THALES

Reconciling vulnerability response with certifications

U13b - ICMC16

May 19th, 2016

Fabien Deboyser

Agenda

Certification overview

- Why do we need security certification?
- A changing landscape

Security vulnerability

- Discovery of a security vulnerability in the product lifecycle
- Types of security vulnerability – operational phase

Assurance continuity

- Why do we need an efficient vulnerability response?
- Assurance continuity amongst certification schemes
- Challenges

Conclusion

- Opportunities for FIPS 140
- Open issue

THALES

Why do we need security certification?

Market requirement

Common approach and recognition

- Assess the security
- Provide a level of assurance

Under constraints

- Time-to-market, state-of the art

THALES

A changing landscape

New technologies: high-connectivity, permits field updates

- Internet of Things, everything is connected

Development processes are more flexible, better tools, more frequent releases

- Agile development process, static/dynamic tools for code review

Data protection is critical!

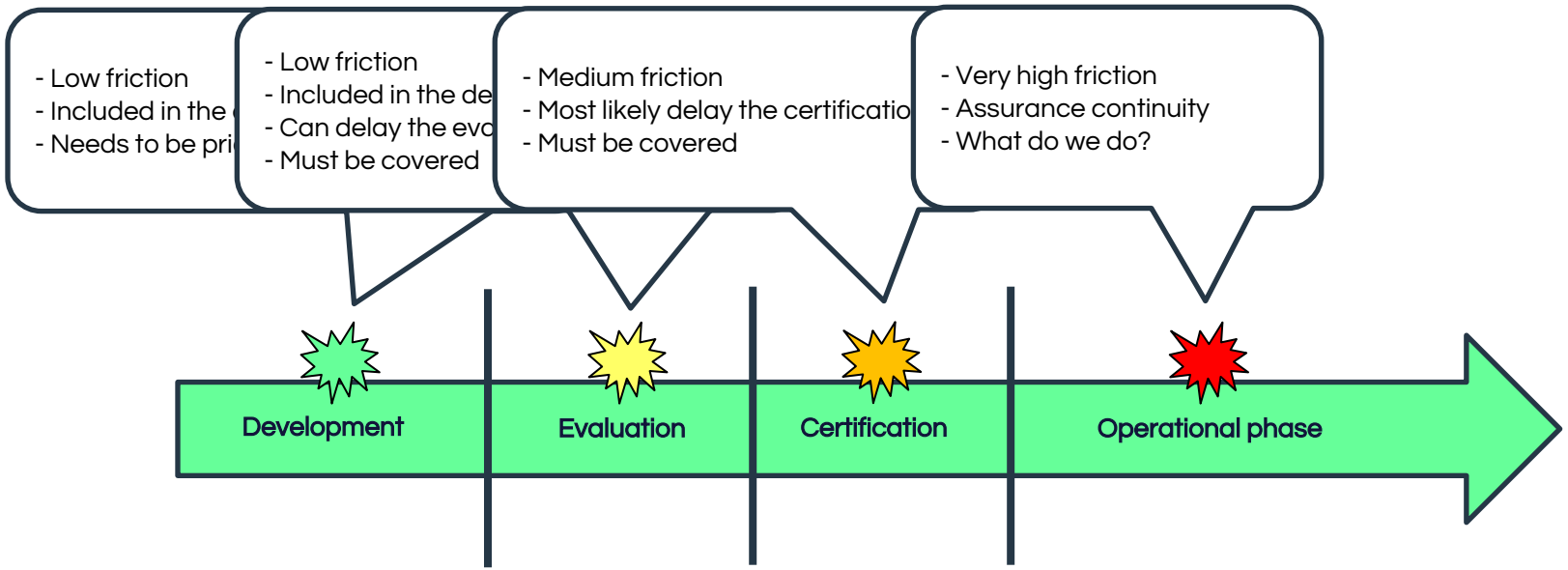
- Biometrics, payment information, merge between safety and security

Attacks are improving

- More connections, a lot to win, benefits from past experiences, tools

THALES

Discovery of a security vulnerability in the product lifecycle



THALES

Type of security vulnerability - operational phase

On a FIPS non-security relevant feature -> 1SUB

- Can still have an impact on security, eg buffer overflow
- Denial of Service

On a FIPS security relevant feature -> 3SUB

- Cryptographic algorithm, authentication method
- Product has a security breach, can be mitigated by some rules or requires an update

Most likely, patch or update

- Will consist of a very tiny modification
- Is necessary and time-critical

THALES

Why do we need an efficient vulnerability response?

To correct a known security vulnerability (public or internal)

- Having a secure product, efficiently protected
- Responsibility of the developer to the customer, reputation of the company

Time efficient

- Reduce the risk that the vulnerability is exploited
- Reduce the time of exposure

THALES

Assurance continuity amongst certification scheme

FIPS 140-2

- 1SUB if the fix is a non security relevant feature, otherwise 3SUB
- 3SUB, heavy process and long, similar as a recertification
- Security update must first be certified, in the meantime non-FIPS certified

Common Criteria

- Scheme dependent – UKSP01 Assurance continuity, ANSSI CC note 6 & MAI/P/01, …
- Impact Analysis Report from the developer + Report from the lab on the impact
- Security update must first be certified, in the meantime non-CC certified

PCI

- PTS Program Guide v1.5
- Process for dealing with Security breach or compromise
- Developers must inform and work with PCI lab to mitigate or prevent further security breach or compromise
- Continuity of the certification - 24th hour turnaround

THALES

Challenges

- Disclosure of known security issues
- Releases are delayed until certification is obtained
- Release is made but some customer's won't or can't upgrade until certification is obtained
- Latest version more secure than the certified version
  - Ignore certification status? As certified versions are known to be less secure than the latest version

THALES

Improving FIPS 140

Dedicated process for security vulnerabilities

- Distinct from 3SUB-recertification and 1SUB
- Time efficient to reduce the impact of the vulnerability

Update package

- Impact Analysis Report, produced by the vendor
- Standardized approach based on a template

What does the laboratory need to produce?

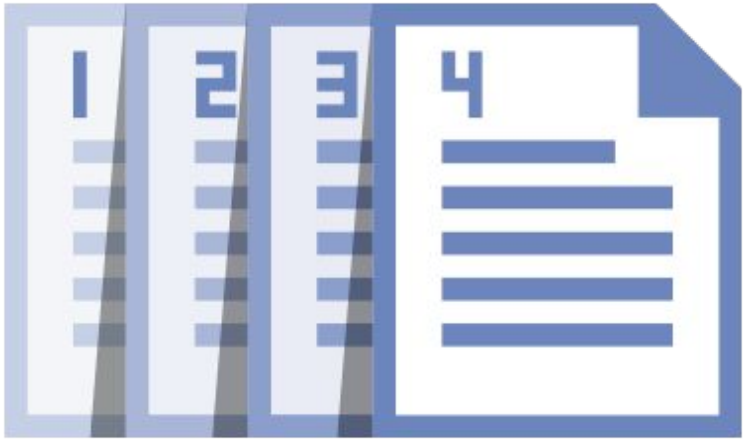
- Something light and efficient!
- Ideally the Impact Analysis Report (with comments?)
- Labs are accredited!!

THALES

Product versioning: Open question

Product versioning

- How to manage the certificates for product versions that are susceptible to a security vulnerability?
- What about users that are not impacted?



THALES

Thank You

Fabien Deboyser
Certification Engineer
Thales e-Security

fabien.deboyser@thalesesec.com
+1 954-302-6564

THALES