Brave New World of the Internet of Things

Bryn Lewis

devMobile Software Consultant, Christchurch

Advancing Expertise in Software Testing

Agenda

Introduction

Hype, Challenges, Numbers, Trustworthiness, Privacy, Security

Things

Where, Constrained, Security

Connectivity

Protocols, Transports, Security, Architecture

Securing Things

Broken, Hardware, Software, Connectivity, Services

Testing Things

Hardware, Firmware, Software, Connectivity, Security, Services, Scale

Questions

Introduction

- “Any sufficiently advanced technology is indistinguishable from magic”

  Arthur C Clarke

- “Computers think using etchings in poisoned sand and measure time using vibrating crystals so if you were looking for magic you found it”

  @ComputerFact

Hype

- Nest purchased Dropcam for $555M
- Google $3.2Billion purchase of Nest
- Currently 300K developers need, 4.5M by 2020
- 26B devices by 2020
- Economic impact of $4T to $11T by 2025
- 2015-4800 devices/min 2020–7900 devices/min
- $US20 billion M&A activity in 2016

Emerging Challenges of Things

Scale

Numbers of devices and users
Volumes of data and network traffic
50%-70% of data is never used

Pace of Innovations

Innovation pressure: analysis, command and control
Skill pressure: data science, new platforms

Environmental

Security & privacy threats
Diversity of devices and composite devices
Emerging standards
New competitors

Lots of things

1 Million clients

Device Identities management

Ingest data

X Gbyte/sec

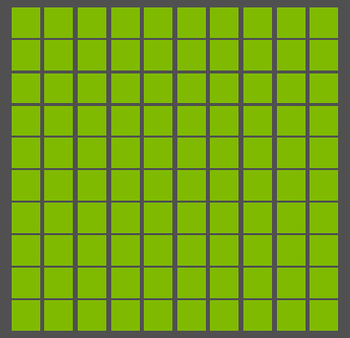
Real-time Analytics

1 million events /sec

Historic and Predictive Analytics

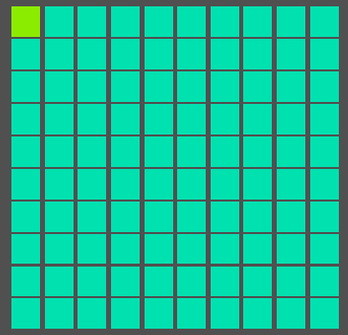
X PByte, batch processing

Makers.
Prototypes.
Hackathons.



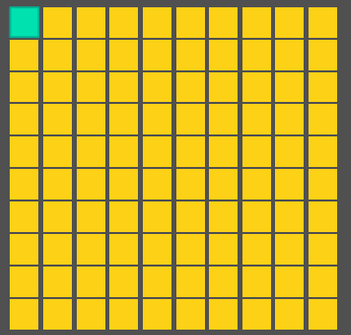
100

Enterprise
Scale



10,000

Consumer
Products



1,000,000

Trustworthy things

- Many IoT solutions control critical systems at the heart of our industrial and civil infrastructure.
- Digital security will be increasingly interwoven with physical safety of life and equipment.
- Many IoT solutions will provide very deep and near-real time insight into industrial and business processes, as well as into homes and the immediate personal environment.

People and things

- “Who is seeing my data?”
- “I see purposeful obfuscation and lack of transparency on the part of companies. Understanding is easier when a company is interested in telling me what they are doing with my data first, then interested in making a profit second.”
- At least half of consumers expressed extreme discomfort with the use and sale of their data in connected ‘real world’ environments.

Where are the Things

Personal

Smartphones, watches, glasses, fitness bands, medical implants

Domestic

Smart metering, burglar alarms, appliances, electric vehicle charging

Transportation

Cars, light trucks, big trucks, vehicle fleets

Industry

Factories, farms, ships, oil rigs

Municipal

Street lighting, waste water , water supply, drainage

Energy Management

Transmission, Generation: Hydro, Tidal, Fossil fuels, Wind power

Constrained Things

Cost

BoM, supply chain, development tools, development hardware, library availability

Processor power

Algorithms, cryptographic algorithms, tool support, IP stack

Electrical power

Power conservation, battery size, type & construction, solar powered, heat load

Memory

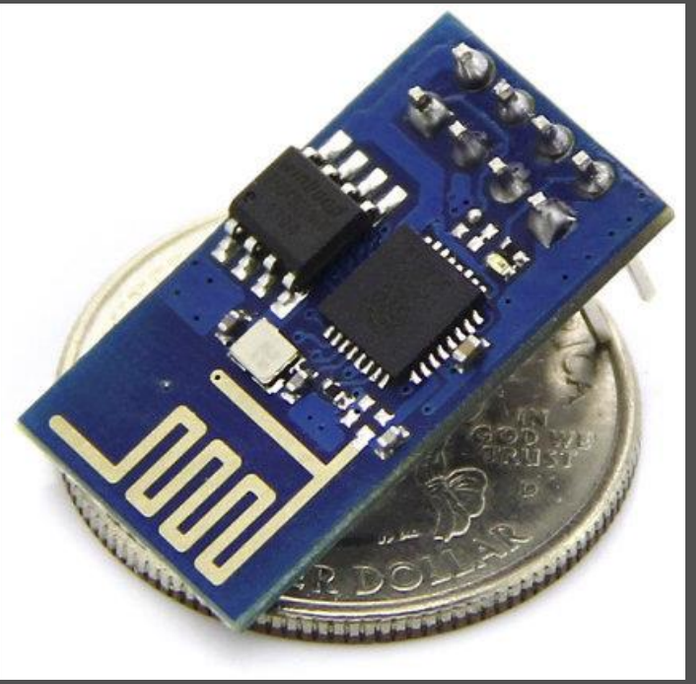
RAM, non-volatile, algorithms, cryptographic algorithms

Connectivity

Wired, wireless, protocols, bandwidth, payload size, power consumption

Support

Product lifetime, certification, updates, field service , disposal



Securing Things - STRIDE

Spoofing

CPU,RAM, Exchanging secrets

Tampering

CPU,RAM, Storing secrets

Repudiation

Data validity, commands, and time

Information Disclosure

Reverse engineering, sensor data, customer data

Denial of service

Communications coprocessors, minimal attack surface

Elevation of privilege

Robust protocols, encryption HTTPS, API Keys

Connecting Things

Protocols
DIY, HTTP, AMQP, CoAP, MQTT, XMPP

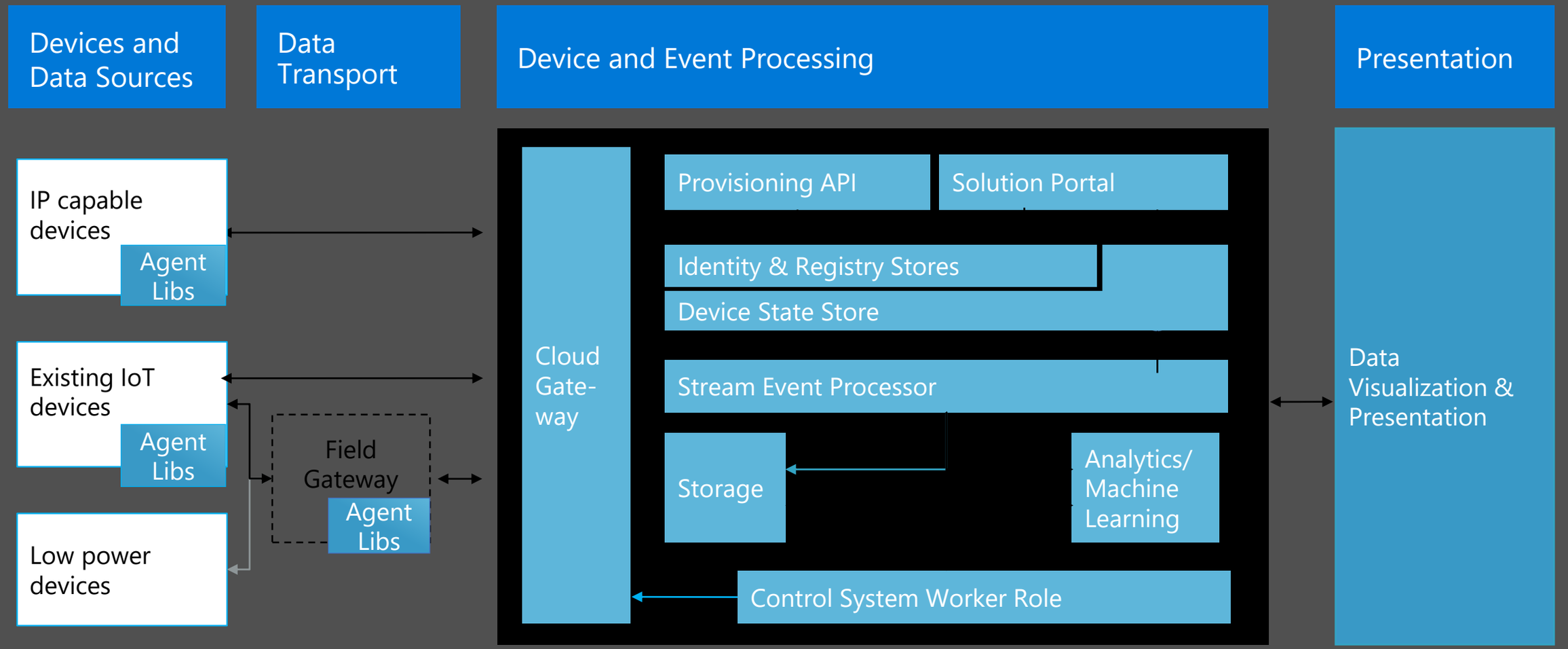
Personal area
BLE, ISM, nRF24

Local Area
Wifi, Xbee, nRF24, 6LowPAN, LoRA, Wired

Wide Area
Wired, 2G,2.5G,3G,4G,?G, Inmarsat, Iridium

Security
DIY, Secure Sockets, Network based, Authentication

IoT Reference Architecture



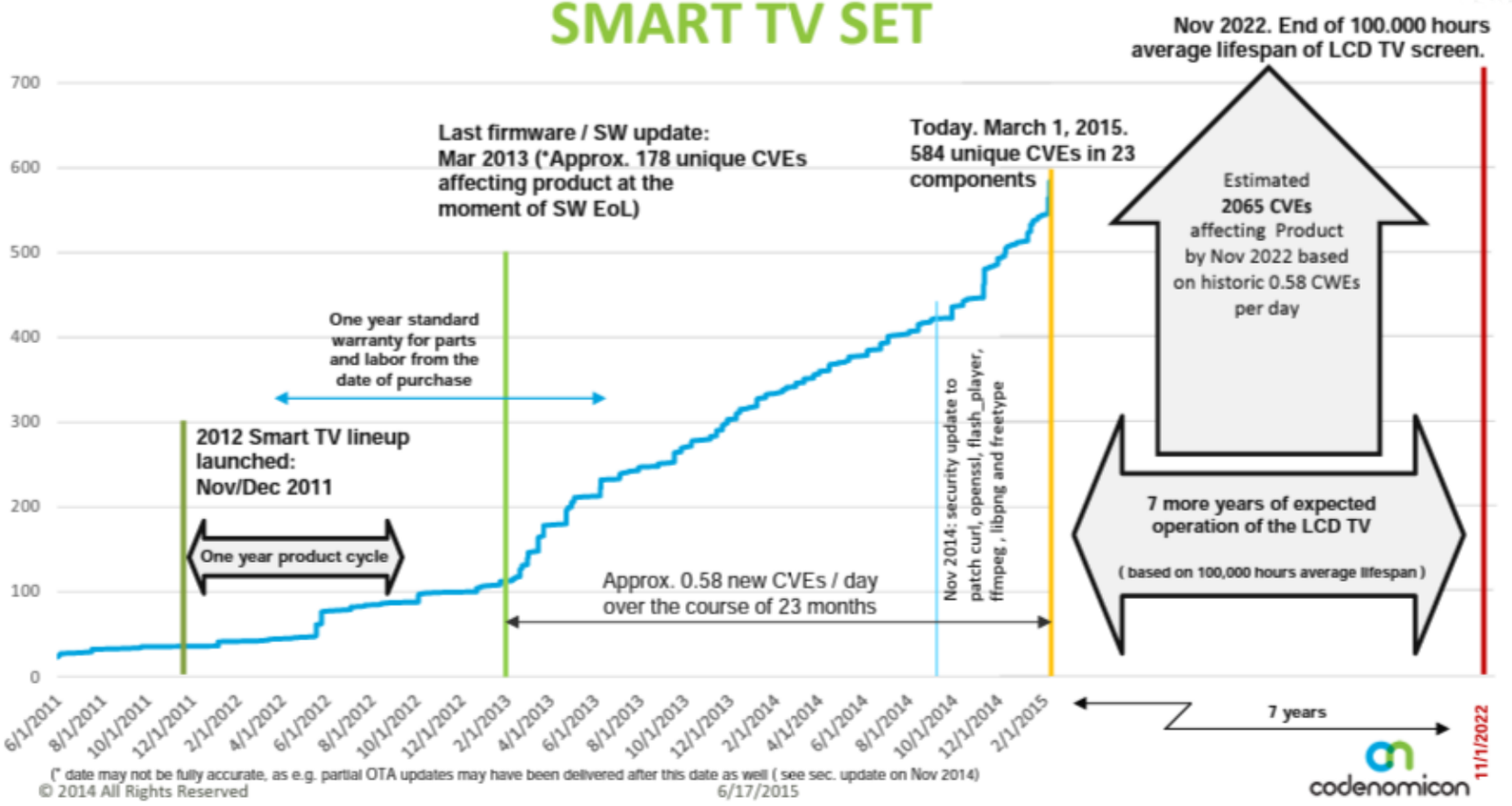
Field gateway demo

- Bryn Lewis

Broken Things

- 1.4 million Jeep vehicles
- 787 Dreamliner Generator Control Unit
- Hello Barbie
- Alphabet->Nest->Revolv acquhire
- German nuclear plant malware
- Glass flight deck malware distribution system
- Shodan
- @InternetOfShit

SMART TV SET



(* date may not be fully accurate, as e.g. partial OTA updates may have been delivered after this date as well (see sec. update on Nov 2014)

© 2014 All Rights Reserved

6/17/2015

codenomicon

Testing the Hardware of Things

Highly specialised

Organisations perform as a service

Standards compliance

Underwriters Laboratories (UL), European Conformity (CE)

Environmental

Temperature, humidity, vibration, shock

Electrical

Voltage spikes, cycling, brownouts

Tamper resistance

Evidence, destruction

Testing the Firmware of Things

Peripheral devices

What happens when a sensor or actuator goes bad

Update Mechanism

Selective updates or a DoS attack in the making

Reliability

How could it break

Robustness

Degrades gracefully outside of normal operating parameters

Supportability

How do we fix it when it breaks

Testing the Software of Things

Sensor & Actuator Emulation

How does system react to unexpected values, if instructions are ignored, feedback loops fail

Configuration & Provisioning

How does system react to unexpected configuration or provisioning information

Reliability

Is the system always available

Robustness

Does the system handle the unexpected

Correctness

Are the telemetry data values and commands handled as expected

Testing the Connectivity of Things

Protocol sniffing

Reverse engineering, packet injection, message spoofing, time variance

Endpoint simulation

Device, Field gateway, server, infrastructure, authentication services, time

Networking

Latency, Jitter, Packet loss, DNS issues, corruption, time

Interoperability

Discovery, exchange, disconnection, versioning

Custom hardware, software & tooling

Hard to reproduce interactions and timings

nRF24 Sniffer

- Bryn Lewis

Testing the Security of Things

Attack surface

Across all parts of system understand & reduce

Reverse engineering

What useful information can an attacker get about how system works

Specialised hardware and software

Pushing the system around in unexpected ways

Update infrastructure

Could an attacker install software, can we recover from a compromise

Protocols

Known vulnerabilities & limitations

Interoperability

Do we trust other systems

Testing the Services of Things

Scalability

Many users, load spikes, starting under load, while upgrading

Performance

Latency, jitter, while upgrading, telemetry from real & test clients

Reliability

Always available, gracefully degradation, how many 9s

Security

Minimising attack surface, devices vs. humans, information disclosure,

Supportability

Telemetry, remote management, infield upgrades

Data management demo

- Bryn Lewis

Testing Things at Scale

Canary deployments

Upgrade and monitor a subset of the customers

Device simulation

Simulate activity & data points it would be hard to generate with a real device

Field gateway simulation

Simulate device activity it would be hard to generate with real devices

Infrastructure Service simulation

Difficult to reproduce failure modes, outages, performance issues

User simulation

Usage personas, service failures, starting under load

Summary

Enabled by hardware

A microcontroller in every chicken in every pot

Enabled by manufacturing

Mass production and supply chain

Enabled by cloud computing

Global scale with a credit card and a laptop

Enabled by Open Standards

Must play nice with others

Questions…

@KiwiBryn

blog.devmobile.co.nz

Bryn.lewis@devmobile.co.nz