

Investigating cryptography deployments in security-certified products with sec-certs

Vashek Matyas & Yasir Yakup Demircan matyas@fi.muni.cz, 561938@mail.muni.cz
Centre for Research on Cryptography and Security, Masaryk University, Czechia
Joint work with Petr Svenda, Jan Jancar, Adam Janovsky, Martin Ukrop, Stanislav Bobon, Vladimir Penaz, Lukasz Chmielewski, Jaroslav Reznik, and many others (thank you all!)

CROCS
Centre for Research on Cryptography and Security

WHY DID WE CARE (AGAIN) ABOUT CC?

CVE-2017-15361 (RoCA)

- [CVE-2017-15361]: practical factorization of certain RSA keys.
- Billion+ devices affected.

- ⚠ How many products certified under Common Criteria are impacted?

Common Criteria – certified products/systems

- FIPS 140
  - 5500+
    - 1000 active today

1778 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems	20	140
Biometric Systems and Devices	2	3
Boundary Protection Devices and Systems	36	231
Data Protection	49	209
Databases	9	89
Detection Devices and Systems	6	76
ICs, Smart Cards and Smart Card-Related Devices and Systems	759	1506
Key Management Systems	5	53
Mobility	42	97
Multi-Function Devices	218	541
Network and Network-Related Devices and Systems	223	742
Operating Systems	43	213
Other Devices and Systems	302	878
Products for Digital Signatures	51	137
Trusted Computing	13	58
Totals:	**1778**	**4973**
	Grand Total:	**6751**

Common Criteria

NIST FIPS 140-2/3

NVD vulnerability database
https://nvd.nist.gov/

Base Score: 8.8 HIGH

National Certificate Authorizing Schemes (BSI, ANSSI, NAIP…)

Certified product

Vendor

Evaluation laboratory

NIST CMVP (Cryptographic Module Validation Program)
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/

Common Criterial Certification portal
https://www.commoncriteriaportal.org/

NIST CMVP portal

List of platforms and vulnerabilities (CPE, CVE)

Certification artifacts (Certificate, Security Target, Security Policy…)

sec-certs

sec-certs git repository
https://github.com/crocs-muni/sec-certs

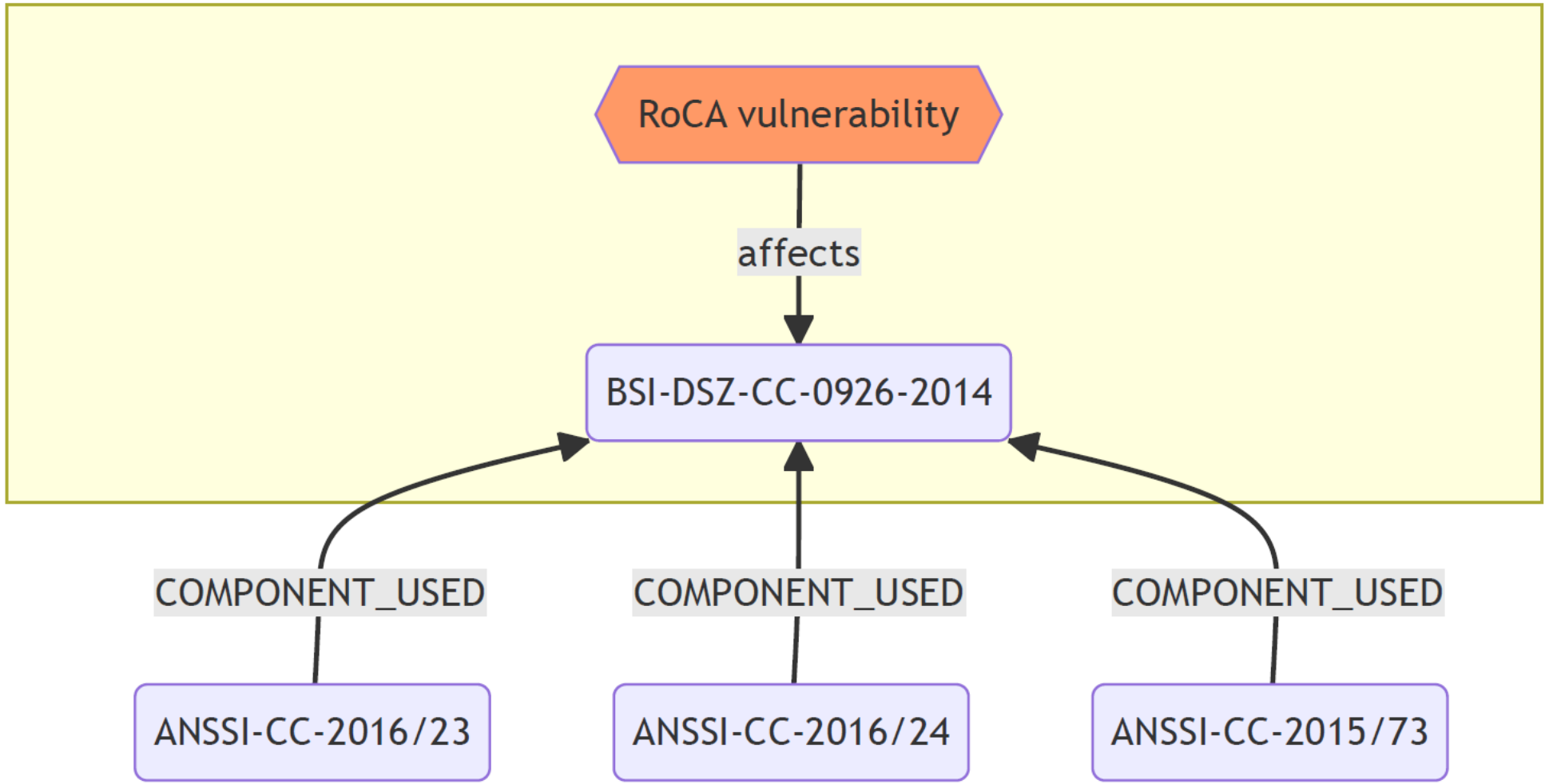
sec-certs webpage
https://sec-certs.org/

Extracted data (JSON)

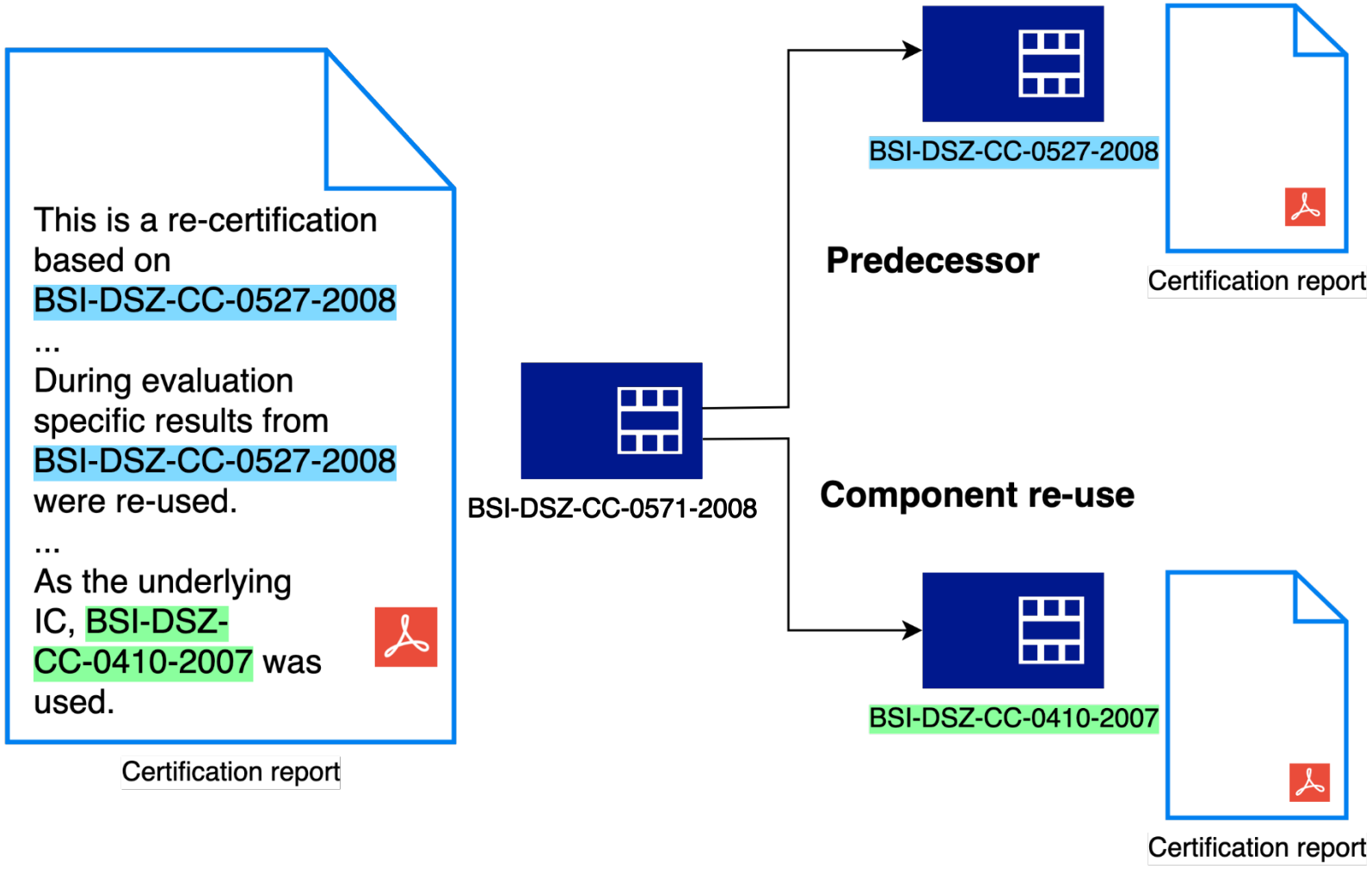
sec-certs API
Python CLI, Jupyter Notebooks, Binder, Docker

Analyses and visualizations

CVE-2017-15361

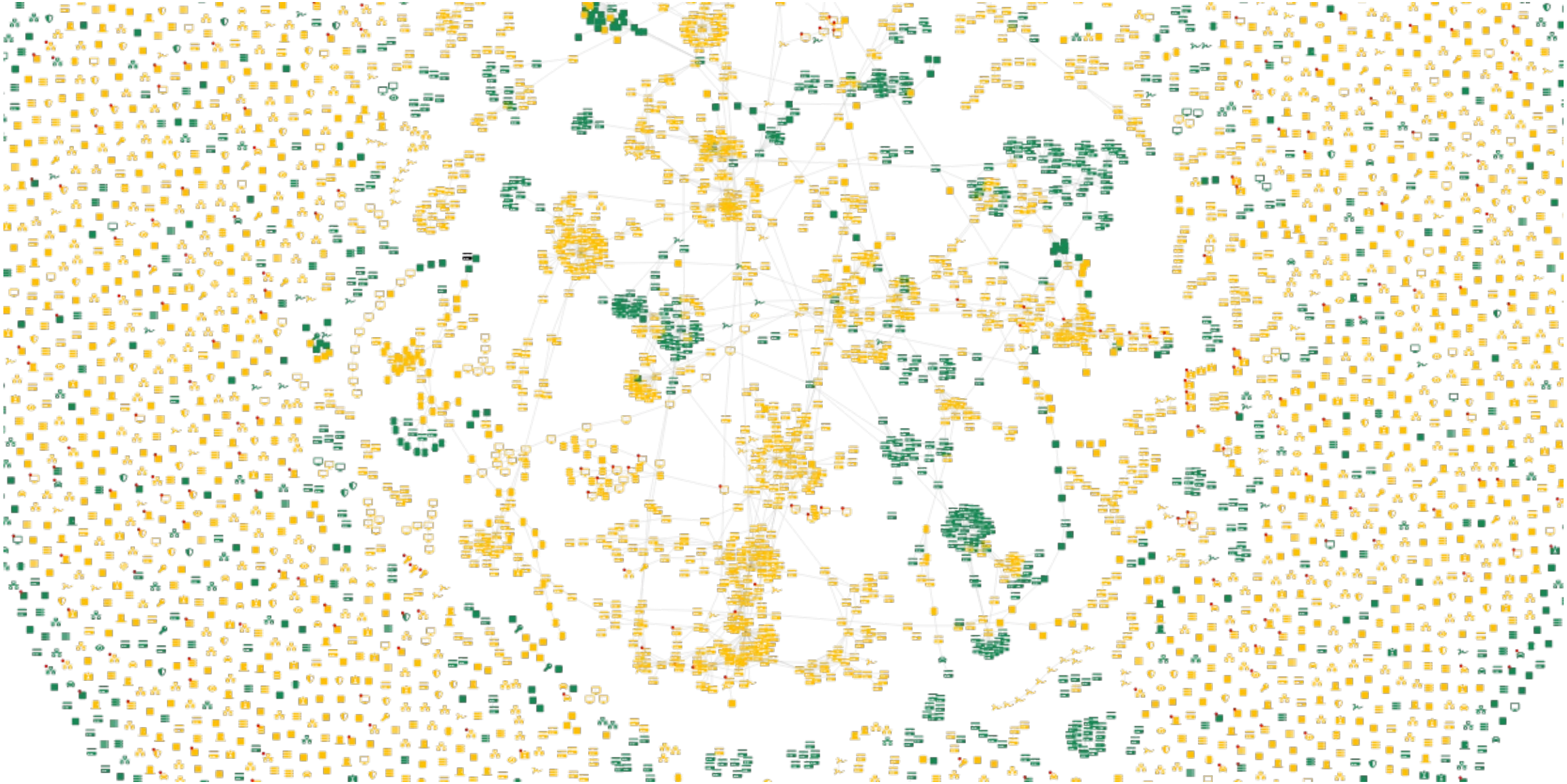


Building the reference graph



Building the reference graph

- Each device is a **vertex**.
- A reference from device A to device B is a **directed edge**.
  - The reference is indicated by the presence of a foreign certificate ID within the artifacts.
- The categorical context of the reference, e.g. `COMPONENT_USED`, is an **edge label**.
- We worked with 6k vertices and 3k edges.



Few major observations from reference analyses

- Top-10 products are used in 16% of all active smartcards.
  – These are microcontrollers, typically with cryptographic functionality.
- Higher reach is positively associated with higher evaluation assurance level.
- A vulnerability in cryptographic functionality would spread from high-reach devices to approx. 70% of their dependants.
  – Affecting 50+ certified products, RoCA was not an outlier.

In a nutshell

- We have developed a pipeline for automated processing of Common Criteria artifacts.
  - We also cover FIPS 140, EUCC and NVD vulnerability DB
  - Mapping of dependencies among certificates
  - Continuous insights into certification ecosystem
  - Support for more transparency in security certifications
- The analysis is tedious due to artefacts *produced by humans and meant to be consumed by humans*.

Two case studies investigating crypto in certificates

1. OpenSSL (and derivates) utilization in certified products

2. Mapping of selected crypto weaknesses – how they came (and some have gone) within certified products

Case Study #1 – Research Questions

1. Is OpenSSL prevalent? If so, how much?

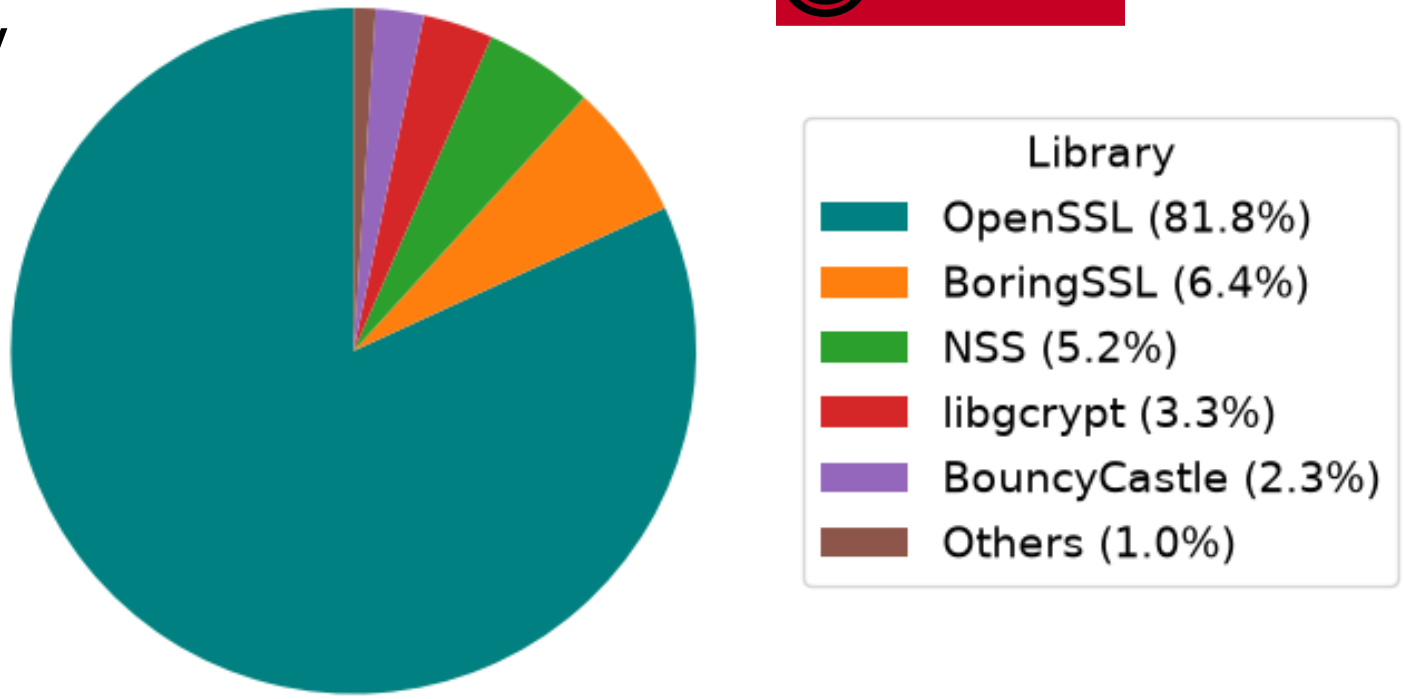
2. What vendors use OpenSSL the most?

3. Who are the competitors?

OpenSSL Dominance

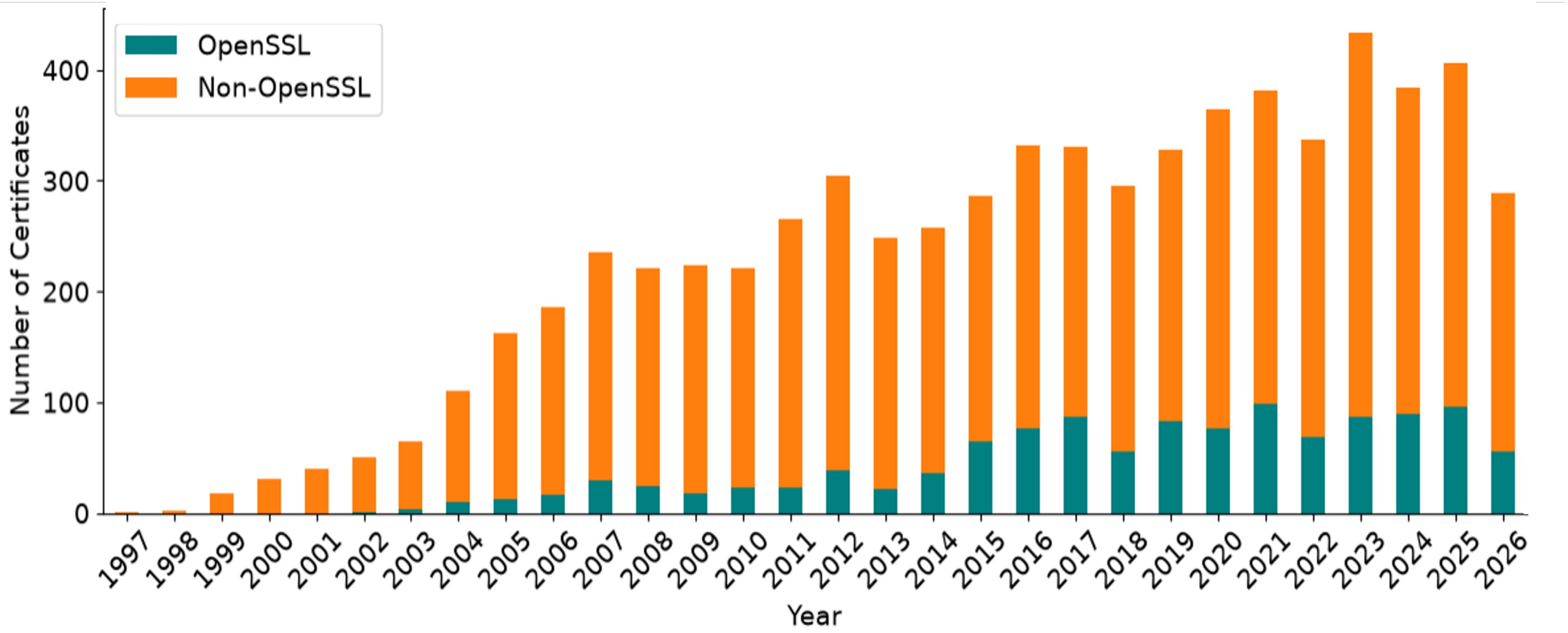
OpenSSL dominance in security certifications

- 17% Common Criteria
- 16% FIPS 140

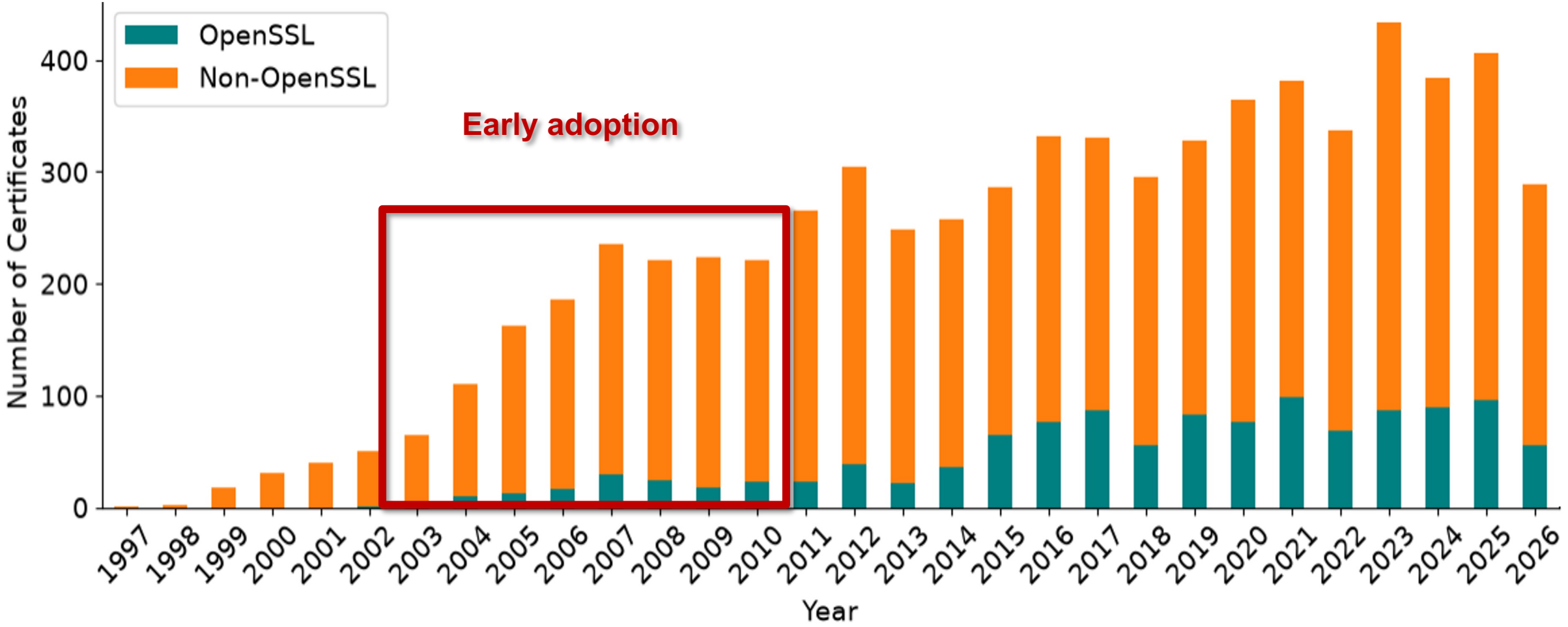


Distribution of crypto libraries

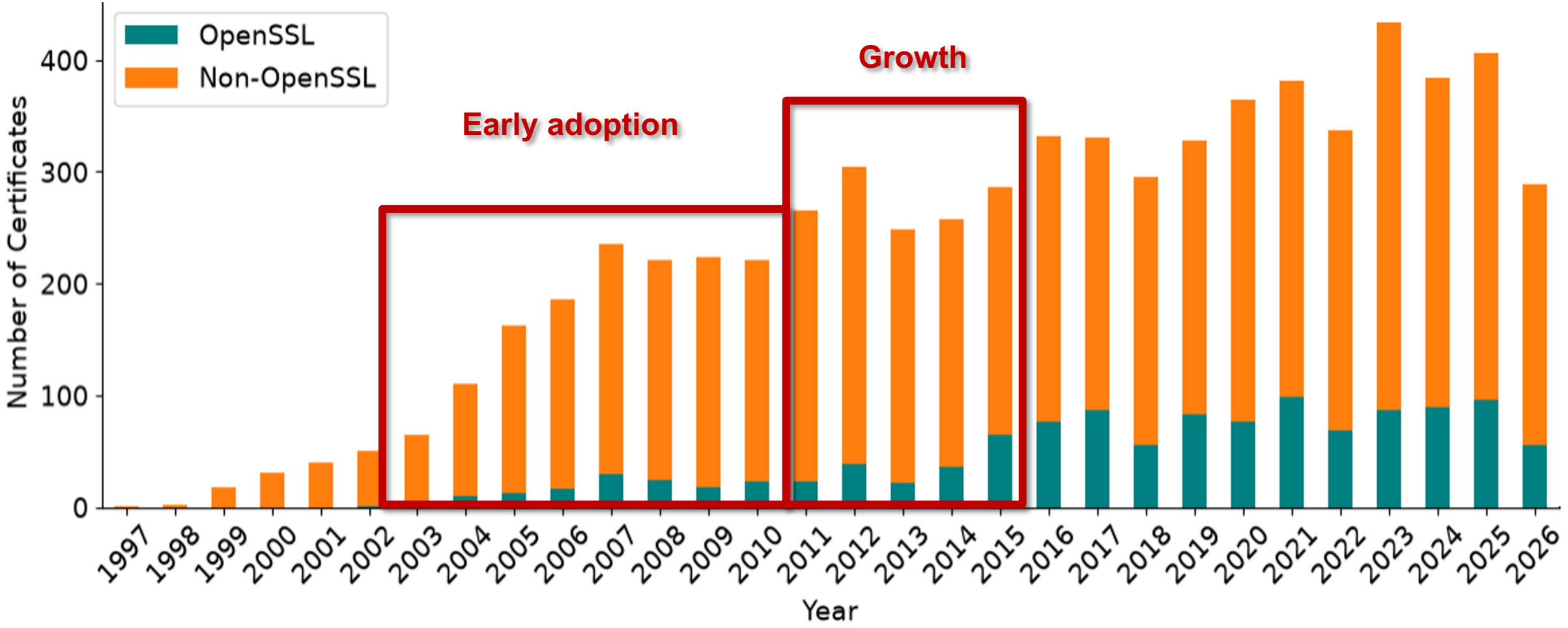
Common Criteria: OpenSSL's Footprint



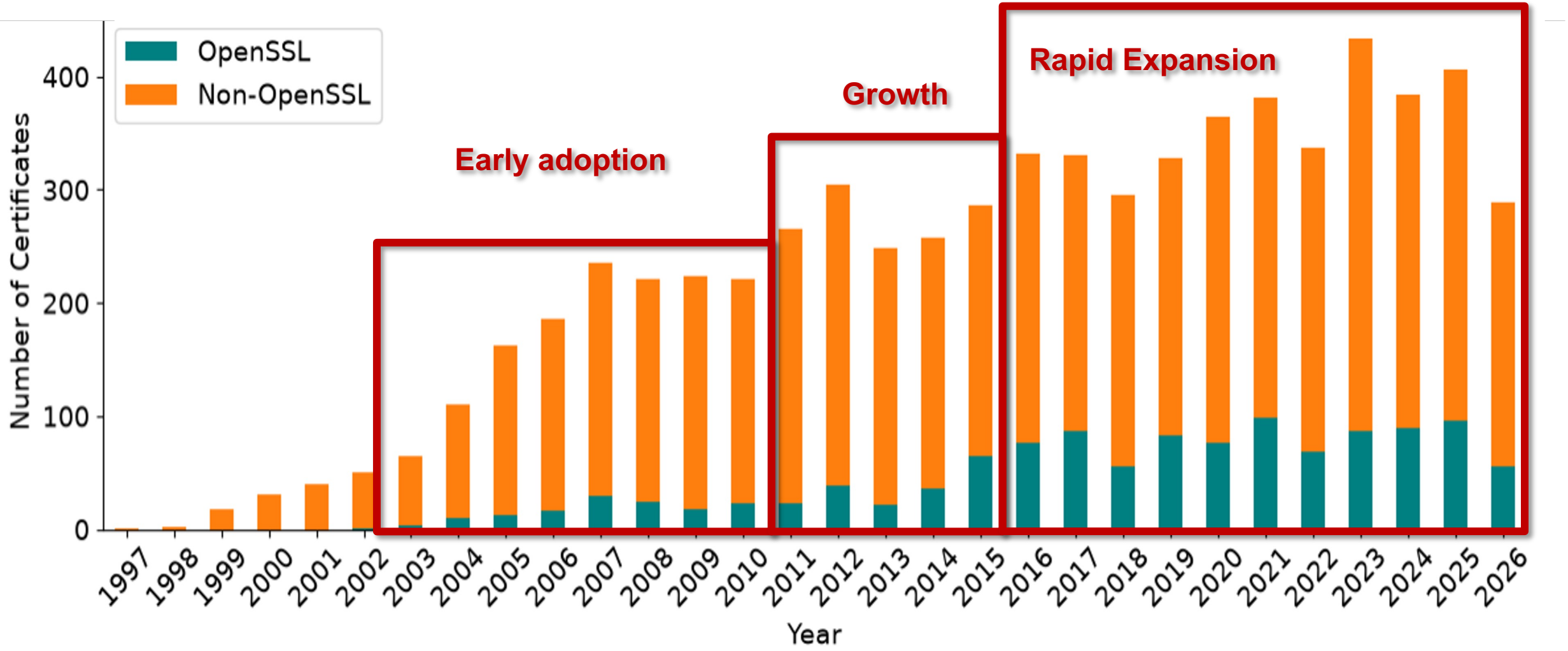
Common Criteria: OpenSSL's Footprint



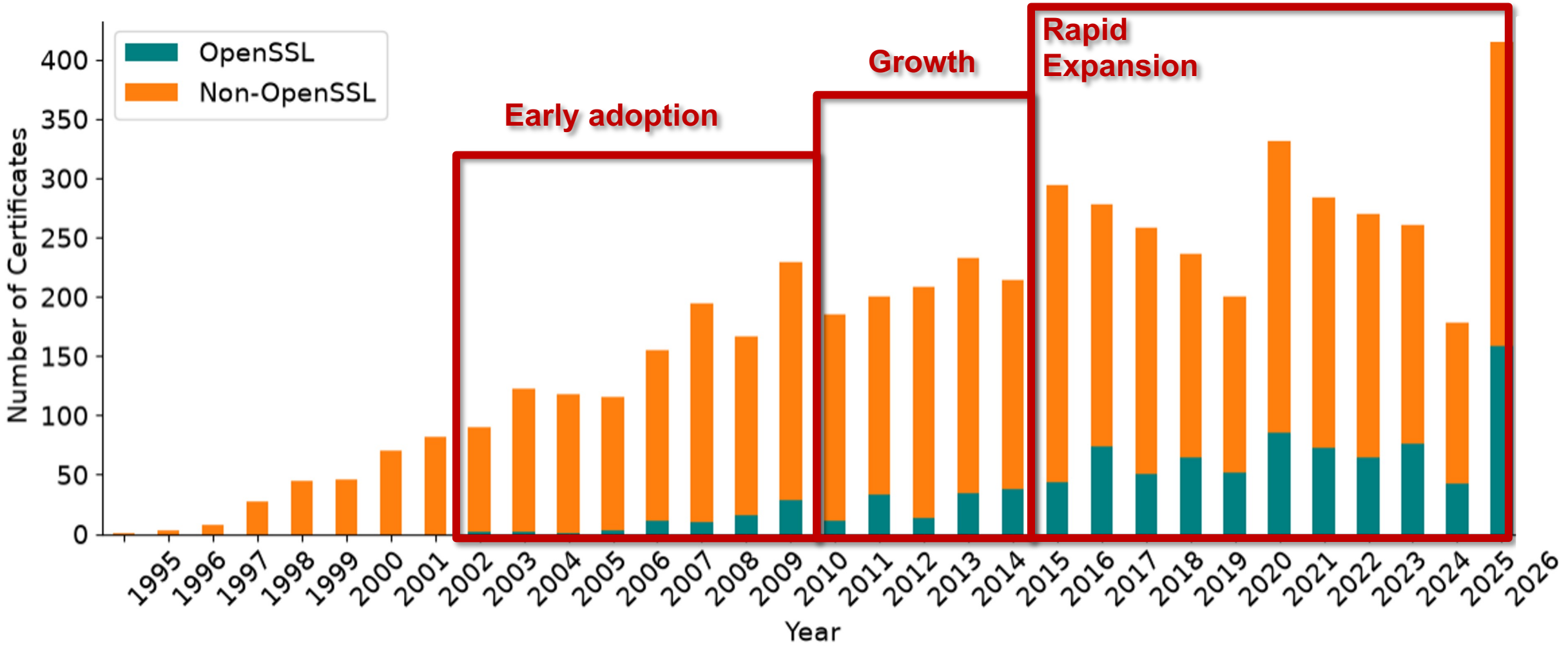
Common Criteria: OpenSSL's Footprint



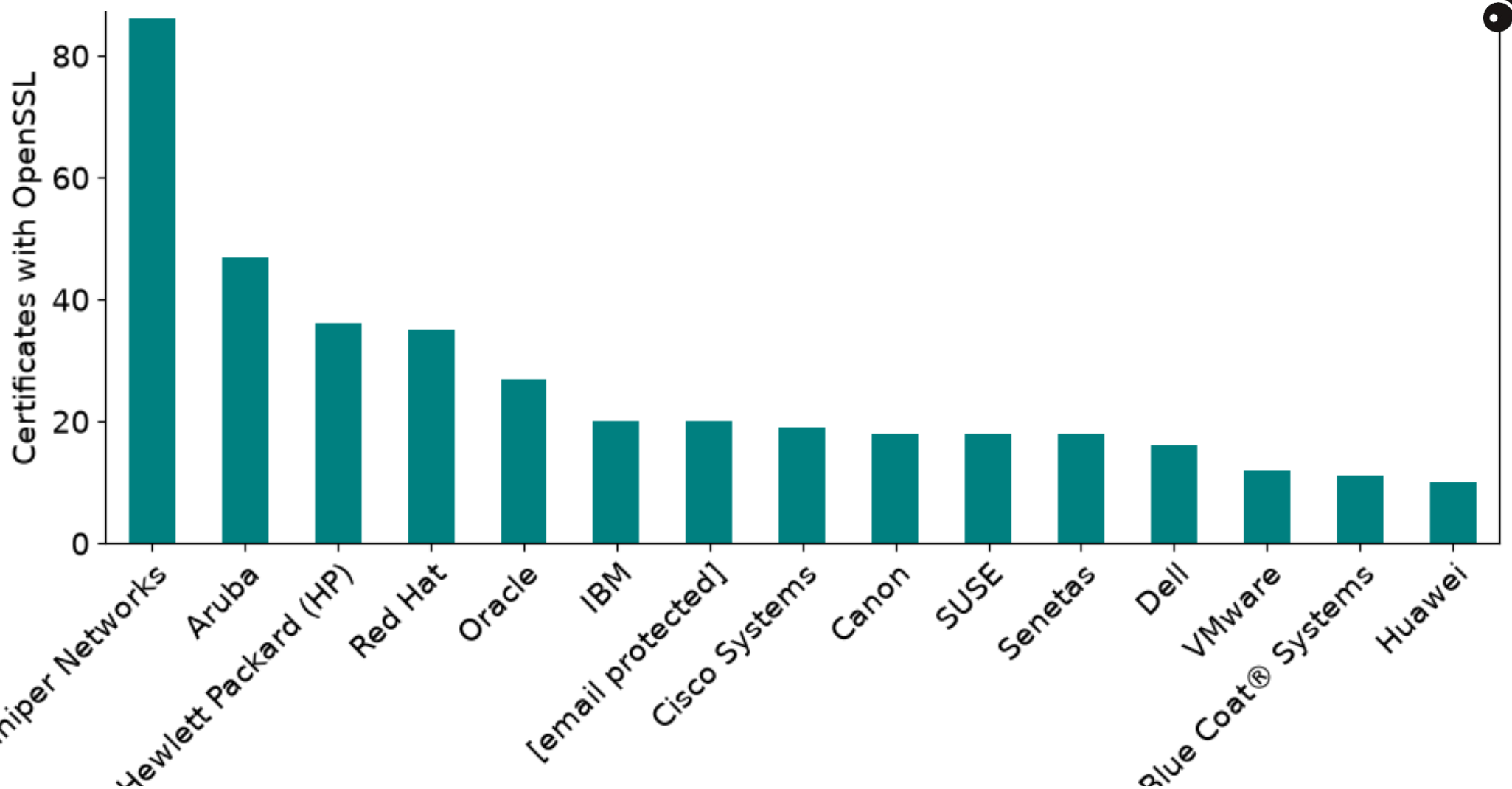
Common Criteria: OpenSSL's Footprint



OpenSSL in the FIPS 140 Ecosystem

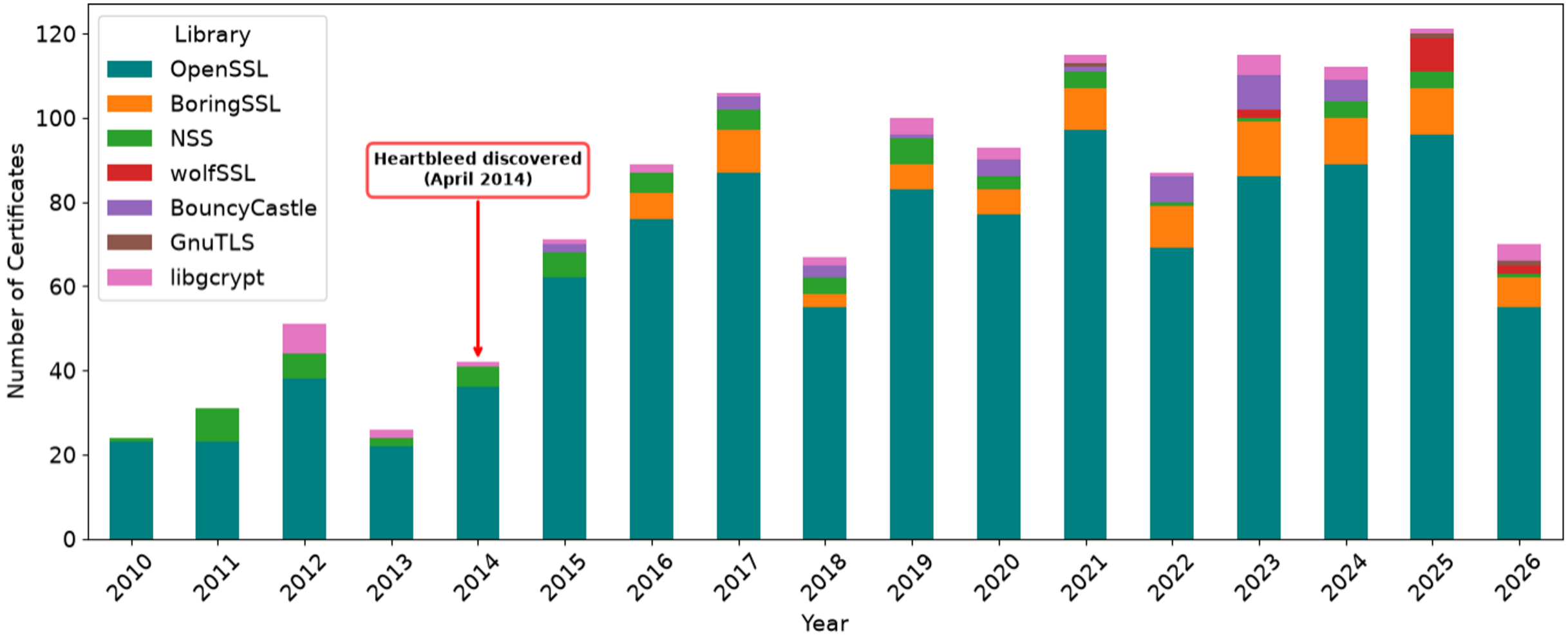


Top 15 Vendors Relying on OpenSSL

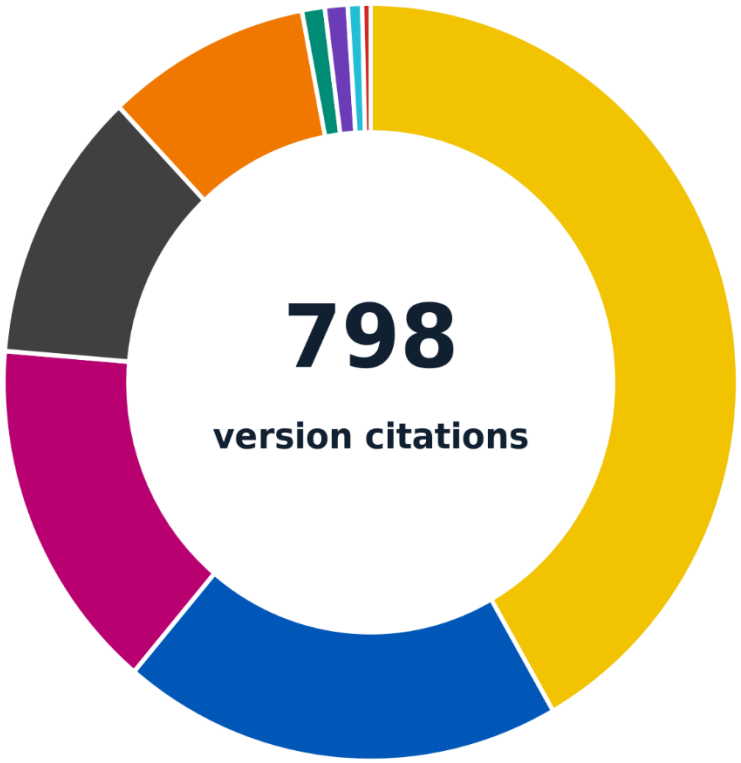


Appearance of OpenSSL alternatives

Common Criteria

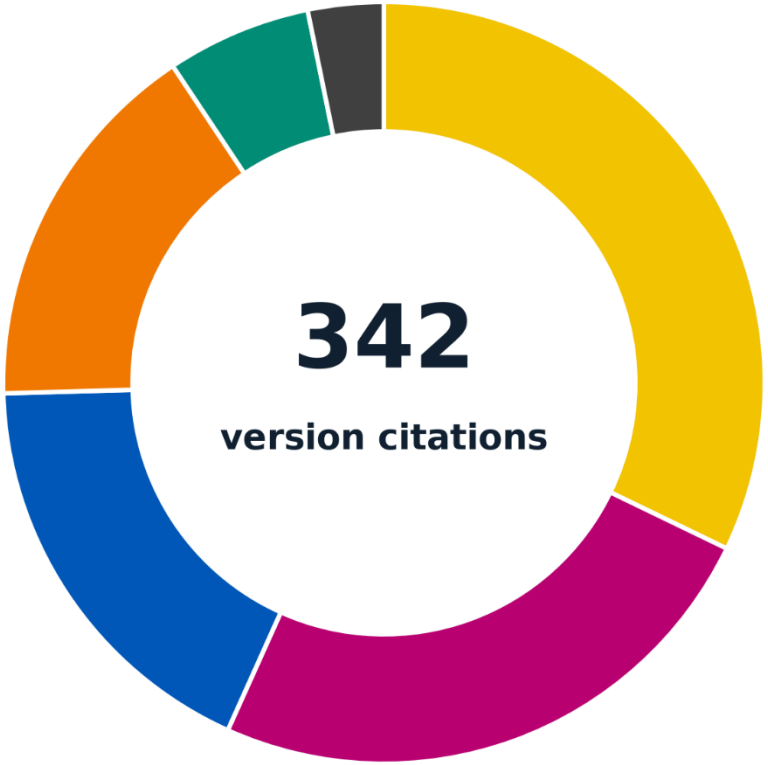


OpenSSL Version Branch Distribution



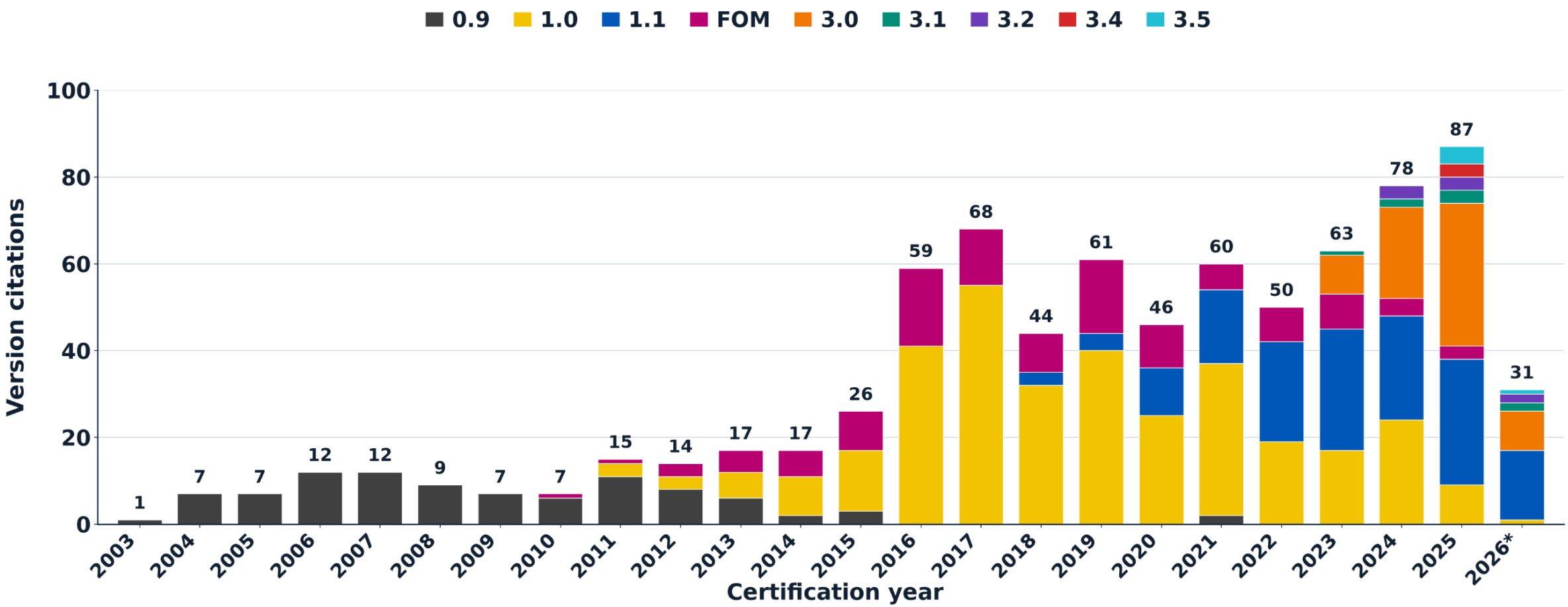
BRANCH	CITATIONS	SHARE
1.0	333	41.73%
1.1	155	19.42%
FOM	121	15.16%
0.9	93	11.65%
3.0	72	9.02%
3.1	8	1.00%
3.2	8	1.00%
3.5	5	0.63%
3.4	3	0.38%

OpenSSL Version Branch Distribution



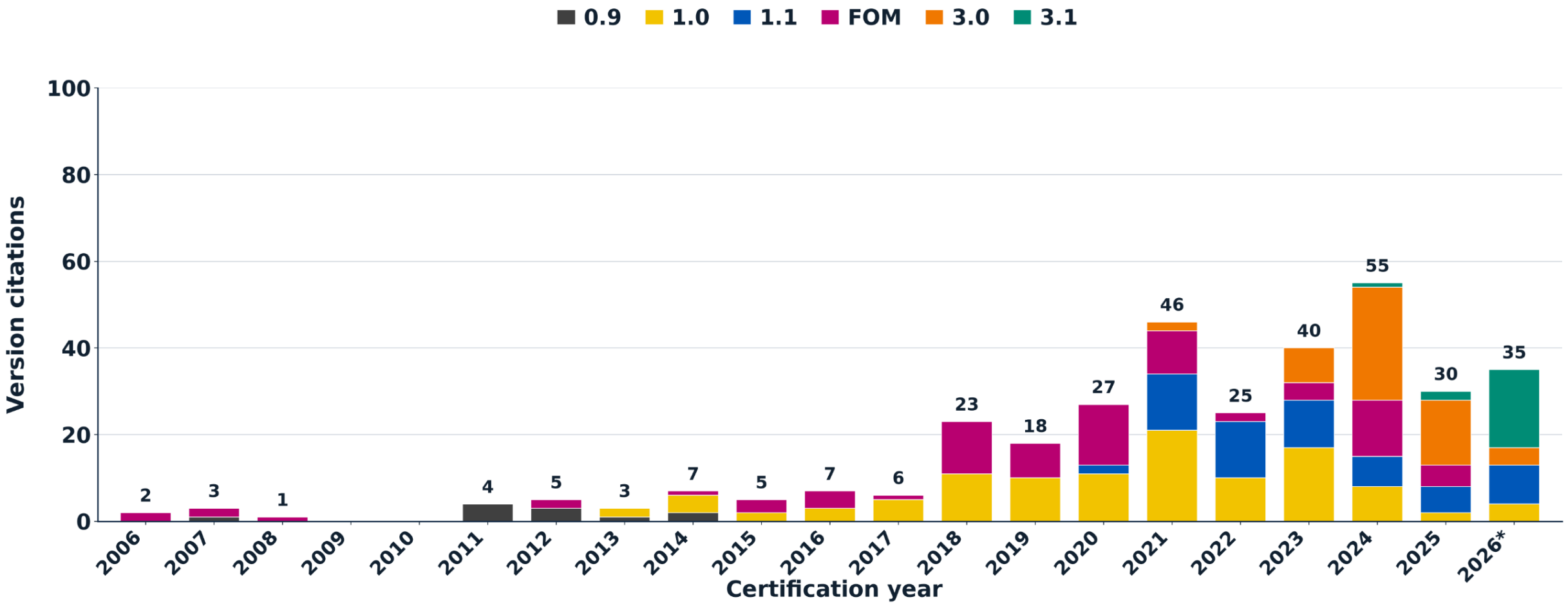
BRANCH	CITATIONS	SHARE
1.0	110	32.16%
FOM	84	24.56%
1.1	61	17.84%
3.0	55	16.08%
3.1	21	6.14%
0.9	11	3.22%

OpenSSL version usage in years



*2026 is partial: latest supplied CC certification date is 2026-04-12.

OpenSSL version usage in years



*2026 is partial: latest supplied FIPS certification date is 2026-04-14.

Active certificates by year per OpenSSL version

FIPS 140-3™

Active status on 2026-09-20 / 117 certificates / grouped into branches

OpenSSL branch	2021	2022	2023	2024	2025	2026*	ROW TOTAL
0.9	0	0	0	0	0	0	0
1.0	1	2	5	4	1	4	17
1.1	1	8	8	5	4	7	33
FOM	1	1	3	12	5	0	22
3.0	2	0	7	20	14	4	47
3.1	0	0	0	1	2	18	21

Certification year

Certificates: 0 | 1-3 | 4-9 | 10-19 | 20+

Active certificates by year per OpenSSL version

Common Criteria

Active status on 2026-09-20 / 211 certificates / grouped into branches

OpenSSL branch	2021	2022	2023	2024	2025	2026*	ROW TOTAL
0.9	2	0	0	0	0	0	2
1.0	4	8	5	18	9	1	45
1.1	4	17	17	19	24	12	93
FOM	4	4	4	4	3	0	19
3.0	0	0	5	14	30	9	58
3.1	0	0	0	1	2	2	5
3.2	0	0	0	3	3	2	8
3.4	0	0	0	0	3	0	3
3.5	0	0	0	0	4	1	5

Certification year

Certificates: 0 | 1-3 | 4-9 | 10-19 | 20+

Case Study #1: Key Findings and Impact



Dominant cryptographic library
in CC and FIPS
(17% of all certificates)



Data insights for

- certification trends,
- vendor strategies,
- technology adoption patterns.

Case Study #1: Key Findings and Impact





Dominant cryptographic library
in CC and FIPS
(17% of all certificates)

Data insights for

- certification trends,
- vendor strategies,
- technology adoption patterns.

Information previously hidden in 10k+ unstructured documents

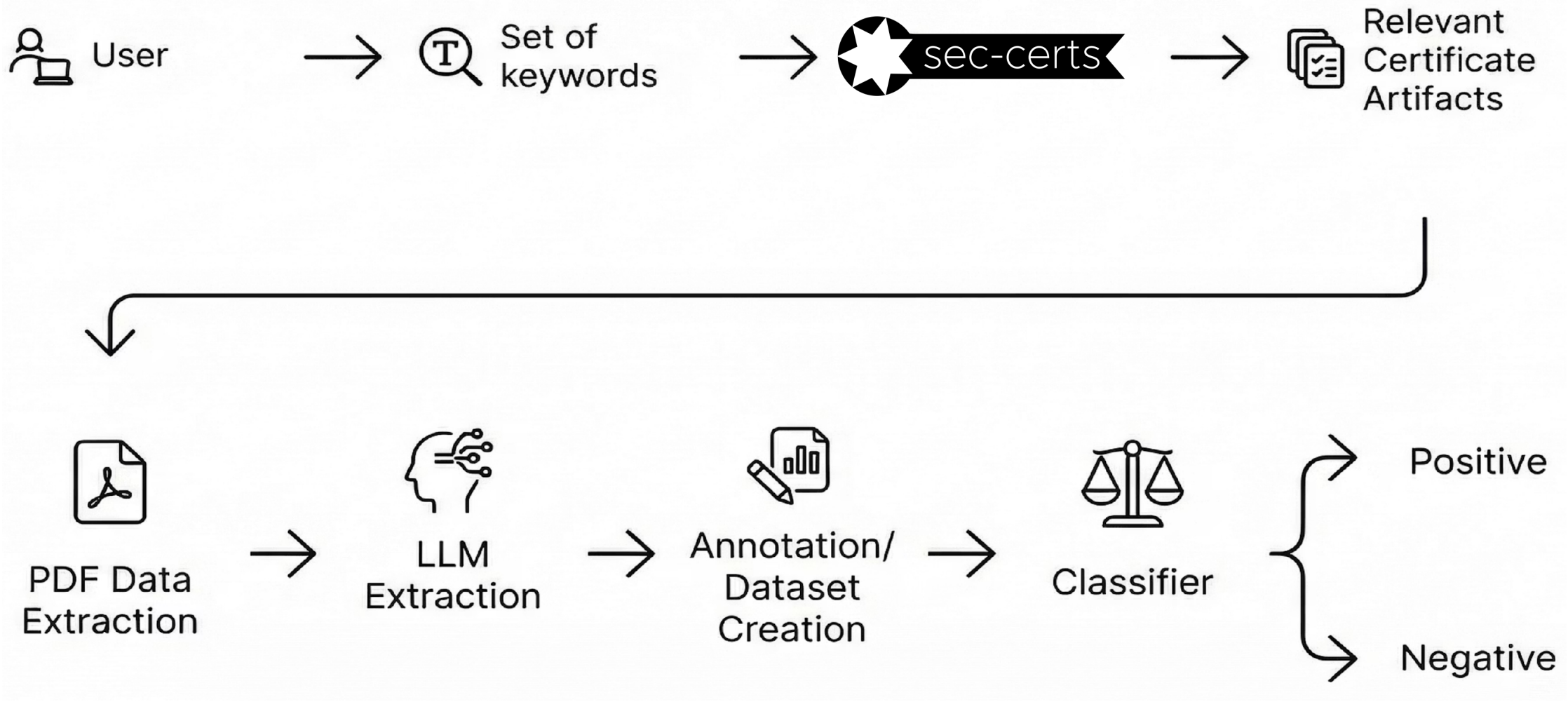
Case study – Selected Cryptographic Weaknesses

Insecure Configuration	Human Errors	Deprecated Standards
• Using a cryptographic primitive or protocol in a known insecure state. • Old TLS version with an insecure cipher suit.	• Weaknesses without a specific discovery date. • Hardcoded PRNG seed keys • Static Ivs, etc.	• Practices like using cryptographic algorithms after their weaknesses are discovered. • DUAL_EC_DRBG after 2015 backdoor discovery.

Key inspected weaknesses:

- Weak TLS Ciphers
- SHA-1
- Hardcoded Keys
- X9.31 PRNG
- DUAL_EC_DRBG

Workflow


User
Set of keywords
sec-certs
Relevant Certificate Artifacts
PDF Data Extraction
LLM Extraction
Annotation/ Dataset Creation
Classifier
Positive
Negative

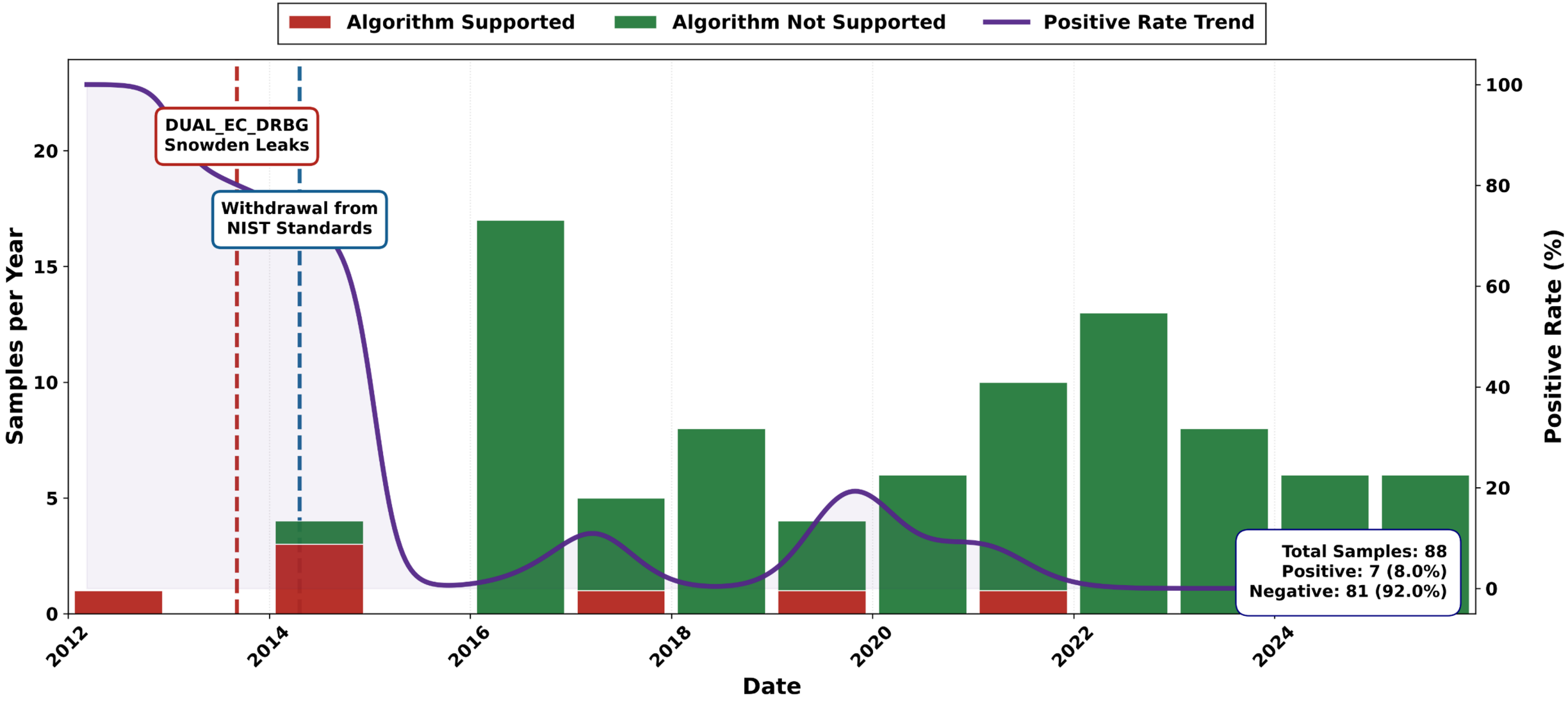
Dataset and Methodology

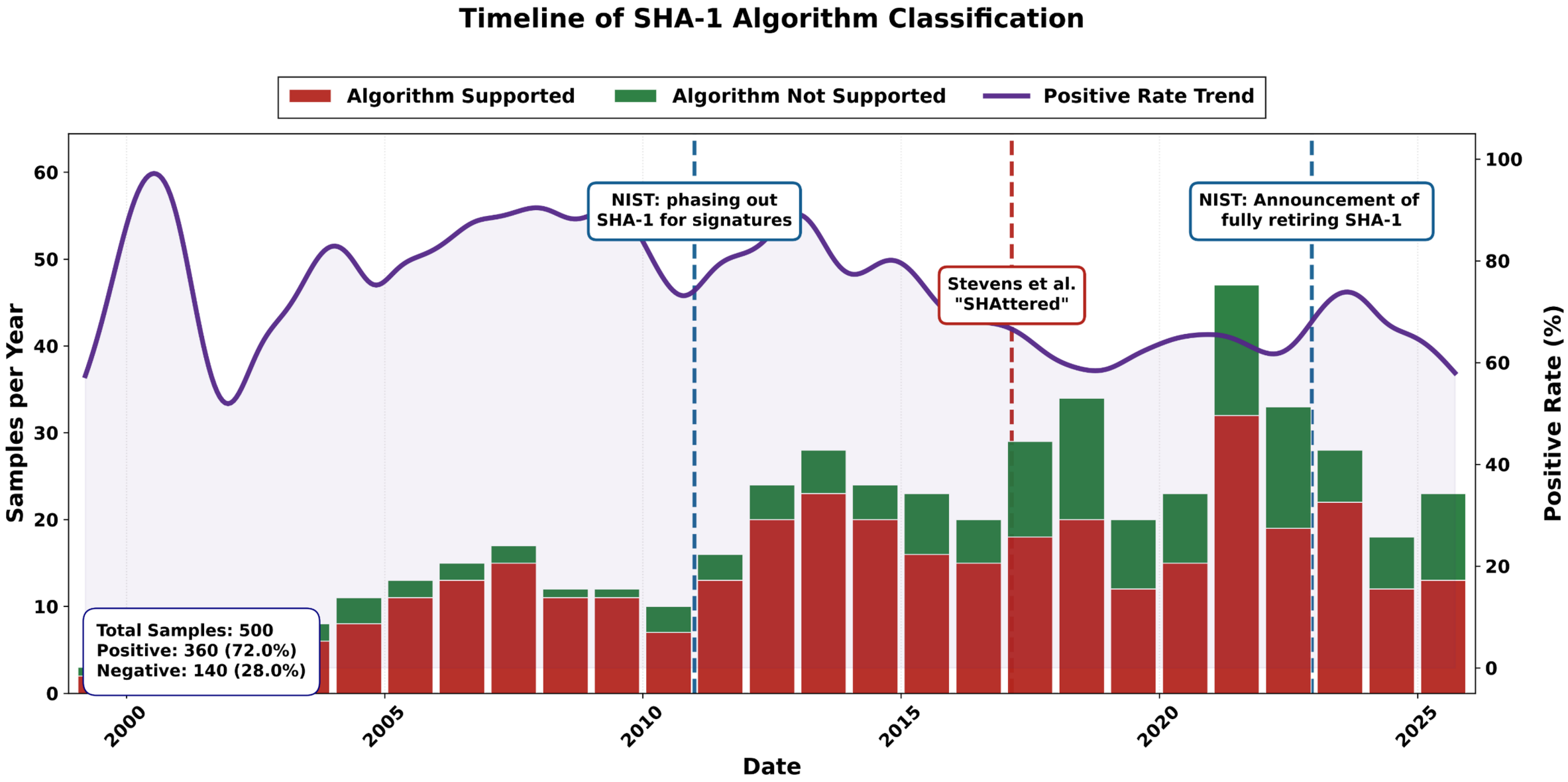
- **Sample Size**:
  1,050 certificate artifacts labeled by 6 annotators
- **Strategy**:
  double-annotation strategy to consistency
- **Conflict Resolution**:
  Any inter-annotator conflicts were resolved through 1-1 discussion
- **Exclusion Criteria**:
  Unresolved records marked as *unknown* (33 samples)

Key Challenges

- 🗄️ Imbalanced Datasets: Handling disparities in data distribution effectively.(Synthetic data or Original data)
- 📄 Parsing Errors: Dealing with incorrect PDF parsing and sentence segmentation issues. (Docling or PyPdf)
- 🔍 Extraction Reliability: Reliably extracting relevant sentences for accurate analysis. (REGEX or Sentence Transformers)

Timeline of DUAL_EC_DRBG algorithm Classification




Timeline of SHA-1 Algorithm Classification
Algorithm Supported
Algorithm Not Supported
Positive Rate Trend
NIST: phasing out SHA-1 for signatures
Stevens et al. "SHAttered"
NIST: Announcement of fully retiring SHA-1
Total Samples: 500
Positive: 360 (72.0%)
Negative: 140 (28.0%)
Samples per Year
Positive Rate (%)
Date
0
10
20
30
40
50
60
0
20
40
60
80
100
2000
2005
2010
2015
2020
2025

Users of the sec-certs.org tool

- Owners/users of certified devices / security researchers
  - What security claims are made?
  - What certificates to additionally monitor?
  - Notification after new (possibly relevant) vulnerability is found
  - Analyze impact of vulnerability (e.g., ROCA case)
- Vendors of certified products
  - Are we under/over certifying with respect to competition?
  - Who is certifying products of our type and what were requirements in past?
- Certification bodies
  - Performance of labs, suspiciously short validity, non-standard cert. claims…
  - Impact of certification requirements (SARs) on the actual security

Users of the sec-certs.org tool

- Certification laboratories
  - Are we comparable with other laboratories? What are the trends?
- Government agencies & corporations
  - Processing additional non-public documents
  - Attaching additional metadata (test results, powertrace…) and its governance
    - Generate sec-certs “web” locally with additional information
- General public
  - Easy access to information (interactive webpage, info from multiple sources…)
  - Ecosystem insights: What is standardized? Change in time?

Come and play – with sec-certs!

https://sec-certs.org/

Thank you for your attention!

sec-certs

Cyber Security for Europe

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

CAT

CYBERSECURITY CERTIFICATION AND ASSESSMENT TOOLS