Blind In/On-Path Attacks *and Applications to VPNs*

William J. Tolley†‡, Beau Kujath†‡, Mohammad Taha Khan§, Narseo Vallina-Rodriguez¶£, and Jedidiah R. Crandall†‡

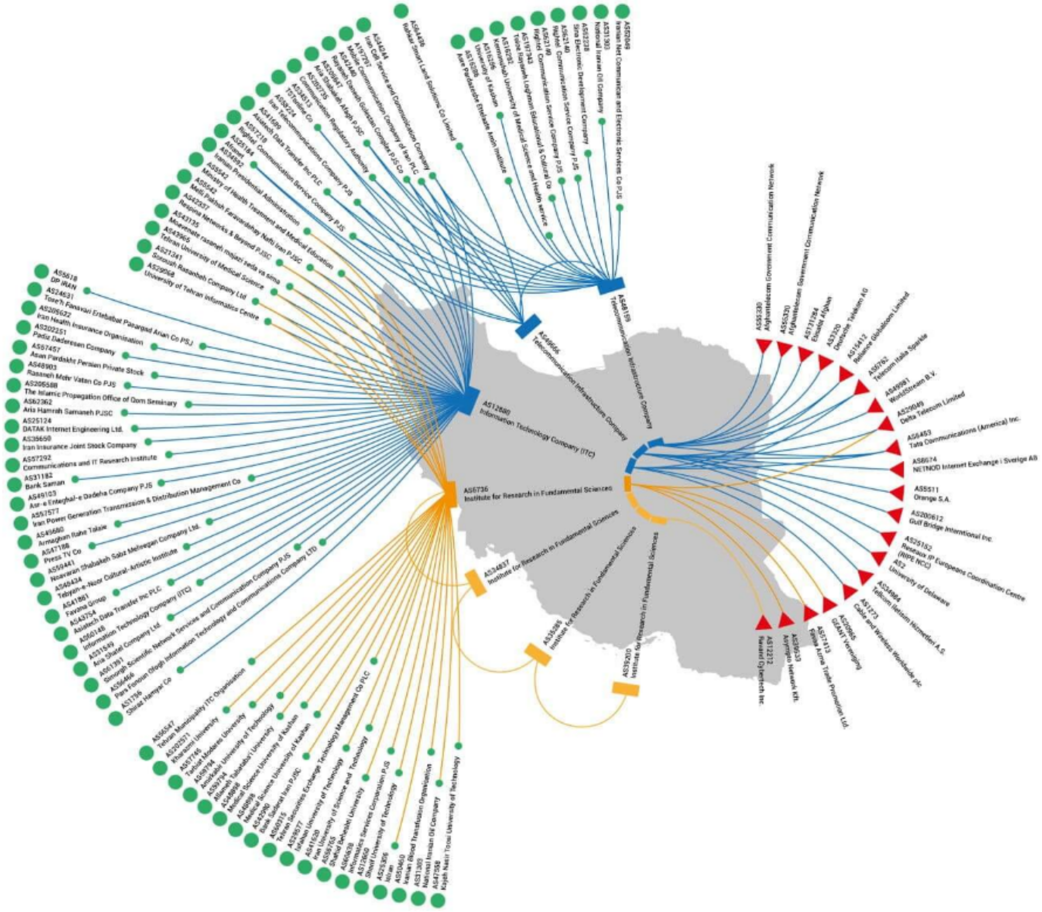
Arizona State University†, Breakpointing Bad‡,
Washington & Lee University§,
IMDEA Networks Institute¶, International Computer Science Institute£

Research question

Do VPNs (and related technologies such as Psiphon, Orbot, *etc.*) protect the connections tunneled through them from inference, interference, and hijacking?

- Public Wifi
- State-controlled cell tower
- In-path state-controlled ISP

In-path state-controlled ISP


AS64436
Rahbar Smart Land Solutions Co Limited
AS52049
Iranian Net Communication and Electronic Services Co PJS
AS31303
National Iranian Oil Company
AS52238
Sina Electronic Development Company
AS62140
Rightel Communication Service Company PJS
AS197343
Toloe Rayaneh Loghman Educational & Cultural Co
AS16262
Kermanshah University of Medical Science and Health service
AS16256
University of Kashan
AS16265
Aria Pardazeshe Etelaate Amin Institute
AS44244
Iran Cell Service and Communication Company
AS197207
Mobile Communication Company of Iran PLC
AS42440
Rayaneh Danesh Golestan Complex PJS Co
AS205647
Aria Shabakeh Afagh PJSC
AS202735
Communication Regulatory Authority
AS34513
TSTonline Co
AS58224
Iran Telecommunications Company PJS
AS41689
Asiatech Data Transfer Inc PLC
AS57218
Rightel Communication Service Company PJS
AS25184
Afranet
AS34592
Iranian Presidential Administration
AS5542
Ministry of Health Treatment and Medical Education
AS5542
Melli Pakhsh Faravardehay Nafti Iran PJSC
AS42337
Respina Networks & Beyond PJSC
AS43135
Moavenate rasaneh majazi seda va sima
AS43965
Tehran University of Medical Science
AS21341
Soroush Rasanheh Company Ltd
AS29068
University of Tehran Informatics Centre
AS5618
DP IRAN
AS24631
Tose'h Fanavari Ertebabat Pasargad Arian Co PSJ
AS205622
Iran Health Insurance Organisation
AS202251
Padiz Daderesan Company
AS57457
Asan Pardakht Persian Private Stock
AS48903
Rasaneh Mehr Vatan Co PJS
AS205588
The Islamic Propagation Office of Qom Seminary
AS62362
Aria Hamrah Samaneh PJSC
AS25124
DATAK Internet Engineering Ltd.
AS35650
Iran Insurance Joint Stock Company
AS57292
Communications and IT Research Institute
AS31182
Bank Saman
AS49103
Asr-e Enteghal-e Dadeha Company PJS
AS57577
Iran Power Generation Transmission & Distribution Management Co
AS49680
Armaghan Rahe Talaie
AS47188
Press TV Co
AS59441
Noavaran Shabakeh Sabz Mehregan Company Ltd.
AS49424
Tebyan-e-Noor Cultural-Artistic Institute
AS41861
Favana Group
AS43754
Asiatech Data Transfer Inc PLC
AS50148
Information Technology Company (ITC)
AS31549
Aria Shatel Company Ltd
AS61391
Simorgh Scientific Network Services and Communication Company PJS
AS56466
Pars Fonoun Ofogh Information Technology and Communications Company LTD
AS1756
Shiraz Hamyar Co
AS56547
Tehran Municipality ITC Organisation
AS202571
Kharazmi University
AS57745
Tarbiat Modares University
AS59794
Amirkabir University of Technology
AS59794
Allameh Tabatabai'i University
AS48898
Medical Science University of Kashan
AS48898
Medical Science University of Kashan
AS42990
Bank Saderat Iran PJSC
AS60315
Tehran Securities Exchange Technology Management Co PLC
AS39577
Isfahan University of Technology
AS41620
Iran University of Science and Technology
AS56765
Shahid Beheshti University
AS60638
Informatics Services Corporation PJS
AS12660
Sharif University of Technology
AS25306
Istran
AS50460
Iranian Blood Transfusion Organisation
AS31385
National Iranian Oil Company
AS47558
Kajeh Nasir Toosi University of Technology
AS12880
Information Technology Company (ITC)
AS6736
Institute for Research in Fundamental Sciences
AS34837
Institute for Research in Fundamental Sciences
AS35285
Institute for Research in Fundamental Sciences
AS35200
Institute for Research in Fundamental Sciences
AS49666
Telecommunication Infrastructure Company
AS48159
Telecommunication Infrastructure Company
AS55330
Afghantelecom Government Communication Network
AS55330
Afghantelecom Government Communication Network
AS131284
Etisalat Afghan
AS3320
Deutsche Telekom AG
AS15412
Reliance Globalcom Limited
AS6762
Telecom Italia Sparkle
AS49981
WorldStream B.V.
AS29049
Delta Telecom Limited
AS6453
Tata Communications (America) Inc.
AS8674
NETNOD Internet Exchange i Sverige AB
AS5511
Orange S.A.
AS200612
Gulf Bridge International Inc.
AS25152
Reseaux IP Europeens Coordination Centre (RIPE NCC)
AS2
University of Delaware
AS34984
Tellcom Iletisim Hizmetleri A.S.
AS1273
Cable and Wireless Worldwide plc
AS20965
GEANT Vereniging
AS57413
Fibre Arma Trade Promotion Ltd.
AS39533
Asympto Networks Kft.
AS12212
Ravand Cybertech Inc.

Reproduced and cropped from https://www.article19.org/ttn-iran-november-shutdown/

Attacker with *.facebook.com SSL/TLS cert

[protected] from Tehran, IRAN, CC BY-SA 2.0 https://creativecommons.org/licenses/by-sa/2.0, via Wikimedia Commons

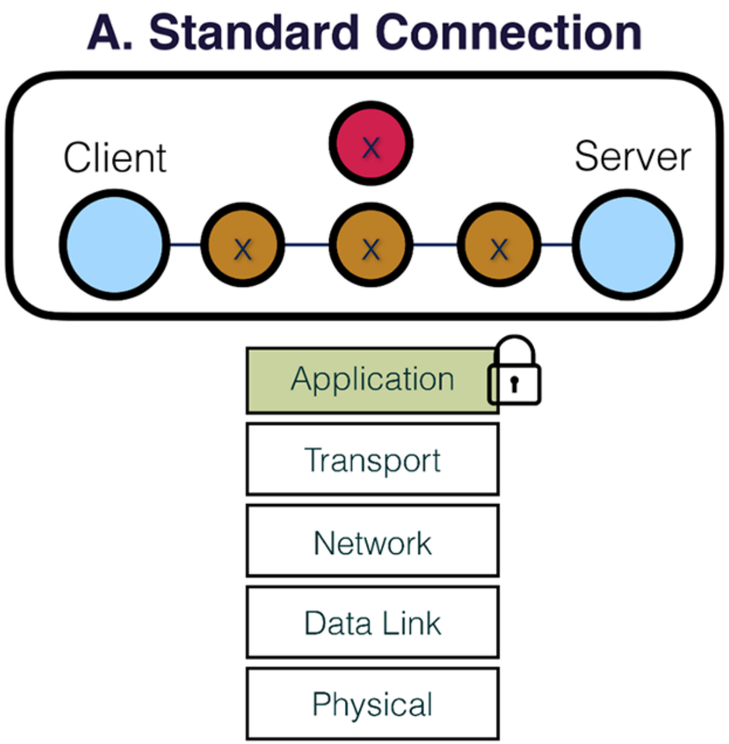
(https://commons.wikimedia.org/wiki/File:Iran_election_(2).jpg)

What if....

What if the Facebook users in Iran in 2009 had all used TLS and a VPN?

E.g. the latest version of WireGuard from May, 2021

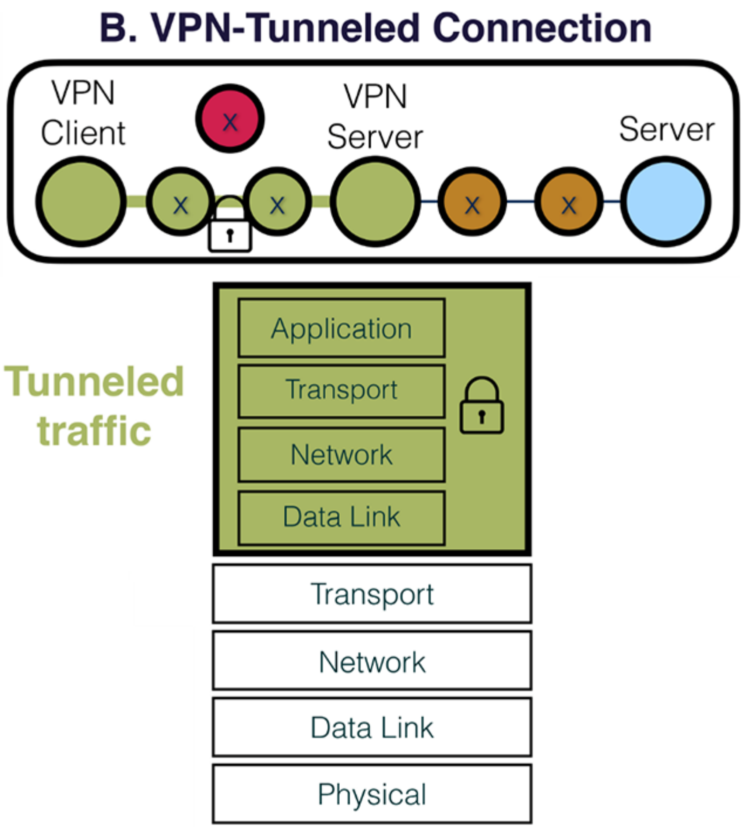
Need for new terminology



A. Standard Connection

- 🟠 X Traditional in/on-path attacker
- 🔴 X Traditional blind off-path attacker
- 🟢 X Blind in/on-path attacker

New terminology: *Blind In/On-Path Attacker*



B. VPN-Tunneled Connection

VPN Client

VPN Server

Server

Tunneled traffic

Application

Transport

Network

Data Link

Transport

Network

Data Link

Physical

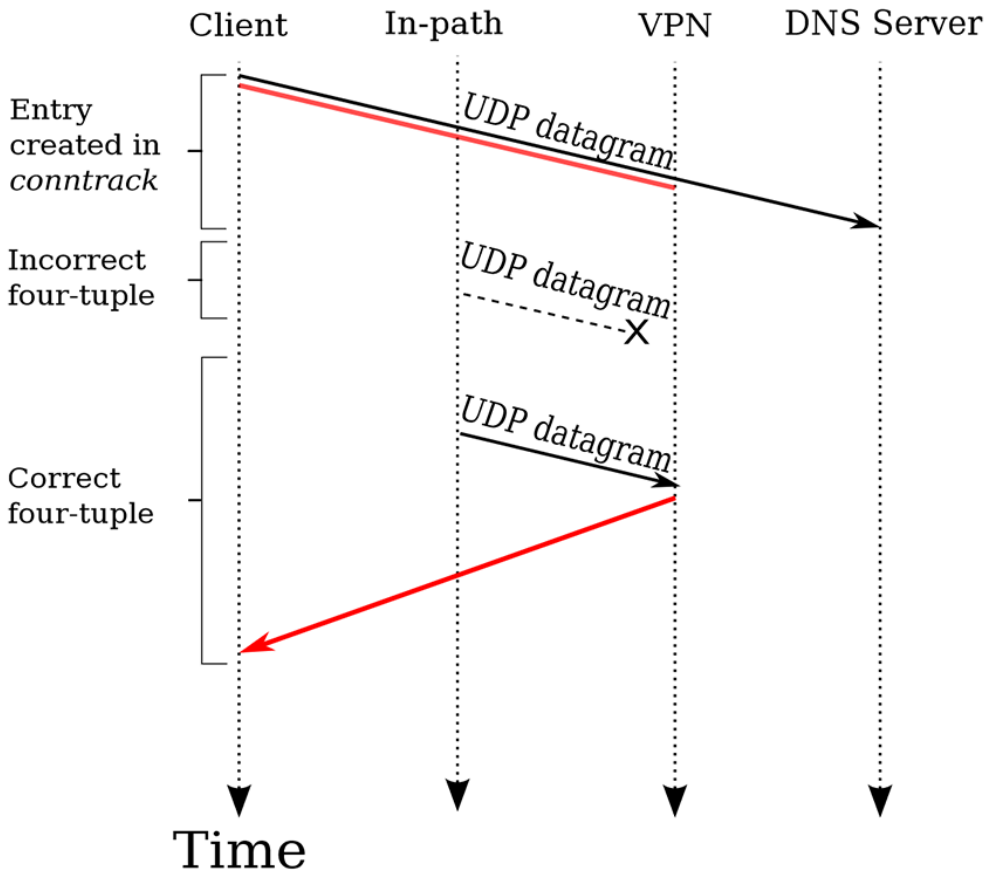
🟠 Traditional in/on-path attacker

🔴 Traditional blind off-path attacker

🟢 Blind in/on-path attacker

Server-side attack on DNS over UDP

UDP Port Inference



IP	UDP			DNS		
. . .	. . .	dst port	. . .	. . .	TXID	. . .

- Off-path attacker
  - $2^{16} \times 2^{16} = 2^{32}$, ☹
- In/On-path attacker
  - $2^{16} + 2^{16} = 2^{17}$
  - 32,768× faster than 2^{32} ☺

Is hijacking DNS practical?

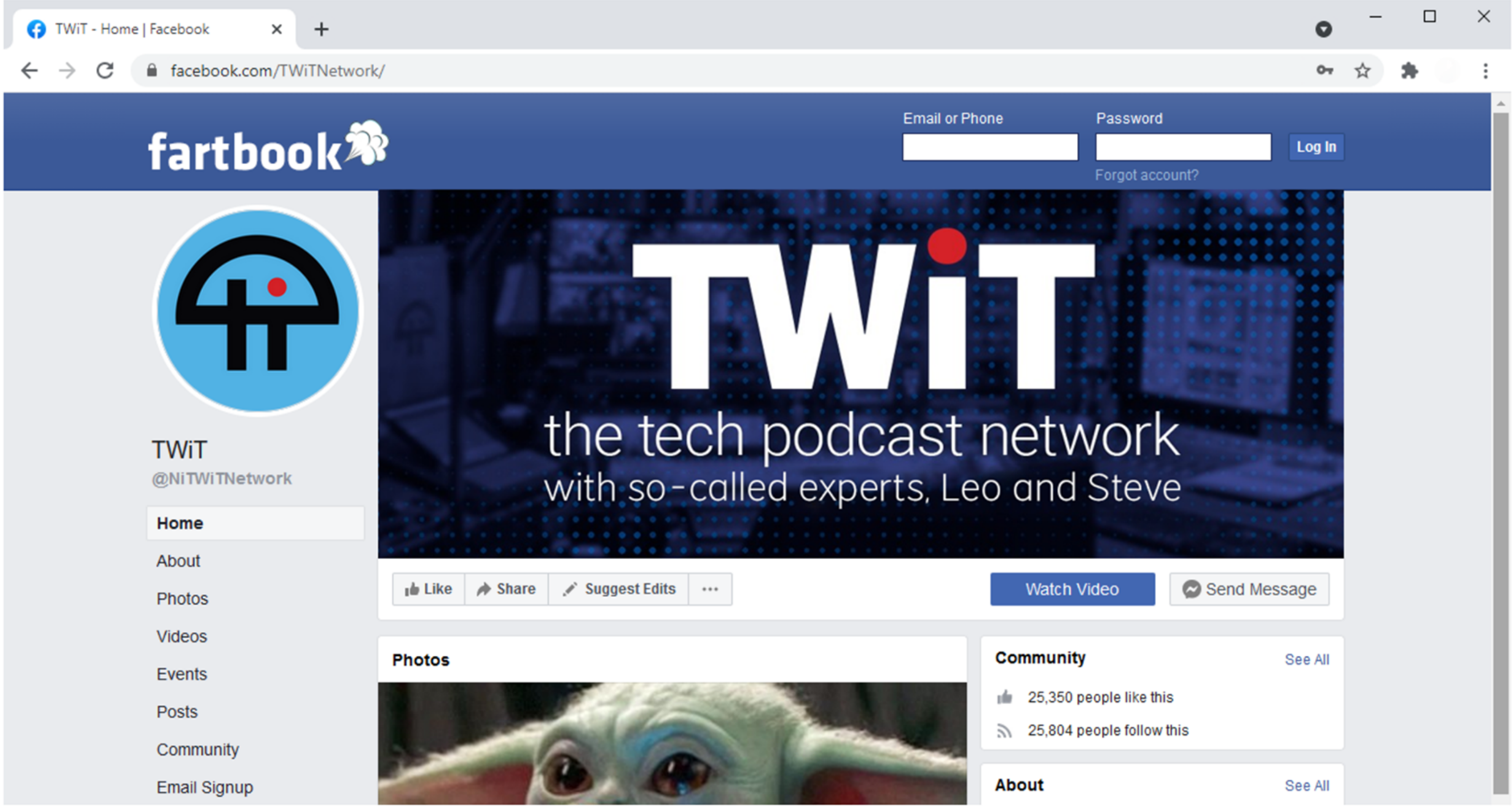
Tested for different DNS timeouts:

- 15 seconds (*e.g.*, Android 11): 75.3% successful
- 10 seconds (*e.g.*, Ubuntu 20.04): 48.1% successful
- 5 seconds (*e.g.*, Firefox 80.0.1): 11.6% successful

The timeout of DNS queries is controlled by applications

Falls back to system's default settings when unspecified

Man-in-the-middle despite TLS and VPN



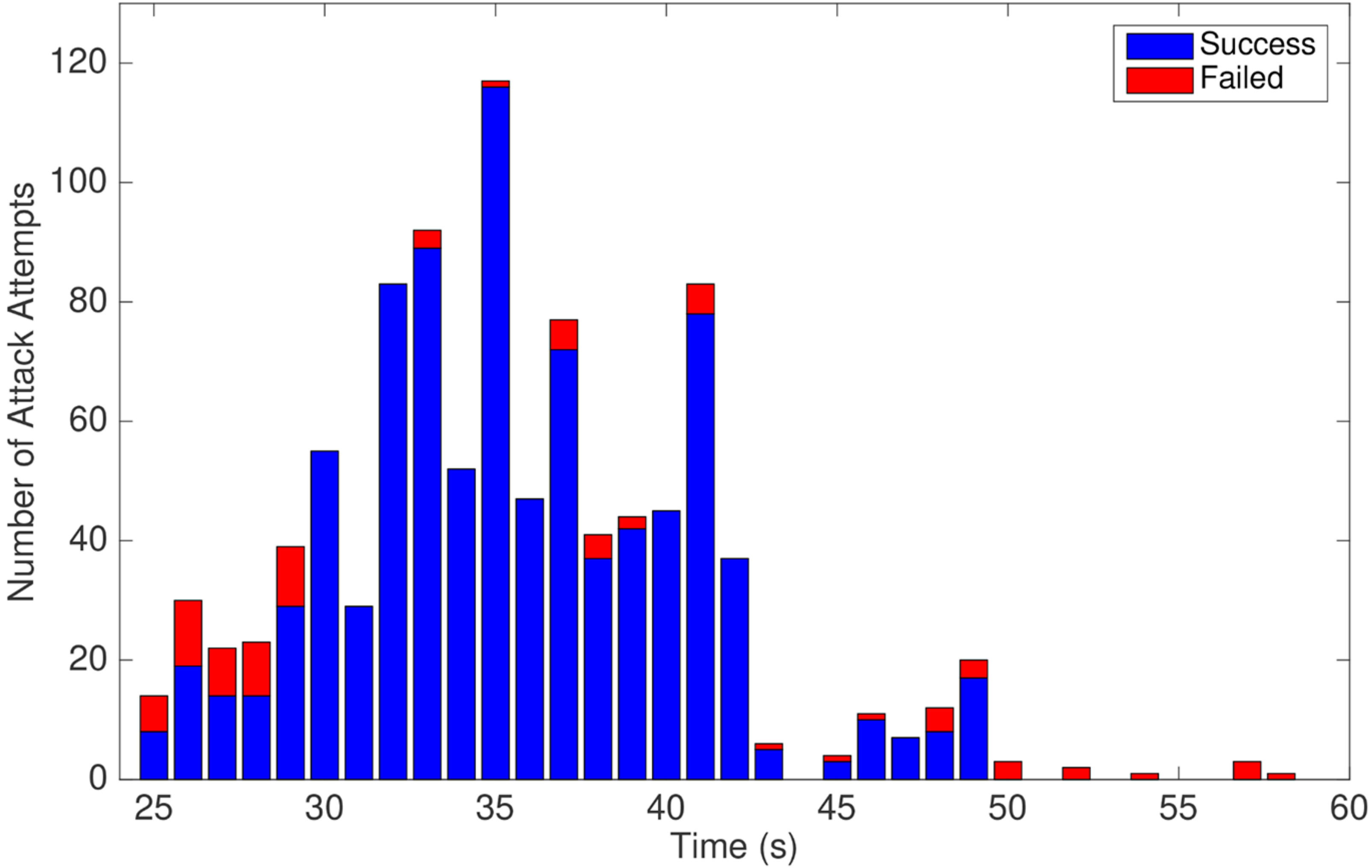
Client- *vs.* server-side attacks

- We also did *client-side attacks*
    - Infer that a client is connected to a VPN
    - Infer the existence of TCP connections in the VPN tunnel
    - Reset or even hijack active TCP connections
- The DNS over UDP attack you just saw is *server-side*
    - Interface and all packet fields are identical for attack *vs.* legitimate traffic
    - It's also possible to do any of our TCP attacks above server-side

Disclosure and mitigation

- Ethical Disclosure
  - CVE-2019-9461
  - CVE-2019-14899
  - Correspondence with Linux kernel developers
- Mitigation
  - *Client-side* ***mitigated*** *by many vendors by distinguishing the interface*
  - *Server-side totally* ***unmitigated*** *by any vendor despite ethical disclosure*

Client-side results



Future work

- Have client-side attacks actually been mitigated by vendors?
- How practical are server-side attacks for a real ISP?
- Can we detect and prevent server-side attacks?
- What about things like Shadowsocks?
- What about padding, *etc.*?
    - *e.g.*, obsfproxy
- What else can go wrong when you stack layers of abstraction on top of each other and encrypt them?

Conclusion

- You can encrypt your packets, but you can't hide their existence, timing, or size
- Blind in/on-path attackers should be considered when designing any protocols that might be tunneled (*e.g.*, in a VPN)

Thank you!

- Contact: william@breakpointingbad.com
- Artifact: https://git.breakpointingbad.com/Breakpointing-Bad-Public/vpn-attacks

- This material is based upon work supported by the U.S. National Science Foundation under Grant nos. 1518523, 1518878, 1801613, and 2007741, as well as the Open Technology Fund and the Ministry of Science and Innovation (Spain) (PID2019-111429RB-C22).