National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

2019 Report

NIAP continued to make a difference in 2019 – 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), to representing the U.S. in the international Common Criteria Recognition Arrangement (CCRA). NIAP continues to pursue activities which provide the most value for our users, meeting US government National Security Customer needs.

Process Improvements

NIAP focused on infrastructure improvements through website enhancements and development of web tools used to assist in the evaluation process. In 2019, NIAP developed a new NIST Certificate Review Tool which has been officially implemented for all new product evaluations. This new tool streamlined the process, increased transparency, and reduced the review time to more efficiently complete evaluations. It improves NIAP's ability to track and manage the Certificate Reviews eliminating the dependence on email. As a result, this new feature has greatly benefited the NIAP team by reducing the time needed to complete Certificate Reviews, in line with NIAP Policy #5, thus improving overall evaluation timelines.

Handling Vulnerabilities in Evaluated Products

NIAP encourages user installation of vendor-delivered bug fixes and security patches as part of good cybersecurity practice. Frequently the consequences of not patching can be severe and effective management of vulnerabilities are an important mitigation.

In 2019, NIAP contacted more than 70 vendors with products listed on the Product Compliant List (PCL) in response to release of new vulnerabilities. NIAP Policy #17, requires vendors to report security vulnerabilities to NIAP along with a mitigation plan for their affected products. The mitigation responses provide assurance that the products on the PCL address all known security vulnerabilities, allowing National Security System customers to reduce risk of exploitation.

Evaluated Products

A total of 74 evaluations were completed in 2019. 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.

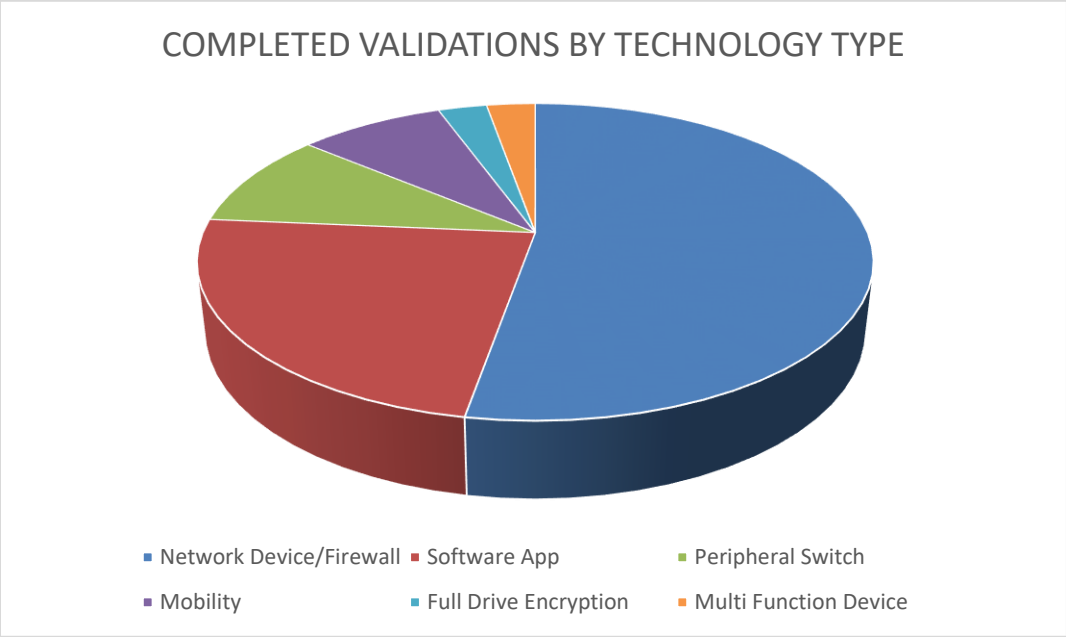

Figure 1. 2019 Completed Validations by Technology Type

Protection Profiles (PPs) and collaborative Protection Profiles (cPPs)

In 2019, NIAP developed new PPs to serve our customers. Seven (7) new Protection Profile Modules (PP-Modules), which define security requirements and test activities for TOE types complementary to one or more PPs, were published. NIAP also updated five (5) PPs/Functional Packages (FPs), converted three (3) Extended Packages to PP-Modules (in alignment with Common Criteria v3.1 Release 5), and endorsed four (4) updated collaborative Protection Profiles (cPPs).

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.

PPs Completed in CY2019

Product	New/Revision	Technology Type
cPP for FDE: Authorization Acquisition v2.0E	Minor	Encrypted Storage
cPP for FDE: Encryption Engine v2.0E	Minor	Encrypted Storage
PP for Application Software v1.3	Minor	Application Software
Functional Package for TLS v1.1	Minor	Network Encryption
cPP for Network Devices v2.1	Minor	Network Device
PP for General Purpose Operating System v4.2.1	Minor	Operating System
PP for Mobile Device Management v4.0	Major	Mobility
PP-Module for MDM Agent v1.0	Module Conversion	Mobility
PP for Peripheral Sharing Devices v4.0	Major	Peripheral Switch
PP-Module for Audio Input Devices v1.0	New	Peripheral Switch
PP-Module for Audio Output Devices v1.0	New	Peripheral Switch
PP-Module for Keyboard/Mouse Devices v1.0	New	Peripheral Switch
PP-Module for User Authentication Devices v1.0	New	Peripheral Switch
PP-Module for Video/Display Devices v1.0	New	Peripheral Switch
PP-Module for File Encryption v1.0	Module Conversion	Encrypted Storage
PP-Module for File Encryption Enterprise Management v1.0	New	Encrypted Storage
PP-Module for SSL/TLS Inspection Proxy v1.0	New	Traffic Monitoring
cPP-Module for Stateful Traffic Filter Firewalls v1.3	Minor	Firewall
PP-Module for VPN Gateways v1.0	Module Conversion	Virtual Private Network

Figure 2. 2019 Completed Protection Profiles

Common Criteria Recognition Arrangement (CCRA)

NIAP took over as Common Criteria Development Board (CCDB) liaison to the Common Criteria Users Forum (CCUF) in 2019 and looks forward to continued close collaboration between the CCDB and CCUF.

collaborative Protection Profiles (cPPs)

During 2019, 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. NIAP fully supports development of cPPs according to the terms of the CCRA.

CCDB Crypto Working Group

The CCDB Crypto Working Group (WG) finalized a general CC framework for cryptographic protocols and updates to the FCS_RBG SFR. These were both incorporated into the next International Standards Organization (ISO) update of the Common Criteria (ISO 15408). Inclusion of mutually agreed upon cryptographic requirements enables harmonization of such requirements for use in PPs and product evaluations across all CC Schemes.

Outreach

Throughout 2019, NIAP continued outreach efforts to ensure the commercial IT security needs of the NSS Community were 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 2019 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, National Defense University (NDU), the International Cryptographic Module Conference (ICMC), International EU CSA Conference, International Common Criteria Conference (ICCC), two Common Criteria Users Forums (CCUF), as well as a number of CSFC vendor engagements.

NIAP participated in the 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.

NIAP briefed two sessions at the 2019 International Cryptographic Module Conference (ICMC). The NIAP Director and a representative from NIST's Computer Security Division jointly briefed on NIST and NIAP's continued collaborative efforts. NIAP also briefed their current efforts and approach for determining and allowing for processor equivalency for NIAP cryptographic evaluations. This conference facilitated collaboration with key stakeholders on a variety of topics regarding cryptographic certification.

Upcoming Engagements:

RSA	February 2020
CCUF	March 2020
ICMC	April 2020

Commercial Solutions for Classified (CSfC)

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 Program Management Office (PMO) for a number of vendor hosted 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. NIAP participated in a panel discussion during the 2019 CSfC Tech Day, and provided detailed insight into the NIAP evaluation process to interested vendors considering going through the process for the first time. NIAP answered a variety of questions including details on NIAP's Assurance Continuity process and the criteria for extending the certificate validity date of a NIAP evaluated product. 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.

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

NIST Cryptographic Algorithm Validation Program (CAVP) and/or Cryptographic Module Validation Programs (CMVP) certificates continue to help eliminate redundant cryptographic testing within the USG, thereby, 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.

In 2019, NIST completed development of the Automated Cryptographic Validation Test System (ACVTS), i.e., NIST CAVP algorithm validation testing using an Automated Cryptographic Validation Protocol (ACVP), which fully automates the cryptographic algorithm testing allowing for quicker (almost instant) algorithm validations. NIST announced in October 2019 that the ACVTS is operational and the recommended path for obtaining algorithm validations. Effective 1 July 2020, ACVTS will be the only means of obtaining a CAVP certificate.

NIAP fully supports NIST ACVP testing and updated Policy #5: "Applicability and Relationship of NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) to NIAP's Common Criteria Evaluation and Validation Scheme (CCEVS)" and "Frequently Asked Questions for NIAP Policy #5" to align with NIST's ACVP. The (new) NIAP Policy #5 takes effect 01 March 2020. Notable changes included:

- The updated policy mandates that the evaluation documentation describe all tested configurations down to processor manufacturer, model number, and microarchitecture version (e.g. Intel Xeon E5-2620v1, Sandy Bridge) and requires it to match the processor specified on the CAVP certificate.
- While equivalency arguments may be accepted for products and platforms, the updated policy mandates that at least one product instance must be fully tested on at least one platform with all cryptography mapped to a CAVP certificate. This ensures that the operational environment claimed in evaluations closely aligns with the operational environment for which the cryptographic algorithms were validated.
- NIAP recognizes NIST CAVP/CMVP certificates regardless of whether CAVS or ACVT was used. However, the ACVTS includes tests for some evaluation activities (for example, testing for 4096-

bit RSA keys) that are not included in the CAVS tool. Therefore, the ACVP testing is required to meet those assurance activities.

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 standards are currently moving forward to the Draft International Standard (DIS) stage and are expected to be sent out for final review/vote mid-year 2020. Any comments will be discussed at the Fall 2020 ISO meetings and if no substantial issues or objections are raised, they will be published in Fall 2021. NIAP continued to review and provide comments on the drafts and worked with the ISO editorial team throughout the year to ensure USG interests are embodied in the update.

Looking Forward

In 2020, NIAP projects steady increases in the number of evaluated commercial products eligible for procurement. NIAP 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. This includes efforts to provide solutions for conducting evaluations of products residing in virtual environments where the platform is ever-changing.

In addition, expect further progress on automation efforts within NIAP as work continues to streamline, improve, and ensure consistency in evaluations.

Have ideas, suggestions, or concerns?

NIAP would like to hear from you.

Contact us at niap@niap-ccevs.org.