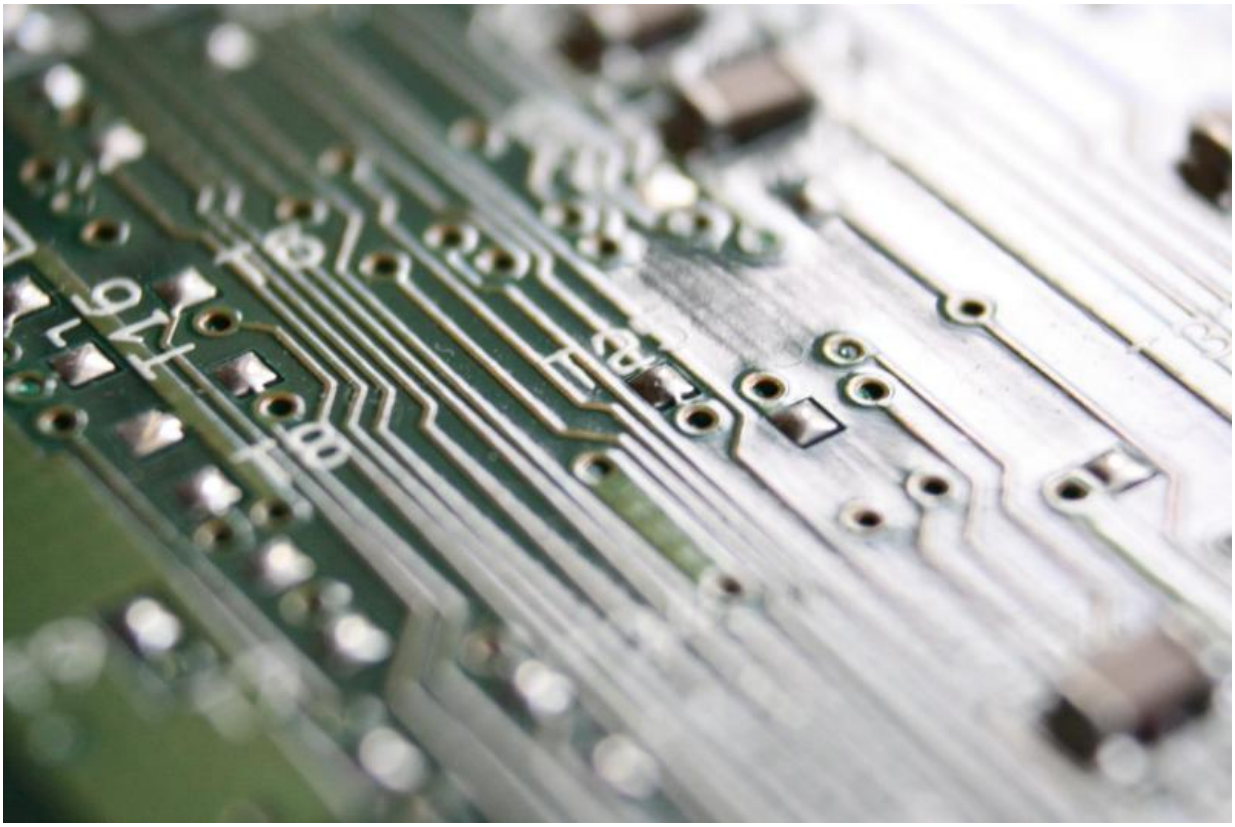
Cryptography: Security engineers announce Project Wycheproof

December 21 2016, by Nancy Owano



Credit: Public Domain

(Tech Xplore)—"Many of the algorithms used in cryptography for encryption, decryption, and authentication are complicated, especially when asymmetric, public key cryptography is being used," said Peter

Bright on Monday in *Ars Technica*. "Over the years, these complexities have resulted in a wide range of bugs in real crypto libraries and the software that uses them."

Bright was giving us a bigger picture view in light of the good news from Google. On Monday Google announced the release of Project Wycheproof. This should ease some pain.

The project involves a set of security tests that check cryptographic software libraries for known weaknesses.

Daniel Bleichenbacher and Thai Duong, security engineers with Google, announced the test suite on the Google Security Blog. They said this was "a collection of unit tests that detect known weaknesses or check for expected behaviors of some cryptographic algorithm."

The first set of tests are written in Java, the two said, as Java has a common cryptographic interface. In turn they could test multiple providers with a single test suite.

They blogged that their project provides tests for most cryptographic algorithms, including RSA, elliptic curve crypto, and authenticated encryption.

Their Github page said the tests detect whether a library is vulnerable to attacks, including invalid curve attacks, biased nonces in digital signature schemes and Bleichenbacher's attacks.

Google has put code for Wycheproof on GitHub for public perusal, said Chris Brook in *Threatpost*. The project, he added, comes two weeks after Google debuted a fuzzer to help developers discover programming errors in open source software.

How does their project help? They blogged that good implementation guidelines are hard to come by and that understanding how to implement cryptography securely requires digesting decades' worth of academic literature. They said "with Project Wycheproof developers and users now can check their libraries against a large number of known attacks without having to sift through hundreds of academic papers or become cryptographers themselves."

All the same, though, they said Project Wycheproof was "by no means complete. Passing the tests does not imply that the library is secure, it just means that it is not vulnerable to the attacks that Project Wycheproof tests for."

Justin Duino in *9to5Google* said, "there are new vulnerabilities being found every day which means that Project Wycheproof will continue to grow with the help of contributors."

The engineers did report progress nonetheless. So far they developed over 80 test cases that uncovered more than 40 security bugs. (They found that they could recover the private key of widely-used DSA and ECDHC implementations.) Some tests or bugs are not open sourced, as they are being fixed by vendors.

Why did they choose the name Wycheproof? Mount Wycheproof is a hill in the town of Wycheproof, Victoria, Australia. They said Mount Wycheproof was the smallest mountain in the world. "The smaller the mountain the easier it is to climb it!"

More information: — security.googleblog.com/2016/1 … ject-wycheproof.html

— github.com/google/wycheproof