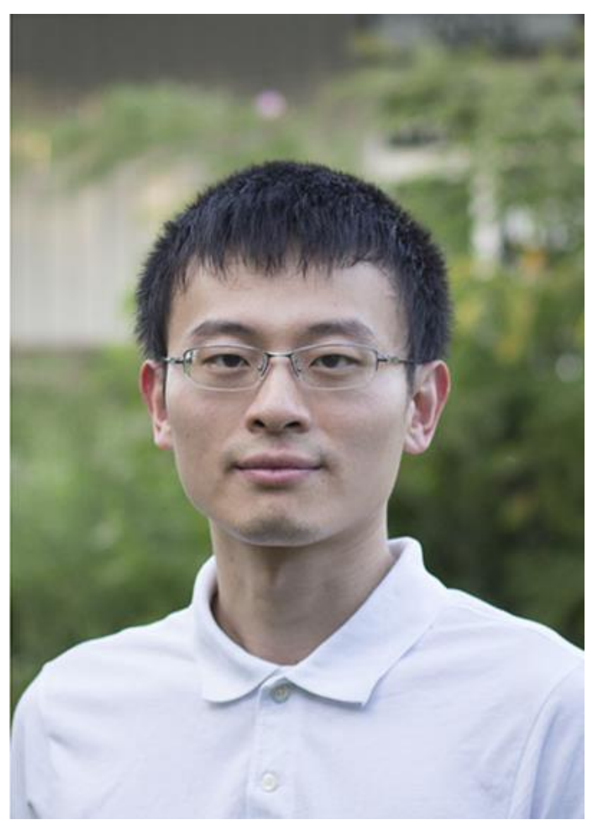
SaTC: CORE: Small: Deep Learning for Insider Threat Detection

Shuhan Yuan   Utah State University   shuhan.yuan@usu.edu

https://yuan.shuhan.org/projects/2021_insider/



Introduction

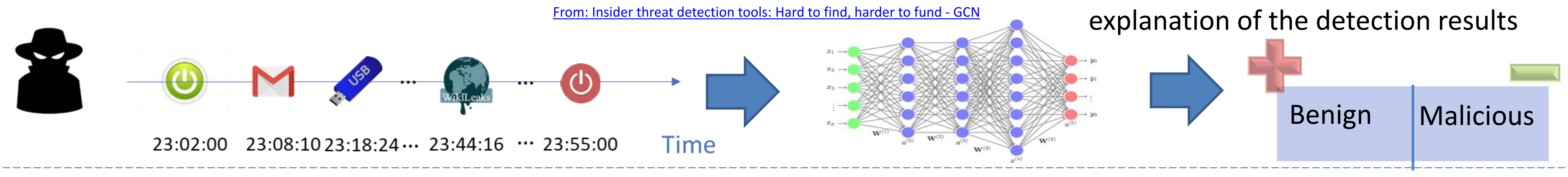
What are the malicious insiders?

- malicious people within organizations who abuse their authorized access in a manner that compromises the confidentiality, integrity, or availability of the organization's information or information systems. [CMU CERT]

From: Insider threat detection tools: Hard to find, harder to fund - GCN

Goal of this project

- is to develop a deep learning framework that can detect malicious sessions with subtle and adaptive activity changes from insiders by leveraging the limited malicious samples and further identify malicious activities from the detected malicious sessions in order to provide an explanation of the detection results



Challenges

I. Extremely Unbalanced Data
   - Malicious activities from insiders are extremely rare in real-world scenarios

II. Subtle Activity Changes
   - Attacks from insiders are subtle and hard to notice

III. Adaptive Activity Changes
   - Increasing the sophistication, scale, and speed of their attacks to evade detection

IV. Fine-grained Insider Threat Detection
   - Limited information at the activity level

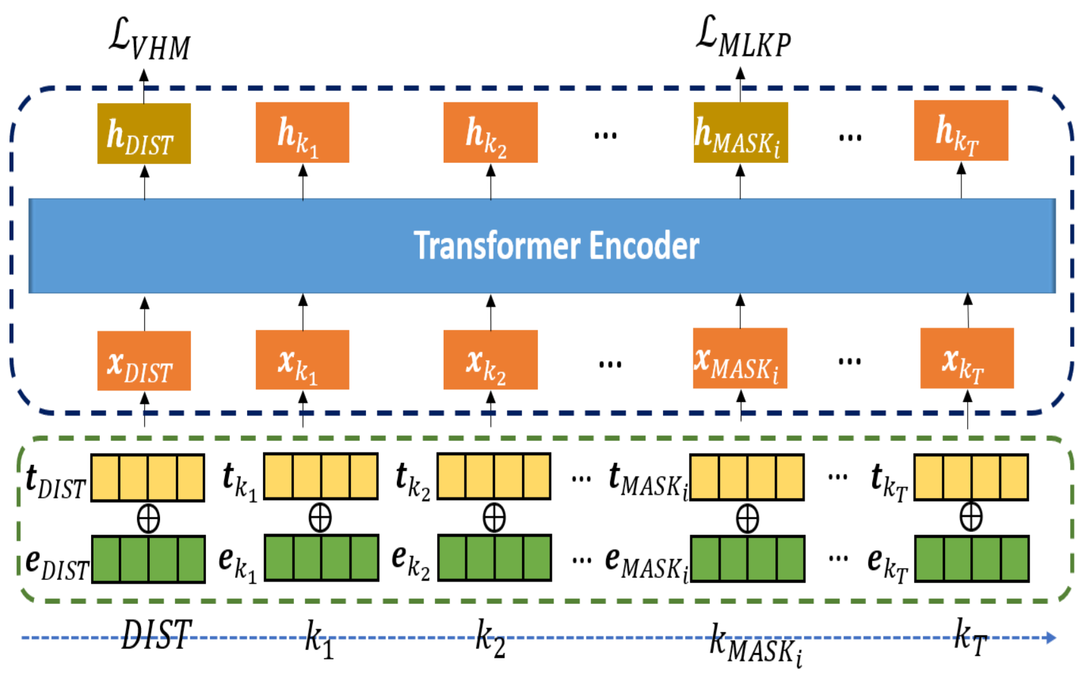
Scientific Impact

The developed approaches can be adapted to the broader tasks of fraud detection.

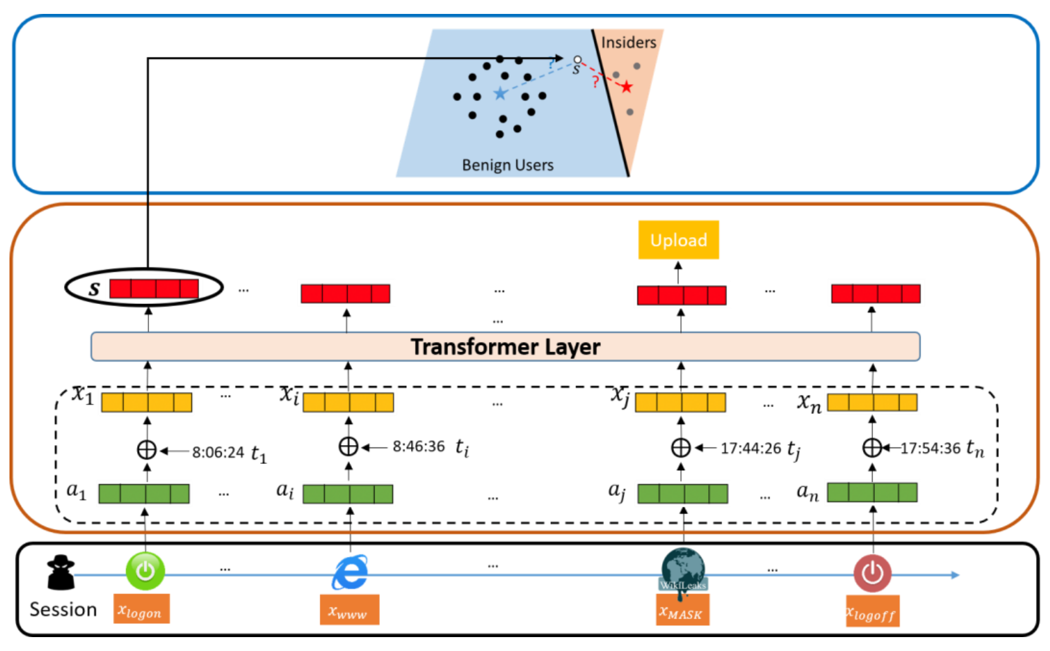
- Capture complicated activities from fraudsters without using any labeled data
- Detect subtle malicious activities via disentangled representation
- Identify adaptive attacks from fraudsters via reinforcement learning
- Interpretable fraud detection

Solutions

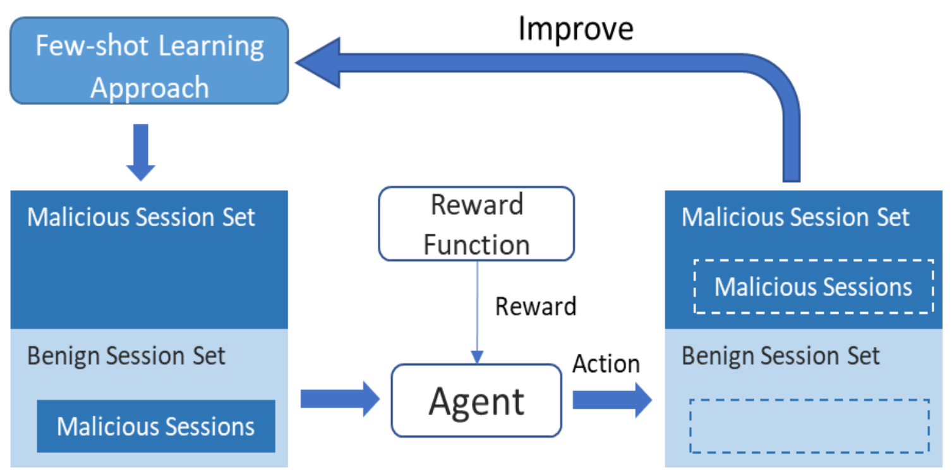
I. Self-supervised Representation Learning



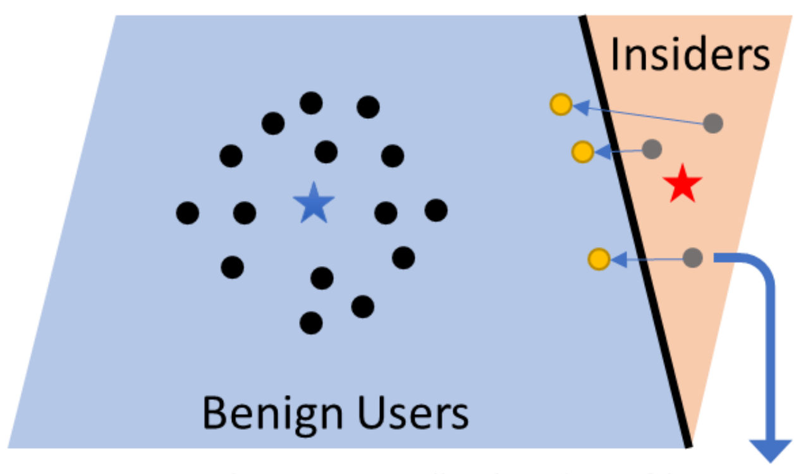
II. Few-shot Insider Threat Detection



III. Adaptive Detection via Reinforcement Learning



IV. Counterfactual Explanations



- *Remove the activity "uploading files to wikileak.org"*

Broader Impact on Society

- Benefit to industries and governments who are frequently under attack from malicious attacks
- Potentially promote collaboration between researchers, industries, and governments.
- Adapt to achieve fraud detection, leading to a broader application with broader participants

Broader Impact (Education)

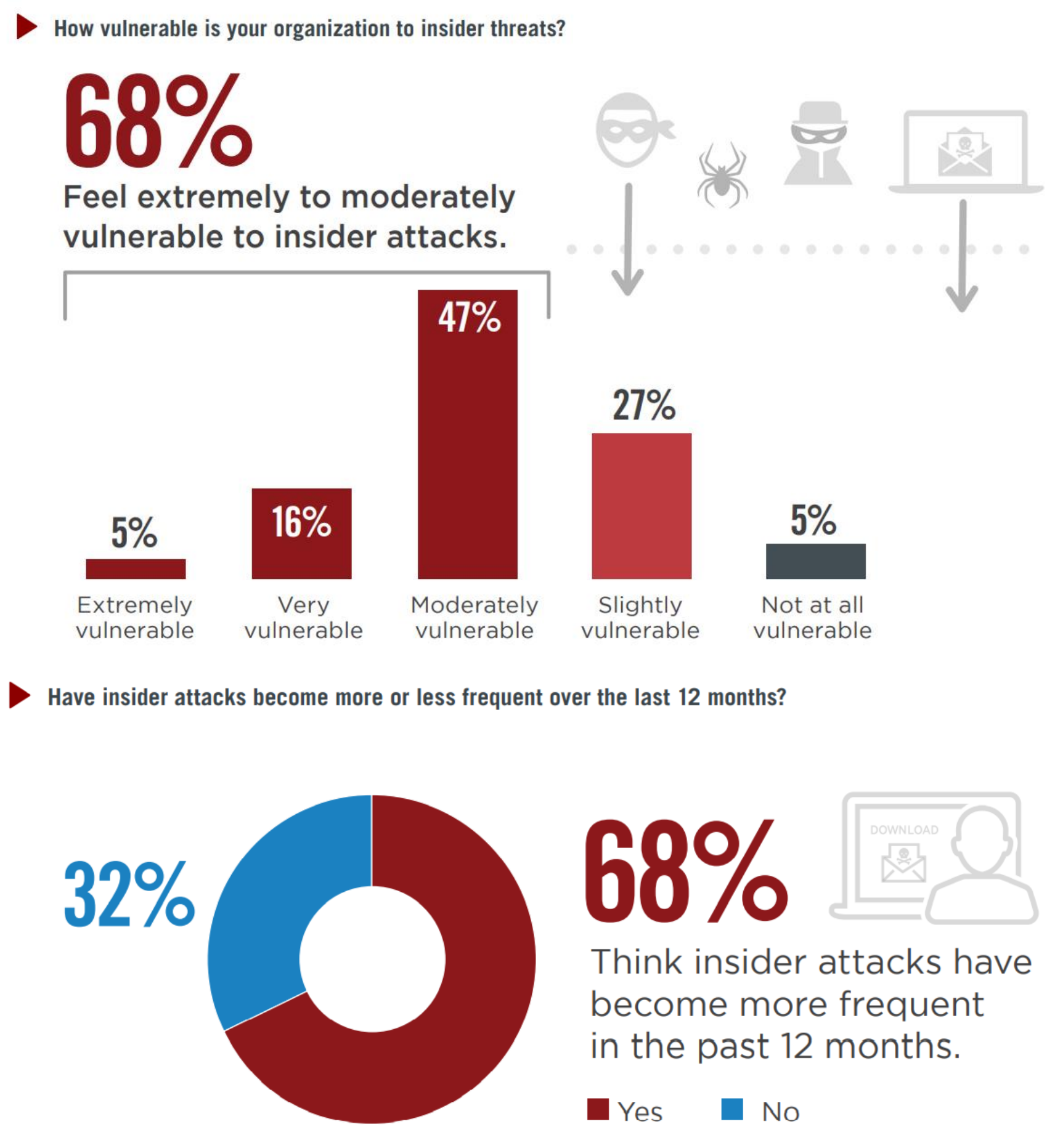
Integrated with coursework

- Course Topic
- Course Project
  - Dataset
  - Algorithms

Date Range	516 days
Normal Users	3995
Insiders	5
# Device Events	1,511,828
# Email Events	10,994,957
# File Events	2,014,883
# HTTP Events	117,025,216
Malicious Events	428
Threat User-Sessions	68

CERT Insider Threat Dataset

Broader Participation



How vulnerable is your organization to insider threats?

68% Feel extremely to moderately vulnerable to insider attacks.

Have insider attacks become more or less frequent over the last 12 months?

68% Think insider attacks have become more frequent in the past 12 months.

Source: 2020-Insider-Threat-Report-Gurucul.pdf (cybersecurity-insiders.com)

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting)
June 1-2, 2022 | Arlington, Virginia