FUJITSU

shaping tomorrow with you

The Internet of Things and Security

Roger Whiteley

@Roger_W_FDE

Fujitsu Distinguished Engineer, STEM Ambassador

v2.0 BCS Edinburgh 7th March 2018

Distinguished Engineer

60 CELEBRATING SIXTY YEARS 1957 - 2017

STEM AMBASSADORS ILLUMINATING FUTURES

Agenda

FUJITSU

- Thank You's
- Cyber Security – why is this stuff important?
- Internet of Things – Connected Everything
- Connected Infrastructure
- What is a Thing?
- Attack Vectors
  - Devices
  - Networks
  - End Points
- Discussion & Questions

Thank You's

FUJITSU

- Last month's BCS Edinburgh presenter, Dave Stubley from 7 Elements
  - Because I learnt new ways that people get conned
  - And the difference in between a state actor and a script kiddie.....
- Sheridan – the tour guide at TNMoC next door to Bletchley Park
  - Because I never knew the 80 column punch card dated from the 1800's, and loads of other things on a very informative tour

Cyber Security 2018 – why is this stuff important?

FUJITSU

Finally, Cyber is coming in from the cold into mainstream media, why?

- GDPR
- Identify theft
- Denial of Service
- Inference from insecure data transmissions / Personal data leakage
- Weak device and application security

- A message for ALL CFO's – there **IS NO ROI** on Cyber security, GDPR is concentrating minds on the potential fines – not a TalkTalk style slap on the wrists

Cyber Security 2018 – GDPR

FUJITSU

- GDPR – the punishment for losing customer data could put your business out of business
- Couple of personal and very recent examples
  - I got a text message from my credit card provider half an hour before I tried to use it...

    telling me they'd just blocked it, WHY?
  - I got a phone call purporting to be from my mobile provider – it was, but it made me think
- Expect an email from every web-site and online shop asking you to verify your email subscription preferences – make sure you read the questions before ticking the boxes – especially the one giving them explicit permission to share YOUR details with third parties

FUJITSU

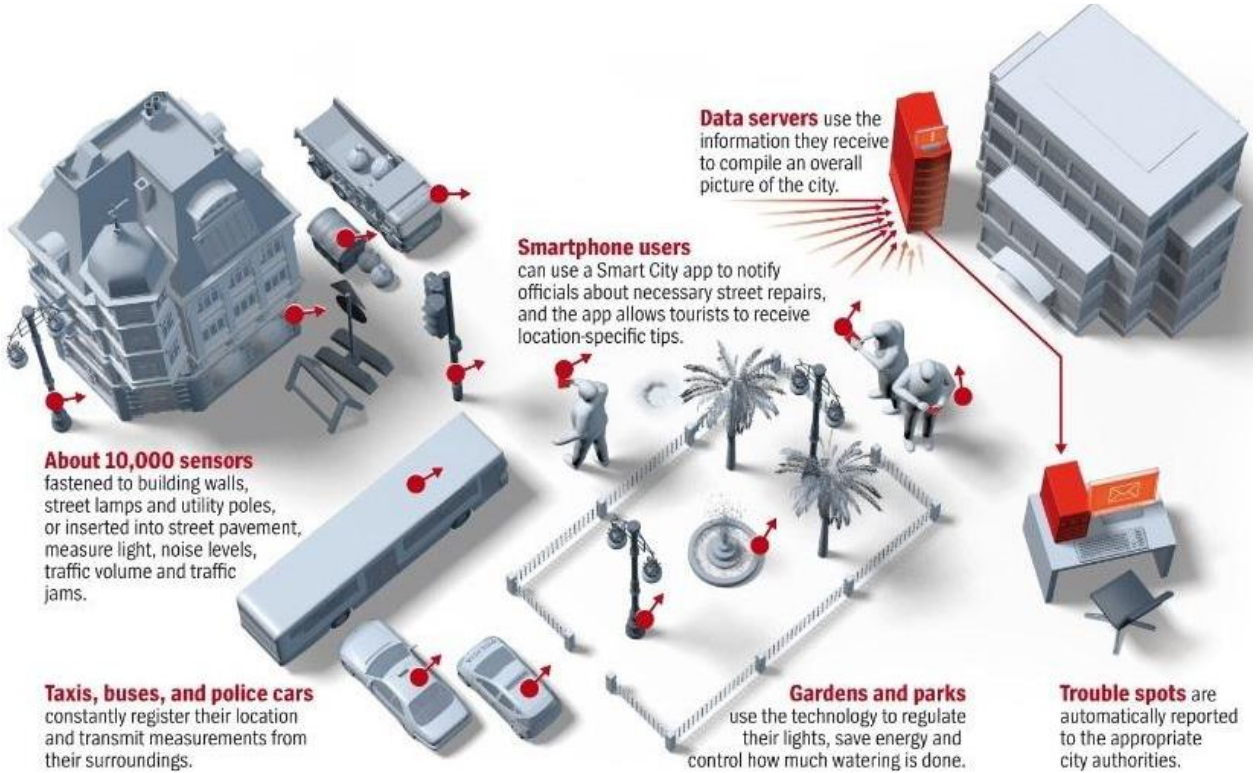
shaping tomorrow with you

The Internet of Things – connected everything

There are useful ‘things’, and not so useful...

Recap – 'Things' I've spoken about before

FUJITSU



So what is a Thing?

FUJITSU

‘Things’ for our conversation

FUJITSU

Connected Sensors / Toys

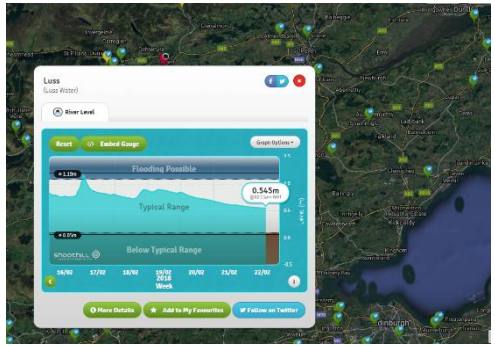
FUJITSU

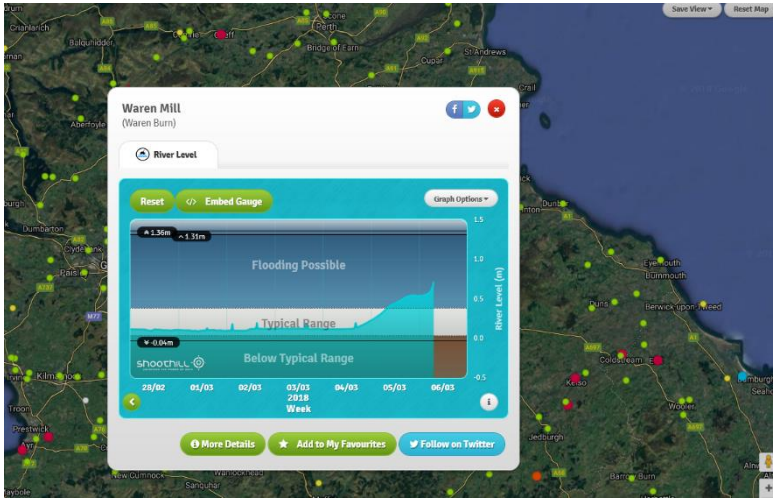
- Sensors are everywhere – but an unconnected sensor has no value – Data has more value than oil
- 'Smartphones'
- Fitbits
- 'Smart watches'
- Are only smart with connectivity – usually some wireless network

- Toys – adult and kids – Teddy bears leaking conversations, adult toys leaking pretty much anything

Useful Applications of Things…. [and Open Data]

- Environmental monitoring and control
  - Rivers / Floods / Tides





  - Agriculture – micro managing water table levels for irrigation of crops
  - Frost alerts
- Traffic Cameras / River Cameras

Examples of Useful Things…. (2)

FUJITSU

- Industrial Control and Monitoring –
  - Distributed monitoring systems,
  - Smart factories
  - Extended supply chain
  - Employee safety
- Meters – 'smart' or otherwise
- Bovine step counters, not Fitbit's, but a means of detecting when a cow enter oestrus
- Smartphones – not dumb phones, have: accelerometers, GPS, light sensors, cameras, speech recognition – useful if you can crowdsource anonymous accelerometer and location data to detect potholes…

And Should We Worry about Security?

FUJITSU

- If the 'Thing' is a single use object, with a defined life, for example a machine readable tag – or a device with low value with information collected / transmitted with little economic value – probably not
- If the 'Thing' is a high value object with a long projected life which collects data of material value – almost certainly yes

A message for Start-Ups

- Security MUST be integral from the very start of product concept and development
- Problems cost much more to fix later
- Get an independent review of your Security Methodology/Design/Architecture before cutting code
- If you haven't got a means of applying software updates at a later date, GET ONE

Attack Vectors

FUJITSU

- Networks
- Devices
- Data in Transit and Endpoints
- People - through social engineering or just plain stupidity

It's a big place....

Industrial #IoT is entirely dependant upon Networks of some description

Networks

FUJITSU

IoT is totally reliant on networks

- ‘Metropolitan’
  - LoRaWan
  - 3 / 4 / 5 Generation Mobile
- House or Office
  - LDP 433 MHz
  - Bluetooth Low Energy BLE / Bluetooth beacons
  - Zigbee
  - z wave
  - Passive WiFi

My particular favourite -

Networks - The Hotel Control System...

FUJITSU

- Android controlled lightswitches - I stayed in a hotel with Android controlled lightswitches and it was just as bad as you'd imagine

  - Three devices, all Android tablets, two using RJ45 cables – but not secured in any way

  - Reinforces the message there's no substitute for a Common Sense RISK ASSESSMENT – the hotel guest simply disconnected the RJ45 cable and used it to plug in his own device!

Networks – the iKettle WiFi

FUJITSU

- Hackers found a way into the iKettle which exposed the WiFi password – even changing the configuration doesn't reset the default device password, at least not with the Android app, it does with iOS.

- Further reading [The Register iKettle London Map]

- So its only a matter of time before someone hacks the latest must have #Internet of Toasters

Networks – Attack Vectors

FUJITSU

- Physical connections –there are standards to block unauthorised device access e.g. 802.1X, and you could just prevent access to the connectors
- Wireless makes attack vectors simpler because attacks can be done externally with no physical access necessary
- Packet Sniffers – capturing data
- Jamming technology
  - Direct means of accessing or blocking legitimate access to your home network OR IoT cloud
  - Leaves your Range Rover unlocked in Central London, which has resulted in the police recommending use of a Krooklok!

Engineering

FUJITSU

- All the examples in this talk demonstrate a simple lack of **Common Sense Engineering**
- Reinforced by lack of customer awareness because:
  - Customers buy devices that have default passwords and userids and NEVER change them – this is what enables Botnets using security cameras
  - Users do not change privacy settings from Defaults.
- The latest, biggest DDOS attack last week on Github used insecure open internet database services
- Experience of physical crimes such as burglary have shown that applying the most basic security measures makes perpetrators go somewhere else, because there's always someone with weaker (no) security
- Scanning your Internet router public IP address is a routine starting point looking for ways into your network – inbound ports for gaming devices are open by default ☹

So there's a world of possibility.....

FUJITSU

Devices (1) Car Hacks

FUJITSU

- Fiat Chrysler issued a safety recall affecting 1.4m vehicles in the US, after security researchers showed that one of its cars could be hacked. On 21.07.2016, tech magazine Wired reported the car could be hacked via its internet-connected entertainment system.

Credit – BBC / Wired

- A bug in Mitsubishi's PHEV Outlander WiFi makes it possible to disable the car alarm

Devices (2) Listening Devices, or bugs

FUJITSU

- The TV that states '**Our Smart TVs record your living room chatter'** - Smart TV's voice recognition system will not only capture your private conversations, but also pass them onto third parties – without your consent

- **Alexa – seems like a good idea, but not if you value your privacy**

Devices (3) Medical Devices

- The Johnson & Johnson 'One Touch Ping' insulin pump uses an unencrypted radio link between the pump and the metering controller which can be up to 3m away, which makes it possible to send injection commands on demand, which could cause an insulin overdose
- Problems with a Pacemaker device in the USA were discovered and that information used to 'sell-short' the manufacturer's stock, before disclosure of the vulnerability
- These examples show that its not 'merely' a DDOS that's at stake here – overdoses and damaging businesses financially demonstrate the pitfalls of ignoring security

Cyber Network Attack Prevention

FUJITSU

- Prevent physical network access – metal cabinets, secured connections
- Block unauthorised devices from accessing physical network connections
- Don't *assume* your ISP provided router is really secure
- Encryption of data in transit:
  - Smart Meters – every new smart meter in the UK has the same encryption key AND it only connects to WiFi

Take Away Why is this important? – someone with network access can infer from reading the unencrypted meter readings when you are in, or out, without ever visiting your house

New Stuff #1

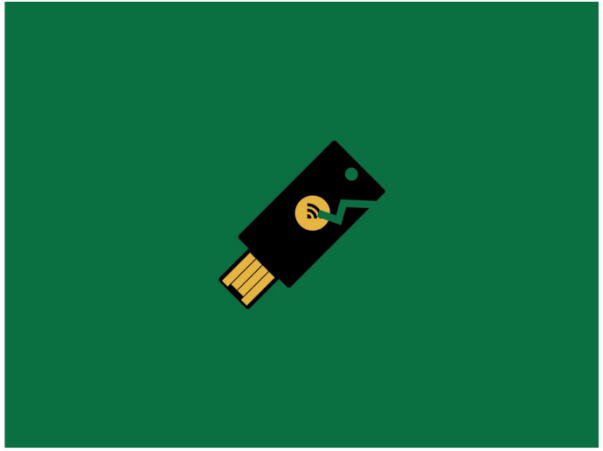
FUJITSU

RedDrop: New sophisticated Android malware spies on you, steals data and racks up huge phone bill

The malware has been found lurking in 53 apps masquerading as image editors, calculators and language learning apps.

ANDY GREENBERG SECURITY 03.01.18 11:54 AM

CHROME LETS HACKERS PHISH EVEN 'UNPHISHABLE' YUBIKEY USERS



And I've not mentioned Spectre or Meltdown – right now these are HARD vulnerabilities to exploit, until tools get into the wild and reach the script kiddies

New Stuff #2

FUJITSU

- The largest DDOS attack on Github lasted less than a week before the Memcache bug was exploited to generate a 1.7Tbit DDOS attack
- The moral of this story is DO NOT EVER expose systems with weak or NO authentication to the Internet!

End Point Attacks

FUJITSU

- Disable SSL – a 12 year old bug is still being exploited in the wild, unless you know the version of SSL is up to date
- If you don't need it, disable uPnP/PNP on your router
- The 1Tbit DDoS attack on kerebsonsecurity.com used 150 THOUSAND compromised Camera Security systems, like this one

Cyber Attacks on End Points

FUJITSU

- If you cannot update the software on your endpoint devices, its only a matter of time before the rewards for finding a way in make it worth looking for one
- No IoT device I have come across supports more advanced security such as Trusted Hardware

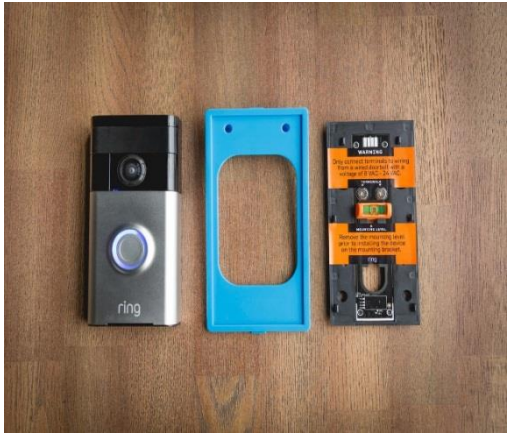
Take Away IoT devices MUST be upgradeable using Over The Air (OTA), this can be done, even with an ESP8266 device, so there is no excuse.

Home Automation

FUJITSU

The Wireless Doorbell

- You cannot make this up..
- Fix the device to the front of your house/flat/boat
- The removable front gives direct access to the reset button from which SOMEONE ELSE can hijack the settings including your WiFi security key!
- As seen on on TV...



Take Away Its no longer about simply borrowing your Wi-Fi bandwidth – its about being able to access ANY of your logons or passwords that are not protected with HTTPS / SSL. Even unsigned certificates are MORE secure than no certificate

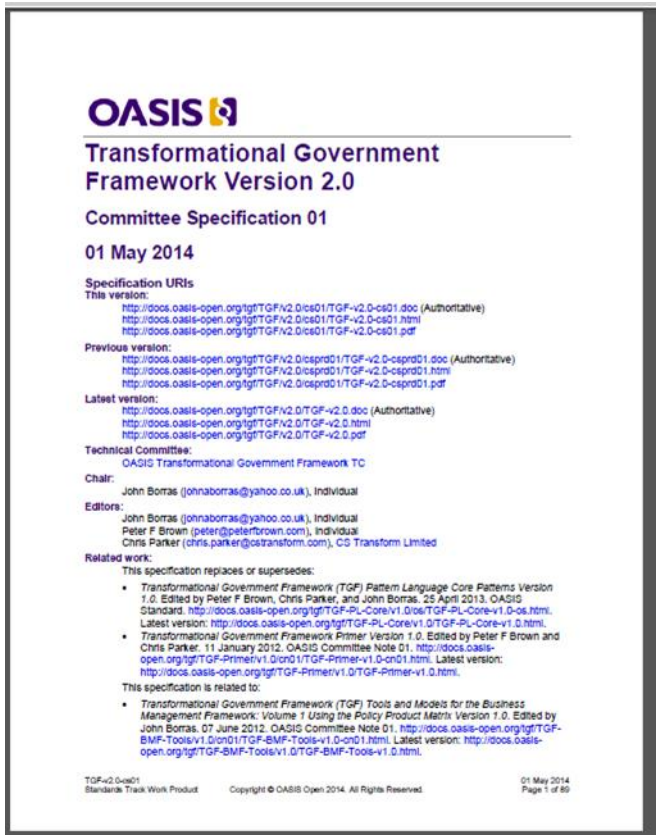
The Alexa / Facebook Problem

FUJITSU

- Alexa: '*I want a Dolls House*'
  - Billed automatically to the customers Amazon account
  - Story covered on TV
  - Lots of Dolls Houses delivered to Amazon customers that just happened to be watching the TV report
- Have you changed your Alexa privacy settings – so that your history of conversations is purged?
- Have you turned off Facebook facial recognition?
  - **You SHOULD, if you value YOUR privacy**
  - **How many sites have YOU stored your payment details on?**

The Stamdards are Coming, but tediously SLOW

FUJITSU



OASIS

Transformational Government Framework Version 2.0

Committee Specification 01

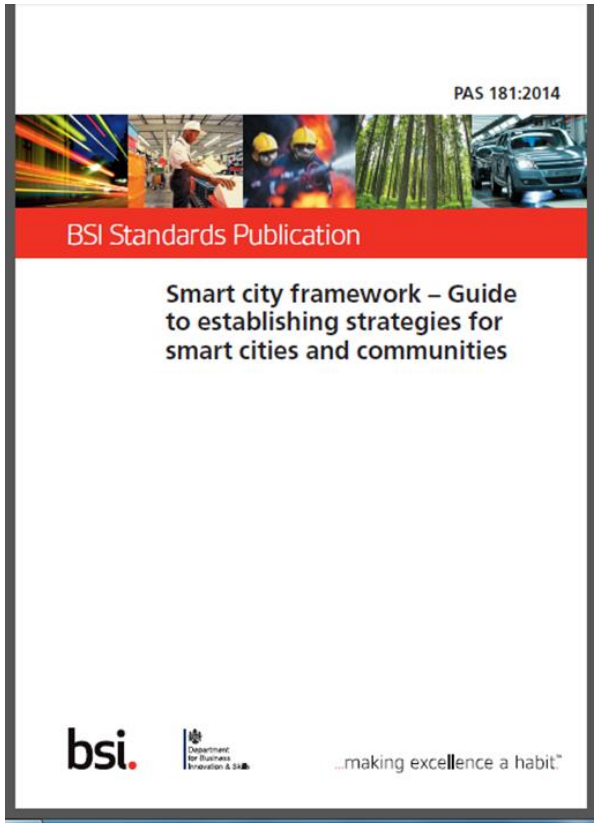
01 May 2014

Specification URIs
This version:
http://docs.oasis-open.org/tgf/TGF/v2.0/cs01/TGF-v2.0-cs01.doc (Authoritative)
http://docs.oasis-open.org/tgf/TGF/v2.0/cs01/TGF-v2.0-cs01.html
http://docs.oasis-open.org/tgf/TGF/v2.0/cs01/TGF-v2.0-cs01.pdf
Previous version:
http://docs.oasis-open.org/tgf/TGF/v2.0/csprd01/TGF-v2.0-csprd01.doc (Authoritative)
http://docs.oasis-open.org/tgf/TGF/v2.0/csprd01/TGF-v2.0-csprd01.html
http://docs.oasis-open.org/tgf/TGF/v2.0/csprd01/TGF-v2.0-csprd01.pdf
Latest version:
http://docs.oasis-open.org/tgf/TGF/v2.0/TGF-v2.0.doc (Authoritative)
http://docs.oasis-open.org/tgf/TGF/v2.0/TGF-v2.0.html
http://docs.oasis-open.org/tgf/TGF/v2.0/TGF-v2.0.pdf
Technical Committee:
OASIS Transformational Government Framework TC
Chair:
John Borras (johnaborras@yahoo.co.uk), Individual
Editors:
John Borras (johnaborras@yahoo.co.uk), Individual
Peter F Brown (peter@peterfbrown.com), Individual
Chris Parker (chris.parker@cstransform.com), CS Transform Limited
Related work:
This specification replaces or supersedes:

- *Transformational Government Framework (TGF) Pattern Language Core Patterns Version 1.0.* Edited by Peter F Brown, Chris Parker, and John Borras. 25 April 2013. OASIS Standard. http://docs.oasis-open.org/tgf/TGF-PL-Core/v1.0/os/TGF-PL-Core-v1.0-os.html. Latest version: http://docs.oasis-open.org/tgf/TGF-PL-Core/v1.0/TGF-PL-Core-v1.0.html.
- *Transformational Government Framework Primer Version 1.0.* Edited by Peter F Brown and Chris Parker. 11 January 2012. OASIS Committee Note 01. http://docs.oasis-open.org/tgf/TGF-Primer/v1.0/cn01/TGF-Primer-v1.0-cn01.html. Latest version: http://docs.oasis-open.org/tgf/TGF-Primer/v1.0/TGF-Primer-v1.0.html.

This specification is related to:

- *Transformational Government Framework (TGF) Tools and Models for the Business Management Framework: Volume 1 Using the Policy Product Matrix Version 1.0.* Edited by John Borras. 07 June 2012. OASIS Committee Note 01. http://docs.oasis-open.org/tgf/TGF-BMF-Tools/v1.0/cn01/TGF-BMF-Tools-v1.0-cn01.html. Latest version: http://docs.oasis-open.org/tgf/TGF-BMF-Tools/v1.0/TGF-BMF-Tools-v1.0.html.



PAS 181:2014

BSI Standards Publication

Smart city framework – Guide to establishing strategies for smart cities and communities

bsi.

Department for Business Innovation & Skills

...making excellence a habit.™

PAS 182:2014

BSI Standards Publication

Smart city concept model – Guide to establishing a model for data interoperability

bsi.

Department for Business Innovation & Skills

...making excellence a habit.™

Standards... or Lack of Standards...

FUJITSU

- This is an RJ45 socket right?
  - No, it's a fully fledged implementation of an http web server
  - So who's responsible for fixing the security holes?
    - The Vendor?
    - The End User?
    - Safety recalls for critical issues in cars do NOT achieve 100%
    - Will every self combusting Samsung Note 7 be returned?
    - A while ago, Tesla updated the software on their cars to fix a security bug....

Building your own IoT devices..

FUJITSU

Hot off the Press....

As featured in RaspberryPi magazine issue 67 – Mozilla launches Project Things – using a Pi as an IoT gateway to Zigbee and Z-Wave
A Pi will perform as an integration hub for HomeKit, Google, Alexa &c.
Mozilla submitted the WebThing API to W3C on 15th February 2018

Take Away If you want control, build your own devices, Weather Stations, Locking systems, and upgrade / manage them with Ansible

This post pretty much sums it up...

FUJITSU

- The Registers' IoT Viewpoint as of Monday 24th Oct 2016
- There is a proliferation of industry ‘standards’ bodies and frameworks and IoT enabling ‘hubs’
- Not all those ‘hubs’ will survive – Dr. Joseph Reger, Fujitsu Fellow, CTO Fujitsu EMEIA in his blog post

Essential Capabilities for IoT Endpoints

FUJITSU

- Device Management
  - Bootstrapping - key management, Service provisioning, ACL
  - Configuration - device settings and updates to parameters
  - Firmware update – application and system software, bug fixes
  - Fault management – error reporting, device status query
- Application
  - Configuration and control
    - None Repudiation
    - Application settings, control commands
  - Reporting
    - Changes in sensor values, alarm and event notification

Certifications... and Memberships

FUJITSU

- Underwriter's Labs UL2900 certification isn't a free document – it is $800 US
- How many #IoT devices are already installed?
- The market supersedes standards if the standards take too long or are too hard to implement – this happens – OSI networking for example
- For practical implementation advice, look to the consortia who are developing USABLE 'standards'

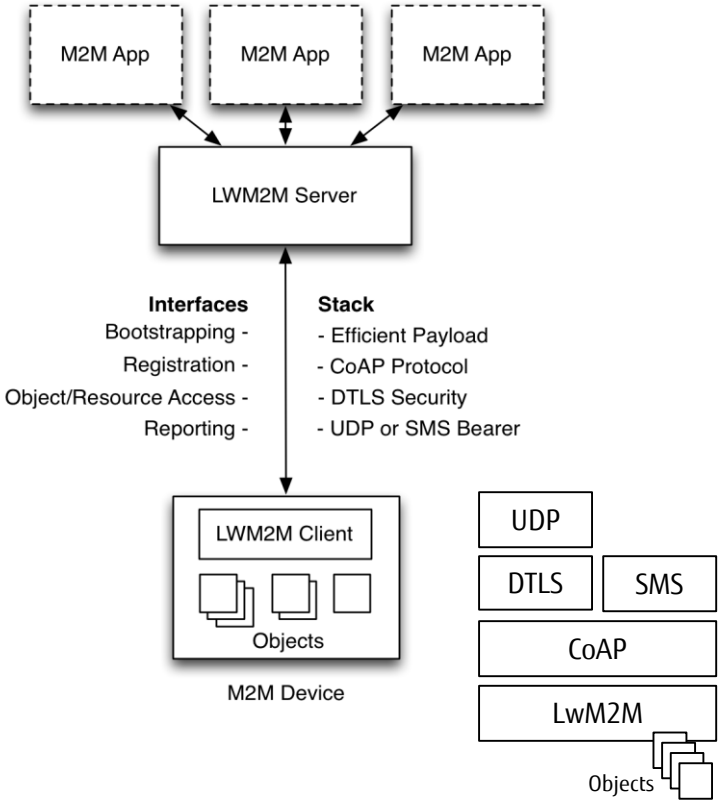
Vendors / Frameworks / ‘Standards’

FUJITSU

- Where to go for help..
- Standards Organisations such as - OMA, oneM2M – Fujitsu is a member of both
- Open is Good!

- If you want to integrate and roll your own, you don’t need anything more sophisticated than MQTT

LwM2M Architecture



- M2M Applications
  - Application abstraction through REST API
  - Resource Discovery and Linking
- LWM2M Server
  - Uses CoAP*
  - Re-uses the Resource Directory
  - Gateway and Cloud deployable
- LWM2M Clients are Devices
  - Device abstraction through CoAP and objects.
  - Works over any IP network connection

* CoAP – Constrained Application Protocol

LwM2M Specifications

FUJITSU

- Requirements, architecture and technical specifications are available for download at Open Mobile Alliance LwM2M Spec
- The software is on GitHub

FUJITSU

shaping tomorrow with you

Some Guidance

Security and your Home Automation System

FUJITSU

- Food for thought..
- If you can control your lights / central heating remotely then so, in principle, can someone else - or read your website passwords or decide when to break in because they know you are out..
- Gateways are the hub of the Home Automation System but there are NO proper standards, per se, only Vendor Frameworks or Vendor Implementations...
- Choose a Framework: for example HomeKit, which has support from multiple manufacturers of HA devices
- Or choose a specific Vendor implementation:
  - The key point is – they are all different, and who has control over the timing and frequency of updates??
  - A repeat of the Android phone problem – the upgrade path for Android phones is chaotic because responsibility falls somewhere between the device manufacturer and the network provider

Key Takeaways

FUJITSU

- Security through:
  - Solution Design
  - Solution Implementation
  - Product selection
  - Vendor Support and awareness
  - Customer Support and awareness
  - Open source
- Security is NOT an afterthought
- Choose your products with care, otherwise you might finish up with multiple gateways for lights, heating, your front door, and the probability that either your devices are hijacked for nefarious means OR you are leaking personal data OR BOTH

Common Sense Actions you CAN take #1

FUJITSU

- Disable PnP AND WPS on your Internet router / Access Points – this punches holes straight through your firewall which are used to compromise Cameras and PVRs
- Disconnect or turn off your Cameras and PVRs NOW, they are probably being actively used in DDOS attacks unless they are on an isolated network, behind a firewall
- Enable Two Factor Authentication on your critical devices and accounts, inconvenient, but not difficult
- Further reading here: Hacked Home Routers
- **ALWAYS CHANGE DEFAULT PASSWORDS AND USERIDS**
- **CHECK PRIVACY SETTINGS – ESPECIALLY ALEXA AND FACEBOOK**

Common Sense Actions you CAN take #2

FUJITSU

- Don't root mobile phones
- Consider ignoring incoming call numbers you don't recognise
- Put your contactless cards in metallised foil envelopes, or cut a corner off, or use your mobile phone contactless payment system, if YOU trust it
- If your car has Keyless unlocking, put your car keys in a metal box when you are at home and the car's outside.
- AND consider a Krooklok type device

Final Thought #1

FUJITSU

- Who do YOU TRUST?

Final Thought #2

FUJITSU

- Tomorrow is International Womens' Day, so I thought it would be good to put up a few role models, no prizes for knowing who they are! Except the last picture on the bottom right..











Final Point

The birth of Computing took place here, in the UK,
powered by the need to break encrypted messages

to keep the Bombe on the Bletchley Park Estate
they are running a Crowdfunding Appeal.....

They need £50,000 to rehome the Turing-Welchman Bombe
from Bletchley Park Museum to
The National Museum of Computing

Just Google 'tnmoc bombe' – PLEASE!