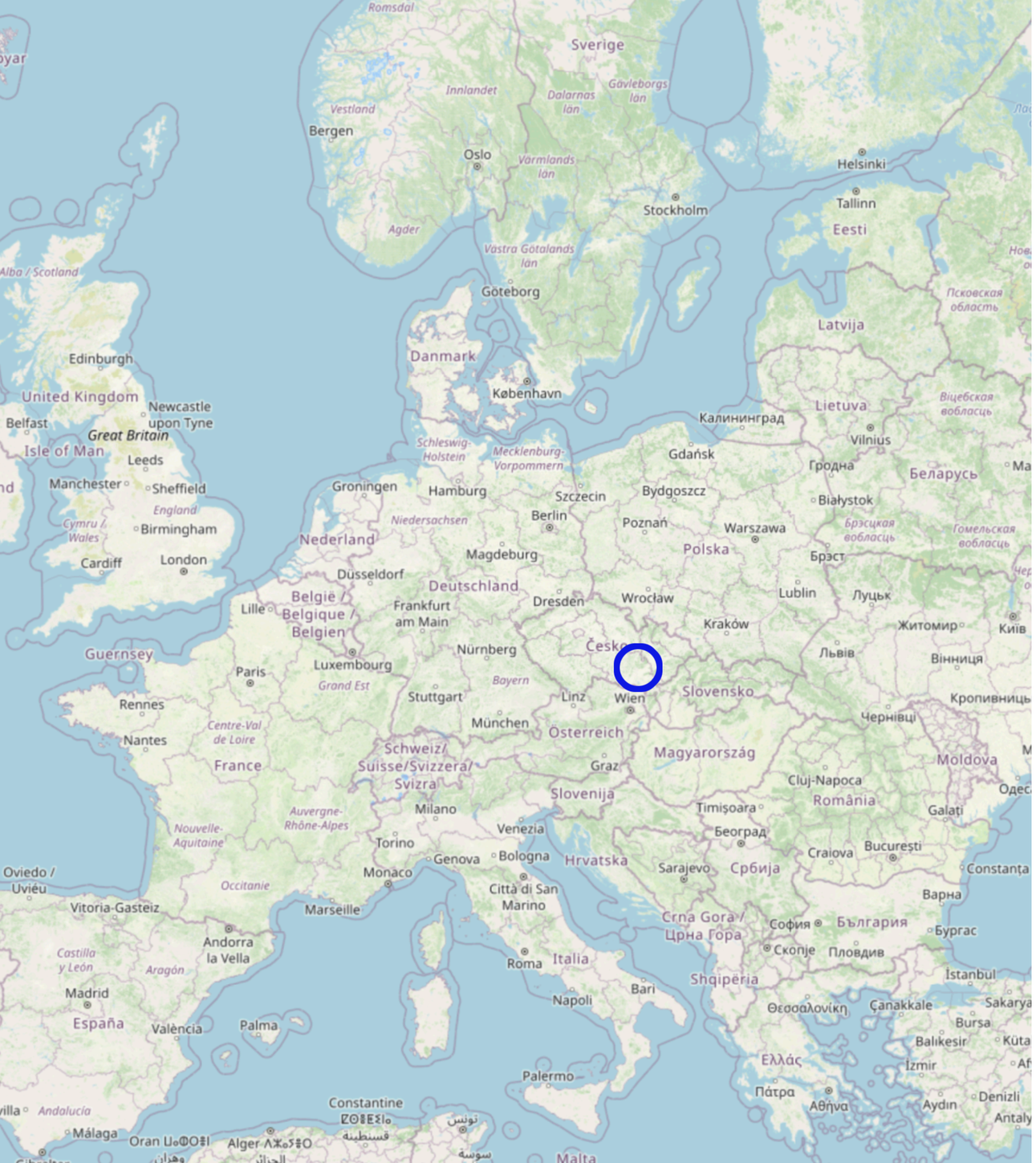
MUNI
FI

Insights from Automated Large-Scale Analysis of FIPS 140 Certificates

International Cryptographic Module Conference
San Jose, 2024

Adam Janovsky | adamjanovsky@mail.muni.cz



MUNI

CROCS

Centre for Research on Cryptography and Security

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*

Matus Nemec
Masaryk University,
Ca' Foscari University of Venice
mnemec@mail.muni.cz

Marek Sys†
Masaryk University
syso@fi.muni.cz

Petr Svenda
Masaryk University
svenda@fi.muni.cz

Dusan Klinec
EnigmaBridge, Masaryk University
dusan@enigmabridge.com

Vashek Matyas
Masaryk University
matyas@fi.muni.cz

What (if any) certified devices are affected?

sec-certs.org

Search

Search and browse through certificates and extracted metadata.

Analysis

View our analysis of the certification landscape.

References

Explore interactive reference graph of FIPS-certified devices.

Vulnerabilities

Display existing vulnerabilities in certified products.

Cryptographic Module for Intel® Converged Security and Manageability Engine (CSME)

Certificate #4158

Webpage information ?

Status	active
Validation dates	17.02.2022 , 21.08.2023
Sunset date	21-09-2026
Standard	FIPS 140-2
Security level	1
Type	Firmware-Hybrid
Embodiment	Multi-Chip Stand Alone
Caveat	When operated in FIPS mode
Description	The Cryptographic Module for Intel® Converged Security and Manageability Engine(CSME) (hereafter referred to as 'the module') is classified as a multiple-chip standalone firmware-hybrid module for FIPS 140-2 purpose. The module consists of both hardware and firmware. The hardware portion is the Converged Security Engine (CSE) and the firmware portion is the crypto driver process of the Manageability Engine (ME). The two portions form the logical cryptographic boundary and they combine as Converged Security and Manageability Engine (CSME) to perform cryptographic functions within the Cannon Point PCH applications executing on the CSME.
Version (Hardware)	3.0
Version (Firmware)	2.5 and 2.6
Tested configurations	• embedded IA-32 dedicated to support the functionality of the CSME firmware version 12.0.70.1652 running on Cannon Point PCH with Intel Whiskey Lake with device firmware version 12.0.70.1652 • embedded IA-32 dedicated to support the functionality of the CSME firmware version 12.0.70.1652 running on Intel Cannon Point PCH with Intel Coffee Lake with device firmware version 12.0.70.1652
Vendor	Intel Corporation
References	This certificate's webpage directly references 0 certificates, transitively this expands into 0 certificates.

Certificate Webpage

Security policy

Security target | PDF | TXT

Cryptography

Symmetric Algorithms

AES, AES-256, RC4, TDEA, SM4, HMAC, HMAC-SHA-256, HMAC-SHA-512, CMAC

Asymmetric Algorithms

RSA-OAEP, ECDH, ECDSA, ECC, Diffie-Hellman, DH

Hash functions

SHA-1, SHA-256, SHA-224, SHA-384, SHA-512, MD5, PBKDF

Schemes

MAC, Key Agreement

Randomness

TRNG, DRBG

Elliptic Curves

P-256, P-384, P-224, P-521, NIST P-224

Block cipher modes

ECB, CBC, CTR, OFB, GCM

Device

Security

Other

Updates

- 04.07.2024 The certificate data changed. + Show diff

Certificate changed

The web extraction data was updated.

- The module_type property was set to `Firmware-Hybrid`.

- 18.09.2023 The certificate data changed. + Show diff

Certificate changed

The web extraction data was updated.

- The validation_history property was updated, with the `[[1, {'_type': 'sec_certs.sample.fips.FIPSCertificate.ValidationHistoryEntry', 'date': '2023-08-21', 'validation_type': 'Update', 'lab': 'ATSEC INFORMATION SECURITY CORP'}]]` values inserted.
- The fw_versions property was set to `2.5 and 2.6`.

The PDF extraction data was updated.

- The keywords property was updated, with the `{'fips_certlike': {'__update__': {'Certlike': {'__delete__': ['AES1']}}}}` data.
- The policy_metadata property was updated, with the `{'pdf_file_size_bytes': 611387, '/Title': 'FIPS 140-2 Non-Proprietary Security Policy', '/Creator': 'Microsoft Word', '/CreationDate': "D:20230710181745+00'00'", '/ModDate': "D:20230710181745+00'00'", 'pdf_hyperlinks': {'_type': 'Set', 'elements': ['https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-56b.pdf', 'https://platformsw.intel.com/']}}` data.

The computed heuristics were updated.

- The extracted_versions property was updated, with the `{'_type': 'Set', 'elements': ['2.5', '2.6']}` values added.

The state was updated.

- The policy_pdf_hash property was set to `4b0fb0ed8154ed1da2eb798d6db3986662a35d7e7ce08815c5ff1c4a6ca0987d`.
- The policy_txt_hash property was set to `fea13655d938d42ffd4fb1ffc91d18bdf64dfe0e070668eca893d3deb4b8422f`.

Full-text search

- Full-text search over certification artifacts.
- Can be used to mine suspicious phrases.
- Great for assessing vulnerability impact 👍.

EUCLEAK

Side-Channel Attack on the YubiKey 5 Series

(Revealing and Breaking Infineon ECDSA Implementation on the Way)

Thomas ROCHE

All of these CC certificates are public and come along with public security target and certification report documents that contains valuable information about the chip and firmware versions. Furthermore, the BSI has a quite nice database search engine [5] that helps in finding the different documents. We also must mention the great SEC-CERTS initiative [13, 12] that ended up in a powerful CC documents search engine [6].

FIPS 140

Fulltext search

Query

hard-coded in the module

Search | Display network | Advanced options

Search certificate reports and security policies. Supports the Whoosh query language.

Took 0.227 seconds

found **2** records, displaying **1 - 20**

#4187	Aviat Networks Eclipse Cryptographic Module	Security Policy	active

Integrity key A fixed and **hard coded** key used in the firmware load conditional

The cryptographic boundary of the **module** is the hardware chassis. The **module** is a hardware **module** with firmware running on the NCC card within

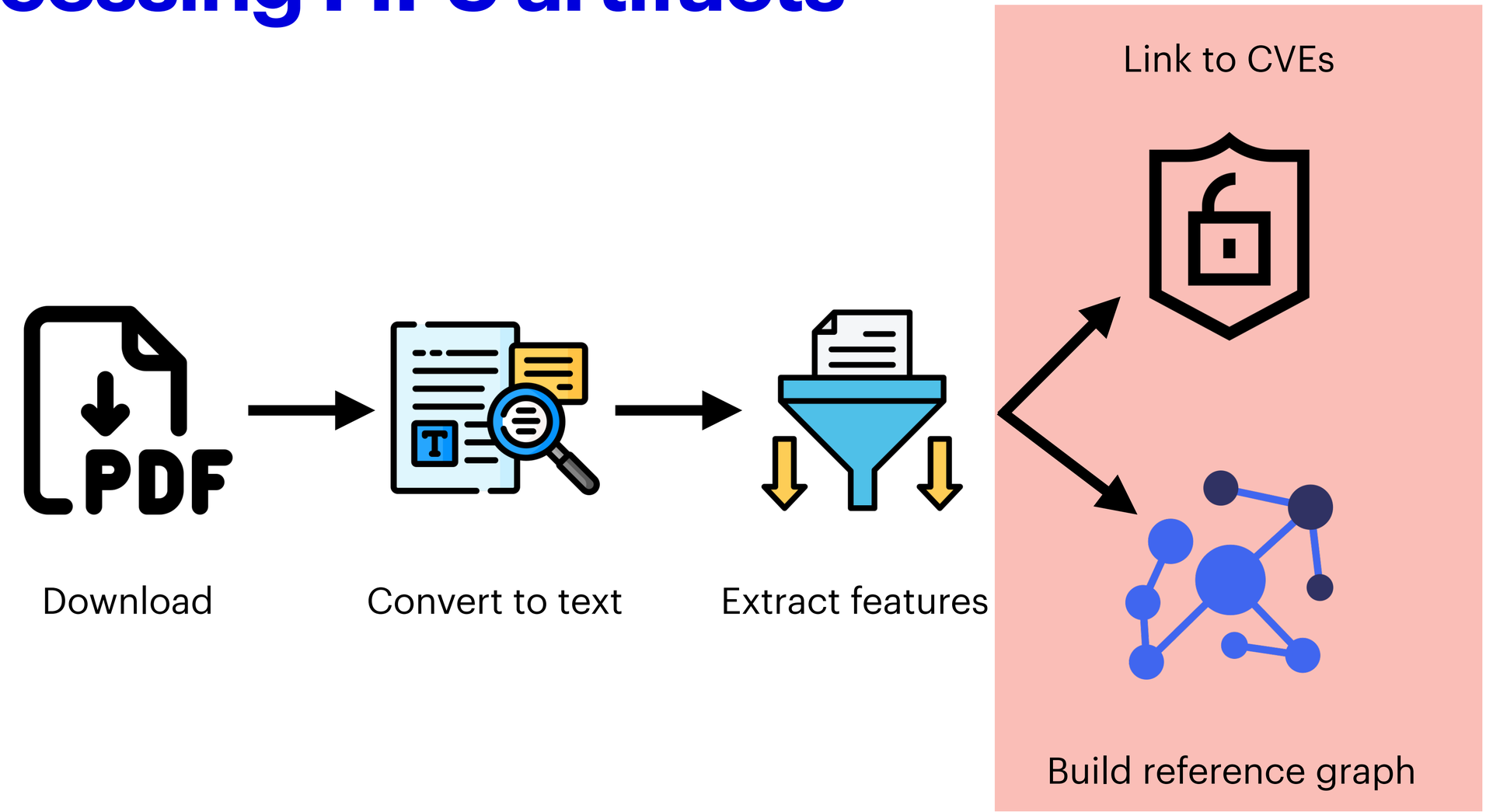
the firmware loads the new image into **module** and reboots the **module** to allow the new firmware to become operational

sec-certs Python API

```
dataset = FIPSDataset.from_web_latest()
print(f"The loaded FIPSDataset contains {len(dataset)} certificates")

>>>> Downloading FIPS Dataset: 60.5MB [00:37, 1.69MB/s]
>>>> The loaded FIPSDataset contains 4758 certificates
```

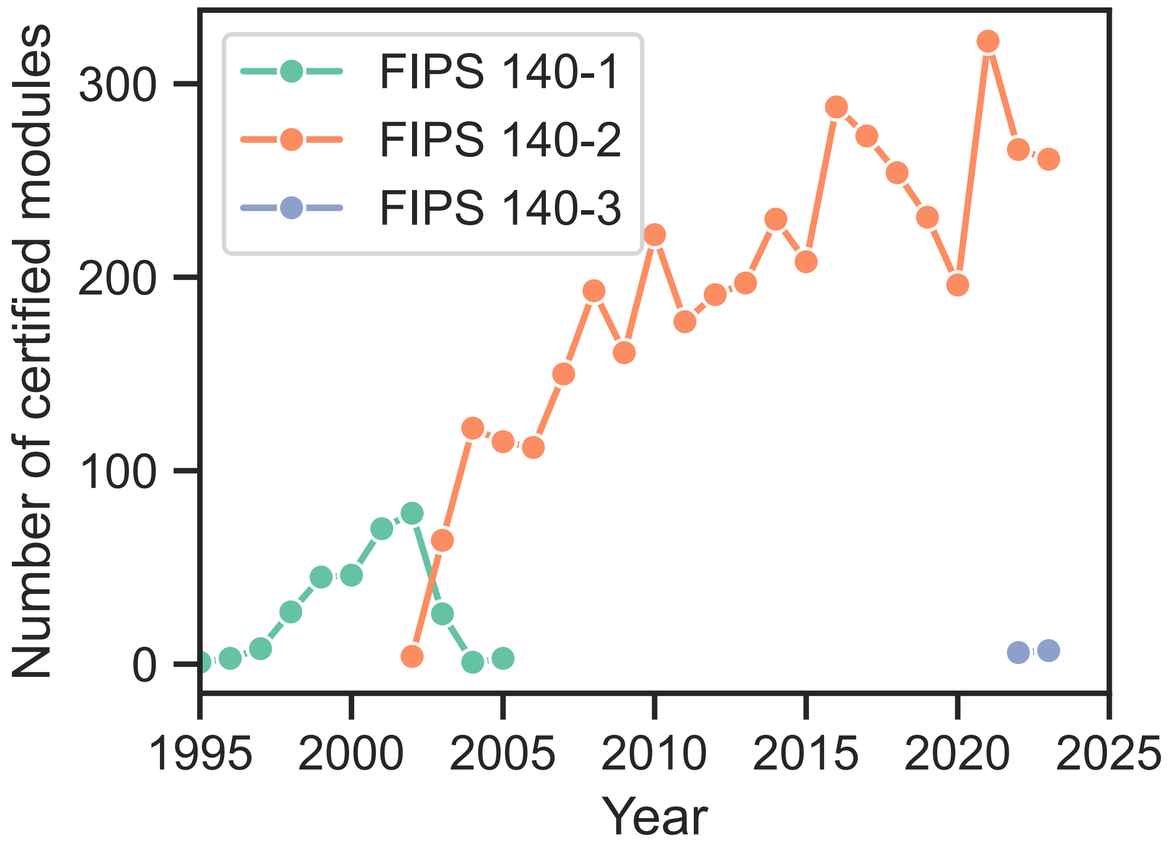
```
df = dataset.to_pandas()

# Get only certs from the last three years
last_three_years = df.loc[df.date_validation > pd.Timestamp("2021-01-01")]
print(f"Number of certs since 2021-01-01: {last_three_years.shape[0]}")

# Get only the FIPS 140-3 certs
fips_140_3 = df.loc[df.standard == "FIPS 140-3"]
print(f"Number of FIPS 140-3 certs: {fips_140_3.shape[0]}")

# Show statistics about security levels
df.level.describe()

>>>> Number of certs since 2021-01-01: 977
>>>> Number of FIPS 140-3 certs: 79

>>>> count    4757.000000
>>>> mean        1.667858
>>>> std         0.733841
>>>> min         1.000000
>>>> 25%         1.000000
>>>> 50%         2.000000
>>>> 75%         2.000000
>>>> max         4.000000
```

Processing FIPS artifacts

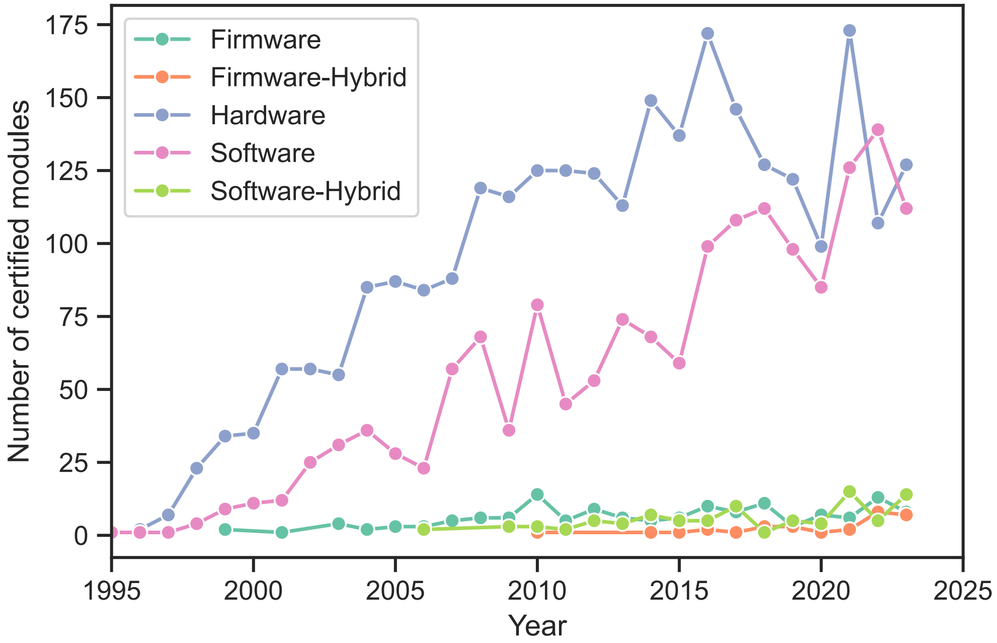


Ecosystem insights 🚀

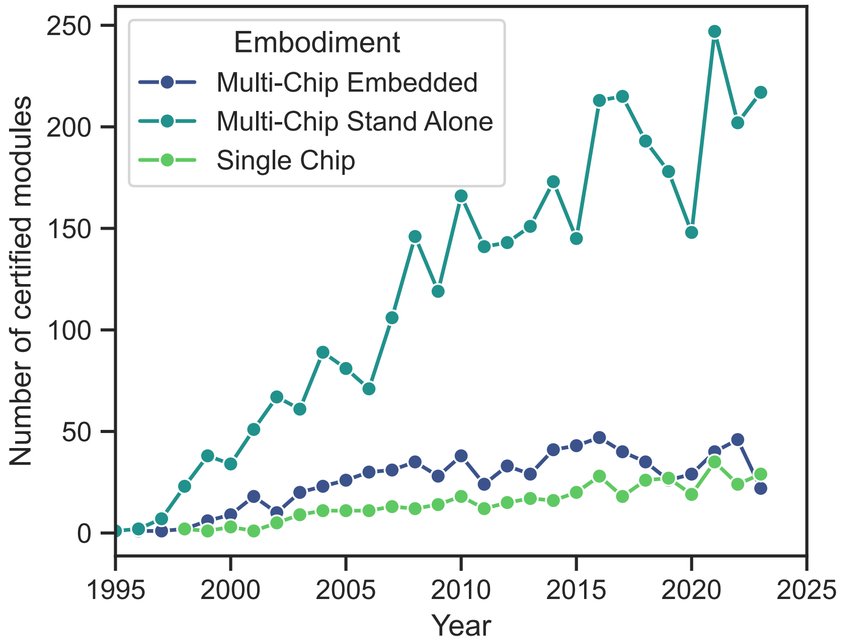
Number of yearly certified modules



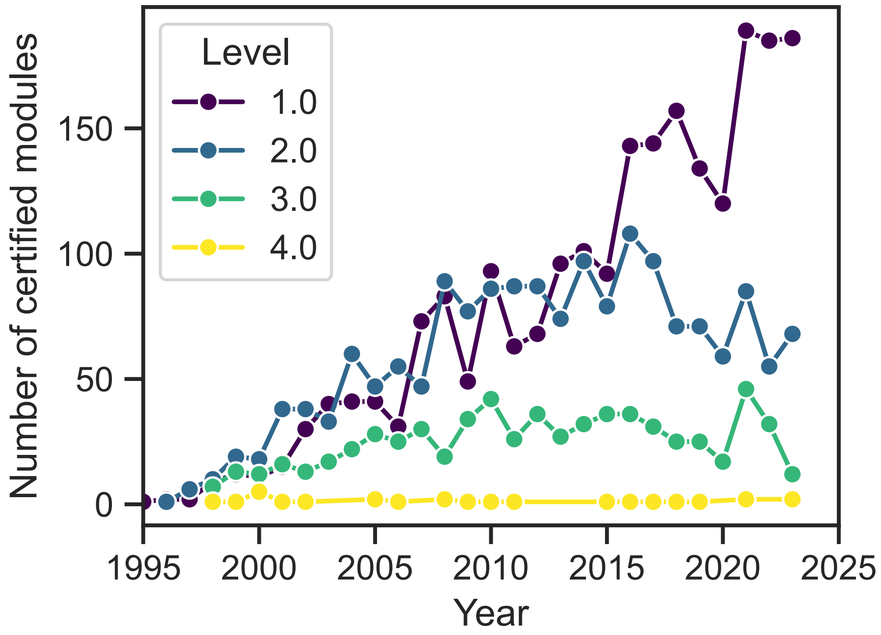
Different module types



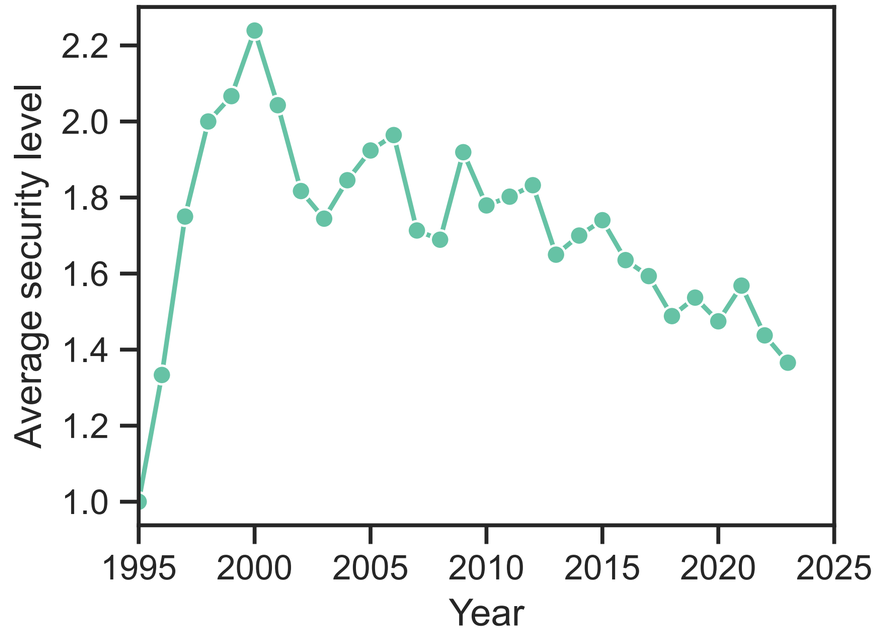
Different embodiements



Security levels popularity



Average security level



Certification progress monitoring

Implementations under test (IUT)

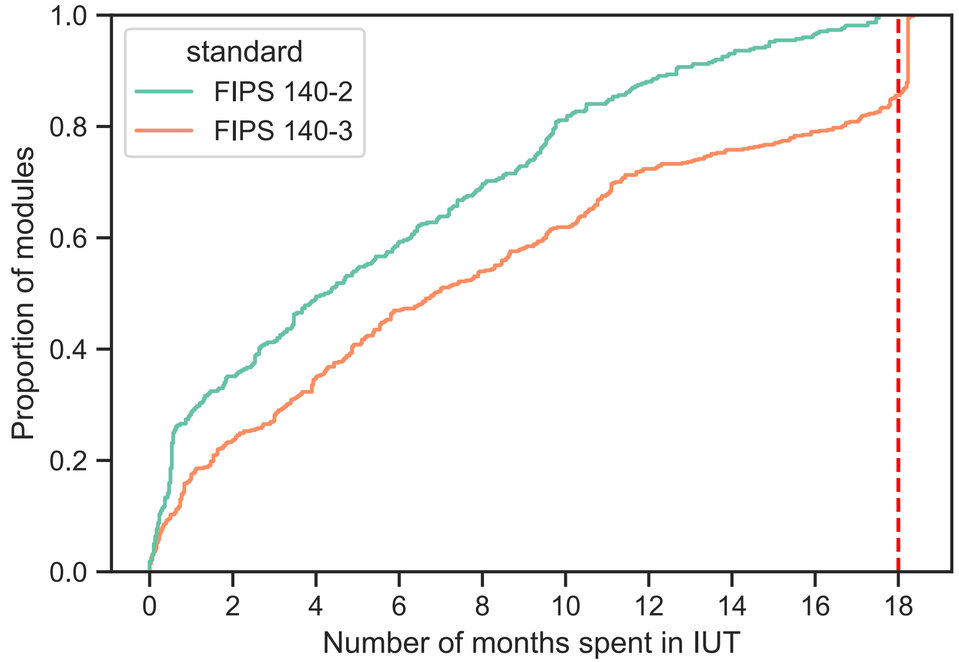
> *The IUT list is provided as a marketing service for vendors who have a viable contract with an accredited laboratory for the testing of cryptographic module.*

Modules in process (MIP)

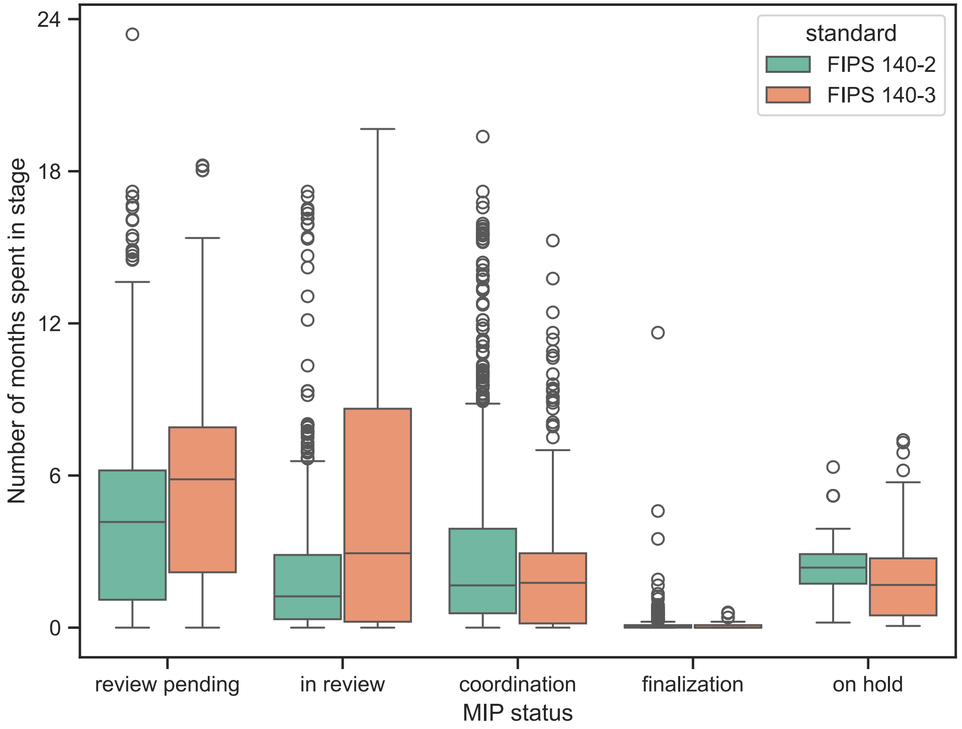
> *The MIP list contains cryptographic modules on which the CMVP is actively working.*

- On hold
- Review pending
- In Review
- Coordination
- Finalization

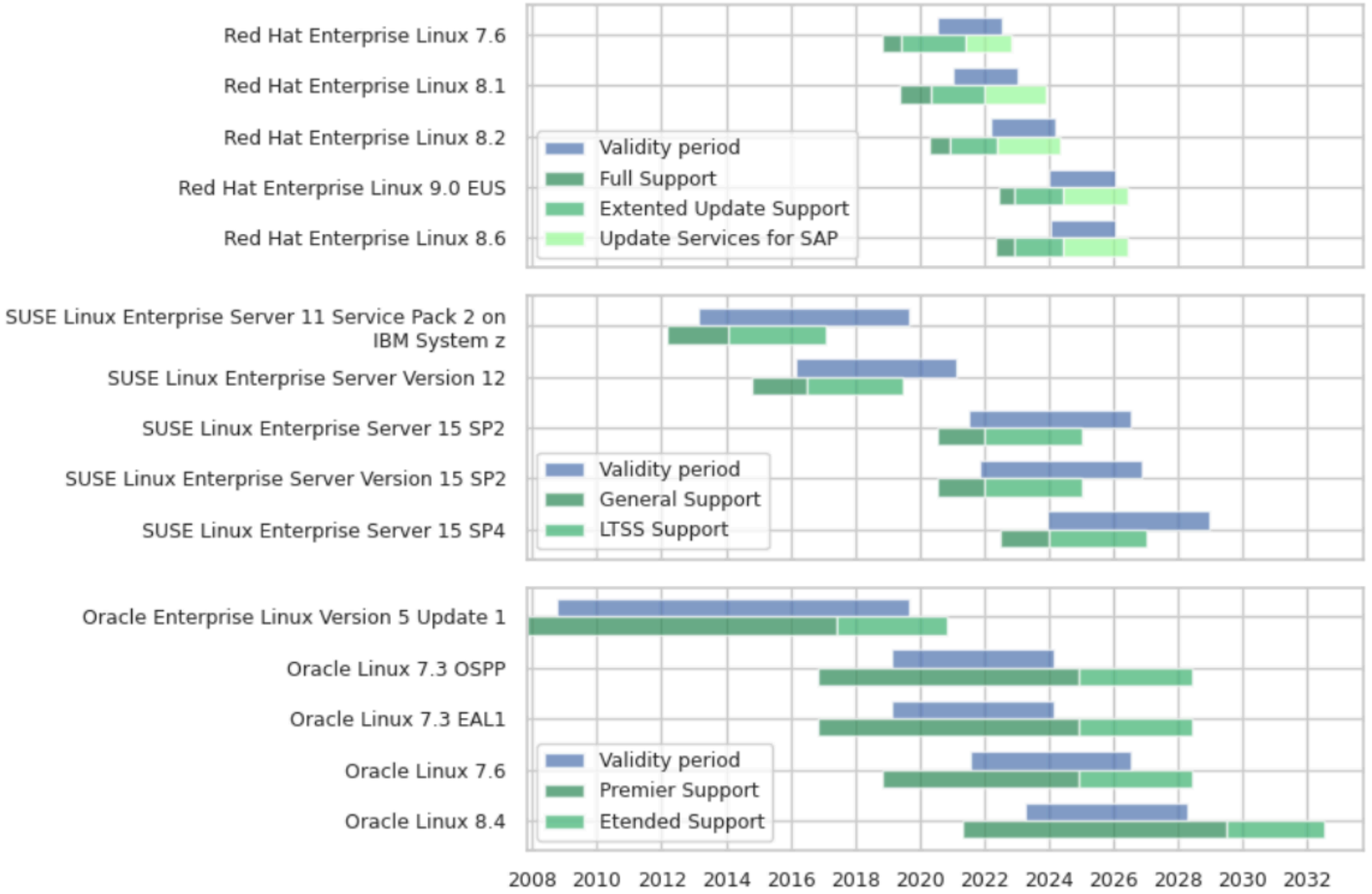
Time spent in IUT



Time spent in MIP stages



CC not doing much better...



~~Future work~~

What we’re failing at 🤷

Matching certified products to CVEs

- 💡Link certified modules to *published* vulnerabilities they suffer from.
- Each CVE lists affected configurations (CPEs).
- TPM-Fail CVE: `cpe:2.3:h:st:st33tphf2espi:-:*:*:*:*:*:*:*`
- FIPS module: Trusted Platform Module ST33TPHF2ESPI & ST33TPHF2EI2C
  - But, with different firmware 😢.

Configuration 2 (hide)

cpe:2.3:o:st:st33tphf2ei2c_firmware:73.5:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:st:st33tphf2ei2c_firmware:73.9:*:*:*:*:*:*:*

Show Matching CPE(s)

Running on/with

cpe:2.3:h:st:st33tphf2ei2c:-:*:*:*:*:*:*:*

Show Matching CPE(s)

Hunting exploitable misconfigurations

- Cryptographic-primitive misconfiguration can lead to exploitable vulnerability.
- 💡Configuration is conveyed by security policy doc.

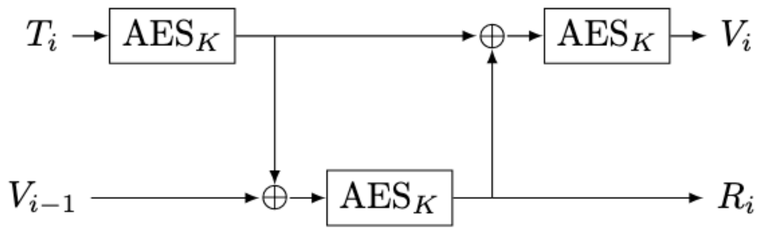


Figure 1: Each iteration of the ANSI X9.31 PRG generation function (G) inputs a timestamp T_i and a seed V_{i-1} and produces an output block R_i and a new seed V_i.

Example: misconfigured X9.31 PRNG

Practical state recovery attacks against legacy RNG implementations

Shaanan N. Cohney
University of Pennsylvania
shaanan@cohney.info

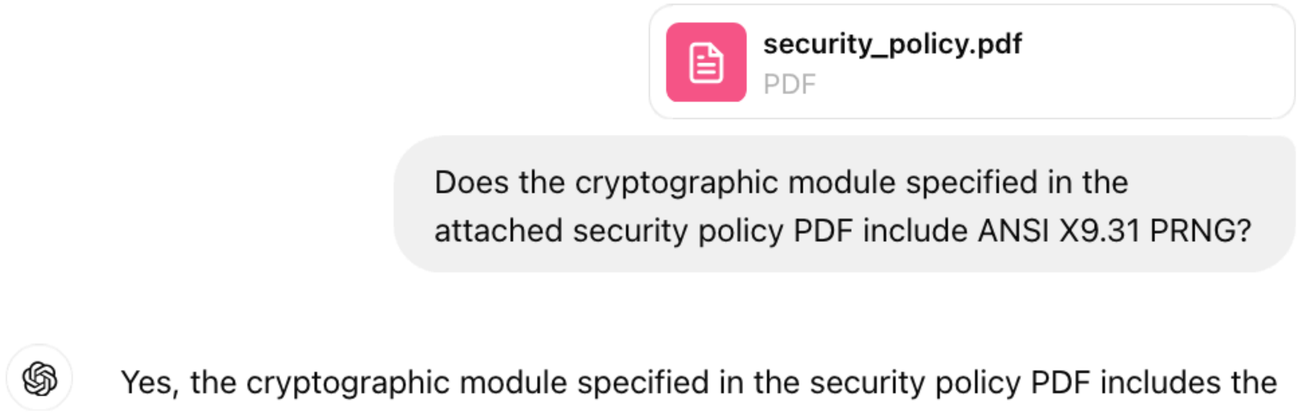
Matthew D. Green
Johns Hopkins University
mgreen@cs.jhu.edu

Nadia Heninger
University of Pennsylvania
nadiah@cis.upenn.edu

3 FIPS AND HARDCODED X9.31 KEYS

As discussed in Section 2.2, the NIST design description for the X9.31 random number generator [40] does not specify how the block cipher key should be generated or stored. However, vendors who wish to obtain FIPS certification are required to produce a detailed public "security policy" document describing their cryptographic implementations and key management procedures. We performed a systematic study of the security policies for products certified for the X9.31 PRG to understand how many vendors publicly documented a potential hard-coded key vulnerability. We obtained the list of certified devices from the NIST web site [52].

Hunting exploitable misconfigurations



Hunting exploitable misconfigurations

Which underlying cryptographic primitive is used in this particular instance of X9.31? 3-DES or AES?

The ANSI X9.31 PRNG in this instance uses 3-Key Triple-DES as the underlying cryptographic primitive (security_policy) .

Hunting exploitable misconfigurations

How is the secret key for the underlying 3-DES instance of the X9.31 algorithm generated and stored in this module?

The secret key for the 3-Key Triple-DES instance of the ANSI X9.31 algorithm (referred to as the RNG seed key) is ”rated and stored in the module as follows:

- **Generation**: The RNG seed key is generated during the manufacturing process and is stored securely within the module.
- **Storage**: The RNG seed key is stored as part of the module's Critical Security Parameters (CSPs) in a secure, non-volatile memory. It is loaded into the module at the factory and is not modifiable by any external entity (security_policy) .

Hunting exploitable misconfigurations

Is a single key used for the lifetime of the module? Are the keys shared between different module instances?

- **Single Key Use**: Yes, a single RNG seed key is generated and stored for the lifetime of each module instance. The key is not updated or replaced during normal operation.
- **Key Sharing**: No, the keys are not shared between different module instances. Each module instance has its own unique RNG seed key generated and stored securely during manufacturing (security_policy) .

Building reference graph

- Dependency networks well studied in software packages.
- We investigated the dependency network in Common Criteria
- When vulnerability impacts the dependency, it may translate to the referencing product.

Small World with High Risks:
A Study of Security Threats in the npm Ecosystem

Markus Zimmermann and Cristian-Alexandru Staicu, *TU Darmstadt;* Cam Tenny, *r2c;*
Michael Pradel, *TU Darmstadt*

An empirical comparison of dependency network evolution in seven software packaging ecosystems

Alexandre Decan[1] · Tom Mens[1] · Philippe Grosjean[1]

Chain of Trust: Unraveling References Among Common Criteria Certified Products

Adam Janovsky(✉), Łukasz Chmielewski, Petr Svenda, Jan Jancar,
and Vashek Matyas

Building reference graph

Certificate #4424

Details

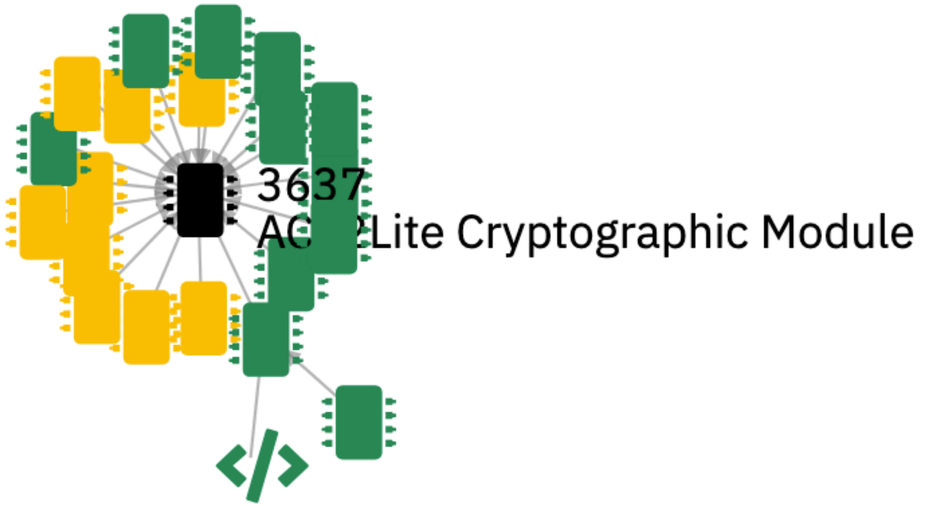
Module Name	Cisco Catalyst 9800 (40/80) Wireless Controllers
Standard	FIPS 140-2
Status	Active
Sunset Date	9/21/2026
Overall Level	1
Caveat	When operated in FIPS mode. This module contains the embedded module ACT2Lite validated to FIPS 140-2 under Cert. #3637 operating in FIPS mode.
Security Level Exceptions	• Roles, Services, and Authentication: Level 3 • Mitigation of Other Attacks: N/A
Module Type	Hardware
Embodiment	Multi-Chip Stand Alone
Description	The Cisco Series Wireless Controllers, are a highly scalable and flexible platform that enables system-wide services for mission-critical wireless networking in medium-sized to large enterprises and campus environments.
Tested Configuration(s)	• N/A

Approved Algorithms

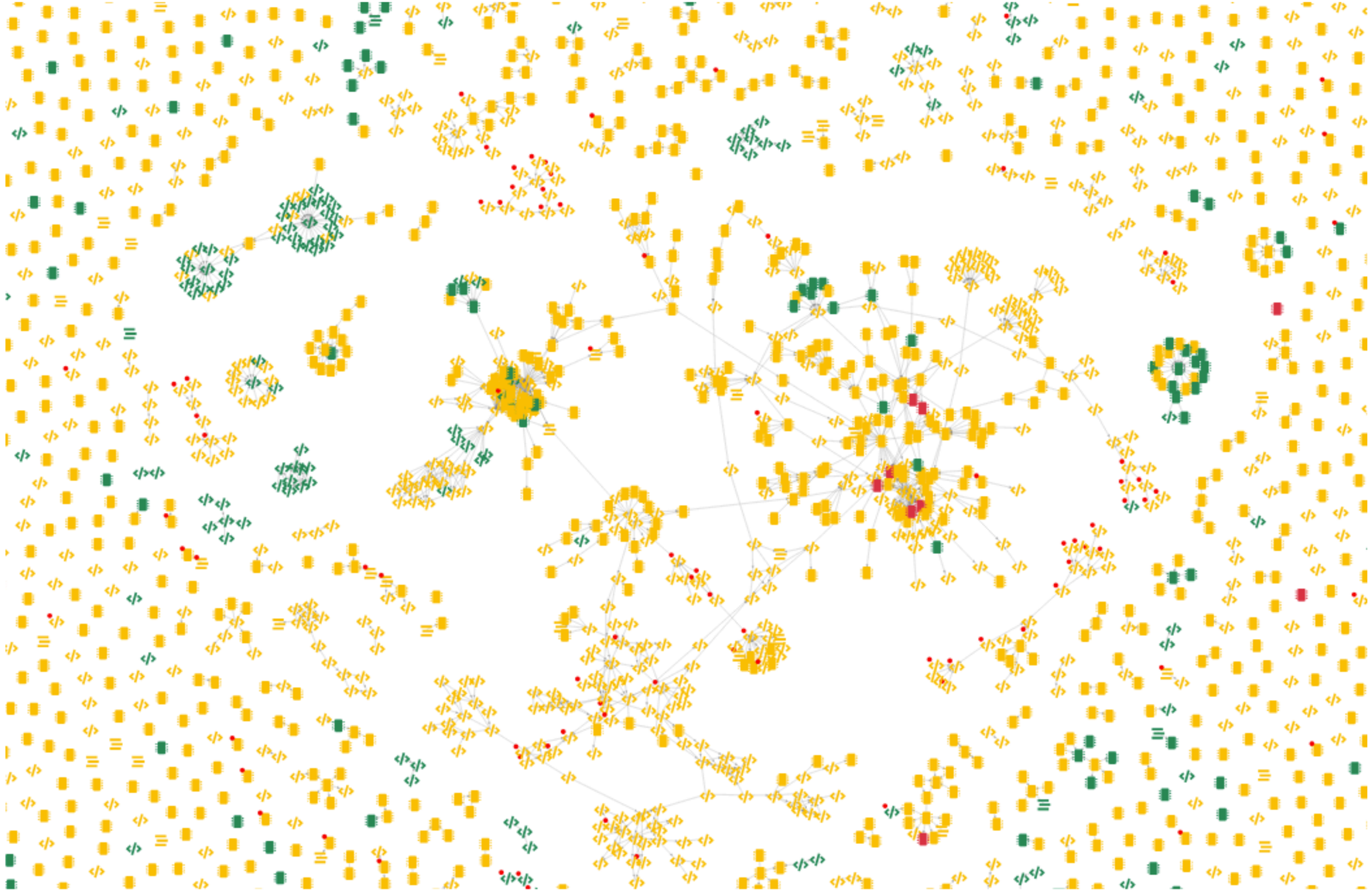
AES	Certs. #2346, #A877 and #A1462
CKG	vendor affirmed
CVL	Certs. #A877 and #A1462
DRBG	Certs. #A877 and #A1462
ECDSA	Certs. #A877 and #A1462
HMAC	Certs. #A877 and #A1462
KAS	KAS-SSC Certs. #A877 and #A1462, CVL Certs. #A877 and #A1462
KAS-SSC	Certs. #A877 and #A1462
KTS	AES Certs. #A877 and #A1462 and HMAC Certs. #A877 and #A1462; key establishment methodology provides between 128 and 256 bits of encryption strength
RSA	Certs. #A877 and #A1462
SHS	Certs. #2023, #A877 and #A1462

Building reference graph

- Turns out that ACT2Lite module is quite important one.
- It constitutes an important target for adversaries.
- It constitutes an important asset for vendors.



Building reference graph



Making certification artifacts machine-processable

- Efforts to automate cryptographic module validation program 👏.
- NIST/Vendors: Assign robust module and algorithm identifiers.
- NIST/Vendors: Assign each module with CPE record.
- NIST: Replace security policy PDFs (with XML?)
- NIST/Vendors: Promote SBoMs (NIAP policy for Common Criteria) 👏.
- NIST: Publish FIPS CMVP web snapshots.

Summary

- Monitoring the certification artifacts yields more visibility into the ecosystem.
- Deep analysis is thwarted by lack of structure.
- Artifacts written in natural language? Leverage natural language processing.
- Sec-certs conceived to aid vulnerability impact assessment.
- Our weekly-updated results available from sec-certs.org.

Follow up

- Talk to us here.
- Tell us if we’re wrong.
- Mail us feature requests.

Learn more at sec-certs.org