FRADE: Flash cRowd Attack DEfense


Dr. Jelena Mirkovic
mirkovic@isi.edu

Dr. Genevieve Bartlett
bartlett@isi.edu

Brandon Paulsen
pauls658@d.umn.edu

Jaydeep Ramani
jramani@isi.edu

Abhinav Palia
palia@usc.edu

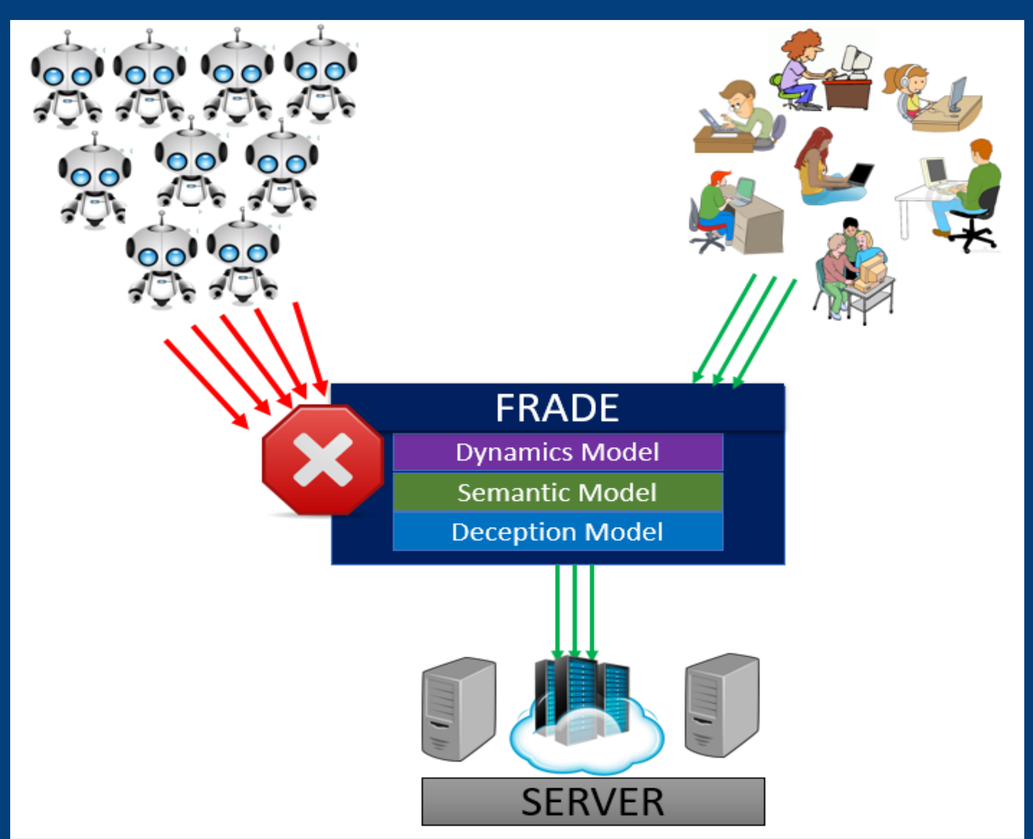
Rajat Tandon
rajattan@usc.edu

Flash Crowd Attack(FCA) is a DDoS attack that consumes the resources of a targeted service with legitimate-looking service requests generated by numerous bots. Flash-crowd attacks are hard to detect as bots request for genuine content. Attacker may further employ many bots, each sending requests at a low rate.

Problems with the existing defense methods:

- **CAPTCHAs**: annoying to humans, and can be defeated by machine learning
- **Request rate limiting**: not useful as FCA uses many bots, each generating a low-rate stream of requests
- **Feature-based detection**: high false positive and false negative rate
- **Decoy hyperlinks**: ineffective against bots that analyze the page's source

FRADE is a defense mechanism against the Flash Crowd Attacks which differentiates authentic users from bots. Bots are blocked and the targeted system runs smoothly, even in the presence of the attack.



FRADE models three different aspects of human interaction with application-level content to distinguish humans from bots: request dynamics, request semantics and how humans process visual cues. While bots can trick FRADE's models, they must severely reduce their request output. This forces attackers to use orders-of-magnitude larger botnets for a successful attack.

FRADE Models:

Dynamics Model (DYN): Models the **dynamics** of user-server interaction. There are three sub-models:

- DYN1 – models rate of requests for click-content
- DYN2 – models rate of requests for embedded content
- DYN3 – models rate of costly requests

Each model learns the rate in specific time windows from service logs containing mostly legitimate clients. If these thresholds are exceeded the model flags the client as bot.

Semantic Model (SEM): Models the **sequences of requests** by client, i.e., how humans navigate through server content. While humans follow semantically logical browsing patterns, bots request links randomly. We learn probabilities of request sequences from service logs, and flag clients that generate low-probability sequences as bots.

Deception Model (DEC): We embed decoy objects, such as overlapping images, into Web pages. These objects are invisible to human users but visible to bots. We take special care to make these objects similar to the real objects in the page's source code.

Current Status:

- Dynamics, semantic and deception models are implemented.
- Developed smart bots to launch FCA on three of our mirror websites (Imgur, Wikipedia, Reddit) to test our defense strategy
- Running a user study and preparing a publication:
  - We launch distributed smart bot attacks on mirror websites and measure objective and subjective service quality

Next Steps:

- Measure and improve scalability of FRADE
- Investigate how to extend the FRADE's semantic model to protect sites with personalized content (e.g., social networks)
- Investigate how to extend FRADE to other services, such as DNS

Interested in meeting the PIs? Attach post-it note below!

http://steel.isi.edu/projects/frade

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

Information Sciences Institute
STEEL Security Research Lab@ISI
USC University of Southern California