Toward Continuous Certification

International Cryptographic Module Conference
May 19, 2017
Washington, DC

Lightship Security

What is “Continuous Certification”?

“Certification at the speed of development”

Motivations - Certifications

Certification results are consistently inconsistent

Existing certification processes are too slow, costly and impractical

Motivations - Developers

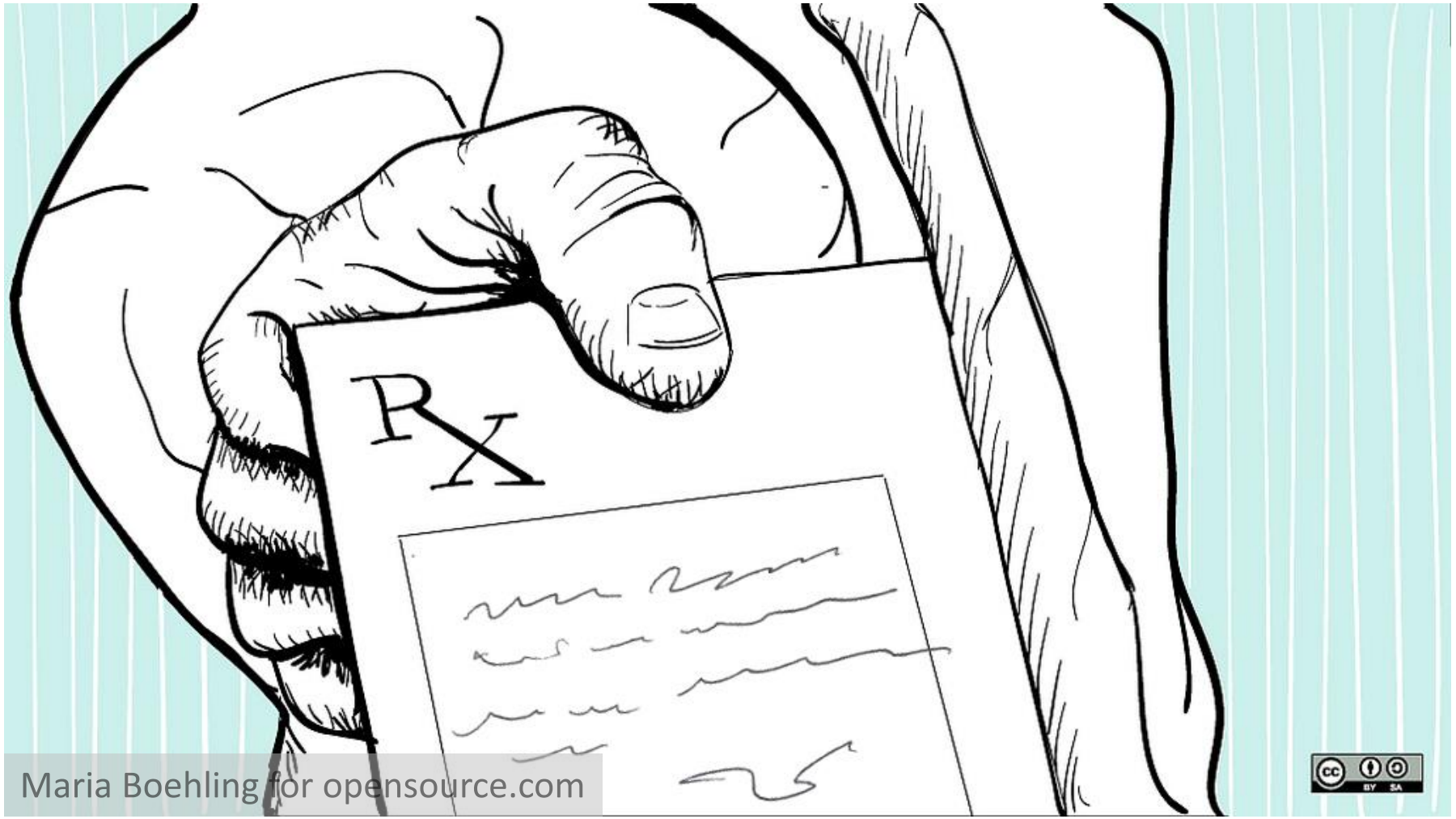
Innovation in development releases

Continuous integration
Continuous testing
Continuous delivery

Lack of innovation in certification

Better suited to waterfall model of development
Requires custom documentation
Unfriendly to ever-evolving software

Evolution of Common Criteria



Maria Boehling for opensource.com

Example: Testing TLS

- "Old" CC way:

  "Thou shalt use TLS to protect a channel from modification and disclosure."

  …document what you do…

  …and test however you wish.

- "New" CC PP way:

  "Thou shalt only allow and use the following TLS versions and ciphersuites and follow RFC(s) *xxxx*; thou shalt allow RSA, DHE and ECDHE key exchange mechanisms; thou shalt only allow the following EC curves; thou shalt use X.509 certificates in the following ways…"

  Oh, and by the way, here's the 25+ specific tests you must execute and pass…

Painting the Picture

Start with an engaged and educated vendor

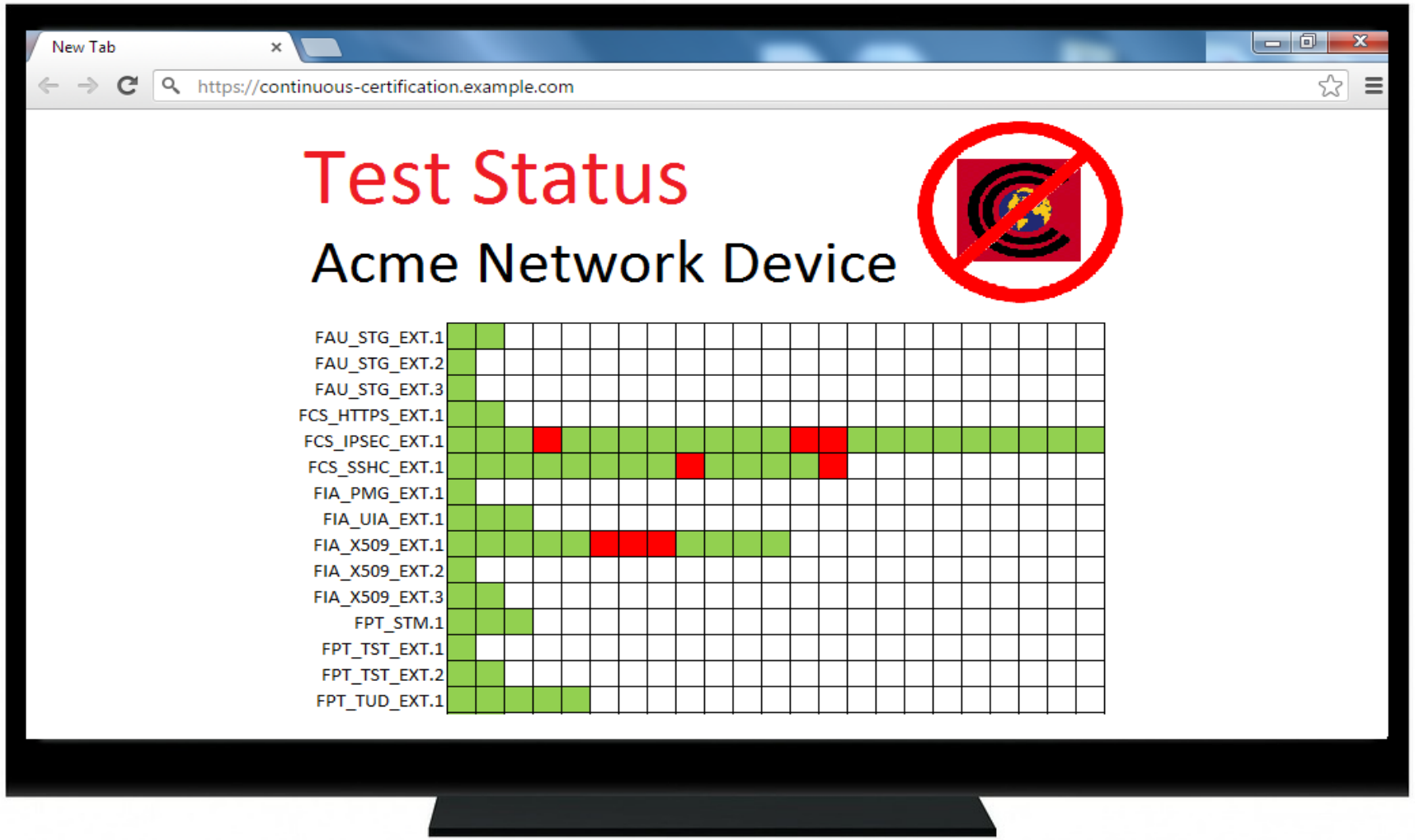
Work with a prescriptive standard

(Abstracting Tests in Prescriptive Standards)

- Test requirement is abstracted from underlying implementation

- (Simple) Example FPT_STM_EXT.1:

"Test 1: If the TOE supports direct setting of the time by the Security Administrator then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly."


New Tab
https://continuous-certification.example.com
Test Status
Acme Network Device
FAU_STG_EXT.1
FAU_STG_EXT.2
FAU_STG_EXT.3
FCS_HTTPS_EXT.1
FCS_IPSEC_EXT.1
FCS_SSHC_EXT.1
FIA_PMG_EXT.1
FIA_UIA_EXT.1
FIA_X509_EXT.1
FIA_X509_EXT.2
FIA_X509_EXT.3
FPT_STM.1
FPT_TST_EXT.1
FPT_TST_EXT.2
FPT_TUD_EXT.1

- Trust gained by lab and scheme re: vendor's results and processes
- As trust grows, QA results can lead to faster and faster evaluation cycles
- Eventually, trust can lead to direct submissions

Challenges

- Resource constraints of parties
- Trust in testing and integrity of results
- Ongoing role of independent third parties
- Evolving standards
- Issues with assurance activities
- International acceptance

Example Certification Industry Innovations

- Common Criteria Protection Profiles
  - Small baseline technology-specific functional requirement templates
  - Evolution to prescriptive testing
  - Time-constrained evaluations
  - NIAP allows security patching (an acknowledgement of the challenge)
- NIST's Automated Cryptographic Validation Protocol (ACVP)
  - Direct submissions of algorithm validations
- France's ANSSI CSPN
  - Short-term time-constrained practical functional/pen testing-based assurance

Thank you

Automation good

Walk among network racks as

Certified lights blink

(Burma shave)

Lightship Security

info@lightshipsec.com