Analyzing the Great Firewall of China Over Space and Time

Roya Ensafi, Philipp Winter, Abdullah Mueen, Jed Crandall
June 30, 2015
The Battle Over Information Control On The Internet
State of the Art

- Rent a **control** machine (VPS)
- **Cooperate** with volunteers

**Advantages**
- Root access

**Disadvantages**
- Not always possible to rent VPS in interesting area
- Expensive
- Could put volunteers in danger
Motivation

- We can't have access to all machines
- Machines follow RFC rules plus OS implementation
- Can we come up with ways to use them to measure FROM?
Side channels turn ordinary machines into vantage points!

- Advantages
  - No root access required
  - No need for special software on any machine

- Disadvantages
  - Limited to TCP/IP layer
Analyzing the GFW Over Space & Time

- Country-wide distributed NIDS
- Surprisingly sophisticated
  - Deep packet inspection
  - Active probing for unknown protocols
- Blocks Tor relays by dropping packets of **TCP handshake**
Outline

- Discuss idle scans, a special kind of side channel
- Explain practical idle scans
- Use practical idle scans to provide a better understanding of the Great Firewall (GFW)
Hybrid Idle Scan

Idle port scanning uses side channel techniques to bounce scans off of a “server” host to stealthily scan a “client”.

Hybrid idle scans (spooky scans) can detect the direction of blocking between a client and server. It is simple, effective, and unobtrusive. (Ensafi, et al. PAM’14)

Requirements:
- Global IPIID machine for the client
- Server that has open port
No direction blocked

SYN Backlog
0

Server

Client

Client IPID: 1000

(1) SYN/ACK

(2) IPID: 1000

MM

Hybrid Idle Scan
No direction blocked

SYN Backlog
0

Server

Client

MM

(1) SYN/ACK
(2) IPID: 1000
(3) Spoof SYN

Client IPID: 1000
No direction blocked

1. SYN/ACK

2. IPID: 1000

3. Spoof SYN

4. SYN/ACK

5. RST, IPID: 1001

Client IPID:

1000

1001

SYN Backlog

0

1

0
Hybrid Idle Scan

No direction blocked

SYN Backlog
0
1
0

Client IPID:
1000
1001
1002
Hybrid Idle Scan

Server to Client Blocked

SYN Backlog
0
1

Server

Client

MM

(1) SYN/ACK

(2) IPID: 1000

(3) Spoof SYN

(4) SYN/ACK

(5)

(6) SYN/ACK

(7) IPID: 1001

Client IPID:
1000
1001
Hybrid Idle Scan

Server to Client Blocked

- SYN Backlog: 0
- Client IPID: 1000
- Client IPID: 1001

Client to Server Blocked

- SYN Backlog: 0
- Client IPID: 1000
- Client IPID: 1004
What Did We Want to Learn?

● Many open questions about the GFW and Tor
  ○ Does censorship of Tor differ for users in different regions?
  ○ Does filtering depend on **when and where** you are?
  ○ How good is the GFW at blocking Tor?
  ○ Is it always Server-to-Client blocking or also Client-to-Server blocking?
  ○ Does blocking change from one ISP to another?

● Revisit old beliefs about the GFW
  ○ Is filtering **centralized**?
Methodology - Relays and Clients
We ran hybrid idle scans for 27 days.

Each pair of clients and servers were tested hourly for a day.
Results: No Obvious Geographical Pattern

No geographical or topological pattern is visible. Instead, the distribution matches the geographic Internet penetration patterns of China.
Analyzing the GFW Over Space & Time

- Mostly **Server-to-Client Blocking**
- **SYN/ACK dropping** (IP and port)
- If **RST passes** through GFW, then **SYN also will**
- CERNET clients could **more often communicate** with servers throughout the day
- Some relays were **always reachable** throughout the day

<table>
<thead>
<tr>
<th>Client Interest, Server Source</th>
<th>$S \rightarrow C$ (Count, %)</th>
<th>None (Count, %)</th>
<th>$C \rightarrow S$ (Count, %)</th>
<th>Error (Count, %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN Tor-Relay</td>
<td>116,460 (81.52)</td>
<td>555 (0.39)</td>
<td>786 (0.55)</td>
<td>25,061 (17.54)</td>
</tr>
<tr>
<td>CN Tor-Dir</td>
<td>8,922 (64.91)</td>
<td>31 (0.23)</td>
<td>2,696 (19.61)</td>
<td>2,097 (15.25)</td>
</tr>
</tbody>
</table>
Analyzing the GFW Over Space & Time

- Mostly **Server-to-Client Blocking**
- **SYN/ACK dropping** (IP and port)
- If **RST passes** through GFW, then **SYN also will**
- CERNET clients could **more often communicate** with servers throughout the day
- Some relays were **always reachable** throughout the day

<table>
<thead>
<tr>
<th>Client, Server</th>
<th>$S \to C$ (%)</th>
<th>None (%)</th>
<th>$C \to S$ (%)</th>
<th>Error (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN Tor–Relay</td>
<td>116,460 (81.52)</td>
<td>555 (0.39)</td>
<td>786 (0.55)</td>
<td>25,061 (17.54)</td>
</tr>
<tr>
<td>CN Tor–Dir</td>
<td>8,922 (64.91)</td>
<td>31 (0.23)</td>
<td>2,696 (19.61)</td>
<td>2,097 (15.25)</td>
</tr>
</tbody>
</table>
Take Away Messages

- Side channels **practical** and enable **broad coverage**
- ...but **not flexible** and **care** must be taken when used
- CERNET **treated differently** than rest of country
- Filtering **centralized**, and **quite effective**
Questions / Comments?

Thank You!
Ethical Considerations

- **Want to learn if two remote hosts can talk to each other**
  - Different approaches have different issues
  - Rented VPS could cause trouble for VPS provider

- **Deciding if a given measurement is ethical on a case-to-case basis**
  - Technique perfectly fine in situation X ...
  - … but irresponsible in situation Y

- **Mitigations**
  - Use routers instead of clients
  - Measure an entire (e.g) /24
Real Data

Phase 1: just query IPID
Phase 2: send 5 spoofed SYN packets per sec & query IPID for 120 sec

Server to client blocked
No direction blocked
Client to server blocked
Censored Planet

Use practical idle scans to **provide a framework to globally measure censorship**
The Great Firewall's Active Probing

- Ran measurements and analyzed initial data:
  - 3 JavaScript-implemented Tor relays are accessible almost always

- Evidence of Active probing for Tor relays
  - Every 24+ h, GFW flushes blocked IPs

- Evidence of IP spoofing
  - GFW owns at least 248 netblocks that are used to spoof IPs