Security of Software-Defined Networking

Instructor: Mingming Chen

Email: mingc@ksu.edu

Website: https://mzc796.github.io/

Course Description
Software-Defined Networking (SDN) is a centralized network architecture for Next Generation Networks. This course explores the vulnerabilities of SDN, with an emphasis on the SDN control plane. Students will study well-established attack vectors—including race conditions, flow-entry misuse, replay-based topology poisoning, and DDoS—as well as strategies to fortify SDN controllers and networks against such threats. The course combines research-driven discussions with hands-on labs using **OpenDaylight**/**ONOS** **and** **Mininet**, enabling students to reproduce canonical attacks and experiment with defenses.

Topics Covered

- SDN architecture, threat model, and attack surfaces
- SDN controller vulnerabilities: race conditions, datastore semantic gap, synchronization breaches, cross-app interference, flow entry-induced topology poisoning
- Flow and packet manipulation: buffered packet hijacking, flow-entry conflicts, link fabrication
- Direct attacks: relay/replay topology poisoning, spoof-based poisoning, DDoS on the control plane
- Case studies from recent research (CCS, USENIX Security, NDSS, S&P, SIGCOMM, etc.)
- Fortification strategies: secure discovery, application isolation, anomaly detection, controller hardening

---

Learning Outcomes

By the end of this course, students are expected to:

1. Be familiar with the SDN architecture and related concepts
2. Analyze the security vulnerabilities of SDN control and data planes.
3. Reproduce representative SDN attacks in a simulated environment.
4. Design and test defense mechanisms to improve resilience.
5. Critically review and present research papers on SDN security.

6. Apply lessons from SDN security to broader programmable networking and CPS contexts.

Course Structure

- **Lectures & Discussions** (concepts, research papers)
- **Labs** (guided SDN attacks/defenses using OpenDaylight + Mininet)
- **Seminars** (student-led paper presentations)
- **Final Project** (design/implement an SDN attack or defense prototype)

Evaluation

- Labs (30%)
- Paper Presentations (30%)
- Final Project (30%)
- Participation (10%)

AI Policies

AI tools are encouraged in this course. Part of the course evaluation is based on how students interact with AI, including how they ask questions, refine prompts, challenge results, and validate conclusions.
