Re-thinking Network Security in the Presence of Unknown Network Elements

Soo-Jin Moon
4th year Ph.D. Student
Carnegie Mellon University
Advisor: Vyas Sekar
Research Area: Network Security
A Vulnerable Network!

Networks: explosion of **unknown network elements** → leave **gaps for attacks**
A Vulnerable Network!

Networks: explosion of unknown network elements → leave gaps for attacks

Motivating Question

How do we secure networks composed of network elements whose security implications are unknown?
Methodologies

- Automatically infer behavioral models (e.g., state machine)
- Automatically discover potential attack vectors
Methodologies

- Automatically infer behavioral models (e.g., state machine)
- Automatically discover potential attack vectors

From black-box observations
Vision: Black-box Approach to Network Security

Purposes

• Automatic patching
• Verification and testing
• Understand adversaries’ capabilities ➔
Proactively mitigate adversaries from inferring the system

End-user devices  Network functions  Applications

Limited access to code / binary
My Work

Inferring the behavioral models of network elements
• Alembic: Black-box Model Inference for Stateful Network Functions.  
  (Under submission)

Discovering potential attack vectors
• AmpMap: Map of Amplification-Inducing Queries to Network Servers.  
  (In preparation)