ECE 572: Security, Privacy, and Data Analytics

Summer 2020

Course Project

Graduate Students of ECE 572 class are required to complete a project that consists of **3** parts:

Part 1) Security/Privacy Data Collection:

Objective: Demonstrate the data capturing capability on computing devices or networked environment.

Description: Students need to setup an environment on their own computing devices (desktop computer, laptop, mobile devices, etc.) where they are able to install and use data capturing tools (log monitoring tools, web proxy tools, network sniffer tools, etc.). Students need to practise both benign and malicious actions to simulate regular and attacking activities on the devices or network environment. (students can practise benign and malicious activities using either a single application or multiple applications). Students need to capture the related data as much as possible using the data capturing tools chosen by the students. (remember that data can be captured from multiple entries, e.g. application logs, operating system even logs, network traffic, etc.)

Part 2) Security/Privacy Data Interpretation:

Objective: Demonstrate the capability of data interpretation for data captured in a typical computing/networked environment.

Description: Students need to consolidate the captured data in Part 1 and prepare the raw data for security/privacy analysis. More specifically, students need to identify significant data elements from the raw dataset, and explain the **data origin (where the data come from)**, **data format**, and **the meaning of the data elements** (what is the data used for).

Part 3) Security/Privacy Data Analytics:

Objective: Demonstrate the capability of data analysis for data captured in a typical computing/networked environment.

Description: Students need to analyse the captured data in Part 1 and interpreted in Part 2 for security/privacy analysis.

Students need to use analytical methods and techniques in information security that they will choose to uncover hidden patterns, security breaches, attacks, injections, etc, from the data captured from a collection of server logs and other sources such as router log files.

Project Deliveries:

1) Students will team up by five on the project.
2) Students need to deliver a **demo/presentation** and a **report.**
3) Both the Demo and report should cover students work for all 3 parts of the project.
4) Project Evaluation will be based on the quality of both presentation and report.

IMPORTANT DATES

Report Due: **July 30th, 2020**

Presentation Date: **July 30th, 2020**

GENERAL GUIDELINES

The format for written reports is 8.5 x 11" white paper, stapled in the upper left corner. NO plastic or cardboard or cellophane covers. NO binders. Submit report and presentation slides in both hard copies and electronic forms, the hard copy one needs to be submitted on the presentation day for grading and return, the electronic one should be submitted before the report due day.

Grading of written reports and presentations/demos will be based upon substantive content, appropriate organization and use of allotted report size or presentation/demo time, and effectiveness of the presentation or report. Multiple errors in grammar and spelling are unprofessional and detract from the clarity of your report or presentation and will be graded accordingly, so use a spell checker!

PRESENTATION/DEMO GUIDELINES

Plan to give a 10 minutes presentation. Presentations should be self-contained, and should be clear and precise. Briefly introduce the topic including any background information, describe the investigation, development, or experimentation that was conducted, and provide any demonstrations developed as part of the project, or describe the results of the investigation or experimentation. The following format is suggested:

(1) Title. Name the topic.

(2) Outline. Summarize the full presentation.

(3) Introduction. Provide any background material necessary to understand the topic.

(4) The body of Your Presentation**.**

- Explain the data capturing setup, the approach and the technologies, tools, etc.

- Explain key/significant data elements captured and identified in your dataset for security analysis.

- Explain your data analytics approach and results.

(6) Conclusion.

(7) Questions and discussion.

REPORT GUIDELINES

The project report should be neat, readable, and self-contained. Also, it should be written with the readers in mind. Therefore, you should include adequate references and/or background materials and you should use tables, diagrams, graphs, figures, and portions of printouts to enhance readers' comprehension of your project.

The following format is suggested. You don't have to follow it exactly. Some sections may not be needed, or additional sections may be necessary. In all cases, please type and paginate your report!

(1) Abstract.

(2) Summary. Gives succinct information on the purpose, methods, results and conclusions reported.

(3) Introduction. Include background material and discuss the scope and limitations of your project.

(4) Discussion. The body of your report. This includes the methodology used. Be sure to fully describe any figures, tables or diagrams you include.

(5) Results.

(6) Conclusions.

(7) Appendices, including supporting material as needed.

DEADLINES

By June 8th: Email me and CC the TAs your group members.

By July 30th: Email me and CC the TAs your group report and group presentation.

TAs : Abdul Aleem Syed; E-mail: aleemshah110@gmail.com;
Araya Chaowalit; E-mail: araya.chaowalit@gmail.com