Internet of Things

Push of technology requires a push in security

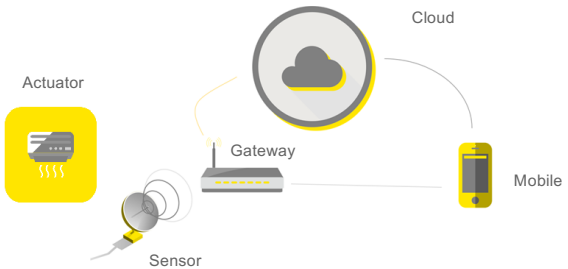
Building a better working world

Who am I?

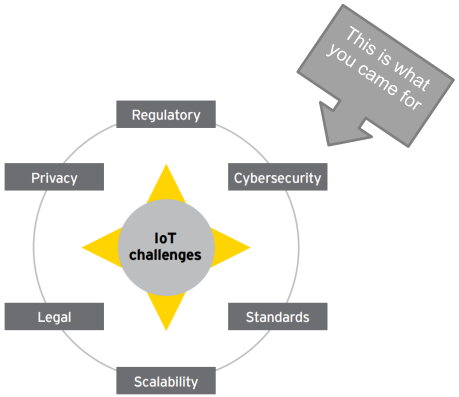
- Lucas Kauffman
- Senior IT Security consultant
- 4 years of experience (3 years in Belgium, 1 in Singapore)
- Contributor to Security Stack Exchange (platform for Q&A on information security)
- I like breaking things
- Beer enthusiast

What is Internet of Things?

> *A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.*



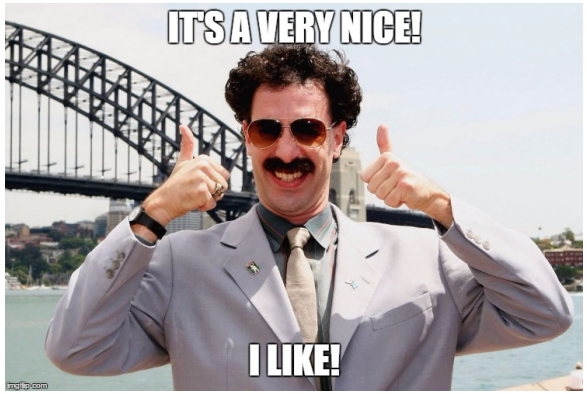
What are the issues with IoT?



Our experience testing IoT

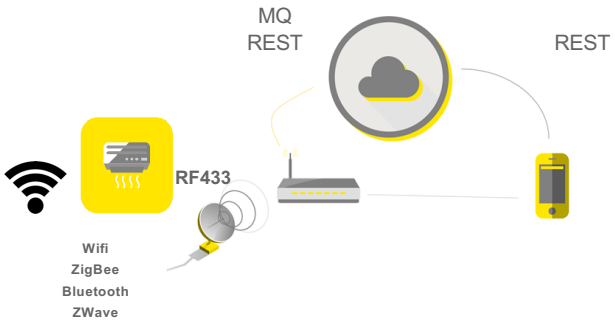
- Vendors both locally and international
- Small and large companies
- Different types of architectures
- All, but two had significant vulnerabilities
- Vulnerabilities keep coming back
- It's not because they don't want to, it's because they don't know.
- But…

But… they want to learn!



So what did we see?

General architecture



Threat vectors: Elderly monitoring

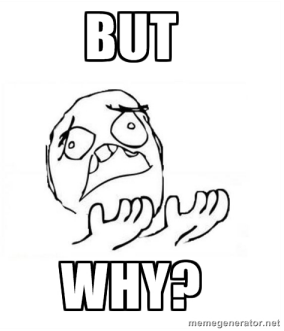
- Gateways used as botnet
- Mass surveillance of users
- Individual surveillance (theft)
- Disruption of service (fake emergency alerts)
- Spoofed telemetry
- Abuse of signals to cause fire
- …

High impact vulnerabilities

Unauthenticated internet facing update mechanisms	▸ Remote code execution ▸ Used together with another vulnerability to enumerate all gateways on the internet ▸ Automated exploitation of all box
SQL/JSON Injection on a "cloud" web interface	▸ Retrieve medical and activity data of subjects ▸ Retrieve personal data of subjects including addresses ▸ Using addresses and activity data (we know when someone is not home)
Bad design	▸ Backend was able execute commands on all routers ▸ Mobile applications log on to database directly ▸ Commands are sent using clear text and unsigned MQ messages
Don't trust anyone	▸ Too much reliant on the network security ▸ Gateway is trusted (e.g. no input validation on data pushed by the gateway)

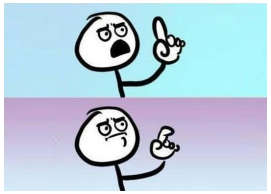
Old friends

- SQL Injection
- Cross Site Scripting
- CSRF
- Bad crypto/clear text communication
- Bad password hashing algorithms
- Command injection
- No patching
- Bad authentication
- Direct backend resource access



Why?

- Start up companies must have a functional prototype
- Focus is on features and functionality, not security
- Limited experience
- Security takes time
- Security is hard to get right
- IoT does not have a lot of reference architectures or standards
- No budget for security reviews



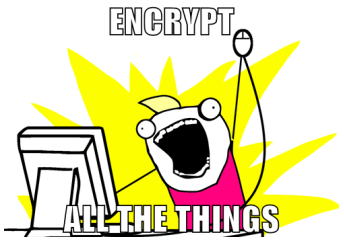
So how do we tackle these things?

We need security by design and reference architectures

- A single component should not be able to compromise another component
- Component communication should be encrypted
- All communication should be authenticated (Don't trust anyone!)
- Do proper threat modeling
- Be flexible!
- Don't think "they will never find out" (because we will)

Encryption

- Encrypt all communication
- Authenticate all communication
- Use standards
- Cryptography is hard, so don't roll your own
- Don't fail open or fallback



Validate input and use proper output encoding

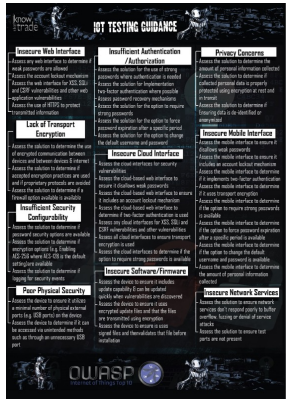
- Don't trust any input coming from the user:
  - Mobile device
  - Gateway
  - Sensors
- Do strict validation
- Whitelist is better than blacklist
- Use vetted frameworks for application development

But most importantly… awareness

IoT Project

Attack Surface Areas

Testing Guide | Top Vulnerabilities



But most importantly… awareness

- Doing IoT security at security conferences will show security to those interested in security
  - These are generally not the people who end up making mistakes
- We need to take security to general IoT conferences, meetups, etc…
- 15 minute slots with a brief awareness overview
- Make them aware and enthusiastic about security!

Summary

- People want to attach everything to the Internet (and they're not taking care of security)
- Mistakes are made due to security objectives being less important than business objectives
- There is a lack of awareness with regard to security
- We need more standards, good examples and reference architectures
- We need to take it to their communities

Q&A

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

APAC no. UEN 198905395E

ey.com