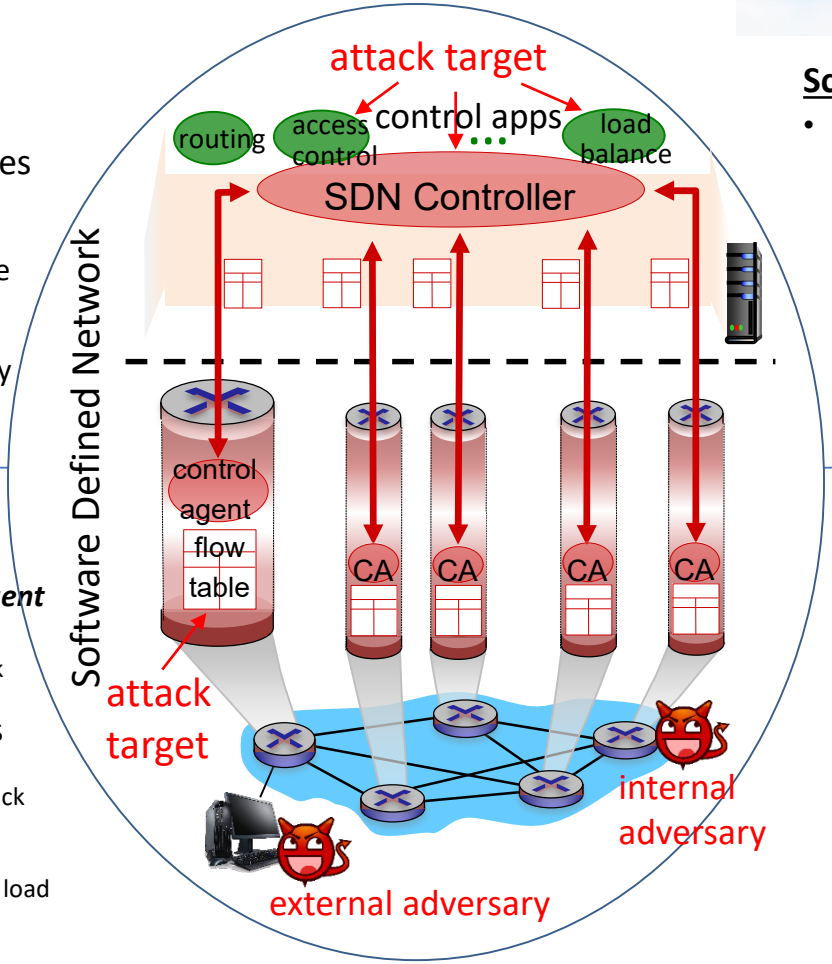
SaTC: CORE: Small: Adversarial Network Reconnaissance in Software Defined Networking

PennState College of Engineering | INSTITUTE FOR NETWORKING AND SECURITY RESEARCH

Challenge:

- The ***data-control plane separation*** in SDN introduces new attack surfaces:
  - Data plane relies on commands from a remote controller
  - Control plane relies on network state reported by distributed switches



Scientific Impact:

- Identify new attacks exploiting the vulnerabilities of SDN through ***adversarial reconnaissance***:
  - What information can be learned by an adversary
    → static configuration parameters & dynamic traffic parameters
  - What is the consequence of exposing this information
    → intelligent attacks

Solution:

- ***Adversarial inference*** and ***intelligent attacks*** on SDN:
  - Host-based reconnaissance & attack
    - E.g., use RTTS to infer flow table size/policy/load → intelligent DoS attack
  - Switch-based reconnaissance & attack
    - E.g., use own loads to infer load distribution at other switches → intelligent misreporting attack on load balancer

Broader Impact and Broader Participation:

- Raise awareness of SDN's vulnerabilities and motivate new designs with better resilience
- Disseminate results to the research community (1 INFOCOM, 1 ICDCS, 1 SecureComm, 3 journals, open-source code)
- Train next-generation network and security workforce (2 PhD, 3 MS, including 2 female)
- Support BPC activities (Girls Who Code, CSE Girls' Camp)

Award#: 1946022, Awardee: Penn State University, PI: Ting He, Co-PI: Patrick McDaniel, Email: tinghe@psu.edu, mcdaniel@cse.psu.edu