Double-Spending Fast Payments in Bitcoin due to Client versions 0.8.1

Report

Author(s):
Karame, Ghassan O.; Gervais, Arthur; Ritzdorf, Hubert

Publication date:
2013

Permanent link:
https://doi.org/10.3929/ethz-a-009900750

Originally published in:
Technical Report / ETH Zurich, Department of Computer Science 789

Double-Spending Fast Payments in Bitcoin due to Client versions 0.8.1

Arthur Gervais
ETH Zurich
8092 Zürich, Switzerland
arthur.gervais@inf.ethz.ch

Hubert Ritzdorf
ETH Zurich
8092 Zürich, Switzerland
hubert.ritzdorf@inf.ethz.ch

Ghassan O. Karame
NEC Laboratories Europe
69115 Heidelberg, Germany
ghassan.karame@neclab.eu

Abstract

In this article, we discuss a possible exploit in Bitcoin that arises from the simultaneous adoption of client versions 0.8.1 and 0.8.2 (or 0.8.3) in the network. In version 0.8.2, Bitcoin clients no longer accept transactions with non-strict signature encoding. As we show, this incompatibility with prior client versions can potentially lead to a double-spending attack in a fast payment setting in Bitcoin. The attack can only work when merchants operate on any client version prior to 0.8.2. Our aim is therefore to raise the awareness of merchants to adopt version 0.8.2 (or 0.8.3) if they are willing to accept fast payments [1].

Attack Description

In what follows, we briefly describe the main intuition behind the envisioned double-spending attack.

Model

We consider a fast payment scenario in Bitcoin, in which the time between the exchange of currency and goods is short (i.e., in the order of a couple of minutes). In this setting, we assume that a merchant does not await for a received Bitcoin transaction to be confirmed, but simply checks that the transaction has been received by its client before serving its clients. Here, we assume that the merchant runs Bitcoin version 0.8.1, and that a considerably large fraction of the peers (including mining pools) in the Bitcoin network have adopted version 0.8.2. Our analysis described hereafter equally applies if a large fraction of Bitcoin peers adopt client version 0.8.3.

Description

Up to version 0.8.1, a transaction signature could contain for instance zero padded bytes and the signature check would still be valid. Since version 0.8.2, transactions with signature with excessive padding will no longer be accepted to the memory pool of nodes nor will they be relayed to other nodes.

1. The adversary sends a transaction TX_1 with a zero-padded signature to the merchant.

2. TX_1 will be relayed to the miners. Miners that use the Bitcoin version 0.8.2 will not accept the transaction in their memory pool, and thus not include it into a block. Miners with an older Bitcoin version will accept it.

3. The adversary waits for a small time t (e.g. 1-5 minutes), until he acquired service from the merchant.

4. If within t, TX_1 was still not included in a Bitcoin block, the adversary sends another transaction TX_2 that double-spends the inputs of TX_1 to the benefit of a new Bitcoin address that is controlled by the adversary. TX_2 is not padded with additional zeros.

5. Since most peers in the network use version 0.8.2, they will accept TX_2 (and will reject TX_1). The higher is the fraction of peers that use version 0.8.2 (or 0.8.3), the larger is the likelihood that TX_2 is included in a block, and that the attack succeeds.

References

[1] Ghassan O. Karame, Elli Androulaki, Srdjan Capkun, *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin.* In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2012 (to appear), Related technical report: Cryptology ePrint Archive Report 2012/248, 2012.