EAGER: Towards a Traffic Analysis Resistant Internet Architecture

Award #1643020, Kuang-Ching Wang (PI), Richard Brooks (Co-PI)

The Holcombe Department of Electrical and Computer, Clemson University, SC

❑ Motivation & Objective

We propose an alternative to current end-to-end communication that removes traffic analysis vulnerabilities by using SDN-based solutions.

Unlike existing proxy-based solutions (e.g., Tor, Psiphon, Decoy routing), our method avoids using intermediate nodes.

❑ Communications with dynamic IP

Core concept: bind communication sessions to *randomized*, *short-lived* and *perpetually changing* IPv6 address.
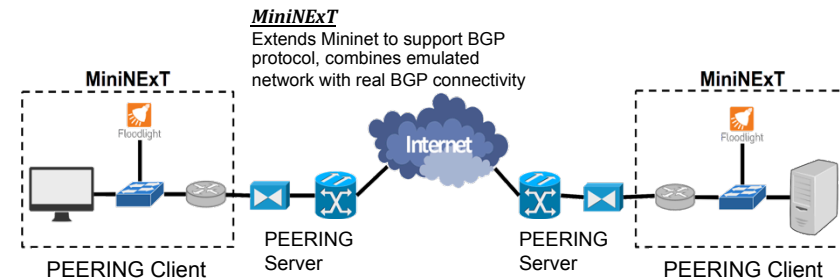
Two scenarios:

BGP-based : SDN at network edge (e.g., ovs on each host), and BGP routing in the core.

SDX-based : SDN at network core (e.g., Internet exchange point), and no longer dependent on BGP prefix announcement.

Scenario One: BGP Injection

Scenario Two: SDX Forwarding with BGP Injection
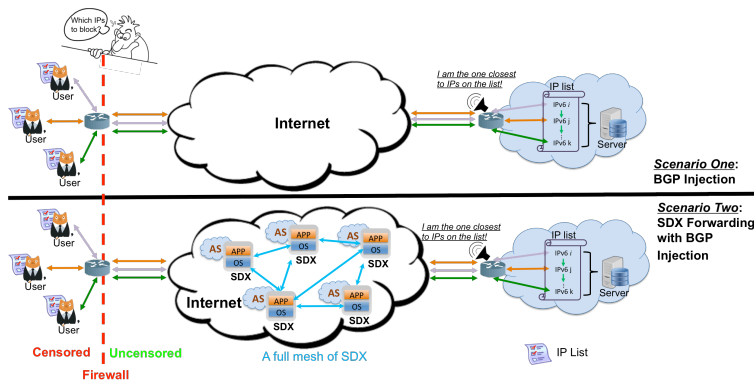
❑ Demonstration on PEERING testbed

- ▪ A BGP testbed supported by NSF for experimenters to exchange BGP routes and traffic with real ISPs (8 ASNs in US, EU and South Africa).
- ▪ Experimenters announce BGP prefixes at selected Point of Presences (PoPs).

MiniNExT
Extends Mininet to support BGP protocol, combines emulated network with real BGP connectivity

PEERING Client   PEERING Server   PEERING Server   PEERING Client

❑ Future Work and Direction

Traffic analysis-resistance analysis

- ▪ Header-based
- ▪ Payload-based (DPI)
- ▪ Side-channel analysis

- • Real network traffic will be used as background traffic to assess our method against anomaly-based detection.

GENI Testbed: Global Federated Experiments

With GENI's federated international testbeds, we plan to conduct larger scale experiments that interface the Internet through different geographic locations to observe and validate its data plane behaviors.

From BGP to SDX

Moving intelligence from the edge into SDX.