Offer 20180215-00-00
Prepared for The Open Source Technology Improvement Fund, Inc

By Markus Vervier / sales@x41-dsec.de

2018-02-23

X41 D-SEC GmbH
Dennewartstr. 25-27
D-52068 Aachen
Amtsgericht Aachen: HRB19989

Document History

Revision	*Date*	*Change*	*Editor*
0	2016-12-14	Initial Document	E. Sesterhenn
1	2016-12-20	Updated Document	M. Vervier
2	2016-12-23	Corrections	E. Sesterhenn, M. Vervier

Proposal Recipient

Derek Zimmer
The Open Source Technology Improvement Fund, Inc

X41 D-Sec GmbH Contacts

Markus Vervier
CEO / Head of Research
Dennewartstr. 25-27
D-52068 Aachen
markus.vervier@x41-dsec.de
+49 241 980 94185

Eric Sesterhenn
Principal Security Consultant
Dennewartstr. 25-27
D-52068 Aachen
eric.sesterhenn@x41-dsec.de
+49 241 980 94186

1 Executive Summary

This document provides details of our proposal for a review for Bulletproofs as implemented by Monero Research Labs. It includes a breakdown of all proposed services and costs.

A cryptographic review of the paper, proofs, and C++ implementation will be performed. The estimated financial effort for this project is 31,350.00 USD. Thank you for giving us the opportunity to propose our services to you. We hope the following information will help you in your decision about our future cooperation.

If you have any queries about the services, costs or would like to discuss anything contained in this proposal, please feel free to reach out any time to sales@x41-dsec.de.

M. Vervier

Markus Vervier

2 Project Description

The Monero project is implementing Bulletproofs to replace the Borromean-style range proofs for the transactions in their highly private coin. For this they require a limited-scope analysis of the bulletproof prove/verify algorithms to answer the following questions:

1. Does the code accurately represent the prove/verify algorithms from the bulletproof white paper?
2. Does the implementation allow an attacker to generate a false proof that an honest verifier judges as correct?
3. Does the implementation allow an attacker to examine an honest prover's proof and gain information about the hidden amount or other masks?

In order to answer these questions, X41 D-Sec GmbH proposes a cryptographic review of the cryptographic design and the code. This will ensure that the underlying mathematics are sound and the code is equivalent to the proven equations. Additionally, a code review with focus on implementation errors is performed to ensure that no language specific bugs are present, which might allow an attacker to abuse the crypto coin.

The audit will be based on the original paper[1], the translated proofs[2] and the C++ code[3].

X41 D-Sec GmbH will provide all findings in a technical report, along with a management summary. Each finding will be rated according to critically and a solution advice for the issue will be given.

[1] http://web.stanford.edu/~buenz/pubs/bulletproofs.pdf
[2] https://github.com/b-g-goodell/research-lab/tree/master/source-code/BulletProofs
[3] https://github.com/moneromooo-monero/bitmonero/tree/bp-multi/src/ringct

2.1 Project Investment

Monero Cryptocurrency Audit

1	Cryptographic review of the paper, proofs, and C++ implementation	24,750.00 USD x 1	24,750.00 USD
2	C++ Code review with focus on implementation errors of the C++ code (4000 lines of code)	6,600.00 USD x 1	6,600.00 USD

SUBTOTAL	31,350.00 USD
VAT	0.00 USD
TOTAL	**31,350.00 USD**

3 Team

The following specialists will be assigned to the project:

3.1 Phillipp Lay

Phillipp Lay is a cryptographer and mathematician with experience in design and review of cryptosystems and algorithms.

Notable works include:

- QRTAN Protocol, Zero-Knowledge OTP verification with QR-encoded challenges.
- QR Pairing, soft-token rollout protocol.
- Push Authentication Protocol, Authentication protocol based on ed25519.

His private projects related to cryptography are listed at `https://github.com/phlay`

3.2 Markus Vervier

Markus Vervier is Head of Research and Managing Director at X41 D-Sec GmbH. Software security is his main focus of work. During the last 15 years of professional experience in offensive IT security he worked as a penetration tester and security consultant and was doing active security research.

Notable works include:

- extensive experience in the field of code-review, reverse engineering, and vulnerability analysis of applications on various platforms and architectures;
- reverse engineering and security analysis of embedded firmware for mobile devices (Android device baseband firmware);

- discovery of the first vulnerabilities in the *Signal Private Messenger*[4];
- speaker at Infiltrate, HITBSECCONF and Troopers security conferences about offensive security topics such as baseband reverse engineering and application security;
- memory corruption vulnerability in *libOTR*[5].

3.3 Eric Sesterhenn

Eric Sesterhenn is working as an IT Security consultant for more than 15 years, working mostly in the areas of penetration testing and source code auditing.

Notable works include:

- identified vulnerabilities in various software projects including the Linux kernel;
- analysis of complex software applications and infrastructures and extensive experience in code reviewing, penetration testing, and vulnerability analysis;
- part of the winning team of the Deutsche Post Security Cup 2013;
- speaker at 30C3 about fingerprinting Java applications (lightning talk).

[4] `https://pwnaccelerator.github.io/2016/signal-part1.html`

[5] `https://x41-dsec.de/lab/advisories/x41-2016-001-libotr/`

4 Confidentiality

This offer and it's contents are intellectual property of X41 D-Sec GmbH. Any changes need to be approved in writing by X41 D-Sec GmbH. Duplication and propagation to third parties require explicit consent by X41 D-Sec GmbH.
X41 D-Sec GmbH grants *Monero Reserach Labs* the right to publish this offer as part of the vendor selection process and for transparency.

5 Insurance

X41 D-Sec GmbH is insured by *Hiscox Europe Underwriting Limited* during research projects with a professional liability insurance of up to 1,000,000 €. Necessary documents can be provided on request.

6 About X41 D-Sec GmbH

X41 D-Sec GmbH is an expert provider for application security services. Having extensive industry experience and expertise in the area of information security, a strong core security team of world class security experts enables X41 D-Sec GmbH to perform premium security services.

Fields of expertise in the area of application security are security centric code reviews, binary reverse engineering and vulnerability discovery. Custom research and a IT security consulting and support services are core competencies of X41 D-Sec GmbH.

7 Terms and Conditions

This offer is subject to the following terms and conditions:

1. Location of provided services: remote.
2. Travel expenses will be billed according to the actual expenditures.
3. Any additional services need a separate commercial agreement.
4. A separate penetration testing agreement will be signed before the test in order to define and verify the legal scope of all tests.
5. All prices quoted are net, excluding VAT. All prices are quoted in USD.
6. One person-day (PD) equates eight hours.
7. Latest end of project: 2018-06-01
8. This quotation is a non-binding offer until your order is confirmed by X41 D-Sec GmbH and an order confirmation is sent to you. In case of sending an order confirmation by X41 D-Sec GmbH the quotation gets a binding offer.
9. This proposal is valid until 2018-04-01.

8 Acceptance

8.1 Client

I hereby confirm the acceptance and accept all terms and conditions as defined in this proposal:

Full Name

Title

Date

Signature (The Open Source Technology Improvement Fund, Inc)

Full Name

Title

Date

Signature (The Open Source Technology Improvement Fund, Inc)

Please submit two signed copies by mail to X41 D-Sec GmbH. A preliminary order may be sent via email or fax in order to allocate resources and speed up the beginning of the project.

8.2 X41 D-Sec GmbH

We hereby confirm the order:

Full Name

Title

Date

Signature (X41 D-Sec GmbH)

Confirmed Date of Project Begin