The ”Mathematical Aspects and Applications of Modern Cyber” course’s final project’s guidelines

Teddy Lazebnik

3.3.2023

This document outlines the objectives of the project and how it will be evaluated. It is short as I give you as much space to be creative with your projects as possible.

The Task

The task is simple - write in English a 1200-6000 word document summarizing an academic paper about the mathematics of cybersecurity. You can either pick one, send me an email and get it approved or choose one from the list below. Please try to make sure you do not pick the same paper as other members of the course.

Document guideline

The report should be structured as follows, and answer the questions below. **Structure**: Title, authors, abstract (up to 150 words), introduction, related work, paper review, conclusion and applications, references. You can change it if you have a good reason. The Introduction outlines shortly the relevance of the reviewed work, the main reported outcome, its place in the field, and any additional points you feel are important for the reader before the main part of the body. The related work section includes **other** works (not the reviewed work) and their connection to the reviewed work. The idea is that you shortly tell the reader what is the more general context of the work in the field. The paper review section is just the review - this should be the longest section. Make sure you answer the main questions such as the novelty of the work, the objective it has, what methodology it uses, what are the main results, and how one can use its outcome in practice. Finally, the conclusion and application section in your own thoughts and ideas on how **you** or anyone else can use the new knowledge of the reviewed paper to solve **similar** objectives. The last section is your real place to be creative and extend the scope and improve the quality of the work.

Make sure you properly cite the relevant references in the document. Of note, less than 10 references will be strange... This is not ”a must” but think about it.

Possible Papers for Review

You can choose automatically all the papers that met one of the following categories:

- Anything after 2010 from *Computers and Security.*
- Anything after 2019 from *Security and Communication Networks.*
- Anything after 2015 from *Journal of Cybersecurity.*
- Anything after 2016 from *Journal of Information Security and Applications.*
- Anything after 2020 from *Journal of Computer Virology and Hacking Techniques.*

In addition, some specific papers that you can use:

- Dynamic Extraction of Initial Behavior for Evasive Malware Detection - `https://www.mdpi.com/2227-7390/11/2/416`

- Detection of Unknown DDoS Attack Using Reconstruct Error and One-Class SVM Featuring Stochastic Gradient Descent - `https://www.mdpi.com/2227-7390/11/1/108`
- Design and Evaluation of Unsupervised Machine Learning Models for Anomaly Detection in Streaming Cybersecurity Logs - `https://www.mdpi.com/2227-7390/10/21/4043`
- Scalability of k-Tridiagonal Matrix Singular Value Decomposition - `https://www.mdpi.com/2227-7390/9/23/3123`
- Home Cryptographic Hardware and Embedded Systems — CHES 2000 Conference paper A Timing Attack against RSA with the Chinese Remainder Theorem - `https://link.springer.com/chapter/10.1007/3-540-44499-8_8`
- Social Engineering: Hacking into Humans - `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391`
- Social engineering attack framework - `https://ieeexplore.ieee.org/abstract/document/6950510?casa_token=kYL0A_EiNDcAAAAA:NY5UN5Wf951PntX4LQp40T0sFZKWKhTPAIyw4d9UrpZfGYdyxHUS4lUA1YdRd8IDTeaIxPU`

Score

The score will be assessed by the following factors:

- How well the related work is done, mapping the location of the reviewed work among the other works in the field.
- How well the problem is defined and formalized
- How well the novelty of the reviewed work is defined
- How well the methodology is explained and demonstrated
- How well the results and conclusions are analyzed and put into practice context.