ECE 4311 "Network Forensics" Project Requirement

Project objective

One of the major requirements for this course is a project on aspect of Network Forensics or other cybersecurity aspects. Each group can choose any topic they are interested in but related to the cybersecurity area.

Project types

The project could be a theoretical research project or a hands-on lab project.

- Theoretical research project:
  - Read at least 20 articles that are published in the area of Digital security, examine the theoretical work and criticize it.
  - Among the articles, at least 60% should be journal papers, white papers or conference proceeding papers.
  - The articles should be published within the past three years. It is not acceptable to cited all references from hyperlinks.
  - General introductory subjects of cyber/digital security is not accepted. For example, an introduction of denial of service (DoS) attack to networks will not accepted. It should be an in-depth research of a specific topic related to the area of cyber/digital security, e.g. a specific DoS attack to networks technique and its countermeasure, analysis of network traffic bottleneck, enterprise Wide Area Network (WAN) optimization, traffic management for fixed and mobile networks, and etc.
- Hands-on lab project:
  - Download a tool (or write a program), use it in a physical or simulated network and actually conduct experiments related to tasks of cyber/digital security.
  - At least three experiments should be conducted in your project. Sample experiments such ass network attack scenario, analyzing cybercrime, etc.

Possible project topics

The topics include but not limited to:

- Use tools to automatically verify a running configuration
- Advanced Persistent Threat (APT) attack
- Ransomware attacks
- Security of things, IOT Threats
- Intrusion detection and prevention
- Endpoint, perimeter, and network-based security
- Endpoint Detection and Response
- Security Autonomics (cloud and SDN controllers)
- Security strategy/planning and security operations organizations
- Dynamic Risk Management
- Security information sharing
- Security and privacy, Authentication, Biometrics
- Encryption, Quantum insecurity

- Fine-Grained Security Model
- End-to-end security Architecture
- Security for industrial control systems

Project proposal

- A project proposal (Word format) is required to be submitted by the due date posted on the Blackboard.
- In the proposal, the following items should be included:
  - Project Title
  - Group Number
  - Team Members
  - Project Summary.
  - Project Objectives
  - Project Deliverables

Project report

- The report (Word format) must be submitted by the due date posted on the Blackboard.
- The format of the report:
  - Minimum 16 and Maximum 24 pages are required.
  - Margins should be 1.25 inches left and right and 1 inch top and bottom.
  - Spacing should be single line. Page number is required.
  - The heading is upper case, at the left margin, and boldfaced. The text is below the heading at the left margin.
  - Text should be in a 12-point Times New Roman font and left-right alignment.
  - Tables and figures should be in a 12-point Times New Roman font, centered, and numbered sequentially and titled individually.
- The hands-on lab project report should include:
  - Title page
  - Abstract
  - Table of contents
  - Introduction (a summary of project objectives)
  - Experimental methodology
  - Experimental results
  - Summary of challenges and how they were solved
  - Conclusions
  - References
- The theoretical research project report should include:
  - Title page
  - Abstract
  - Table of contents
  - Introduction (What was the research problem? Why is this problem important?)
  - Literature review (How did the authors investigate the research problem?)
  - Discussion (What are the authors' findings? What do these findings tell you?)
  - Conclusion
  - References

- Examples of the reference writing
  - Article or Chapter in an Edited Book
    Author, A. A., & Author, B. B. (Year of publication). Title of chapter. In A. A. Editor & B. B. Editor (Eds.), *Title of book* (pages of chapter). Location: Publisher.
  - Article in journal paginated by volume

    Harlow, H. F. (1983). Fundamentals for preparing psychology journal articles. *Journal of Comparative and Physiological Psychology, 55*, 893-896.
  - Article in a magazine

    Henry, W. A., III. (1990, April 9). Making the grade in today's schools. *Time, 135*, 28-31
  - Edited book with an author or authors

    Plath, S. (2000). *The unabridged journals.* K. V. Kukil (Ed.). New York, NY: Anchor.
  - Article from an online periodical

    Author, A. A., & Author, B. B. (Date of publication). Title of article. *Title of Online Periodical, volume number* (issue number if available). Retrieved from http://www.someaddress.com/full/url/
- Grading policy
  - The amount of work accomplished: 60%
  - The organization of the project report: 20%
  - The usefulness of the project and the degree of relation to digital/cyber security: 20%

  By following the above rules, the instructor has the right to grade students' report at his own discretion.