SaTC: CORE: Small: Towards Label Enrichment and Refinement to Harden Learning-based Security Defenses

Gang Wang, University of Illinois at Urbana-Champaign
Xinyu Xing, Northwestern University

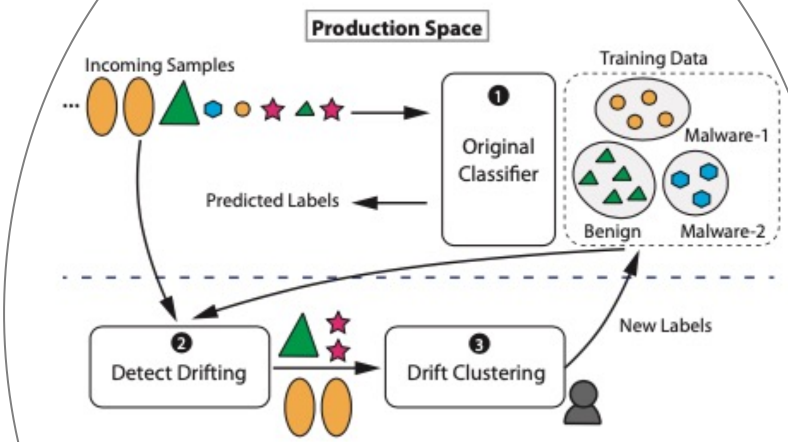
Challenge:

- A learning-based security system often performs worse over time
- **Concept drift** caused by behavior changes from both benign and malicious players

Solution:

- Self-supervision + domain-specific insights: obtain supervision from the data itself
- Proactively detect drifting samples
- Enrich/refine noisy labels for higher-quality labels

Project #: CNS-2055233
Contact: gangw@Illinois.edu
https://gangw.cs.illinois.edu



Concept drift detection and drift analysis for dynamic model updating

Example applications:
- Malware detection
- Bot detection

Scientific Impact:

- New methods and tools to measure, characterize concept drift for learning-based malware detection systems
- Harden malware classifier training against concept drift

Broader Impact and Broader Participation:

- Technology transfer working with industry partners (Blue Hexagon, IBM)
- New course, summer REU projects
- Mentor underrepresented students