



PROVE & RUN

IoT Security

Christophe Pagezy, co-CEO

77, avenue Niel, 75017 Paris, France

contact@provenrun.com

IoT: the threats of remote attacks

Connected devices can be remotely controlled by hackers

All devices at once

Without warning signs

Without easy remediation



Allowing them to cause a lot of harm

Physical damage to users or surrounding equipment

Interruption of operations

First step for other attacks (botnet)



Hackers can leverage this to extort money from manufacturers

Their activity can be very profitable even for high initial investments (>\$1M) for designing attacks

IoT: the threats of remote attacks

Hackers are exploiting software bugs/errors, especially in the most complex part of the software stack (OS, communication stacks, etc)



How IoT security differs from IT security ?

- At least one of the embedded system will get into the hands of the hackers, be reversed engineered.
Flaws and weakness will be found.
- Standard security measures **will be much weaker** when applied on embedded systems,
- Multi-purpose and generic **processors that are used to replace electronic functions,** can when reprogrammed by hackers be extremely dangerous.

The Dismal State of IoT Security

A Hard and Hidden Issue

- Many people don't care
 - Security as externality
 - Not my problem!
- Many people don't get it
 - Cybersecurity \neq Safety
 - Cybersecurity $>$ Crypto
- We'll all get breached
 - Phishing, hacking, ...
 - Then, what happens?

A Late Addition

- IoT is growing fast
 - Connecting many things
 - Not always suited
- Hard for technologies
 - Linux can't follow
 - Many (un)known vulnerabilities
- No Trusted Computing Base
 - Too much trust in software
 - Not trustworthy, will break



How to answer to the challenge ?

A

Understand what is at stake :

- Conduct Security Analysis to understand the threats and define the **security requirements** for your IoT/connected devices

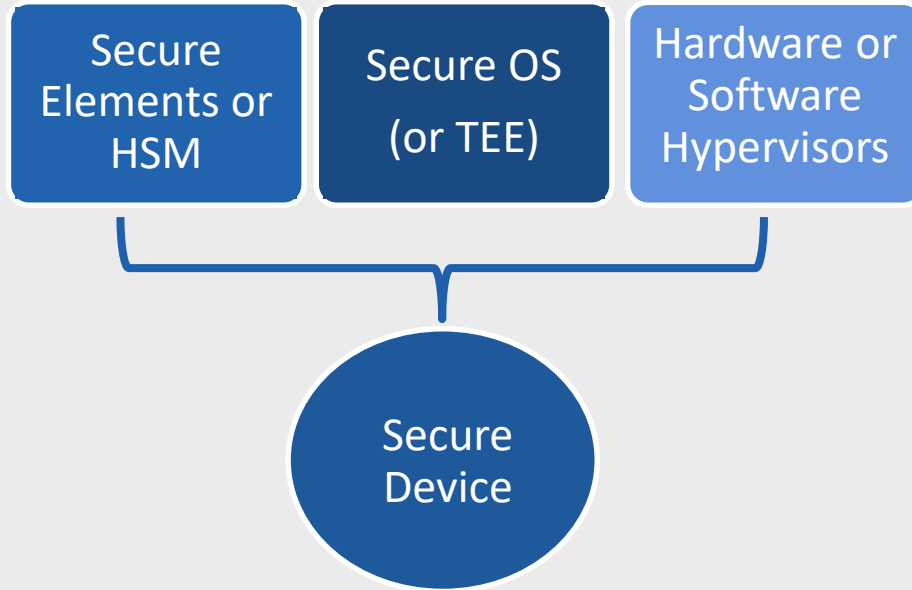
B

Secure-by-design connected devices:

- Security needs to be integrated at the design stage of the connected devices (**security-by-design**)
- Using state-of-the-art technologies

Technologies needed to secure devices

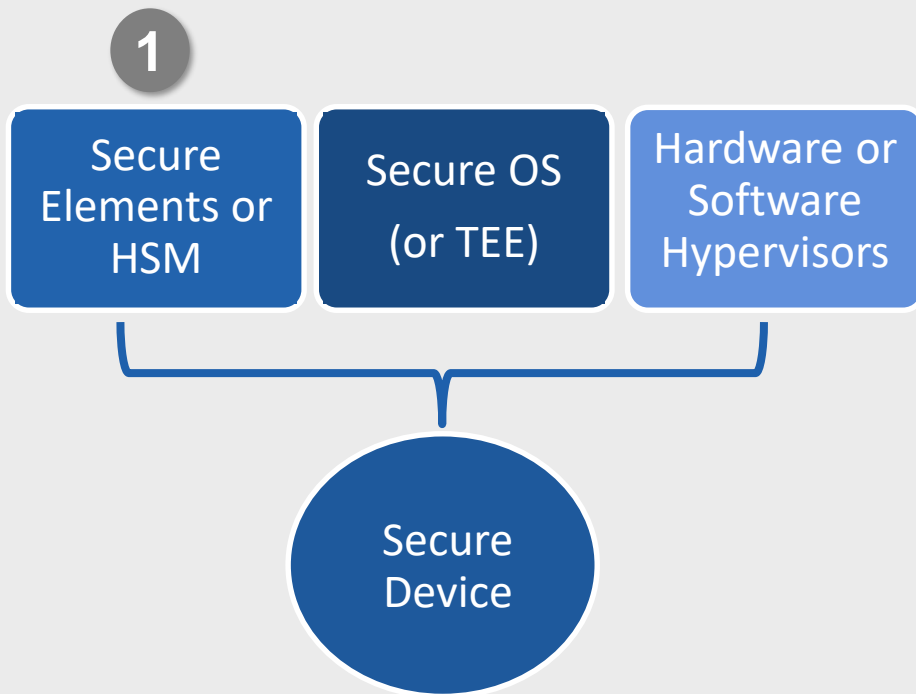
Security-by-design Toolbox



Depending on the security requirements security engineers need to use some or all of them

TEE: Trusted Execution Environment

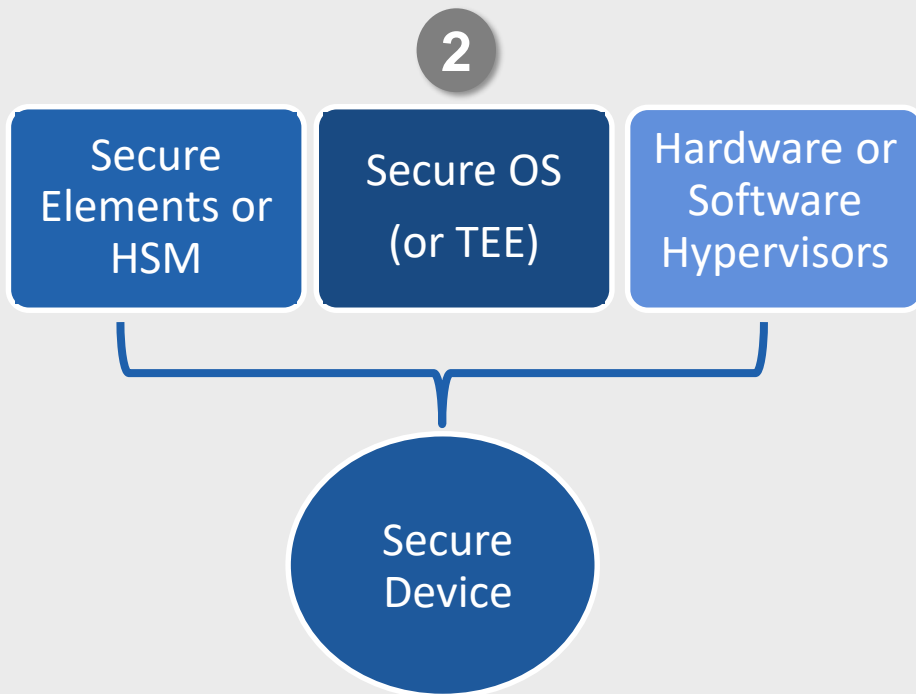
Technologies needed to secure devices



1

Useful for protecting keys and cryptographic operations. State-of-the-art solutions are **widely available on the market**

Technologies needed to secure devices

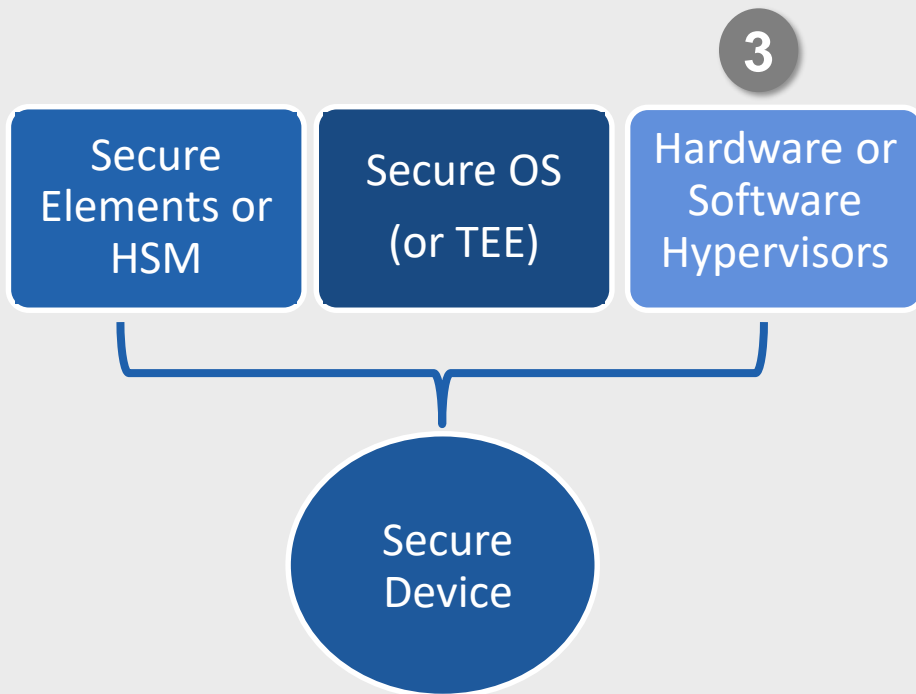


2

A secure OS is always needed to execute the security services (Firmware Update, IDS, Firewall/Filters, Key management, etc.). **Always part of the TCB**

TCB: Trusted Computing Base

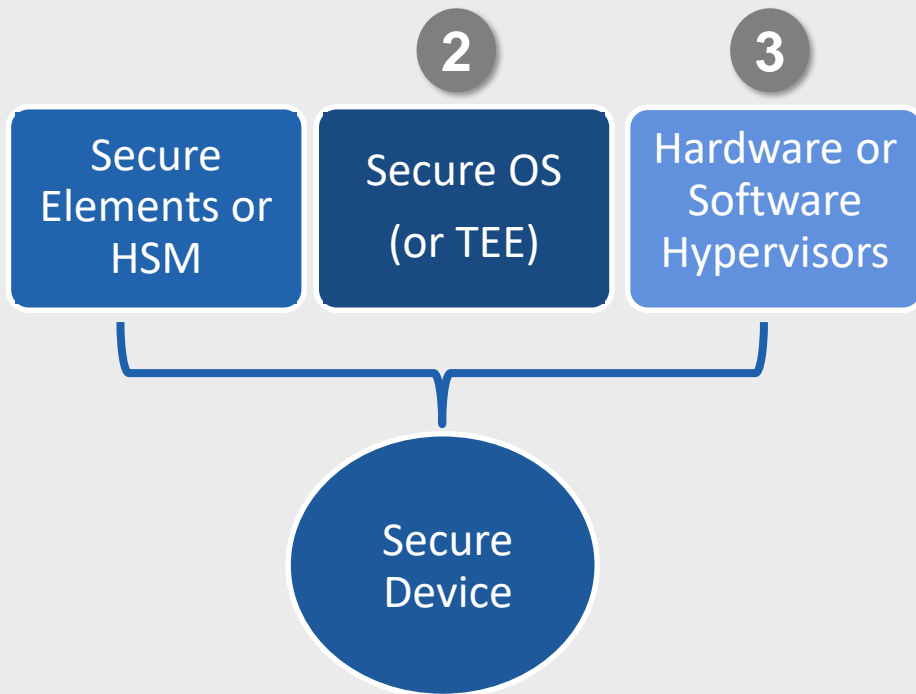
Technologies needed to secure devices



3

Hypervisors are useful to virtualize hardware or create virtual hardware isolation **but this does not remove the need of a secure OS**

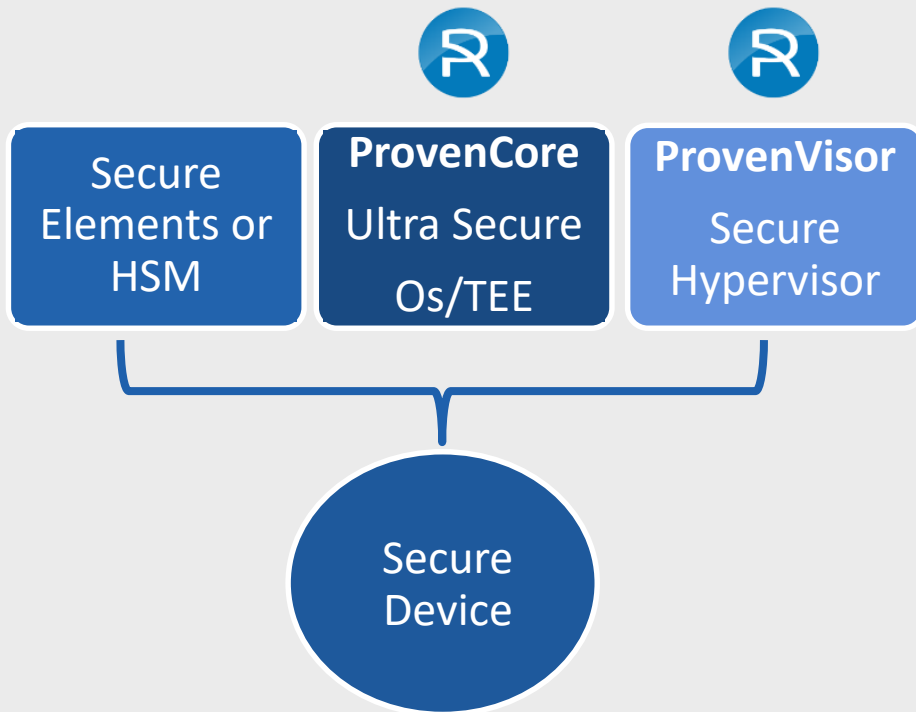
Technologies needed to secure devices




2 3

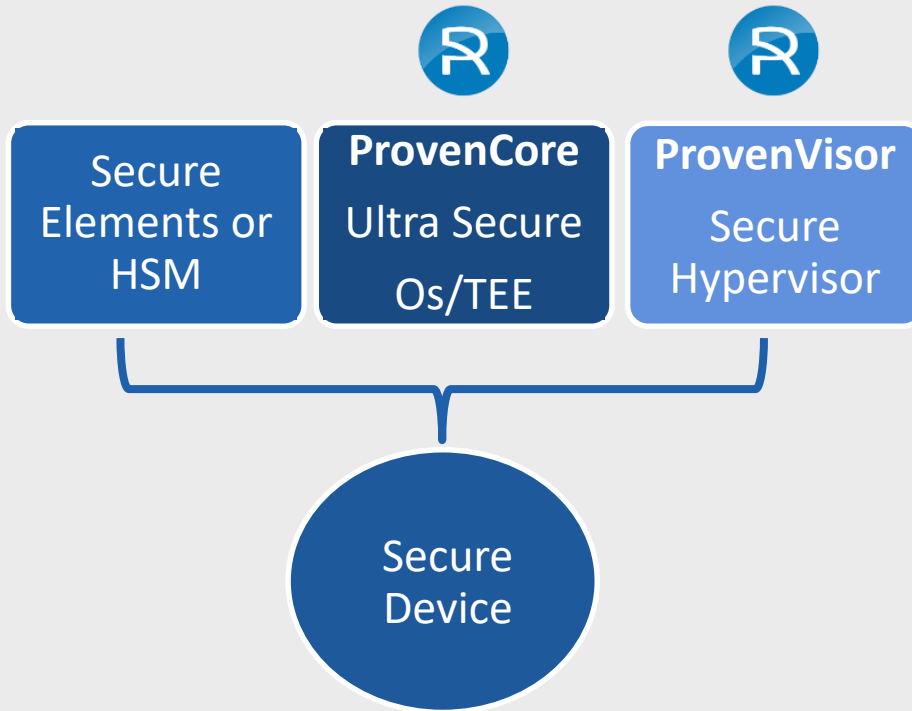
Traditional solutions available on the market **do not meet the security requirements** (too many bugs and vulnerabilities available to hackers)

Why ProvenCore and ProvenVisor ?



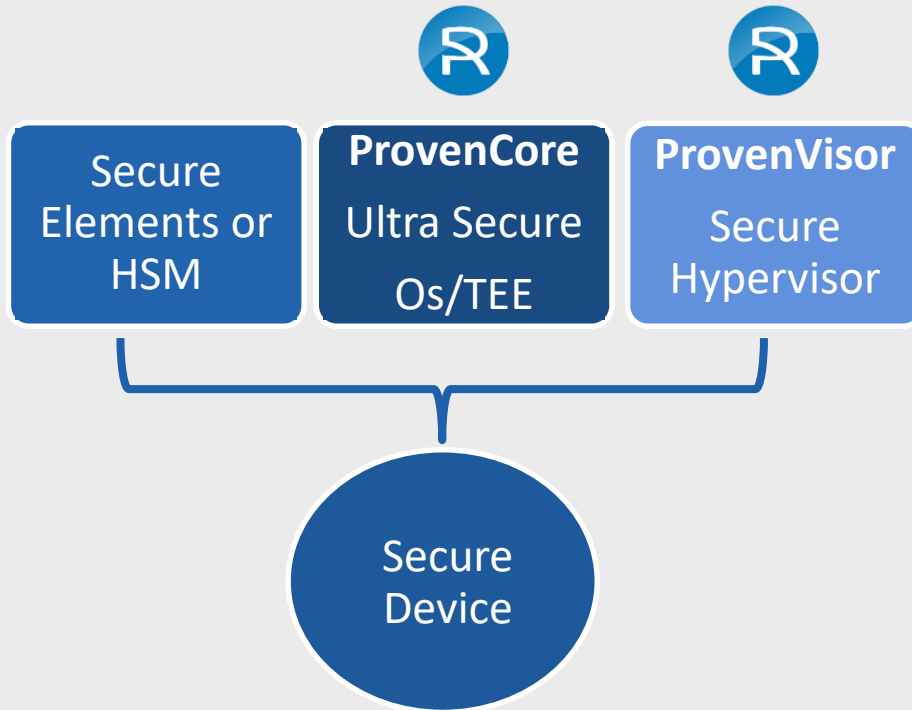

We developed **ProvenCore and ProvenVisor** to fill the gap, **embedding key security requirements in their design**

What is unique with ProvenCore/ProvenVisor ?



Key security properties and the most complex parts are **formally proven**, meaning they are **as close as possible to zero defaults**.

What is unique with ProvenCore/ProvenVisor ?




**No room left for
hackers to exploit
vulnerabilities**

Security: Certification is the final judge



ProvenCore Common Criteria EAL7 certified

This is a world première

There is no other TEE or Secure OS at that level of security

Why using a less Secure OS ?

Key benefits of ProvenCore & ProvenVisor ?

More Security

Resistance to the most sophisticated attacks

No certification uncertainty
(whatever the regulatory requirements)

Lower Costs

Reduced Cost of Ownership (superior code quality and maintainability)

Development of security services becomes simpler and cheaper

If you want to know more...

- Contact us
 - christophe.pagezy@provenrun.com
 - +33 6 21 01 62 18
 - www.provenrun.com



**Cost effective off-the-shelf software solutions
to protect connected systems against remote
cyberattacks**