ITL BULLETIN FOR SEPTEMBER 2018

AUTOMATED CRYPTOGRAPHIC VALIDATION (ACV) TESTING

Apostol Vassilev, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

The number and complexity of Internet-based breaches continues to climb every year, as documented by the incidents described in the Verizon 2018 Data Breach Investigations Report (DBIR). That report illustrates that many of the important products that we depend upon (e.g., databases, web applications, network routers/switches, end-user devices) are the target of persistent and advanced attacks. Cryptography can be a key defense against such attacks since even if a system is breached, encrypted data would be useless to the attackers.

The Computer Security Division (CSD) of the Information Technology Laboratory, National Institute of Standards and Technology (NIST), selects and standardizes cryptographic algorithms as NIST-approved for use within the U.S. federal government. CSD specifies the relative strength of various cryptographic algorithms and describes contexts where the use of those algorithms may or may not be suitable. However, the strength of cryptographic protection depends not only on the theoretical properties of the algorithms but also on the correctness and robustness of their implementation in hardware and software.

When organizations implement the NIST-approved algorithms into modules within their products, NIST validates that those modules meet standards for correct and robust implementation. U.S. federal government users are required to use validated NIST-approved cryptography, based upon requirements described in Federal Information Processing Standards (FIPS) 140, *Security Requirements for Cryptographic Modules*. Revision 2 of this standard is the current release, commonly referenced as FIPS 140-2; it was released on May 25, 2001, superseding the original version, FIPS 140-1.

NIST has been hard-pressed to keep up with the expanding and increasingly complex array of technologies implementing cryptography. The number of products with cryptographic capabilities used by federal agencies is exploding, and those products are undergoing constant updates and patching. Every consumer is familiar with this trend – a new mobile phone is hardly out of the box before there is a notification for updates of the software.

The Need for Speed

Another recommendation of the Verizon DBIR is that organizations should patch promptly, including application of patches to update cryptographic modules. Technology products are complex and the cost of fully testing them to

[1] Larry Feldman and Greg Witte are former NIST Associates from G2, Inc.

guarantee trouble-free use is prohibitively high. As a result, products contain vulnerabilities that hackers and product vendors are competing to discover first: for the vendors to fix, and for the hackers to exploit. Patching the products changes the game for hackers and slows down their progress. Thus, patching promptly is a way of staying ahead of the hackers. An example is a recent set of Internet browser upgrades to eliminate vulnerable versions of Transport Layer Security (TLS) and to implement newer versions of the TLS protocol. However, patching also changes the environment in which a cryptographic module runs and may change the module itself, thus invalidating the previously validated configuration. Federal users face a dilemma in which frequent updates and patches are important for staying ahead of the attackers, but the existing NIST validation process does not permit rapid implementation of these updates while maintaining a validated status.

Project Overview

Figure 1 shows that algorithm and module testing are currently performed by external Cryptographic and Security Testing (CST) laboratories that are accredited as part of the National Voluntary Laboratory Accreditation Program (NVLAP). These laboratories use the NIST Derived Test Requirements (DTR), Implementation Guidance (IG), and applicable CMVP guides to test the cryptographic modules. However, current testing requires human reviews of complex technical products, which has been shown ineffective and inefficient. According to the existing process, the CST laboratories must perform 100 percent independent testing of the module implementations under test (IUT) submitted by the vendors, which raises questions about the depth of testing and the scalability of the current programs.

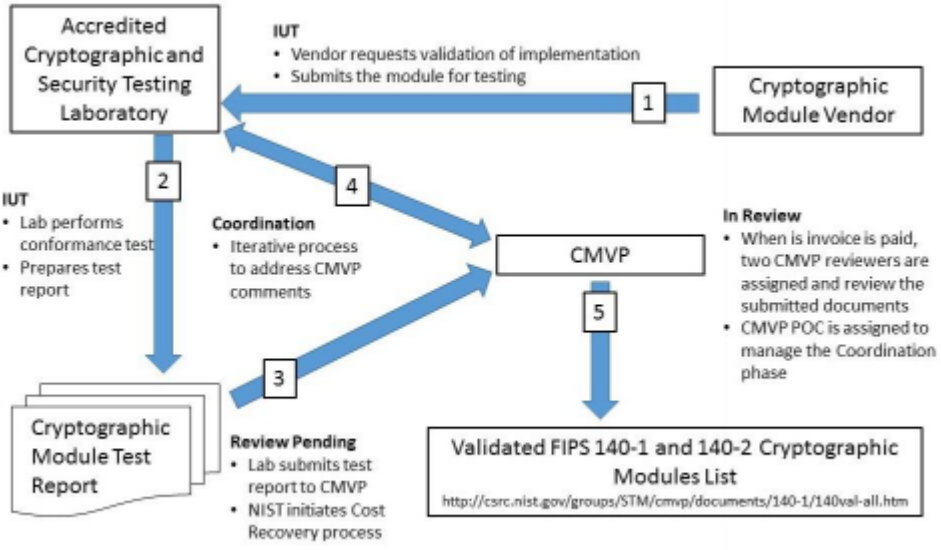

Figure 1: Current Cryptographic Module Validation Overview

Automation Project Implementation

NIST is attempting to automate module validations, working with producers of technology with cryptographic capabilities and their government users of FIPS 140-validated modules. A key objective of the automation project is to develop new automation-based processes to help improve the efficiency and effectiveness of cryptographic

module testing, based on adoption of best practices that industry partners have found to be effective. The project will exploit machine learning and artificial intelligence to develop test procedures and techniques for automating assurance of module compliance to FIPS 140. Another objective is the identification of techniques and procedures that provide continued assurance of operational compliance to FIPS 140 throughout modules' life cycles. Successful achievement of these goals is expected to help reduce the time required for the validation cycle, reducing validation costs and enabling models like "just-in-time validation."

The new structure of the CMVP, shown in Figure 2, leverages automation through computer analysis of test results. The testing is performed by the company developing the technology, and the test evidence, in the form of machine-readable data, is submitted to the NIST ACV server for analysis and validation based on machine learning. The project is being implemented through four major phases over several years. Phases 1 and 2 have been completed and involved the selection and documentation of the technical approach for automating algorithm testing, including working prototypes. Phase 3 is in progress and includes a draft report about the approach, review of feedback received, and publication of the final report. Several elements of Phase 4 are complete, including development of a draft accreditation criteria for establishing a new scope in NIST's Handbook (HB) 150-17, *NVLAP Cryptographic and Security Testing*, and issuance of the first official algorithm certificates through the automated NIST server based on the Automated Cryptographic Validation Protocol (ACVP) protocol for selected algorithms. Also in progress are pilot automated module validations with several technology companies from different classes of technology.

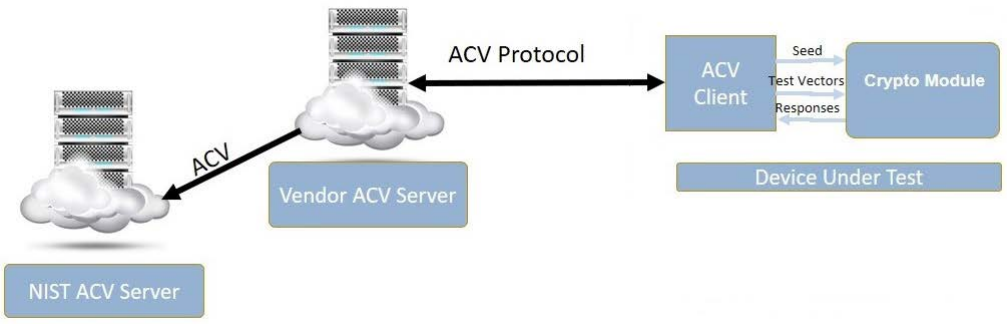

Figure 2: Updated CMVP Structure Leveraging Automation

Conclusion

NIST continues to work on ways to identify and enable efficient methods to keep pace with rapidly changing cryptographic technology while supporting federal users' needs for quick and effective validation of cryptographic algorithms and modules. As the NIST CMVP improvement project progresses, NIST will continue to inform the cybersecurity community about results, findings, and updated guidance. Those interested are invited to monitor the project's progress as NIST performs pilots of the automated validation and rolls out a complete set of Cryptographic Algorithm Validation Program (CAVP) and CMVP capabilities with automated testing.

Additional Resources

Automated Cryptographic Validation Testing, https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing

The algorithm testing automation project on GitHub, https://github.com/usnistgov/ACVP.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov