Privacy-Preserving Detection of Inter-Domain SDN Rules Overlaps

Arnaud Dethise[1,2], Marco Chiesa[2], Marco Canini[1]

[1] KAUST, [2] Université catholique de Louvain

SDN inter-domain deployment is dangerous!

- SDN routing expressiveness is ***higher*** than in BGP

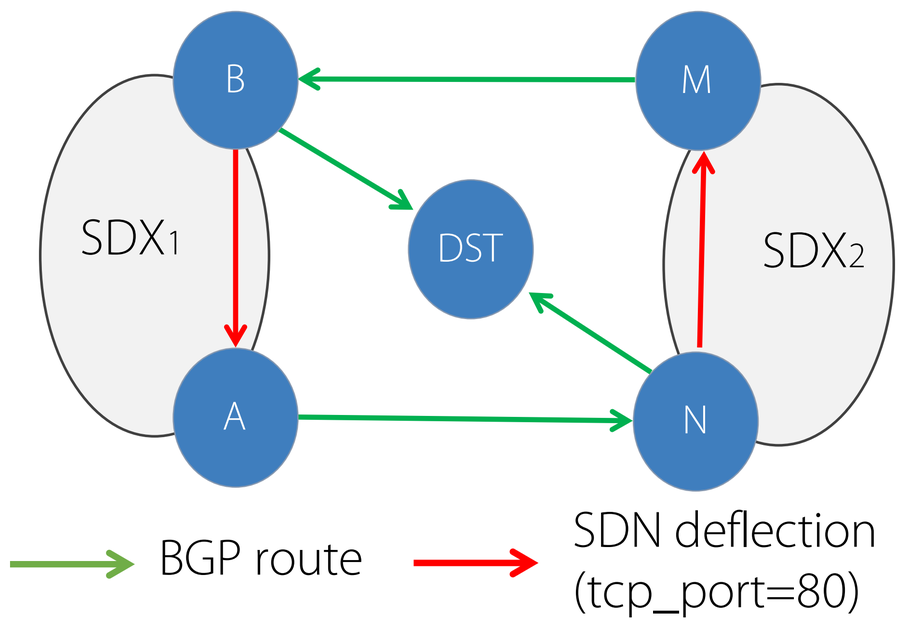
SDN source/destination IP/TCP, …

BGP destination IP only

- When deployed for inter-domain routing (e.g. at IXPs), SDN can be used to ***deflect*** specific traffic from BGP routes …with risk of permanent forwarding loops [1]

Forwarding loop example

- Networks *M* and *A* route their traffic towards a destination *DST* using paths *(M, B, DST)* and *(A, N, DST)*, resp.
- Networks *B* and *N* steer their HTTP traffic towards *A* and *M* resp. by installing SDN deflection at their Software-Defined eXchanges (SDXes)
- A loop through *M, B, A,* and *N* is created for HTTP traffic!



Detecting forwarding loops: Trading efficiency and correctness for privacy

- Detection correctness depends on the completeness of the shared forwarding information
- **Alternative #1**: One can share all forwarding information to achieve correctness at the price of privacy
- **Alternative #2**: One can hide some information to increase privacy at the price of correctness [1]
- **Our approach**: We want to **preserve correctness and privacy while still achieving practical runtimes**

DISTINCT-MATCH primitive

- A new privacy-preserving SDN verification primitive that allows any two networks, each one holding a set of SDN rules, to **verify whether the match space of the two sets of rules overlap**
- Based on Secure Multi-Party Computation (SMPC)

	match bits							
R1	1	*	*	1	0	*	1	0
R2	1	*	0	*	0	*	1	*

overlap on 1*010*10

	match bits							
R1	1	*	*	1	0	*	1	0
R2	1	*	0	*	1	*	1	*

distinct match

Practically good SMPC performance!

SDXes latency	Number of SDN rules				Baseline
	1	50	500	5000	
1 ms	5	9	24	33	3
10 ms	41	60	90	264	21
100 ms	401	599	839	2528	201

SMPC online evaluation in milliseconds

- Distinct-Match run time is comparable to network delay between the two SMPC parties

Detecting Inter-SDX forwarding loops

- We outsource SMPC to the SDXes → speed up by 5x
  - **SDXes learn whether some bits in the rules match or not but do not learn the contents of these rules**
- An SDX verifies if there exist networks downstream that deflect packets matching a given SDN rule, and iteratively follows deflections towards the next hop
  - **If a chain leads back to the SDX verifier → a forwarding loop is found**

FUTURE RESEARCH: Internet Network Verification vs. Privacy

- An operator wants to verify **general** properties of the Internet routing such as forwarding loops, blackholing, stability, and more without leaking any private information

ENDEAVOUR

This research is (in part) supported by European Union's Horizon 2020 research and innovation programme under the ENDEAVOUR project (grant agreement 644960).

[1] R. Birkner et al. "SDX-Based Flexibility or Internet Correctness? Pick Two! ", SOSR 2017