A Comparative Study of Website Fingerprinting Attacks in V2 and V3 Onion Services of Tor Networks

Olusegun Akinyemi[1], Donghoon Kim[1], Doosung Hwang[2]

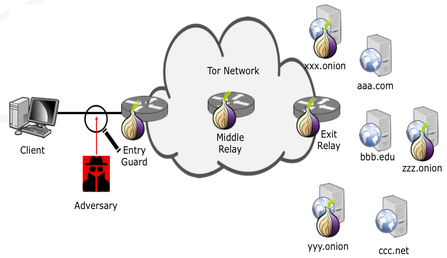
[1]Arkansas State University, [2]Dankook University

Motivation

- Website fingerprinting attacks have revealed a vulnerability in the Tor network.
- Previous studies have shown success rates against the V2 onion service network.
- With the transition to V3 onion services, there has been no recent research on the impact of these changes on website fingerprinting attacks.
- This work analyzes the differences between V2 and V3 onion services and their effect on website fingerprinting attacks with V2 and V3 datasets of Tor networks affect the website fingerprinting attacks

Background & Threat Model

- V3 onion services started in January 2017 with the release of Tor version 0.3.0 and most of V3 running in 2021
- V3 has a new type of address with 56 characters and advanced authentication with Ed25519 elliptic curve



- An adversary is able to observe the network traffic from a client to the entry Tor router (entry guard) and the traffic from the exit Tor router to a destination client to de-anonymize the connection
- Examples: Tor router owner, ISP, or local network administrator

Data & Features

- 10 onion services and each service has 150 instances
- Two different features
  - ❑ 141features (CUMUL + a part of 125 features)

Studied	Feature	No.
Oh *et al.* [5]	Packet general information (44) Cell sequence length (4) Packet inter arrival time (27) Burst information (24) Cell ordering (18) Concentration (8)	125

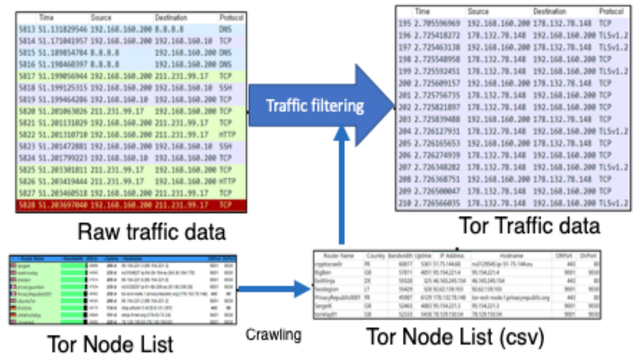
Table 1: Feature Vectors

  - ❑ 104 CUMUL features
    - 4 basic features (the number of incoming/outgoing packets and the sum of incoming/outgoing packets)
    - 100 cumulative sum of packets based on linear interpolant

Approach

To find out the vulnerability of Tor onion services and genera websites, we implemented a framework.

- The framework can collect network traffic
- The framework can filter the collected traffic to consist only of Tor-related traffic



Analysis

- Table 1 shows the results with multi-plication on V2 and V3 onion services. Removing the first several packets

Onion Services	Model	Metrics	Feature vectors	
			CUMUL	141 features
V2	RF	Accuracy	0.6427	0.6826
		Precision	0.626	0.686
		Recall	0.624	0.682
		F1-score	0.62	0.678
		Time (secs)	1.577172	0.440608
	XGB	Accuracy	0.68	0.7066
		Precision	0.69	0.71
		Recall	0.68	0.71
		F1-score	0.68	0.71
		Time (secs)	6.042695	4.9324
V3	RF	Accuracy	0.8847	0.924
		Precision	0.886	0.93
		Recall	0.886	0.924
		F1-score	0.886	0.924
		Time (secs)	1.073523	0.34441
	XGB	Accuracy	0.8933	0.9166
		Precision	0.9	0.92
		Recall	0.89	0.92
		F1-score	0.89	0.92
		Time (secs)	4.851979	3.594631

Table 1: Multi classification.

- V3 onion services have a higher performance metrics: V3 (88.27% to 91.66%), compared with V2 (91.4% -> 87.7%)
- This outcome indicates that V3 is more vulnerable to website fingerprinting attacks than V2

Conclusion

- V3 onion services offer improved performance and security compared to V2 onion services.
- Despite making changes, V3 was not successful in addressing the vulnerability to website fingerprinting attacks, as indicated by the experimental results.
- Our experiments may have limitation on the different environments and fewer onion services

HOTSOS 2023
10TH ANNUAL
HOT TOPICS *in the* SCIENCE OF SECURITY
APRIL 3 - 5, 2023 | *Virtually hosted by* The National Security Agency
hotsos.org