NCSU Science of Security Lablet  
Transitional Relevance and Research Summary Statement

Name:  
Sheng Liu

Hard Problem Area:  
Resilient Architectures

Overall Research Goal(s):  
What do you ultimately hope to show with your research? This section can involve some jargon, but try to relate these goals to your broad impact section. Start with the larger goal(s) and narrow the scope towards your specific study (and specific goals, below).

The reactive operation of software-defined networking (SDN) switches gives rise to a timing side-channel in which an attacker can test for the recent occurrence of a target flow by judiciously probing the switch with forged flows. The goal of our research is to evaluate the effectiveness of this timing side-channel attack and build defense to mitigate it with reasonable overhead.

Broad Impact:  
Why is your research important? This section should avoid any technical jargon and should be meaningful to the general public. Try to keep this down to five sentences. This should be hierarchical: the broad impact decomposed into more specific impacts that connect your overall research goals to your more specific goals.

The move toward software-defined networking (SDN) is one of the dominant trends in the networking landscape today. As enterprises plan to adopt SDN, the top of mind issues are network security and user privacy. Security issue can cause disruption of network service or leakage of user privacy. In this work, we are trying to enhance the network security and protect the privacy of users to provide good quality of service.

Specific Research Goals:  
Lay out the steps you are going to take to achieve your overall research goal. You can get technical here.

- Develop a formal method to measure the information leakage exploited by this attack. This model needs to capture the practical challenges related to rule evictions to make room for other rules; rule timeouts due to inactivity; the presence of multiple rules that apply to overlapping sets of flows; and rule priorities.
- Propose an effective method to mitigate this attack without sacrificing too much performance. Specifically, the delay suffered by the flow needs to be minimized and the correctness of the policy should be guaranteed.
• Deal with the scalability issue of our proposed method. (Each switch can install over 1000 rules and there may be a large number of switches in the network.)

**Proposed Data Collection (if applicable):**
What data will you collect to answer your research goals? How will you collect it? Will it be an observational study, randomized comparative experiment, or simulation study? Include potential biases and be prepared to explain how the data will achieve your specific research goals.

Currently, we set up our simulation environment using Mininet (a virtual network tool) and the real-world Cisco router configurations from Stanford University’s backbone network. In the future, we plan to implement our protocol on real-world testbed.

**Success Criteria:**
How will you determine whether you satisfied your specific and overall research goals?

The effectiveness of our defense can be evaluated by conducting experiments on our simulation environment with and without the proposed scheme. The metrics include the accuracy of the attack and the delay suffered by the flows as a function of network size and distribution of flow occurrence.

**Anticipated Difficulties, Limitations, and Criticisms:**
What will make the above specific research goals difficult to achieve? How do you plan on dealing with these difficulties if they arise?

The major difficulties include:
• The practical challenges including rule evictions, rule timeouts, rule overlapping and rule priorities complicate our model to quantify the information leakage.
• To mitigate the information leakage, the controller may steer the system toward more coarse-grained rules, raising the question of the optimal balance between coarse-grained and fine-grained control.
• We should minimize the overhead, especially the delay suffered by the flows.
• The scalability of our system would be another limitation of our proposed protocol.