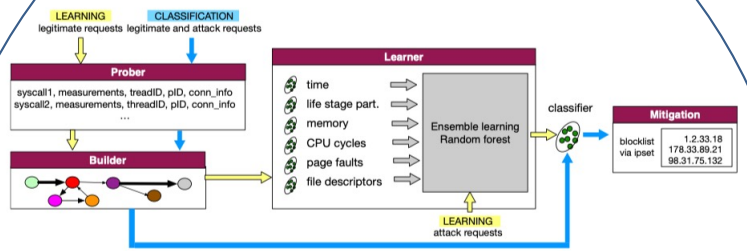
SaTC: CORE: Small: Hardening Systems Against Low-Rate DDoS Attacks

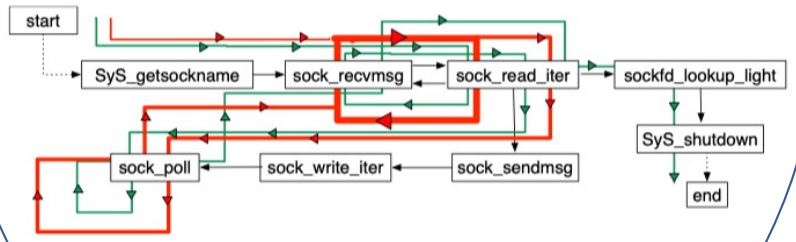
USC Viterbi School of Engineering Information Sciences Institute

Challenge:

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



Leader architecture



Connection life diagram showing differences in legitimate and attack connections

Solution:

- Monitor resource usage per application and per connection in Linux kernel
  - Learn legitimate usage patterns
  - Detect anomalous usage, and block anomalous sources

Scientific Impact:

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

Broader Impact and Broader Participation:

- Make online services robust against low-rate DDoS
- Application and attack agnostic
- Code released on Github https://github.com/STEELISI/LEADER
- Two practical exercises for teaching about low-rate DDoS are shared via DeterLab testbed

USC Information Sciences Institute

Pis: Jelena Mirkovic and Christophe Hauser

Students: Rajat Tandon, Nicolaas Weidemann, Haoda Wang, Tyler Kann

Award # 1815495