CCY3101- Software Security

Project Description

Project Scenario:

You are working with the cybersecurity team in a software company specializing in building customized software systems according to clients' needs. You, with your team, are responsible for performing security testing and threat modeling for the software products during and after the software development lifecycle (SDL) to ensure the production of secure software systems.

Your company got a request from one of the universities in your city to reimplement its financial system with the task of adding a new web-based portal for students to access relevant financial services. After that, your company is required to do thread modeling for the overall financial system of the university. The newly implemented financial system of the university must have the following requirements:

- There is a new web-based portal for university students to access the university's financial system.
- The newly implemented portal will allow students to access the university's financial system with the limited ability to view their current balance and payment history, set up payment accounts, make one-time payments, and set up automatic payments.
- The university already has an existing financial system, with a front-end web interface and back-end database, all hosted/located in its own data center.
    - Authorized University staff/users access the system from either their workstations on the internal network or remotely through an already implemented secure web portal (located in the data center **DMZ**):

        - Internal network traffic is encrypted between the user workstation and the application server, as well as data transfer between the application and the database server.
        - Certain database records are also encrypted.
    - Staff remote access sessions occur over a **VPN** connection to the staff web portal, then use an encrypted connection to the application server:
        - User authentication is managed by an Active Directory (**AD**) account within the relevant domain.
        - Application access (authorization) is managed by an AD Security Group Policy Object (**GPO**).
- This new implementation will allow students to connect to the University Web Portal using HTTPS, but **without** a VPN:
    - The Web Portal server is located within the data center's **DMZ** and uses encrypted connections to internal resources (i.e., domain controllers and other servers).
- Students will be authenticated through an Active Directory (**AD**) domain, separate from the staff/faculty domain:
    - There will be a Student AD Domain Controller within the **DMZ**, which will validate student user login credentials from the secure Web Portal.
    - After successful login, the Web Portal will display the University application(s) available to the student, based on membership in the applicable AD Security Group.
- OS and security software on staff internal workstations are managed by the University IT department; patches and updates occur automatically, so the staff/user doesn't need to take any action.
- Remote systems connecting to the University Web Portal are required to also have current OS and security software installed with automatic updates enabled; as well as having the current version of any supported web browser.