)





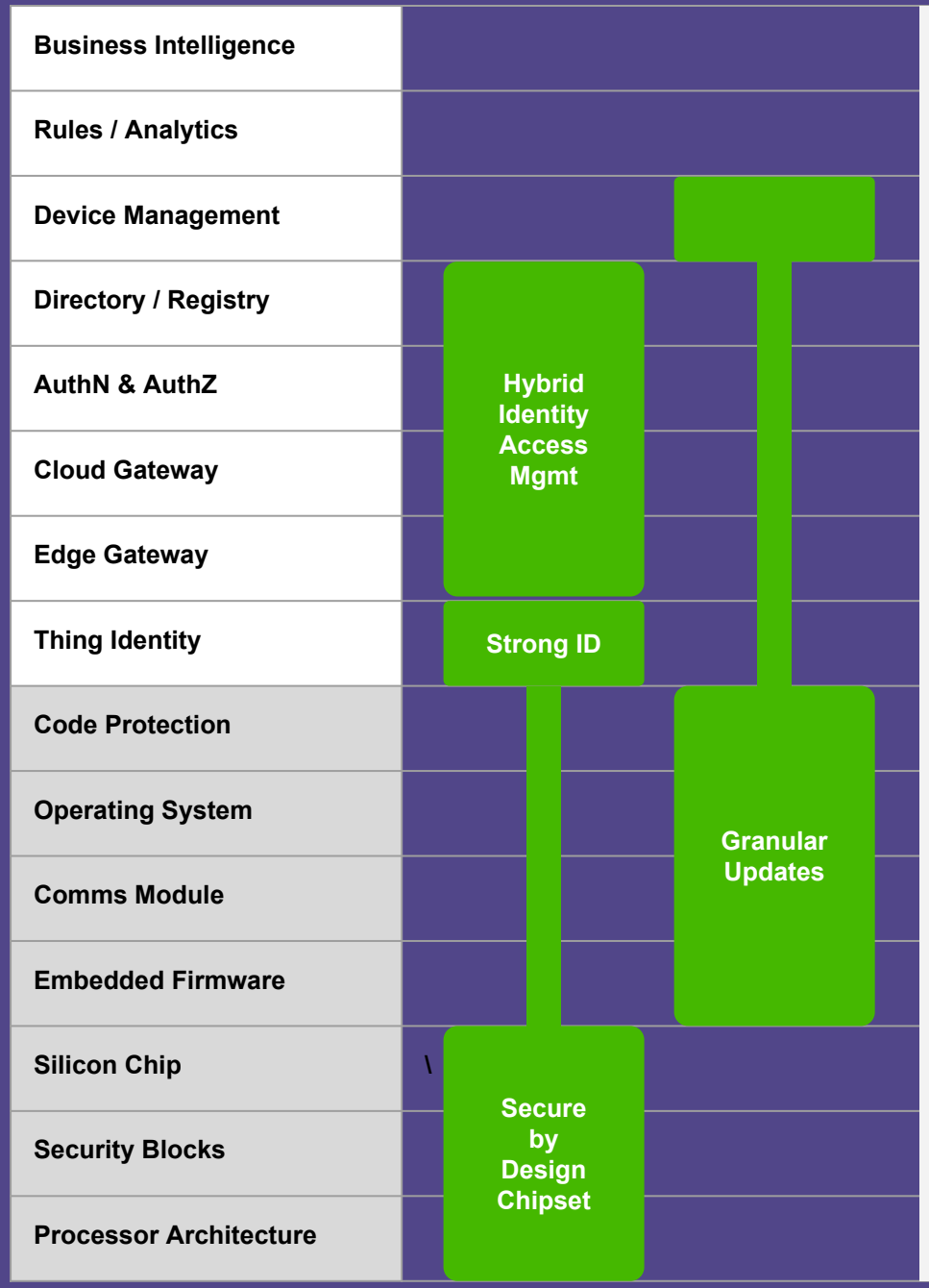
Maintain Trust

Identify provenance of software components

Secure and granular update capability

Apply least privilege principles

Remove unauthenticated/unauthorized ports



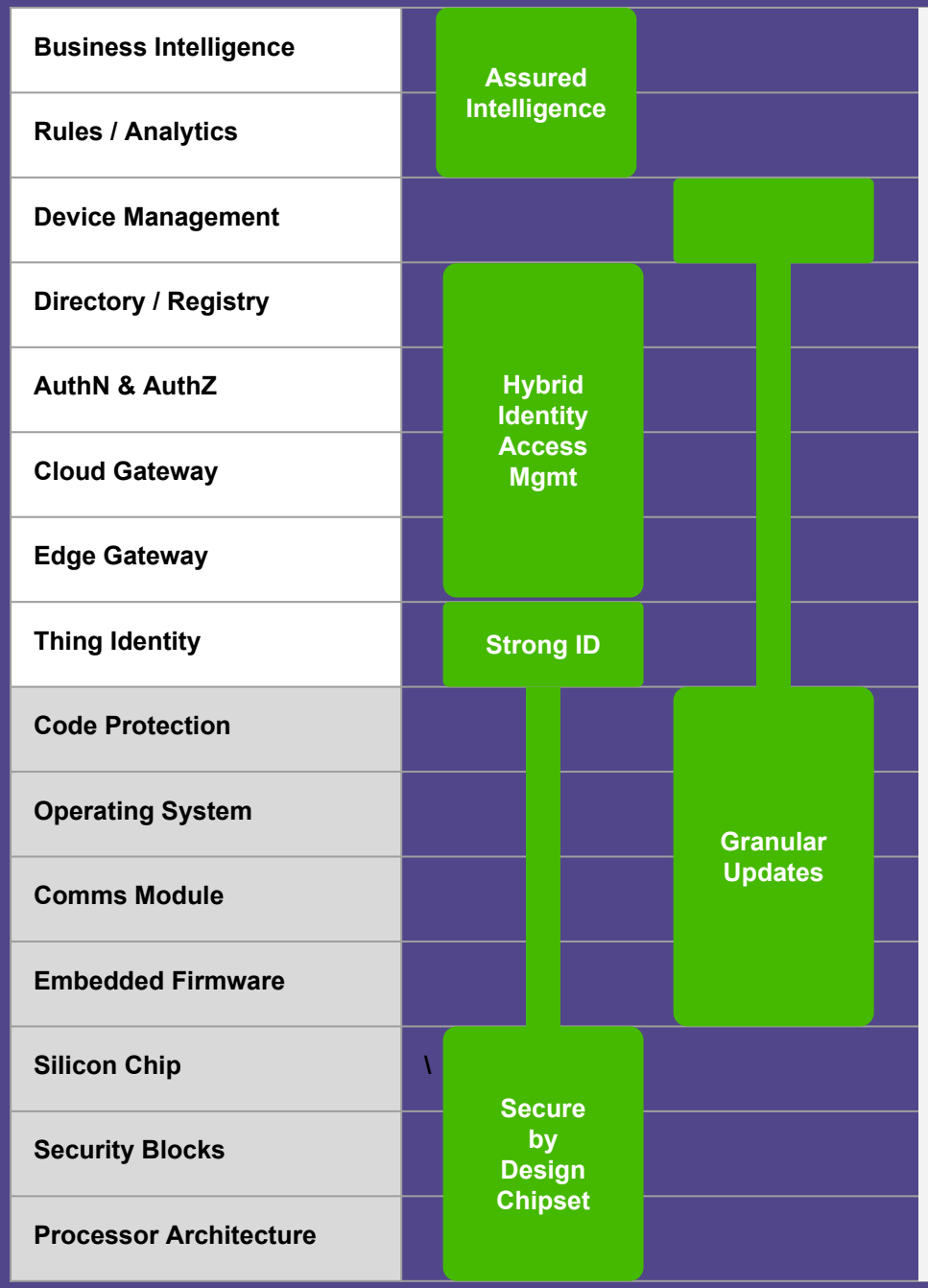
Know Your Things

IAM on edge for operational resilience

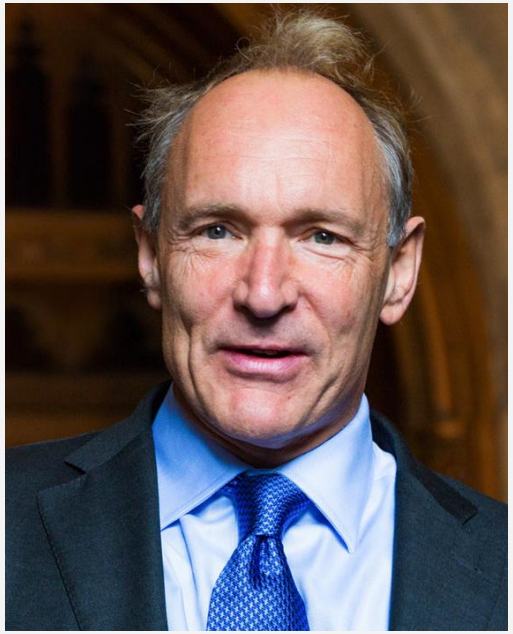
IAM on-premises

IAM for multi-cloud IoT platforms (Hybrid Agility)

Connect Users and Things with IAM



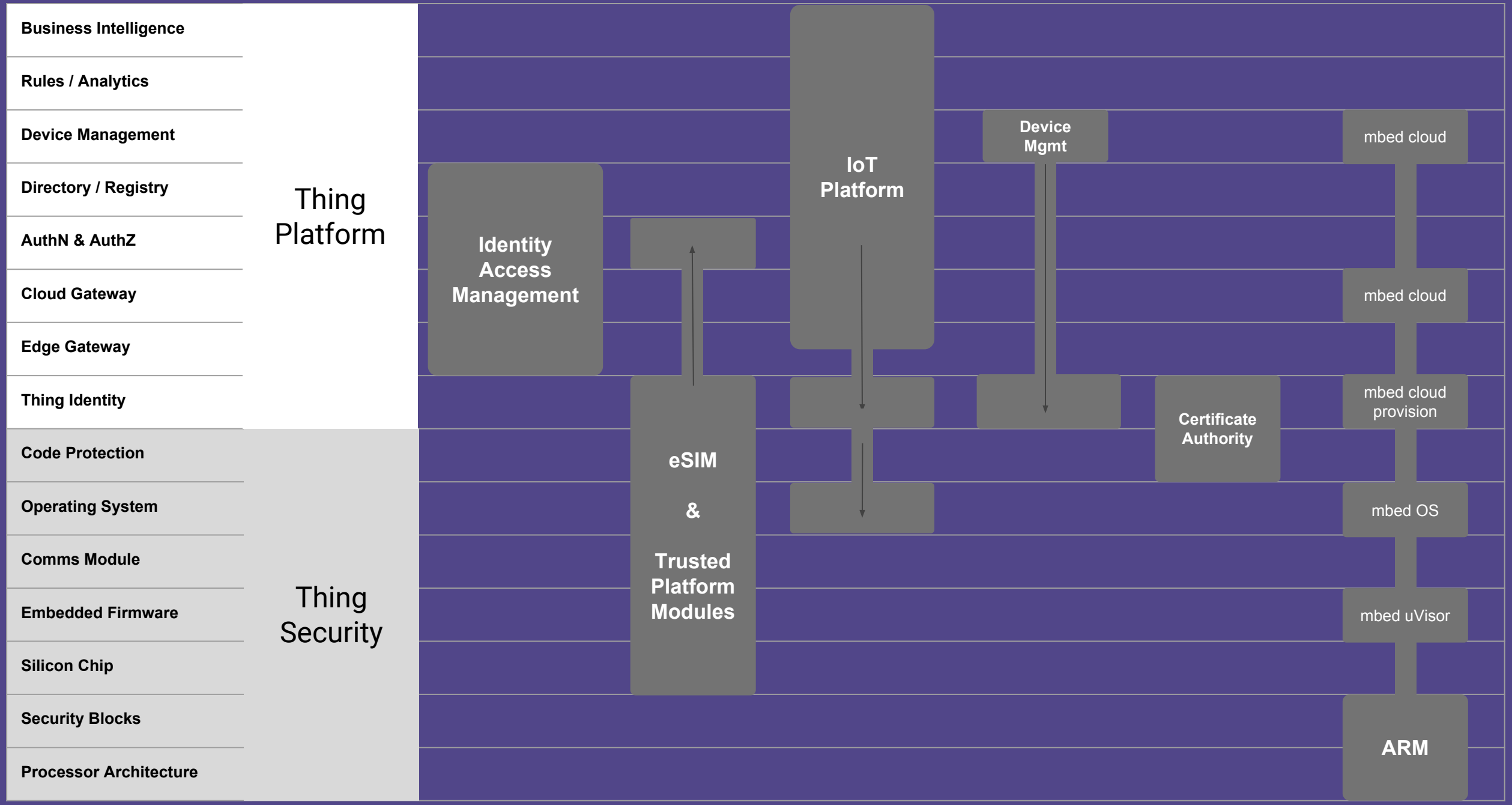
CLEAN DATA



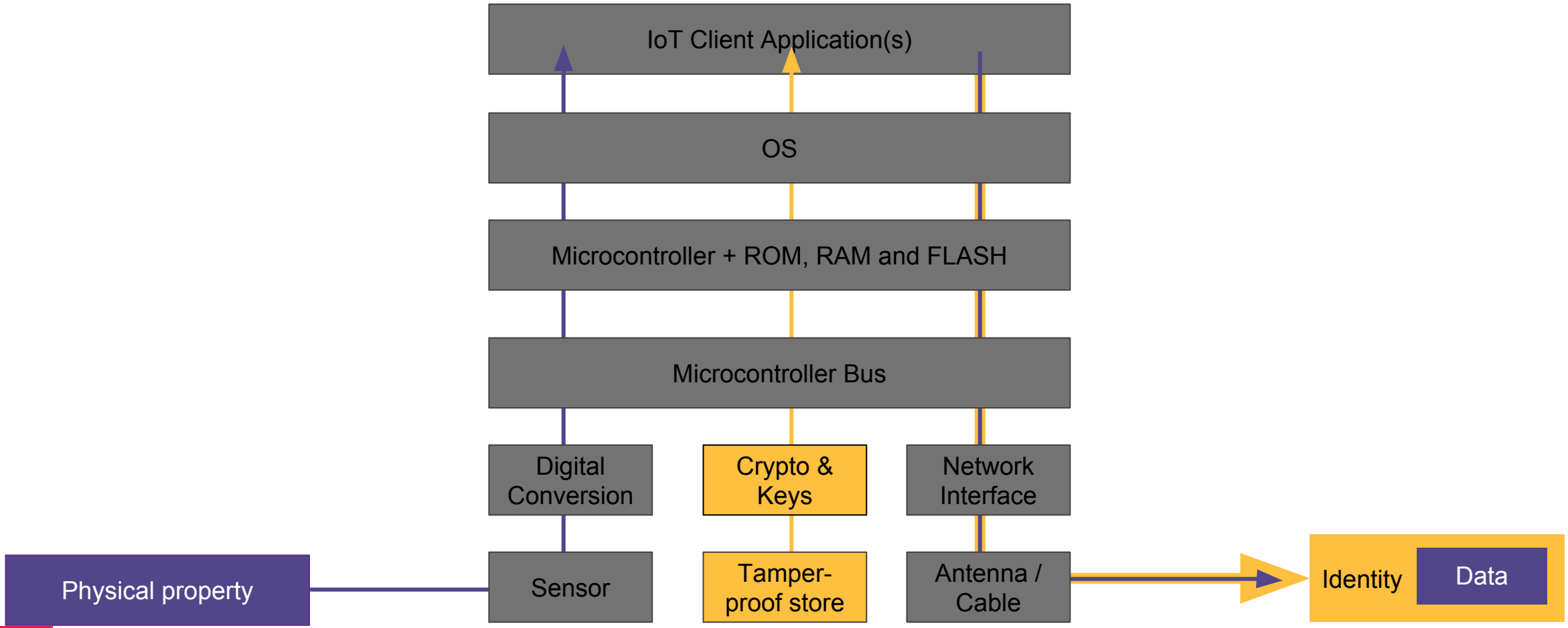
1 November 2016 - Tim Berners-Lee in *the Guardian* on Open Data Institute

Clean data will:

"restore [...] a democratic system based on knowledge, based on facts and truth"


Business Intelligence
Rules / Analytics
Device Management
Directory / Registry
AuthN & AuthZ
Cloud Gateway
Edge Gateway
Thing Identity
Thing Platform
Code Protection
Operating System
Comms Module
Embedded Firmware
Silicon Chip
Security Blocks
Processor Architecture
Thing Security
Identity Access Management
IoT Platform
Device Mgmt
mbed cloud
mbed cloud
mbed cloud provision
Certificate Authority
eSIM & Trusted Platform Modules
mbed OS
mbed uVisor
ARM

How do your Things protect identity?



The secret life of Things

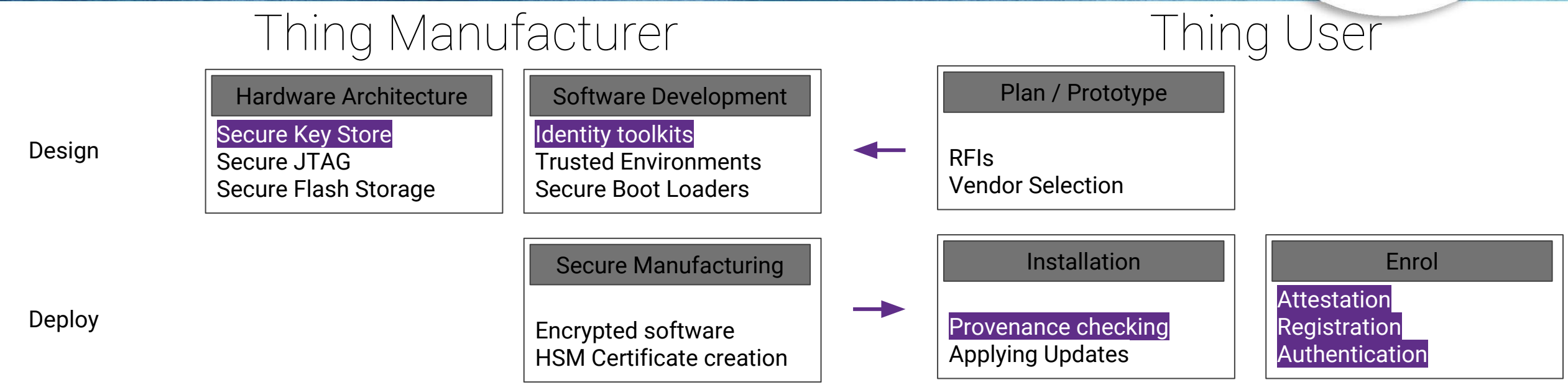
Thing Manufacturer

Thing User

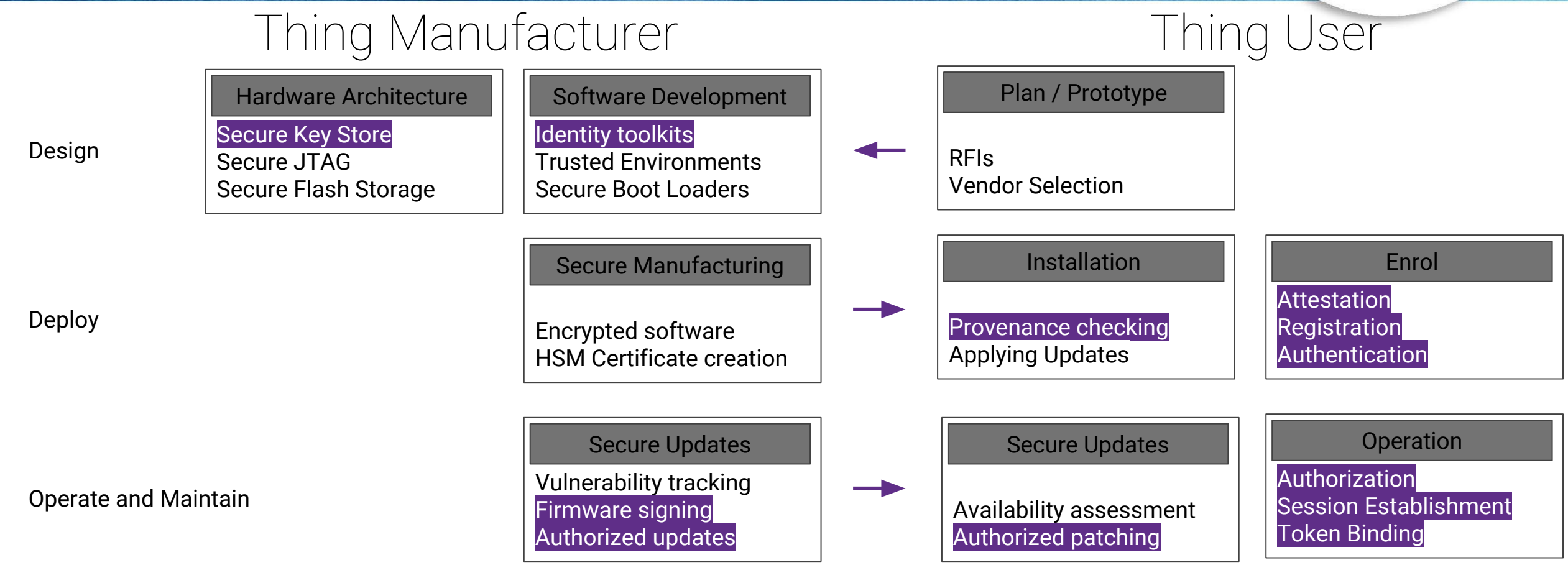
Design

Hardware Architecture	Software Development	Plan / Prototype
Secure Key Store	Identity toolkits	RFIs
Secure JTAG	Trusted Environments	Vendor Selection
Secure Flash Storage	Secure Boot Loaders	

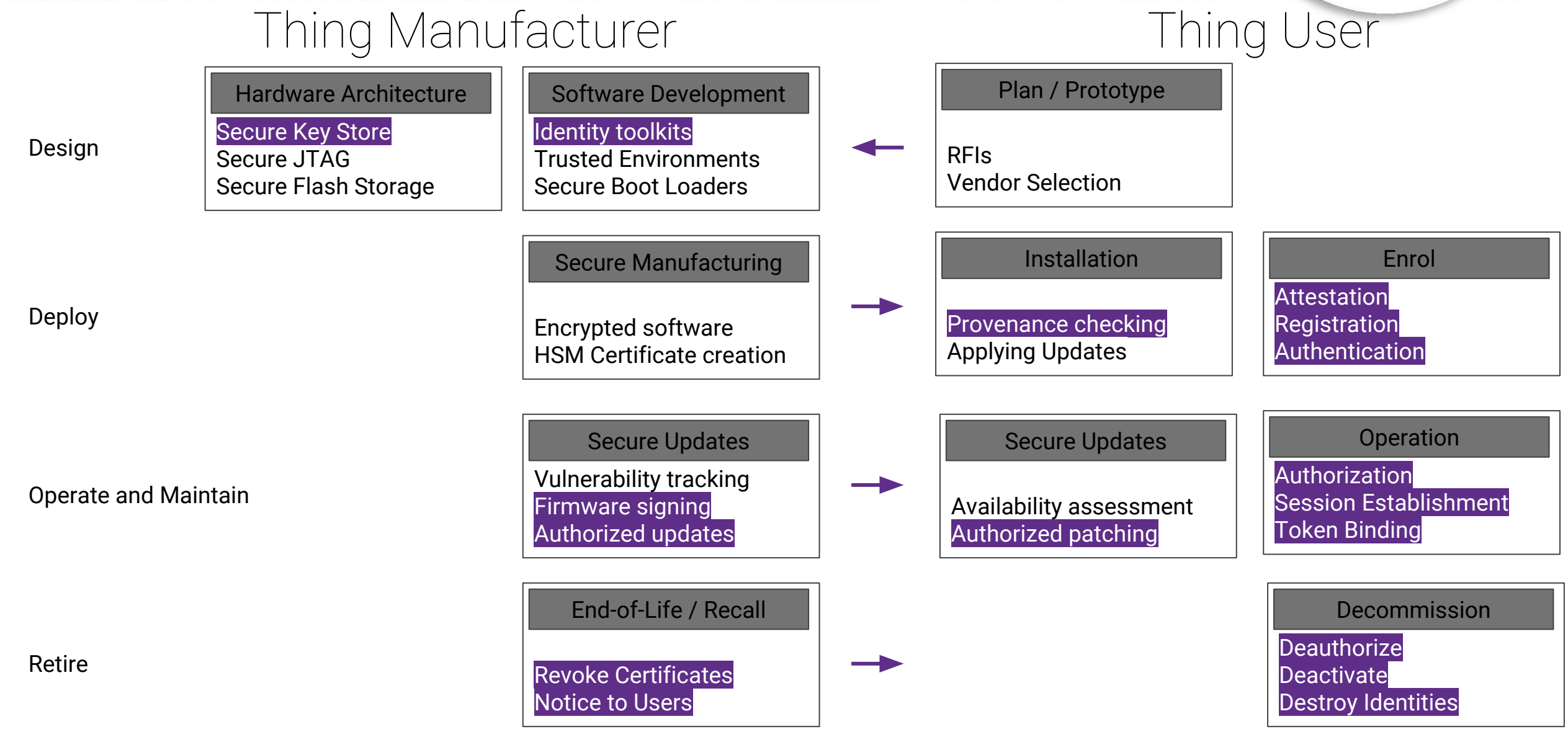
The secret life of Things



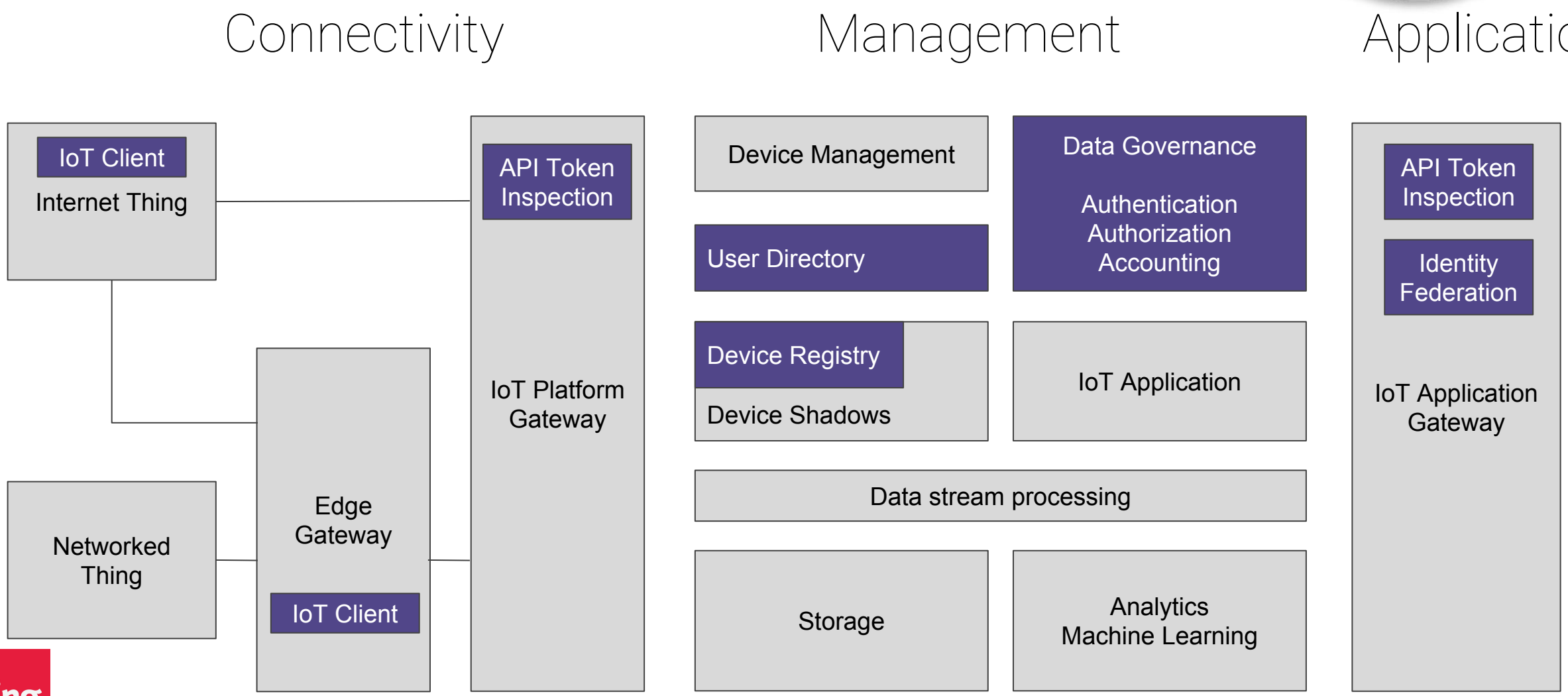
The secret life of Things



The secret life of Things



Identity in IoT Platforms



Identity Standards and Tools Available

Function	Standard or Technology
Key Protection in Things	Global Platform SE, TEE, RoT Trusted Computing Group TPM DICE Physically Unclonable Functions
Attestation	FIDO Meta Data Service Android 8 Hardware backed key attestation
Registry	LDAP, Graph Database, SQL, NoSQL, Dynamic Client Registration
Authentication	X.509 Certificates, OCSP stapling, CRLs FIDO Silent Authenticators
Session Security & Data Integrity	(D)TLS 1.3 session tokens, HMAC connectionless message integrity
Authorization	OAuth 2.0, Device Flow, ACE, Token Binding, Proof of Possession
Identity and Privacy	OpenID Connect, UMA

Proof of Possession

Proves that a private key is used.

Does not prove what possessed that key.

A clear need for Things to prove how they will keep possession of keys.

Internet of Things wants

YOU

What can you do?

- Today - Know your Things 20 minute survey
  - Start the conversation between IoT and IAM groups
  - surveymonkey.com/r/Ping-IAMoT
- 3 months - IAM and IoT cross-org collaboration
  - Identify Things, protocols, standards, platforms, data integrity, update mechanisms, registries and access controls
- 6 months - IAMoT requirements in RFIs
  - Form an IoT platform & IAM strategy

Summary

Hardware key attestation for Proof of Possession

Every Thing needs to keep secrets

Clean data through IAM will assure intelligent IoT

Thank you

Please connect at the Ping Identity booth South Expo #1021

linkedin.com/in/rob-atakama

surveymonkey.com/r/Ping-IAMoT