Computer Security

09r. Review – Assignment 9

Paul Krzyzanowski

TAs: Fan Zhang, Shuo Zhang

Rutgers University

Fall 2019

Question 1

What is an input in a Bitcoin transaction?

An input is a list of references to past transactions that show where you received the coins.

Question 2

What is the purpose of change in a bitcoin transaction?

Every input (past transaction) has to be used up completely.

If there is any leftover bitcoin, it is sent back to the owner as change.

Once a transaction has been referenced, the input is considered "spent" and cannot be reused.

Bitcoin nodes keep an index of unspent transactions as an optimization to avoid searching through spent transactions.

Question 3

How do bitcoin nodes agree on the order of transactions?

Transactions are grouped into blocks: a new block is created approximately every 10 minutes, contains approximately 4,000 transactions, and is about 1 MB in size

Transactions in one block are considered to be concurrent.

To add a block to the blockchain, each node solves a math problem

- It modifies a field in the block until a SHA-256 hash of the block is less than a specific value.
- This value is called **proof-of-work**.

Whoever solves it first proposes the block as the next block in the chain.

Question 3 (continued)

How do bitcoin nodes agree on the order of transactions?

Having two or more nodes compute the proof of work at around the same time is extremely unlikely.

If this does happen then we will have a competing chain: two versions of the blockchain

- This can also happen if some bitcoin nodes fail to communicate with others … or if some run malicious software.

Eventually, other blocks get added to the blockchain

- The chain with the most blocks (longest) is considered the legitimate one and it wins

Question 4

What does an attacker need to do to create a double spending attack?

You need to modify past transactions:

- If Alice sent 0.5 BTC to Bob, she will change that transaction to send 0.5 BTC to Charles instead.
- However, she would need to compute a new proof of work value for that block so the hash will be valid
- Bitcoin uses hash pointers: a block contains a hash pointer to the previous (earlier) block
- She would need to compute proof of work values for all newer blocks so that her modified version of the blockchain is valid

Question 4 (continued)

What does an attacker need to do to create a double spending attack?

However, new transactions are always coming in, making the blockchain get longer as new blocks get added

- Alice would need to change the existing blockchain but also compute proof of work values for new blocks faster than ***everyone else*** in the network so that she would have the longest valid chain.
- If she can do this then her chain becomes the official version of the blockchain and everyone updates their copy.
- This is called a **51% attack**. To have a chance of succeeding, you need more compute power than the reset of the systems in the Bitcoin network combined.
- This is why transactions further back in the blockchain are considered to be more secure.

Question 5

What is the **same-origin policy** in web browsers?

It's a security mechanism that does not allow scripts in one web page to make requests to a domain in a different origin.

For two web pages to have the same origin, the URL must contain:

- **Same protocol**: http is different than https
- **Same domain name**: www.rutgers.edu is different than rutgers.edu
- **Same port number**:
  www.rutgers.edu:80/index.html is different than
  www.rutgers.edu:8080/index.html

Question 6

How does **DNS Rebinding** subvert the same-origin policy?

A malicious DNS server provides an address for a domain name with a short TTL (time to live)

This causes the operating system to do another DNS name lookup when a script on a page from that domain requests more content from the domain

- The next time the DNS server is contacted, it returns a different address to a query of the domain name - that of a local system on the user's network.
- The browser treats it as the same origin because the domain name did not change.

Question 7

The June 2019 release of the Google Wifi access point software “improved web security by blocking DNS rebinding.” What does **DNS Rebinding Protection** do?

Do a google search for this: Google Wifi Help at

https://support.google.com/wifi/answer/9144137?hl=en

States that DNS rebinding protection "blocks the use of private IP ranges by public domains.”

This makes sure that scripts on public web pages cannot reference private IP addresses. Private addresses are for internal networks and are not routable on the Internet:

- 192.168.x.x
- 172.16.x.x – 172.31.x.x
- 10.x.x.x

The end