Concordia Institute for Information System Engineering

(CIISE)

INSE 6120

Cryptographic Protocols and Network Security

Project Plan

Monero and ZCash

Submitted to:

Professor Dr. Ivan Pustogarov

Submitted By:

Student Name	Student ID
Arun Prasad Karunanithi	40220964
Raghavendran Raghunathan	40220965
Naveen Sesetti	40206610
Meetsinh Parihar	40217262
Gayatri Tangudu	40221830
Priya Meghana Raavi	40221227
Bhavya Panner Selvam	40205936

ABSTRACT

Since it was established that Bitcoin only provides a small amount of privacy, numerous cryptocurrencies have emerged that leverage privacy-enhancing cryptographic techniques such the usage of ring signatures and zk-SNARKs. Monero and Zcash are, in turn, two of the most well-known cryptocurrencies that employ these methods. With the aim of providing a side-by-side comparison of Monero and Zcash's privacy mechanisms and identifying the various cryptographic primitives employed there, a study has been carried out. A decentralised cryptocurrency is called Monero. It achieves anonymity and fungibility by utilising a public distributed ledger with privacy-enhancing technologies that obfuscate transactions. When compared to other cryptocurrencies like Bitcoin, Zcash is a cryptocurrency that uses cryptography to give its users greater anonymity.Monero was identified to be vulnerable to two attacks that could compromise privacy. The first attack shows that transactions can be de-anonymised due to the limited number of mixins chosen for the ring signature. The second attack shows that it is possible to correctly guess which mixin the real input is the majority of the time. Based on these vulnerabilities, three improvements are suggested and tested. The first is a different ring signature scheme that allows for constant sized transactions. It was shown that this scheme offers a viable solution to incentivise the use of more mixins. The second is a different sampling algorithm that increases the effective untraceability of the real input. The implementation resulted in better effective untraceability than what is currently achieved by Monero. Finally, a more secure stealth address generation algorithm is presented and implemented. This study critically assesses the advantages and disadvantages of the proposed improvement.Here, we can also see how the Zcash Protocol is vulnerable to the ITM Attack (a linkability attack against shielded transactions), and how Hush is the first cryptocurrency to include a defensive mitigation against it, known as "Sietch". Sietch is already in use and being improved iteratively in response to professional input. This is not a research paper on wishful thinking. Networks and production code are described. We start by reviewing all of the published metadata attack techniques that can be employed against Zcash Protocol blockchains. This covers their threat model and projected attack costs. The "ITM Attack" is a specific example of a new category of blockchain-targeting metadata attacks that the author refers to as "Metaverse Metadata Attacks" in the next section of the article. Cryptocurrencies that prioritise privacy, like Zcash or Monero, seek to offer solid cryptographic assurances for transaction confidentiality and unlinkability. In this article, we outline side-channel techniques that enable remote adversaries to get around these defences.We outline two ongoing attacks—REJECT and PING—on the way in-band secret distribution is implemented in the primary Zcash client. High level: Depending on whether the client is the payee or not, these attacks take advantage of variations in how a client handles transactions. All nodes accept the specially crafted transactions that are sent out by the REJECT attack, but only the payee rejects them outright in their response. The PING attack sends a transaction to a node, then, based on the time of the node's response to the "ping" message, determines if the node is the transaction's payee. We offer a broad category of traffic analysis and timing side-channel assaults against receiver privacy. An active remote adversary can use these methods to determine the (secret) payee of any Zcash or Monero transaction