galois

Improving the Coverage and Effectiveness of the World's Highest Algorithmic Testing Standards

> *We sat down with Galois to discuss the problem and introduce our solution. Shortly afterwards, the Galois team presented a plan for boosting the assurances we can gain from our system. The assurances added to ACVTS allow us to have more confidence in the testing we provide to the federal government consumers. We hope to expand the research into other algorithms and open source implementations.*
>
> **CHRISTOPHER CELI,**
> **CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM MANAGER**
> NIST

NIST

Company name
National Institute of Standards and Technology (NIST)

Industry
Government agency

Website
https://www.nist.gov

NIST:

The National Institute of Standards and Technology (NIST) is one of the oldest physical science labs in the U.S. In addition to conducting basic research, NIST is responsible for maintaining standards across several technology areas including machine learning, cybersecurity, and cryptography. In some cases, NIST is tasked by the federal government to validate these standards for operational systems.

Challenge: NIST has adopted automation to provide faster validations for cryptographic technologies and wants to meet or exceed the level of rigor achieved with human-centric testing

Agencies (and their vendors) seek NIST's validation for their cryptographic modules due to Federal mandates and the institute's high standards for correctness and security. NIST's Federal Information Processing Standards (FIPS) 140 is provisioned into two programs: the Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP).

The CAVP program has recently developed the Automated Cryptographic Validation Testing System (ACVTS) to make the validation process easier. The automation platform allows NIST to focus on its core mission of providing deeper and more substantive checks for cryptographic module validation.

ACVTS must be able to detect flaws in a broad range of cryptographic algorithms using a black-box testing model that assumes no knowledge of the underlying implementations.

The ACVTS platform must rapidly generate unique test vectors to be effective. These vectors need to provide a high degree of coverage over the implementations and algorithms being tested.

Challenge

1. Agencies and their vendors seek validation from NIST for their cryptographic modules, but the process is time-consuming.
2. NIST's Automated Cryptographic Validation Testing System (ACVTS) platform is designed to make the validation process easier, but it must rapidly generate unique test vectors to be effective.
3. ACVTS vectors must provide a high degree of coverage over the implementations and algorithms being tested.

Solution

1. Galois deployed lightweight formal verification techniques to augment ACVTS.
2. Our methods produced test vectors offering higher coverage and more assurance for their correctness.
3. We generated high-coverage test vectors for reference implementations like OpenSSL that served as a proxy for other implementations.
4. Galois translated high-coverage test parameters into concrete test vectors using executable specifications of cryptographic algorithms written in Cryptol.

Solution: Galois's formal verification improved coverage and provided greater assurance, giving agencies and their vendors additional value from the validation process

Galois used lightweight formal verification techniques to enhance ACVTS. Galois's methods produced test vectors offering higher coverage and more assurance for their correctness. Galois's solution consisted of two parts: test coverage and test correctness.

Test Coverage: A test framework for cryptographic algorithms should provide coverage over both the implementation code paths and the algorithm specifications.

ACVTS's black-box testing model makes full code coverage impractical for all implementations under test. As a remedy, Galois used formal techniques to automatically extract high-coverage test vectors from reference implementations like OpenSSL. OpenSSL is particularly effective in this setting as it serves as the basis for a significant number of the modules NIST validates. High-coverage test vectors have a higher likelihood of detecting implementation flaws and enable metrics-driven assessments of test quality.

Test Correctness: The second piece of Galois's approach translated high-coverage test parameters into concrete test vectors using executable specifications of cryptographic algorithms written in Cryptol, a domain-specific language for cryptography.

Automatic extraction of test parameters:

Galois applied a technique called concolic execution to automatically extract high-coverage test parameters. These test parameters identified a minimal set of input conditions needed to cover all of the statements, branches, and algorithm-specific parameter selections in a piece of cryptographic code.

A high degree of trust:

Cryptol specifications closely resemble their mathematical counterparts and are often proven equivalent to cryptographic implementations written in general-purpose programming languages. As a result, Cryptol specifications provide a high degree of trust in their correctness.

How can we help?

From U.S. defense and intelligence agencies to global technology companies working on the edge of what is technologically possible, we ensure that you don't have to blindly trust the software underlying your systems.

Do you want to ensure the correctness of your complex code?

We'd love to learn about your business and see if we can help.

Portland, OR
Arlington, VA
Dayton, OH

contact@galois.com
Tele. 503.626.6616
Fax 503.350.0833