**INFO 5100 Application Engineering and Development Final Project Statement**

**Due Date: April 22, 2016**

**Cyber-Security Project**

The three elements of cyber-security are assets to be protected, threats, and security operations. The assets include devices, people as employees, applications, databases of client and employee private data. The threats are malicious attacks targeting the valuable assets. Security operations are the people and organizational support structure that work diligently to protect the valuable assets from attacks.

Develop a cyber-security application that will enable an industry (financial or healthcare) to cooperate to fight cyber-attacks. Cyber-crimes are better fought through sharing of intelligence information. Your use-cases will involve building applications to enable cyber-security operation centers manage the full attack life-cycle referred to as the Kill-Chain, typically described as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Mandiant describes the attack lifecycle as reconnaissance, initial compromise, establish a foothold, escalate privileges, internal reconnaissance, move laterally, maintain a presence, and complete the mission (Mandiant, 2010; Mandiant 2013).

You are required to build a Java application to simulate how cyber-security operations work for an industry (say a consortia of banks). Since the time is limited it is okay to use pre-prepared network traffic. Also, allow for a mechanism where an attacker can input these attributes into the system). Or you can use random number generators for the data points. Each of the data points must be within a specified range consistent with the specific data type. We suggest that you research what are the normal and abnormal traffic on the different parameters.

**The deliverables,**

1. The complete application
2. Object model for your application
3. Presentation
   1. The problem statement
   2. Approach
   3. Implemented Features
   4. Architecture (roles and responsibilities)
   5. Object model of the cyber application
   6. Screen shots of the 5 most important screens in your application

Reference:

https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf