Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

Review-Report Crypto Library TweetNaCl-js

Cure53, Dr.-Ing. M. Heiderich, Dr. Jonas Magazinius, Joachim Strömbergson

Overview

This document stems from a broader report dedicated to the findings of a source code audit commissioned by the US-based Deletype LLC enterprise and completed by Cure53. The project was carried out by two members of the Cure53 team and an external consultant from Assured AB in Sweden. *TweetNaCl-js* [URL] was one of the two cryptographic libraries assessed during this assignment.

In terms of the origins and rationale of the assignment, the project was requested, commissioned and funded by the US-based Deletype LLC enterprise. The company sought to make sure that the software in question was as secure as possible. This was clearly tied to the fact that some of the Deletype's services normally rely on the cryptographic items in scope. The sources positioned in scope of this audit for TweetNaCl-js were delivered to the testing team via Github repositories and the audit took place in late January and early February of 2017, ultimately concluding on February 8th, 2017. The time budget for the completion of this assessment entailed three work days (for TweetNaCl-js), which were primarily spent on thorough source code analysis, yet account also for the time needed for reporting, communication and final write-up.

Verdict

The overall outcome of this audit signals a particularly positive assessment for TweetNaCl-js, as the testing team was unable to find any security problems in the library. It has to be noted that this is an exceptionally rare result of a source code audit for any project and must be seen as a true testament to a development proceeding with security at its core.

To reiterate, the TweetNaCl-js project, the source code was found to be bug-free at this point. Apart from the core code audit, a small-set of applicable test cases from Google's Wycheproof project [URL] was ported to JavaScript for the purpose of testing the broader functionality of the library. Still, TweetNaCl-js held up well to both the review and security tests, ultimately making a solid impression. It is hoped that the TweetNaCl-js team continues on this path of considerable dedication to security matters.

In sum, the testing team is happy to recommend the TweetNaCl-js project as likely one of the safer and more secure cryptographic tools among its competition.