Hardening Systems Against Low-Rate DDoS Attacks

Low-rate denial-of-service (LRD) attacks deny service by depleting some limited resource at the end host or a network device. This makes the device unable to process legitimate clients' traffic. Since LRD attacks are very low-rate, they are challenging to detect and handle at the network level. This makes the attack traffic a needle in a haystack of legitimate traffic. On the other hand, detecting LRD at application would require changes to many applications, and would only be effective against specific attack variants.

This effort will develop, implement and evaluate the *Leader* defense. Leader will build profiles that describe how external requests, clients, applications and the entire device use system resources. These profiles, called "connection life stages," contain information about the type and the amount of the resource used, the order in which the use occurs, and the time that each chunk of resource is being held. Leader compares instantaneous profiles to baseline profiles at connection, client, application and device level to detect denial of service and identify the resources being affected. Leader further uses connection life stages to perform anomaly detection, which is used for attack diagnostics and mitigation. In rare cases when the profiles do not show anomalous use of resources, or cannot attribute it to specific connections or clients, Leader resorts to offline binary analysis of affected applications. This analysis helps us understand how code paths in the application use system resources and identify possible code changes to increase robustness to LRD attacks. Leader defense is implemented as an OS module, and thus protects the deploying device against all LRD attacks at the OS and the application level.