Course Introduction

This course will study the use of machine learning for cybersecurity applications. Many security applications have large amounts of data related to the system and adversarial actions. Our ability to identify the type of machine learning algorithms that are useful for specific security applications can help us to improve the defense against attacks and also anticipate the potential attack variants that may arise in the future. Even when one does not know the type of attack, if the machine learning algorithms can identify any anomaly, then the next level of security checks can be performed by other means or experts.

But nothing comes in life for free, and this holds for machine learning in the context of cyber too! Another point to remember is, "Beware of what you add to your tool bag! You may have an adversary manipulating your machine learning itself." This leads to adversarial machine learning, where the machine learning could be tricked into failing the detection!

Attacks on Google Video, Toxic Comments, and Google Vision are some of the fun examples where simple modifications make the machine learning algorithms fail!

We will start with setups where machine learning will be helpful in cybersecurity. As indicated in the course title, it will be a hands-on course on applying machine learning to cybersecurity applications. Machine learning algorithms will be introduced as needed.

Lectures

1. Introduction to Machine Learning (ML) for CyberSecurity
2. Email Spam Detection using Supervised Learning (**Scheduled Release of Homework #1**)
3. Knocking down CAPTCHAs
4. Efficient Network Anomaly Detection Using k-means (**Scheduled Release of Homework #2**)
5. Use of NLP for Instruction Set Architecture Identification
6. Malicious Event Detection with Decision Tree **(Scheduled Release of Homework #3)**
7. Catching Impersonators and Hackers Red Handed
8. Financial Fraud and How Deep Learning can Mitigate It
9. Adversarial Machine Learning
10. Student presentations of Course Projects

Textbook

Hands-On Machine Learning for Cybersecurity by Soma Halder and Sinan Ozdemir; Packt Publisher. You can read it online and links it to an external site. [packtpub.com] for free with your UW NetID. Alternatively, you can obtain physical copies from the UW library or University bookstore.

References

1. ***AI for CyberSecurity by Alessandro Parisi; Packt Publishers***
2. ***Machine Learning for Cybersecurity by Chiheb Chebbi; Packt Publishers***
3. ***Machine Learning for Penetration Testing by Emmanuel Tsukerman; Packt Publishers***
4. ***Adversarial Machine Learning by Vorobeychik and Kantarcioglu; Morgan and Claypool Publishers***

Labs

Throughout the course, we will have eight labs, during which you will learn and practice various machine-learning algorithms and use them to solve cybersecurity problems. Below is a tentative schedule for all lab sessions:

1. Python basics review and introduction of typical data analysis libraries
2. Machine learning pipeline for cybersecurity problems
    - Case study: spam email detection
3. A small step into deep learning and convolutional neural network (CNN)
    - Case study: breaking Captchas with neural network
4. Dimensionality reduction and data visualization
    - Case study: network anomaly detection and visualization
    - Dataset: KDD Cup 1999 dataset (We will reuse these in lab 6)
5. Autoencoder and clustering algorithm
6. Data oversampling and decision tree algorithm
    - Case study: detecting and categorizing network attacks
    - Dataset: Kaggle credit card fraud detection dataset (We will reuse these in lab 8)
7. Ensemble learning

Homeworks / Project

We plan to have three homework throughout the whole course. Throughout the quarter, you will also get the chance to form groups with others to work on a course project **we may suggest, or your team could suggest. We won't have any homework in the last two weeks so you can focus on the project**.

Grading

- Homework: 45% (15% each)
- Project: 55%
    - Proposal: 5%
    - Checkpoint report: 10%
    - Final presentation: 15%
    - Final report: 25%

Course Announcements and Discussions

- Announcements
    - We will post course announcements and updates to Canvas and the class mailing list These announcements will also be forwarded to the Slack workspace used by this course (see below).
- Discussions – Slack
    - We will use Slack workspace PMP-595-W-2023 for the course discussions. Feel free to use this Slack to post your questions on the course material, lectures, homework, and projects or answer the assigned questions if you can help. Instructors and TAs will also answer these questions promptly.
    -

Course Policy

- Please complete the homework by yourself and only copy code from others or the internet with an understanding of what it is doing.
- You are encouraged to discuss lab and homework content with your classmates offline and on the discussion board. However, please limit your discussion to ideas and not share the code. Specifically, do not copy-paste any homework answers into the discussion board.
- Please submit homework and project materials online by the posted due date. Throughout the quarter, we will provide you with 6 late-day credits for the three homework, which you can use to submit one or more assignments without penalty. If you have used all six days, however, each additional late day will result in a 20% penalty in the corresponding homework.
- Please submit project reports and presentations on time. The project does not have any credit days, as there is a UW deadline for submitting the grades shortly after the final exam week.

- Washington state law requires that UW develop a policy for the accommodation of student absences or significant hardship due to reasons of faith or conscience or for organized religious activities. The University of Washington policy, including information about requesting accommodation, is available at Faculty Syllabus Guidelines and Resources. Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form available at https://registrar.washington.edu/students/religious-accommodations-request/Links to an external site.

See you all in EE PMP 595 course in Winter 2023.