Fuzzing the Lightning Network

Matt Morehouse

https://github.com/morehouse

What is fuzzing?

- https://en.wikipedia.org/wiki/Fuzzing

Why fuzz the LN?

- To find bugs.

Why are LN bugs bad?

- Bad user experience.
- Money is at stake.

Money at Stake

- Credit card

Money at Stake

- Credit card

Money at Stake

- Credit card

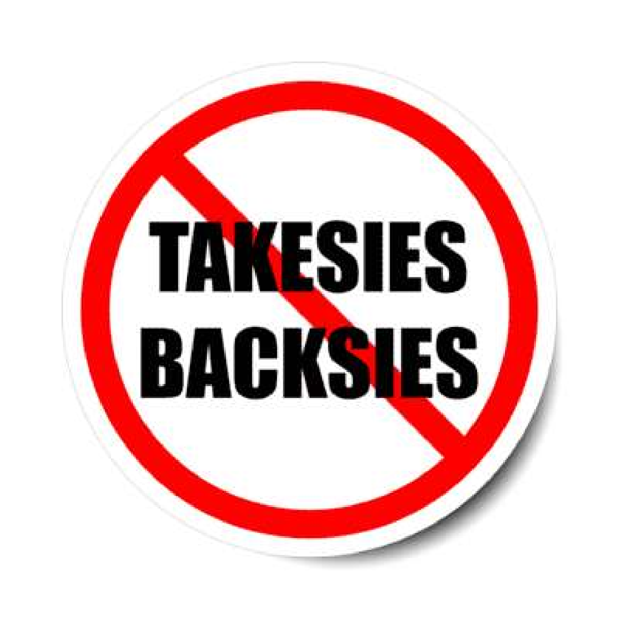
- Lightning

Money at Stake

- Credit card

CUSTOMER SERVICE

- Lightning



Money at Stake

- LN nodes *need* to be online to prevent theft.
- Any crashes put funds at risk.

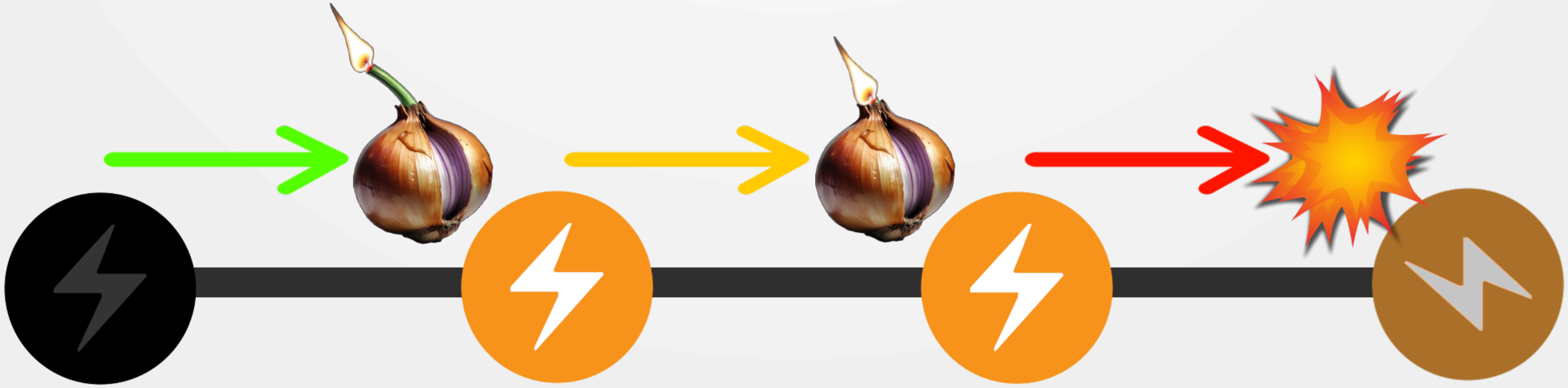
Example Bugs

Example Bugs

- CLN invoice parsing (prior to 23.11)
  - Paying certain invoices caused:
    - Crashes
    - Reading uninitialized memory
    - Buffer overflows
    - Undefined behavior
  - Discovered by fuzz testing (joint work @dergoegge and @morehouse).
  - https://morehouse.github.io/lightning/cln-invoice-parsing/

Example Bugs

- LND onion bomb (prior to 0.17.0)
  - Any node could be instantly and repeatedly crashed by sending malicious onion packets.
  - Source of attack concealed by onion routing.
  - Discovered by fuzz testing (@morehouse).
  - https://morehouse.github.io/lightning/lnd-onion-bomb/



State of LN Fuzzing

State of LN Fuzzing

State of LN Fuzzing

- Not great.

State of LN Fuzzing

- LND

State of LN Fuzzing

- LND
  - 1-2 years ago:
    - 58 basic encode/decode fuzz tests.
    - All fuzz tests were bit rotten and no longer ran.
    - No public corpora.

State of LN Fuzzing

- LND
  - 1-2 years ago:
    - 58 basic encode/decode fuzz tests.
    - All fuzz tests were bit rotten and no longer ran.
    - No public corpora.
  - Today:
    - 106 basic encode/decode fuzz tests.
    - Fuzz regression tests run in CI on public corpora.
    - Minimal new contributions from anyone but @morehouse.

State of LN Fuzzing

- CLN

State of LN Fuzzing

- CLN
  - 1-2 years ago:
    - 11 basic fuzz tests.
    - 4 fuzz tests were effectively useless due to bugs.
    - No public corpora.

State of LN Fuzzing

- CLN
  - 1-2 years ago:
    - 11 basic fuzz tests.
    - 4 fuzz tests were effectively useless due to bugs.
    - No public corpora.
  - Today:
    - 70 basic fuzz tests.
    - Fuzz regression tests run in CI on public corpora.
    - Minimal new contributions from anyone but @morehouse.

State of LN Fuzzing

- CLN

State of LN Fuzzing

- CLN
  - Maintenance issues:
    - UBSan checks inadvertantly disabled.
    - Fuzz regression tests disabled in CI.

State of LN Fuzzing

- eclair

State of LN Fuzzing

- eclair
  - A few randomized (“fuzzy”) tests.
  - No modern fuzz tests (e.g., using Jazzer https://github.com/CodeIntelligenceTesting/jazzer/).

State of LN Fuzzing

- LDK

State of LN Fuzzing

- LDK
  - 60 basic fuzz tests.
  - 3 state machine fuzz tests.
  - Fuzz tests run in CI.
  - Continuous fuzzing by Chaincode Labs.
  - Private corpora maintained by @TheBlueMatt and Chaincode Labs.
  - No major contributions in the past 1-2 years.

State of LN Fuzzing

State of LN Fuzzing

- Little investment by node maintainers in the past few years.

State of LN Fuzzing

- Little investment by node maintainers in the past few years.
- Many maintainers are unfamiliar with fuzzing best practices.

State of LN Fuzzing

- Little investment by node maintainers in the past few years.
- Many maintainers are unfamiliar with fuzzing best practices.
- Few outside contributors (@morehouse, @dergoegge).

Contributing

Contributing

Contributing

- Need more contributors!

Contributing

- Need more contributors!
- Continuous fuzzing for LND and CLN, with coverage reports.

Contributing

- Need more contributors!
- Continuous fuzzing for LND and CLN, with coverage reports.
- Fuzz testing for eclair.

Contributing

Contributing

- More differential fuzzing:
  - Invoice (de)serialization
  - Commitment transactions
  - LND: Decred secp256k1 vs libsecp256k1

Contributing

Contributing

- More state machine fuzzing:
  - Channel funding
  - Commitments and HTLCs
  - Splicing
  - On chain resolution
  - Network graph (gossip)
  - Watchtowers

Questions?