Things have Identities Too

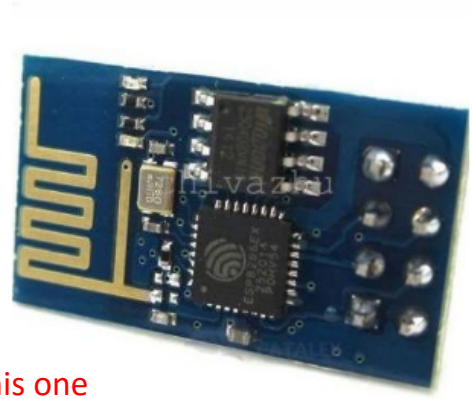
You have 100 guests coming to campus, they wont all arrive at the same time, some are going to want only internet access but some will want access to your protected networks. They are all running some bizarre operating system with no anti-virus or up to date patches and only a few people really know what they are doing there in the first place. Some of the guests may leave with new ones replacing them, they wont give you any notice of this but will want the same access.

Sounds like an Identity Management problem

Devices in Directories

- We have had Devices in our directories for a long time
  - Windows NT introduced the idea of a “Computer Account”
  - eDirectory had the same notion
- Have many of the same attributes as a person
  - They run a parallel authentication process with a fully managed password solution
- We don’t normally think about them because we don’t need to manage them
- Over the years we have added other items such as equipment to GALs to make them easy to book and track

What are “Things”



Esp8266 Esp-01 Serial Wifi Wireless
from eBay.com.au - 100fys

ESP8266 ESP-01 Serial WIFI Wireless Transceiver to Enlarge ESP8266 ESP-01 Serial WIFI ...

See more details at eBay.com.au - 100fys »

$2.55 (GBP1.57)
Free shipping
eBay.com.au - 100fys

Shop

- Typically small form factor and low cost
  - Don’t run a full operating system
  - Only have small computational power *remember this one
- Specifically designed around one or two inputs
- Low power devices, often called LPWAN (low power WAN)
  - Fridges
  - Lights
  - Air Conditioners
  - Dispensing machines
  - Air quality
  - Ultrasonics
  - Cameras
  - Wearables
  - Temperature / Humidity
  - …….Basically anything you can think of

Where will(do) we see them;

- Researchers
  - Cheap remote monitoring
- Faculties
  - Building Management
  - Asset monitoring
- Teaching
  - Engineering
  - Computer Science
  - Creative industries

Key Information

- Power usage is key consideration
  - lots of times you wont have mains power there to run them, this is what drives small computing power and low bandwidth transmissions
- Other consideration is $$, the more you pay the more compute you get, also the more power you use

Cost $

$10

$50-$70

$200+

Types of connections

- **Wifi**
  - Our network
  - Two way, can send and receive
  - High throughput
  - No limit on amount of data sent

- **LoRaWAN**
  - Probably our network, although there are commercial providers
  - Two way , can send and receive
  - Low throughput (51 – 222 bytes)
  - No limit on amount of data sent

Network Management

- **Sigfox**
  - Not on our network, they do their own wireless and backhaul
  - mostly one way, they do offer a small number of uploads per day
  - Low throughput 12 bytes
  - Limited number of uploads per day

- **3G/4G/5G and commercial LPWAN (Cat-M1)**
  - Not on our network, they do their own wireless and backhaul (Telstra / Optus / Vodafone etc.)
  - Two way, can send and receive
  - High throughput
  - No limit on amount of data sent

Contract Management

So what??

- Th
  la

Often thought of as an “IT Issue”, the conversation about your fridge monitor is misbehaving is very different to a conversation about your staff member is misbehaving, both can have the same outcome

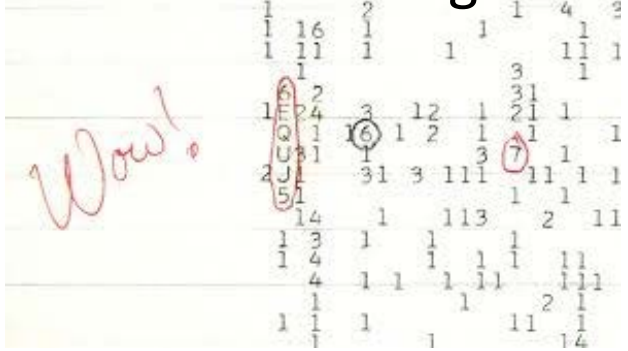
    - This also opens another hole, it is very easy to plug into them and change them , they are not monitored and no one will question you.
  - In some cases, to update them you must physically plug into them
  - Code is often developed by inexperienced people or pushed out in a rush
- These devices may sit in privileged networks such as building management networks

What if it all goes wrong?

- Long history of hacked devices to gain access, in or out
  - Use the devices to access privileged networks to disrupt, steal or modify

These devices may be your worst behaved user and they are on 24/7.

  - Estimated 500,000 – 600,000 devices infected with Mirai malware
- **This looks like a security issue but the tools and language to manage this number of objects are IdM**
  - This data will form the basis of papers, if there are 100 sensors collecting data, how do you ensure they are all trustworthy, without missing the “Wow!” moment



Identity lifecycle

Recruit
- Find the best applicant

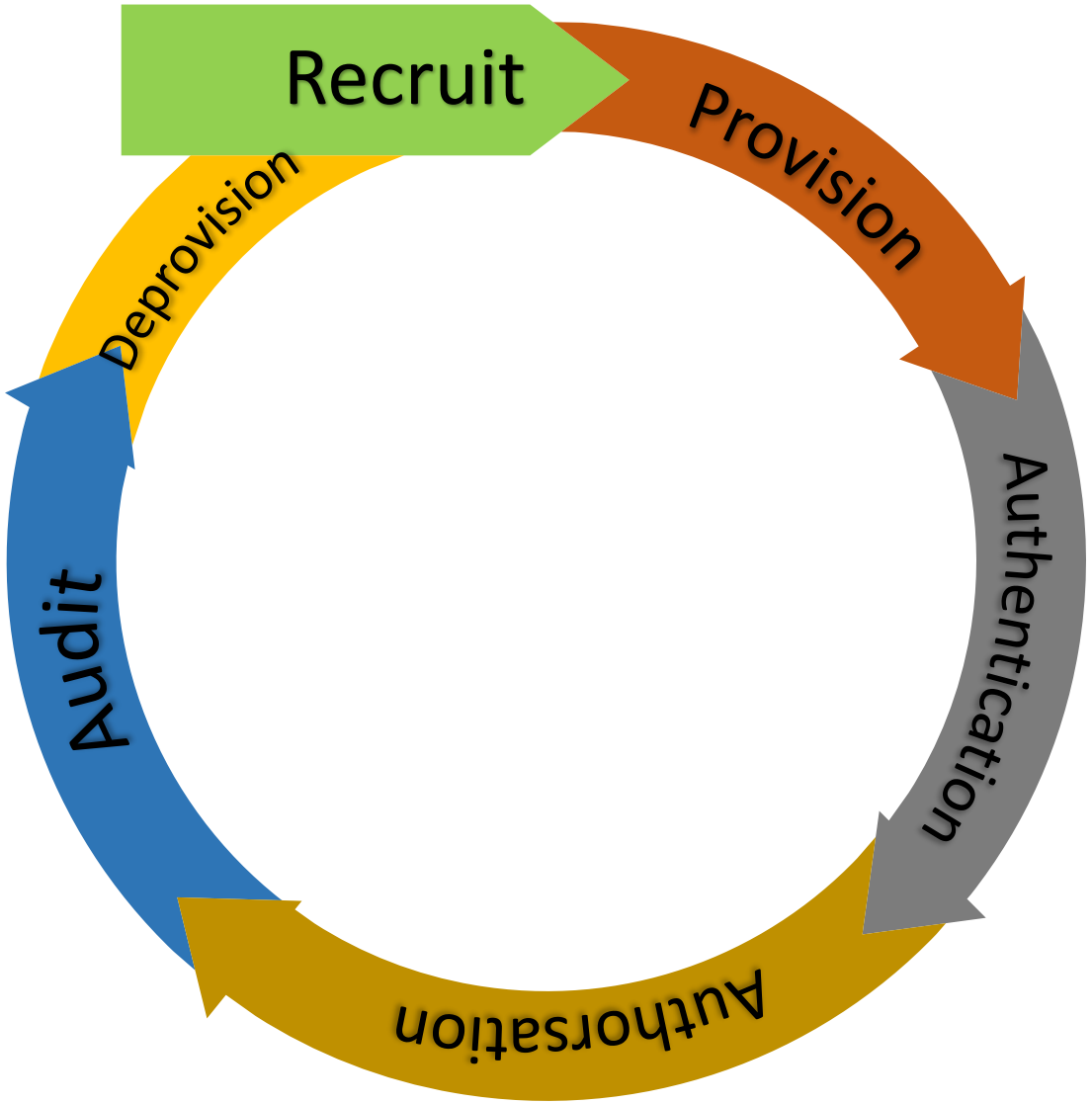
Provision
- Create the persons account

Authentication
- Validate the identity

Authorisation
- Right to access systems
- Relationships and roles

Audit
- Monitor use

Deprovision
- Remove configuration
- Remove data



IoT lifecycle

Recruit
- Research and purchase the device

Provision
- Create the device account

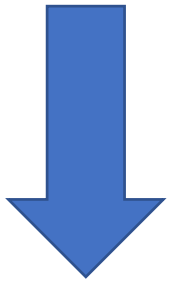
Authentication
- Validate the device

Authorisation
- Right to access systems
- Relationships to people and systems

Audit
- Monitor use

Deprovision
- Remove configuration
- Remove data

You have 100 guests coming to campus, they wont all arrive at the same time, some are going to want only internet access but some will want access to your protected networks.
They are all running some bizarre operating system with no anti-virus or up to date patches and only a few people really know what they are doing there in the first place.
Some of the guests may leave with new ones replacing them, they wont give you any notice of this but will want the same access.



- A researcher has purchased 100 IoT devices to monitor sensors all over the campus, they wont all arrive at the same time, they will all need internet access.
- You faculties people have purchased new sensors for your building management sensors, the contractor is here to install them and is waiting at the front desk, they need to write to the BMS database.

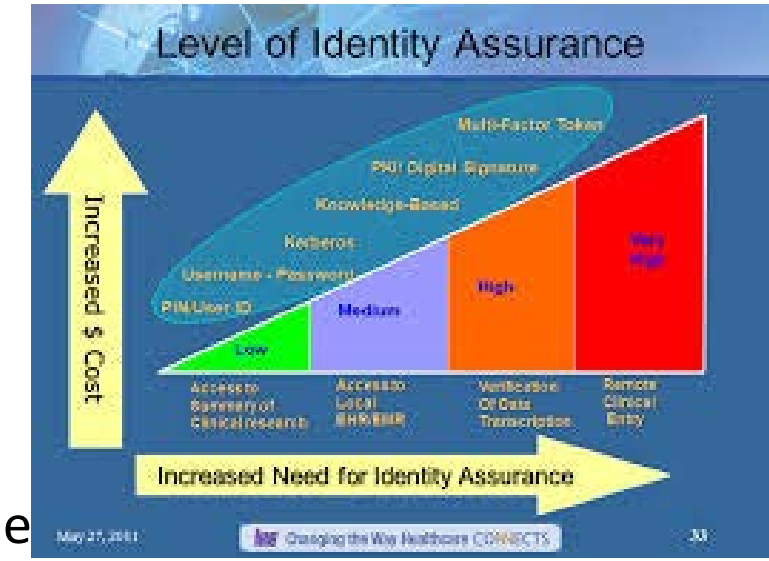
Language - Authentication

- IdM
  - The process of validating the identity of user; the user is who he/she says they are.
  - Typically, this is accomplished through a username/user ID and password pair.
  - often thought of as “logging in”
- IOT
  - The process of validating the identity of a “thing”
  - Unique identifier + connection information for network
    - MAC address + network Pre-Shared key
    - Blockchain + network Pre-Shared key

Language - Authorization

- IdM
  - The process of deciding if a user should have access to service
  - Typically thought of in terms of allowing access to an application or specific data
  - Typically done via group membership based upon meeting access requirements
    - employment contract
    - enrolment
- IOT
  - The process of deciding if a thing should have access to a service
  - The service in this case most typically will be the internet
    - We still need to track it (Metadata retention, AARNet, AusCert, etc)
  - Most probably based upon an “attestation” process where the responsible person will need to periodically review the access of their “things” via self service portal

Language - Assurance Level (LOA)



IdM

- A number (0-4) that defines the confidence in the identity of the individual who has the credential
  - Typically based around the creation of the account and the processes used to verify the identity
- This notion is being complemented with a broader “trust” model that uses real time user patterns to define how much we trust a user credential

IOT

- Still developing what this looks like but will be two faceted;
  - At creation, the person creating the device will have a LOA and trust level
  - On going, how do we know the data has not being tampered with, do we trust the device
    - not really our responsibility, but we may find ourselves storing “sample data” or “data thresholds”

What do we need

Same as a person;

- Who is responsible for the traffic
  - Think AARNet agreement and Federal Govt metadata retention
- Know what access it needs (Authorisation)
- Level of confidence (LOA)
- Way to turn it off – bearing in mind the password is the same for lots of them
- Auditing
- Self service – we don’t want to manage this
- Automated Deprovisioning
- Location - Where is the device
  - Important for data context
  - How do we find it if we need to reset it

What does this look like?

- Wifi network (SSID) with a Pre-shared key, most of these devices wont do advanced authentication
  - allow specific MAC addresses
- Directory
  - SQL database or similar
    - could be AD (eDir) with some custom attributes if you wanted to but just keep in mind object limits
  - IdM language for object attributes
    - Bring the maturity of IdM to this space, we are solving the same problem so lets not reinvent the wheel
- Self Service page for onboarding
- Work flow to get responsible people to periodically re-attest access requirement

Why us

- Already have a mature(ish) solution that is working with our network an
  - **I don't think that we should be "Managing" the IOT solution.**
- Ou **What we can do is offer a lot of maturity into** se inf **the setup and running of the solution.**
- We are focused on a "lifecycle" rather then the "binary" type of thinking that can be prominent in other support teams
- Introducing IdM language to Researchers will help them in the future when things like confidence levels start to matter to them (ScienceDMZ)

* Required

1. Responsible Officer *
Email address

Enter your answer

2. Device(s) MAC address and location , one per line *
MAC address and location separated by semi-colon. example :- 00:12:34:56:78:90 ; Room B21

Enter your answer

3. Access required *

- Internet
- Other

4. Length of time required for *
Maximum of 6 months, the responsible officer