

**Technological Institute of the Philippines**  
**College of Information Technology Education**

**Assignment 2.1 Cyber Threat Modeling (Part 1)**



Score

Group Name: TechWhiz

Names:

Castillo, Alysson Kyle V.

Macam, Ignacio Jr., J.

Morales, Neil Irvine B.

Paragas, Renz Jordan B.

Tribaco, Alfie C.

IT42S1

Dr. Jenalyn Raviz  
Professor

## IT024 – Cyber Threat Modeling

### Assignment 2.1 Cyber Threat Modeling (Part 1)

#### 1. Intended Learning Outcome (ILO)

At the end of this practice set, the students are expected to:

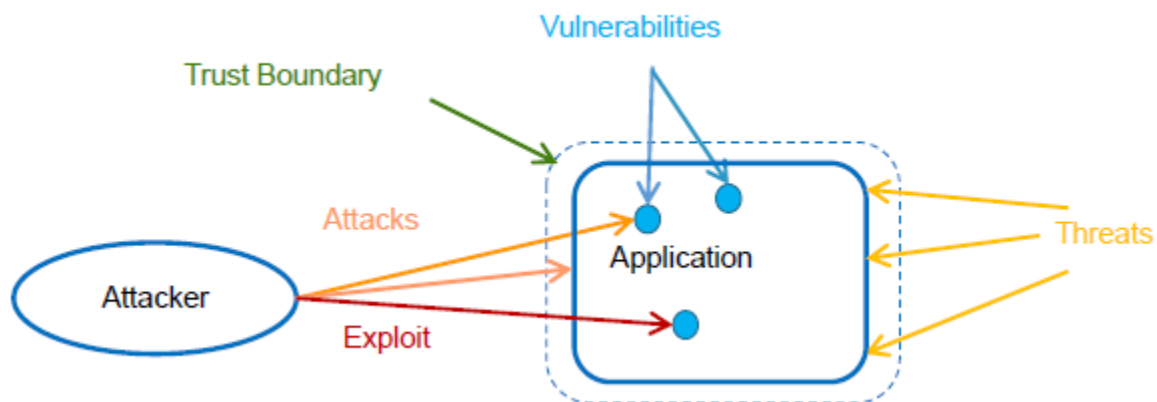
Students can discuss some of the unique challenges in the field of cybersecurity that differentiate it from other design and engineering efforts.

Students can identify the goals and summarize the overall process of threat modeling.

Given a description of a system, students can predict and prioritize some potential threats and the human impacts of those threats.

#### 2. Discussion:

##### Threat Modeling



Vulnerability: a software defect with security consequences

Threat: a potential danger to the software

Attack: an attempt to damage or gain access to the system

Exploit: a successful attack

Trust Boundary: where the level of trust changes for data or code

### Risk Rating Exercise Using DREAD

Threats	D	R	E	A	D	Total	Risk Rating
Network Sniffing	3	2	2	2	1	10	Medium
Denial of Service (DoS) attack	2	3	1	2	3	11	Medium
SQL Injection	3	1	3	3	1	11	Medium
<b>TOTAL RISK RATING</b>						32	High

#### Risk Rating

High - 12 - 15

Medium - 8 - 11

Low - 5 - 7

#### Overall Threat Rating

Critical (34–45): Critical vulnerability; address immediately.

High (23–33): Severe vulnerability; consider for review and resolution soon.

Medium (12–22): Moderate risk; review after addressing severe and critical risks.

Low (1–11): Low risk to infrastructure and data.

### DREAD Risk Rating Applied to Sample Threat

Threat Description	An attacker could use <u>network sniffing</u> tools to capture and analyze network traffic of the student's data.
Threat target Risk rating Attack Techniques Countermeasures	School Network System Medium Network packet sniffer, Packet sniffing device Use secure protocols such as SSH, SFTP, or SCP to transfer files, SSL/TLS encryption for web traffic, and VPN encryption for remote access.
Threat Description	The school's website may be targeted with a <u>DoS attack</u> to flood it with requests.
Threat target Risk rating Attack Techniques Countermeasures	Web application services Medium Application-layer attacks, Protocol Attacks, Volumetric attacks Implement a robust firewall, Use traffic monitoring and anomaly detection software, Enable rate limiting
Threat Description	An attacker can exploit <u>SQL injection</u> vulnerabilities by injecting malicious SQL statements into a school web app.
Threat target Risk rating Attack Techniques Countermeasures	Student Database Servers Medium Use of website that has text fields that allow/use SQL statements Input validation, Avoid dynamic SQL queries, Implement logging and monitoring, Use parameterized queries or prepared statements

### **3.1 Briefly discuss the following:**

**3.1.1 Company Name/System:** Student Information Management System

**3.1.2. Version:** 1.0

**3.1.3. Document Owner:** TechWhiz

**3.1.4. Description of the company:** This system allows schools to manage student data, including personal information, enrollment, attendance, grades, and academic performance. It simplifies the process

of storing, retrieving, and updating student records, making it easier to track student progress and generate reports.

### **3.1.5. Participants:**

CIO - Castillo, Alysson Kyle V.

CISO - Macam, Ignacio Jr., J.

Penetration Tester - Paragas, Renz Jordan B.

Developer - Tribaco, Alfie C.

Quality Assurance - Morales, Neil Irvine B.

### **3.1.6. Reviewers:**

CSO

### **3.1.7. External Dependencies**

#### Database System

- Oracle, MySQL, or Microsoft SQL Server

#### Operating System

- Linux

#### Web Server

-Apache

#### Cloud Hosting

-Azure

## **4. Group Observation**

DREAD risk analysis is an important process in assessing and managing the security risks associated with a student information management system in an educational institution. It helps in identifying vulnerabilities, prioritizing risk mitigation measures, ensuring compliance with regulations and standards, making informed decisions, and continually improving the security posture of the student information management system to protect the student data and safeguard the institution's reputation.

## **5. Individual Synthesis**

**Member 1 - Castillo, Alysson Kyle V.**

It is important to know the threats and risks that can affect the computer system so that the security management can strengthen their defense to ensure that the data will be protected. DREAD threat modeling is one of process to identify those threats that can understand the threats that can affect the system.

**Member 2 - Macam, Ignacio Jr., J.**

Predicting and prioritizing potential computer system threats is essential for effective risk management, proactive mitigation, resource allocation, mitigation of human impacts, compliance with regulations and standards, and ensuring business continuity and resilience. It enables organizations to take necessary measures to protect their computer systems, mitigate risks, and safeguard the interests and well-being of individuals who rely on those systems.

**Member 3 - Paragas, Renz Jordan B.**

When we were talking about the threats, the first thing we needed to do was how we could handle it. As we team, we are able to know the importance of the overall factors just like risk against the cyber threats. We could easily identify the threats by just doing the DREAD threat modeling. by this process we can easily understand the different threats that affect on the system.

**Member 4 - Tribaco, Alfie C.**

Knowing the threats with its risk factor will be useful on how the security team approaches these different threats. By listing different counter measures or solutions and in depth analysis for each threat are recommended to fully understand the list of actions that need to be taken in the process of occurrence of these cybersecurity threats. It is important to also know the overall factors like risk techniques to identify things that are not anticipated in just one look at the threat. This is also to identify things like in the DREAD threat modeling where it will identify how a specific threat can be done easily, how many are affected and how much severity can affect this threat to the whole system.

**Member 5 - Morales, Neil Irvine B.**

Threats are made by different factors throughout the program as we all progress due to a newer version of technology. It is a must to always learn the basic factors on how to counter these kinds of threats as well as being able to prepare and predict any sort of possibilities that our programs might be infected. With this said we are in need to be fully aware of any new updates because we are required to do so to have a full understanding and knowledge on how we can fix things just in case any threat happens. With that having extensive understanding with threat we can have a low risk when progressing in our system.

**Technological Institute of the Philippines**  
**College of Information Technology Education**

**Assignment 3.1 Cyber Threat Modeling (Part 2)**



Score

Group Name: TechWhiz

Names:

Castillo, Alysson Kyle V.

Macam, Ignacio Jr., J.

Morales, Neil Irvine B.

Paragas, Renz Jordan B.

Tribaco, Alfie C.

IT42S1

Dr. Jenalyn Raviz  
Professor

## IT024 – Cyber Threat Modeling

### Assignment 2.1 Cyber Threat Modeling (Part 2)

#### 1. Intended Learning Outcome (ILO)

At the end of this practice set, the students are expected to:

- Students can discuss some of the unique challenges in the field of cybersecurity that differentiate it from other design and engineering efforts.
- Students can identify the goals and summarize the overall process of threat modeling.
- Given a description of a system, students can predict and prioritize some potential threats and the human impacts of those threats.
- Distinguish the Use Scenario, Roles, and Assets in Cyber Threat Modeling

#### 2. Discussion:

##### **Background for all scenarios**

Before the main threat model meeting, we collected the following background information. This information applies to all the usage scenarios we identified for the sample architecture:

- Boundaries and scope of the architecture
- Boundaries between trusted and untrusted components
- Configuration and administration model for each component
- Assumptions about other components and applications

##### **Use Scenarios Examples (Student Information Management System)**

1. Students can view their respective data in a database - Grades, Personal Information and other data related to the student.
2. Teachers/Faculty can add data in the database - Teachers can add students on specific sections or blocks.
3. Teachers/Faculty can edit data in databases - editing grades and editing personal information. attendance of the students.
4. Students can request for enrollment - request and process of enrollment of a certain student.
5. Students can login to the site - student correct credentials are needed to be passed, otherwise the user would not be able to access the features.
6. Admin can create, read, update, delete in the database - admin has full access to the database.
7. Parents can login to the site - parents' correct credentials are needed to be passed, otherwise the user would not be able to access the information of their child.
8. Parents/Guardians can view the grade of their child - Parents can view all of the grades and other useful information about their child's performance.
9. School staff can read and write students information - this can be used in different ways like managing the tuition fee, library information, and other features.



10. Students can search the database(s) - Can access learning materials database information (Journals)
11. Students can put holds on some items for checkout - request and hold any circulating item inside the online library
12. Staff can search the database(s) - apply almost any database, including article databases and variety of topics
13. Faculty can do anything students or staff can do
14. Faculty can place items on an invisible list
15. Faculty can access limited account information

### **Roles (deviation from OWASP) Examples (Student Information Management System)**

- Invalid user
  - User that may not have the correct username, password, or other required credentials to authenticate and gain access to a system or service.
  - Attempted to authenticate and failed
- Students
  - Students are the primary users of a student information system. They use the system to access their personal information such as enrollment details, class schedules, grades, and other academic-related information.
  - Authenticated student with read-only access
- Teachers/Faculty
  - Teachers or faculty members use the student information system to manage various aspects of student information, including entering grades, updating attendance, managing assignments, and communicating with students and parents.
  - Authenticated teacher/faculty with read-write access
- Administrators
  - Administrators, such as school or university administrators, use the student information system to manage and oversee various administrative tasks related to student data, including enrollment, registration, scheduling, reporting, and managing system permissions.
  - Authenticated administrator with full privileges

- Parents/Guardians
  - Parents or guardians of students may also have access to the student information system to view their child's academic progress, attendance, and other relevant information. This allows parents to stay informed and engaged in their child's education.
  - Authenticated parent/guardian with read-only access
  
- School/University Staff
  - Other school or university staff members, such as counselors, registrars, and academic advisors, may also use the student information system to manage student data and provide support services to students.
  - Authenticated school staff with read-write access

### **Assets Examples (Student Information Management System)**

- Student Records
 

Student records, including personal information, enrollment details, academic performance, attendance records, and other sensitive data, need to be secured to protect the privacy and confidentiality of students.
- User personal information
 

Personal user data typically contains name, address, and contact details and is used to determine if the book has already been returned.
- User Accounts
 

User accounts within the student information system, including student accounts, faculty accounts, and administrator accounts.
- User credentials
 

Used to authenticate and authorize users in a computer system or application. They typically consist of a unique username or user ID and a corresponding password or other authentication credentials, such as a fingerprint, smart card, or security token.
- Website system
 

Users and administrators log in to the website using web browsers. Other characteristics included are the address, contact information, and if the library is open or closed.
- DB system
 

The database system stores a lot of information and keeps track of all users, administrators, available books, and books on loan.

- Availability of the web server

The term "website availability" refers to the ability of people to successfully access a particular website. If entering a URL or clicking a link from social media, email, referral websites, or other sources leads to the expected content, that website is "accessible." Another term for availability is "uptime."

- Availability of the DB server

Database availability refers to the amount of time the database system is up and allows end users connecting to the server to access the database using normal login procedures.

- User code execution on web site

Code injection vulnerabilities occur when you can manipulate the output or content of a web application to trigger server-side code execution. A poorly written web application that allows users to modify server-side files (such as posting to a message board or guestbook) may be able to insert code into the application's scripting language.

- User DB read access

To send these requests to the database, you need a read-only user bound to one of the IP addresses. This user may have access to all the data in the database, or may have restricted access to certain tables or columns in the data schema.

- Faculty /Admin code execution on the website

When managing a website, one of the most important maintenance tasks is managing security. This helps prevent the most common types of security attacks, such as: B. Remote code execution. Without the necessary precautions, hackers can break into your website and steal your sensitive information.

- Faculty /Admin DB read/write access

Read Access: Users with read-only access can see existing backup policies, server schedules, and DR plans, but cannot create or edit existing policies or plans. Write access: Users can create or edit existing backup policies, server schedules, and DR plans. However, you are not allowed to change account settings such as time zone, notifications, member access, etc. Administrator access: Administrators have access to all available features, such as the ability to add members and change permissions.

- Ability to create users

During implementation, you can use the Create User task to create a test application user. By default, this task creates minimal personal records and user accounts. After implementation, you need to create an application user using the Hire Employee task. We do not recommend running the user creation task after the deployment is complete.

- Ability to audit system events

To audit activity, you need to identify the command or process that initiates the audit event and ensure that the event is listed in the system's / etc / security / audit / events file. You can easily associate audit events with users by grouping similar events into audit classes.

### 3.1 Briefly discuss the following:

#### 3.1.1 Use Scenario

**The guideline lays out five basic steps for how to define a cyber security asset:**

1. **Identify Cyber Assets Associated with a Critical Asset.** A responsible entity should inventory and evaluate cyber assets in order to identify those that might impact any of their critical assets. Cyber assets to consider include, but are not limited to:
  - Control systems
  - Data acquisition systems
  - Networking equipment
  - Hardware platforms for virtual machines or storage
  - Secondary or supporting systems such as virus scanners, HVAC systems, and uninterruptible power supplies (UPS)
2. **Group Cyber Assets.** Cyber assets can be grouped by different features and characteristics to simplify the process of defining cyber security assets. Categories can include cyber assets that communicate with specific software. Another example is a group based on the ability to support a particular significant asset.
3. **Determine Cyber Assets Which are Essential.** Evaluate an asset's impact on critical assets according to the following criteria:
  - Is it essential to the reliable operation of a critical asset?
  - Does it display, transfer, or contain information necessary for real-time operational decisions?
  - Would its loss, degradation, or compromise affect the reliability or operability of the bulk power system?
4. **Identify Cyber Assets with Qualifying Connectivity.** According to standard CIP-002 R3, cyber assets that meet any of the following requirements are "critical":
  - It uses a routable protocol to communicate outside the Electronic Security Perimeter (ESP).
  - It uses a routable protocol within a Control Center.
  - It is dial-up accessible.
5. **Compile the List of Critical Cyber Assets.** Once you have evaluated your cyber assets and identified those that are critical to the security of your critical assets, you need to document them in a list to comply with the NERC-CIP standard.

### 3.1.2. Roles (deviation from OWASP)

Applications have a few kinds of functionalities and administrations, and those require access authorizations in view of the necessities of the client. That client could be:

- an overseer, where they deal with the application functionalities.
- an examiner, where they audit the application exchanges and give a definite report.
- a help engineer, where they help clients investigate and fix issues on their records.
- a client, where they associate with the application and advantage from its administrations.

To deal with these purposes and some other use cases for that application, job definitions are arranged (all the more normally known as RBAC). Given these jobs, the client is fit to achieve the expected undertaking.

#### Test Objectives

- Distinguish and record jobs utilized by the application.
- Endeavor to switch, change, or access another job.
- Audit the granularity of the jobs and the requirements behind the consent given

#### Instructions to Test

Jobs Identification - The analyzer ought to begin by recognizing the application jobs being tried through any of the accompanying strategies:

- Application documentation.
- Guidance by the developers or administrators of the application.
- Application comments.
  - Fuzz possible roles:
  - cookie variable (e.g. role=admin, isAdmin=True)
  - account variable (e.g. Role: manager)
  - hidden directories or files (e.g. /admin, /mod, /backups)
  - switching to well-known users (e.g. admin, backups, etc.)

#### Switching to Available Roles

After identifying possible attack vectors, the tester needs to test and validate that they can access the available roles

Some applications define a user's role at creation time, either through strict checks and policies, or by ensuring that the user's role is properly protected by a signature generated by the backend. The statement that roles exist does not mean that they present a vulnerability.

#### Review Roles Permissions

After accessing the roles on the system, the tester needs to understand the permissions granted to each role

Support software engineers should not be able to perform administrative functions, manage backups, or perform transactions on behalf of users.

### **3.1.3. Assets**

#### **4. Group Observation**

We talked about three situations: usage scenarios, roles, and assets as an observation. Utilization depicts how someone is utilizing the current object or frame. The utilization of a planned item or location that is in the planning stage is hypothetical. The program contains many types of functionality and administration, and depending on the demands and responsibilities of the user, different permissions are needed. Resources are things that give someone or something else present, potential, or future financial advantages. In this context, a resource is anything you own or are entitled to.

#### **5. Individual Synthesis**

##### **Castillo, Alysson Kyle V.**

It describes the usage scenario of how someone uses a product or existing system also the design scene is a kind of description that is used for system design or product design. Those applications have multiple types of roles and responsibilities that those features and services require permission based on the users. The asset is one of the potential financial benefits that provide to the individual or entity.

##### **Macam, Ignacio Jr., J.**

This practice set shows how people use products or systems, and how designers create those systems. Different users may have different roles and responsibilities, and may need different levels of access to features and services. "Assets" are the potential financial benefits that individuals or entities can receive from using the product or system. Listing the assets in a cyberthreat model helps identify the most valuable and important resources that need to be protected from potential cyber attacks. By understanding which assets are critical to the organization, security measures can be prioritized and resources can be allocated effectively to minimize the risk of cyber threats. Additionally, identifying assets can help in creating a response plan in case of a cyber attack, as it helps to focus on the most important assets and prioritize their protection.

##### **Paragas, Renz Jordan B.**

The use scenario outlines a person's utilization of an existing system or product. A design scenario is a description of how the system or product being designed will be used. Depending on the demands and duties of the user, applications offer a variety of features and services that call for permissions. An asset is something that offers a person, group, or other entity current, potential, or future financial rewards. The thing you own or possess is thus the asset.

### **Tribaco, Alfie C.**

This activity depicts different use cases in terms of its use scenario where it focuses on the main usage of different features of the system and it also includes its limitations based on the user's role. Since there are three main users the faculty, students and staffs which if we don't include the admin and other users, these three main users alone have differences when it comes to their access on the system, where the authorization and permissions comes into place and the roles of these users will be appropriate to their level of access of the mentioned assets. Assets can be categorized on which are essentials and what are critical assets that can be documented and be prioritized when it comes to applying certain security measures for these factors.

### **Morales, Neil Irvine B.**

In this activity we are talking about why it needs a group of people to completely run an activity with each personnel having different tasks and duties to fulfill. Having one another do a certain role and responsibility will not only make the task faster but also efficient as there will be no lapses to mind. Within the activity we also tackled certain scenarios on how we can fully utilize the use of an existing system to and improve it with the help of our Assets and Resources, these things can also be used to further improve the overall performance and quality of the work.


### **Honor pledge with signature**

  
ALYSSON KYLE V. CASTILLO

  
ALFIE C. TRIBACO



  
RENZ JORDAN B. PARAGAS

  
NEIL IRVINE B. MORALES

**“I accept responsibility for my role in ensuring the integrity of the work submitted by the group in which I participated.”**

## 6. References:

EC-Council. (2022, May 29). Dread threat modeling: An introduction to qualitative risk analysis. Cybersecurity Exchange. Retrieved April 8, 2023, from <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/#:~:text=Overall%20Threat%20Rating%20The%20overall%20threat%20rating%20is,Severe%20vulnerability%3B%20consider%20for%20review%20and%20resolution%20soon.>

Versify, JB. (2018, June 13). How do I define a cyber security asset? Versify Solutions. Retrieved April 8, 2023, from <https://www.versify.com/how-do-i-define-a-cyber-security-asset/>

WSTG - latest. WSTG - Latest | OWASP Foundation. (n.d.). Retrieved April 8, 2023, from [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/03-Identity\\_Management\\_Testing/01-Test\\_Role\\_Definitions](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/03-Identity_Management_Testing/01-Test_Role_Definitions)

Cyber Security Exchange (n.d.) DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. Retrieved April 8, 2023, from <https://eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/>

Dawid C. (2014, May 14) Qualitative risk analysis with the DREAD model. Retrieved April 8, 2023 from <https://resources.infosecinstitute.com/topic/qualitative-risk-analysis-dread-model/>