Evaluating Evasion in Network Intrusion Detection Systems

Three-Phase Project Summary

Miguel Pinto Mátyás Szikra Ahmed Lotfy

May 4, 2025

Phase 1: Initial Modeling

- Dataset selected: CICIDS2017
- Trained Isolation Forest for unsupervised anomaly detection
- Aimed for high recall while maintaining class balance
- Unsupervised model underperformed on real traffic
- Switched to Random Forest (supervised)
- Performed initial tuning and evaluation

Reference: Liu et al. (2012) – Isolation-Based Anomaly Detection

Phase 2: Real Traffic Generation

- Deployed two VMs: victim and attacker
- Generated low-and-slow `nmap` attack traffic
- Collected realistic benign traffic in controlled setup
- Some additional synthetic samples used
- Custom scripts extracted CIC-style features
- Data exported as labeled CSV files

Reference: Ring et al. (2018) – Detection of Slow Port Scans in Flow-Based Network Traffic

Phase 3: Adversarial Evaluation and Tuning

- Real data used to further tune the supervised model
- Designed and tested:
  - Whitebox attacks
  - Greybox attacks
  - Blackbox attacks
- Integrated strongest evasive samples into retraining
- Created a final optimized blackbox attack
- Final model tested for robustness

Reference: Yazdanpour et al. (2023) – Adversarial Evasion Attacks in NIDS

Team Contributions

- **Ahmed Lotfy**: Led Phase 1. Selected CICIDS2017 dataset, trained Isolation Forest and Random Forest models, and performed initial tuning and validation.
- **Mátyás Szikra**: Led Phase 2. Built traffic environment with VMs, generated low-and-slow `nmap` scans, captured benign traffic, and extracted CIC-style features.
- **Miguel Pinto**: Led Phase 3 and served as team lead. Designed and executed whitebox, greybox, and blackbox evasion attacks, retrained the model with evasive samples, and coordinated the project.

Thank You!

Project repository: `github.com/mcpinto0608/data_sec_project.git`