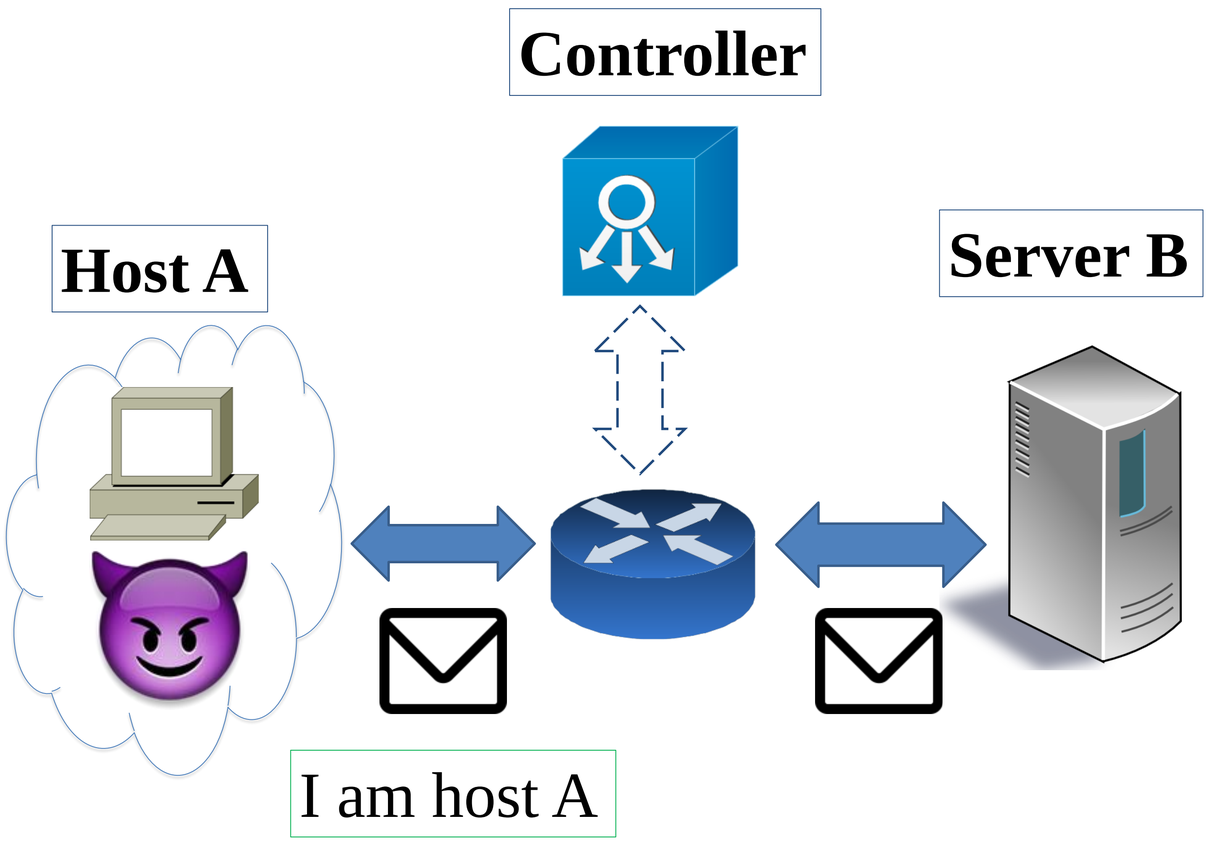
Resilient Architectures

Flow Reconnaissance via Timing Attacks on SDN Switches

Sheng Liu
UNC Chapel Hill
Mike Reiter
UNC Chapel Hill

SDN Timing Attack



Match Fields	Action	Timeout	Priority
Host A to Server B	Forward	100 s	2

Innovations & Uniqueness

- Timing attack:
  - use timing side-channel to make traffic analysis
- Switch Markov model considering:
  - rule expiration
  - rule eviction
  - rule dependency
- Select the optimal probe packet using information gain to maximize the expected accuracy of the attack

Technical Approach

- Raise awareness of this timing side-channel attack and try to build resilient system to defend against it.
- So far we have accomplished:
  - Using timing attacks to make traffic analysis
  - Building a switch Markov model considering rule timeout, rule eviction and rule overlapping
- Next step:
  - Build defense to mitigate this attack
  - Apply our model to other applications

Benefits & Deliverables

- Benefits:
  - Check if your system is vulnerable to this attack
  - Build defense to mitigate the attack
- Collaboration:
  - Data including flow statistics and policy configurations helps us demonstrate the efficacy of this attack and build defense
- Seeking other applications of the switch model, such as model checking or network performance optimization