An ISP-Scale Deployment of TapDance

Presented by Nikita Borisov (@nikitab)

https://refraction.network/
The 65 countries covered in Freedom on the Net represent 87 percent of the world's internet user population. Over 1.2 billion internet users, or forty percent of global users, live in three countries — China, India, and the United States — that span the spectrum of internet freedom environments, from Free to Not Free.
Internet Filtering

• Applies at many layers
  • DNS manipulation
  • BGP manipulation
  • DPI / content inspection
  • Packet filtering: IP/port
Cat-and-mouse game

- Censors **identify** and **block** proxies
- Circumventors **deploy** and **distribute** new proxies
- Advantage if proxies are:
  - Harder to find
  - Faster to deploy
  - Harder to block
  - Easier to distribute
**TapDance**: End-to-Middle Anticensorship without Flow Blocking
TapDance Protocol Overview

(TLS Handshake)

K

Tag

<Encrypted Incomplete HTTP Request>

<Encrypted TapDance Response>

<Encrypted Proxy Request (blocked.com)>

<Encrypted HTTP Response (blocked.com HTML)>

K
Incomplete HTTP request example

GET / HTTP/1.1
Host: www.site.com
X-Ignore: u]DhsYGxVxEvuZEHESra...
Incomplete HTTP request example
\x1e\x91\xb2\xce\x94\x8a\x6b\x3c\x78\x8c\x6f\x03\x5e\xef\x97\x34\xf1\x2e\xc6\xe6\x7f\x10\xc8\x46\xf9\x25\x6a\x0c\xff\x6d\x38 ... \x70\xd7\x2c\x63 ...

Decrypt
Shared Secret: ; Client random: ...
Figure 3: TapDance Overview — (1) The client performs a normal TLS handshake with an unblocked decoy server, establishing a session key $K$. (2) The client sends an incomplete HTTP request through the connection and encodes a steganographic tag in the ciphertext of the request, using a novel encoding scheme (Section 4.2). (3) The TapDance station observes and extracts the client's tag, and recovers the client-server session secret $K$. (4) The server sends a TCP ACK message in response to the incomplete HTTP request and waits for the request to be completed or until it times out. (5) The station, meanwhile, spoofs a response to the client from the decoy server. This message is encrypted under $K$ and indicates the station's presence to the client. (6) The client sends a TCP ACK (for the spoofed data) and its real request (blocked.com). The server ignores both of these, because the TCP acknowledgment field is higher than the server's TCP SND.NXT. (7) The TapDance station sends back the requested page (blocked.com) as a spoofed response from the server. (8) When finished, the client and TapDance station simulate a standard TCP/TLS authenticated shutdown, which is again ignored by the true server. (9) After the connection is terminated by the client, the TapDance station sends a TCP RST packet that is valid for the server's SND.NXT, silently closing its end of the connection before its timeout expires.
TapDance Trial Deployment

• Worked with two mid-size ISPs:

  - 10 (or 40)-Gbps Mirror
  - Management interface

  TapDance station
  1U server w/
  4x10Gbps Intel X710 NIC
University of Colorado Network

Upstream

Science network

Campus network

Bro Cluster

10 Gbps Mirror

Management interface

TapDance station
Reachable site discovery

AS 237
AS 104

<List of trusted TLS sites>

Timeout
TCP window

<List of sites that meet timeout/window thresholds>

TapDance Client

~900 reachable sites

<List of TapDance-compatible reachable sites>
TapDance client

- 100% in Go
- Partnered with Psiphon
  - Integrated TapDance in Psiphon’s Android app
  - Deployed to ~70K users in censored countries via remote update
Total traffic
Detectability

• A TapDance connection looks *different* from regular web browsing
  – DNS request
  – Connection scheduling
  – TLS negotiation (ClientHello, SNI)
  – HTTP request sizes
Detectability

• A TapDance connection looks *different* from regular web browsing
  – DNS request
    • DoH/DoT
  – Connection scheduling
    • QUIC / ORIGIN Frame
  – TLS negotiation (ClientHello, SNI)
    • Encrypted SNI
  – HTTP request/response sizes
    • HTTP/2 PUSH
Detectability

• A TapDance connection looks different from regular web browsing
  – DNS request
    • DoH/DoT
  – Connection scheduling
    • QUIC/ORIGIN Frame
  – TLS negotiation (ClientHello, SNI)
    • Encrypted SNI
  – HTTP request/response sizes
    • HTTP/2 PUSH

Privacy from network observers makes censorship harder!
Looking for new ISP partners!

An ISP-Scale Deployment of TapDance

https://refraction.network/