

Towards more transparent security certifications - mining Common Criteria and FIPS140-2 certificates

This webinar, organised by CyberSec4Europe took place on 19 February 2021 at 11:00 CET and was presented by Petr Švenda, Ph.D. The recording of the event is now available online.



CyberSec4Europe

The security certification reports might be long but are also a trove of publicly available data about otherwise proprietary devices and other products otherwise available only under NDA. While downloading and reading a single certificate is easy, reasoning about the whole ecosystem's characteristics now with more than ten thousand certified devices based on human-written documents is different. Are there observable systematic differences between the Common Criteria and FIPS140-2 certificates? Can I quickly find if my device is using a certified component recently found vulnerable? And most importantly, can we measure and quantify if the whole process is actually increasing the security of the products being certificated?

The webinar presented a data-based insight into certification ecosystems with a tool developed in the CyberSec4Europe project (SecCert).

Petr Švenda is an Associate Professor at the Masaryk University, Czech Republic. He dreams about a more open and transparent world of cryptographic smartcards. Then tries to make this dream true by developing open tools for assessment of implementation security, occasionally finding some vulnerabilities in certified devices like ROCA (CVE-2017-15361) or Minerva (CVE-2019-15809).

More information

Recording of the webinar

Related topics

Cybersecurity

Strengthening trust and security

Source URL:

<https://digital-strategy.ec.europa.eu/library/towards-more-transparent-security-certifications-mining-common-criteria-and-fips140-2-certificates>