Security of Bitcoin light wallets (aka SPV)

Renaud Lifchitz
September 9th, 2017

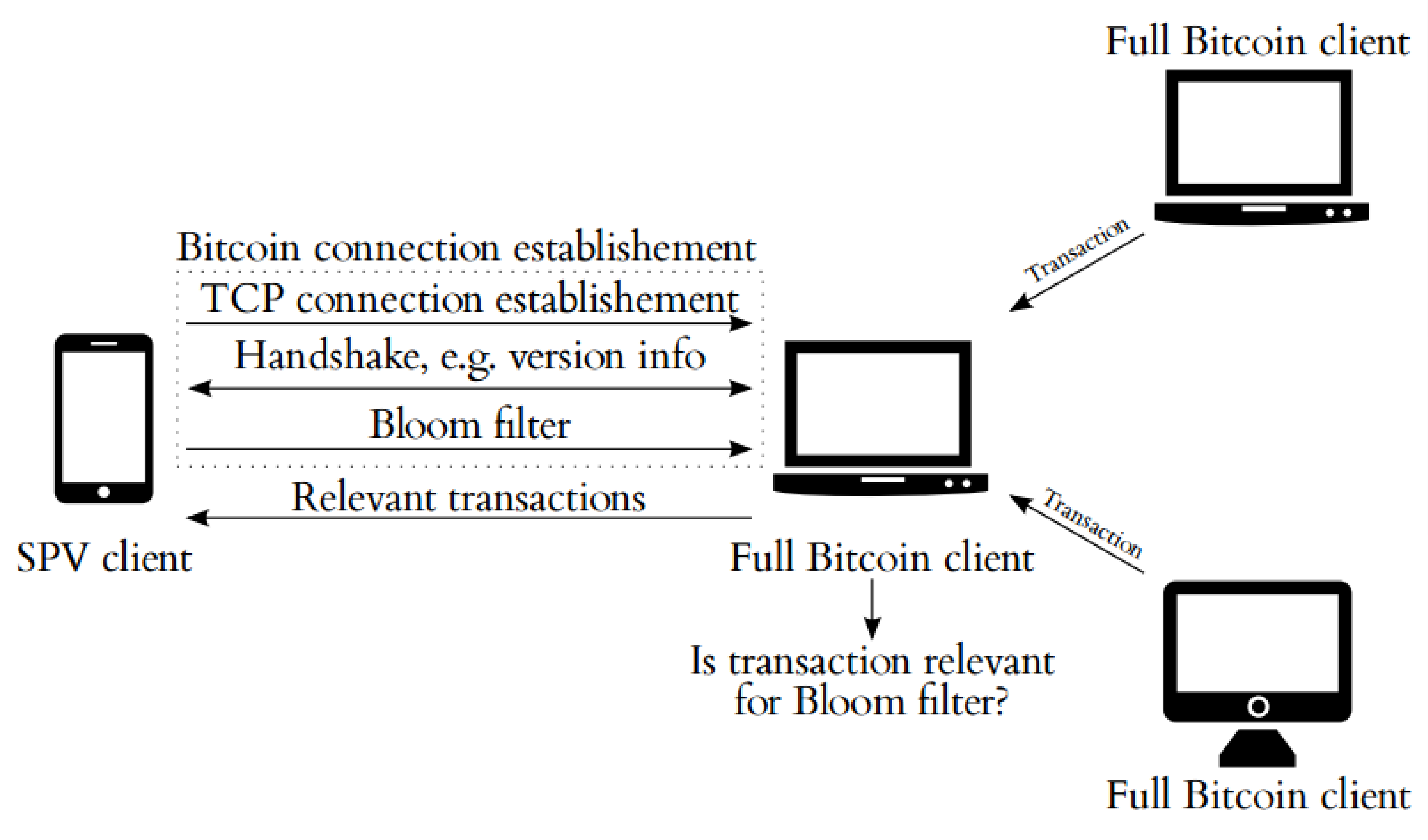
Speaker’s bio

- Senior security expert working @ Econocom Digital Security (https://www.digitalsecurity.fr/en/)
- Main interests:
  - Security of protocols
  - Wireless protocols
  - Cryptography
  - Blockchain!
- Bitcoin & Ethereum developper & enthusiast
- Public presentations: https://speakerdeck.com/rlifchitz
- Twitter: @nono2357

What are light wallets?

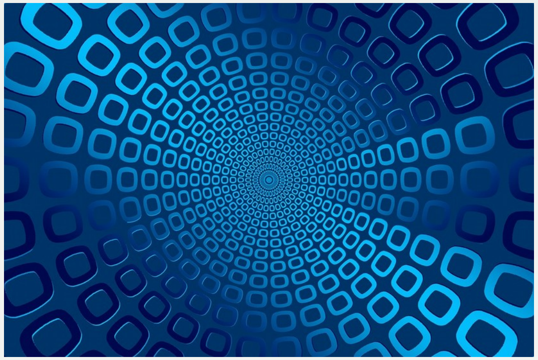
- Light wallets = lightweight clients = thin clients
- A kind of wallet that doesn't need to download the full blockchain to work
- SPV (Simplified Payment Verification):
  - Most light wallets use SPV
  - SPV suggested in original Bitcoin paper: https://bitcoin.org/bitcoin.pdf
  - Use of all block headers and tx count to know if a transaction was already included in the blockchain (only ~ 4.2 Mb/year)
  - Use of Bloom filters to request&match its own transactions

What are light wallets?



Source: https://eprint.iacr.org/2014/763.pdf

Bloom filters



- Space-efficient data structure
- Used to test whether an element is a member of a set without storing the full set
- Probabilistic but... no false negative!
  (only few false positive)
- Used in SPV to know what transactions can be related to some user's addresses

Bitcoin light wallets examples

- Most smartphone wallets... for performance reasons
- Jaxx: https://jaxx.io/
- Electrum: https://electrum.org/

Peer discovery

- Needed to connect to full nodes to:
  - Download block headers
  - Submit Bloom filters
  - Download specific transactions
- Possibilities to bootstrap the discovery:
  - Hardcoded list of nodes
  - Use of DNS seeds
- Sensitive because an attacker can set up malicious nodes
- Sybil attacks: if an attacker is able to set up a lot of malicious nodes, the victim will probably pick one of them...

Peer discovery – DNS seeds

```
$ host seed.bitcoin.sipa.be
seed.bitcoin.sipa.be has address 83.149.125.79
seed.bitcoin.sipa.be has address 150.140.188.181
(... 21 other IPv4 hosts ...)
seed.bitcoin.sipa.be has address 104.199.142.247
seed.bitcoin.sipa.be has address 37.120.174.32
seed.bitcoin.sipa.be has IPv6 address 2607:5300:204:40f1::
seed.bitcoin.sipa.be has IPv6 address 2001:0:9d38:90d7:3858:553f:92ce:18b8
(... 11 other IPv6 hosts ...)
seed.bitcoin.sipa.be has IPv6 address 2001:0:4137:9e76:24f9:302a:4d39:ee08
seed.bitcoin.sipa.be has IPv6 address 2001:0:9d38:6ab8:18c2:3a46:a1ec:987c

$ host seed.bitcoin.sipa.be
seed.bitcoin.sipa.be has address 37.120.174.32
seed.bitcoin.sipa.be has address 104.199.142.247
(... 21 other IPv4 hosts ...)
seed.bitcoin.sipa.be has address 150.140.188.181
seed.bitcoin.sipa.be has address 83.149.125.79
seed.bitcoin.sipa.be has IPv6 address 2001:0:9d38:6ab8:18c2:3a46:a1ec:987c
seed.bitcoin.sipa.be has IPv6 address 2001:0:4137:9e76:24f9:302a:4d39:ee08
(... 11 other IPv6 hosts ...)
seed.bitcoin.sipa.be has IPv6 address 2001:0:9d38:90d7:3858:553f:92ce:18b8
seed.bitcoin.sipa.be has IPv6 address 2607:5300:204:40f1::
```

DNS seeds are **predictable** because of DNS Round-Robin!

Typology of possible attacks

- An attacker might:
  - Spoof some full nodes
  - Block some SPV requests
  - Spoof some SPV requests
  - Sniff some SPV requests
  - Block some SPV answers

- But spoofing full answers shouldn’t be possible because of transactions hash verification
- IMHO, most possible attacks are LAN attacks against SPV user or full Bitcoin node

Local network (LAN) attacks

- If the attacker is on the same local network as the victim:
  - Prevent any (full or light) node from working (denial of service)
  - Spoof any node request/response
  - Spoof any unprotected request (HTTP) to a Bitcoin explorer API or web site

Local network (LAN) attacks

- A lot of techniques can be used:
  - ARP cache spoofing/poisoning
  - DNS cache spoofing/poisoning
  - DHCP spoofing
  - ICMP redirect
  - MAC flooding

Privacy issues

- SPV queries can be quite easily sniffed
- An attacker might associate user IP address, submitted Bloom filters and downloaded transactions to know all addresses of a given user
- See “On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients” (by Gervais et al.): https://eprint.iacr.org/2014/763.pdf

Summary of possible impacts

- An attacker can:
  - Known (nearly) all victim’s Bitcoin addresses (or a superset of them)
  - Associate user IP, addresses, and owner together
  - Prevent the user to use SPV by blocking the network (denial of service)
  - Prevent any outgoing transaction from being broadcasted
    → the victim cannot spend bitcoins
  - Prevent any ingoing transaction from being seen
    → the victim cannot see earnings/incoming transactions
  - Spoof unprotected requests to API/web sites
    → create arbitrary fake transactions

My recommendations about SPV

- To make an attack more difficult:
  - Use a VPN, or better a VPN connection to your own full Bitcoin node
  - Don’t directly use hardcoded nodes or DNS seeds (but use their direct or indirect neighbors)
  - Don’t use a precise Bloom filter
  - Cross-check with requests to a clean blockchain explorer API (HTTPS only, public CA, use of CRL) : tx count, balance, ...

Thank you!

follow me on twitter

@nono2357

Any questions?

BTC: 1GfztUeyrt3ewxdCHXNr58SPaidUrswoJj