Security Architecture

Cryptography: course for master's degree in EDGE COMPUTING

Michał Melosik, PhD

Lecture outline

1. Threat modeling @ system level
2. Attack types
3. HTTPS, TLS
4. CA & Certificates
5. Vulnerabilities: CVSS, CWE, CVE
6. Standardization of security approach

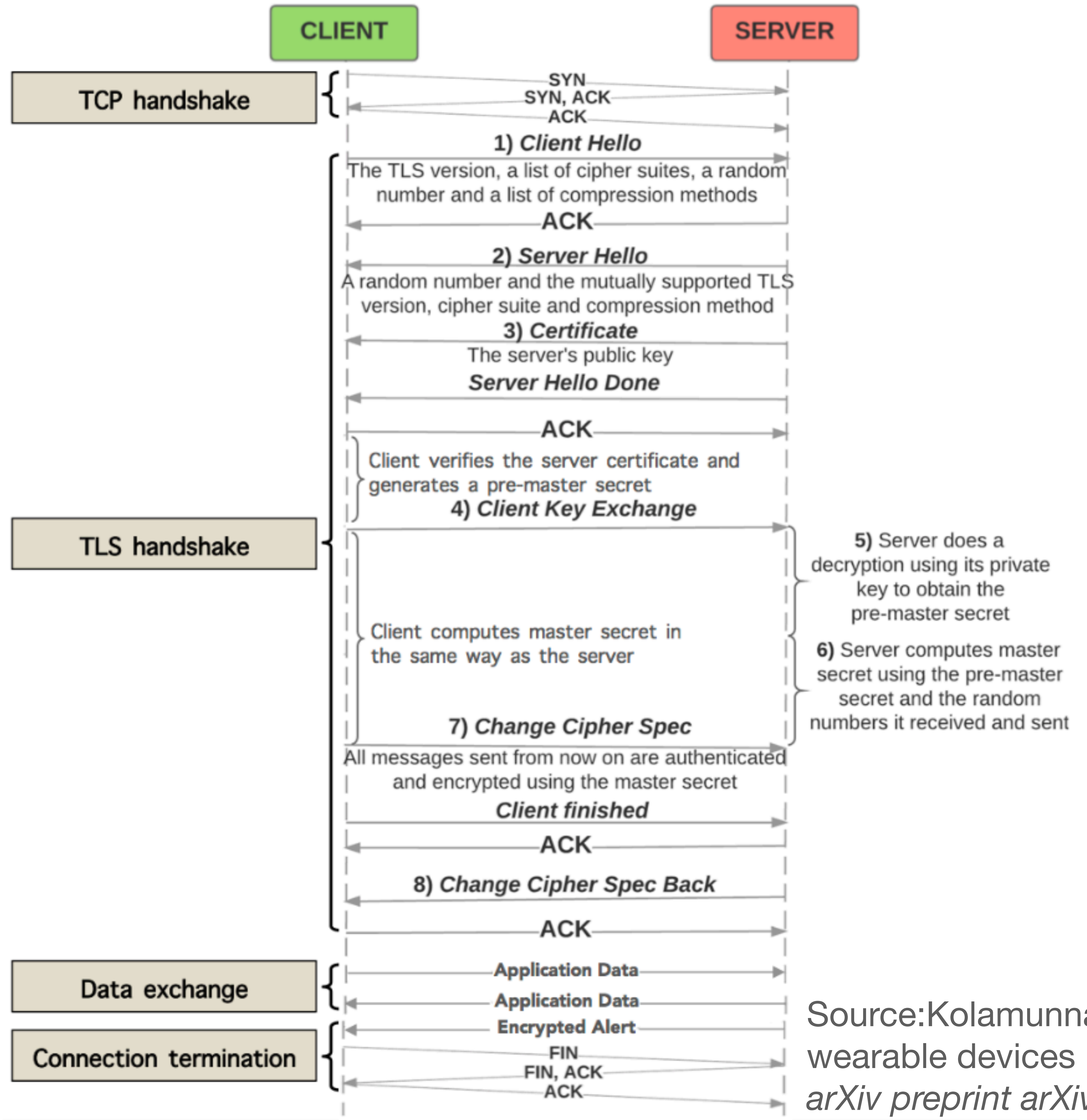
Attacks in cryptography

What is the practicality of their implementation and execution?

- Brute force attack
- Ciphertext-only attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Known plaintext attack
- Key and algorithm attack
- Differential cryptanalysis
- Linear cryptanalysis
- Side channel attacks
- Replay attacks
- Man-In-The-Middle
- Birthday Attack

HTTPS, TLS

As representative examples of protocols



CLIENT

SERVER

TCP handshake

SYN

SYN, ACK

ACK

1) *Client Hello*

The TLS version, a list of cipher suites, a random number and a list of compression methods

ACK

2) *Server Hello*

A random number and the mutually supported TLS version, cipher suite and compression method

3) *Certificate*

The server's public key

Server Hello Done

ACK

Client verifies the server certificate and generates a pre-master secret

4) *Client Key Exchange*

5) Server does a decryption using its private key to obtain the pre-master secret

Client computes master secret in the same way as the server

6) Server computes master secret using the pre-master secret and the random numbers it received and sent

TLS handshake

7) *Change Cipher Spec*

All messages sent from now on are authenticated and encrypted using the master secret

Client finished

ACK

8) *Change Cipher Spec Back*

ACK

Data exchange

Application Data

Application Data

Connection termination

Encrypted Alert

FIN

FIN, ACK

ACK

In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL).

The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Source:Kolamunna, H., Chauhan, J., Hu, Y., Thilakarathna, K., Perino, D., Makaroff, D., & Seneviratne, A. (2016). Are wearable devices ready for HTTPS? Measuring the cost of secure communication protocols on wearable devices. *arXiv preprint arXiv:1608.04180*.

CA & Certificates

Certificate Authority (CA)

Certification authority (**CA**) is an entity that:

- stores,
- signs,
- issues digital certificates.

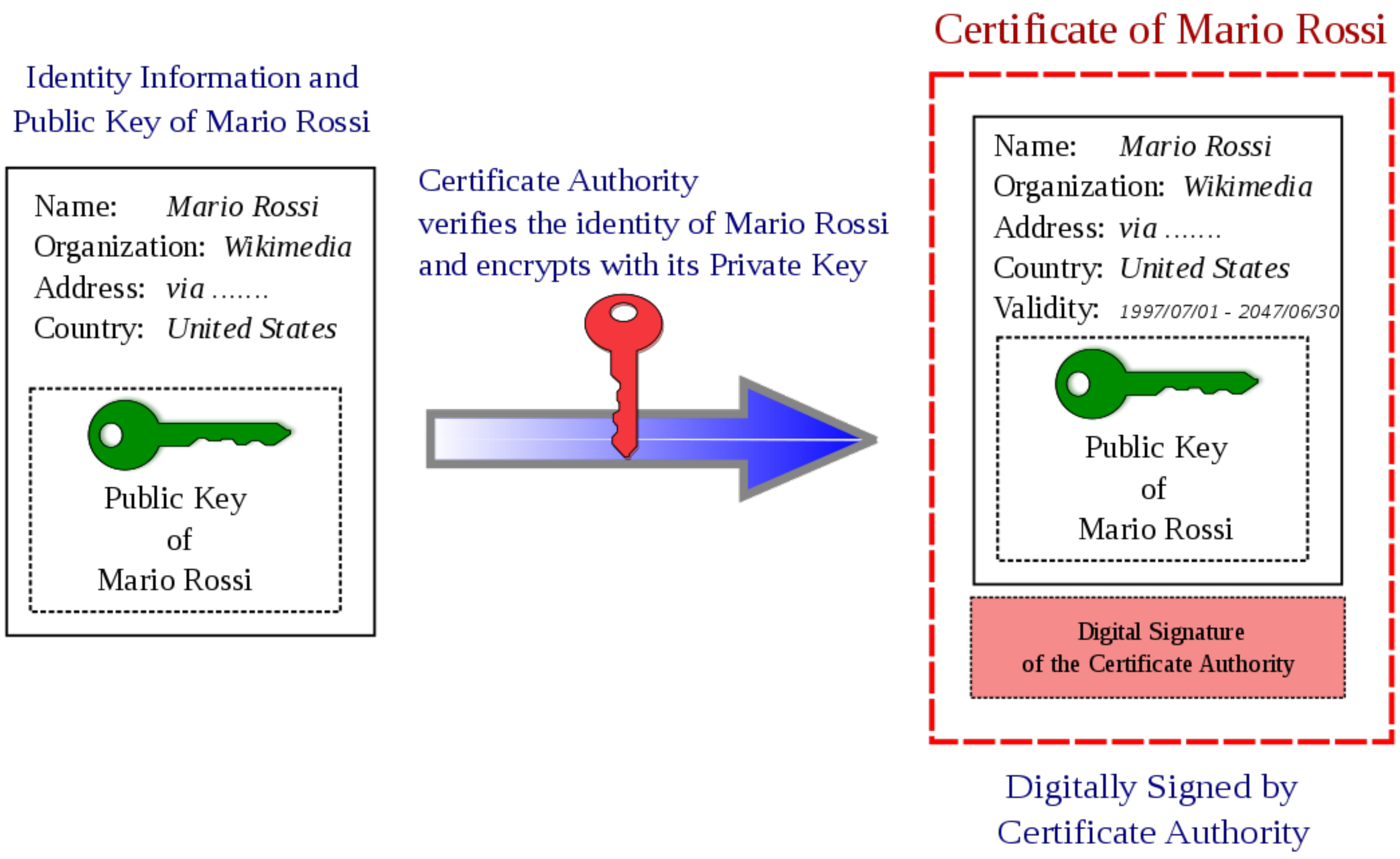
A digital certificate certifies the ownership of a public key by the named subject of the certificate.

This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key.

A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.

CA & Certificates

Certificate Authority (CA)



Source (09.12.22): https://en.wikipedia.org/wiki/Certificate_authority

CA & Certificates

Authorization certificate

In computer security, an attribute certificate, or authorization certificate (AC)is a digital document containing attributes associated to the holder by the issuer.

When the associated attributes are mainly used for the purpose of authorization, AC is called authorization certificate.

CA & Certificates

Authorization certificate - contents

- Version
- Holder
- Issuer
- Signature algorithm
- Serial number
- Validity period
- Attributes
- Signature value

Vulnerabilities

Basic terms

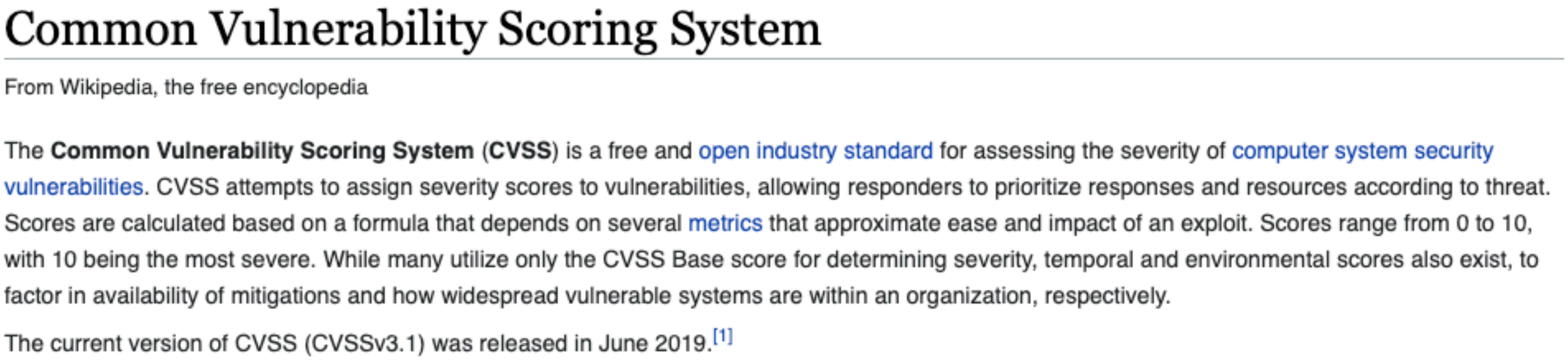
- **Vulnerability**: a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability.

- **Threat**: the likelihood or frequency of a harmful event occurring.

- **Risk**: the relative impact that an exploited vulnerability would have to a user's environment.

CVSS

What does wikipedia have to say about it?



Common Vulnerability Scoring System

From Wikipedia, the free encyclopedia

The **Common Vulnerability Scoring System** (**CVSS**) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease and impact of an exploit. Scores range from 0 to 10, with 10 being the most severe. While many utilize only the CVSS Base score for determining severity, temporal and environmental scores also exist, to factor in availability of mitigations and how widespread vulnerable systems are within an organization, respectively.

The current version of CVSS (CVSSv3.1) was released in June 2019.[1]

CVSS

Numeric system

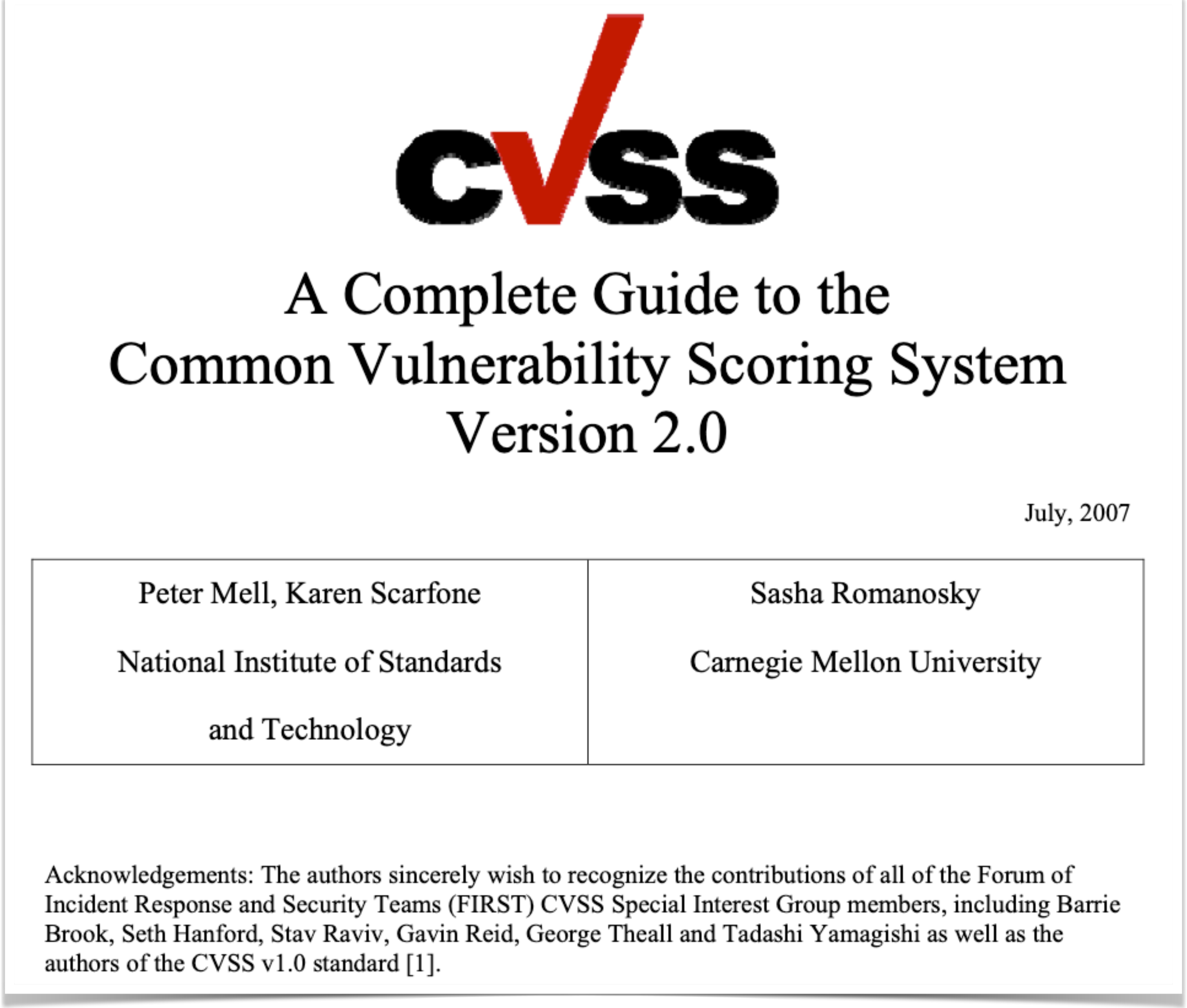
Numeric system for define the potential threat individual components pose to a system.

- 0.0 = No threat to the system
- 0.1-3.9 = Low
- 4.0-6.8 = Medium
- 7.0-8.9 = High
- 9.0 - 10.0 = Critical

The lower the score, the less risky the vulnerability poses to the entire system, whereas a 10.0 score needs to be addressed immediately.

Where to find professional information about CVSS?

[https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51198]



A Complete Guide to the Common Vulnerability Scoring System Version 2.0

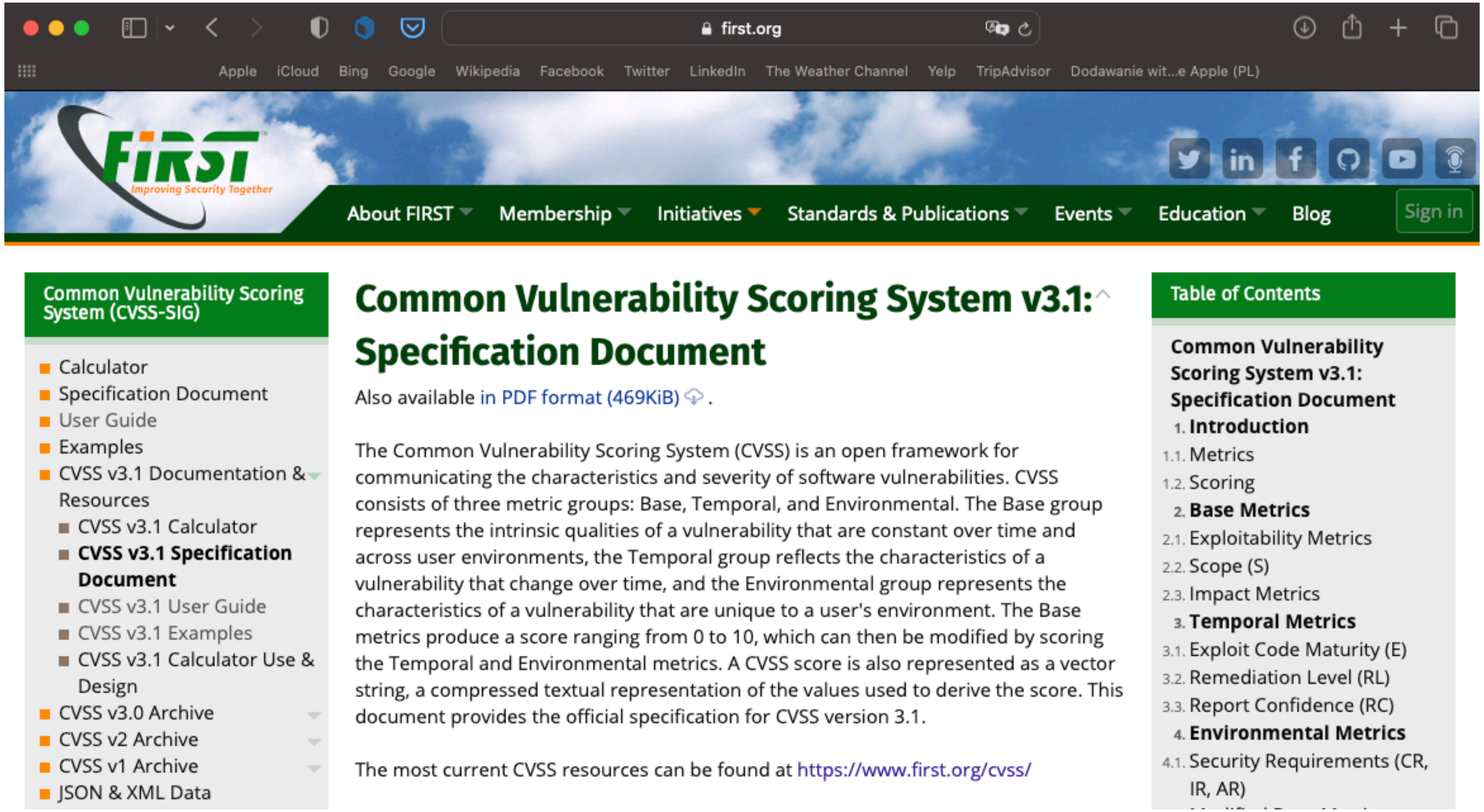
July, 2007

Peter Mell, Karen Scarfone National Institute of Standards and Technology	Sasha Romanosky Carnegie Mellon University

Acknowledgements: The authors sincerely wish to recognize the contributions of all of the Forum of Incident Response and Security Teams (FIRST) CVSS Special Interest Group members, including Barrie Brook, Seth Hanford, Stav Raviv, Gavin Reid, George Theall and Tadashi Yamagishi as well as the authors of the CVSS v1.0 standard [1].

Where to find professional information about CVSS?

[https://www.first.org/cvss/v3-1/]



Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- User Guide
- Examples
- CVSS v3.1 Documentation & Resources
  - CVSS v3.1 Calculator
  - **CVSS v3.1 Specification Document**
  - CVSS v3.1 User Guide
  - CVSS v3.1 Examples
  - CVSS v3.1 Calculator Use & Design
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data

Common Vulnerability Scoring System v3.1: Specification Document

Also available in PDF format (469KiB) .

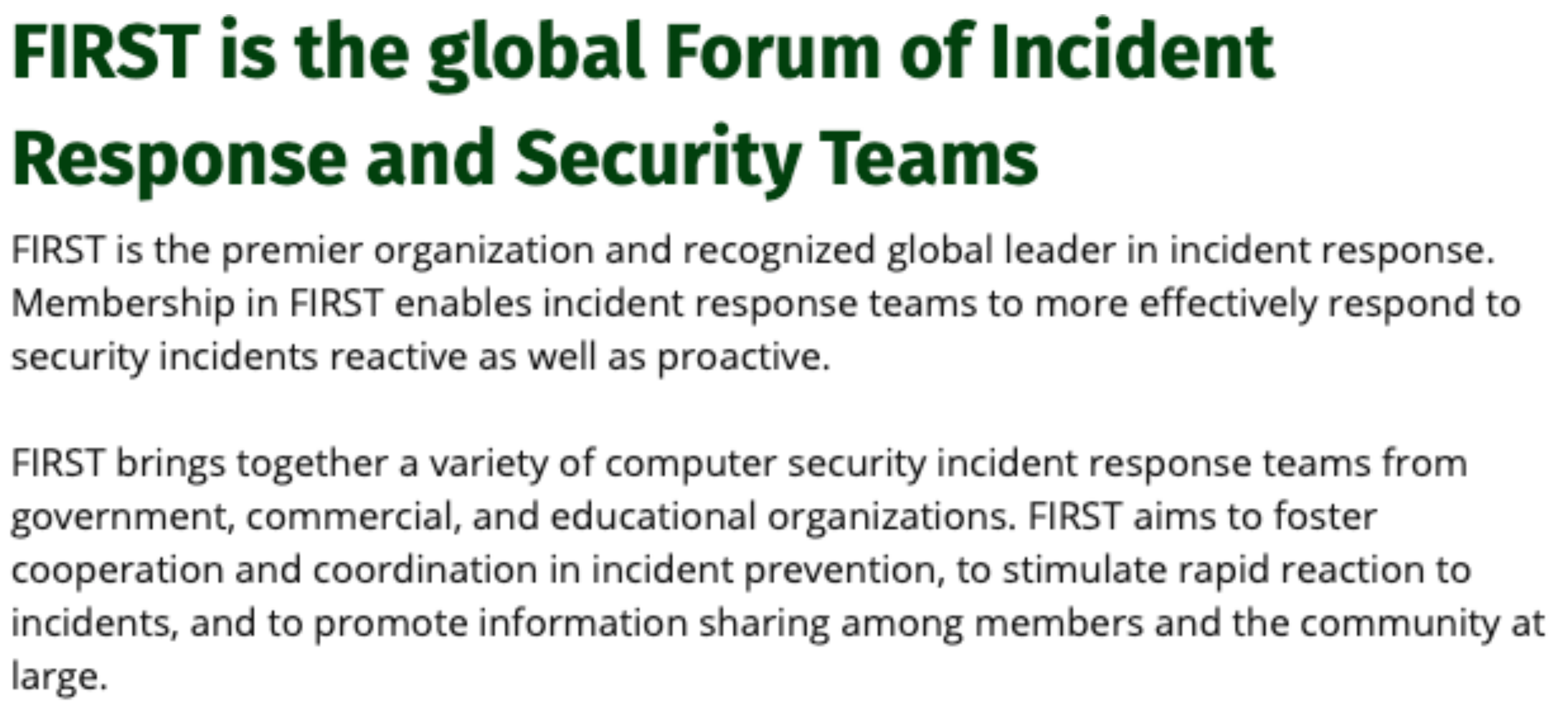
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 3.1.

The most current CVSS resources can be found at https://www.first.org/cvss/

Table of Contents

FIRSR.org

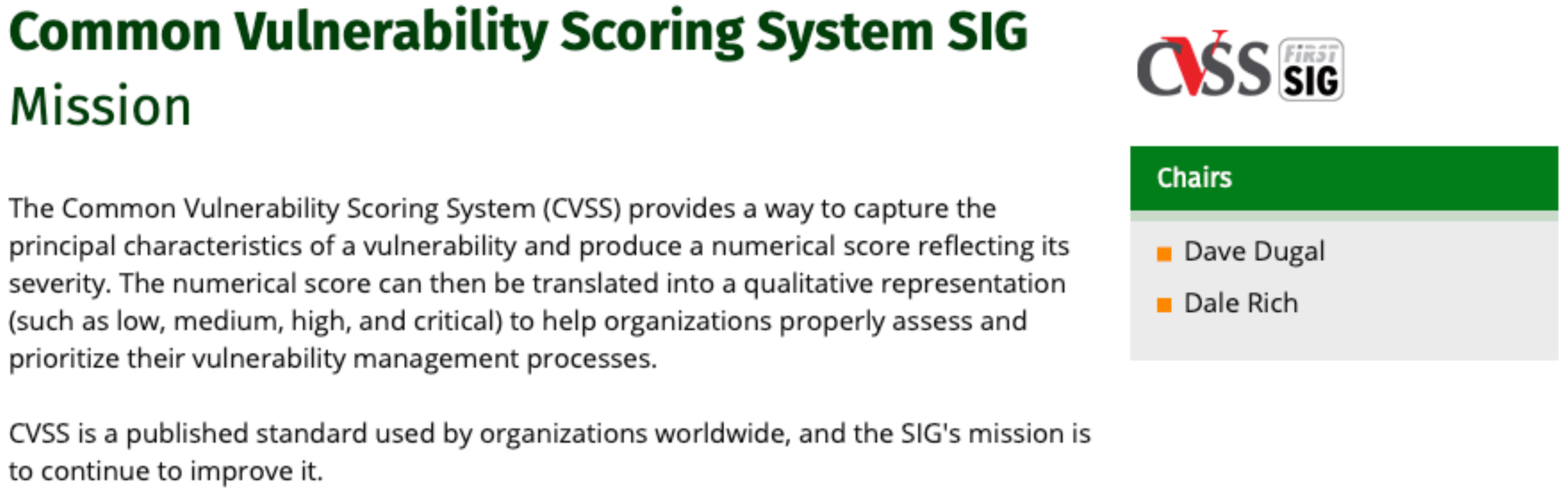
What do they do?



FIRST is the global Forum of Incident Response and Security Teams

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.



Common Vulnerability Scoring System SIG

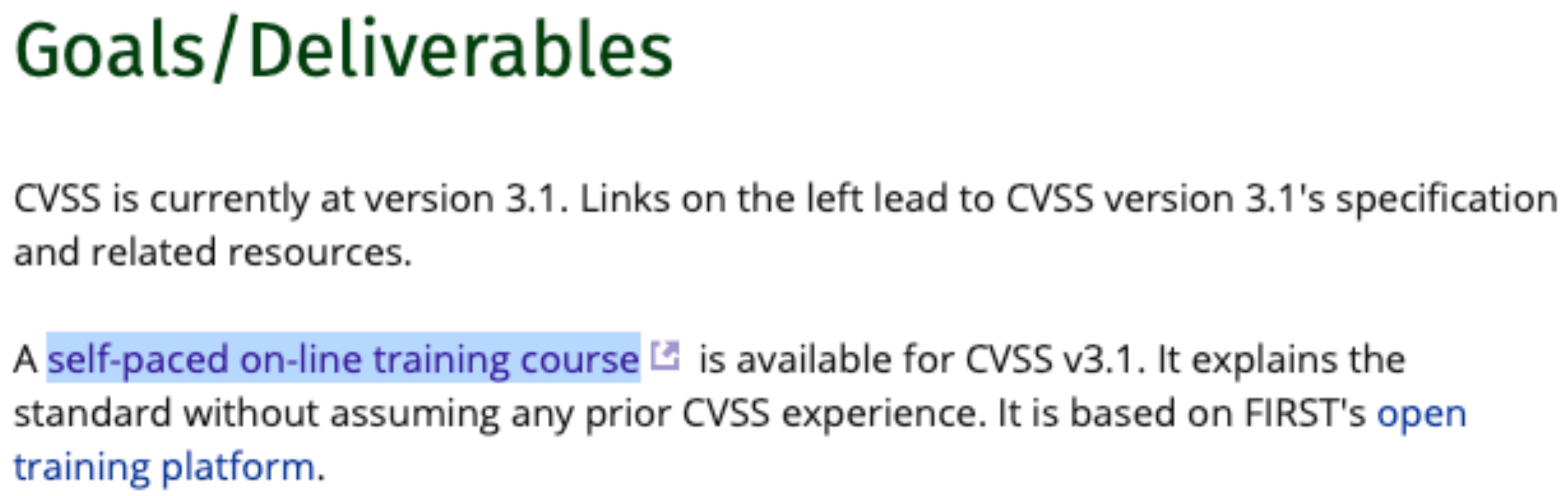
Mission

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.

Chairs

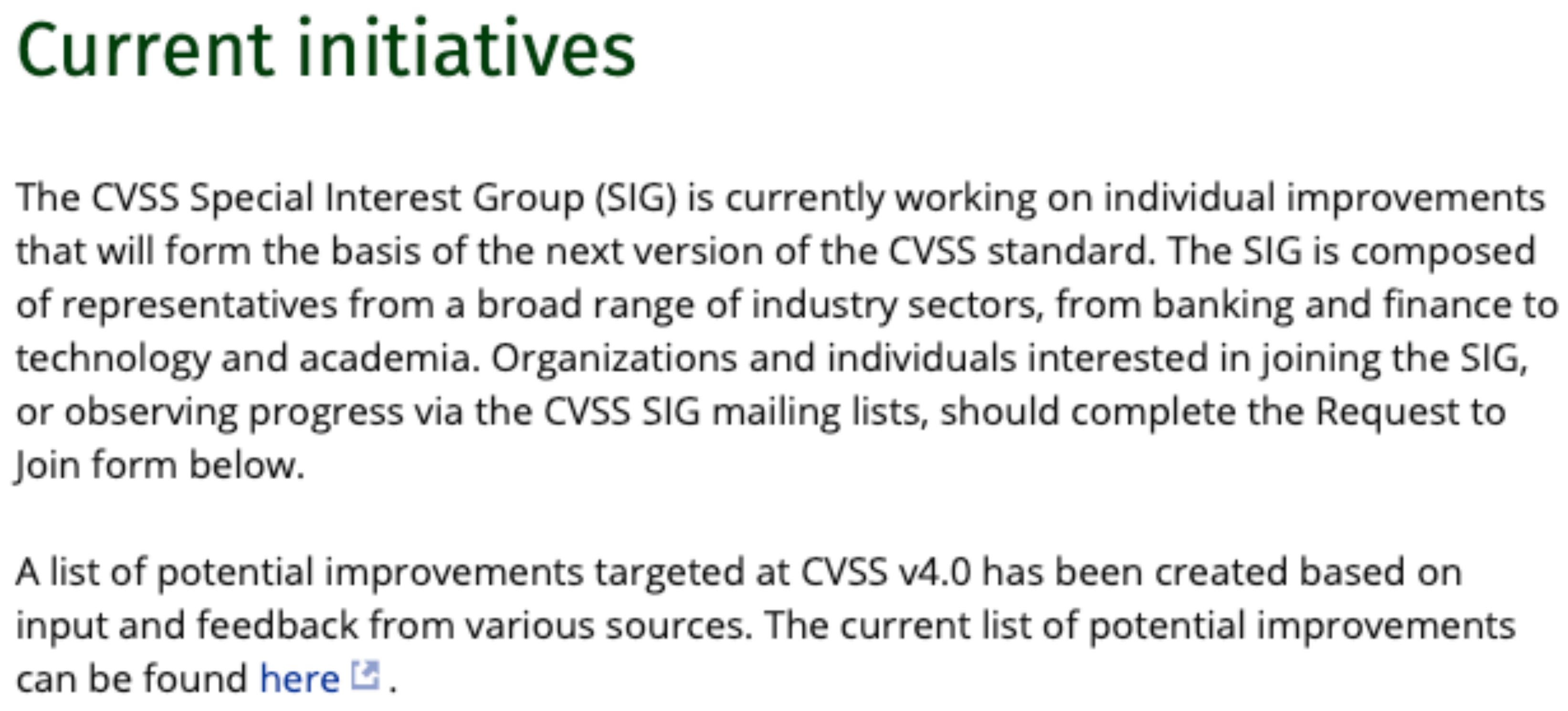
- Dave Dugal
- Dale Rich



Goals/Deliverables

CVSS is currently at version 3.1. Links on the left lead to CVSS version 3.1's specification and related resources.

A self-paced on-line training course is available for CVSS v3.1. It explains the standard without assuming any prior CVSS experience. It is based on FIRST's open training platform.



Current initiatives

The CVSS Special Interest Group (SIG) is currently working on individual improvements that will form the basis of the next version of the CVSS standard. The SIG is composed of representatives from a broad range of industry sectors, from banking and finance to technology and academia. Organizations and individuals interested in joining the SIG, or observing progress via the CVSS SIG mailing lists, should complete the Request to Join form below.

A list of potential improvements targeted at CVSS v4.0 has been created based on input and feedback from various sources. The current list of potential improvements can be found here.

Who is using CVSS?

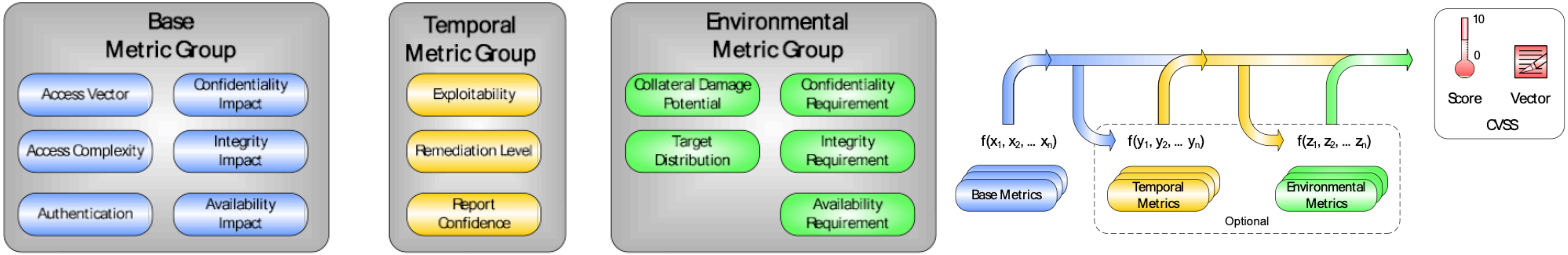
Utility rationale

- Vulnerability Bulletin Providers
- Software Application Vendors
- User Organizations:
- Vulnerability Scanning and Management:
- Security (Risk) Management:

CVSS

Metric groups

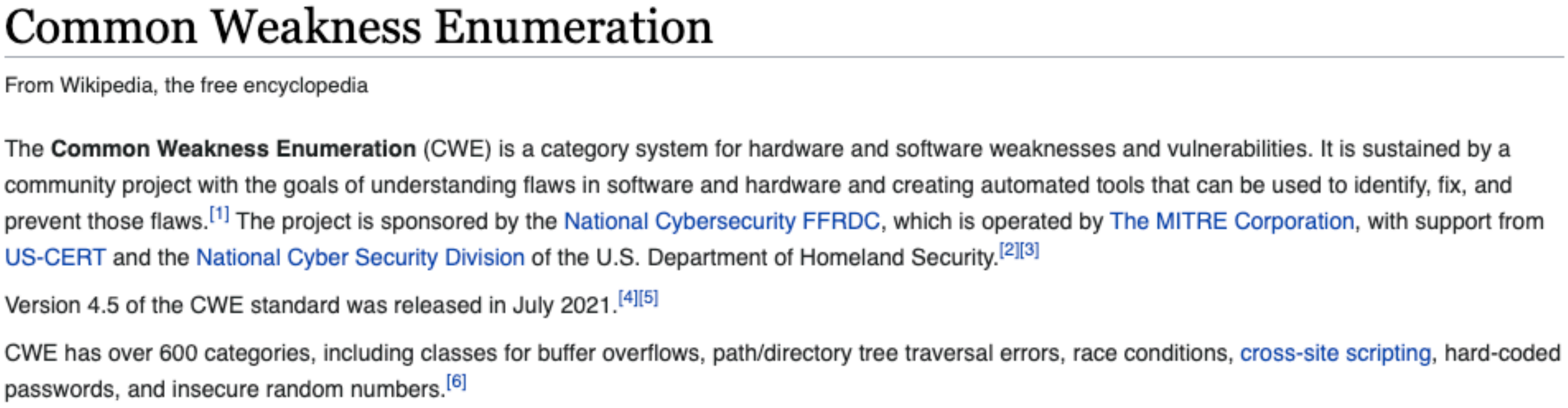
CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics



Source (12.12.22): https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51198

CWE

What does wikipedia have to say about it?



Common Weakness Enumeration

From Wikipedia, the free encyclopedia

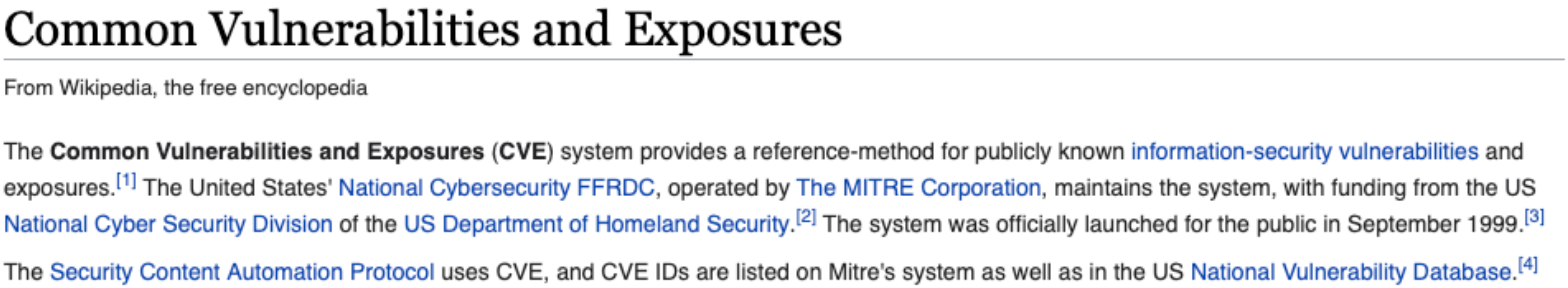
The **Common Weakness Enumeration** (CWE) is a category system for hardware and software weaknesses and vulnerabilities. It is sustained by a community project with the goals of understanding flaws in software and hardware and creating automated tools that can be used to identify, fix, and prevent those flaws.[1] The project is sponsored by the National Cybersecurity FFRDC, which is operated by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security.[2][3]

Version 4.5 of the CWE standard was released in July 2021.[4][5]

CWE has over 600 categories, including classes for buffer overflows, path/directory tree traversal errors, race conditions, cross-site scripting, hard-coded passwords, and insecure random numbers.[6]

CVE

What does wikipedia have to say about it?



Common Vulnerabilities and Exposures

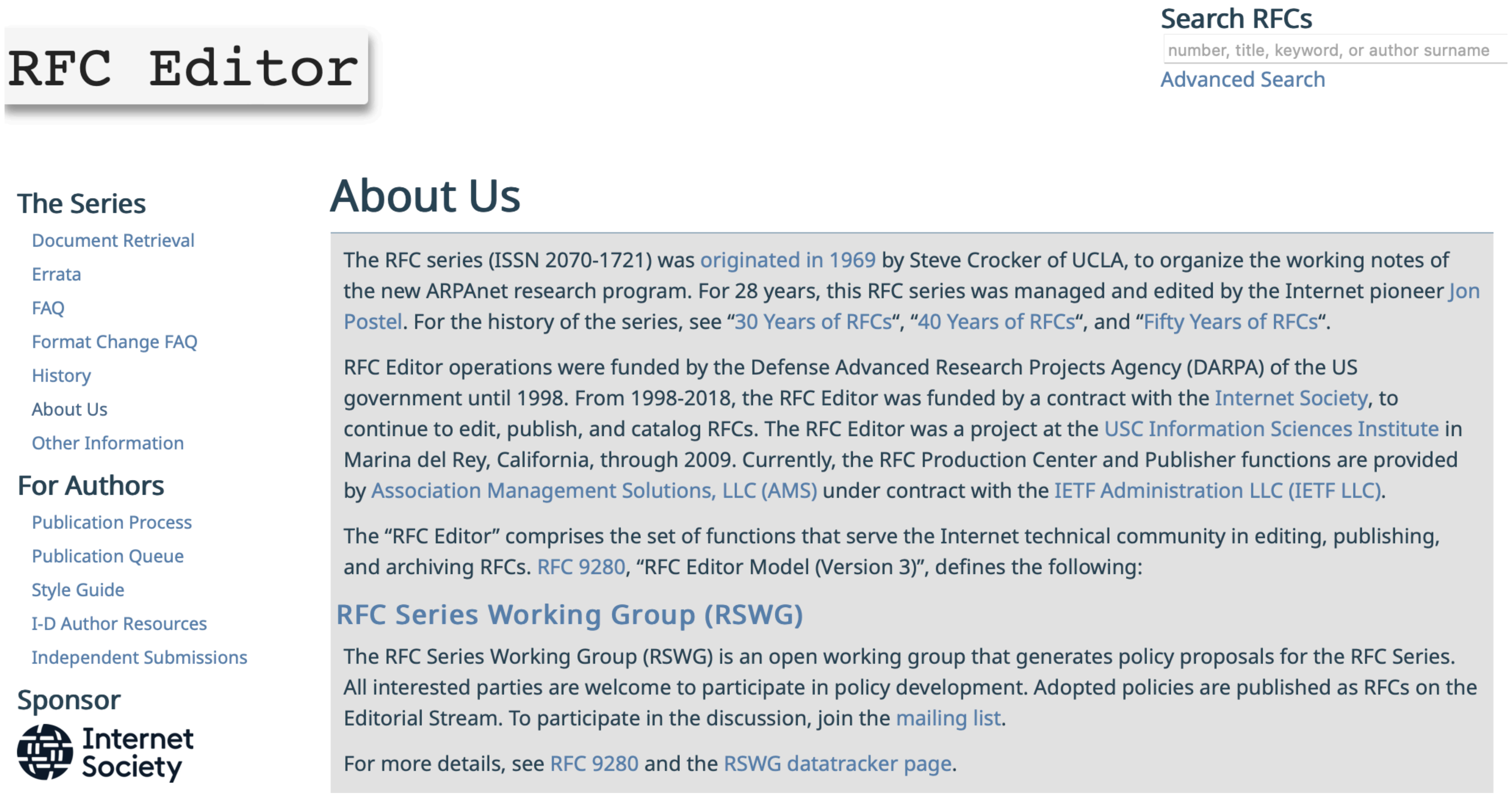
From Wikipedia, the free encyclopedia

The **Common Vulnerabilities and Exposures** (**CVE**) system provides a reference-method for publicly known information-security vulnerabilities and exposures.[1] The United States' National Cybersecurity FFRDC, operated by The MITRE Corporation, maintains the system, with funding from the US National Cyber Security Division of the US Department of Homeland Security.[2] The system was officially launched for the public in September 1999.[3]

The Security Content Automation Protocol uses CVE, and CVE IDs are listed on Mitre's system as well as in the US National Vulnerability Database.[4]

Standardization of security approach

RFC



RFC Editor

Search RFCs

number, title, keyword, or author surname

Advanced Search

The Series
- Document Retrieval
- Errata
- FAQ
- Format Change FAQ
- History
- About Us
- Other Information

For Authors
- Publication Process
- Publication Queue
- Style Guide
- I-D Author Resources
- Independent Submissions

Sponsor

Internet Society

About Us

The RFC series (ISSN 2070-1721) was originated in 1969 by Steve Crocker of UCLA, to organize the working notes of the new ARPAnet research program. For 28 years, this RFC series was managed and edited by the Internet pioneer Jon Postel. For the history of the series, see "30 Years of RFCs", "40 Years of RFCs", and "Fifty Years of RFCs".

RFC Editor operations were funded by the Defense Advanced Research Projects Agency (DARPA) of the US government until 1998. From 1998-2018, the RFC Editor was funded by a contract with the Internet Society, to continue to edit, publish, and catalog RFCs. The RFC Editor was a project at the USC Information Sciences Institute in Marina del Rey, California, through 2009. Currently, the RFC Production Center and Publisher functions are provided by Association Management Solutions, LLC (AMS) under contract with the IETF Administration LLC (IETF LLC).

The "RFC Editor" comprises the set of functions that serve the Internet technical community in editing, publishing, and archiving RFCs. RFC 9280, "RFC Editor Model (Version 3)", defines the following:

RFC Series Working Group (RSWG)

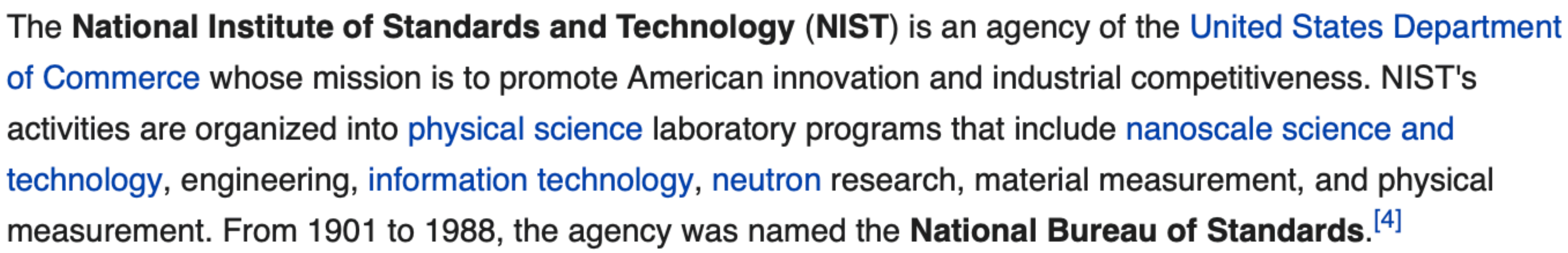
The RFC Series Working Group (RSWG) is an open working group that generates policy proposals for the RFC Series. All interested parties are welcome to participate in policy development. Adopted policies are published as RFCs on the Editorial Stream. To participate in the discussion, join the mailing list.

For more details, see RFC 9280 and the RSWG datatracker page.

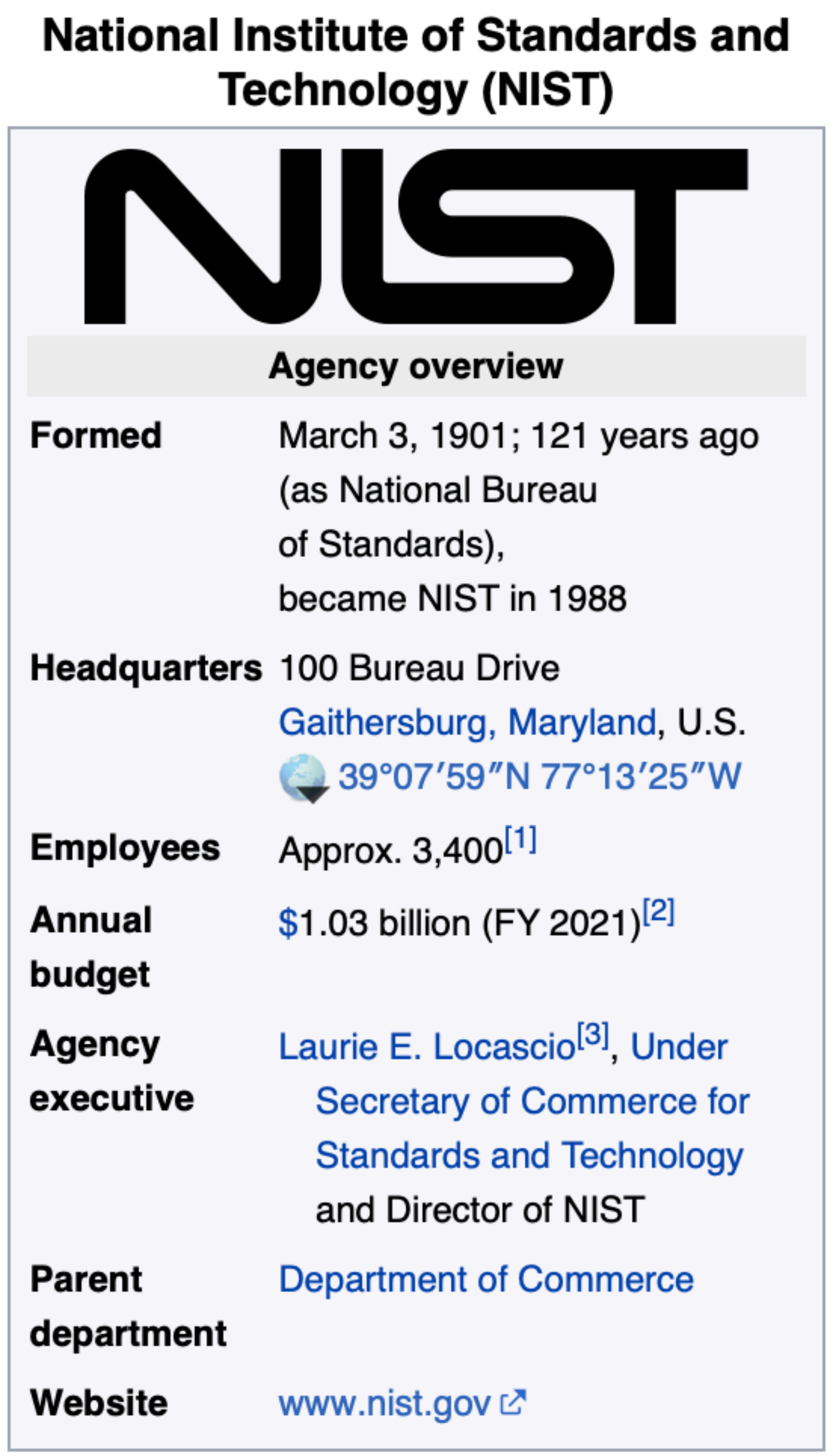
Selected examples (20.12.22): https://www.rfc-editor.org/rfc/rfc7696

Standardization of security approach

NIST - What does wikipedia have to say about it?



The **National Institute of Standards and Technology** (**NIST**) is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness. NIST's activities are organized into physical science laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement. From 1901 to 1988, the agency was named the **National Bureau of Standards**.[4]



National Institute of Standards and Technology (NIST)

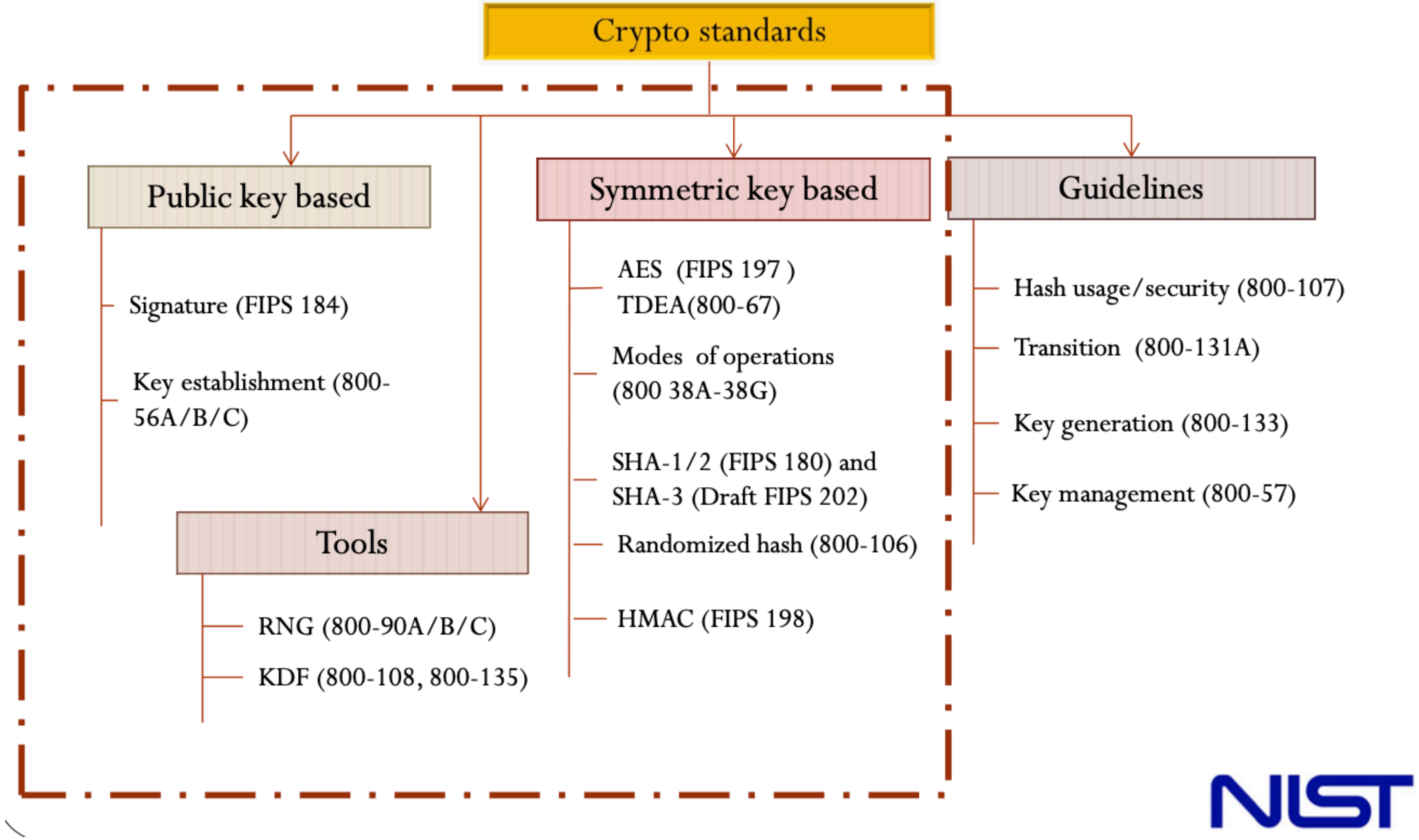
NIST

Agency overview

Formed	March 3, 1901; 121 years ago (as National Bureau of Standards), became NIST in 1988
Headquarters	100 Bureau Drive Gaithersburg, Maryland, U.S. 39°07′59″N 77°13′25″W
Employees	Approx. 3,400[1]
Annual budget	$1.03 billion (FY 2021)[2]
Agency executive	Laurie E. Locascio[3], Under Secretary of Commerce for Standards and Technology and Director of NIST
Parent department	Department of Commerce
Website	www.nist.gov

Standardization of security approach

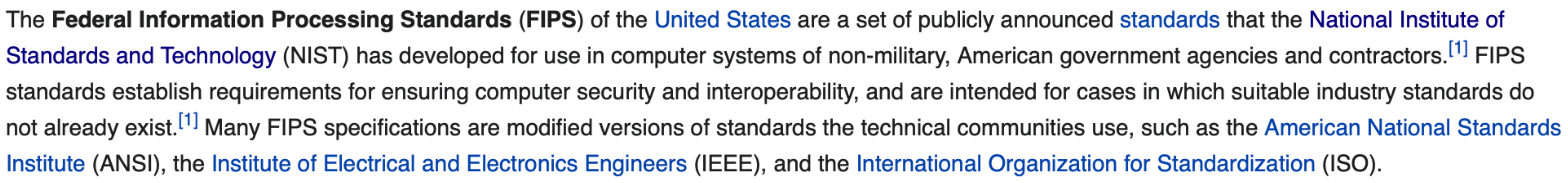
Some NIST standards



Full source (29.11.22): https://csrc.nist.gov/CSRC/media/Presentations/NIST-Cryptographic-Standards-Their-Adoptions-in/images-media/ispab_june-11_crypto-standards_lchen.pdf

Standardization of security approach

FIPS - What does wikipedia have to say about it?



The **Federal Information Processing Standards** (**FIPS**) of the United States are a set of publicly announced standards that the National Institute of Standards and Technology (NIST) has developed for use in computer systems of non-military, American government agencies and contractors.[1] FIPS standards establish requirements for ensuring computer security and interoperability, and are intended for cases in which suitable industry standards do not already exist.[1] Many FIPS specifications are modified versions of standards the technical communities use, such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), and the International Organization for Standardization (ISO).

Standardization of security approach

FIPS types

FIPS 137 (Federal Standard for Linear Predictive Coding)

FIPS 140 (Security requirements for cryptography modules)

FIPS 153 (3D graphics)

FIPS 197 (Rijndael / AES cipher)

FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems)

FIPS 201 (Personal Identity Verification for Federal Employees and Contractors)

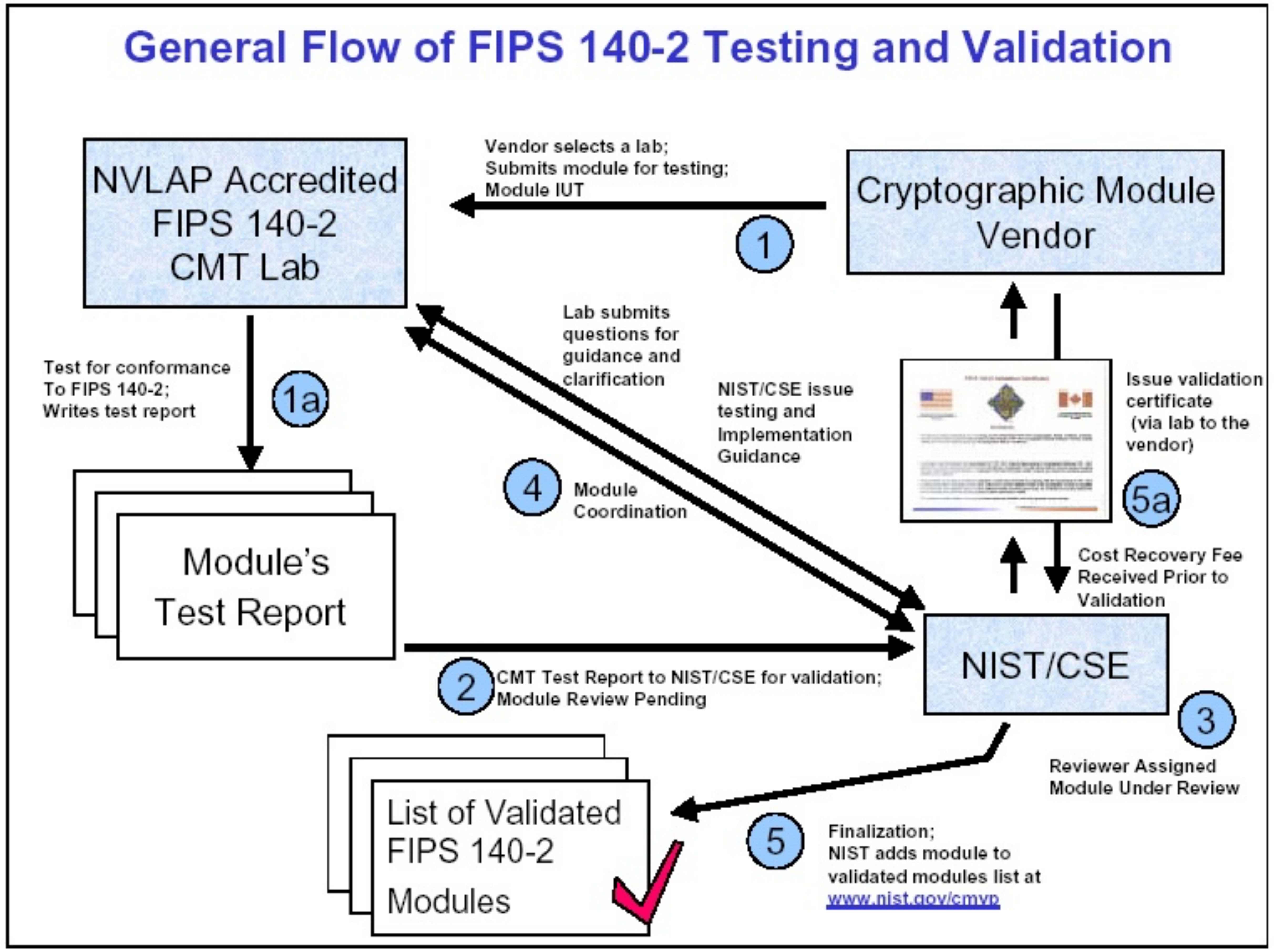
Standardization of security approach

FIPS 140 - 4 levels of security

- **FIPS 140-2 Level 1** the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent.
- **FIPS 140-2 Level 2** adds requirements for physical tamper-evidence and role-based authentication.
- **FIPS 140-2 Level 3** adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- **FIPS 140-2 Level 4** makes the physical security requirements more stringent, and requires robustness against environmental attacks.

Standardization of security approach

Validation process for FIPS 140-2



General Flow of FIPS 140-2 Testing and Validation

NVLAP Accredited FIPS 140-2 CMT Lab

Cryptographic Module Vendor

1 Vendor selects a lab; Submits module for testing; Module IUT

1a Test for conformance To FIPS 140-2; Writes test report

Module's Test Report

Lab submits questions for guidance and clarification

NIST/CSE issue testing and Implementation Guidance

4 Module Coordination

2 CMT Test Report to NIST/CSE for validation; Module Review Pending

NIST/CSE

3 Reviewer Assigned Module Under Review

5a Issue validation certificate (via lab to the vendor)

Cost Recovery Fee Received Prior to Validation

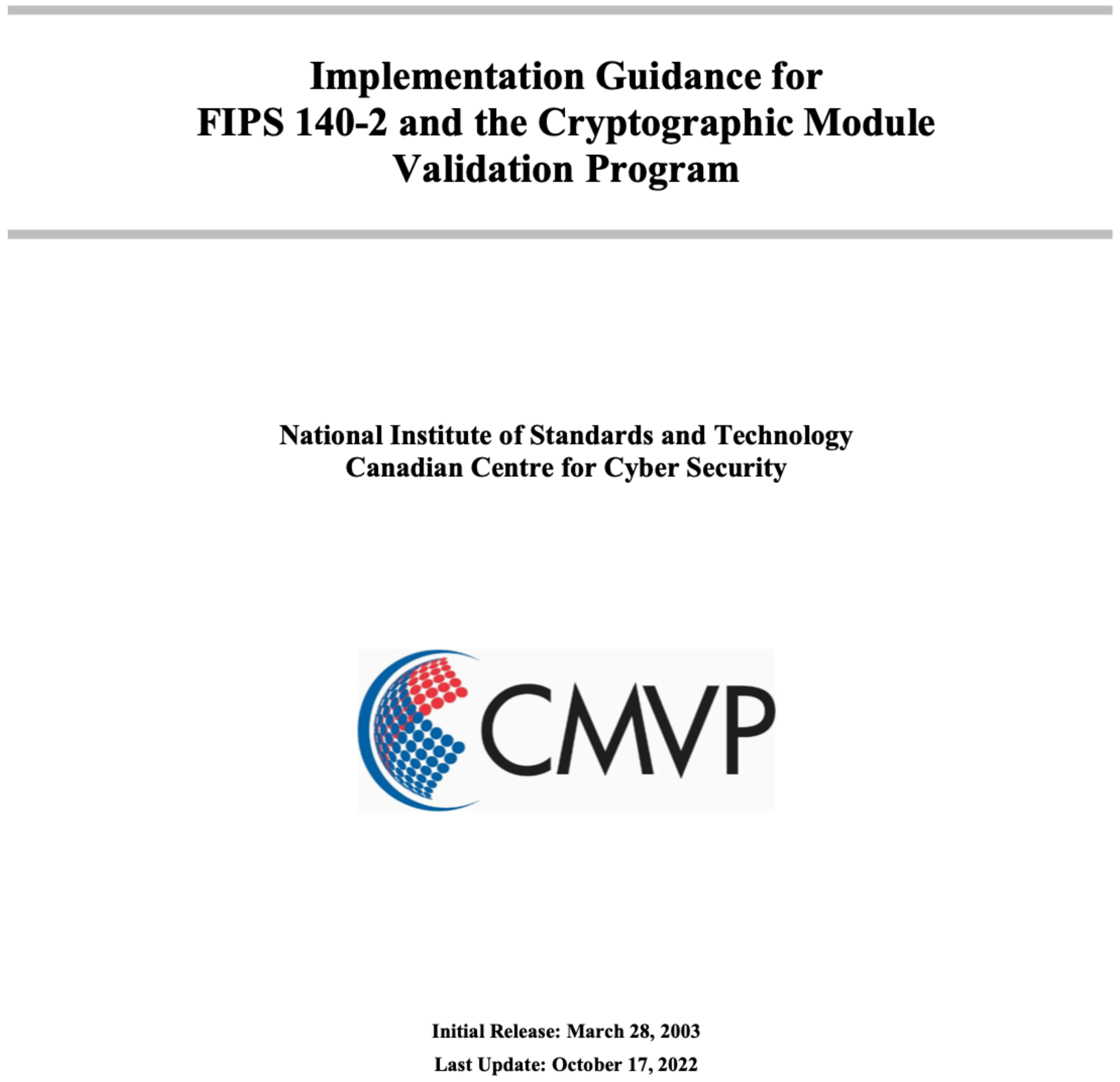
5 Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

List of Validated FIPS 140-2 Modules

Source (16.12.22): https://en.wikipedia.org/wiki/FIPS_140-2

Standardization of security approach

FIPS 140-2



**Implementation Guidance for
FIPS 140-2 and the Cryptographic Module
Validation Program**

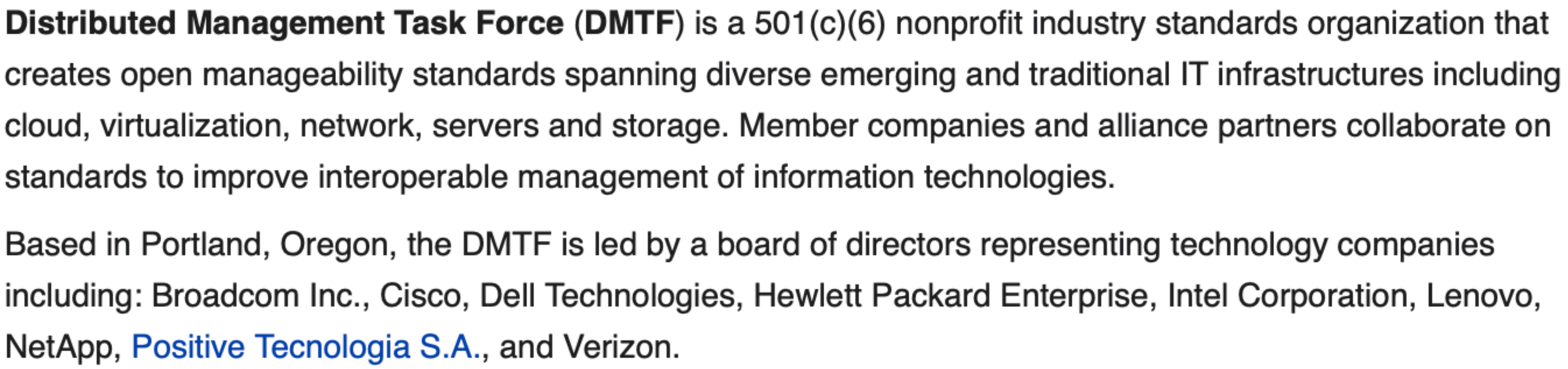
**National Institute of Standards and Technology
Canadian Centre for Cyber Security**

**Initial Release: March 28, 2003
Last Update: October 17, 2022**

Source (18.12.22): https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

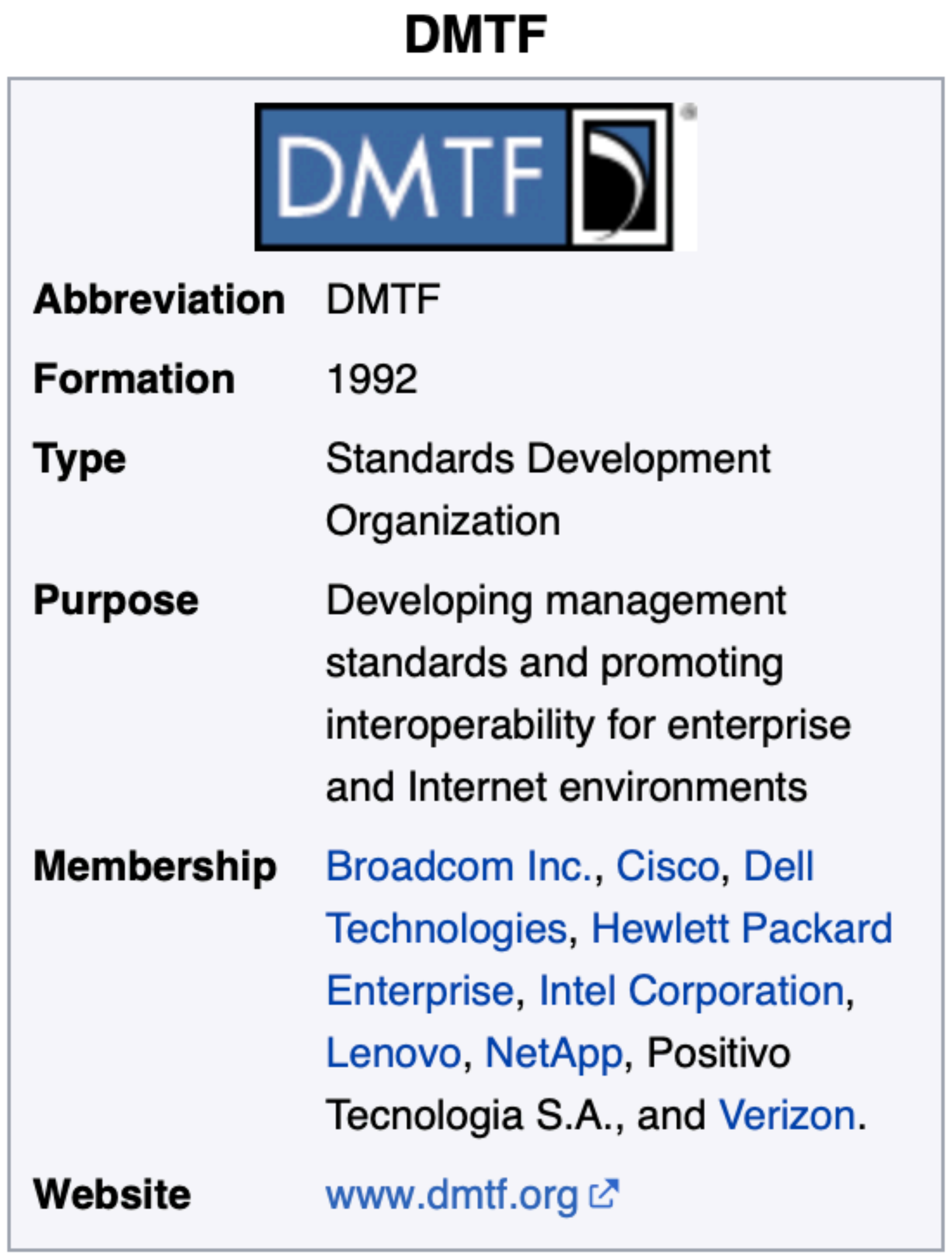
Standardization of security approach

DMTF - What does wikipedia have to say about it?



Distributed Management Task Force (**DMTF**) is a 501(c)(6) nonprofit industry standards organization that creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage. Member companies and alliance partners collaborate on standards to improve interoperable management of information technologies.

Based in Portland, Oregon, the DMTF is led by a board of directors representing technology companies including: Broadcom Inc., Cisco, Dell Technologies, Hewlett Packard Enterprise, Intel Corporation, Lenovo, NetApp, Positive Tecnologia S.A., and Verizon.

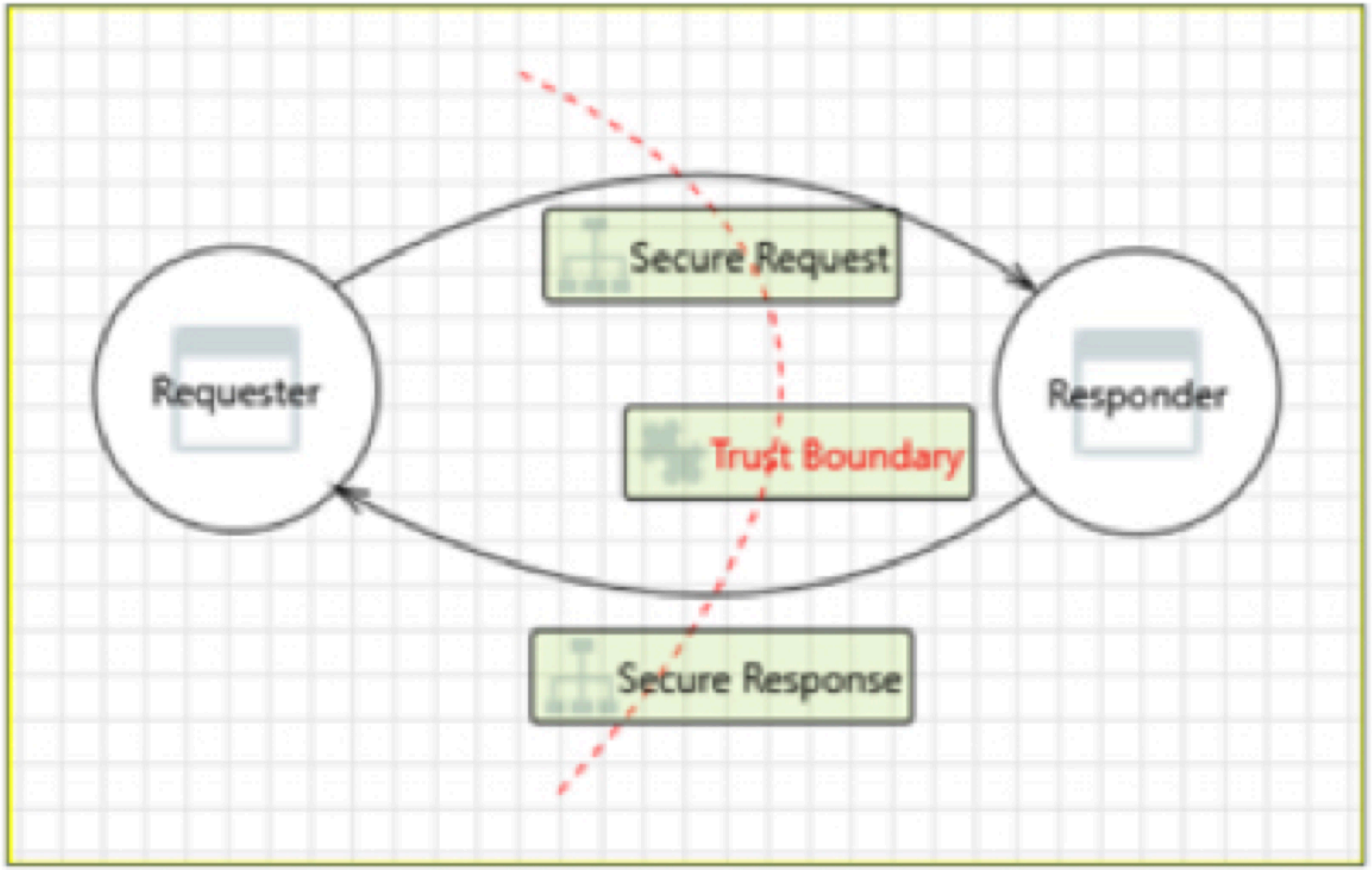


DMTF

Abbreviation	DMTF
Formation	1992
Type	Standards Development Organization
Purpose	Developing management standards and promoting interoperability for enterprise and Internet environments
Membership	Broadcom Inc., Cisco, Dell Technologies, Hewlett Packard Enterprise, Intel Corporation, Lenovo, NetApp, Positivo Tecnologia S.A., and Verizon.
Website	www.dmtf.org

Standardization of security approach

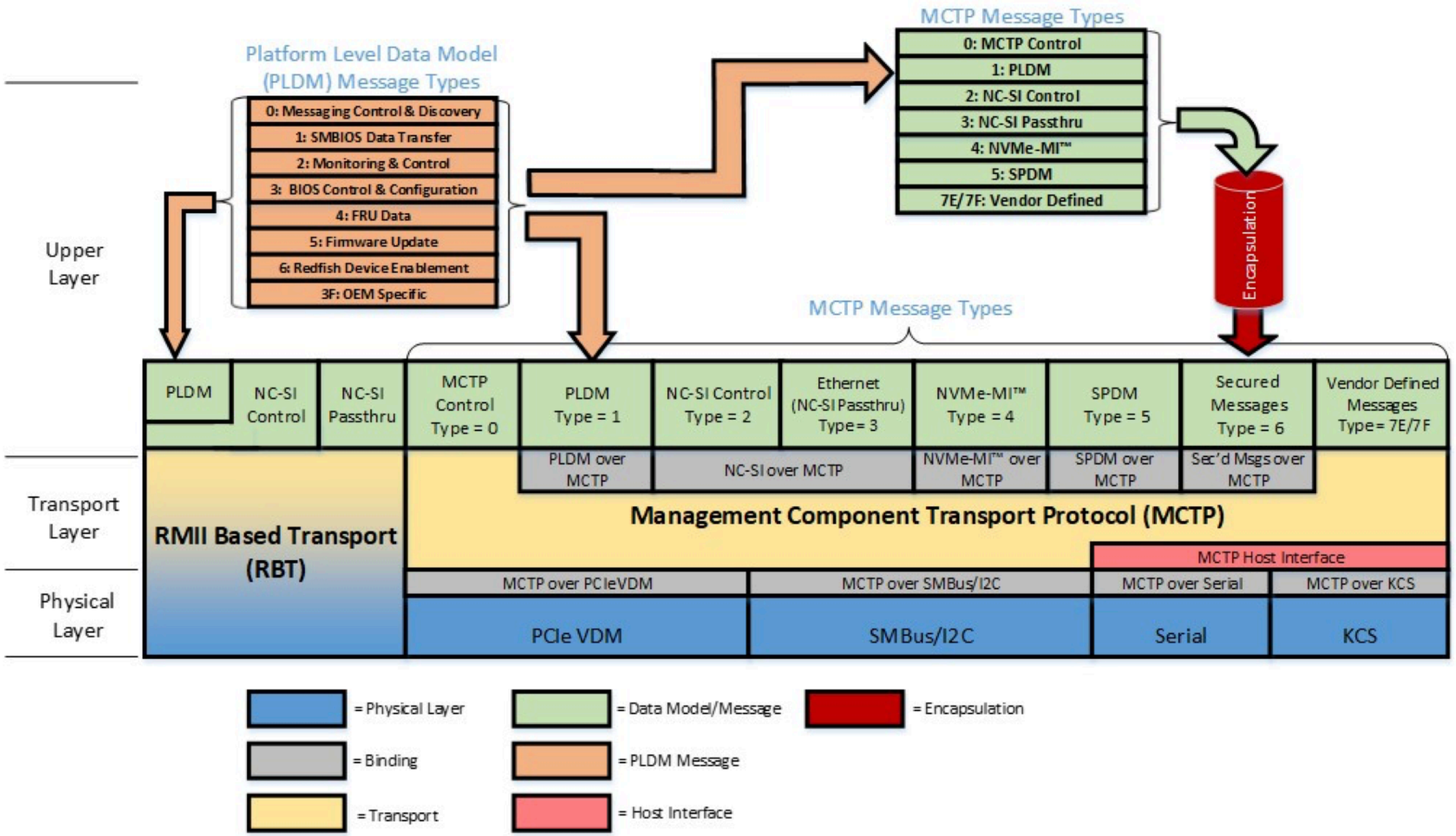
SPDM threat model



Source (19.12.22): https://www.dmtf.org/sites/default/files/standards/documents/DSP2058_1.2.0.pdf

Standardization of security approach

SPDM over MCTP



Platform Level Data Model (PLDM) Message Types

- 0: Messaging Control & Discovery
- 1: SMBIOS Data Transfer
- 2: Monitoring & Control
- 3: BIOS Control & Configuration
- 4: FRU Data
- 5: Firmware Update
- 6: Redfish Device Enablement
- 3F: OEM Specific

MCTP Message Types

- 0: MCTP Control
- 1: PLDM
- 2: NC-SI Control
- 3: NC-SI Passthru
- 4: NVMe-MI™
- 5: SPDM
- 7E/7F: Vendor Defined

Encapsulation

Upper Layer

Transport Layer

Physical Layer

MCTP Message Types

PLDM | NC-SI Control | NC-SI Passthru | MCTP Control Type = 0 | PLDM Type = 1 | NC-SI Control Type = 2 | Ethernet (NC-SI Passthru) Type = 3 | NVMe-MI™ Type = 4 | SPDM Type = 5 | Secured Messages Type = 6 | Vendor Defined Messages Type = 7E/7F

PLDM over MCTP | NC-SI over MCTP | NVMe-MI™ over MCTP | SPDM over MCTP | Sec'd Msgs over MCTP

RMII Based Transport (RBT)

Management Component Transport Protocol (MCTP)

MCTP Host Interface

MCTP over PCIeVDM | MCTP over SMBus/I2C | MCTP over Serial | MCTP over KCS

PCIe VDM | SMBus/I2C | Serial | KCS

🟦 = Physical Layer

⬜ = Binding

🟨 = Transport

🟩 = Data Model/Message

🟧 = PLDM Message

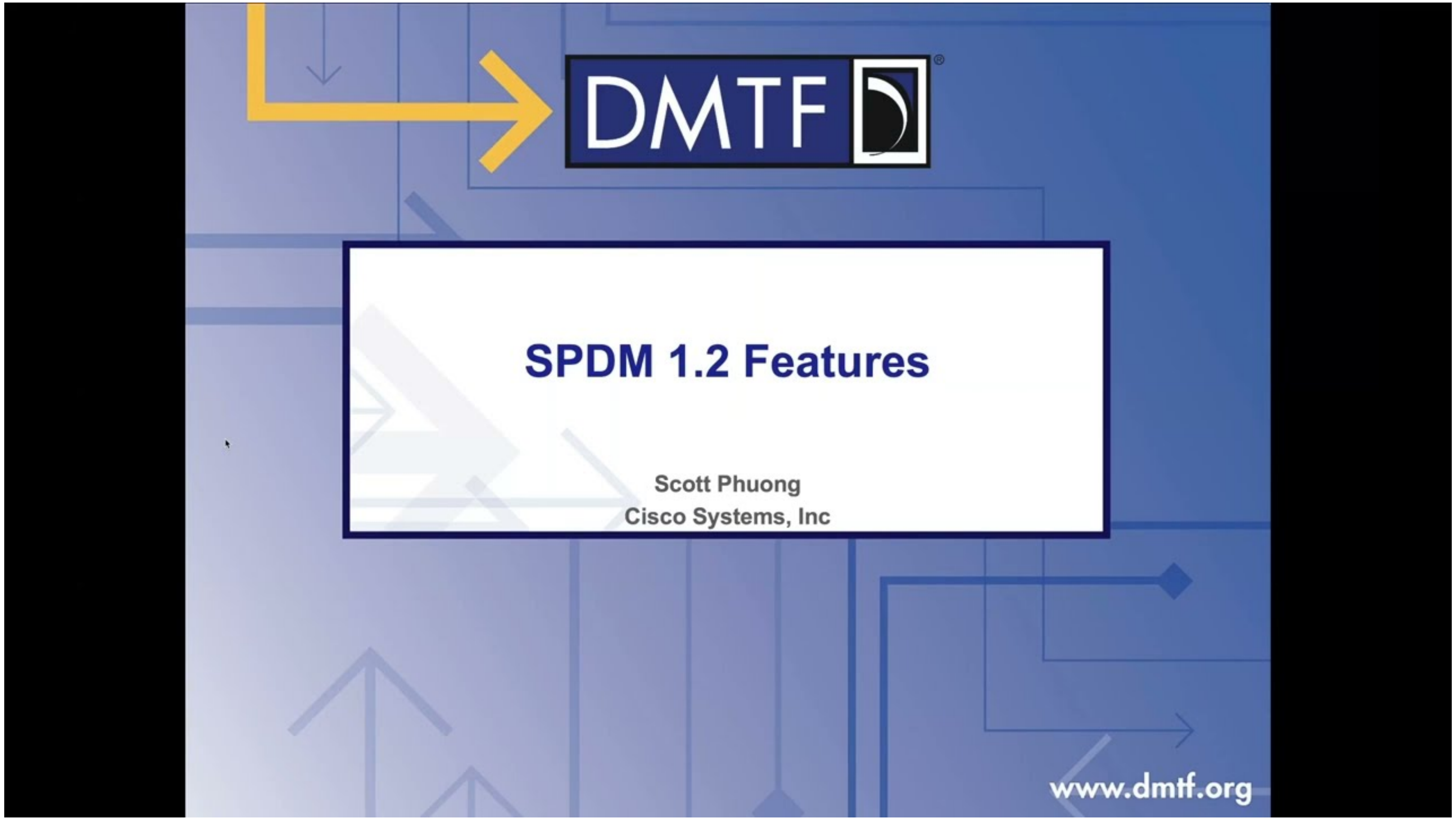
🟥 = Host Interface

🟥 = Encapsulation

Source (19.12.22): https://www.dmtf.org/sites/default/files/standards/documents/DSP2058_1.2.0.pdf

Standardization of security approach

DMTF (SPDM protocol) - external video for teaching purposes



SPDM 1.2 Features

Scott Phuong
Cisco Systems, Inc