Detecting Application-layer Denial-of-Service Attacks In-Flight with FineLame

Henri Maxime Demoulin, Isaac Pedisich, Nikos Vasilakis, Vincent Liu, Boon Thau Loo, Linh Thi Xuan Phan

University of Pennsylvania

ATC 2019
An asymmetry problem

TLS renegotiation

Server does 10x more computation than the client!

We need to monitor per-request, in-flight and automated.
Finelame

Stack

- application
- User-space libraries
- Kernel-space libraries

Finelame

- Request mappers
- Resource monitors

Shared data structures

- PID → Request ID (RID)
- RID → <resource usage>
- RID → outlier score
- Model parameters

Anomaly detection engine

Gather training data

Share model parameters
See you at ATC!