CryptoExamples: Secure, minimal, complete, copyable and tested code examples for Crypto APIs

Kai Mindermann, M.Sc.*, Dr. Stefan Wagner*

*Institute of Software Technology, University of Stuttgart

Programmers have to integrate security functionality in their programs more and more. For this they should rely on existing cryptographic libraries, which offer their functionality through an application programmable interface (API). The usage of these crypto APIs is often not possible without thorough knowledge of the offered cryptographic methods. Especially this is expected from an API. An approach for an improvement through documentation is to provide example code. This happens equally unsatisfying. Alternative sources like StackOverflow answers provide examples, but these are often insecure.

Our approach for an improvement, *CryptoExamples* [1], provides an open-source platform on which secure and tested code examples for common usage scenarios of cryptography APIs are available, are reviewed and can be contributed. Empirical investigations from a controlled experiment show that the examples significantly reduce security bugs in produced code. At the Crypto-Day we not only want to present the CryptoExamples platform itself but also the corresponding, from our view very common and easy, process (see Figure 1) for contributions via git and their review.

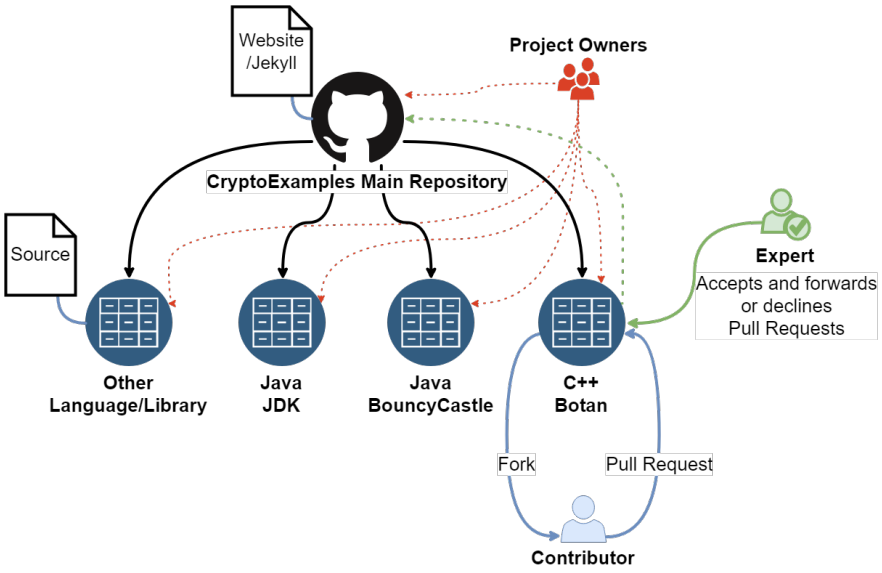

Figure 1: Process visualization for contributions, their review and the structure of the platform *CryptoExamples* for cryptographic code examples.

References

[1] Mindermann, Kai et al. *CryptoExamples - an open-source platform for secure, minimal, complete, copyable and tested cryptographic code examples*, `http://www.cryptoexamples.com/` (Visited on 2018-04-26), 2017.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-21