DoS on a Bitcoin Lightning Network channel

Willem Rens

July 5, 2018

MSc Systems and Network Engineering
University of Amsterdam
Research Project 2

Introduction

- Bitcoin has a hard time scaling.
- The Bitcoin Lightning Network was proposed in 2015 by Poon and Dryja.
- A low-latency payment network using Bitcoin's blockchain as its arbitration layer.

Potential DoS vulnerability?

"If one does not broadcast a transaction at the correct time, the counterparty may steal funds."

Research questions

- Can bitcoin in a Lightning Network channel be stolen by a successful DoS attack?
- Is it possible to carry out this attack in version 0.4.2 of the Lightning Labs Lightning Network daemon?

Related work

- McCorry et al. (2016) Regarding Lightning Network channels they state: "The revocation mechanism requires both parties to **check the Blockchain periodically** to detect if a previously revoked channel state has been submitted"
- BitPico (2018) DDoS sends down 20% of Lightning nodes.

Approach to answer research question 1

RQ1. Can bitcoin in a Lightning Network channel be stolen by a successful DoS attack?

1. Explore the design of preventing old channel states to be accepted into the blockchain.
2. Create theoretical attack.

Lightning channel fundamentals

- Bitcoin's scripting system.
- The Lightning Network is created by bidirectional payment channels.
- Real Bitcoin transactions, but not included in the blockchain.

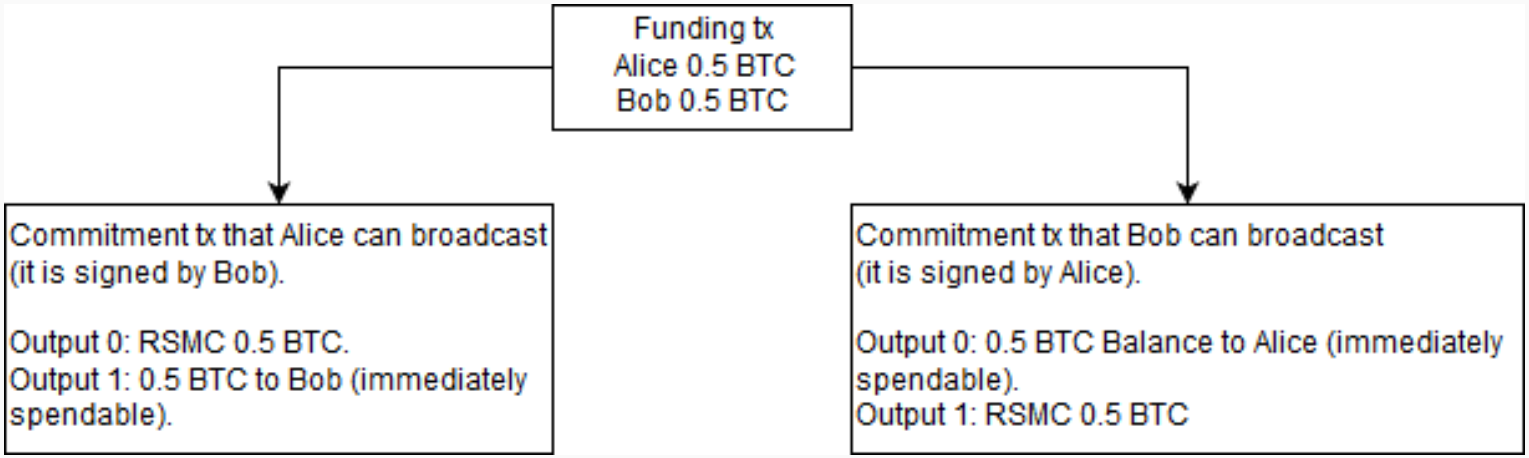
Funding transaction

The transaction that creates a channel. It has a multisignature output.

Commitment transaction

A transaction that embodies a channel state and pays out the respective balances to each channel actor.

Old channel state invalidation



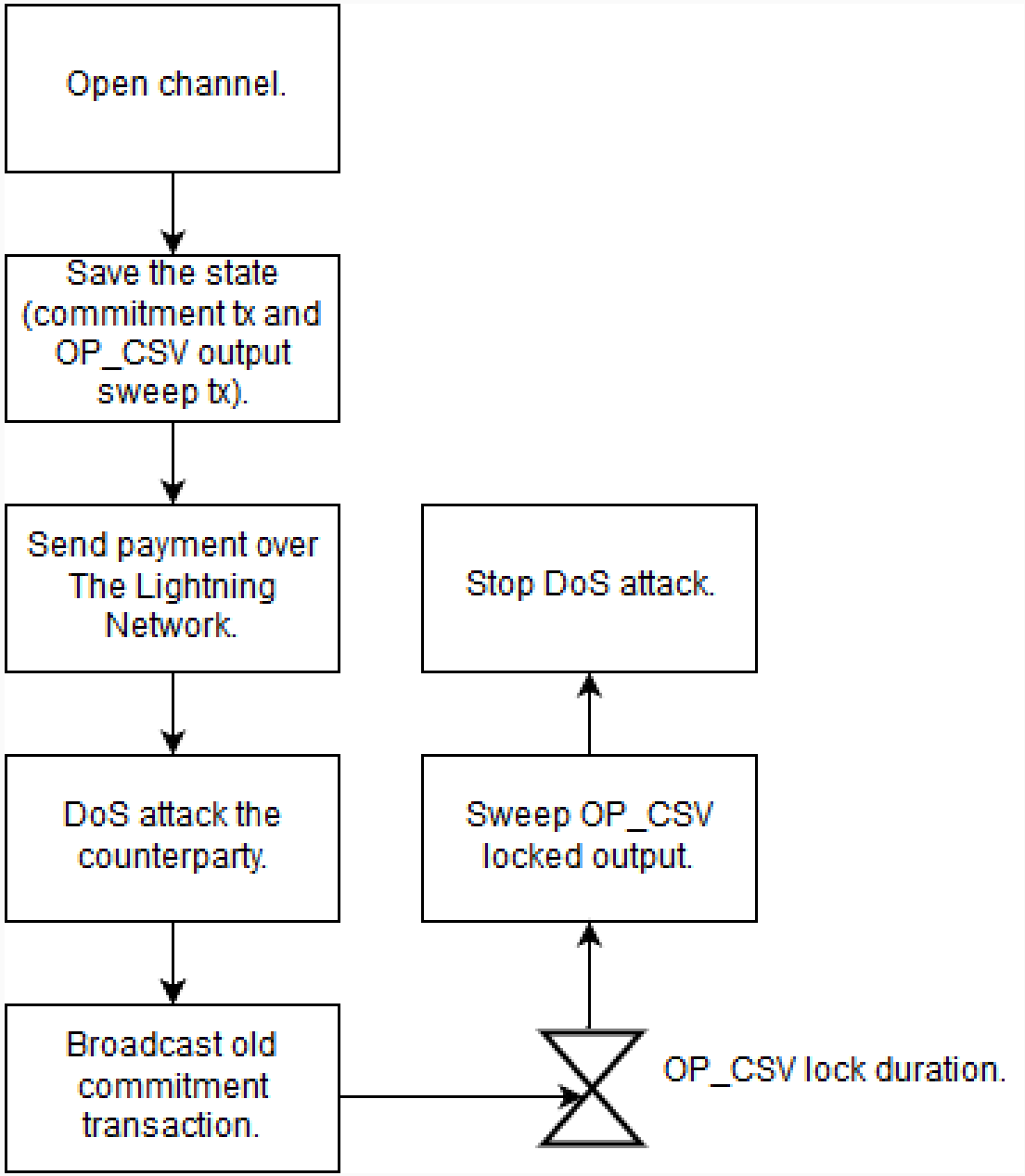
- RSMC spendable in two ways
  - By broadcaster after a relative time-lock has finished, enforced by OP_CSV.
  - By counterparty when using a Breach Remedy Transaction(BRT).

Old channel state invalidation

So to invalidate an old state, actors exchange the needed data to create the BRT.

It follows that, broadcasting an old commitment transaction gives the counterparty an opportunity to claim all the bitcoin in the channel during the time-lock. After the time-lock both can claim the bitcoin.

The Attack in theory



Approach to answer research question 2

RQ2. Is it possible to carry out this attack in version 0.4.2 of the Lightning Labs Lightning Network daemon?

1. Bitcoin core v0.16.0[1] on Bitcoin's testnet3.
2. Lighting Labs Lightning Network daemon[2](LND) v0.4.2-beta.
3. Mallory opens channel with Alice.
4. Mallory pays Alice over the Lightning Network.
5. Mallory tries to get old favorable channel state in Bitcoin's testnet3 blockchain.

[1] https://bitcoin.org/en/release/v0.16.0
[2] https://github.com/lightningnetwork/lnd/releases/tag/v0.4.2-beta

Approach to answer research question 2

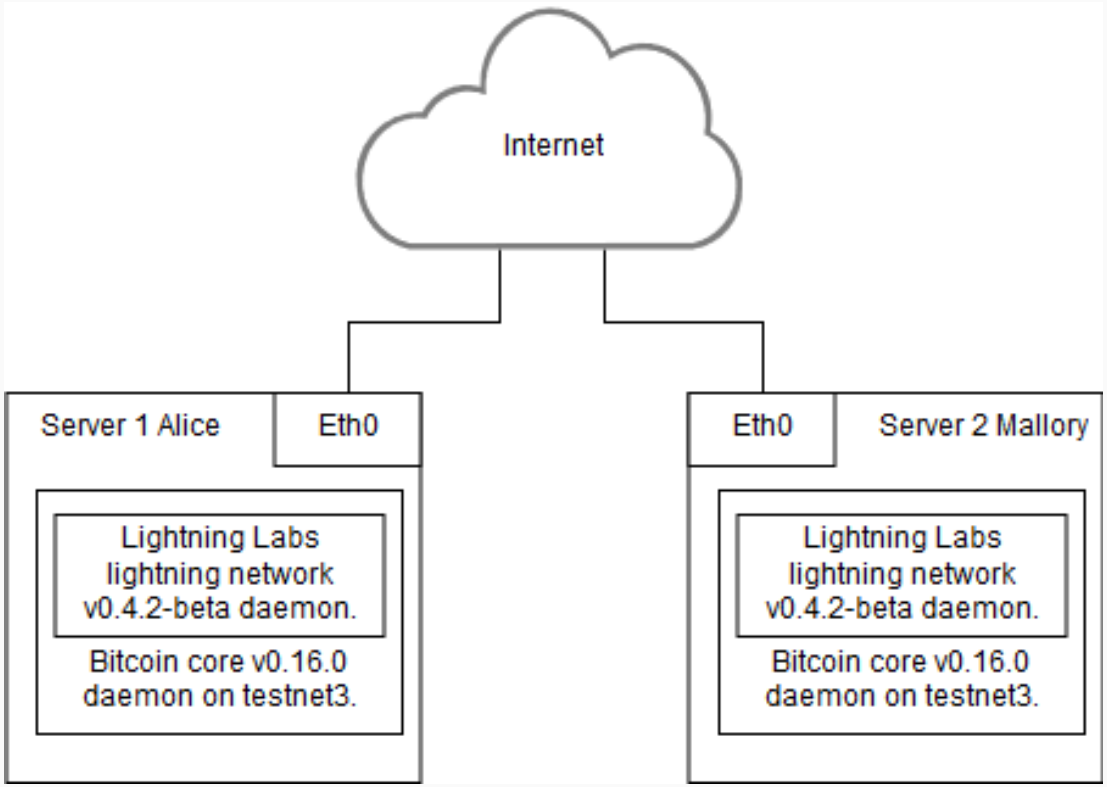


Figure 2: The server set-up during the experiment(s). Server 1's Eth0 interface will be disabled to simulate a successful DoS attack.

Getting access to an old channel state in the LND

To attack we need the commitment and time locked output sweep transaction.

- Adjusts source code to log the relevant transactions (see paper for details).
- Save old state data directory and initialize the LND with it.

DoS duration

The time lock is expressed in blocks, that must pass after the commitment transaction is confirmed on the blockchain.

- Time lock duration scales linearly according to the channel value.
- Max 2016 blocks (14 days), min 144 blocks (1 day).

Attack results

- Attack success: Mallory got all her bitcoin back (minus transaction fees).
- Expected attack time: 24 hour and 10 minutes (145 blocks).
- Actual attack time: 43 hours, 3 minutes and 49 seconds.

See paper or back-up slides for relevant transaction ID's.

Discussion

- Only short up-time is needed for the counterparty.
- Price of \$6700 per bitcoin: attack is profitable at an estimated attacking cost that is lower than \$3.33 per hour.

$$hourlyAttackerCostLimit = \frac{(bitcoinChannelValue * bitcoinPrice) - TxFees}{(144/(OP\_CSVlocktime + 1))/24}$$

- Watchtowers

Conclusion

- Attack presented in theory.
- Successfully executed this attack using the LND.
  - Although simulated, a real DoS attack would achieve the same results.
- In the Lightning Network it is **possible** to claim bitcoin that belongs to a counterparty by making use of a DoS attack.
- For profit attacks not yet seen in the wild.
  - Hard-coded channel value limit.
  - Acceptance limited to a few early adopters.
- Lightning Network software is in beta.

Future work

- Real DoS instead of simulation.
- Multi-hop channel context.

Questions?

Backup slides: transaction ID's

Transaction type	Transaction ID	In blockchain?
Funding transaction	7d0d80c916fc956e555ae4d2bb516ac4 9dc8efbb990bb9427317d8e2e1bbba17	Yes
Old channel state commitment transaction	b06cc0d70d3a8faef975aab390c87027 4c9b963cde8d3754f1959f1874d620fc	Yes
Time locked output sweep transaction	099f1135d7ff29a318f31c45dff2b69e 7e3ea6971d2b68dd9a5974f8738a7e07	Yes
Latest channel state commitment transaction	ef5c8326cf522f0a4f30c818e8de8613 585b2768f22d5b98b6c29e7c3e99d726	No.

Table 1: Relevant Bitcoin testnet3 transactions.

Backup slides: different channel closures