NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 54: Blockchain Security - III

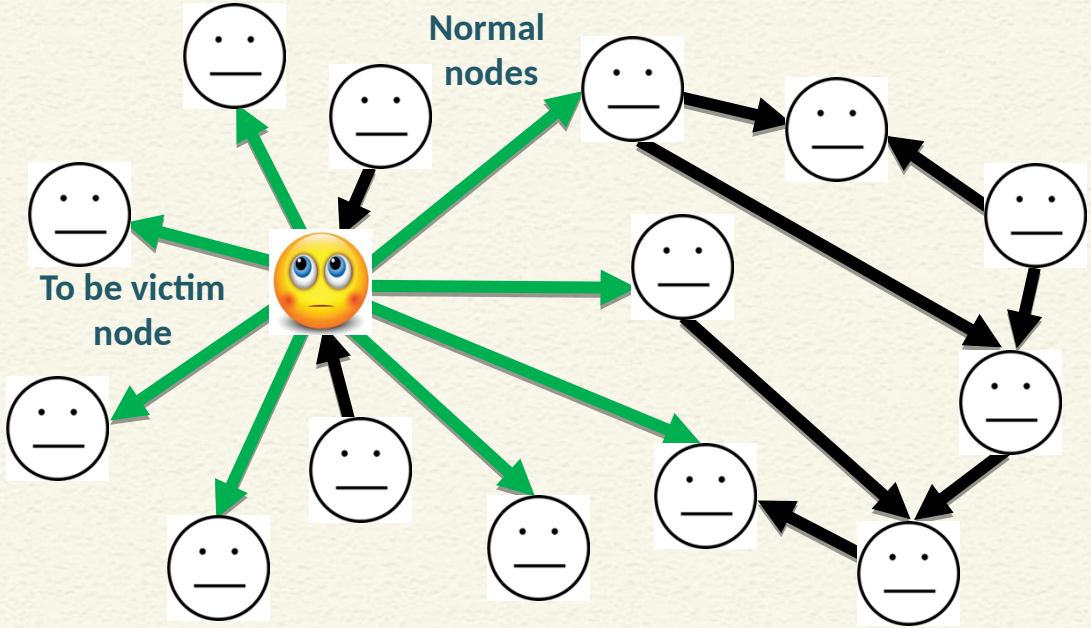
CONCEPTS COVERED

- Eclipse Attack
- Front-running Attack

KEYWORDS

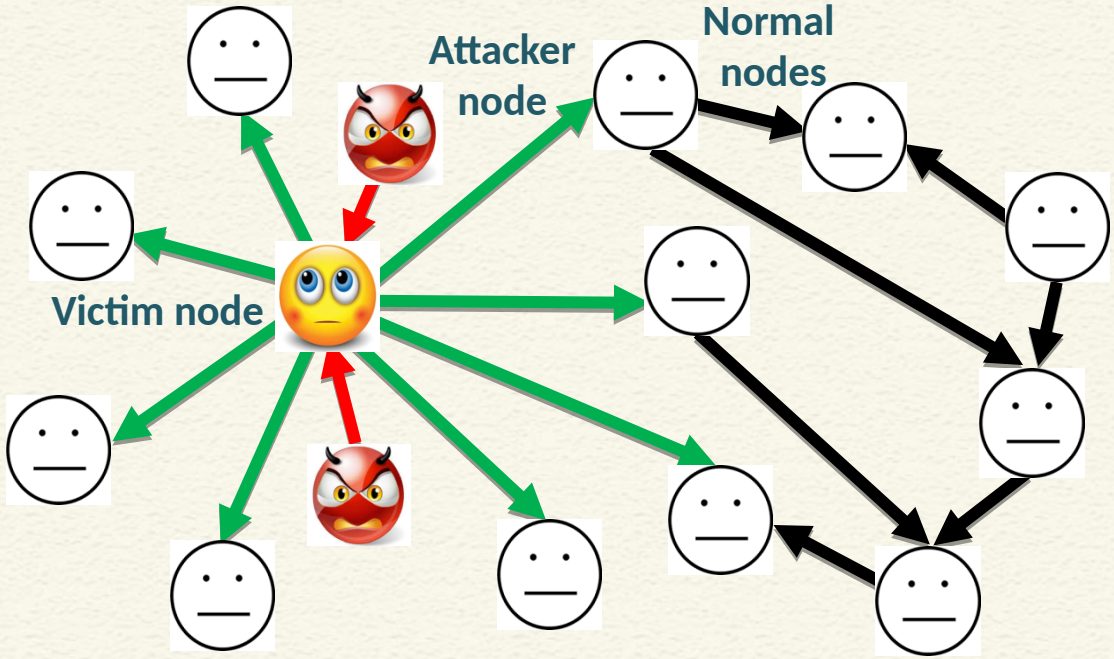
- Eclipse Attack
- Peer-to-Peer Network
- Front-running Attack
- Displacement, Insertion, Suppression

Eclipse Attack

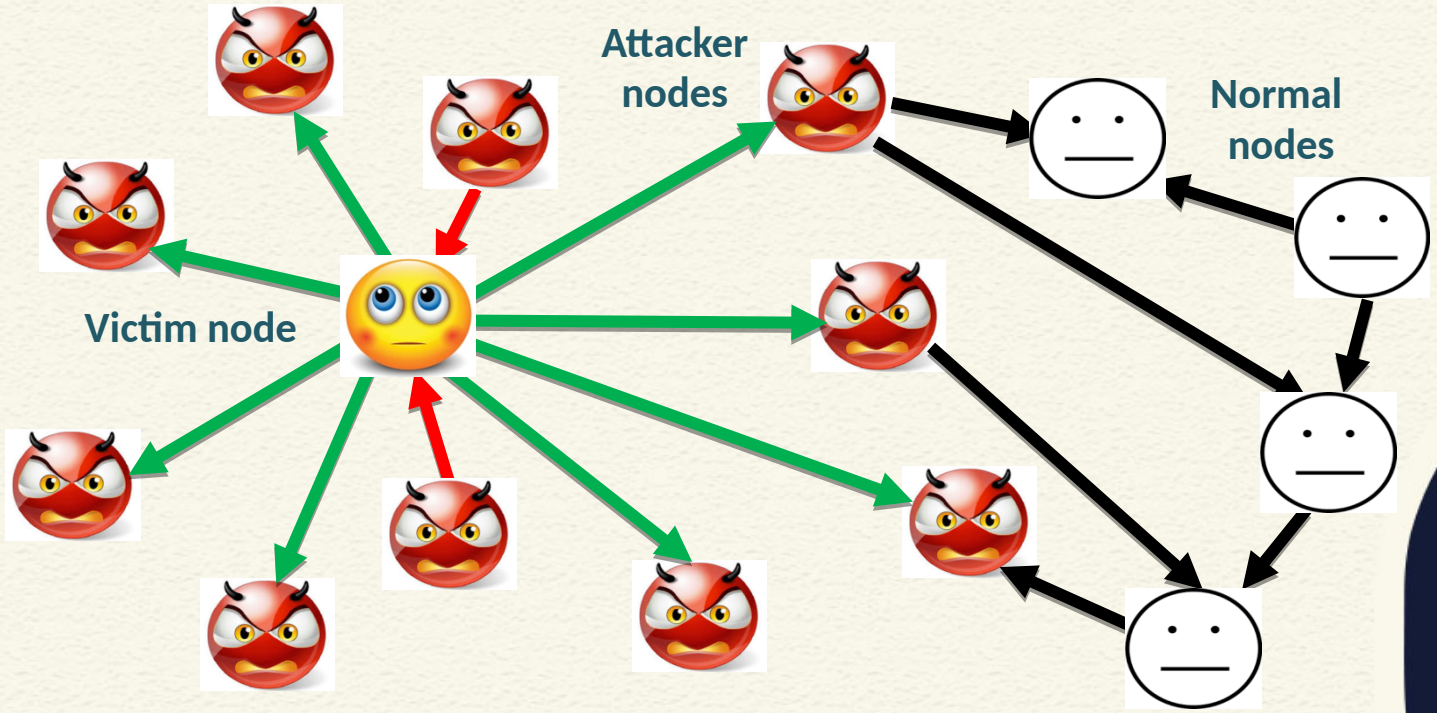


"Eclipse Attacks on Bitcoin's Peer-to-Peer Network", Ethan Heilman, Alison Kendler, Aviv Zohar and Sharon Goldberg, 24th USENIX Security Symposium, 2015

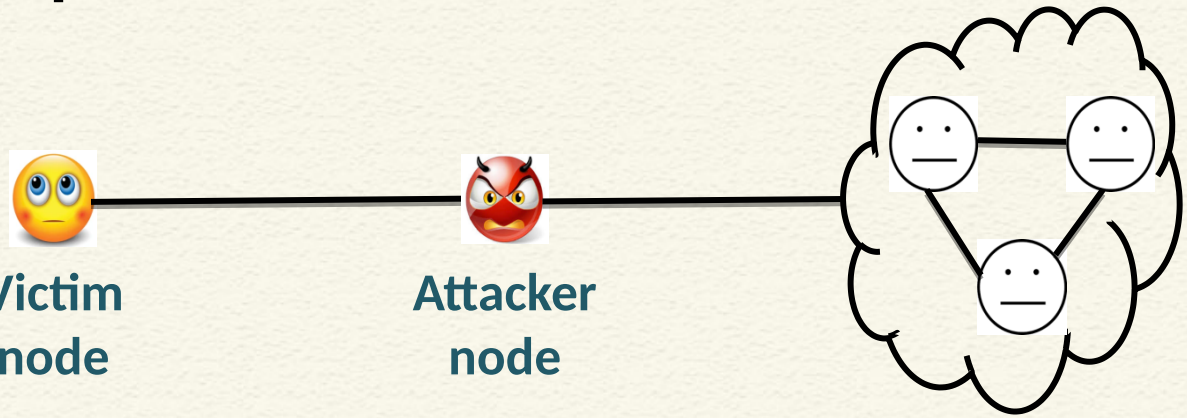
Eclipse Attack



Eclipse Attack



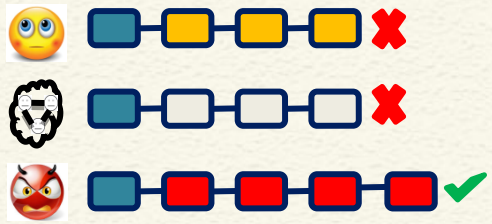
Eclipse Attack



Off-path attack - attacker controls end-hosts, but not key network infrastructure between the victim and the rest of the bitcoin network

Eclipse Attack

Benefit: 51% attack with 40% mining power

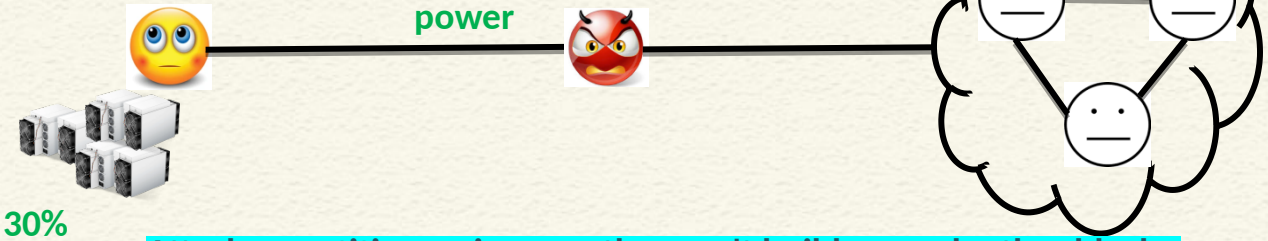


30% Hashing power

40% Hashing power

30% < 40%

40% >30%



30% Hashing power

Attacker partitions miners so they can't build on each other blocks

The attacker then outcompetes each partitioned miner

Eclipse Attack

Attacker populates the victim node's peer tables with attacker's IP addresses

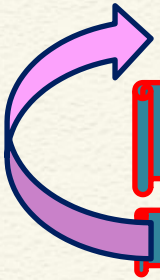
Victim node restarts and loses current outgoing connections

The victim establishes all new outgoing connections to attacker IP addresses

Eclipse Attack

1. Populating of IP addresses

- ✓ Each node picks its peers from IP addresses stored in two tables
  - ➢ New table: IPs the node has heard about
  - ➢ Tried table: IPs the node peered with some point
- ✓ The tables also store a timestamp for each IP
- ✓ Each table stores the IPs in buckets
- ✓ To find an IP to make an outgoing connection to:
  1. Choose new or tired table to select from
  2. Select an IP with newest timestamp
  3. Attempt an outgoing connection to that IP



Attacker populates tables with attacker IPs so that the victim node only connects to the attacker IPs

Selection Bias: Attacker ensures its IPs are the newer one

Eclipse Attack

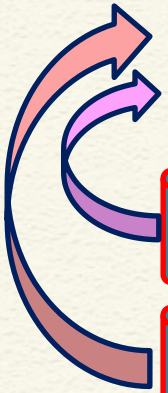
2. Restarting node event is natural?

- ✓ Software/security updates
- ✓ Packets of death/DoS attacks
- ✓ Power/network failures
- ✓ ISP outages

Eclipse Attack

3. Bucket eviction

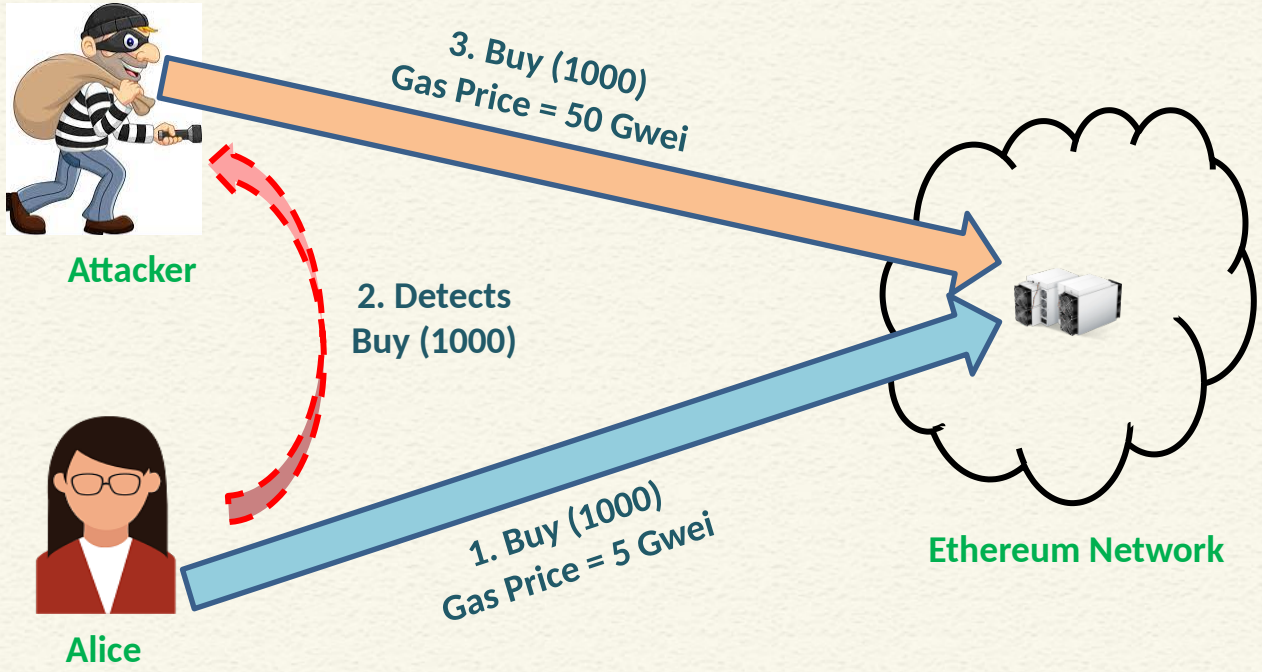
- ✓ The bucket is full, and an IP is inserted into it
  1. Randomly selects 4 IPs
  2. Delete oldest IP
  3. Insert new IP



Eviction Bias: Attacker IPs will always have the **most recent timestamps**

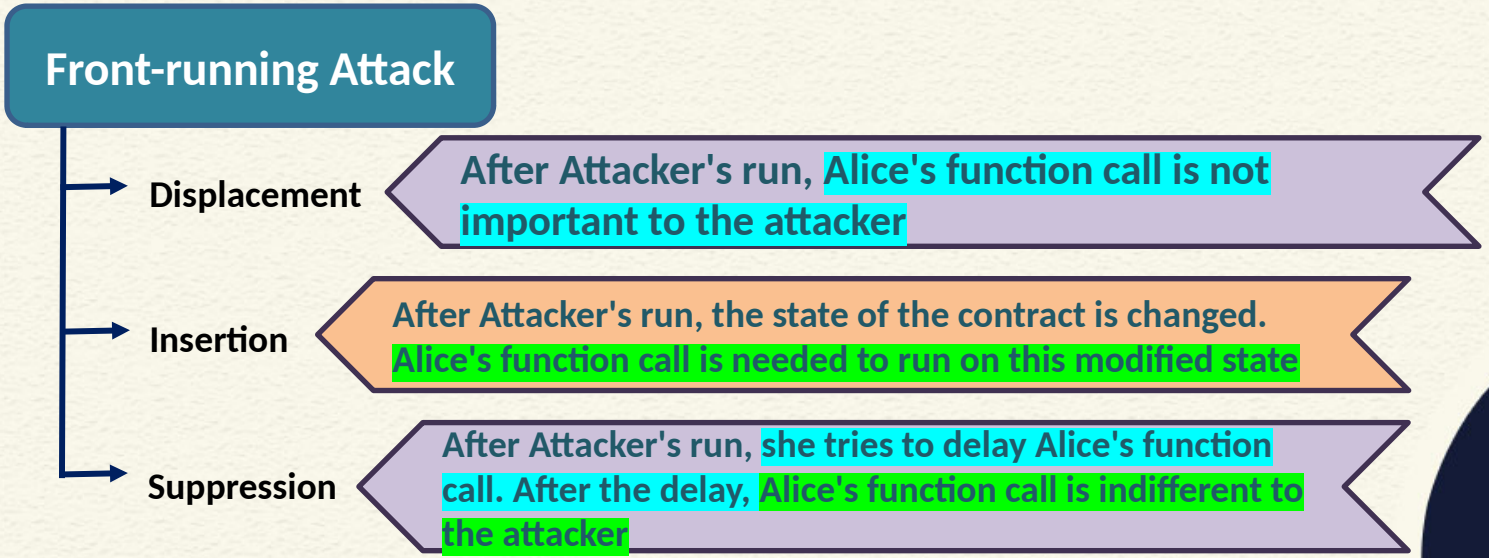
Try-Try-Again: If an attacker IP replaces another attacker IP, the evicted IP is resend and eventually replaced by honest IP

Front-running Attack



"SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain", Shayan Eskandari, Seyedehmahsa Moosavi and Jeremy Clark, FC 2019 Workshops, 2020

Front-running Attack



Front-running Attack

Front-running Attack
(Displacement / Insertion / Suppression)

- **Asymmetric** — Alice is trying to cancel an offer, and Attacker is trying to fulfill it first
- **Bulk** — Attacker is trying to run a large set of functions and Alice is trying to buy a limited set of shares offered by a firm on a blockchain

Front-running Attack

Markets and Exchanges: Spotting a profitable cancellation transaction

(Unordered) mempool

[...]
Cancel (order 100)
Breed (cryptokittie 1, cryptokittie 2)
Buy (order 101)
Bid (B_j)
Register (B_i)
[...]

Adversarial miner mines a block with preferred order

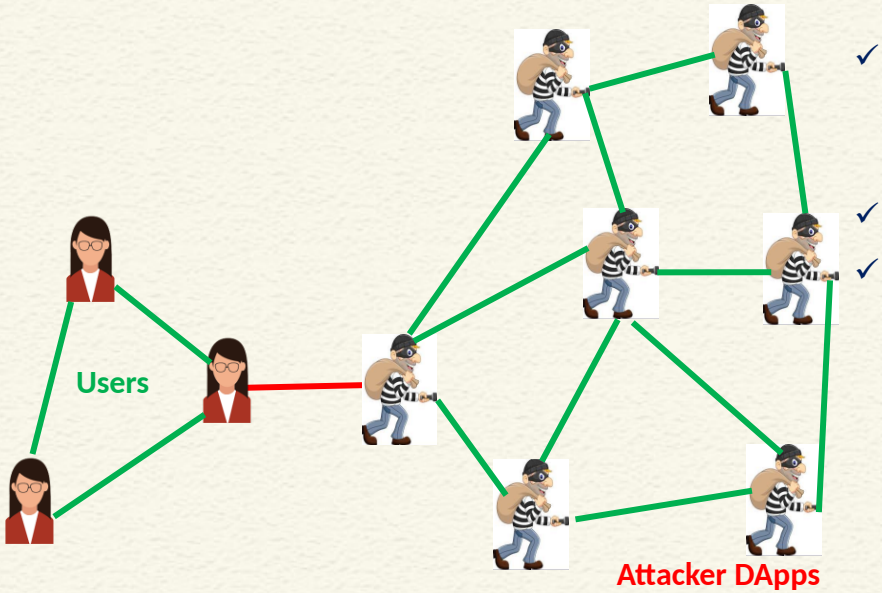
Ethereum Network

Reordered Block

Block Height #N
Register (B_i)
Buy (order 100)
Cancel (order 100)
Buy (order 101)
Bid (B_j)
Breed (cryptokittie 1, cryptokittie 2)

Front-running Attack

Gambling: Bribing miners for prioritizing themselves



- ✓ When the timer of Fomo3D game reached about 3 minutes, the winner bought 1 ticket and then sent multiple high gasPrice transactions to her own DApps
- ✓ Transactions congested the network
- ✓ Bribed miners to prioritize them ahead of any new ticket purchases in Fomo3D

CONCLUSIONS

- Described eclipse attack and front-running attack
- Importance of identifying attacks on blockchain and suggesting remedies
- Combining multiple attacks

REFERENCES

- Web resources as mentioned from time to time


Thank
you