Privacy at the communication layer

CS-721

Tor: The Second-Generation Onion Router
Roger Dingledine, Nick Mathewson, 2004

Carmela Troncoso
http://carmelatroncoso.com/
Tor directory servers

Directory
TOR
Relays

TorProject.org
Tor directory servers

10 directory servers
Tor Directory Servers

10 Directory Servers

Directory
Tor
Relays

Alice

Bob

Directory Authorities

MORH - 128.308.3.25:3 - RELAY AUTHORITY
TORS - 86.54.24.21:3 - RELAY AUTHORITY
D2UM - 41.172.105.8:3 - RELAY AUTHORITY
TONSA - 88.94.34.23:3 - BROCE AUTHORITY
GABBEL - 121.188.40.99 - RELAY AUTHORITY
DANNEBERG - 193.232.44.244 - RELAY AUTHORITY
URRAS - 208.82.223.34 - RELAY AUTHORITY
MATAUSKA - 192.25.99.9 - RELAY AUTHORITY
FARVAKHAR - 191.30.175.223 - RELAY AUTHORITY
LONGCLAW - 19.254.238.52 - RELAY AUTHORITY
Tor directory servers

Every hour:

- DAs compile a list of all known relays & flags & stuff
- DAs submits this “status-vote” to all the other authorities (DAs collect missing)
- DAs cobine parameters, sign and send to the other DA’s

- There **should** be a majority agreeing on the data -> **consensus**

- **Consensus** published by each DA
Tor Directory Servers

Every hour:

- DAs compile a list of all known relays & flags & stuff
- DAs submits this “status-vote” to all the other authorities (DAs collect missing)
- DAs combine parameters, sign and send to the other DA’s

- There **should** be a majority agreeing on the data → **Consensus**

- **Consensus** published by each DA

https://metrics.torproject.org/collector.html
But can Block Tor!

The Tor Network

Anonymous???
But *can block Tor!*

**Directory**

tor ALL Relays

Alice

Bob

The Tor Network

Tor

TorProject.org
But can Block Tor!

Choice is local!

The Tor Network

Directory

tor ALL
Relays
But can Block Tor!

Directory

Tor ALL Relays

Private information retrieval!

Choice is local!

The Tor Network

Alice

Bob
But can Block Tor!

Directory

tor
ALL
Relays

Private information retrieval!
(SCALABILITY COULD BE A PROBLEM)

Choice is local!

The Tor Network

TorProject.org
But **can Block Tor!**

“Lack of deniability”

**THE TOR NETWORK**

**Lack of deniability**
But *can block Tor!*
But CAN BLOCK Tor!

Directory
TOR
Relays

Alice

Relay

Relay

Relay

Relay

Bob

THE TOR NETWORK

Tor

TorProject.org
Censorship circumvention - Bridges

IPs not publicly available
Censorship circumvention – finding Bridges

BridgeDB

web
email

Bridge IP

Alice

Relay

Relay

Relay

Bob
Censorship circumvention – finding Bridges

BridgeDB

web
email

Bridge IP

default

Alice

Bob

Relay

Relay

Relay

Bridge
Censorship circumvention – finding Bridges

BridgeDB

web
email

Bridge IP

Alice

Relay

Private bridges

default

Bob
Censorship circumvention – finding Bridges

IPs not publicly available
Censorship circumvention – finding Bridges

IPs not publicly available

Can we find or enumerate?
Censorship circumvention – finding Bridges

Alice

IPs not publicly available

Can we find or enumerate?

Bob
Censorship circumvention – finding Bridges

Can we find or enumerate?

IPs not publicly available

Can we find or enumerate?
Censorship circumvention – finding Bridges

Directory for ALL Relays

Alice

Bridge

Relay

Relay

IPs not publicly available

Can we find or enumerate?
Censorship circumvention – finding Bridges

Can we find or enumerate?

IPs not publicly available

Can we find or enumerate?
We exploit...

Two issues known to Tor project since October 2010

1. *Vanilla Tor Certificates*
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won’t be fixed
We exploit...

Two issues known to Tor project since October 2010

1. Vanilla Tor Certificates
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won’t be fixed

2. Open OR Port
   - Bridges have open OR Port with Vanilla Tor
   - Even if they do not offer Vanilla Tor
   - Difficult to fix
We exploit...

1. Vanilla Tor or Certificates
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won't be fixed

2. Open OR Port
   - Bridges have open OR Port with Vanilla Tor
   - Even if they do not offer Vanilla Tor
   - Difficult to fix

Two issues known to Tor project since October 2010

Why don’t we scan all IPs with TLS to find bridges?
We exploit...

1. Vanilla T or Certificates
   - Vanilla T or uses TLS handshake
   - Easy to spot certificates
   - It won't be fixed

2. Open OR Port
   - Bridges have open OR Port with Vanilla Tor
   - Even if they do not offer Vanilla Tor
   - Difficult to fix

Two issues known to Tor project since October 2010

Why don’t we scan all IPs with TLS to find bridges?
We exploit...

1. Vanilla Tor or Certificates
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won't be fixed

2. Open OR Port
   - Bridges have open OR Port with Vanilla Tor
   - Even if they do not offer Vanilla Tor
   - Difficult to fix

Two issues known to Tor project since October 2010

Why don't we scan all IPs with TLS to find bridges?
We use three datasets

**SHODAN**
- Scan 200+ ports with multiple protocols
- 19 ports scanned with TLS
- Indexed data available

**Censys**
- Scan 6 ports with TLS
- Raw + indexed data available
We use three datasets

**SHODAN**
Scan 200+ ports with multiple protocols
19 ports scanned with TLS
Indexed data available

**censys**
Scan 6 ports with TLS
Raw + indexed data available

**Identify candidate bridge IPs**
*(without scanning ourselves!!)*
We use three datasets

**SHODAN**
- Scan 200+ ports with multiple protocols
- 19 ports scanned with TLS
- Indexed data available

**censys**
- Scan 6 ports with TLS
- Raw + indexed data available

**COLLECTor**
- Node-level data on public bridges + relays
- Some bridge data sanitized

*Identify candidate bridge IPs*
*(without scanning ourselves!!)*
We use three datasets:

- **SHODAN**
  - Scan 200+ ports with multiple protocols
  - 19 ports scanned with TLS
  - Indexed data available

- **censys**
  - Scan 6 ports with TLS
  - Raw + indexed data available

- **COLLECTOR**
  - Node-level data on public bridges + relays
  - Some bridge data sanitized

Identify candidate bridge IPs
(without scanning ourselves!!)
Bridge discovery approach
Bridge discovery approach

1. Finding candidate IP addresses
2.
Bridge discovery approach

1. Finding candidate IP addresses
2. Filtering relays
3.
1. Finding candidate IP addresses
2. Filtering relays
3. Verifying IP addresses
Bridge discovery approach

1. Finding candidate IP addresses
2. Filtering relays
3. Verifying IP addresses
4. Identifying private proxies
   - (check descriptor)
5.
Bridge discovery approach

1. Finding candidate IP addresses
2. Filtering relays
3. Verifying IP addresses
4. Identifying private proxies
   - (check descriptor)
5. Classifying as public or private bridge
   - (find sanitized fingerprint)
April 2016:

- 5.3K active public bridges
- 2.3K bridges with clients
Tor Hidden services

DB

IP1

IP2

IP3

XYZ.onion
Tor Hidden services

IP1

IP2

IP3

DB

XYZ.onion
Tor Hidden services

DB

\[ \text{Sig}(\text{IP}_1, \text{IP}_2, \text{IP}_3) \]

XYZ.onion
Tor Hidden services

XYZ.onion?

DB

IP₁

IP₂

IP₃

XYZ.onion
TOR HIDDEN SERVICES

XYZ.onion?

DB

IP1

IP2

IP3

RV

XYZ.onion
Tor Hidden services

Sig(IP1, IP2, IP3)

DB

IP1

IP2

IP3

RV

XYZ.onion
Tor Hidden services

![Diagram of Tor network with IP addresses and a database.]
Locating Tor Hidden services
Locating Tor Hidden services

丹

IP1

IP2

IP3

RV

XYZ.onion
Locating Tor Hidden services

- DB
- IP1
- IP2
- IP3
- XYZ.onion
- RV

Diagram: A database (DB) connects to multiple nodes represented by onions. IP1, IP2, and IP3 are highlighted, with IP3 leading to XYZ.onion. RV is connected to another node, indicating a path to locate the hidden service.
Tor Hidden services

DHT - Distributed Hash Table

DB

HSDir_{n}

HSDir_{k+1}

HSDir_{k+2}

HSDir_{k+3}

HSDir_{k-1}

HSDir_{1}

Desc ID

stuff

cookie
time

STUFF
Set up an HSDir and log all hidden service descriptors published to their node. (profile client requests)

Predictable descriptor ID’s & HSDir controlled => DoS particular HS

Tor Hidden Services

DHT – Distributed Hash Table

HSDir₁ HSDirₖ−₁

HSDirₙ HSDirₖ+₁

HSDirₖ+₂

HSDirₖ+₃

Desc ID

cookie

time

STUFF
Set up an HSDir and log all hidden service descriptors published to their node. (profile client requests)

Predictable descriptor ID’s & HSDir controlled => DoS particular HS
Honions – detecting malicious HDdirs

not advertised
no functionality
CASCADE vs. FREE ROUTES
CASCADE VS. FREE ROUTES

No choice for users

Full flexibility
CASCADE VS. FREE ROUTES

Partitioned anonymity sets
CASCADE vs. FREE routes

Partitioned anonymity sets

and here?
What is tor?

Senders

Receivers

Senders

Receivers

and here?
What is Tor?

Senders

Receivers

Senders

Receivers
What is Tor?

Senders

Stratified

Receivers
Are there more options?

Source based vs. non-source routing

Next week
Crowds: Anonymity for Web Transactions
**Key takeaways**

**Anonymity is hard**
not only need users... too many variables

**Peer-oriented is problematic** – cannot check identities
Malicious nodes can infiltrate (HS, Bridges, full anonymity)

**Different Routing options = properties** – more next week 😊