Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Audit-Report Stealth Address Implementation 02.2023

Cure53, Dr.-Ing. M. Heiderich, Dr. N. Kobeissi

Index

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Introduction

This brief report details the scope, results, and conclusory summaries of a cryptography review and source code audit against the Practical Stealth Addresses protocol specification and software implementation.

The work was requested by Ryan Shea in December 2022 and initiated by Cure53 in February 2023, namely in CW06. A total of 3 days were allocated to reach the coverage expected for this project. The testing conducted for this audit was structured using one distinct Work Package (WP) for execution efficiency, as follows:

- **WP1**: Protocol review against Practical Stealth Addresses specification & software implementation

Cure53 was granted access to the library and commits via GitHub, as well as any alternative means of access required to ensure a smooth review completion. For this purpose, the methodology chosen was white-box and a team comprising two skill-matched senior testers was assigned to the project's preparation, execution, and finalization.

All preparatory actions were completed in January & February 2023, namely in CW05, to ensure the review could proceed without hindrance or delay. Communications were facilitated via a dedicated, shared Signal channel deployed between Ryan Shea, the code author Paul Miller, and Cure53, thereby creating an optimal collaborative working environment. All participatory personnel from both parties were invited to partake throughout the test preparations and discussions. In light of this, communications proceeded smoothly on the whole. The scope was well-prepared and transparent, no noteworthy roadblocks were encountered throughout testing, and cross-team queries remained minimal as a result.

Cure53 gave frequent status updates concerning the test and any related findings, whilst simultaneously offering prompt queries and receiving efficient, effective answers from the maintainers. Live reporting was offered and subsequently conducted via the aforementioned Signal channel. Concerning the findings specifically, the Cure53 team achieved widespread coverage over the WP1 scope items, detecting a total of one issue. The finding was categorized as a security vulnerability with lower exploitation potential.

The report will now shed more light on the scope and testing setup as well as provide a comprehensive breakdown of the available materials.

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

The report will then showcase the one discovered finding. This will be accompanied by a technical description and Proof of Concepts (PoCs) where applicable, plus any relevant mitigatory or preventative advice to action.

In summation, the report will finalize with a conclusion in which the Cure53 team will elaborate on the impressions gained toward the general security posture of the Practical Stealth Addresses protocol specification and software implementation, giving high-level hardening advice where applicable.

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Scope

- **Cryptography reviews & code audit against Practical Stealth Addresses specification & software implementation**
  - **WP1**: Protocol review against Practical Stealth Addresses specification & software implementation
    - **Protocol specification:**
      - https://gist.github.com/shea256/e4a8dccd1e83fa801c7328a0af611798
    - **Implementation**
      - https://github.com/opuswallet/stealth-addresses-implementation/blob/master/src/index.ts
  - **Test-supporting material was shared with Cure53**
  - **All relevant sources were shared with Cure53**

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Cryptography Review

This section documents the testing methodology applied during this cryptography review and code audit, shedding light on the advanced approaches initiated to evaluate the Practical Stealth Wallets specification and codebase. Further clarification concerning areas of investigation subjected to deep-dive assessment is offered, particularly considering the absence of findings exhibiting significant security vulnerabilities on the scope examined by Cure53 for this audit.

Practical Stealth Wallets Review

Cure53 conducted an audit on the specification[1] and software implementation[2] of a *Practical Stealth Wallets* protocol that aims to allow for "*[discreetly] sending cryptocurrency to a recipient without requiring interaction with the recipient or requiring the recipient to maintain a notification service.*"

Cure53 reviewed the cryptographic specification document as well as the source code via manual review. One minor timing leak was found in the software implementation and documented in MBS-02-001.

The timing leak concerns the elliptic curve modulo operation: by observing when the jump from when a relatively instant modulo operation to a relatively time-requiring modulo operation happens, an attacker may be able to learn if private key material resides within a certain bound.

[1] https://gist.github.com/shea256/e4a8dccd1e83fa801c7328a0af611798
[2] https://github.com/opuswallet/stealth-addresses-implementation/blob/master/src/index.ts

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Identified Vulnerabilities

The following section lists all vulnerabilities and implementation issues identified during the testing period. Notably, findings are cited in chronological order rather than by degree of impact, with the severity rank offered in brackets following the title heading for each vulnerability. Furthermore, all tickets are given a unique identifier (e.g., *MBS-02-001*) to facilitate any future follow-up correspondence.

MBS-02-001 WP2: Timing leak in ECDH modulo operation *(Low)*

It was observed that Opus Wallet's Practical Stealth Address Implementation exposed a timing leak in its private key derivation function. Namely, the mod ECDH modulo operation deriving ai will always be relatively instantaneous if *S_i * a_diffiehellman + a_root < n*, and will always take relatively some time if *S_i * a_diffiehellman + a_root > n*.

By observing when the jump from when a relatively instant modulo operation to a relatively time-requiring modulo operation happens, an attacker may be able to learn if *(a_diffiehellman + a_root)* is within a certain bound. We limit the guess values to *a_diffiehellman* and *a_root* since these values are received over the wire, whereas *S_i* is a static, fixed locally derived value.

Affected files:

- *index.ts*
- *noble-curves/src/abstract/modular.ts (dependency)*

Affected code:

```
function deriveSingleUsePrivateKey(params: {
  [...]
}) {
  const S_i = bytesToNumber(params.sharedSecret);
  const a_diffiehellman = bytesToNumber(params.recipientDhPrivateKey);
  const a_root = bytesToNumber(params.recipientRootPrivateKey);
  // ai = S_i * a_diffiehellman + a_root
  const ai: bigint =                                                    ;
  return numberToBytes(ai);
}
[...]
// Calculates a modulo b
export function mod(a: bigint, b: bigint): bigint {
  const result =      ;
  return result >= _0n ? result : b + result;
}
```

It is recommended to replace the elliptic curve modulo operation with a constant-time version.

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Conclusions

The impressions gained during this report - which details and extrapolates on all findings identified during the CW06 testing against the Practical Stealth Address specification/implementation by the Cure53 team.

One minor timing leak was found in the software implementation and documented in MBS-02-001. The impressions gained were positive, the results show that both the specification and the codebase tested in this assessment performed well against a wide range of attacks and vulnerabilities tested.

Cure53 would like to thank Ryan Shea and Paul Miller for their excellent project coordination, support, and assistance, both before and during this assignment.