Security Conference 2022

The challenge in Moving from Horizontal Standards to Vertical Domains

Scott Cadzow, C3L UK

Alternative title

Security Conference 2022

Maximising the use of broad based standards without creating silos

A review of moving from EN 303 645 for IoT, to adopting EN 303 645 to a bit of everything

Security Conference 2022

- A summary of the session objectives
- 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

The session's objectives

Security Conference 2022

- Helping understand the cybersecurity challenges of some IoT vertical sectors
  - EN 62443 Certification. A growing Recognition in the Industry & Energy Ecosystems
  - ML Aided Lightweight Authentication for Internet of Vehicles Network
  - Traffic Data and Vehicles as IoT Sources

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

Security Conference 2022

Firstly, it offers a broad set of very simple principles

Secondly, if provides testing of the principles

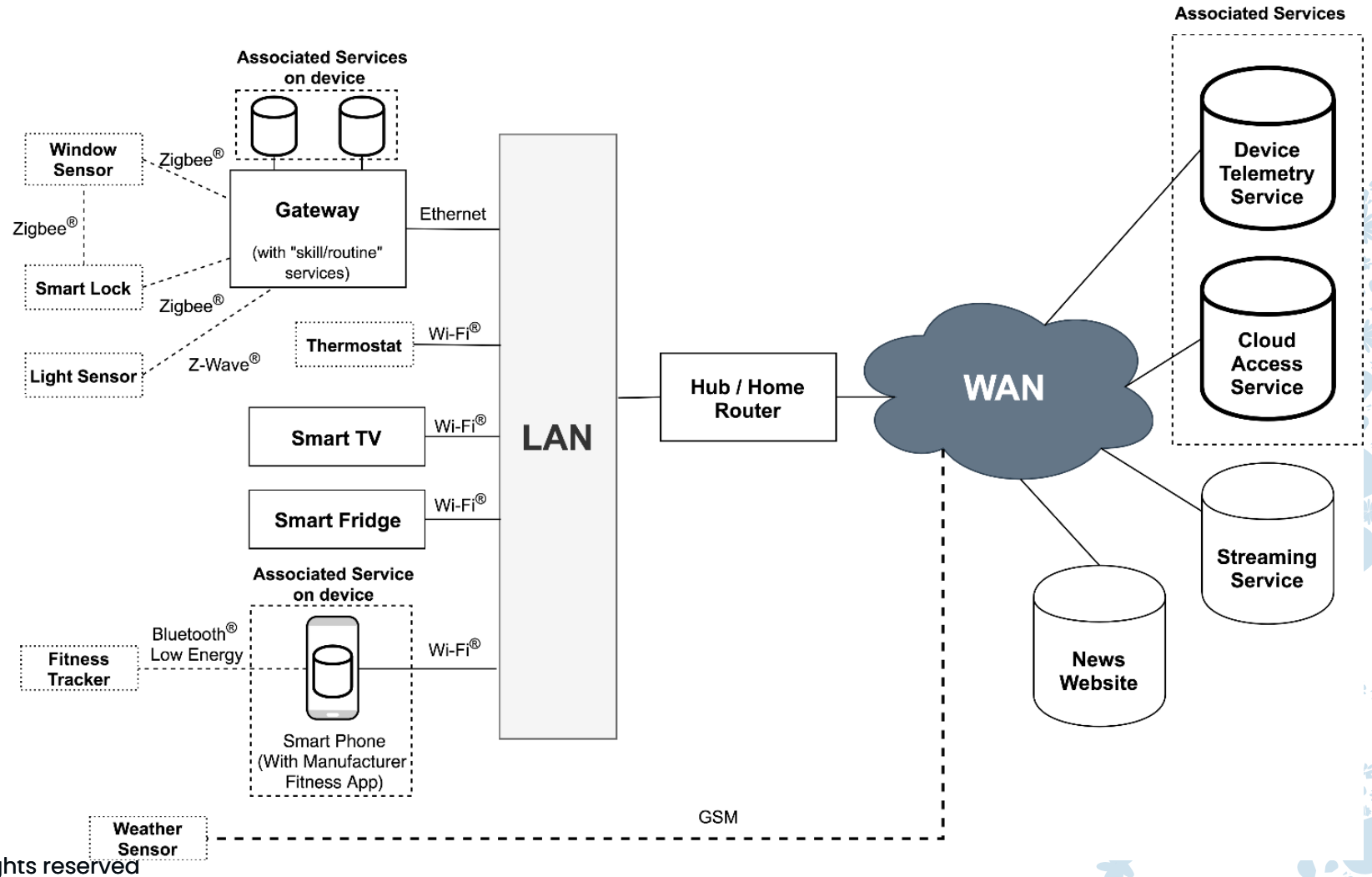
Thirdly, it supports the move to assurance as a root of proof of security attestations

Recommended approach to the definition of IoT Security requirements for Vertical use cases - Home Gateway

Security Conference 2022

- The base or foundation document
- The template – guidance to develop the HG spec.
- Developing the vertical domain spec. for HGs
- The test world and its foundation document
- The test and conformance HG spec.

The IoT scenario – things connected to each other through a network



The template – the basics

Provisions of EN 303 645 are always assumed to apply

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"

The template – the structure

Provisions of EN 303 645 are always assumed to apply

Clause 4:

- As per the EN

Clause 5:

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

Clause 6:

- 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:

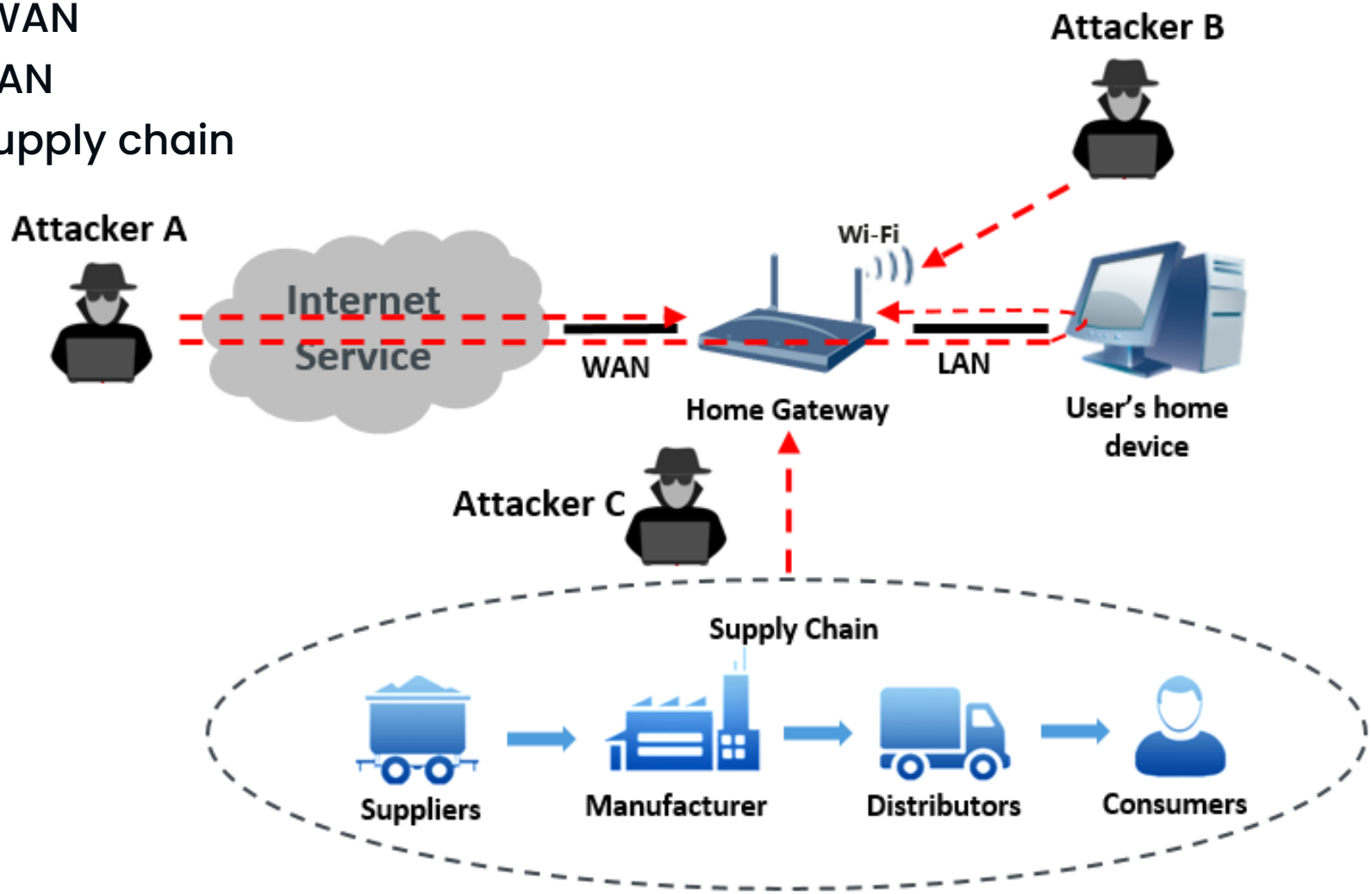
- New provisions specific to the vertical domain in the scope of clause 6

The Home Gateway specialisation

Security Conference 2022

Basic threat model and use cases explored in ETSI TR 03 743

- Attacker A on the WAN
- Attacker B on the LAN
- Attacker C in the supply chain



From the EN to TS 103 848

- The Home Gateway (HG) is not an IoT device as defined in EN 303 645, however, due to its generic character, EN 303 645 is appropriate as baseline for the HG.
- The HG is responsible for network management and is therefore subject to higher requirements than a consumer IoT device concerning the role of an administrator having a higher level of privilege than a user
- TS 103 848 has 18 extensions of EN 303 645, 5 refinements, 3 promotions, 2 exclusions, and 50 additions

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 extending Provision 7.1 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?

- The rationale for changes begins with a risk analysis that identifies the ways in which the HG 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 - HG test extension

- Taking the same approach of identifying the IoT base spec as the framework
- In the first round of development identifying critical extensions → 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

Security Conference 2022

- 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

- 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:

ETSI Security Conference 2022

Any (further) questions?

scott@cadzow.consulting