National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

2018 Report

NIAP continued to make a difference in 2018 – from increasing the number of evaluated products available for U.S. National Security System (NSS) procurement, to further collaboration with industry and U.S. government (USG), and to representing the U.S. in the international Common Criteria Recognition Arrangement (CCRA). In 2018, NIAP focused on automation efforts that increase evaluation/certification consistency. NIAP continues to pursue activities which provide the most value for our users, meeting US government National Security Customer needs.

Automation

NIAP demonstrated efficiency and collaboration through the use of next-generation tooling to develop Protection Profiles, automate Security Target (ST) generation, and support evaluation activity reporting. Subject matter experts supporting NIAP developed a formally-defined XML schema that provides structure for PPs. Use of this schema and tooling available on GitHub, enabled collaborative development of PPs through the use of the Git versioning system, with all changes fully transparent on GitHub. Using such a schema allowed PPs to be viewed as web pages, creating a more dynamic document experience. Nearly a dozen NIAP PPs have already been produced or transitioned to this schema.

The schema also enabled NIAP to pursue automated ST generation. Automated generation of STs becomes possible when PPs are structured according to a well-defined schema, such as that described above. NIAP demonstrated such automated generation of STs during a session at ICCC. This work is expected to spare manual checking and ensure fidelity between NIAP-Approved PPs and STs. While currently available to the Common Criteria community via GitHub, NIAP is working on finalizing this tool for official roll-out.

Interested?

Visit https://github.com/commoncriteria

NIAP also participates in the Common Criteria Users Forum (CCUF) Test Automation Working Group, focused on developing and publishing a set of best practice recommendations for test automation in CC. NIAP is supportive of test automation, where it makes sense, and focusing evaluation time on harder (less prescriptive) security testing.

Process Improvements

NIAP continued to focus on infrastructure improvements through website enhancements and development of web tools used to assist in the evaluation process. NIAP rolled out a new Entropy Assessment Report (EAR) tool to assist with the Check-in review of all new product evaluations. The tool serves multiple purposes for NIAP, including enhanced communication and tracking capabilities, protection of proprietary data, and increased visibility into NIAP project details, which facilitates metrics collection and process improvements. These enhancements improve the Check-in timeline.

NIAP also rolled out a new mechanism to submit official requests for products evaluated in other Schemes to be considered for posting on the NIAP Product Compliant List (PCL). This tool provides a centralized tracking capability for all submitted requests, as well as a communication feature which allows NIAP to easily share updates with the requestor.

The development of these web support tools have improved communications and assisted NIAP in its goal to streamline, improve, and ensure consistency of all evaluations.

Evaluated Products

A total of 79 evaluations were completed in 2018, a 25% increase from 2017. NIAP continued to implement strategies to streamline and improve both the evaluation and validation processes. These strategies ensured consistency among evaluations, increased output, and made more products eligible for NSS procurement.

Network devices comprised the majority of evaluations again this year. This indicates the continued priority of ensuring a device will "behave," regardless of the ultimate security purpose of the device.

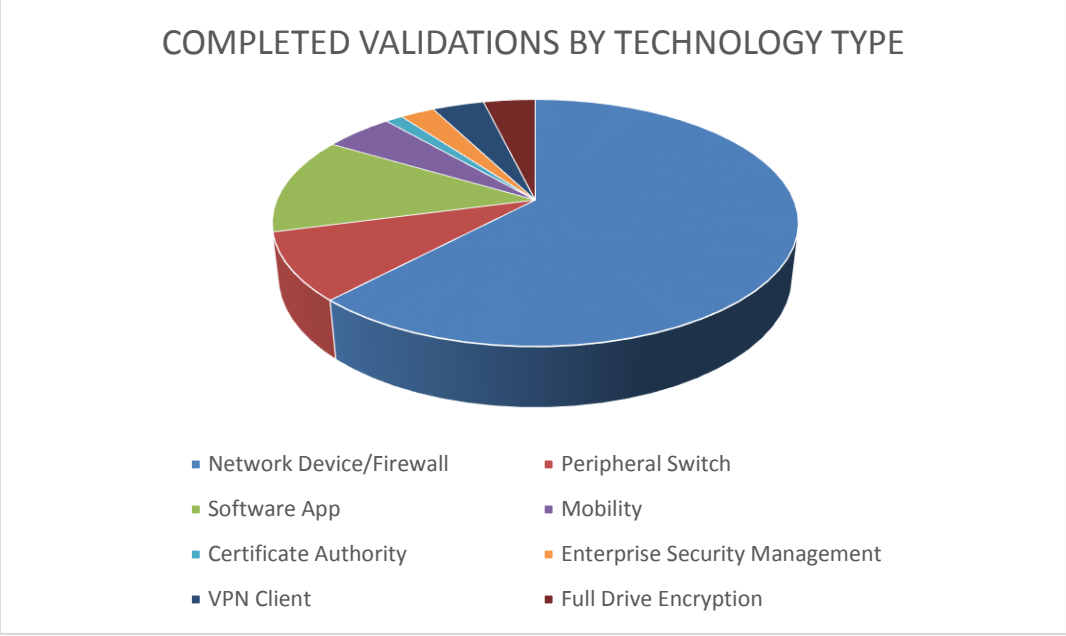


Figure 1. 2018 Completed Validations by Technology Type

Protection Profiles (PPs)

In 2018, NIAP concentrated on development of PP-Modules and Packages, especially with respect to Exact Conformance. As expected, this was a learning curve and required additional time and attention in order to meet both the standard and NIAP goals with respect to clarity and NSS customer needs.

As seen in Figure 2, NIAP published 3 updates to existing PPs, which define security requirements and test activities for a wide range of commercial technologies and 1 new Functional Package. Most notable is the publication of the first NIAP Functional Package. This package, for Transport Layer Security (TLS), describes the security functionality for the TLS secure communication protocol in a way that can be used by PP authors including requirements for TLS or DTLS functionality. A single package containing the security requirements provides consistency in specification and evaluation of such protocols. NIAP presented this work at CCUF in the hopes that the broader community will accept and adopt such an approach.

PPs Completed in CY2018

Product	Technology Type
Functional Package for TLS v1.0	Network Encryption
PP for General Purpose Operating Systems v4.2	Operating System
cPP for Network Devices v2.0E	Network Device
cPP for Stateful Firewalls v2.0E	Firewalls

Figure 2. 2018 Completed Protection Profiles

Did you know?

PP-modules:

- cannot be used alone. They are evaluated as part of a PP-Configuration (a combination of PP-Module(s) and PP(s)).
- complement one or more Base PPs.
- do not have SARs, just inherit the SARs from the Base PP.
- must meet all SFRs in the Base PP
  - may refine or iterate SFRs from Base PP (but cannot reduce the SFRs from the Base PP in any way).
  - can add new SFRs.

Common Criteria Recognition Arrangement (CCRA)

The NIAP successfully completed a two year role as Common Criteria Development Board (CCDB) Chair, handing over responsibility to Spain.

The Exact Conformance Trial period closed on 31 December 2018. While the trial period revealed some adjustments that need to be made to the Addenda, the feedback received from authors and reviewers of PPs and PP-Modules (with respect to the EC Addendum) was generally positive. NIAP identified two areas where simplification was necessary, and did not detract from the overarching goal of Exact Conformance. The first area deals with one Exact Conformance PP claiming Exact Conformance to another PP, and the second deals with the use of packages and Exact Conformance. Solutions were proposed and are being implemented in the ISO 15408/18405 drafts currently being worked.

CCDB Crypto Working Group

The CCDB Crypto Working Group (WG) finalized the Supporting Document Rationale and sent it to the CCDB for review and approval. In addition, the group addressed comments from other CC nations, preparing to incorporate additional ciphers to ensure better coverage of CC nations' cryptographic needs. The WG developed a draft SFR for secure protocols, leveraging the CCUF Crypto Working Group to help test the proposal. The WG provided this work to the editors of ISO 15048 Part 2 for inclusion in the new standard, along with the FCS_RBG SFR. Including mutually agreed upon cryptographic requirements enables harmonization of such requirements for use in PPs and product evaluations across all CC Schemes.

collaborative Protection Profiles (cPPs)

NIAP continued to fully support development of cPPs according to the terms of the CCRA. During 2018, industry continued to lead cPP development in international Technical Communities (iTCs) – serving as iTC leads, technical editors, participating through regular teleconferences, and setting and driving cPP development schedules. This active industry participation and collaboration with government underpins the value of the CCRA, and serves to keep it relevant and viable.

Network Device and Stateful Traffic Filter Firewall cPPs

2018 marked the third consecutive year that contributing member nations evaluated products against the international cPPs. NIAP completed 44 evaluations against the Network Device (ND) cPP, with 24 more Network Device evaluations currently in process.

NIAP completed nine evaluations against the Stateful Traffic Filter Firewall cPP with six Stateful Traffic Filter Firewall evaluations currently in process.

NIAP's validation of products against cPPs is significant in two ways:
it provides NSS users with assurance in validated commercial products, while furthering the CCRA objective of allowing industry to evaluate a product once and sell to many nations.

During the course of the ND cPP evaluations, NIAP's Network Device Technical Rapid Response Team received numerous inquiries on the cPP. NIAP worked with the Network iTC and the Network iTC Interpretation Team (NIT) to resolve questions on the cPPs to ensure consistent application of the requirements during product evaluations. NIAP published 19 Network Device Interpretation Team (NIT) Technical Decisions applicable in our scheme, making these available for all evaluations against the ND cPP. Collaboration with the NIT to resolve cPP questions ensures consistent and clear interpretation of cPP requirements and evaluation activities among all CCRA member nations and across numerous evaluations.

Full Drive Encryption (FDE) cPPs

NIAP completed three evaluations against the FDE cPPs with two more evaluations in process.

NIAP collaborated closely with the FDE iTC and the FDE Interpretations Team (FIT) to resolve questions on the cPPs to ensure consistent application of the requirements during product evaluations. NIAP forwarded 7 requests for interpretation this year and published 9 FIT Technical Decisions applicable in our scheme. NIAP participated in the FDE iTC, which continued work on an enterprise management use case and need for NSS users.

Ongoing international Technical Communities

NIAP continued participation in both the Dedicated Security Component and Software Application iTCs by collaborating with industry to define security functionality and test activities for these technologies. Both iTCs are currently working to complete their first cPP drafts in 2019. These iTCs are industry-led, demonstrating a firm commitment to industry and government collaboration.

NIAP also participated in the Biometrics Security iTC, serving as iTC members to provide insight into the NIAP Mobile Device Fundamentals PP use of Biometrics and work with the iTC to determine how this cPP may work with MDFPP evaluations. NIAP responded to questions and assisted with the testing toolbox under development.

Outreach

Throughout 2018, NIAP continued outreach efforts to ensure the commercial IT security needs of the NSS Community are met through collaborative development of commercial product security requirements and evaluation of products against those requirements. Outreach focused on delivering tailored messages suitable for the intended audience in different environments.

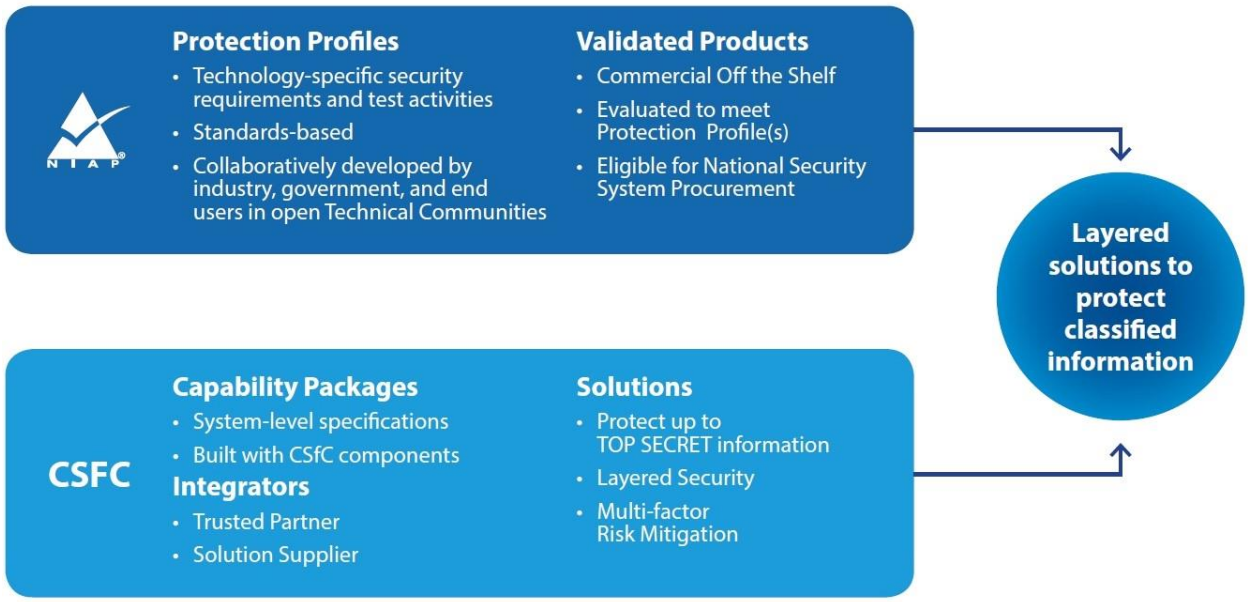
NIAP participated in several security conferences and forums in 2018 to engage directly with users, developers, and Common Criteria Users Forum delegates. These engagements helped bridge the gap between user requirements and product capabilities; and enabled NIAP to explain its process as well as provide updates to NIAP policies and procedures.

Notable conferences and forums attended included RSA, the International Cryptographic Module Conference (ICMC), TechNet Asia, Security of Things, International Common Criteria Conference, two Common Criteria Users Forums, as well as a number of Armed Forces Communications and Electronics Association (AFCEA) TechNets.

Upcoming Engagements:

RSA	March 2019
National Defense University	March 2019
CCUF	April 2019
ICMC	May 2019

Commercial Solutions for Classified



A NIAP validation is the foundational requirement for a product to be included as part of the CSfC program. Vendors who wish to have their products eligible as CSfC components of a composed, layered Information Assurance (IA) solution must build their products in accordance with the applicable NIAP-approved Protection Profile(s) and have their product evaluated according to NIAP requirements.

CSfC selections define the specific PP requirements that must be included as part of a Common Criteria Evaluation for a product to be eligible for use in a CSfC solution. See https://www.nsa.gov/Resources/Everyone/csfc/Components-List/ for selections per technology.

NIAP also collaborated with the CSfC PMO for a number of vendor hosted tech exchanges with cybersecurity product developers to help them understand the concept of a NIAP certification as a prerequisite to becoming part of a CSfC registered solution. These unclassified events gave vendors an opportunity to learn about unclassified technologies and standards developed or used by NSA and improve their chances of developing or selling technologies to NSA and the DoD. NIAP personnel engaged with over 100 industry reps who wanted to learn more about the NIAP mission and how it relates to CSfC and NIST, and how NIAP-validated products keep NSS customers compliant with national policy.

Collaboration with the National Institute of Standards and Technology (NIST)

NIST and NIAP continued collaboration in 2018 to align NIAP validation processes with the NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) – commonly referred to as FIPS. NIAP evaluations require that each product's cryptography have at least a CAVP certificate and preferably a CMVP certificate. NIAP PPs are written so that they can be used internationally by nations that do not participate in FIPS, but a CAVP or CMVP certificate eliminates the need for the Common Criteria Test Lab to conduct some of the PP assurance tests. By eliminating redundant cryptographic testing, CC evaluations are expedited, saving government and industry both time and money.

The NIAP/NIST alignment continues to ensure current evaluated products are available for NSS users by leveraging the results of NIST cryptographic algorithm and module validation programs in NIAP evaluations.

As a result of the NIAP/NIST alignment, during 2018:

- NIAP continued to support and participate in NIST's CMVP Industry Collaboration Working Group (CMVPWG). The CMVPWG, comprised of both industry and government representatives, met regularly throughout the year to explore opportunities for streamlining the CMVP evaluation timeline to improve the operational impact of FIPS 140 validated modules. Working group emphasis is on automated solutions that produce artifacts or evidence that can be verified efficiently by test laboratories. As a result, the Automated Cryptographic Validation Program (ACVP) was developed and will become operational in January 2019. ACVP fully automates the cryptographic algorithm testing allowing for quicker algorithm validations.
- NIAP briefed 3 sessions at the 2018 International Cryptographic Module Conference (ICMC). The conference provided an opportunity to collaborate with vendors, test labs, various policy makers and end users on cryptographic certification and the effect of technology advancements on our current paradigms.
- NIST continued to support NIAP at the CCRA Cryptographic Working Group (WG) meetings. The CCRA Cryptographic WG develops internationally accepted cryptographic evaluation requirements and assurance activities. NIST continued to provide WG participants with much-needed insight into NIST's current CAVP and CMVP testing programs as well as efforts toward the development of automated solutions for algorithm and module testing. The information provided by NIST assists the WG in the continued development of security requirements and evaluation activities for incorporation into cPPs.

International Organization for Standardization (ISO) Common Criteria Update

The Common Criteria is an international standard (ISO 15408) that provides the specification language used to define security functional requirements and test activities for evaluation of commercial IT products. The standard is used by NIAP to develop Protection Profiles used in evaluation of commercial products eligible for NSS procurement. The ISO working group (WG3) continued to solicit comments on various drafts of the updated standard, with the goal of sufficiently addressing the evolution of security functionality in commercial IT products.

The ISO standards are currently at the committee draft stage, with the second committee drafts expected for review in January 2019. NIAP reviewed and provided comments on the drafts and worked with the ISO editorial team throughout the year to ensure USG interests are embodied in the update. NIAP looks forward to the upcoming drafts and discussions on these standards.

Looking Forward

In 2019, expect additional progress on automation efforts within NIAP and other process improvements to help streamline, improve, and ensure consistency in evaluations.

NIAP is currently reviewing all policies and publications to include consideration of product acceptance and Product Compliant List (PCL) publication criteria to ensure alignment with USG-wide Supply Chain Risk Management (SCRM) efforts.

Finally, NIAP projects steady increases in the number of evaluated commercial products eligible for procurement during 2019. We will continue to foster collaboration with industry and other CCRA partners to develop Protection Profiles for evaluating COTS products needed for U.S. National Security Systems.

Have ideas, suggestions, or concerns?

NIAP would like to hear from you.

Contact us at niap@niap-ccevs.org.