DETER: Denial of Ethereum Txpool sERvices

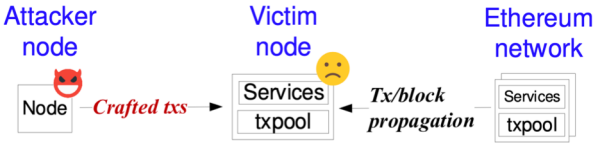
Syracuse University

Kai Li Yibo Wang Yuzhe Tang

Threat Model: a single point of failure

Mining pools and transaction relay services are highly centralized.

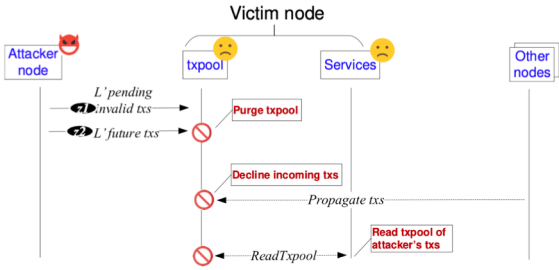
- Attacker node sends crafted transactions to a victim node to disable the victim node's service at a low cost.
- Victim node is a mining pools or relay services

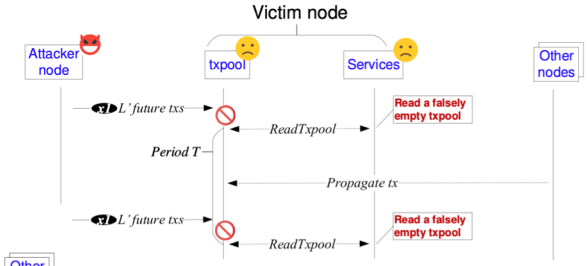


Attack Design: denying the txpool service

Trick a txpool to admit invalid transactions that evict existing normal transactions

- DETER-X:
  - Sending future txs with high price to evict normal txs.
  - No Ether cost.





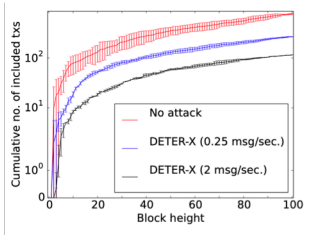
- DETER-Z:
  - Sending latent invalid txs with high price to evict normal txs and occupy the txpool.
  - Low Ether cost.

Mitigation

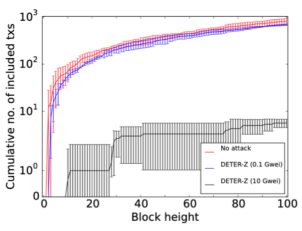
- No admission of future transaction.
- No admission of invalid transaction.
- No admission of tx of the same sender
- No eviction of valid tx by future/invalid tx.
- No eviction of valid tx that transforms existing valid tx into future or invalid.

Evaluation

- The normal node sends pending tx to a victim miner node in a fix rate.
- The attacker sends attack payload to the victim miner node in a fix rate.
- Check the cumulative number of txs included in the mined blocks.



(a) Included txs under DETER-X



(b) Included txs under DETER-Z