SbuSocks: Break the Great Firewall

CSE534 Project

Xuan Li, Caitao Zhan, Runxiang Huang

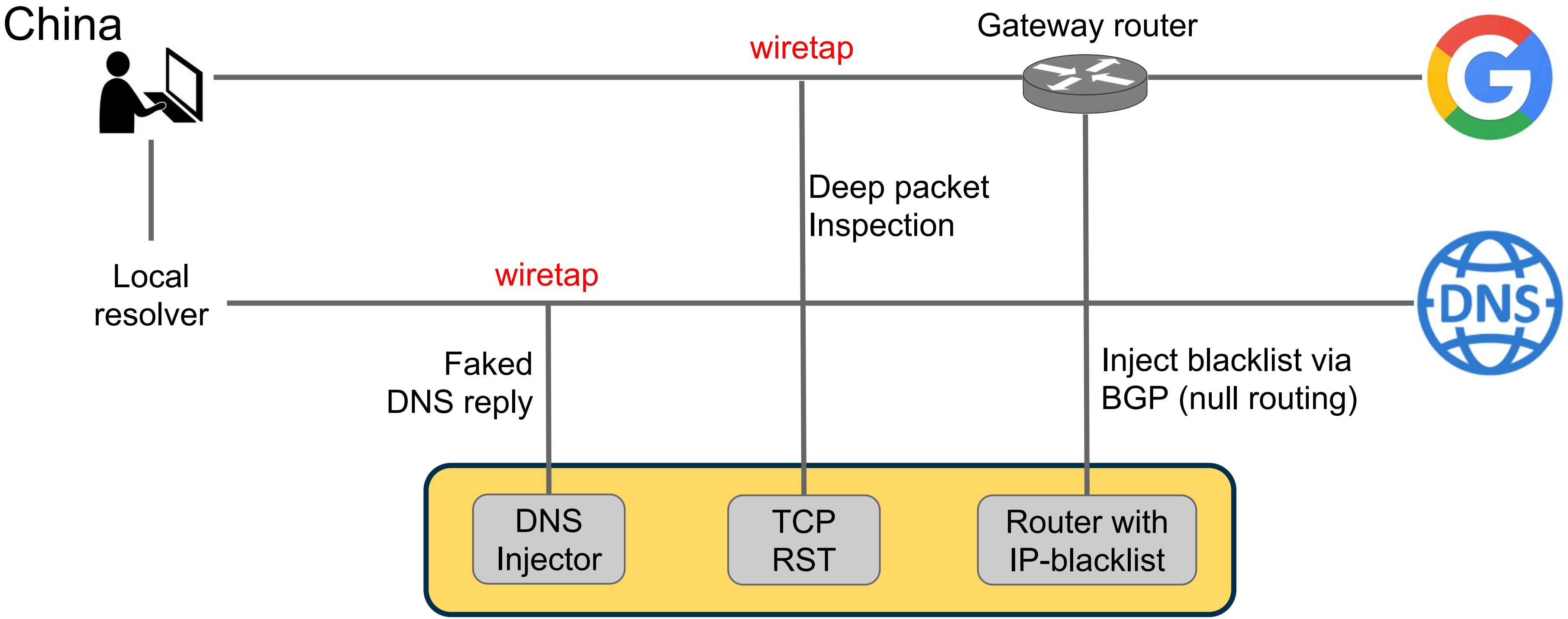
Computer Science Department

May10, 2018

Table of Contents

1. Introduce GFW
2. What we did to break GFW
3. Experiments and take-away messages

GFW: world's largest firewall
So… How does it work?



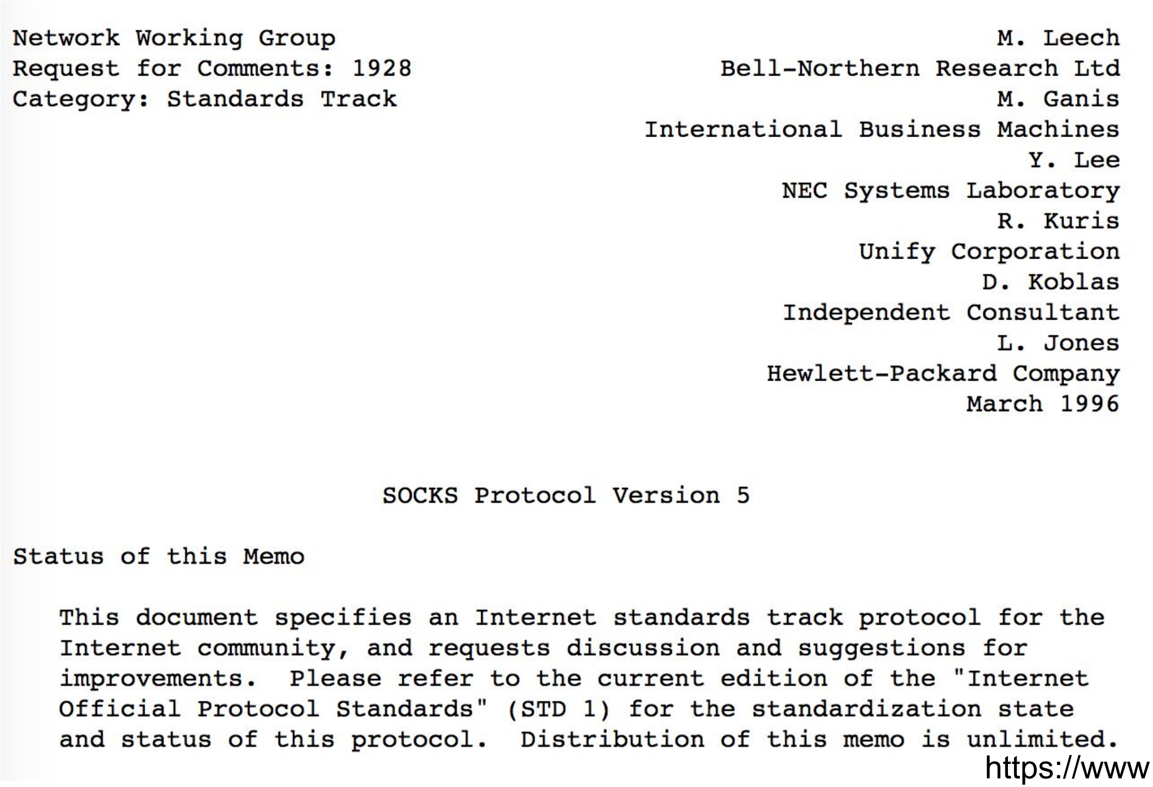
GFW is at international gateways and province-level ISP

Take-away Message

- The basic methodology for breaking the GFW is to find some **proxy** nodes and **encrypt** the traffic.

- We implemented a tool namely ***SbuSocks***, which successfully breaks GFW following the methodology.

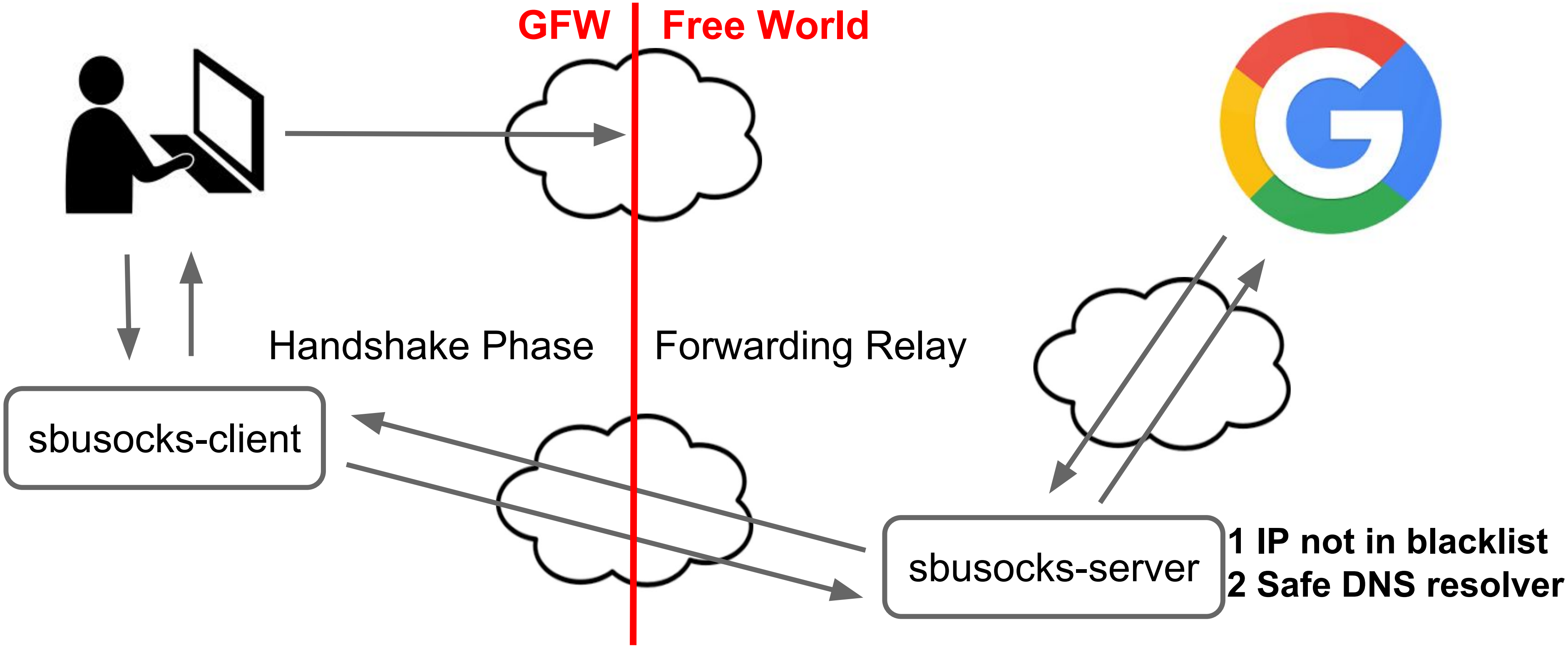
Socks5 (RFC 1928)



```
Network Working Group                                           M. Leech
Request for Comments: 1928                    Bell-Northern Research Ltd
Category: Standards Track                                       M. Ganis
                                         International Business Machines
                                                                  Y. Lee
                                                  NEC Systems Laboratory
                                                                R. Kuris
                                                       Unify Corporation
                                                               D. Koblas
                                                  Independent Consultant
                                                               L. Jones
                                                 Hewlett-Packard Company
                                                              March 1996


                        SOCKS Protocol Version 5

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.
```

https://www.ietf.org/rfc/rfc1928.txt

Socks 5: Handshake + Forwarding Relay



1 IP not in blacklist
2 Safe DNS resolver

Socks5 Protocol

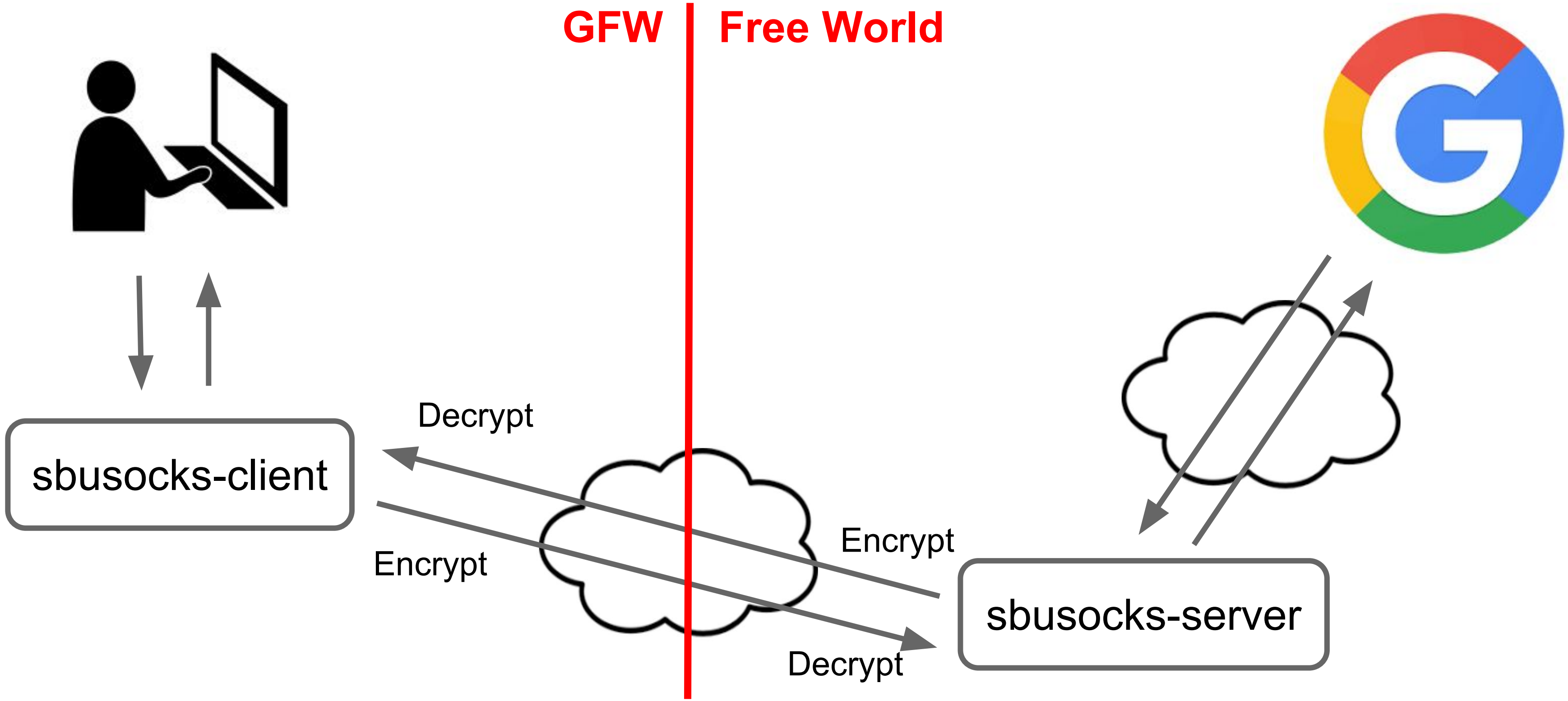
~~IP blacklist~~

~~DNS injection~~

But… How to deal with evil deep packet inspection (DPI) with TCP RST attack?

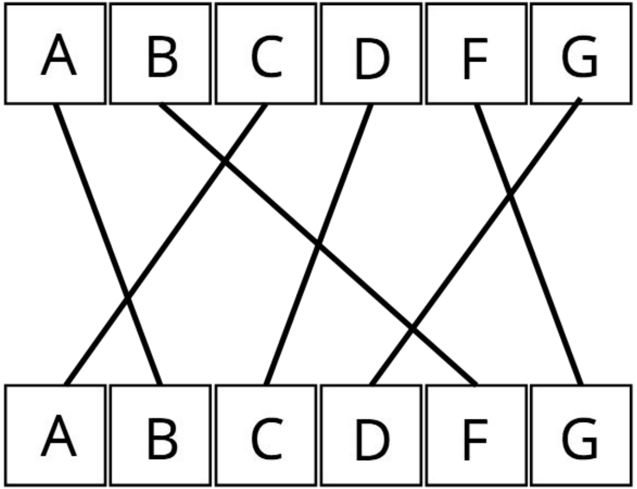
Encryption to the rescue!

Encryption: Obfuscate the DPI



SbuSocks Use: Classic Cryptography

1. Use out-of-band key to set a random state.
2. Use a permutation cipher based on the random state.



```
b'You cannot see me!'  -->  b'\xb0\xeaB\xde,cff\xea\xc7\xde\x8e\xf4\xf4\xde\x95\xf4x'
```

Introduce **SbuSocks**

SbuSocks = Socks 5 + Encryption

https://github.com/caitaozhan/CSE534-Project

Experiment: 8 People in 5 Cities across China

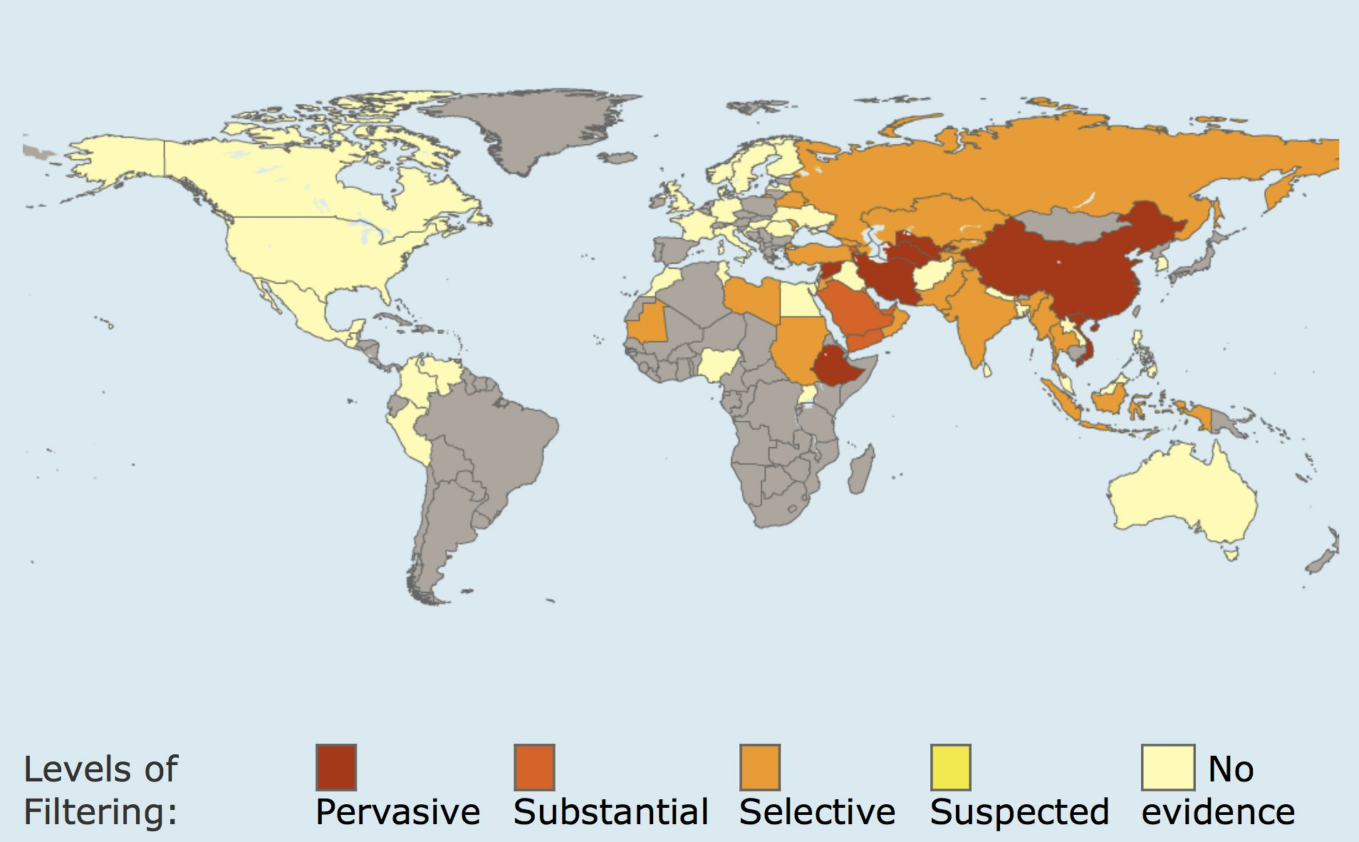
SbuSocks	Hypothesis	Test
Socks5+Encryption	Break GFW	Break GFW
Socks5	[✓ Blocked]	[✓ Break GFW]

More Take-away Messages

- GFW will **let** *very small scale suspicious traffic* **go**, due to economic reasons.

Thank you

Motivation



China

Ethiopia

Iran

Syria

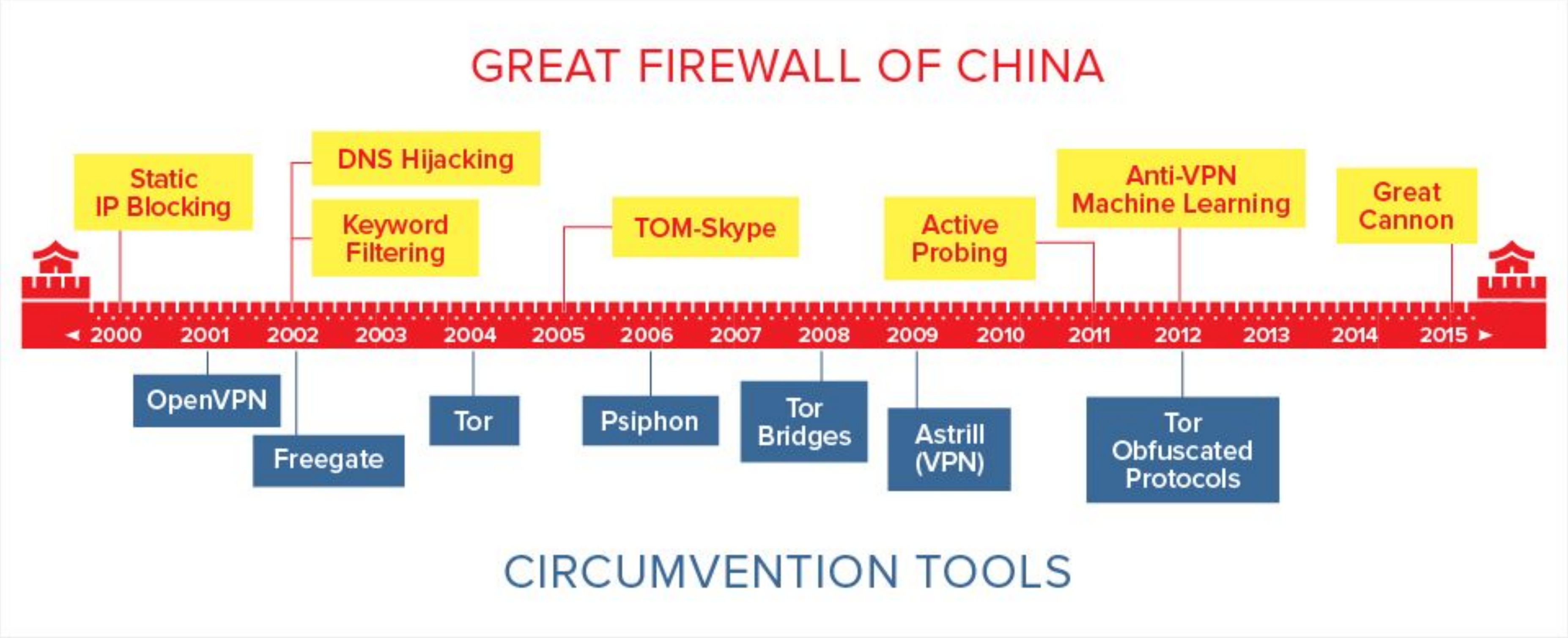
Turkmenistan

Uzbekistan

Vietnam

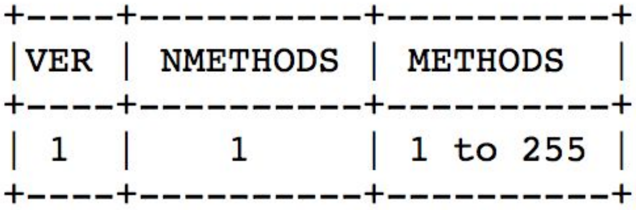
http://map.opennet.net/filtering-pol.html

Related Work: the arms race



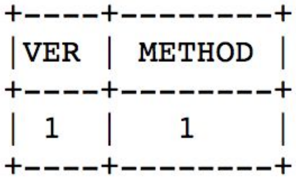
https://blog.thousandeyes.com/the-war-between-chinas-great-firewall-and-circumvention-tools/

Socks5 Protocol Handshake Details



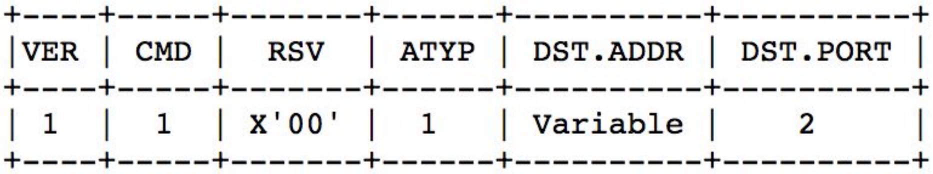
VER	NMETHODS	METHODS
1	1	1 to 255

1. Application → Client



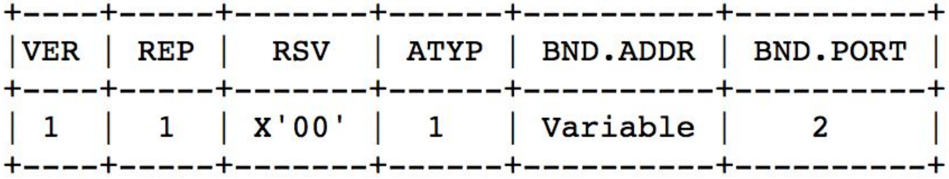
VER	METHOD
1	1

2. Client → Application



VER	CMD	RSV	ATYP	DST.ADDR	DST.PORT
1	1	X'00'	1	Variable	2

3. Client → Server



VER	REP	RSV	ATYP	BND.ADDR	BND.PORT
1	1	X'00'	1	Variable	2

4. Server → Client

Why Socks5

- Elusive.
- Easy to deploy.
- A lot of applications support socks5 protocol. We only need to implement the responding part.

More on Traffic Encryption Obfuscation

- ***Encryption is a method, the goal is <u>obfuscation</u>!***

- **Randomization**: randomize every byte in the packet payload.
- **Mimicry**: masquerade as a whitelisted protocol.
- **Tunneling**: Use a special protocol, such as VPN.

GFW’s New Weapons

1. Active Probing
2. Machine learning
3. DDos attack

The arms race goes on and on...

TCP Relay

Server

Forward streams from the client to the target destination

Forward responses from the target destinations to the client.

Client

Forward streams from the local applications to the server.

Forward streams from the server to local applications

Future Work: Detecting TCP RST Attack

- One major way GFW perform blocking is using TCP RST Attack.
- TCP RST Attack is triggered by keywords. Once GFW detect that the packet contain such keyword, it will send TCP RST to both end of the TCP connection.
- One way to solve this problem is to send an ACK to server/client after receive RST. If RST is send by client/server, then connection ends; if not, RST will be dropped.
- Current detecting system need both server and client implementation.