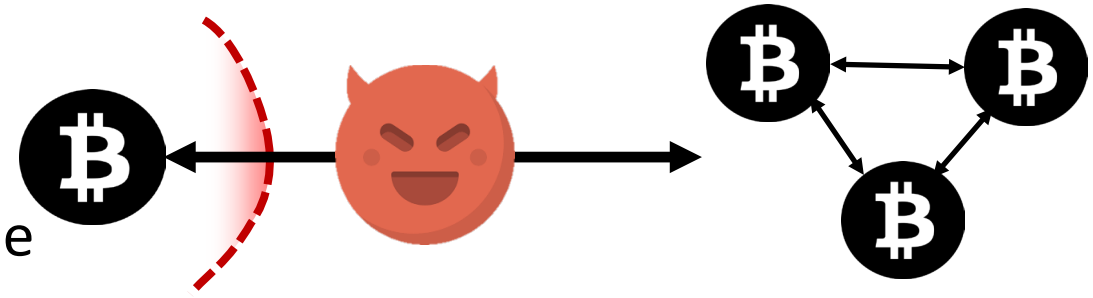
IEEE Symposium on Security and Privacy (**IEEE S&P**) 2020

A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network

Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu, Min Suk Kang

Presented by Hobin Kim

Background – Partitioning attacks



Partitioning ***enables/improves*** several other attacks:

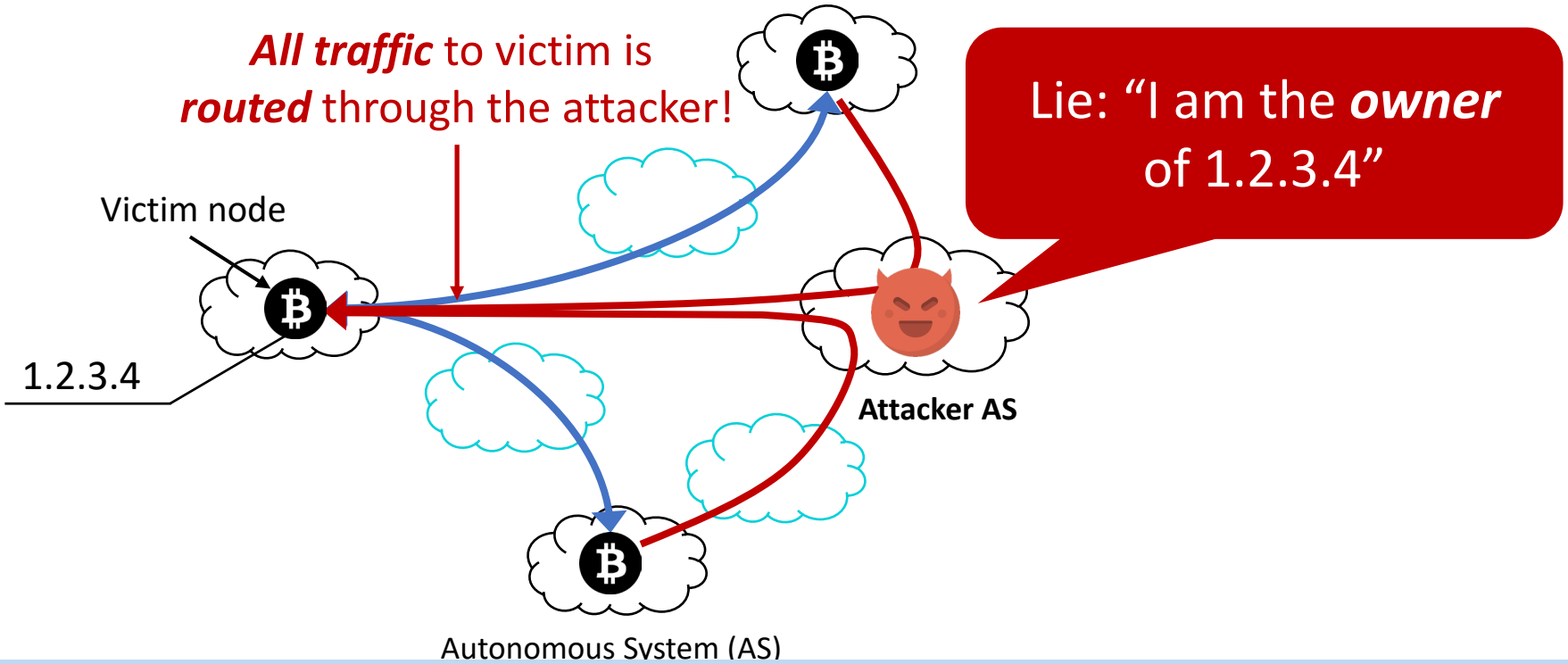
- ✓ 51% attack
- ✓ selfish mining
- ✓ censoring transactions
- ✓ take down cryptocurrencies
- ✓ …

Partitioning attacks: isolate victim node(s) from the rest of network

Related work – Previous work

- Partitioning Attack Against Bitcoin Peer-to-Peer Networks
  - Eclipse attack on Bitcoin's Peer-to-Peer Network (USENIX Security 2015)
  - Bitcoin hijacking attack (IEEE S&P 2017)

Bitcoin hijacking attack

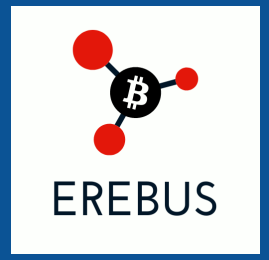


Limitations of the Bitcoin hijacking attack

- Route manipulation is ***immediately visible*** to the public
- Attacker's ***identity*** (AS number) is ***revealed***

Can partitioning attacks be ***stealthier***?

Introduction



Erebus attack

A stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network

001 **Who** can be the attacker and victim?

- Tier-1 and large Tier-2 ASes
- 10K public Bitcoin nodes

002 **How** can be the attack launched?

- Partitioning Bitcoin network w/o any routing manipulations
- Adversary AS fills all peer connections of the victim by patiently influencing the targeted nodes' peering decisions

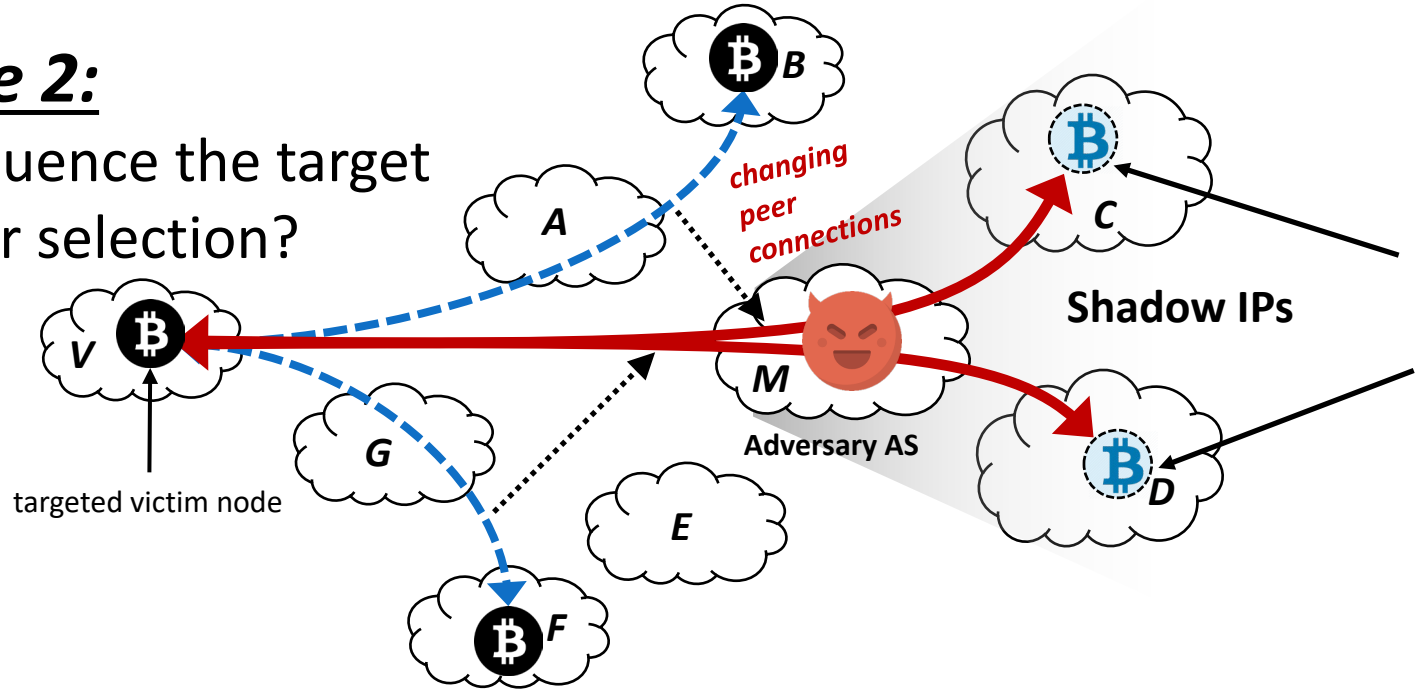
003 Attack **cost**

- Low rate traffic (520 bit/s) during 5-6 weeks

Erebus attack: A ***stealthier*** partitioning attack against Bitcoin network

Challenge 2:

How to influence the target node's peer selection?



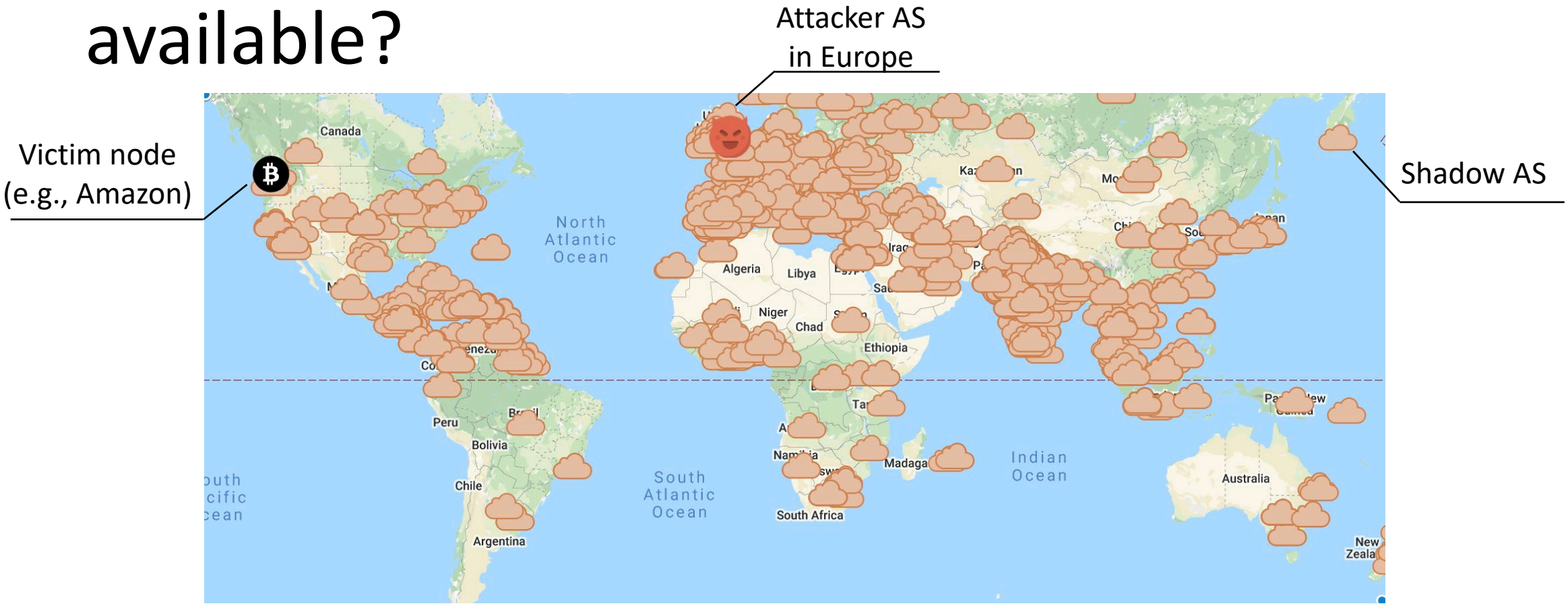
Challenge 1:

Is there enough shadow IPs that the attacker can use?

Idea: ***Indirectly*** force the victim node connects to ***"shadow"*** IPs:

- ✓ ***Shadow IP*** has the victim-to-itself route includes adversary AS
- ✓ Attacker AS is the ***man-in-the-middle*** of all peer connections!

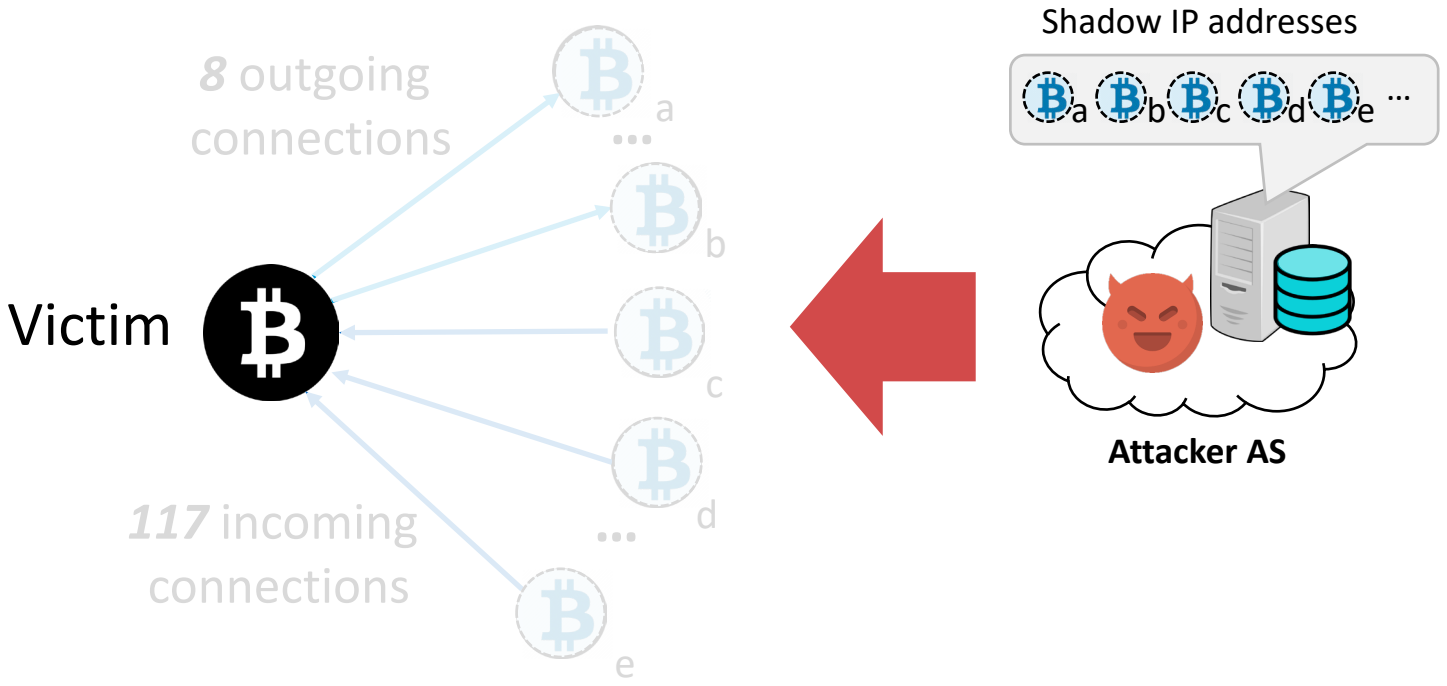
Challenge 1: How many shadow IPs are available?



If attacker AS is big enough (e.g., top-100), it can ***easily*** find

hundreds of shadow ASes => **millions** of shadow IPs

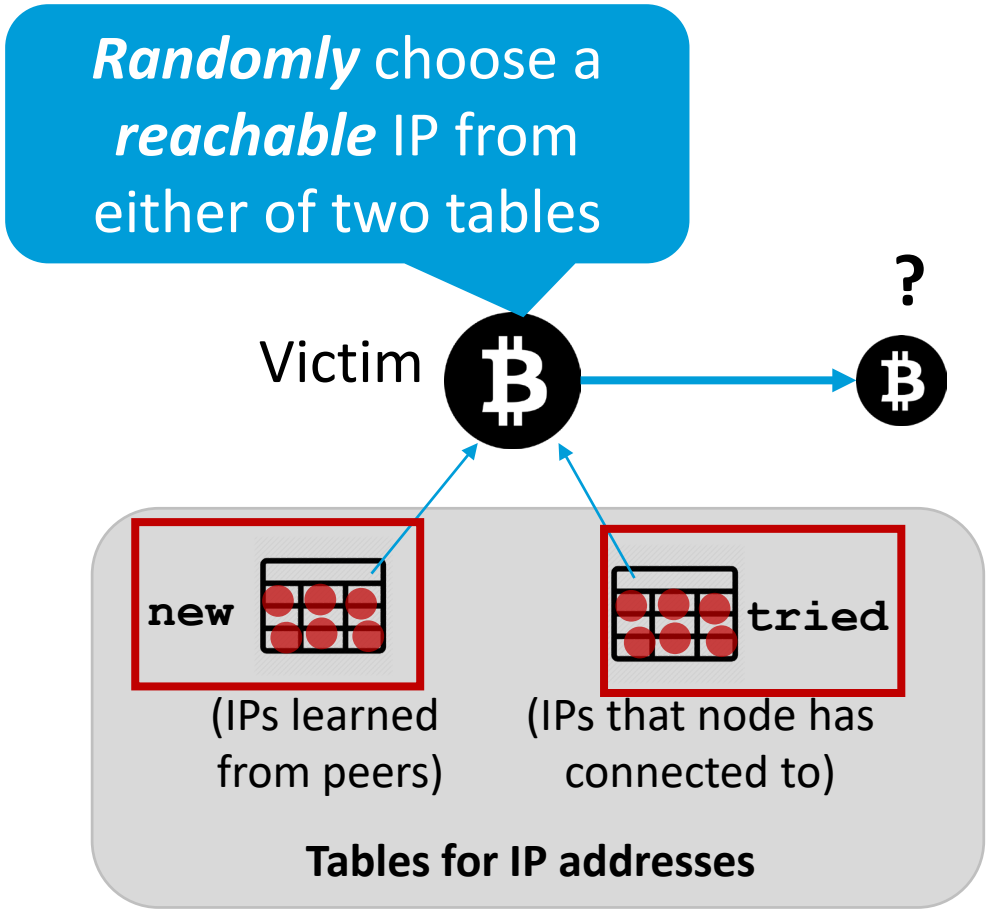
Challenge 2: How does Erebus attacker ***influence*** Bitcoin node's peer selection?



- Occupying 117 incoming connections ***(easier)***
  - ✓Connect to the victim ***on behalf*** of the shadow IPs
- Occupying 8 outgoing connections* ***(much harder!)***
  - ✓Influence the victim to make connections to shadow IPs

(*) 10 outgoing connections since Bitcoin version 0.19.1

How to ***influence*** the victim to connect to shadow IPs?



Our goal: Dominate ***reachable*** IPs in two tables with shadow IPs

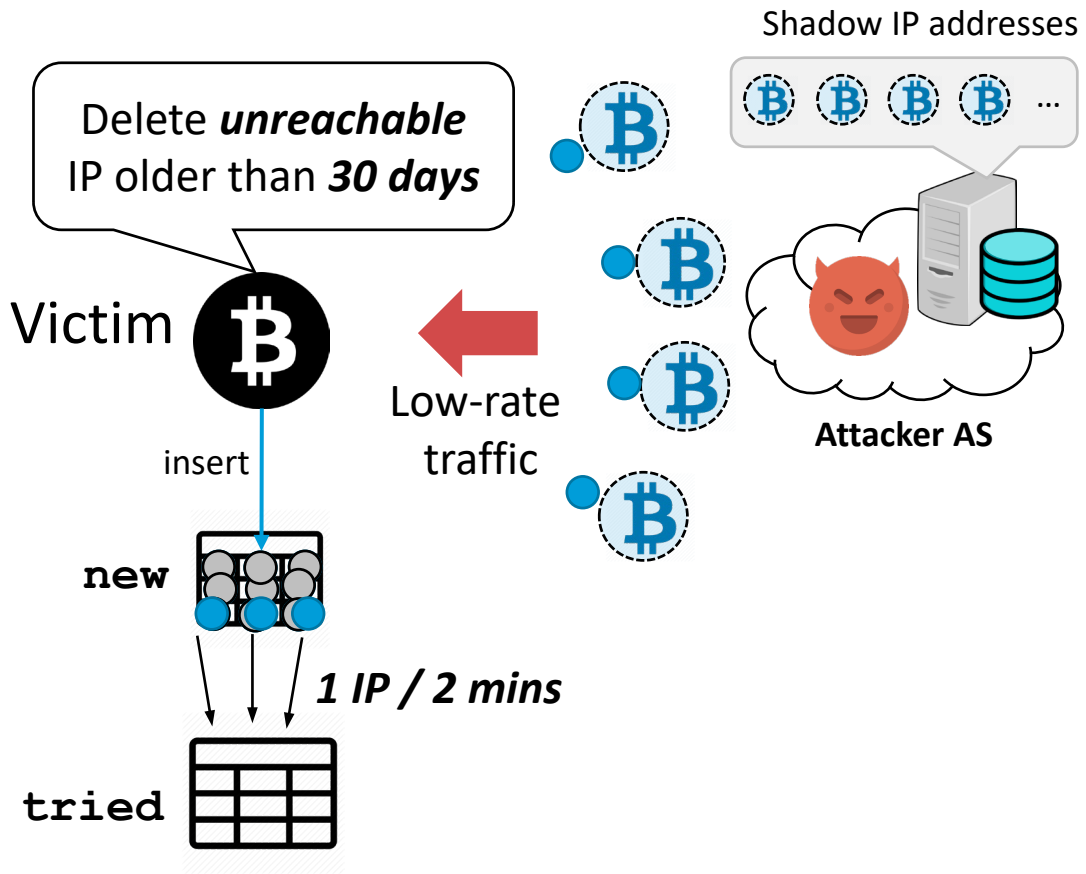
Challenges:

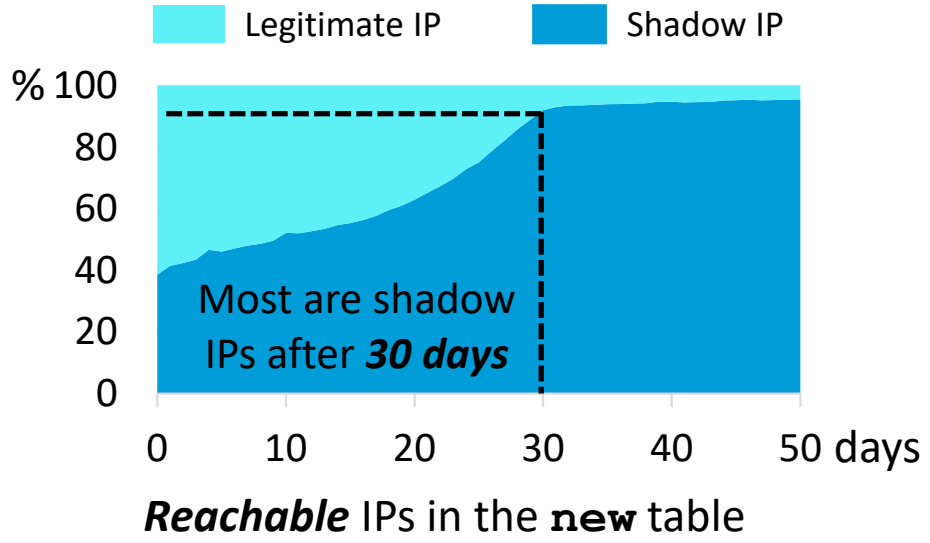
- Several bugs fixed since Bitcoin v0.10.1 (2015)
- Attack is now ***nearly impossible*** with botnets

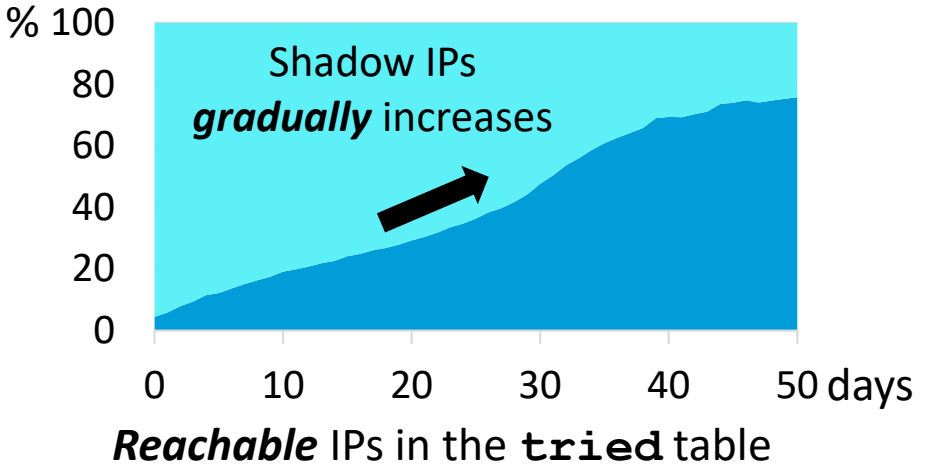
In the old days…

Eclipse attack
(Heilman et al., *USENIX Sec'15*)

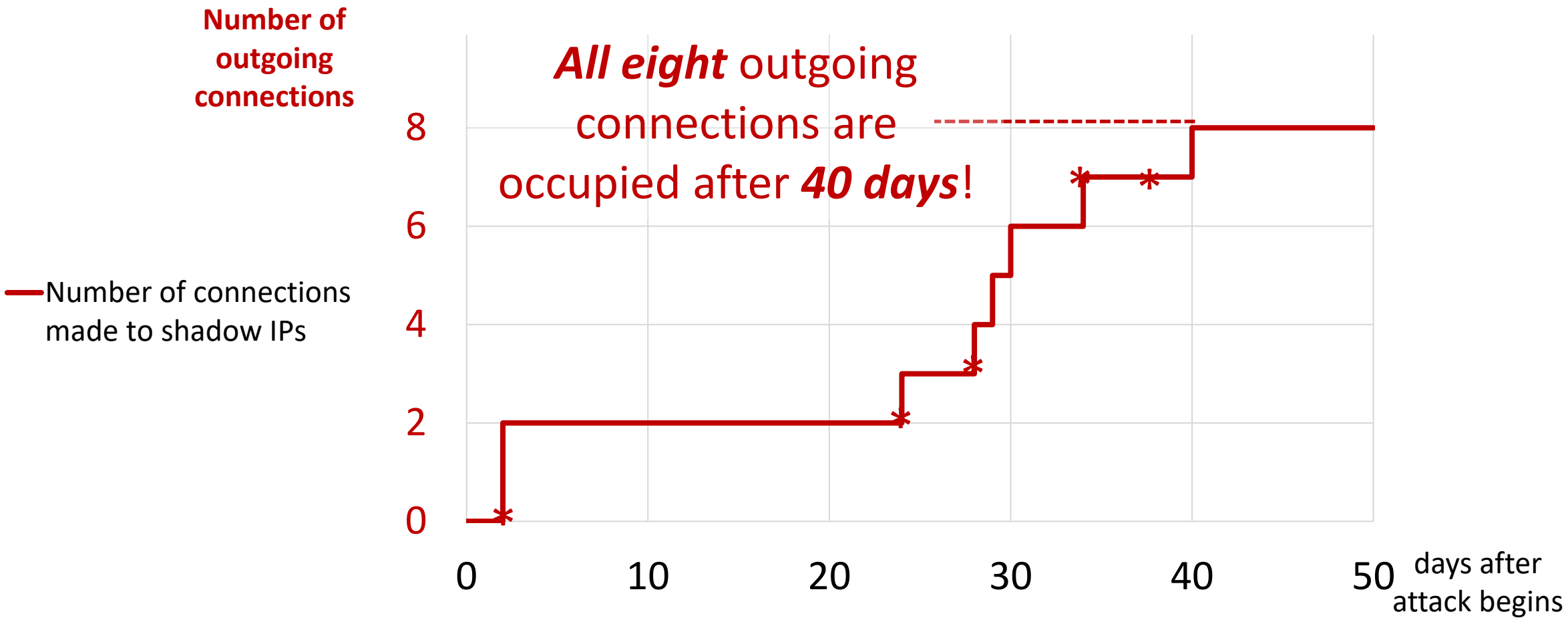
Attack strategy: send ***low-rate*** traffic and ***patiently*** wait







Evaluation: Adversary can occupy ***all*** connections with shadow IPs in ***5 - 6 weeks***



Countermeasures against the Erebus attack

- The Erebus attack exploits the ***topological advantage*** of being large ISPs, ***not*** any specific bugs => ***Hard to counter against!***

- ***Trivial*** (yet ***less practical***) solutions:

  ✓***Trusted*** authority: Whitelist/Blacklist of IPs => ***not permissonless***

  ✓***Third-party*** proxies: VPNs, Tor, relay networks => ***not decentralized***

Bitcoin update after the Erebus attack

- More outgoing connections — *Deployed*
- Incorporating AS topology in the peer selection — *Deployed*
- Protecting peers providing fresher block data — *Discussed*

Summary

EREBUS

- Erebus attack can isolate Bitcoin nodes in a ***stealthy*** manner
  - ✓No route manipulation
  - ✓***Low rate*** attack traffic (520 bit/s per node)
  - ✓Patiently waiting for ***a few weeks***
- Mitigating the Erebus attack is ***hard***
  - ✓***No*** software bugs was exploited
  - ✓Attackers only exploit the ***topological advantages*** of being ISPs

Related work – Future work

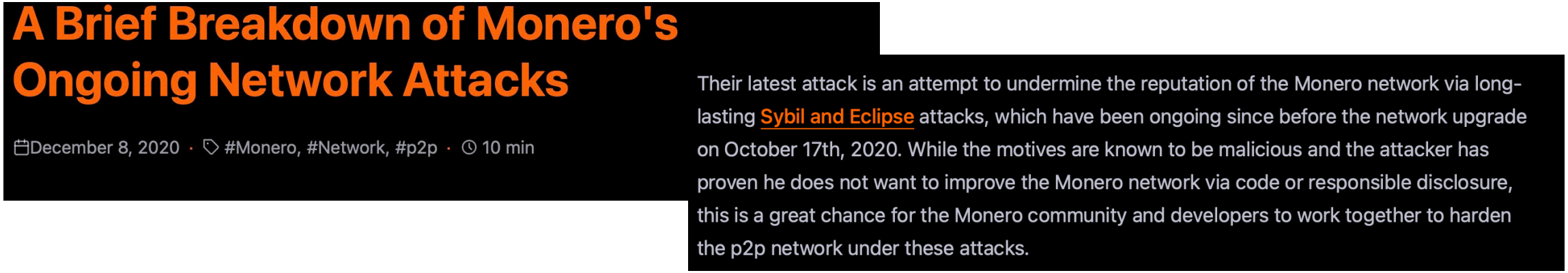
1. Bitcoin Partitioning Attack
   - *SyncAttack: Double-spending in Bitcoin Without Mining Power* by Saad et al. (CCS'21)

2. Defense of the Partitioning Attack
   - *On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin* by Tran et al. (USENIX Sec'21)

3. Ethereum Partitioning Attack
   - *Partitioning Ethereum without Eclipsing it* by Heo et al. (NDSS'23)

Real World Partitioning Attacks on Blockchain

- The breakdown of Monero's ongoing Network on December 8, 2020.
- Attackers executed Sybil and Eclipse attacks
- Attackers spied and dropped the transactions.



Conclusions

- There has been no Erebus attack until now.

- I believe this is because the attacker must make a compromise with large AS in order to carry out the attack, which is costly in comparison to other attacks.

- Does it make sense that no one witnessed the Erebus attack because it was so stealthy? 🤔

Good questions

- Did the bitcoin core security team apply the countermeasure proposed in the paper?

- Is it possible to compel all nodes to update to the latest version which patches the defense policy?

- The paper shows that the Erebus attack is effective in partitioning the Bitcoin network by hindering Bitcoin protocol such as mining decisions. How Erebus attack applied to non-PoW blockchain network?

Best questions

- Could using SCION, another network protocol, instead of TCP protocol be one defense? (박승민)

- How relevant can an experimentation on an emulated system be compared to real world application ? Were the same results really achievable on real-world Bitcoin nodes? (Valentin Guittard)

- Is it possible to apply an Erebus attack on other peer-to-peer blockchain networks and protocols? (김동옥)

Appendix A

- Bitcoin peer-to-peer networking stack is ***widely replicated***
  - ✓Erebus attack also applies on ***34 out of top-100*** cryptocurrencies