Zcash Threat Model and Network Privacy Assessment

The Zcash Foundation

June 4, 2020

1 Introduction

The amount of data leaked about individuals online is every growing. Financial data in particular provides a highly granular lens about personal daily habits, but securing one's own financial privacy is difficult due to the value of tracking financial habits for advertising purposes. Fortunately, Zcash ensures strong financial privacy using zero-knowledge proofs along with randomization techniques [3] to protect against data leakage that could lead to deanonymization of a payer or recipient of Zcash. This approach ensures that the raw bytes of a Zcash *shielded* transaction cannot leak identifiable information about the payer, payee, or amount.

However, an adversary observing the network over which Zcash clients and nodes send transactions could perform passive or active attacks with the goal of linking users and their end recipients, even if that adversary cannot decrypt the Zcash shielded transaction directly. Consequently, it is important to assess the how such adversaries could be successful, what information is required in order to perform such deanonymization attacks, and what such adversaries require to do so.

In this technical report, we consider the above questions, and present the threat model for Zcash more formally, assuming the use of shielded transactions. We identify what constitutes sensitive information in the Zcash ecosystem, what adversaries may exist, and enumerate the attack vectors that such adversaries may employ. From this model, we then consider several different network privacy mechanisms, and analyze the extent to which these mechanisms improve the privacy and security of Zcash users. Finally, we lay out several near-term and long-term recommendations for improvements.

Organization. We begin in Section 2 by discussing background information useful to understanding Zcash and its threat model. In Section 3, we introduce a threat model for Zcash, by discussing sensitive information that attackers could observe in the Zcash network, reviewing possible attacker profiles and their associated capabilities and powers, and finally reviewing a range of potential attack vectors.

[1]

[1] CK says: TODO add in the second half of this work after it is added

2 Background

2.1 Zcash Shielded Transactions

While Zcash does allow for use of unshieleded transactions, in this technical report we focus entirely on the threat model assuming the use of shielded transactions. However, we will now briefly describe the difference between the two transaction types. As mentioned before, unshielded transactions are similar to Bitcoin transactions, and expose the pseudonyms of the payer, payee, and the amount paid. When this information is exposed to the network and persisted indefinitely to the Blockchain, it is effectively "Twitter for your bank account".

Shielded transactions, on the other hand, expose what is essentially a "one time pad" to a network observer. Because not only the transaction information is encrypted, the encryption process itself is randomized such that two transactions that have identical payers, payees, and transaction amounts result in bytes that are completely indistinguishable from randomly-generated bytes. In other words, given only a series of shielded transactions, an adversary would not be able to gain enough information to distinguish any information about the transaction paintext.

2.2 Comparison of Zcash Privacy Expectations to Bitcoin

While Zcash provides the ability to make shielded transactions to completely hide the information contained within a transaction, users of Zcash can also make non-shielded transactions. Because Zcash is a fork of Bitcoin, non-shielded transactions consequently have effectively the same expectation of privacy as plain Bitcoin transactions, which had been proven to be insecure against deanonymization attacks **??**. In this post, we'll evaluate the threat model for Zcash considering only shielded transactions.

While both Zcash and Bitcoin have future goals of stable Tor integration and other network-privacy mechanisms, this routing via an anonymity layer does not prevent attacks that examine the bytes of the transaction itself. So unshielded transactions in Zcash and all Bitcoin transactions leak information to a network observer, which can be exploited to perform deanonymization attacks.

3 Zcash Threat Model

3.1 Analysis of Sensitive Information Exposure

As described in Section 2.1 an adversary could gain more information about a shielded transaction by observing information exposed to the network. Keeping this in mind, and assuming that a transaction is shielded, we now review sensitive information that could be exposed and used for malicious purposes by a adversary. We divide these information leaks into *in scope* to the Zcash threat model, and *out of scope*.

3.1.1 In Scope

Note that an adversary has the ability to observe both *on-chain* visible data as well as information or behaviour that is exposed to the network during the process of submitting a new transaction or receiving a transaction.

Linking (sender identity, transaction, receiver identity): Specifically, this three-tuple of sender identity, transaction, and receiver identity allows for an adversary to link the fact that a specific sender of Zcash made a payment to a specific receiver, even though the amount of the payment is not disclosed. While the sender and receiver identity is not exposed by the Zcash transaction itself, an adversary could gain this information by observing the network or colluding with one of the involved parties. For example, if the recipient is malicious and colludes with a party that can link the sender to their transaction, or if the recipient leaks to a provider which transaction they are interested in, the sender and receiver could be linked to a particular transaction.

Unique fingerprints of user habits: By observing behavior of Zcash transactions sent over the network, an adversary could start to build a "fingerprint" of a user's behavior, partially when using machine learning algorithms to classify traffic. Information that is exposed in this category includes the time of day that a transaction occurs, the frequency of transactions, and even the route that a transaction passes through from sender to receiver.

Further, "on-chain" information could also allow for fingerprintability. For example, fees and timing of transactions could possibly provide additional information to an observer.

3.1.2 Out of Scope

Learning the tuple (sender or receiver identity, transaction): Note that a network observer can also gain a subset of sender/receiver linkability information by observing just a sender *or* receiver's identity linked to a specific transaction. We consider this use case to be out of scope to the threat model of Zcash, as such information—to the best of our assessment—simply leaks that the sender or receiver is participating in sending and receiving Zcash, without any further details. Consequently, we consider such an information leak to be out of scope.

3.2 Adversarial Model

We now review possible adversaries that may be motivated to compromise Zcash users' privacy.

Regular Zcash user. Allowed to send and receive transactions and act outside the protocol, just as a real user.

Regular Zcash Node Operator. Can operate one (or many) full Zcash nodes, and can store and forward all traffic that is sent through the node. Can query for network information, and store and examine all information it receives.

DNS seeder operators. Operates the node that is used by new nodes when bootstrapping to the Zcash network, in order to learn about other nodes in the network to begin communicating with them directly.

Internet Service Providers (ISPs). Can view traffic sent and received from either users or Zcash nodes. Can store observed traffic, forward traffic to other parties, and compare traffic with other traffic.

Government actors. Can issue secret subpoenas and force ISPs and regular Zcash users to take actions they may not wish to take, such as turning over secret keys or server logs.

3.3 Attack Vectors

We now review known attacks in the literature that have been described for decentralized systems similar to Zcash, although not all attacks have been demonstrated against Zcash specifically. Notably, these attacks leverage decentralized networks where information about the network may or may not be consistent.

Epistemic attacks. A network observer could perform an epistemic attack by observing unique routing information that allows for eventual deanonymization of that user. Again, such attacks are possible in Zcash because users do not control routing information for their transaction.

One example of epistemic attacks against cryptocurrency networks involve the probability of "super-connected" nodes that can link the node from which a transaction originated [4, 1].

Fingerprinting attacks. Fingerprinting user behavior when making a transaction can lead to deanonymizing that user, even if shielded transactions are used. Fingerprinting can be performed by a range of adversaries across many different settings. For example, a malicious light wallet node could observe the frequency and timing of a user's transactions, or even the recipient of a user's transaction could create a profile of the person making payments to them via timing and frequency of their payments, even if that user wishes to remain anonymous.

Denial of service attacks. Such attacks could be performed against Zcash nodes, such as DNS seeders refusing to respond to certain queries, or against Zcash users, such as light wallets refusing to service certain classes of IP addresses.

Partitioning attacks. The Zcash network itself could be partitioned, such that some nodes think they are aware of the entire network, but only instead be aware of a small subset of nodes. Such attacks could be performed by DNS seeders (again, by lying about the state of the network), or even by highly-connected nodes. Such attacks are well-known in the literature and in practice and demonstrated to be practical.

End to end correlation attacks. This attack could occur by an adversary that can obtain the (sender identity, transaction, receiver identity) tuple discussed in Section 3. Such an attack is possible only when the recipient uses a light wallet in such a manner that leaks the transaction that the recipient is interested in, as further described in Section [2]. Otherwise, as all recipients

download information about every transaction via a broadcast-like protocol, and hence an adversary cannot gain a true end-to-end view, unless the recipient themselves is compromised or malicious.

References

[1] Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller, and Pramod Viswanath. Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees, 2018.

[2] Jack Grigg George Tankersley. Light Client Protocol for Payment Detection. https://github.com/gtank/zips/blob/light_payment_detection/zip-XXX-light-payment-detection.rst, 2018. last accessed 2020-05-29.

[3] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. Zcash Protocol Specification. https://github.com/zcash/zips/blob/master/protocol/protocol.pdf, 2020. last accessed 2020-05-29.

[4] Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath. Dandelion: Redesigning the bitcoin network for anonymity, 2017.