Sevval Deniz Erkurt (PantherID: 6237614), Spring 2024 CIS 4930, Credits: 3
Instructor: Professor Selcuk Uluagac, https://users.cs.fiu.edu/~suluagac/

*** Title for the special topics study:**
Security Analysis of Adversarial Attacks against Ransomware Detection Systems

*** List of objectives with specific deliverables:**
- Conduct a comprehensive review of current static ransomware detection models.
- Learn and perform tests using different metrics, including accuracy, recall, F-1 score, and precision on both existing and newly developed models.
- Report results and findings (identification of vulnerabilities, types of attacks, and effectiveness of current defenses).
- Implement adversarial attacks used to evade these models such as evasion and poisoning attacks.
- Draft a scientific paper outlining the major findings, methodology, experiments, and results.
- Submit final paper to a conference/journal/workshop and present findings to other students in the group meeting before the term concludes.

*** Method of student performance evaluation:**
- Research paper submission and completion.
- Weekly updates and working hours: M/W/F: 10 am - 4 pm, T/TH: 11 am - 3 pm

*** Planned meeting schedule with the mentor:**
Tuesdays: 11:00 am - 12:00 pm and Fridays: 11:00 am - 12:00 pm