IoT Week 2022

IoT Security – Standards Development for Vertical Domains

Scott CADZOW (C3L, UK)

Rapporteur in ETSI CYBER

Chair ETSI TC ITS WG5 (Security)

Chair ETSI ISG ETI (Encrypted Traffic Integration)

Vice-chair ETSI TC eHEALTH

- What we mean by horizontal and vertical
- The role of EN 303 645 in establishing a baseline
- Specialisation or verticalization fitting the baseline to a vertical domain
- Wrapup and a hint at where we are going next

Setting a baseline - the horizontal

ETSI EN 303 645 – CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

- Setting 13 core principles for consumer IoT security providing 62 provisions
- 5 additional provisions for data protection

ETSI TS 103 701 – CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements

- Tests each provision at both conceptual and functional level

What this baseline offers

Firstly, it offers a broad set of very simple principles

Secondly, if provides testing of the principles

Thirdly, it supports the move to assurance as a root of proof of security attestations

Complemented by ISO/IEC 22443 (industrial sector)

Requires support of risk analysis standards (e.g. TVRA)

Requires support of security management processes (e.g. ISO 2700x)

Requires available standardised security technologies

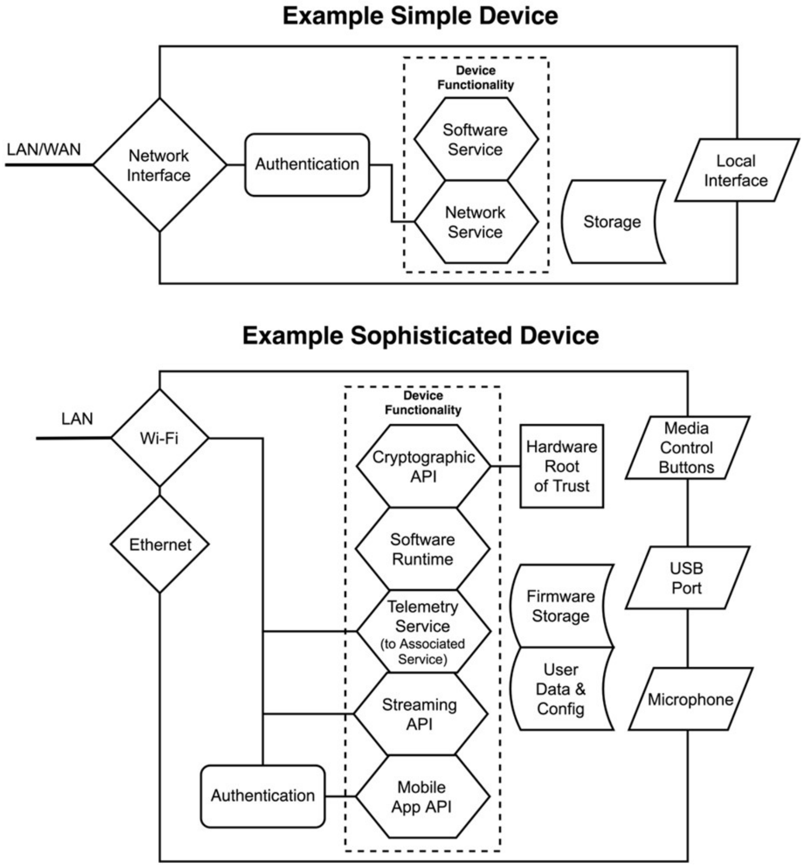
The 13 core principles

IoT Week 2022

1. No universal default passwords
2. Implement a means to manage reports of vulnerabilities
3. Keep software updated
4. Securely store sensitive security parameters
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is secure
9. Make systems resilient to outages
10. Examine system telemetry data
11. Make it easy for users to delete user data
12. Make installation and maintenance of devices easy
13. Validate input data

Many embedded IoT devices don’t fit easily to these principles though

Examples of IoT devices



ETSI IoT Week 2022

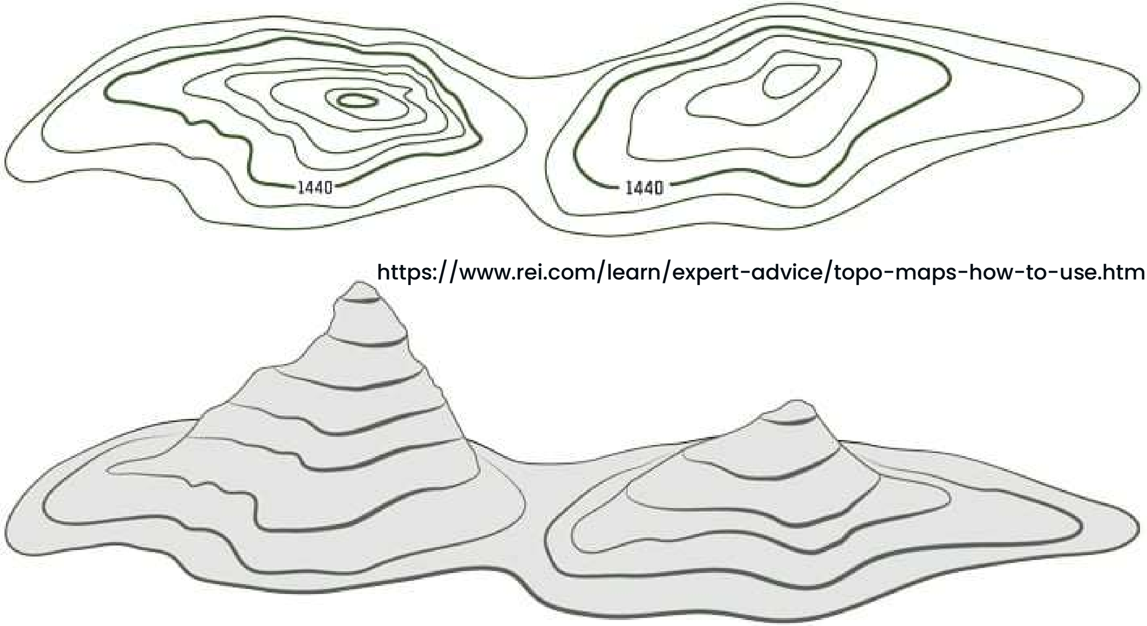
What is the horizon of our horizontal standards?

- Horizontal implies “as far as you can see, all the way to the horizon”
  - This implies everything is in scope of the horizontal standard
  - But only in a 1-dimensional world, whereas the world has 3 or 4 or 5 or more dimensions
  - If we assume the real world has topographical features then the horizontal blanket often unhelpfully masks those features
- The horizontal’s horizon should be far enough to give coverage of what we can see or anticipate
  - Verticalisation assures we pin the horizontal to the real topography of the world our things exist in

IoT’s topography - the need for verticals

- Making the horizontal too deep has a risk of making the standards burden too big for large parts of the IoT landscape
  - Where to level the plane? Not too deep (burden too high), not too shallow (doesn’t help as verticals dominate)
- The verticals’ purpose is to fill the gaps the horizontal plane cannot reach

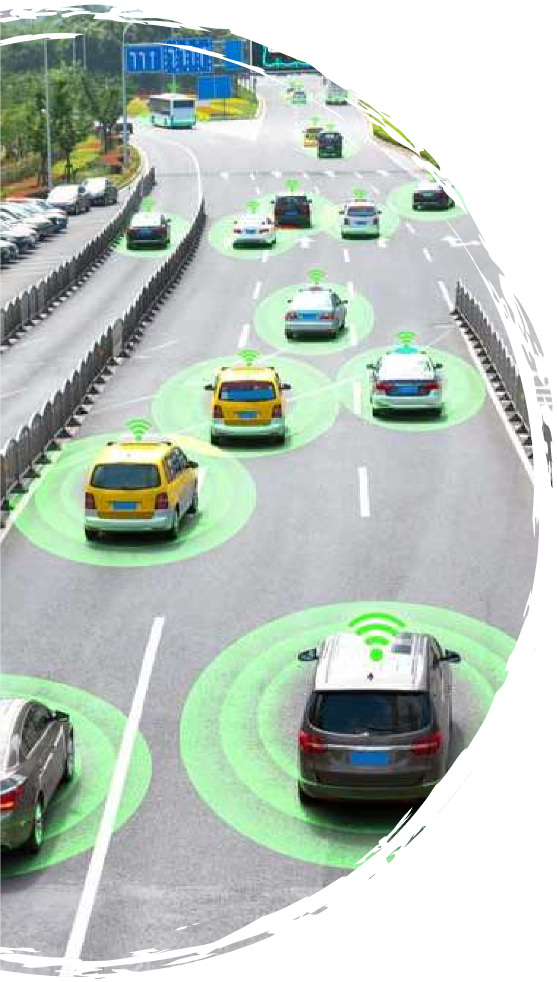
©Roger Dean



https://www.rei.com/learn/expert-advice/topo-maps-how-to-use.html

Recommended approach to the definition of IoT Security requirements for Vertical use

- The base or foundation document
- The template – guidance to develop the vertical spec.
  - Template on ETSI portal
- Developing the vertical domain spec.
- The test world and its foundation document
- The test and conformance spec. for the vertical
  - Test template on ETSI portal



The template - the basics

Information:

- Providing additional information (in the form of informative text) to an unmodified provision

Promotion:

- Promoting a recommendation to a mandatory provision (replacing should by shall)

Refinement:

- Refining a provision with additions or modifications to its normative definition text, including stronger scoping of conditionality

Extension:

- Extending an existing provision with one or more new sub-provisions

Substitution:

- Replacing a recommendation that is not applicable for the [vertical domain] with another recommendation of equivalent effect

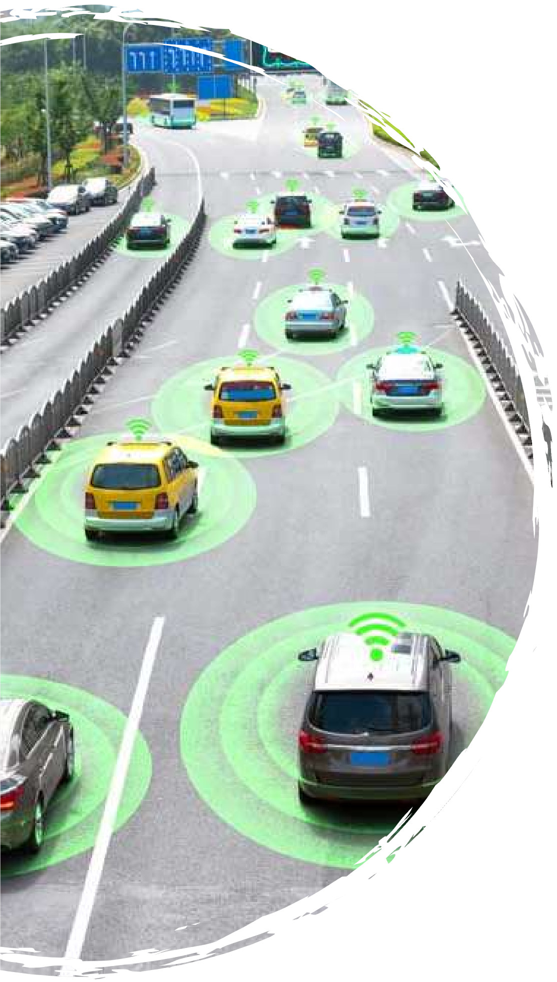
Exclusion:

- Declaring a recommendation or conditional provision as "not applicable"

Provisions of EN 303 645 are always assumed to apply

The template - the structure

Security Conference 2022



Provisions of EN 303 645 are always assumed to apply

Clause 4 (Reporting implementation):

- As per the EN

Clause 5 (Cyber security provisions for consumer IoT):

- Every provision from the EN with the possible application of one or more of the refinements

Clause 6 (Data protection provisions for consumer IoT):

- Every provision from the EN with the possible application of one or more of the refinements

Clause 7:

- New provisions specific to the vertical domain in the scope of clause 5

Clause 8:

- New provisions specific to the vertical domain in the scope of clause 6

How do we extend or add to EN 303 645?

- Base spec in EN 303 645 addresses only one user in IoT whereas an HG has multiple user roles. This is reflected in refining and extending Provision 5.1 as follows:
  - **Provision HG 5.1-1 (extended):** Where Wi-Fi® or administrator passwords are preconfigured in factory default, these preconfigured passwords shall be unique per HG.
  - **Provision HG 5.1-4 (extended) a:** HGs shall allow an administrator to set the Wi-Fi® password.
    Provision HG 5.1-4 (extended) b: The HG shall provide to the local administrator a simple mechanism to change the Wi-Fi® password.
  - **Provision HG 5.1-4 (extended) c:** The HG shall provide to an administrator a simple mechanism to change the administrator password (local to local, remote to remote).
  - **Provision HG 5.1-5 (refined):** The HG shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.
  - **Provision HG 7.1-1 (added):** The supply chain should be designed in such a way that leakage of the HG specific credentials is prevented.

How to decide on the form of deviation from the EN? (Examples from HG)

- The rationale for changes begins with a risk analysis that identifies the ways in which the vertical is not a simple IoT device
  - For the HG this is documented in TR 103 743
  - The template provides the algorithm for determination of the form of deviation
- Some vertical markets become complex because of their nature
  - For an HG this is from serving two distinct domains - the home network, the “internet”
  - For something like a smart-door-lock there are ethical concerns not always apparent for simple IoT devices (a constrained but mission critical decision)
  - In general, the IoT baseline with its 13 core principles can be seen to apply to any connected device or application

The next stage - test extension

- Taking the same approach of identifying the IoT base spec as the framework
- In the first round of development identifying critical extensions → for HG the changes in TS 103 848 leading to like for like changes and extensions over the baseline test spec of TS 103 701
    - For the HG this is being developed in ETSI work item CYBER/DTS-0066
    - As for the base spec the template provides the algorithm for determination of the form of deviation

In summary - slide 1 of 2

- The horizontal base spec has to be as broad as can be
  - The role of EN 303 645 is to be simple and broad
  - Reinforces security by default and privacy by design
- Clear rules for managing how to extend from horizontal to vertical specialisations

In summary - slide 2 of 2

- EN 303 645 provides a baseline for all connected devices with the 13 principles being appropriate to any connected device, or service
- “Vertical” specialisation takes account of the peculiarities of the “vertical” environment
  - For the HG the fact it acts as the trusted element spanning the home and the “internet”
  - For a smart door lock it links the physical locking function to the cyber locking function
  - For eHealth it links medical health with cyber health
- The “vertical” specialisation has to have rationale in a distinct sector analysis

Thank you for your attention

Follow us on:

Any (further) questions?

scott@cadzow.consulting