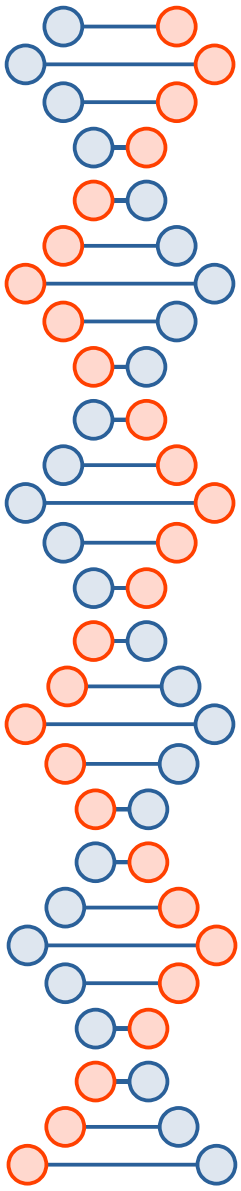
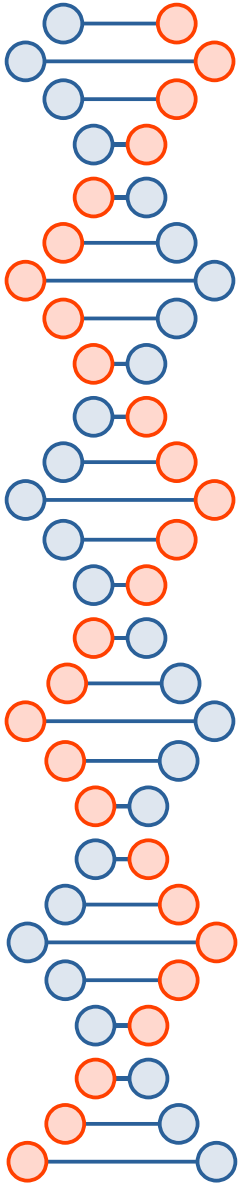


DPI of encrypted traffic

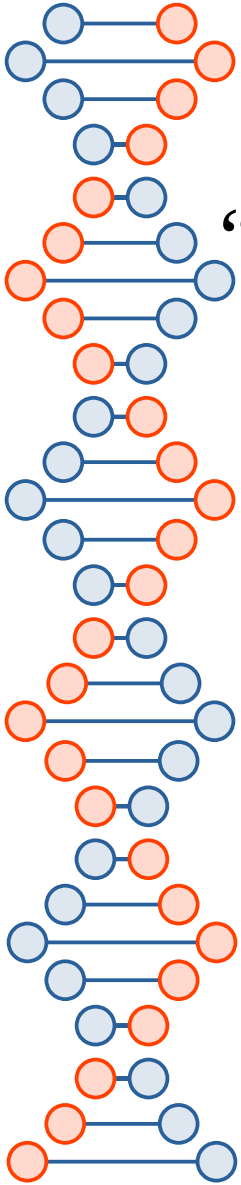
CSE 548 Spring 2025

jedimaestro@asu.edu



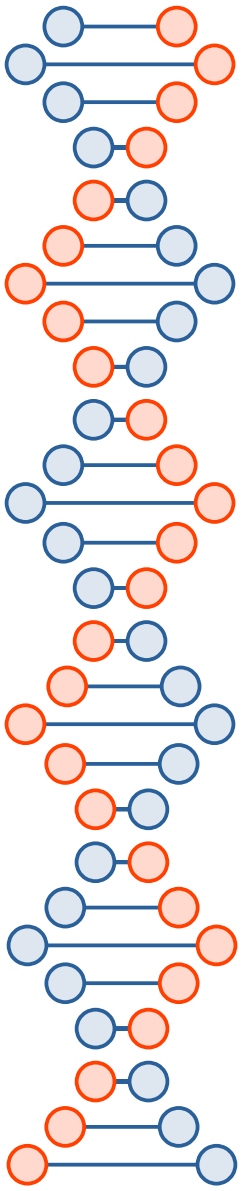
“Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect.”

— Bruce Schneier (2009). *Schneier on Security*, p. 69, John Wiley & Sons.



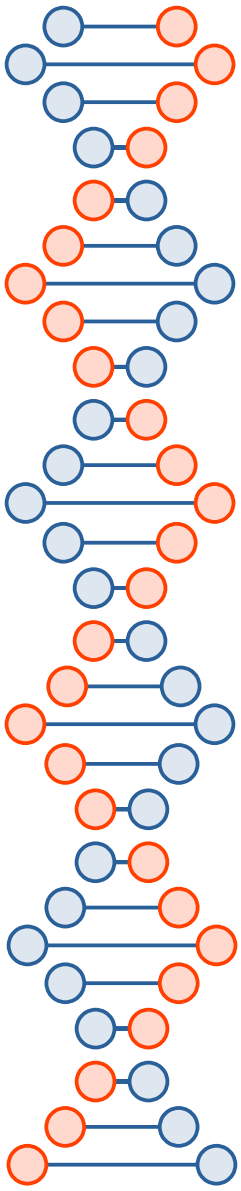
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

— United Nations Universal Declaration of Human Rights, Article 12.



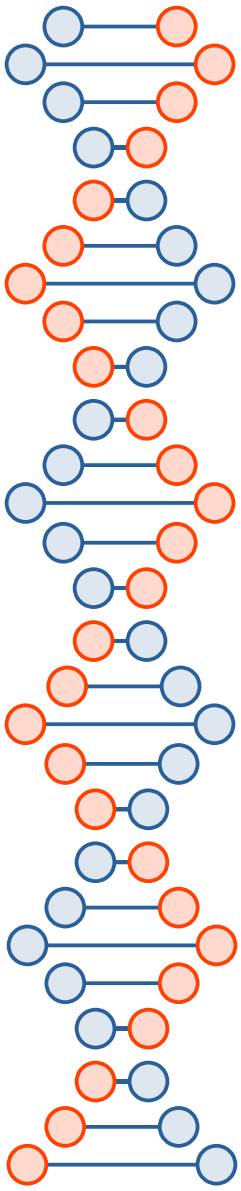
Crypto Wars and related events

- Phil Zimmerman and PGP, crypto exports
  - https://en.wikipedia.org/wiki/Pretty_Good_Privacy#Criminal_investigation
  - https://en.wikipedia.org/wiki/Bernstein_v._United_States
- Operation Sundevil
  - https://www.cybereason.com/blog/malicious-life-podcast-operation-sundevil-and-the-birth-of-the-eff
  - https://www.eff.org/pages/mitch-kapor-john-barlow-interview
- Clipper Chip (Clinton administration)
  - https://www.mattblaze.org/papers/eesproto.pdf



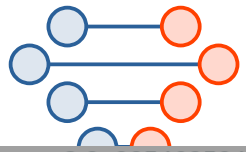
What were the Crypto Wars about?

- In the context of this talk:
  - Fears that government restrictions would weaken the ability of individuals to use strong cryptography for private communications.
  - Fears that simply having or using specific software would be criminalized.



Current state of affairs

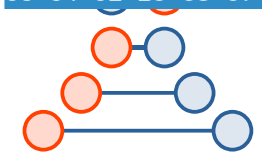
- U.S. and “the West” – Crypto wars are now about platforms and apps, *e.g.*, EARN IT Act, Tik Tok bans, end-to-end messaging apps
  - https://en.wikipedia.org/wiki/EARN_IT_Act
  - https://en.wikipedia.org/wiki/Restrictions_on_TikTok_in_the_United_States
  - https://en.wikipedia.org/wiki/Blocking_of_Twitter_in_Brazil#Blocking
  - https://www.reuters.com/technology/uk-us-hold-private-talks-resolve-apple-encryption-order-bloomberg-news-reports-2025-03-13/
- China – Encryption allowed, restricted by SNI (Server Name Indicator, *i.e.*, platforms and apps)
  - https://gfw.report/publications/usenixsecurity23/en/
- Russia – Also SNI-based censorship, and the government is a trusted certificate authority
  - https://diwenx.com/assets/files/tspu-imc22.pdf
  - https://keep.lib.asu.edu/items/193350

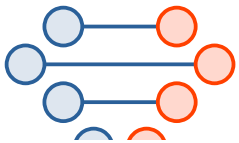


3	0.005462504	10.155.30.179	18.205.53.136	TCP	74	40186 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS
8	0.067175913	18.205.53.136	10.155.30.179	TCP	74	443 → 40186 [SYN, ACK] Seq=0 Ack=1 Win=2684
24	0.195979757	10.155.30.179	18.205.53.136	TLSv1.2	104	Application Data
26	0.196261196	18.205.53.136	10.155.30.179	TLSv1.2	104	Application Data
28	0.196849481	10.155.30.179	18.205.53.136	TLSv1.2	108	Application Data
22	0.195647004	18.205.53.136	10.155.30.179	TLSv1.2	144	Application Data
18	0.134217638	10.155.30.179	18.205.53.136	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, En
21	0.195646933	18.205.53.136	10.155.30.179	TLSv1.2	270	New Session Ticket, Change Cipher Spec, Enc
25	0.196261086	18.205.53.136	10.155.30.179	TLSv1.2	352	Application Data
11	0.067795926	10.155.30.179	18.205.53.136	TLSv1.2	624	Client Hello
19	0.134536166	10.155.30.179	18.205.53.136	TLSv1.2	656	Application Data, Application Data
10	0.067787461	10.155.30.179	18.205.53.136	TCP	1264	40186 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len
14	0.131083829	18.205.53.136	10.155.30.179	TLSv1.2	1264	Server Hello
16	0.131154339	18.205.53.136	10.155.30.179	TLSv1.2	3202	Certificate, Server Key Exchange, Server He

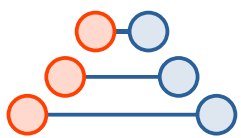
```
▾ Extension: server_name (len=19)
    Type: server_name (0)
    Length: 19
  ▾ Server Name Indication extension
      Server Name list length: 17
      Server Name Type: host_name (0)
      Server Name length: 14
      Server Name: boredpanda.com
▾ Extension: Reserved (GREASE) (len=1)
```

```
70  59 7f 51 d5 11 9b ec 81  33 ba 62 5b f0 d5 54 35   Y·Q····· 3·b[··T5
80  80 24 34 4c 3f 3f e7 42  99 35 fd 08 01 f3 77 db   ·$4L??·B ·5····w·
90  3d 46 d2 b5 96 ce cf c5  45 e9 e2 2b 00 1d 00 20   =F····· E··+··· 
a0  d2 2c b8 f7 90 4f 37 6b  36 5a 09 32 ab 9a d7 52   ·,···O7k 6Z·2···R
b0  f7 30 d3 a5 f7 a0 60 3a  e4 0f a1 e2 3d e6 d5 61   ·0····`: ····=··a
c0  00 00 00 13 00 11 00 00  0e 62 6f 72 65 64 70 61   ········ ·boredpa
d0  6e 64 61 2e 63 6f 6d 1a  1a 00 01 00              nda.com· ····
```





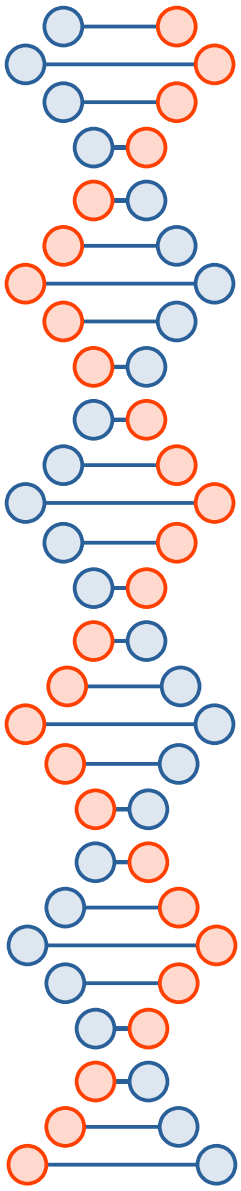
...
zz.....#...3....zz.....A.. t....I...
...\.?n..Sy.nTo.z.2..L..#t...>.P+....d%%..2Ar....q..Q.Tx?...\.....g...$e..A...O.k.RE..%
.....wg..r../1....T.kq.....0x$..x....."e .).s(F.
...dw\.*....hH.+v....FY.I.2.....[..J.2.3.I.|.@s.Ie..8..76]...$".U...?..Cr.H..o..&.(...{.t...
....c..k1.,qM.....Y.Ch.6...I."......$.q.....M5..ZWM.\.bKEJo.4^.....+..8.....AQ....Av.p..@.....&....d=..Y..E..c.Y...y..y.wNbd:.....:+1.+7a`
{.....+...:..P2.k..LOc...(f.8.QR/X.A.U;c.],'...._..T
.1.Fv.M. ..e...X .'8X.....y..v9.....zWF.....L..1cy"...%..HY>...#.iC..+$#0.$..+....@.[.....>...4,X.r.....Sq.f....\%"x
....7Z.w;...o..q.....u.z./..,.F..WY8.....+.^"%G#k...{..U".j..M.....49..2x cng1.P..v..".J..V$6.I:Aq...v.x
c.I...&..-..`..t..@A..M..?!m;C..|r.EF....)W....j..2..V..-....&....M.,.K..F..4R.5..{z....G.tQ..z...M#:%.e...B....K+A"B.....&....W]"...)...ru....A{.1syn..1.
\i..P.`j2T.'..w....8.\.V0..[C...t..I..C}..QF....&..+..Th+.....
.
.+uIG....7Pk
F,,@.lEL<.....7..Q..=?Q..D(.x.=...w...s..@n+.t..H.P
./ ...D.....-..Y..0a.:... ...j...:I.V|.q.Z=.'..|D.U.A$R..yye..!.....c.3[...3.,j...p..v.....H6.Q..(.%..
.....8.1...+@..#.6.x..,x[....z...r...j!.....) ..:`V..Y.Q.....3.b[..T5.$4L??.B.5....w.=F.....E..+... .,...O7k6Z 2...R.
0....`:....=..a.....boredpanda.com.....I...h.....x.h.i@..:5$...VA..}....&..... .....z...q.e..
}9x%....gng...../.. .....h2.#.....0...0.....>.tK...%..e....0
. *.H..
.....0<1.0 ..U....US1.0
..U.
..Amazon1.0...U....Amazon RSA 2048 M030..
250301000000Z.
260330235959Z0.1.0...U....www.boredpanda.com0.."0
  * H



(Encrypted Client Hello, or ECH, is a way to hide the Server Name Indicator, or SNI)

In November 2024, Russia began blocking Cloudflare's implementation of Encrypted Client Hello (ECH), a privacy-focused extension of the TLS protocol. *"This technology is a means of circumventing restrictions on access to information banned in Russia. Its use violates Russian law and is restricted by the Technical Measure to Combat Threats (TSPU),"* the statement by the Russian Internet regulator read.

https://adguard-dns.io/en/blog/encrypted-client-hello-misconceptions-future.html

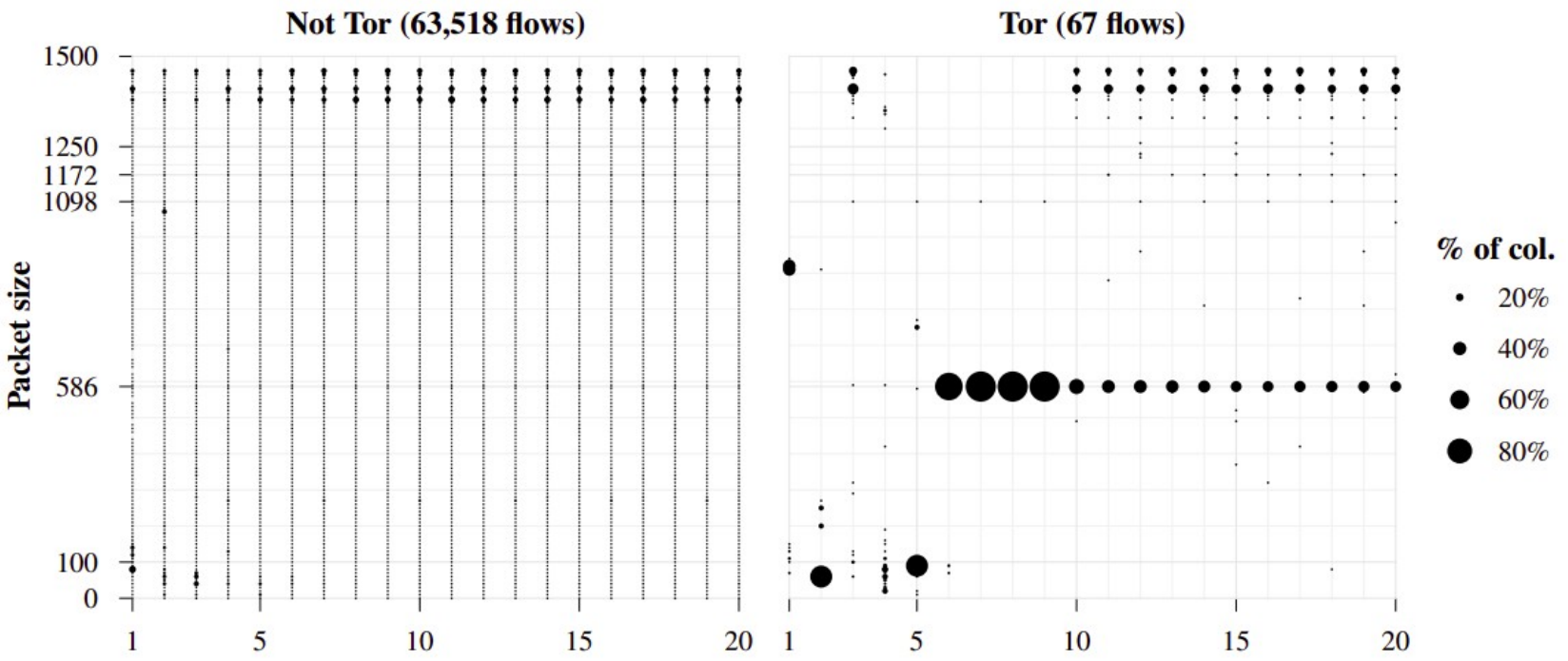


What this lecture is about: if you get past SNI filtering (*e.g.*, with a VPN), can encryption hide which apps and platforms you're using, or hide the fact that you're using a VPN?

StegoTorus: A Camouflage Proxy for the Tor Anonymity System

Zachary Weinberg,[1,2] Jeffrey Wang,[3] Vinod Yegneswaran,[2] Linda Briesemeister,[2]
Steven Cheung,[2] Frank Wang,[3] and Dan Boneh[3]

[1]Carnegie Mellon University [2]SRI International [3]Stanford University



- https://censorbib.nymity.ch/pdf/Winter2013b.pdf

ScrambleSuit: A Polymorph Network Protocol to Circumvent Censorship

Philipp Winter
Karlstad University

Tobias Pulls
Karlstad University

Juergen Fuss
Upper Austria University of Applied Sciences

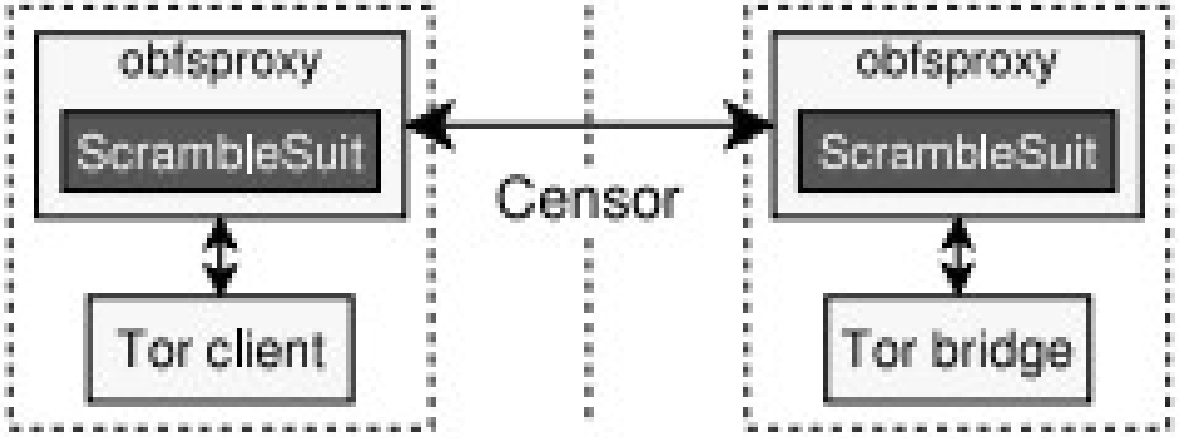
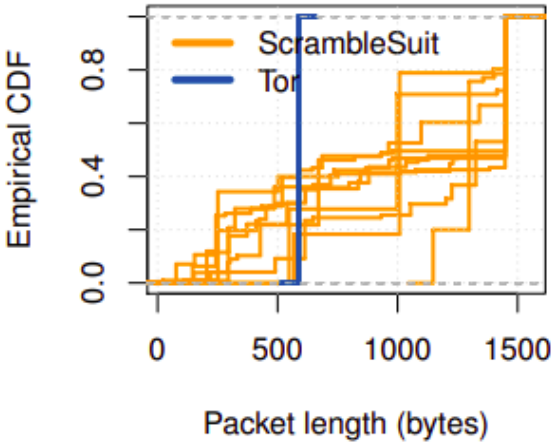
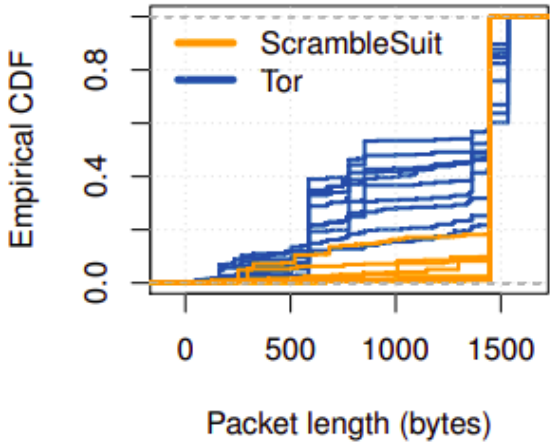


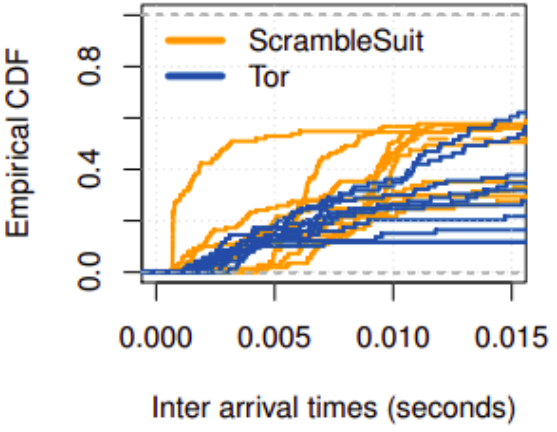
Figure 2: ScrambleSuit is a module for obfsproxy which provides a SOCKS interface for local applications. The traffic between two obfsproxy instances is disguised by ScrambleSuit.



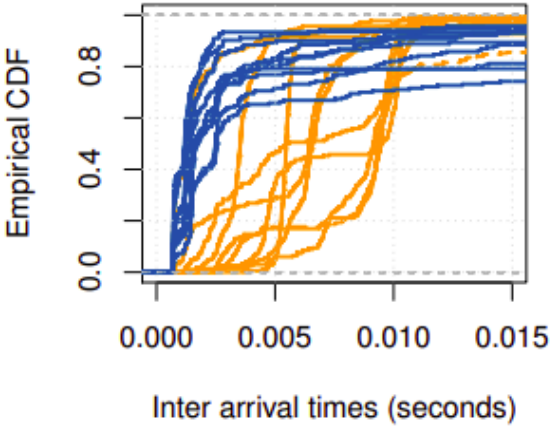
(a) Client-to-server.



(b) Server-to-client.



(c) Client-to-server.



(d) Server-to-client.

How many of you have broken no laws this month? That's the kind of society I want to build. I want a guarantee - with physics and mathematics, not with laws - that we can give ourselves real privacy of personal communications.

---John Gilmore

“apps and platforms” → “protocols”

Two approaches

- Try to look nothing like the banned protocol that you are

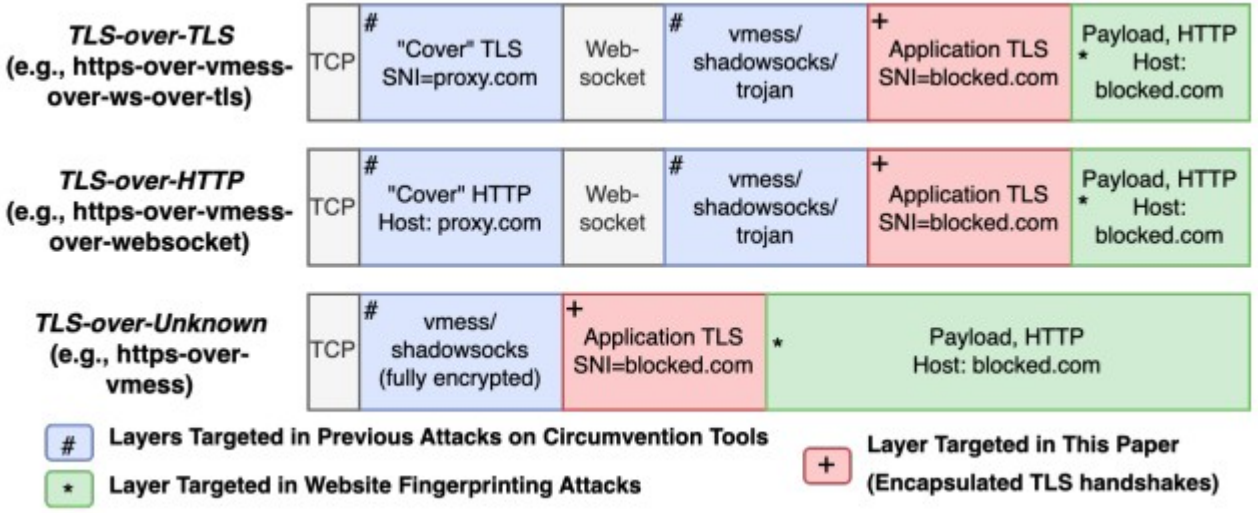
- Try to look like a protocol that everyone is using that is not banned

Fingerprinting Obfuscated Proxy Traffic with Encapsulated TLS Handshakes

Diwen Xue* Michalis Kallitsis† Amir Houmansadr ‡ Roya Ensafi*

*University of Michigan †Merit Network, Inc. ‡ University of Massachusetts Amherst

USENIX Security 2024



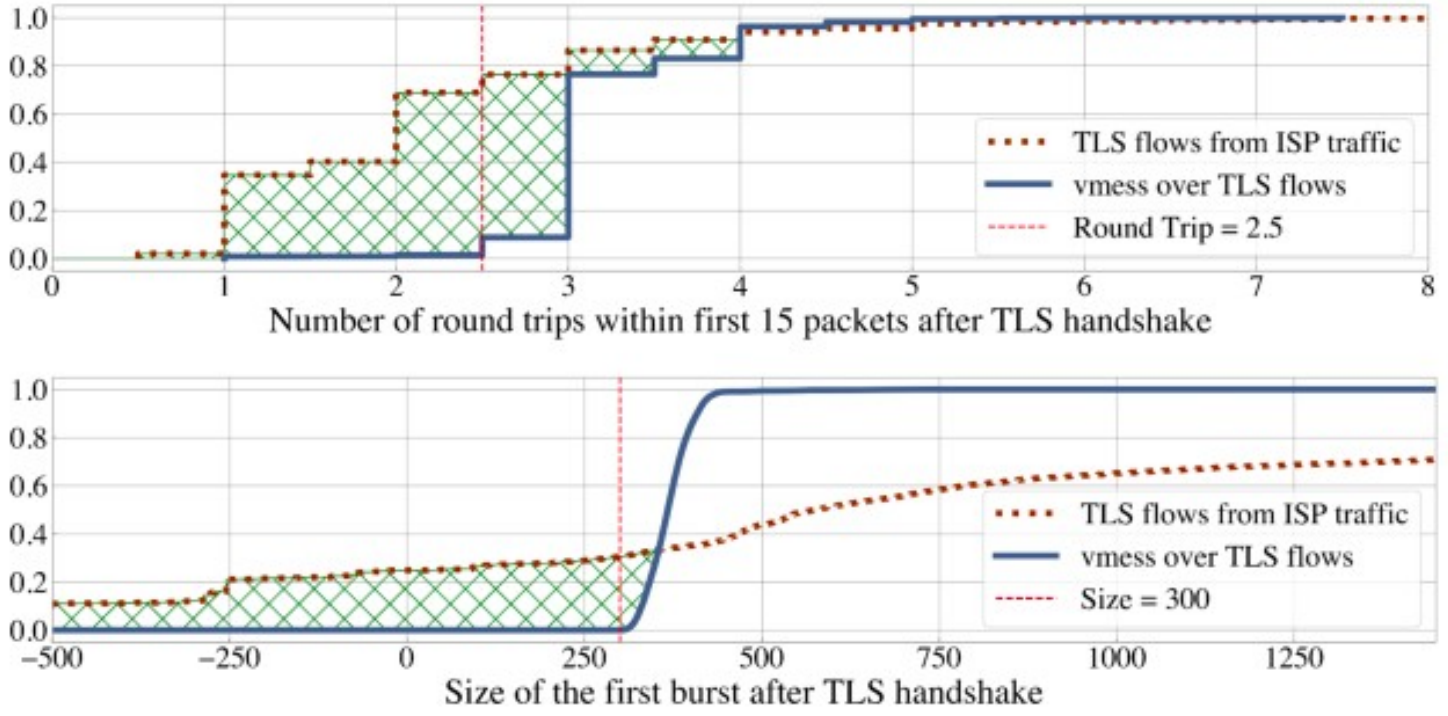


Figure 8: **Round trip count and size of first burst after TLS handshakes.** *TLS-over-TLS* requires more round trips and a larger initial burst due to a second (encapsulated) handshake. Shaded areas highlight dissimilarities that padding and multiplexing cannot obfuscate.

Detecting VPN Traffic through Encapsulated TCP Behavior

Michelina Hanlon
Stanford University

Gerry Wan
Stanford University

Anna Ascheman
Stanford University

Zakir Durumeric
Stanford University

FOCI 2024

- **3WHS:** The presence of a three-way SYN, SYN-ACK, ACK handshake to open the connection (RFC 9293, Section 3.5).
- **500msACK:** The presence of an ACK packet generated within 500 ms of the arrival of a data segment (RFC 9293, Section 3.8.6.3).
- **2RMSS:** The presence of an ACK packet generated after the receival of 2×RMSS bytes of data, where RMSS is the maximum segment size (MSS) specified by the TCP endpoint receiving the segments (RFC 9293, Section 3.8.6.3).

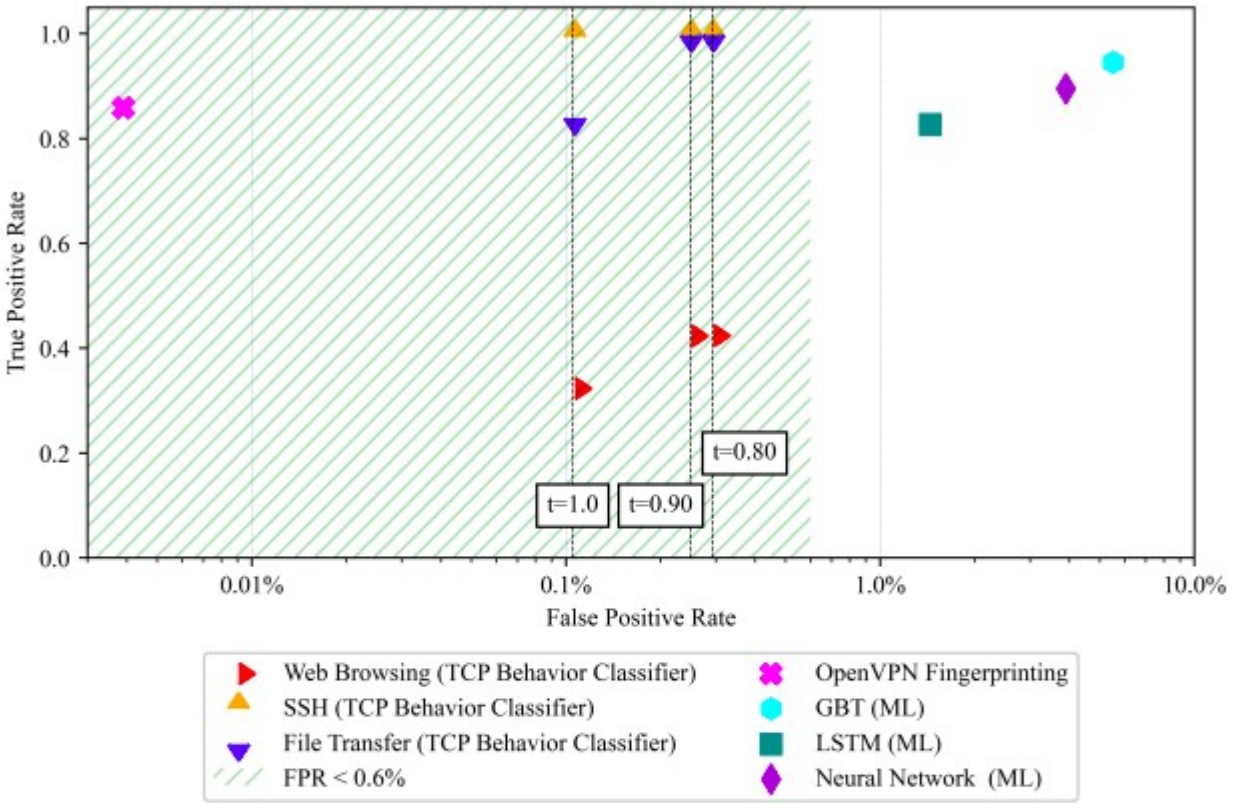


Figure 1: Classifier Results ($t = 1.00, 0.90, 0.80$; $W = 100$). The TPR against the FPR of our classifier (broken down by traffic category) and alternative VPN detection methods. Our protocol-agnostic classifier achieves a FPR an order of magnitude lower than ML detection techniques.

The Discriminative Power of Cross-layer RTTs in Fingerprinting Proxy Traffic

NDSS 2025

Diwen Xue Robert Stanley Piyush Kumar Roya Ensafi
University of Michigan
{diwenx, rsta, piyushks, ensafi}@umich.edu

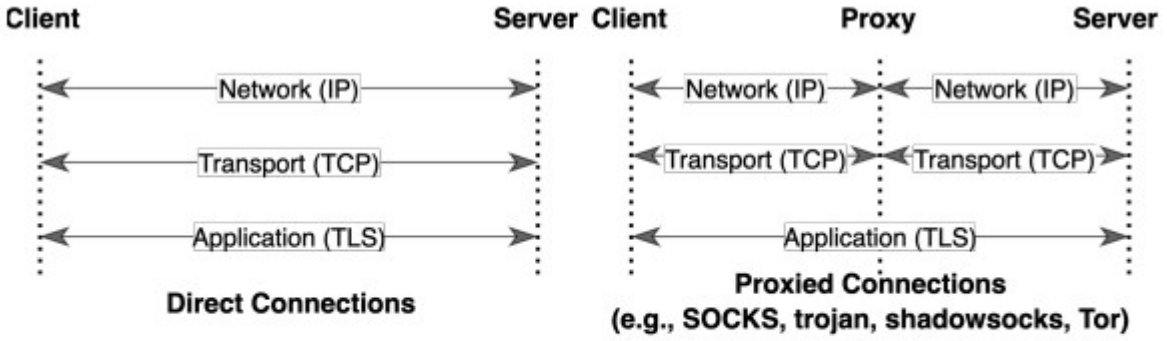


Fig. 2: **Protocol layerings in Direct vs. Proxied Connections.** In proxied connections, transport sessions terminate at the proxy, whereas the application layer connection remains end-to-end. ◇

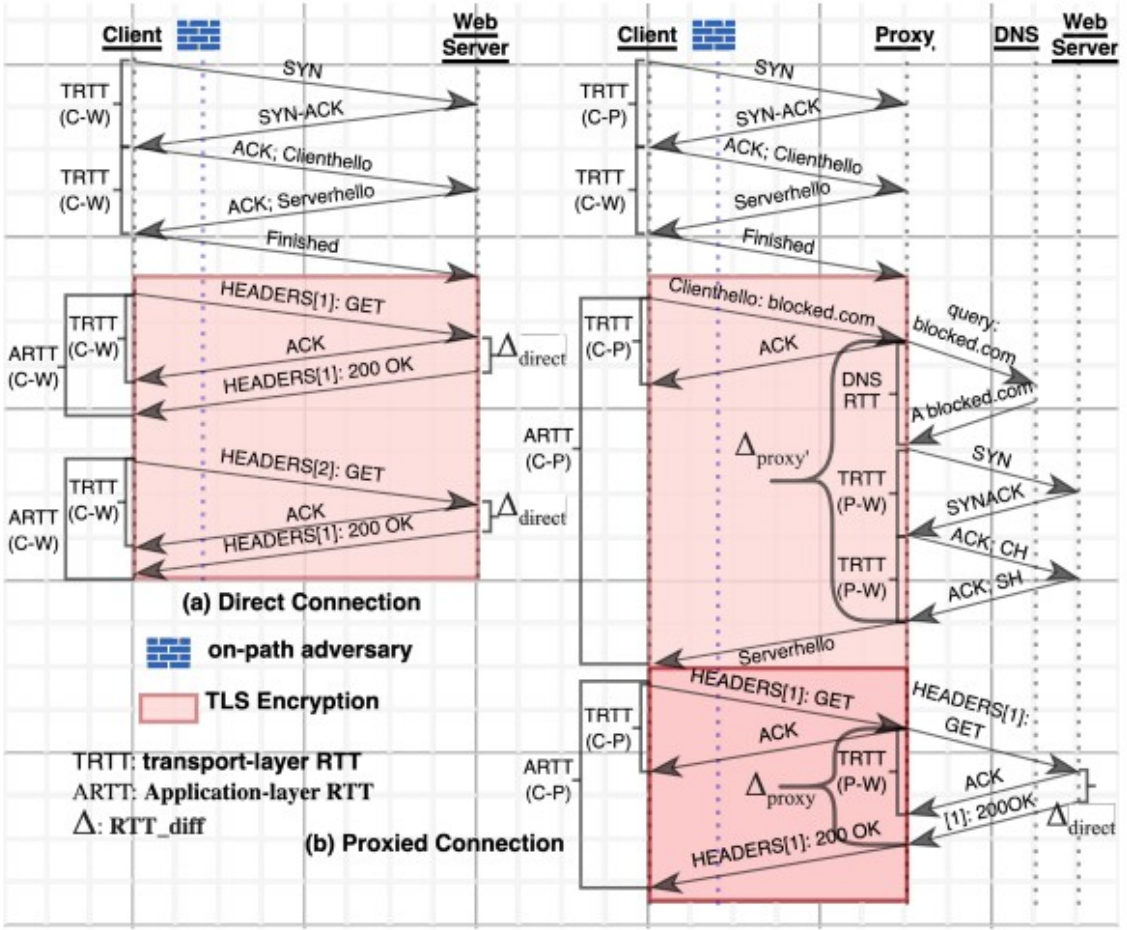


Fig. 3: **Sequence timing diagram for (a) direct HTTPS session vs. (b) TLS-based proxy (vless-over-tls) session.** For the proxied connection, we observe a much higher discrepancy in transport vs. application-layer delay as the sessions at two layers terminate at different endpoints (proxy and the web server, respectively). ◇

Is Custom Congestion Control a Bad Idea for Circumvention Tools?

Wayne Wang
University of Michigan
Ann Arbor, Michigan, USA
wswang@umich.edu

Diwen Xue
University of Michigan
Ann Arbor, Michigan, USA
diwenx@umich.edu

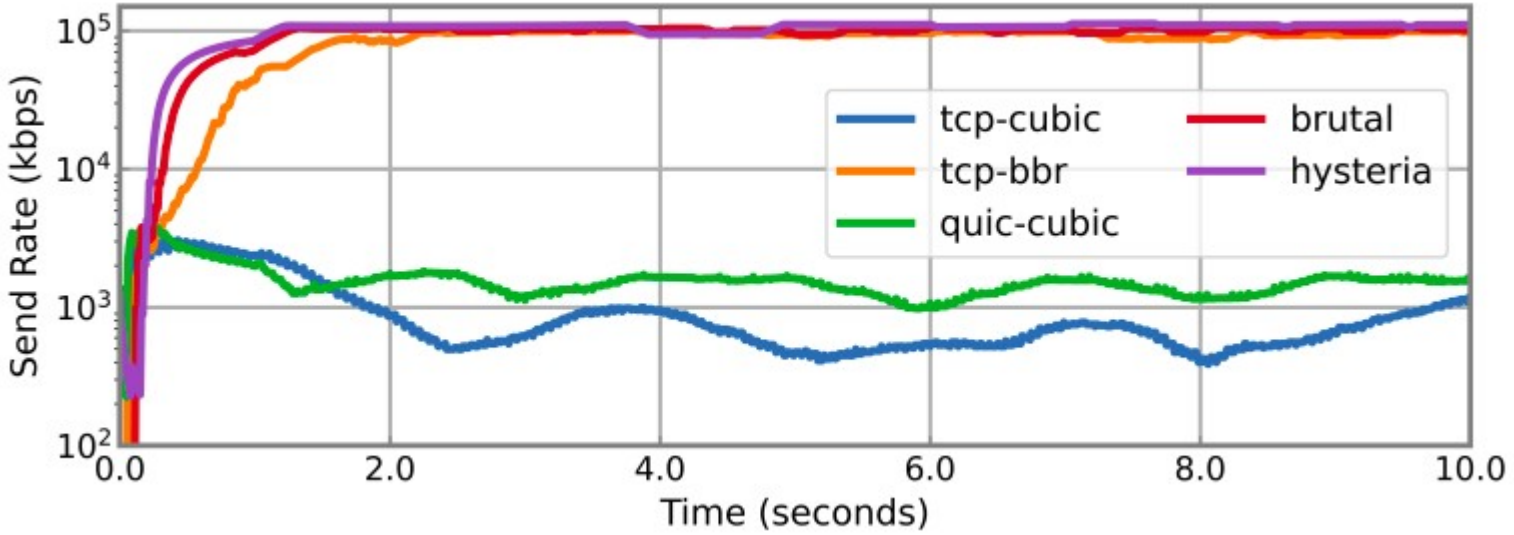
Piyush Kumar
University of Michigan
Ann Arbor, Michigan, USA
piyushks@umich.edu

Ayush Mishra
ETH Zürich
Zürich, Switzerland
aymishra@ethz.ch

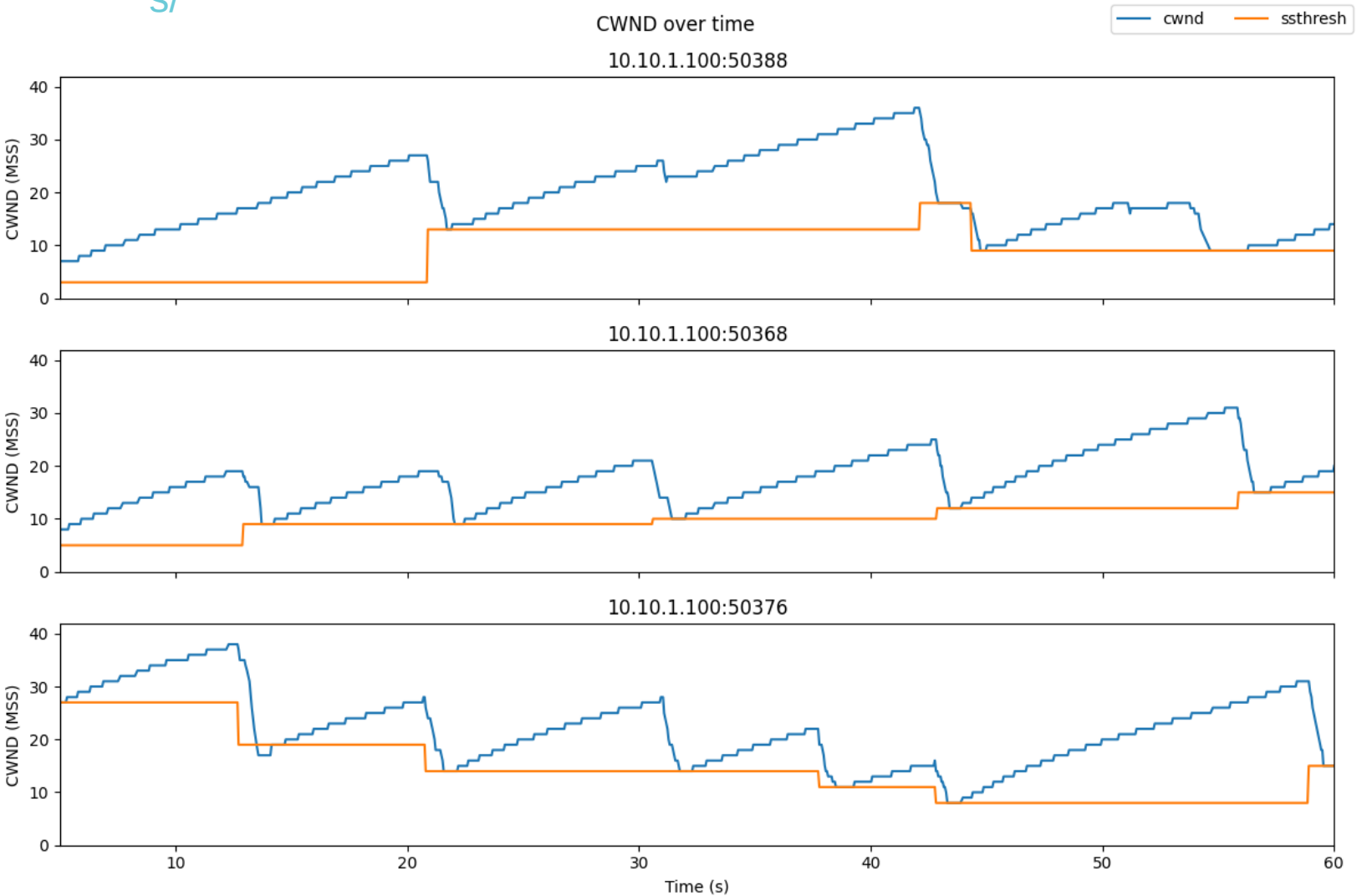
Anonymous

Roya Ensafi
University of Michigan
Ann Arbor, Michigan, USA
ensafi@umich.edu

(FOCI 2025)



https://witestlab.poly.edu/blog/tcp-congestion-control-basics/



Does the DPI need to be nearly perfect *w.r.t.* false positives and false negatives?

- Can shut down VPNs at critical times
- Can collect data about connections over a long period of time
  - https://censorbib.nymity.ch/pdf/Wails2024a.pdf
  - correlate with other data (like financial or social graph information)?
- Can use laws as a deterrent
- Can perform active probing, forensic analysis of confiscated devices, *etc.*
  - *E.g.,* in Brazil: daily fine of fifty thousand reals (US$9,104) for users who bypass the ban with a VPN

OpenVPN is Open to VPN Fingerprinting

Diwen Xue, Reethika Ramesh, and Arham Jain, *University of Michigan;*
Michalis Kallitsis, *Merit Network, Inc.;* J. Alex Halderman, *University of Michigan;*
Jedidiah R. Crandall, *Arizona State University/Breakpointing Bad;* Roya Ensafi,
University of Michigan

https://www.usenix.org/conference/usenixsecurity22/presentation/xue-diwen

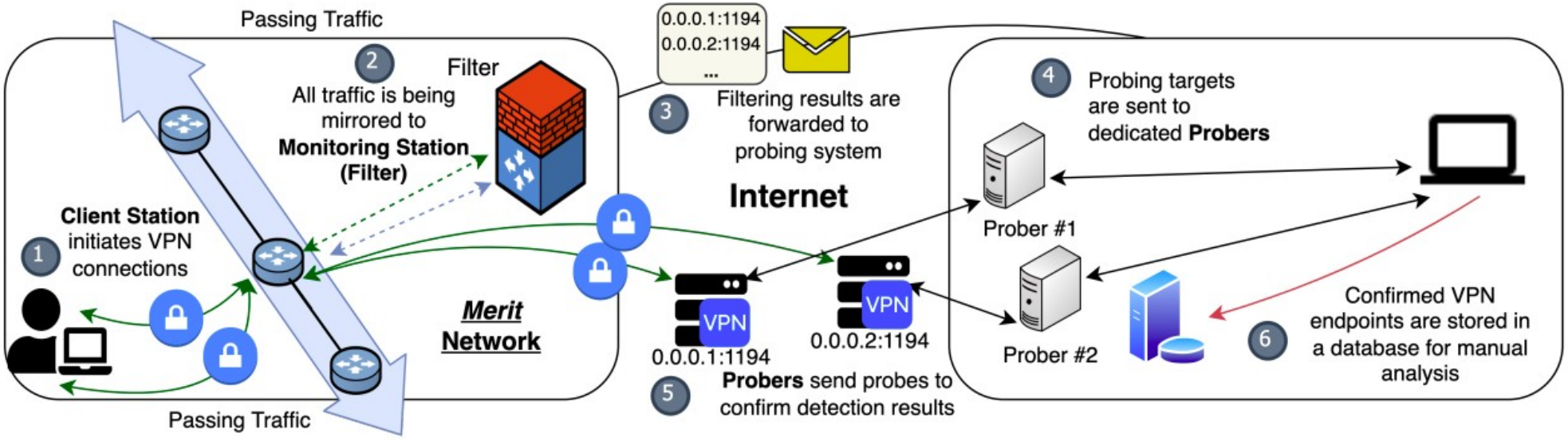
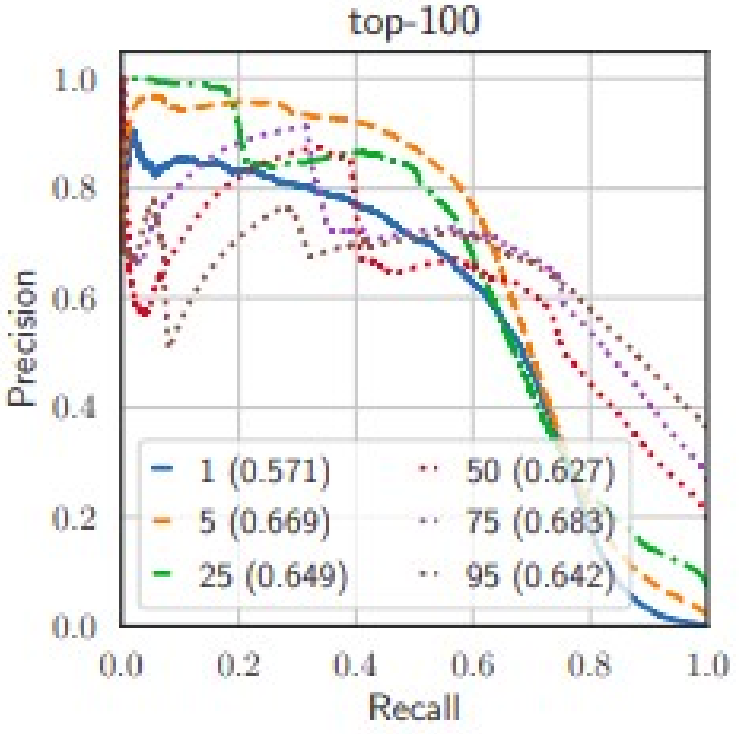


Figure 2: **Framework Deployment on *Merit*** Steps: (1) Client connects to VPN servers. (2) VPN connections, along with passing traffic, are being mirrored to the *Filter*. (3) *Filter* forwards server IP of suspected connections to the probing system. (4) Targets are sent to each dedicated *Probers*. (5) *Probers* send probes asynchronously. (6) Connections confirmed by probing are logged.

Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World

Giovanni Cherubin, *Alan Turing Institute;* Rob Jansen, *U.S. Naval Research Laboratory;* Carmela Troncoso, *EPFL SPRING Lab*

https://www.usenix.org/conference/usenixsecurity22/presentation/cherubin


top-100
Precision
Recall
1.0
0.8
0.6
0.4
0.2
0.0
0.0
0.2
0.4
0.6
0.8
1.0
1 (0.571)
5 (0.669)
25 (0.649)
50 (0.627)
75 (0.683)
95 (0.642)

Websites *vs.* webpages

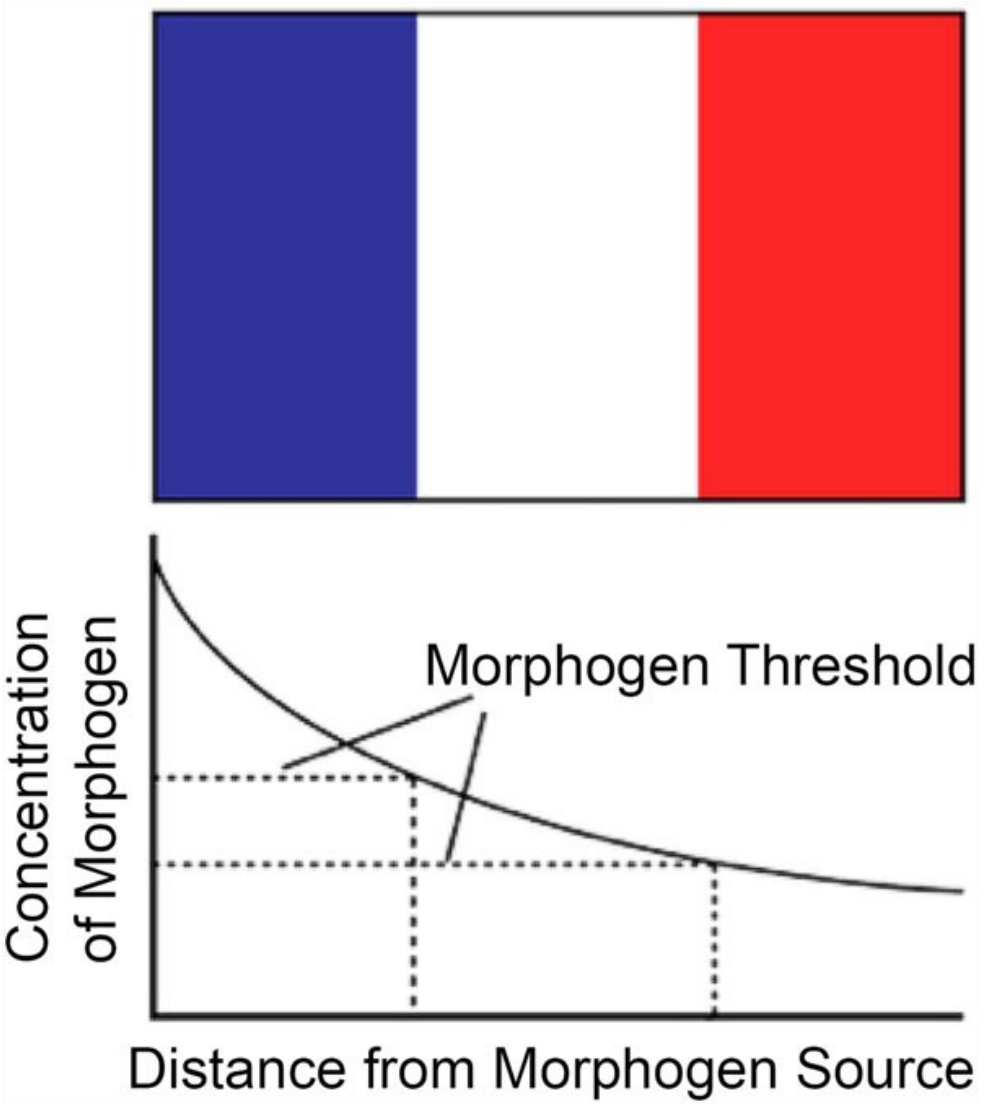
- Website fingerprinting is knowing that you're going to https://en.wikipedia.org, webpage fingerprinting is knowing that you're going to https://en.wikipedia.org/wiki/Operation_Sundevil
- Device fingerprinting, browser fingerprinting, *etc.* are also an issue for VPNs and Tor.

Is there hope?

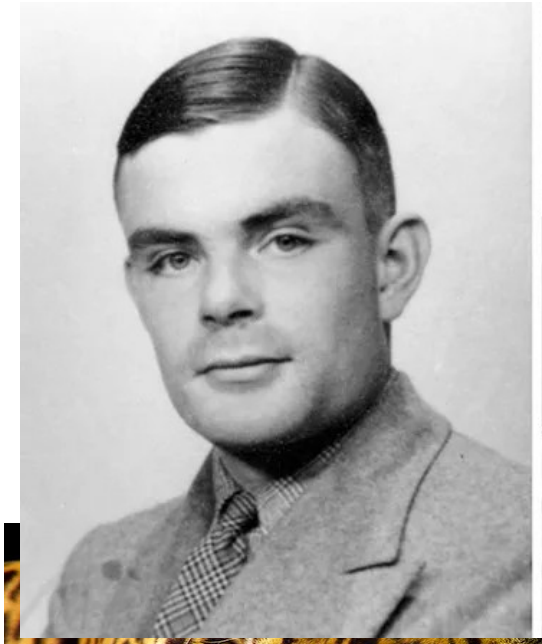
Requirements for traffic obfuscation

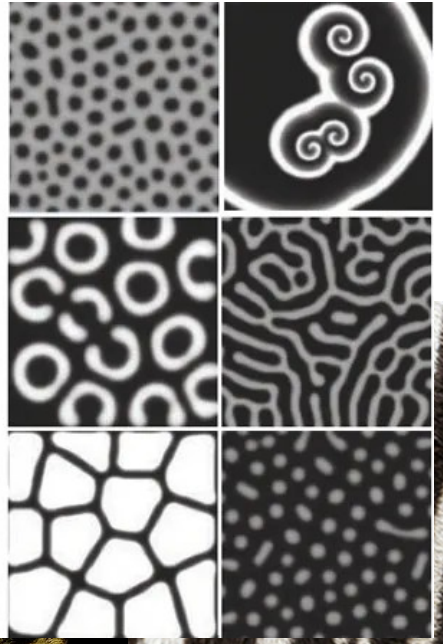
- Has to support the protocols above it, in terms of sending the amount of information needed at the times needed
- Has to not have an obvious signature that can be banned
  - *Diversity* over time and across individuals
- Has to look like the network flows in the natural environment

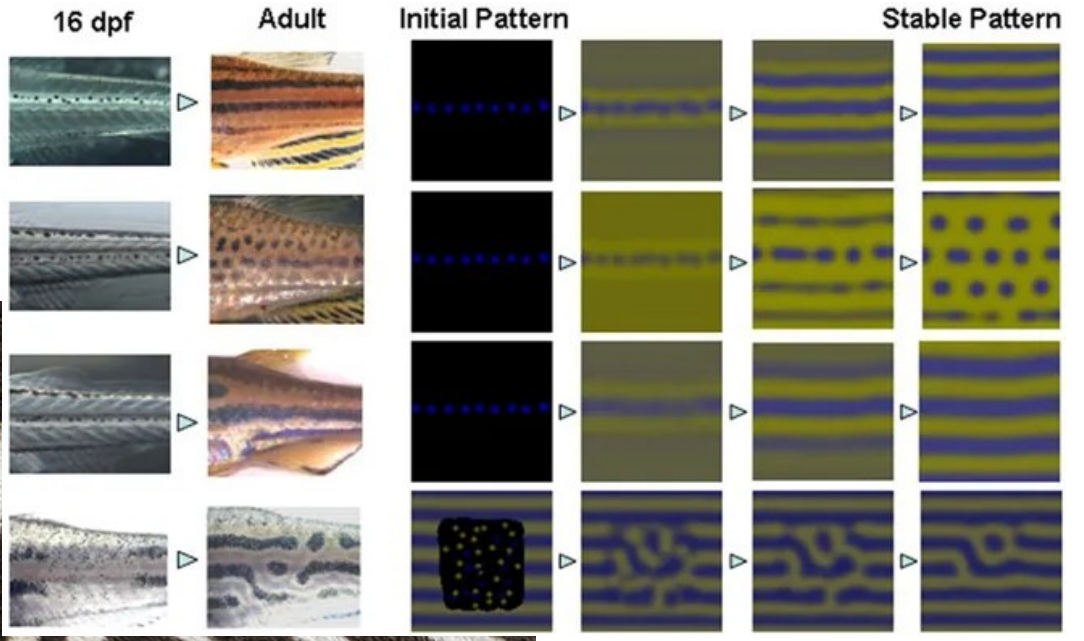
French Flag Model

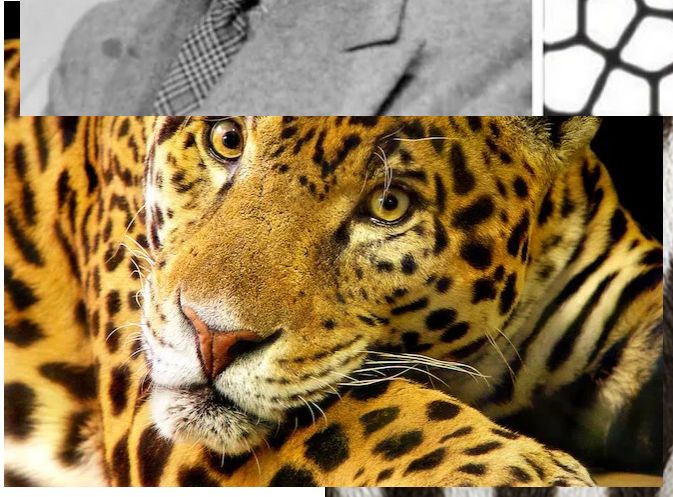


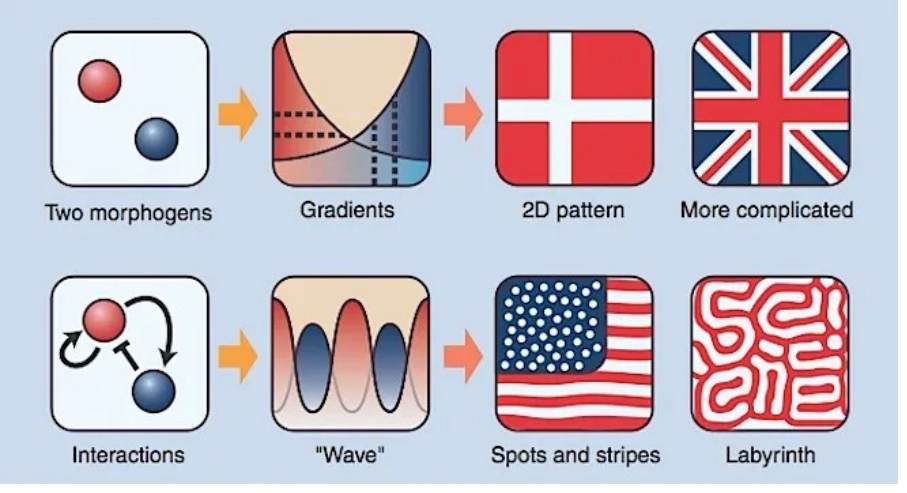
https://www.researchgate.net/figure/The-French-Flag-model-for-positional-information-Based-on-Wolpert-1969_fig6_301250801











https://www.wired.com/2011/02/turing-patterns/

https://censorbib.nymity.ch/