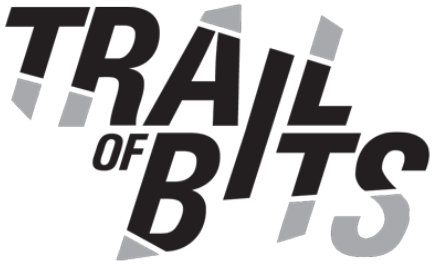

RandomX

Security Assessment Proposal

Prepared For:
Howard Chu | *Monero*
hyc@symas.com

Prepared By:
Dan Guido | *Trail of Bits*
dan@trailofbits.com

Ben Perez | *Trail of Bits*
benjamin.perez@trailofbits.com

Cara Pearson | *Trail of Bits*
cara.pearson@trailofbits.com

Date of Proposal: 5/14/2019
Version: 2.0

Executive Summary

Monero seeks a third party to review the security of the proof-of-work algorithm behind RandomX. Trail of Bits will verify that the RandomX specification is cryptographically secure and does not allow algorithmic or hardware optimizations. The review will also validate that the code matches the specification. The assessment will be performed over a three calendar-week period by two Trail of Bits security engineers, for a total of six person-weeks. Using all provided documentation, Trail of Bits will review the RandomX protocol and codebase for security flaws and weaknesses and then determine possible mitigations available to Monero.

Project Goals and Background

RandomX is a novel proof-of-work (PoW) algorithm that will be used to achieve consensus on the Monero blockchain. Unlike the Bitcoin PoW algorithm, RandomX is designed to run on a consumer-grade CPU and not be amenable to hardware optimizations. To accomplish this, RandomX uses a cryptographic PRNG to generate random instructions from a simplified x86 ISA. Users then execute these random programs on the RandomX virtual machine and output a hash of the final register state as their proof of work. This scheme is unlike anything that has appeared previously in the cryptographic literature and therefore requires careful review.

Possible failure modes of the system include:

- Incorrect use of cryptographic primitives
- Scheme can be made to run faster on specialized hardware
- End register file not sufficiently random
- Implementation does not match specification
- Libraries contain logic or memory-related errors
- Protocol subject to denial of service attacks

Trail of Bits will use its expertise in low-level software, binary analysis, cryptography, and blockchain systems to ensure the RandomX protocol is free of the above vulnerabilities.

Our team has audited blockchain systems ranging from MakerDAO's DAI and SAI stablecoins to entirely new proof of stake protocols. We have used our low-level security expertise to build an entire suite of tools for analyzing EVM smart contracts and now chair the Enterprise Ethereum Alliance Security Task Force. Our cryptographic services team has both built and audited many widely-used libraries and is engaged with cutting edge research on how crypto fails in practice. As RandomX uses ideas from blockchain, cryptography, and computer architecture, our team is uniquely suited to assess its security.

Statement of Work to
Trail of Bits Master Service Agreement

This Statement of Work (SOW) is subject to the terms of the Master Services Agreement between Trail of Bits, Inc. and _____ dated _____ (the "Agreement").

1. Definitions

All capitalized terms used herein and not otherwise defined herein shall have the meanings ascribed to them in the Agreement.

2. Description of Services

Trail of Bits will perform a comprehensive review of both the protocol and implementation to ensure RandomX is free of the vulnerabilities specified in the project goals. To accomplish this, we will break up the audit into three major focus areas

Protocol Review

During the protocol analysis, we will establish whether RandomX is cryptographically secure and the extent to which it can be optimized for special hardware. To accomplish this, we will examine the use of existing cryptographic primitives and verify they are being used properly. We will search for attacks on the protocol as a whole, exploring potential shortcuts that would allow someone to execute the algorithm more quickly. This may involve exploiting the VM and ISA design or some subtle lack of randomness present in the final register file. We will also explore potential DoS attacks during this phase.

When this component of the review is completed, Trail of Bits will recommend any protocol-level fixes that need to be made, along with suggested parameters required to achieve the desired security level.

Code Review

The RandomX codebase consists of a VM, JIT and an AOT compiler all written in C++. Each of these components will require careful manual review to ensure that they adhere to the specification and are free of implementation bugs.

Automated Testing

To ensure that RandomX continues to enjoy a high level of assurance throughout its development lifecycle, Trail of Bits will develop tools and testing suites that can be used after the audit has concluded. Trail of Bits will supply tests to verify cryptographic primitives are generating truly random outputs, along with the end register file state. In particular we will use the Dieharder test suite to establish relevant functions emit truly

random values. Furthermore we will use a combination of fuzzing and symbolic execution to establish the implementation is free of low-level bugs.

3. Risks

Although the duration of the project has been selected to provide a balance between coverage and timeliness, detection of all potential vulnerabilities without the ability to formally prove correctness is impossible. Trail of Bits will mitigate this risk by following a systematic approach in source analysis to ensure high coverage and provide a best-effort assessment in the time allotted.

4. Customer or Third Party Responsibilities

In order to carry out a successful engagement and mitigate project risk, Trail of Bits will require access to the following:

- Access to a designated project sponsor and appropriate technical resources
- Access to all in-scope source code and any documentation for it, preferably via a source code repository

5. Financial Terms

Client will pay Trail of Bits the fees listed below. All services and applicable expenses will be invoiced upon completion of the project for the total amount.

The standard rate for blockchain security assessments is $16,000/week, however, this project has been discounted to $14,000/week due to the client's need for fundraising for this project.

Fees

Project Rate	$14,000 per week
Total Effort	6 person-weeks • 2 person-weeks to review cryptographic specification • 4 person-weeks to review software security NOTE: Trail of Bits projects are done by pairs of engineers.
Expense Estimate	$0
Total Estimated Cost	$84,000
Payment Terms	Net 30, upon completion of the project

6. Project Deliverables

Weekly reports

After each week of the engagement, Trail of Bits will report on actions taken, confirmed vulnerabilities found, and guidance on next steps.

Trail of Bits will provide a readout of the weekly report, typically lasting one hour, with one or more technical representatives from Monero. This meeting will cover flaws identified during the assessment in-depth and offer guidance on structuring remediation efforts and more effective security testing.

Typical weekly reports follow the outline below:

1. Executive Summary
    - Short description of the project and what was tested
    - Analysis of overall security risk based on the findings
    - Brief summary of the recommendations
    - Review of project goals and estimate of coverage
2. Comprehensive List of Vulnerabilities
    - Detailed explanations sufficient to identify and/or reproduce the vulnerability
    - Attack and exploit scenario to provide context for the vulnerability
    - Recommended short and long term mitigation steps
3. Appendices, if applicable
    - Reference material used to support findings
    - Additional detail or context for larger security issues
    - Code used to reproduce or exploit a specific finding
    - Any tools created during the assessment to aid future regression testing
    - Trail of Bits will provide any artifacts developed during the assessment

Example reports can be found on our '[publications](#)' repository on Github.

7. Project Schedule and Location

To the extent that TOB's performance of any hourly based services hereunder are to start on a future date, if TOB is not authorized to start such performance more than 6 months after the date of this SOW or if such services are not fully performed (other than due to the breach by TOB hereunder) before the one year anniversary of the date of this SOW, then the Customer shall pay TOB 50% of the unused hours and this SOW shall automatically terminate upon notice by TOB to Customer.

Services are expected to be performed from Trail of Bits in New York, NY with site visits to Client conducted on an as-needed basis. Client is responsible for any project-related travel expenses.

8. Customer Designated Project Leads

Set forth below is the name and contact information for the person designated by Customer as the primary point of contact for communications under this SOW.

Technical Point of Contact: _____
Name & Email

Administrative / Billing Point of Contact: _____
Name & Email

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

IN WITNESS WHEREOF, the parties hereto have caused this Statement of Work to the Master Service Agreement to be executed as of the date written beneath their signatures below.

TRAIL OF BITS, INC.	**Customer**: _____
By:_____ (Authorized Signature)	By:_____ (Authorized Signature)
_____ (Print or Type Name of Signatory)	_____ (Print or Type Name of Signatory)
_____ (Title)	_____ (Title)
_____ (Execution Date)	_____ (Execution Date)

About Trail of Bits

Since 2012, Trail of Bits has helped secure some of the world's most targeted organizations and products. We combine high-end security research with a real world attacker mentality to reduce risk and fortify code.

Our clientele -ranging from Facebook to DARPA- lead their industries. Their dedicated security teams come to us for our foundational tools and deep expertise in reverse engineering, cryptography, virtualization, malware, and software exploits. According to their needs we may audit their products or networks, consult on the modifications necessary for a secure deployment, or develop the features that close their security gaps.

After solving the problem at hand, we continue to refine our work in service to the deeper issues. The knowledge we gain from each engagement and research project further hones our tools and processes, and extends our software engineers' abilities. We believe the most meaningful security gains hide at the intersection of human intellect and computational power.

References

John Pacific | Cryptography Engineer, NuCypher
john@nucypher.com

Rick Dudley | CEO, Vulcanize
rick@vulcanize.io

Yondon Fu | Software Engineer, LivePeer
yondon@livepeer.org

Byron Cook | Senior Principal, Amazon
byron@amazon.com