EEP 567 2026: Machine Learning for Cybersecurity

Course Information

Class will meet in person **every Wednesday from 6:30 pm to 9:30 pm**, with Zoom meetings available.

Classroom: ECE 269

Zoom link for instruction:

Join the **Course Slack** for updates and Q&As

Instructor: Prof. Radha Poovendran (rp3@uw.edu)

Instructor Office Hours: By appointment and via Zoom

TAs: Qifan Lu and Kyle Zheng

TA Office Hours (Tentative): Online, **every Monday and Saturday from 6:30 pm to 8:30 pm**

Zoom link for TA Office Hours:

Course Introduction

ML4Cyber AI Buddy link is here: https://tinyurl.com/ML4Cyber-AI-Buddy-2026

This course will study the application of machine learning to cybersecurity. Many security applications have large amounts of data related to the system and adversarial actions. Our ability to identify the types of machine learning algorithms useful for specific security applications can help us improve defense against attacks and anticipate potential attack variants. Even if one does not know the type of attack, if machine learning algorithms can identify an 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 model can be tricked into failing at detection!

Attacks on Google Video, Toxic Comments, and Google Vision are fun examples of simple modifications that cause machine-learning algorithms to fail!

With the advent of transformers and LLMs, new opportunities for defenders and attackers have emerged. Throughout the course, we will examine some of the materials.

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 CAPTCHA
4. Transformers in CyberDefense (**Scheduled Release of Homework #2**)
5. Efficient Network Anomaly Detection Using k-means
6. Use of NLP for Instruction Set Architecture Identification from Binaries **(Scheduled Release of Homework #3)**
7. Malicious Event Detection with Decision Tree
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 at UW Library or on an external site for free with your UW NetID. Alternatively, you can obtain physical copies from the UW library or the University bookstore.

Intelligent Course Buddy

Professor Poovendran has developed **an intelligent course buddy** powered by Generative AI for each of you to use for the course. The AI assistant is powered by ChatGPT-4o, has full knowledge of the course lectures and can help students enhance their learning experience. The style is Socratic, so it is interactive learning rather than giving you a final answer. Start your co-learning with the course buddy here.

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 where 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 a convolutional neural network (CNN)
    - Case study: breaking Captchas with a 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 the 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

We will release the student version of the lab notebooks before each class. Each notebook will contain **a number of TODOs which you will complete in the lab session in class**. You must then **submit your notebook on the same day between 9 pm and midnight**. We will **grade your submission and assign 2% of the scores** for each lab to assess your overall class attandance throughout the quarter.

Assignments / Project

We plan to have three homework assignments throughout the course. Throughout the quarter, you will also get to form groups with others to work on a course project **we may suggest, or**

your team could suggest. See the Course Project Page for ideas, requirements, and details. **We have had no homework in the last two weeks so that you can focus on the project**.

Grading

- Homework: 45% (Three with 15% each)
- Labs: 16% (8 lab submissions with 2% each)
- Project: 39%
    - Proposal: 5%
    - Checkpoint report: 10%
    - Final presentation: 10%
    - Final report: 14%

Course Announcements and Discussions

- Announcements
    - We will post course announcements and updates to the **class mailing list** multi_eep567a_wi26@uw.edu. These announcements will also be forwarded to **course Canvas** (here) and **Slack** (see below for the link to join).
- Discussions – Slack
    - We will use Slack workspace "**eep-567-2026**" for course discussions. Feel free to use this Slack channel to post questions about the course material, lectures, homework, and projects, or to answer questions from others if you can help. Instructors and TAs will also promptly answer these questions.
    - **Join the course Slack: https://tinyurl.com/ML4Cyber26Slack**

Course Policy

- Please complete the homework yourself and do not copy code from others or the internet without understanding what it does. Suppose your homework is identical to others or any sample code snippets online; in that case, you will receive zero scores, and we must report it to the College of Engineering.
- You are encouraged to discuss lab and homework content with your classmates offline and on the discussion board. However, please **limit the scope of your questions** and avoid discussing the answers directly. Specifically, **do not copy and paste any homework answers** into the discussion board.

- You can use AI RAG assistants such as ChatGPT for help. In this case, you should **acknowledge using an AI assistant**. Again, you should **not copy and paste the response from the AI assistant**. But beware that LLMs are error-prone, as they are statistical and lack certification for all reactions.
- You must submit homework and project materials online by the posted due date. Throughout the quarter, **we will provide you with six late-day credits for the three homework assignments,** which you can use to submit one or more homework assignments without a penalty. Once you have used all six days, each additional late day will result in a 20% penalty on the corresponding homework.
- You must submit project reports and presentations strictly on time. **Any overdue project materials will receive a score of 0**. The project has no credit days.
- 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/.