CALIFORNIA STATE UNIVERSITY
LONG BEACH

Semester Project

CECS 378 Section 04 – Spring 2021 Cappel

Due: Friday, May 7th by 11:59 PM

The semester project is focused on one of the most important topics within computing security (and information security in general) – That topic is Threat Modeling.

During the semester you will be learning many different topics related to computing security. We will be talking a great deal about risks and threats to computing systems and mitigations to those threats. As we discuss these different topics, you should be thinking about how they might relate to this semester project and whether topics we discuss apply to this effort. The SANS NewsBites might help you as well. As you progress through the semester, you should quickly discover you are building your list of threats and proposed mitigations very quickly.

Your grade on this project will be determined by the quality of the threat findings you produce. You are being asked to identify 100 *legitimate* threat findings along with a *proper* proposed mitigation(s) for the threat. This semester project will represent 20% of your overall grade for the course. You have the entire semester to complete this project.

****WARNING** - This project takes time - Do NOT procrastinate or you will regret it!!**

Background

Long Beach Pharma, Inc. is a new, up and coming pharmaceutical company that is based in Long Beach, California, and they have begun development and testing a vaccine to prevent infections from the Covid-19 virus. The pharmaceutical company has hired *you* to perform a threat model assessment of their existing office, data center, and laboratory facilities located in Long Beach, California. You are to examine all the data gathered on the existing facilities that has been provided by the company's staff and over the next few months identify existing threats and corresponding mitigations to those threats. The one deliverable you will produce for your threat model work will be a completed threat findings spreadsheet that you will deliver to the company's administrators on May 5, 2021 so they have time to mitigate the threats you have proposed prior to the vaccine being approved by the FDA. The company is counting on you to help keep their patient test results and company intellectual property safe. You will be paid by the company in full once the threat findings spreadsheet has been delivered to Long Beach Pharma, Inc. and they are satisfied with the quality of your report.

Threat Modeling

Threat modeling can be broken down into essentially three separate steps:

1. **Data Gathering** (The company's admins provide this – *You* will leverage this data)
2. **Threat Analysis** (*You* will perform this step)
3. **Mitigation & Validation** (LB Pharma admins will do this once the threats are provided)

Task 1 – Examine the existing data provided by the Long Beach Pharma Staff

Perform the following steps to complete this task:

1. Open the Long Beach Pharma Data workbook that was provided by the Long Beach Pharma staff and examine the information provided in these various spreadsheets…
    a. LB Pharma Facilities, Bldg. 1, Bldg. 2, Bldg. 3, & Rack Diagram
    b. Device Listing
    c. Firewall Rules and Data Flows
    d. Information on Windows Servers, Network Appliances, User Devices, Users, and Datastores
    e. Account Information
    f. Information on the Web Server, File Server, SQL Server, and Backup Server.

This represents the 1st step in threat modeling (Data Gathering).

Task 2 – Identify 100 existing Threats and Propose Mitigations for each Threat

Perform the following steps to complete this task:

1. Open the Threat Model Info workbook and review the information provided in these various spreadsheets…
    a. STRIDE Threat Modeling
    b. MITRE ATT&CK Framework
    c. Top 20 CIS Controls
    d. NIST Cybersecurity Framework

    This information should assist you in analyzing the system and identifying threats. We will be discussing these during upcoming lectures, and they should be beneficial.

2. Complete the Threat Findings spreadsheet & identify 100 threats & mitigations.

    I have provided a sample threat finding and mitigation in the threat findings spreadsheet. Your job is to come up with the remaining threats and propose mitigations for each of them. You cannot repeat the same threat across multiple devices. Each threat should be unique and may contain one or several proposed mitigations.

    This represents the 2nd step in threat modeling (Threat Analysis).

Task 3 – Submit your threat findings spreadsheet via *email* to Prof. Cappel.

The findings spreadsheet must be emailed to Prof. Cappel in its native Microsoft Excel format – no other format (including PDF) will be accepted. Excel only!!

Grading

The semester project will be graded based on the following:

1. **100 Points –** You are being asked to produce 100 different threat items.

Note: These items cannot be repeated once per device. They can be listed for multiple devices if and only if the IMPACT statement is different between the entries and the mitigation(s) are different.

2. **100 Points –** You are being asked to produce 100 mitigations for each threat item.

   Note: You can list more than one mitigation for a single threat item if there are multiple ways to lower the residual risk.

3. **5 Extra Credit Points** – You will be given up to five extra credit points if you can come up with five additional threats and their appropriate mitigations.
4. **5 Extra Credit Points** – You will be given up to five extra credit points if you redraw the Data Flow Diagram (DFD) using the drawing application of your choice. The diagram should contain a proposed architecture based on your findings and one that addresses items you list as threats & mitigations. Include all devices or objects on your proposed DFD that you recommend as mitigations. Please email the Data Flow Diagram to Prof. Cappel in PDF format only. No other format will be allowed for this extra credit item.
5. **Final Grade for the Project** – We will add all the points from items 1 thru 4 listed above and divide by 200. That will be your score for the semester project.

Note: This semester project represents 20% of your grade in this course. Please make sure your threats & mitigations are written very clearly and with the required amount of detail. This assignment is due by 11:59 PM on May 7th (No later!).