A Framework to Find Vulnerabilities Using State Characteristics in Transport Protocol Implementations

Samuel Jero, Hyojeong Lee, and Cristina Nita-Rotaru
Department of Computer Science, Purdue University

Motivation
- Transport protocols
  - Responsible for end-to-end communication
  - e.g. TCP, provides reliability, ordering, and fairness
  - STCP, QUIC, etc.
- Many versions and implementations of each protocol
- Testing Models
  - Ignores implementation details
  - Misses implementation bugs
- Testing Implementations
  - Ad-hoc, manual, incomplete testing
  - Numerous bugs and vulnerabilities remain

Design Approach
- Capturing realism: test unmodified implementations
- Malicious / abnormal behaviors
- Collected from previous studies regarding attacks
- Conducted by modifying or injecting messages
- Mitigating state-space explosion problem
- A general framework
  - Not limited to a specific target
    - environment / implementation / protocol

Turret-T Architecture
- Based on Turret, a platform to find attacks in distributed systems
- Runs unmodified target system in virtual machines
- Virtual machines connected with network emulator
- Malicious proxy intercepts packets and inject actions in network emulator
- Controller guides search
- Leverage state information

State Information Leverage

Automated State Classification
Classify states based on observable characteristics through learning phase e.g. time spent, throughput, etc.

State-based Malicious Action Injection

Protocol State Tracking

Insights
- Automatically inject malicious/abnormal behaviors and observe the result without altering the target code or environment
- Reduce the search space and find effective attacks