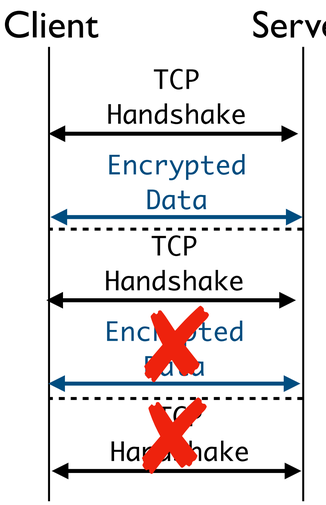
# How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic

Mingshi Wu, Jackson Sippe, Danesh Sivakumar, Jack Burg, Peter Anderson,
Xiaokang Wang, Kevin Bock, Amir Houmansadr, Dave Levin, Eric Wustrow

**Project Homepage**

## What happened?

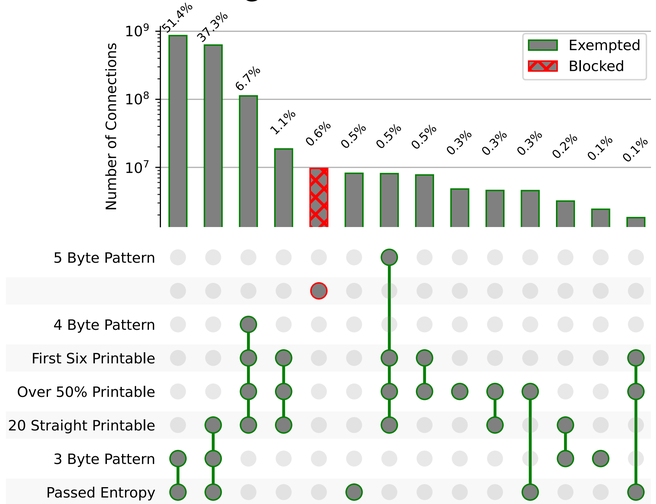



On November 6, 2021, the Great Firewall of China (GFW) started **dynamically blocking fully encrypted traffic in real time.** Such capability affected a large set of censorship circumvention protocols used by **tens of millions of users**.

**Fully encrypted proxies** encrypt all traffic including headers, while protocols like TLS send plaintext headers.

## Evaluating the Detection Algorithm

We simulated the traffic detection algorithm on a network tap at the University of Colorado Boulder. Our evaluation suggests that **the false positive rate of the detection algorithm is as low as 0.6%.**




## Reverse Engineering the GFW

We sent millions of experimental probes past the GFW to reverse engineer what was blocked. We find **five rules** that govern blocking.

**Fraction of `bits=1`**

49 fa e3 91 5c 83 — avg 4 bits/byte — BLOCKED

00 01 02 03 04 05 — avg 1.67 bits/byte — NOT BLOCKED

**Protocol Fingerprints**

f9 ab cd ef 9a 8d c1... — No Match — BLOCKED

GET␣/␣HTTP/1.1\r\n... — HTTP Matches — NOT BLOCKED

16 03 01 00 a5 01 00... — TLS Matches — NOT BLOCKED

Block the connection *unless any of the following hold*

- Fraction of `bits=1` ≤ 42.5% or ≥ 57.5%
- The first six bytes are printable ASCII
- >50% of bytes are printable ASCII
- 20 contiguous bytes are printable ASCII
- Matches the fingerprint for HTTP or TLS

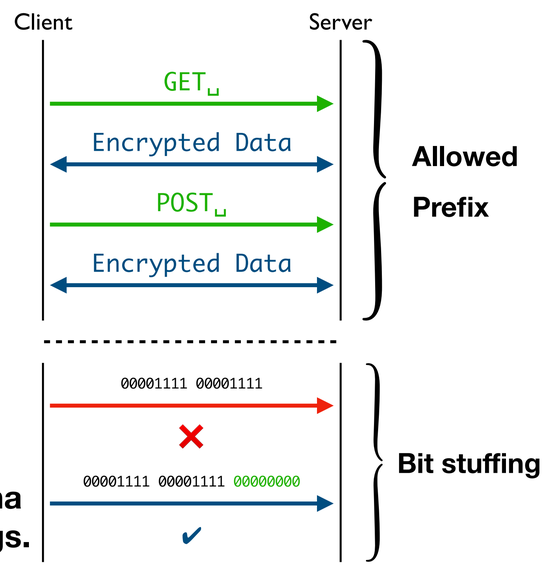
## Effective and Immediate Mitigations

**Patched Tools**

Lantern, Outline, shadowsocks, Psiphon, V2Ray (VMess)

Our research findings have been integrated into **all mainstream fully encrypted protocols.**

These mitigations have helped **tens of millions of users in China and Iran to bypass the blockings.**




## Response Timeline

- **Nov 6 '21** — **Blocking begins. We begin measurement**
- Nov 8-11 '21 — CCP central committee plenary session
- **Nov 16 '21** — **Our initial report**
- **Jan 13 '22** — **First mitigation released**
- Mar 13 '23 — Xi started his third term
- **Mar 15 '23** — **Blocking ends**

We took **immediate actions** to measure and understand the blocking. We **rapidly and responsibly** disclosed our research findings to both anti-censorship tool developers and the general public.

The blocking was likely **politically driven**, as it started 2 days before a major political convention and ended 2 days after the confirmation of Xi's third term.