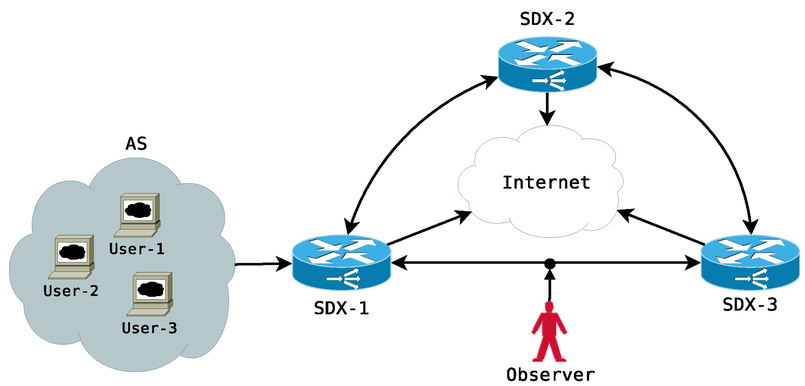
Towards a Traffic Analysis Resistant Internet Architecture

NSF Award #1643020

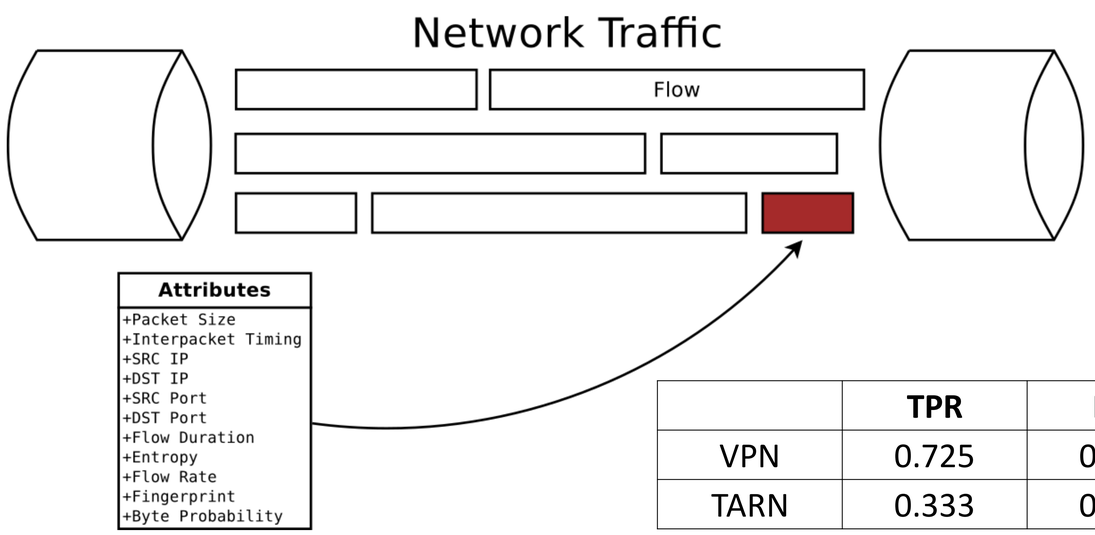
K.C. Wang and Richard Brooks

Clemson University



Challenges:

- Traffic Analysis
- Global Policy
- RHM at the Infrastructure Level



	TPR	FPR
VPN	0.725	0.275
TARN	0.333	0.667

Table 1. Probability of association based on packet size.

	TPR	FPR
VPN	0.431	0.569
TARN	0.342	0.658

Table 2. Probability of association based on inter-packet delay.

Scientific Impact:

- Anonymity Quantification
- SDX Testbed
- IPv6 as a fundamental component in the internet

TARN is an SDX-based privacy tool. TARN is built on the GENI testbed and uses the PEERING BGP testbed to apply network moving target defense techniques at the infrastructure level using IPv6 address prefixes provided by RIPE. Autonomous systems connect with a TARN SDX node through a secure layer two channel, and connections are routed to other TARN SDX nodes through secure layer two channels. By using a Tor-like approach to mixing traffic, we provide anonymity as-a-service.

Our recent work focuses on quantifying the anonymity provided by TARN. We define anonymity as the probability of correctly linking a traffic flow with a user.

Societal Impact:

- Contributing to the Tor Pluggable transports v2.0 standard
- Hackathon in Dakar
- Sustainability through Africtivistes and Danaides (Human Rights NGOs)

Education and Outreach Impact:

- Networking, DDoS, and Resilient Systems classes
- Grad students used and supported GENI and PEERING and discovered BGP issues.
- Presentations/workshops in Moscow, Sydney, Sochi, Dakar, San Diego, and Chicago

Impact Assessment:

- Privacy is increasingly endangered
- MitM and DDoS attacks are a major threat
- BGP hijacking is an ongoing problem

[1] RR Brooks, Kuang-Ching Wang, Lu Yu, G Barrineau, Q Wang, and Jonathan Oakley. Traffic analysis countermeasures using software-defined internet exchanges. In 2018 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC), pages 1–6. IEEE, 2018.

[2] Kuang-Ching Wang, Richard R Brooks, Geddings Barrineau, Jonathan Oakley, Lu Yu, and Qing Wang. Internet security liberated via software defined exchanges. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, pages
19–22. ACM, 2018.

[3] Lu Yu, Qing Wang, Geddings Barrineau, Jon Oakley, Richard R Brooks, and Kuang-Ching Wang. Tarn: A SDN-based traffic analysis resistant network architecture. In 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), pages 91–98. IEEE, 2017.