SaTC: CORE: Small: Hardening Systems Against Low-Rate DDoS Attacks

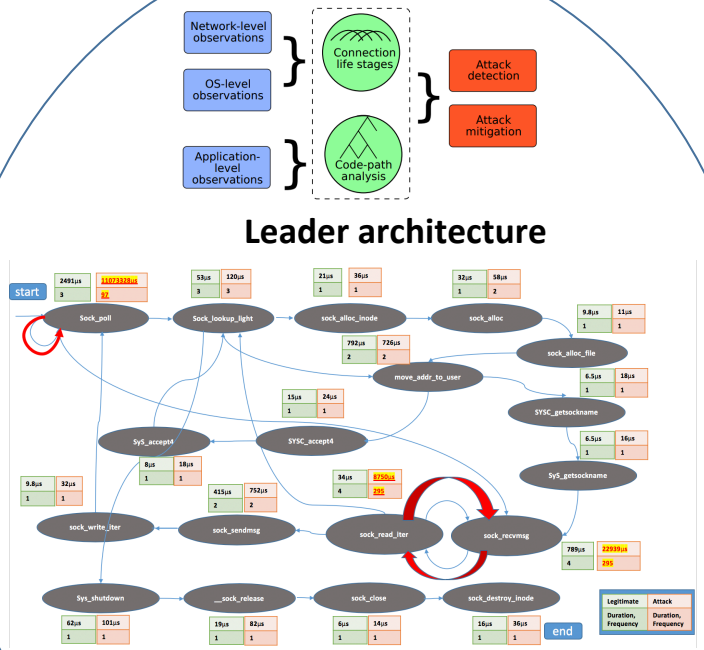
USC Viterbi School of Engineering Information Sciences Institute

Challenge:

- Low-rate DDoS attacks are hard to detect and mitigate
  - Many attack variants
  - Many point solutions
  - Low rate, no network anomaly
- Insight: All these attacks use victim's resources in unexpected ways
  - Abnormal resource usage can signal attacks

Solution:

- Novel combination of runtime system profiling and offline code analysis to reason about resource behavior
  - Characterize legitimate usage
  - Detect anomalous usage
  - Terminate connections or blacklist anomalous sources



Leader architecture

Connection life diagram showing differences in legitimate and attack connections

Scientific Impact:

- Our innovations harden any host against current and future low-rate DDoS
- Learning about application's resource usage is useful to detect bottlenecks and performance problems beyond DDoS

Broader Impact:

- Our solutions will make online services robust against low-rate DDoS
- Our solutions apply to any application that runs on Linux
  - Portable implementation via system tap
  - We will release our code as open source
- Lecture models and practical exercises will be shared via DeterLab testbed

USC Information Sciences Institute
Pis: Jelena Mirkovic and Christophe Hauser
Lead students: Rajat Tandon and Nicolaas Weidemann

Award # 1815495