Routing Attacks in Cryptocurrencies

Maria Apostolaki
ETH Zürich

Joint work with Aviv Zohar, Gian Marti, Jan Müller, Laurent Vanbever
Routing attacks quite often make the news
Russian-controlled telecom hijacks financial services’ Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/27/2017, 10:20 PM
Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

BY ANDY GREENBERG  08.07.14 | 1:00 PM | PERMALINK
BGP hijack steals AWS IP range; cryptocurrency theft ensues
That is only the **tip** of the **iceberg** of routing manipulations
# of monthly prefix hijacks

### October 2015
- Count: 212k

### November 2015
- Count: 176k

### December 2015
- Count: 112k

### January 2016
- Count: 100k

### February 2016
- Count: 119k

### March 2016
- Count: 137k
Can routing attacks impact Bitcoin?
Bitcoin is highly decentralized making it robust to routing attacks, in theory...

- Bitcoin nodes ...
  - are scattered all around the globe
  - establish random connections
  - use multihoming and extra relay networks
In practice, Bitcoin is highly centralized, both from a routing and mining viewpoint.
Mining power is centralized to few hosting networks.

Cumulative % of mining power
68% of the mining power is hosted in 10 networks only
Each attack differs in terms of its visibility, impact, and targets.
Each attack differs in terms of its visibility, impact, and targets

- **Attack 1**
  - Partitioning

- **Attack 2**
  - Delay
This talk…

Attack 1

Partitioning

visible

network-wide attack

generalizable to all Blockchains
Hijacking Bitcoin
Routing Attacks on Cryptocurrencies

1 Background
   BGP & Bitcoin

2 Partitioning attack
   splitting the network

4 Countermeasures
   short-term & long-term
Bitcoin is a distributed network of nodes
Bitcoin nodes establish **random connections** between each other
The Blockchain is a chain of Blocks

Block #42
- prev: #41
  - Tx a1a53743
  - Tx b5x89433
  - ...

Block #43
- prev: #42
  - Tx x5f78432
  - Tx h1t91267
  - ...

Block #44
- prev: #42
  - Tx x5f78432
  - Tx h1t91267
  - ...

21
Miners are grouped in **mining pools**
Mining pools connect to the Bitcoin network through multiple gateways.
Bitcoin connections are routed over the Internet
The Internet is composed of Autonomous Systems (ASes). BGP computes the **forwarding path** across them.
Bitcoin messages are propagated **unencrypted** and **without any integrity guarantees**.
Hijacking Bitcoin
Routing Attacks on Cryptocurrencies

1 Background
BGP & Bitcoin

2 Partitioning attack
splitting the network

4 Countermeasures
short-term & long-term
The goal of a partitioning attack is to split the Bitcoin network into two disjoint components.
The impact of such an attack is worrying

Denial of Service

Revenue Loss

Double spending
The impact of such an attack is worrying

- Denial of Service
- Revenue Loss
- Double spending

Bitcoin clients and wallets cannot secure or propagate transactions
The impact of such an attack is worrying

Denial of Service

Revenue Loss

Blocks in component with less mining power are discarded

Double spending
The impact of such an attack is worrying

Denial of Service

Revenue Loss

Double spending

Transactions in components with less mining power can be reverted
How does the attack work?
Let’s say an attacker wants to partition the network into the left and right side.
For doing so, the attacker will manipulate BGP routes to intercept any traffic to the nodes in the right
Let us focus on node F
F’s provider (AS6) is responsible for IP prefix
AS6 will create a BGP advertisement

![Diagram of AS network with paths and addresses]

- Path: 6
- Path: 8 6
- 82.0.0.0/23
- 82.0.0.1
- Bitcoin symbol
AS6’s advertisement is propagated AS-by-AS until all ASes in the Internet learn about it.
AS6’s advertisement is propagated AS-by-AS until all ASes in the Internet learn about it.
BGP does not check the validity of advertisements, meaning any AS can announce any prefix
Consider that the attacker advertises a more-specific prefix covering F’s IP address
As IP routers prefer more-specific prefixes, the attacker route will be preferred.
Traffic to node F is **hijacked**
By hijacking the IP prefixes pertaining to the right nodes, the attacker can intercept all their connections.
Once on-path, the attacker can drop all connections crossing the partition.
The partition is created
Not all partition are feasible in practice: some connections cannot be intercepted
Bitcoin connections established...

- within a mining pool
- within an AS
- between mining pools with private agreements

cannot be hijacked (usually)
Bitcoin connections established...

- within a mining pool
- within an AS
- between mining pools

Cannot be hijacked (usually)

*but* can be detected and located by the attacker enabling her to build a similar but feasible partition
Same attacker wants to create a different partition
Same attacker wants to create a different partition.
There is a mining pool in the topology
Attacker hijacks all prefixes pertaining to nodes in the orange side.
Attacker hijacks all prefixes pertaining to nodes in the orange side
The attacker drops connections
The partition is created but is ineffective
The partition is **infeasible**
The attacker monitors the connections and detects leakage
The attacker monitors the connections
Theorem

Given a set of nodes to disconnect from the network, there exist a unique maximal subset that can be isolated and that the attacker will isolate.

see paper for proof
We evaluated the partition attack in terms of practicality and time efficiency.

Practicality
Can it actually happen?

Time efficiency
How long does it take?
We evaluated the partition attack in terms of practicality and time efficiency.
Splitting the mining power **even to half** can be done by hijacking **less than 100 prefixes**
Splitting the mining power **even to half** can be done by hijacking **less than 100 prefixes**

*negligible* with respect to routinely observed hijacks
Hijacks involving up to 1k of prefixes are frequently seen in the Internet today.
We also evaluated the partition in terms of time efficiency.
We measured the time required to perform a partition attack \textbf{by attacking our own nodes}.
We hosted a few Bitcoin nodes at ETH and advertised a covering prefix via Amsterdam.

184.164.232.0/22

184.164.232.1-6

Amsterdam

Live Bitcoin network
Initially, all the traffic to our nodes transits via Amsterdam
We hijacked our nodes
We measured the time required for a rogue AS to divert all the traffic to our nodes

diverted bitcoin traffic
cumulative % of connections intercepted

# seconds from start of hijack
It takes less than 2 minutes for the attacker to intercept all the connections.
Mitigating a hijack is a human–driven process, as such it often takes hours to be resolved
Mitigating a hijack is a human-driven process, as such it often takes hours to be resolved.

It took Google close to 3h to mitigate a large hijack in 2008 [6]

(same hold for more recent hijacks)
Hijacking Bitcoin
Routing Attacks on Cryptocurrencies

1. Background
   BGP & Bitcoin

2. Partitioning attack
   splitting the network

4. Countermeasures
   short-term & long-term
Countermeasures exist for both types of attacks
Countermeasures against partition attacks exist

Short-term

Host all Bitcoin clients in /24 prefixes
reduce chances of a successful hijack
Countermeasures against partition attacks exist

**Short-term**
- Host all Bitcoin clients in /24 prefixes
- reduce chances of a successful hijack

**Long-term**
- Deploy secure routing protocols (S-BGP, RPKI)
- prevent partition attacks
Countermeasures against partition attacks exist but are impractical.

Host all Bitcoin clients in /24 prefixes.

Deploy secure routing protocols.
Countermeasures against partition attacks exist but are impractical.

- Host all Bitcoin clients in /24 prefixes
- Increase BGP routing tables
- Deploy secure routing protocols
- ISP collaboration required
Build additional secure channel to allow communication even if the Bitcoin network is partitioned
SABRE = Secure Relay Location + Robust Design

add few clients that connect to each other and to all other clients
SABRE: Additional relay network of relay nodes
Clients connect to at least one relay node
SABRE = Secure Relay Location + Robust Design
SABRE = Secure Relay Location + Robust Design

additional nodes protected against hijacking attacks
SABRE =  Secure Relay Location   +  Robust Design

Open and Resilient against DDoS attacks
Secure Relay Placement

nodes in /24 prefix

peering ASes with no customers

k-connected graph of relays

relays cover most clients
Secure Relay Placement

- nodes in /24 prefix
- peering ASes with no customers
- k-connected graph of relays
- relays cover most clients
- malicious prefix in competition with legitimate ones
If the attacker advertises a longer prefix than the origin
If the attacker advertises a longer prefix all ASes will be vulnerable
The attacker advertises *same length* prefix as the origin
~50% ASes would follow the attacker’s advertisement
Business relations define which AS will follow the attackers advertisement
Secure Relay Placement

nodes in /24 prefix

peering ASes with no customers

k-connected graph of relays

relays cover most clients
Secure Relay Placement

nodes in /24 prefix

peering ASes with no customers

k-connected graph of relays

relays cover most clients

no strictly better prefix advertisement exists
No strictly better advertisement exist
Peering agreement can be revoked
Secure Relay Placement

nodes in /24 prefix

peering ASes with no customers

*k*-connected graph of relays

relays cover most clients

relay connectivity is not affected by any k cuts
Peering agreement can be revoked
2-k connected graph retains connectivity
Secure Relay Placement

nodes in /24 prefix

peering ASes with no customers

k–connected graph of relays

relays cover most clients

relays are in path that are more preferred than any alternative
Secure Relay Placement

nodes in /24 prefix

peering ASes with no customers

k-connected graph of relays

relays cover most clients
SABRE = Secure Relay Location + Robust Design
Software/Hardware co-design

control plane
software

data plane
hardware

SABRE

#A
Software/Hardware co-design is possible because...

programmable hardware

rarely updated state

communication heavy protocol
Software/Hardware co-design is possible because...

programmable hardware

flexible and expressive data plane pipeline

rarely updated state

communication heavy protocol
Software/Hardware co-design is possible because...

programmable hardware

rarely updated state

communication heavy protocol

new Blocks are mined every 10 minutes
Software/Hardware co-design is possible because...

- programmable hardware
- rarely updated state

communication heavy protocol

simple computations, many message exchanges
Software/Hardware co-design is suitable because...

keep up with high demand

dynamic network defenses
Software/Hardware co-design is suitable because...

- keep up with high demand
- sustain DDoS attacks
- Tbps of traffic at line rate
Software/Hardware co-design is suitable because...

keep up with high demand

dynamic network defenses

- Whitelists, BlackLists
- Spoofing Detection
- Amplification mitigation
Hijacking Bitcoin
Routing Attacks on Cryptocurrencies

Bitcoin is vulnerable to routing attacks
both at the network and at the node level

The potential impact on the currency is worrying
DoS, double spending, loss of revenues, etc.

Countermeasures exist
Secure routing is best; SABRE is a good alternative

https://btc-hijack.ethz.ch