An evaluation of the security of the Bitcoin peer-to-peer network

James Tapsell, Raja Naeem Akram, and Konstantinos Markantonakis

Information Security Group,
Royal Holloway

July 30, 2018

jrtapsell.co.uk/bitcoin_2018.pdf

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Table of Contents

1 Introduction

- Who am I?
- Why does security matter?
- What was focused on

2 Seed Integrity

3 Preventing amplification

4 Post Quantum

5 Thanks

Who am I?

- James Tapsell
- Undergraduate student at Royal Holloway, University of London
- Studying *MSci Computer Science (Information Security) with a year in industry*
- I work with the Smart Card Centre, part of the Information Security Group at RHUL
- I take part in CTF competitions, and enjoy developing systems in my spare time

Why does security matter?

- For the Bitcoin currency
  Issues with the Bitcoin network may cause a loss of trust in the Bitcoin network, which may lead to a reduction in value, and also in usage.
- For the Bitcoin miners
  If the network can be exploited this will reduce the value of Bitcoin, resulting in a loss for any miners who own equipment purchased based on the current cost.
- For the internet as a whole As the Bitcoin network is so large, if it can be used to attack systems then the impact may be large enough to affect the wider internet.

What was focused on

- The security of the Bitcoin network was analysed
- There were 2 main points that were analysed
  - The security of the seeds that peers use to find other peers in the network
  - Preventing the Bitcoin network being used as an amplifier for DDoS attacks
- There was also some analysis of the effects of quantum computing on the Bitcoin network.

Table of Contents

1 Introduction

2 Seed Integrity
- What can you do by taking over the seeds
- Types of Attack
- Diagram used
- DNS Seeds

3 Preventing amplification

4 Post Quantum

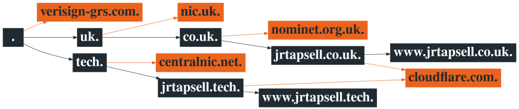
What can you do by taking over the seeds

- Make the network appear to be down to participants
  You could stop certain hosts from being able to participate, if done against high value targets this could raise the chance of an attacker mining blocks.
- Split the network
  You could split the Bitcoin network, causing a netsplit like event, where there are 2 *Bitcoin* networks, by controlling which users end up on which network you may be able to create an situation where you can mine and spend Bitcoins on network A with less effort, as all the larger miners could be put on network B.

Types of Attack

- Attack against one node on-path
  This could be done by the victim's ISP or hosting provider.
- Attack against one node off-path
- Attack against the network
  These could be performed by anyone who wishes to attack the network.

Diagram used



This is the diagram I use to show DNS controlling entities. It gets hostmaster data from domain SOA records.

If an entity controls a parent domain they can affect child domains, and if a set of controllers control all of the seeds they can control the whole network.

- Controlling entities are shown as orange boxes
- Domains are shown as grey boxes
- Grey boxes with looping back arrows show self hosted DNS
- Multiple orange boxes may show the same entity

  Example: `nic.org` and `nominet.org.uk` are both Nominet
- The example diagram on the left shows cloudflare manages both domains

DNS Seeds

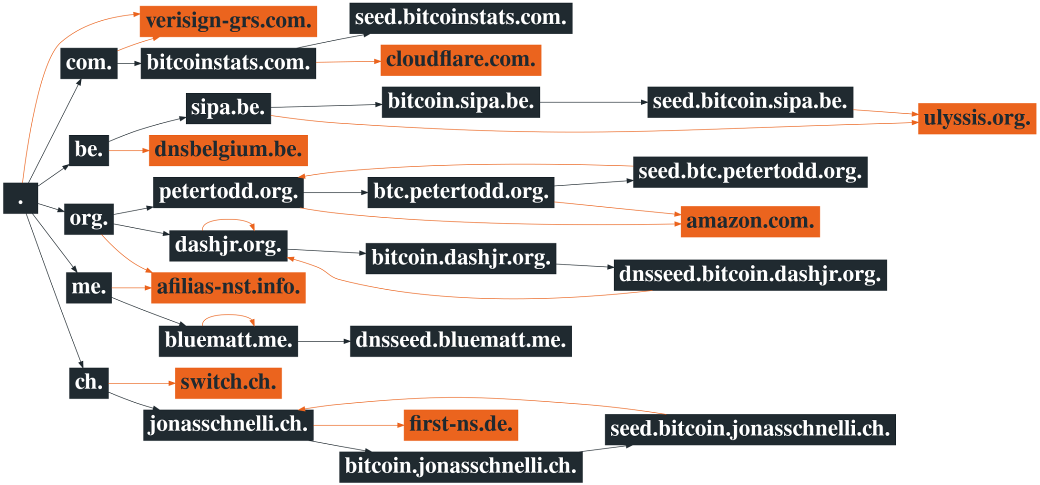

.
com.
be.
org.
me.
ch.
verisign-grs.com.
bitcoinstats.com.
seed.bitcoinstats.com.
cloudflare.com.
sipa.be.
bitcoin.sipa.be.
seed.bitcoin.sipa.be.
ulyssis.org.
dnsbelgium.be.
petertodd.org.
btc.petertodd.org.
seed.btc.petertodd.org.
amazon.com.
dashjr.org.
bitcoin.dashjr.org.
dnsseed.bitcoin.dashjr.org.
afilias-nst.info.
bluematt.me.
dnsseed.bluematt.me.
switch.ch.
jonasschnelli.ch.
first-ns.de.
seed.bitcoin.jonasschnelli.ch.
bitcoin.jonasschnelli.ch.

Table of Contents

1 Introduction

2 Seed Integrity

3 Preventing amplification

- What is a DDoS attack
- What is amplification
- Using Headers
- Using MemPool
- Why is this not happening in the wild

4 Post Quantum

What is a DDoS attack

A DoS attack works by sending traffic to exhaust a resource of the server. This could be one of:

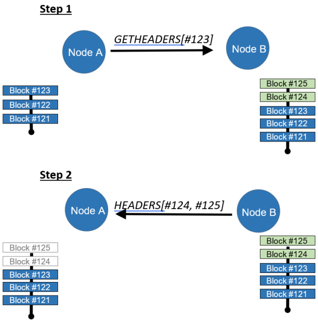
- Bandwidth - Sending so much traffic the server cannot handle it (see LOIC)
- Time - This works by finding a slow command, and using it to take up all of the server's time
- Threads - In some implementations a client can hold a client thread for a long time, if there is a thread cap this can result in a DoS attack

A DDOS (Distributed Denial of Service) expands this by using multiple machines to send the traffic, increasing the amount that can be sent in a time window.

What is amplification

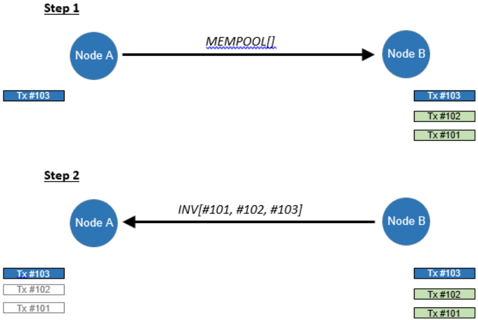
- The limitation to a (D)DoS attack is the ammount of traffic you can throw at a target
- Some systems can be tricked, so that you throw a small amount of traffic at them, and in response they throw a large amount of traffic at another system you choose
- This allows you to turn a small amount of traffic into a large amount of traffic

Using Headers



- A node can request that another node send the IDs of blocks after a certain ID, to allow it to catch up after being offline
- The reply can contain up to 2000 blocks
- Fortunately, the response will only contain the block IDs
- This limits the amplification factor to 1,000

Using MemPool



- In order to mine a miner needs a copy of the unconfirmed transactions
- The reply can contain up to 50,000 transactions
- Fortunately, the response will only contain the transaction IDs
- This limits the amplification factor to 13,000

Why is this not happening in the wild

- Bloating the MemPool on demand would cost
  In order to bloat the MemPool the attacker would have to make a large amount of transactions, which raises the cost of the attack.
- There are other more powerful attacks
  There are other DDoS amplifiers which can get higher amplification factors (51k vs 13k), and are easier to perform than attacks using the Bitcoin network, as they don't require guessing the sequence number.
- This is not protection though, as attackers can mix multiple amplifiers to make the attack harder to detect or prevent.

Table of Contents

1 Introduction

2 Seed Integrity

3 Preventing amplification

4 Post Quantum

- Post Quantum

5 Thanks

Post Quantum

- There are several ways in which quantum computers could threaten the Bitcoin network.
  - They could be able to break the currently used public/private keys
    ECRYPT II estimates the keys will be secure to 2030-2040
  - If an algorithm is found to break mine quickly this may make 51% attacks possible
- Work is ongoing about how the network can be hardened against these attacks.
- There may be issues trying to move old keys to the new system.

Table of Contents

1 Introduction

2 Seed Integrity

3 Preventing amplification

4 Post Quantum

5 Thanks

- Thanks

Thanks

Thank you for listening
Slides: www.jrtapsell.co.uk/bitcoin_2018.pdf
Feedback: feedback@jrtapsell.co.uk / jrtapsell on Keybase