SAND2022-9443C

# The Center for Cyber Defenders

Expanding computer security knowledge

# Malware Detection and Domain Adaptation

Akul A. Goyal – UIUC, Ph.D. Cybersecurity, May. 2024

**Manager: Tiawna L. Cayton 056831, Mentor: Michael R. Smith 05552**


## Problem Statement:

- Static malware analysis provides a powerful tool to security analysts in detecting intrusions
- Out-Of-Distribution (OOD) malware families and adversarial perturbations hinder the effectiveness of static malware analysis
- Domain Adaption/Generalization cannot handle different class families between distributions

## Objectives and Approach:

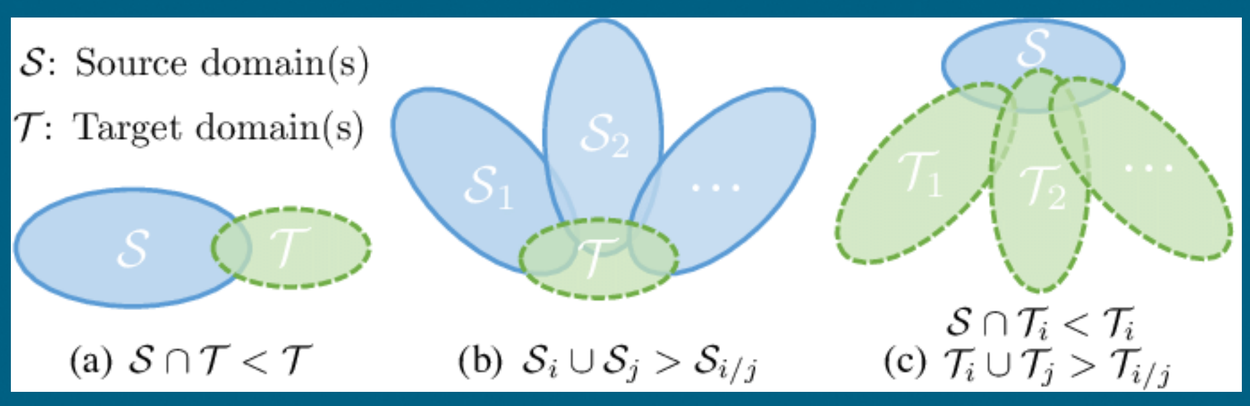
- Use Domain Adaption/Generalization to create a robust static malware classifier
- Proposed Steps:
  - Curate Two Datasets:
    - OOD malware families
    - Adversarial perturbed malware families
  - Use Domain Generalization on adversarial perturbed malware families
  - Use Domain Adaptation on OOD malware families
- Report results

## Results:

- OOD Malware Families:
  - Match families between source and target distribution using multi-class labels
  - For static malware – multi class labels are binary labels indicating whether malware behavior exists or not
- Adversarial Malware Families:
  - Curate dataset of 3 different adversarial attacks
  - Use Domain Generalization to learn invariant features on 2 adversarial families and unperturbed malware family, test against 3rd adversarial attack

## Impact and Benefits:

- By creating a more robust static malware classifier, attackers are less likely to evade detection




Qiao, Fengchun, Long Zhao, and Xi Peng. "Learning to learn single domain generalization." *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2020.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.