ETSI The Standards People

IoT Conference 2023

IoT Security Maintenance → Living Through Existential Threat

Presented by: Scott CADZOW

C3L

July 6th 2023

Agenda

- How do we secure IoT over its lifetime?
- Agility and awareness are key
- The standards we write to support you

What is the baseline for security of IoT?

EN 303 645 and its descendants define a small set of principles lay the foundation of systemic security (CIA paradigm)

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete user data
- Make installation and maintenance of devices easy
- Validate input data

Dealing with threats means dealing with change

- Attackers evolve and the defence chosen today is not going to work tomorrow
  - “Bringing a gun to a knife fight”
- New features in a system introduce new threats
  - There is no such thing as completely tested code and hardware
    - 10 lines of code and a simple library maybe, 10s of million lines of code and thousands of libraries, more than one language, persistent data, caches, online and offline data stores, not so simple.
    - 1 transistor and a few resistors, capacitors maybe, a billion transistors probably not.
    - 1 business unit with a short supply chain maybe, size introduces threats
  - Every new feature has the possibility to impact every existing feature
    - Change of cloud provider? Change of a data structure? Change of UI flow? Change of font or colour scheme?
- Changes in the regulatory environment
  - Is data revealing of a real person?
    - Is data processing AI assisted -- does the AI Act impact how code is evaluated?
  - Is the distribution channel going to impact the way in which code is tested?
    - Digital Markets Act, UK Code of Practice for Apps and App-Stores?

Existential threats

An existential threat is one that when it changes from a threat to an action wipes out the target - the target of the action will not exist afterwards

Some of the things that lead to existential threats:

- Reputation - loss of reputation can be catastrophic and can come from completely unexpected sources, in the extreme is will be existential
- External factors - often related to the supply chain, for example loss of a key raw material may be existential
- Cryptanalysis advances - although well researched all of today's algorithms are being examined to find ways to exploit them, once discovered the threat to that algorithm is sometimes existential
- Computing advance - Quantum Computing will delete any security from RSA and ECDSA, and severely impact the security of AES (and similar) and SHA (and similar)

Mitigating existential threat

- Implement a means to manage reports of vulnerabilities -- then fix them
  - From anywhere and everywhere these feed data on the threat landscape
  - Data gives you the ability of your widget to be ready to mitigate the vulnerabilities
- Keep software updated
  - Not for features but to mitigate the moving threat landscape
  - Only accept updates from known sources → Verify the source, verify the integrity of the update
- Make systems resilient to outages
  - …
- Make installation and maintenance of devices easy
  - Design for maintenance is therefore essential - but has to be secure too

Some more specifics …

- Protection of Reputation
  - loss of reputation can be catastrophic and can come from completely unexpected sources, in the extreme it will be existential
- External factors - often related to the supply chain, for example loss of a key raw material may be existential
  - In supply chain SBOMs, BOMs - sub more → Secure Software Bills of Materials, Secure Bills of Materials.
- Cryptanalysis and computing advances
  - The simple answer is crypto-agility. The problem is that this is poorly and loosely defined.

Making security a business process

- A security breach reflects on the business
- Fixing security breaches requires significant operational and budgetary authority
- The most senior levels of the organisation should be knowledgeable of the threats their operations are exposed to
    - In the regulatory domain it is often expected that compliance is a board level function as penalties are at the organisational level
- Secure by default is not a technical process but a business process
    - This is an important point - the business has to buy into security and not just the developers or the security guy

In summary

- The possibility of an existential threat has to be considered
- Threat mitigation across supply chains and across external factors in general have to be funded and managed from the very top of the organisation
    - Trickle down effect is insufficient - it has be be embedded into the organisation’s design
- Secure by default is not a technical process but a business process
    - The business imperative drives the engineering or technical processes