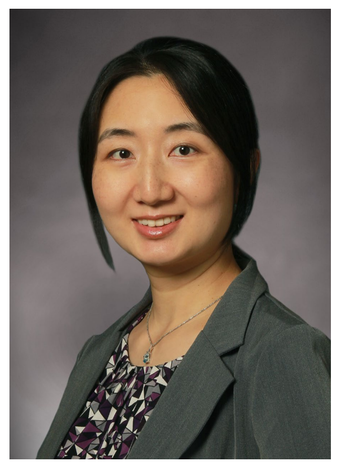
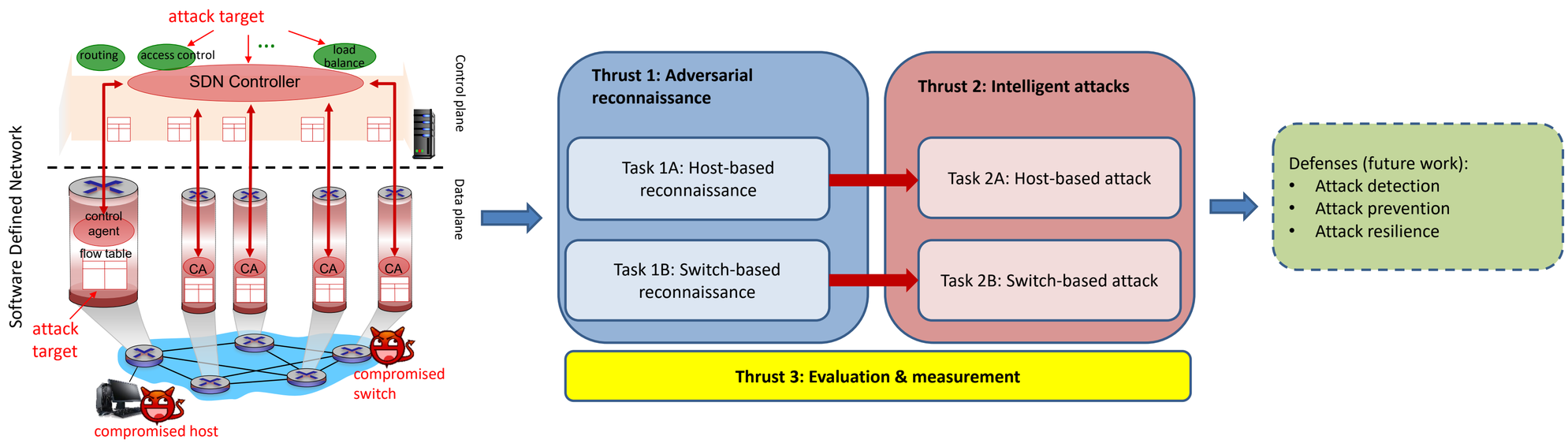
SaTC: CORE: Small: Adversarial Network Reconnaissance in Software Defined Networking



Ting He (PI), Patrick McDaniel (Co-PI)

Video: https://psu.mediaspace.kaltura.com/media/Ting+He+-+SaTC+PI+Meeting+2022/1_1ci77w8d

Website: https://nsrg.cse.psu.edu/research/satc-core-small-adversarial-network-reconnaissance-in-software-defined-networking/



Challenge:

- Data-control plane separation in SDN introduces new attack surfaces
  - Data plane relies on commands from a remote controller for operation
  - Controller's decision relies on accurate network state reported by data plane switches
- Insufficient understanding of the consequences of such separation in face of intelligent adversaries

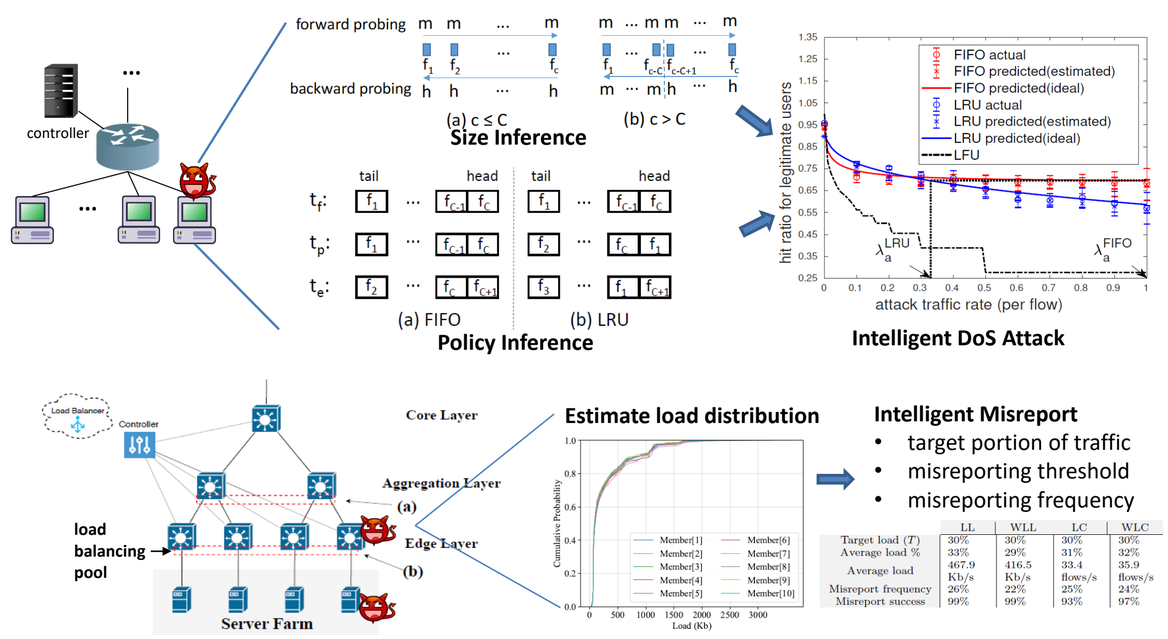
Scientific Impact:

- Identify new attacks exploiting the vulnerabilities of SDN through ***adversarial reconnaissance***, by answering
  - What information can be deduced by an internal/external adversary?
  - What is the consequence of exposing this information?
- Provide guidelines on future SDN designs with better resilience against intelligent adversaries

Solution:

Adversarial inference of ***internal characteristics***:

- Host-based inference & attack on flow table
  - use RTTs to detect table hits/misses for probing packets
  - infer table size using *forward-backward* probing
  - infer replacement policy by *flush-promote-evict* probing
- Switch-based inference & attack on load balancer
  - estimate the load distribution at other pool members based on loads observed at the compromised switch
  - under-reporting: attract an unfairly large portion of traffic
  - over-reporting: cause unfairly large loads on other members



	LL	WLL	LC	WLC
Target load (T)	30%	30%	30%	30%
Average load %	33%	29%	31%	32%
Average load	467.9 Kb/s	416.5 Kb/s	33.4 flows/s	35.9 flows/s
Misreport frequency	26%	22%	25%	24%
Misreport success	99%	99%	93%	97%

Broader Impact on Society:

- Raise awareness SDN's vulnerabilities
- Motivate new designs and best practices
- Generate lessons learned for SDN administrators and developers

Broader Impact on Education:

- Disseminate results to the community
  - 1 INFOCOM, 1 ICDCS, 1 SecureComm, 3 journals, open-source code
- Train new workforce on SDN and security
  - 2 PhD, 3 MS, including 2 female

Broadening Participation:

- CSE summer camp 2021-22: introduce 15-20 middle school girls to cutting-edge topics in CS through week-long interactive programs
- Girls Who Code: provide free coding classes on Sundays to local female middle/high school students
- N2Women: mentor female PhD students to organize panels at INFOCOM'20 and ICCCN'22

Award ID#: 1946022