Vulnerabilities and Threat Analysis for Assignment Management System (AMS) and Mitigation Plan

Submitted By

Md. Tahmidur Rahman Khan (BSSE0801)
Tahlil (BSSE0803)
Tulshi Chandra Das (BSSE0811)
Abdullah Al Jubaer (BSSE0812)
Maloy Kanti Sarkar (BSSE0834)

Submitted To

Md. Shafiul Alam Khan
Professor
IIT
University of Dhaka

Date: 29-10-2019

Contents

ABSTRACT

Threat analysis shows that potential opponents use device instability to achieve their objectives. This establishes and sets an architectural, operational and configuration risk mitigation strategy. Security measures in a risk assessment are a challenge to determine the status of the safety performance of the network and further increase it by increasing the exposure to major threats and vulnerabilities. AMS is a web application for teachers and students that aims to simplify creating, distributing, and grading assignments in a paperless way. The primary purpose of AMS is to streamline the process of sharing files between teachers and students. But significant security concerns have to be addressed for the smart grid, dangers range from threatened availability of energy, to threats of customer privacy.

Chapter 1: INTRODUCTION

In recent years, the rapid diffusion of new technologies and the internet has intensified the need for security as Communications Networks are used to transmit increasingly sensitive information that can be useful and confidential. Network Security refers to the process of safeguarding digital information assets, where the word security means protection from malicious outsiders or insiders. All networks must be secured from threats and vulnerabilities to reach their full potential. The process to identify the threats, which consists in identifying how potential adversaries exploit system weaknesses to achieve their goals and find appropriate countermeasures, is the threat analysis. The method is necessary to define a comprehensive and full set of safety requirements in order to implement the required protections to secure the system efficiently. Therefore, a proper evaluation of threats or vulnerabilities on an existing system enables them to be prioritized, the safety of the system is analyzed and the best improvement plan is suggested.

1.1 OBJECTIVE

The outcome or objective of this document is to identify threat and risk assessment to provide recommendations that maximize the protection of confidentiality, integrity and availability while still providing functionality and usability. The central framework for risk management is a cost-related method, in which the overall process begins with defining the risky assets, assessing its likelihood, establishing a cost and probability associated with an occurrence, and calculating the cost of reducing risk. The definitions of vulnerabilities, resources and threats are important for understanding risk.

1.2 THREAT MODEL AND ITS PURPOSES

As previously stated, threat modeling is a systematic approach for detecting and mitigating threats that may threaten the system and cause resource loss. Below are a few more reasons why simulation of risks should take place.

1 When the time comes to fix it, it is better to identify security faults.
2 It can save company time, profits and credibility.
3 To construct a secure application.
4 Bridging the gap in security among developers.
5 Contains all threats and evaluated threats found.
6 It offers knowledge and awareness of the latest risks and vulnerabilities.

1.3 Threat Analysis Methodology

The threat assessment is a formal process to identify, report and mitigate security risks of a system that can be divided into three main phases: the simulation of hazards, the resource maps and the design of a mitigation plan. The technique suggested includes a new approach to characterizing the process for all these aspects. Modeling threats is a method for evaluating and documenting the safety risk of an application, including the understanding of an adversary's objectives in attacking the system on the basis of the assets of interest. It allows the risks to be reported and vulnerabilities to be identified. Techniques of threat modeling are particularly useful when it is made early in system development, and then the lists of threats and vulnerabilities can be revised if appropriate, with the progress of applications and specifications.

1. Description of the system
2. Identify Assets
3. Determining vulnerabilities and threats
4. Asset Mapping
5. Ranking of threats
6. Risk Management

Chapter 2: Threat Model for AMS

2.1 INTRODUCTION TO AMS

AMS is a web application that aims to creating, distributing and grading assignments in a simplified way. Students can be invited to join a group through a private code. Teacher can share file to a group and post an assignment. Teacher can also check plagiarism of given assignment and grading students' marks. After publishing grading all the students can be viewed their grades. Teacher can give particular format when posting the assignment. After submitting the assignment students can resubmit their assignment. Student and teacher can change their profile settings by confirming their password.

2.2 SECURITY REQUIREMENT OF AMS

Confidentiality: Confidentiality is a defense against unauthorized parties accessing information. In other words, the access to sensitive data can only be accessed by people who are allowed. Imagine the records of your account. If confidentiality has not been maintained, someone who should not have access to it can have access, either by intentional conduct or incidental behavior. A privacy error, commonly referred to as a violation, can not necessarily be remedied. There is no way to reveal the password once it is published.

Integrity: Integrity means ensuring the data is genuine — that the information is not distorted and that its source is authentic. Imagine having a website and selling products online. For example, an attacker can shop on the web site and maliciously alter the prices of your products, so that they can buy anything for whatever price they choose. That would be a failure of integrity, because your information—in this case, the price of a product—has been altered and you didn't authorize this alteration. Another example of a failure of integrity is when we try to connect to a website and a malicious attacker between you and the website redirects our traffic to a different website. In this case, the site you are directed to is not genuine.

Availability: Availability means that authorized users have access to information. If the first two information security elements (see above) can't be compromised by an attacker, they could attempt to conduct attacks, such as a denial of service that would make the website inaccessible due to an insufficient availability of the server.

Access Control: Access control is a security technique to regulate who or what in a computer environment can view or use resources. It is an important security concept that minimizes the risk to the company or organization. There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Authentication: Authentication is a process to determine if anybody or item really is who or what they claim to be. Authentication technology provides device access control, by verifying whether the user's credentials match in an authorized user database or in a software authentication server. Authentication technology, users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID. Most users are most familiar with using a password, which, as a piece of information that should be known only to the user, is called a knowledge authentication.

Non repudiation: Non-repudiation is the assurance that something can't be denied legitimacy. Non-repudiation is a legal concept commonly used in security of information and a service providing evidence of information origin and data integrity. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity of that message.

2.3 Description of the System

- User friendly and efficient system
- Computer based system
- Multiple login System: Instructor and student
- Filtering option
- Plagiarism checking
- Easy to operate
- Notification for each post or comment
- Communicate with Student
- Give format of assignment
- Check format and requirements to submit

- Distribute mark evaluating plagiarism

Students Viewpoint

- User friendly and efficient system
- Computer based system
- Easy to operate
- Resubmission option
- Post and comment
- Multiple access

2.4 Identifying Assets

All losses or violations in the network should be decided in this stage. Assets may be concrete or abstract, specific or a case of use associated with them. Property and their security are very critical as many organizations, instead of securing property, tend to focus on risks, rendering the whole process vulnerable.

1. Web Server
2. Database
3. File System
4. Cache File
5. PHP CodeIgniter
6. User Login Credentials
7. Administrative Resource

2.5 Determining Threats and Vulnerabilities

With the data collected up to now, the threats and potential threats of the network can be identified. A source of risk is identified as any situation or occurrence that is likely to harm a system. Sources are categorized into physical, human and environmental sources according to the risk. By analyzing technical functionalities and sequence diagrams, it is possible to identify the threats and threat-sources. Afterwards the threats have to be correlated with the assets and with the entry points.

The purpose of this step is to create a list of system vulnerabilities that the potential sources of threats can exploit. If all threats and their situations are explained, the manipulation of the threats can be deduced. In the specific cases analyzed in the previous section, a table is filled in with key real vulnerabilities and corresponding menaces. A definition, name and the related hazard will then be allocated to each vulnerability. The use of assault trees is another way to evaluate whether the device is vulnerable to the established threats.

2.5.1 VULNERABILITIES:

Broken authentication: We did not manage session for user at server side. That is why a user can send request using id of another user randomly to get data.

Broken access control: We did not provide any access control policy in any user action.

Insecure deserialization: We did not check and validate deserialized input data to the logic of server-side programming.

No logging and monitoring: In ASM we did not configured any logger to monitor the user activities.

No load balancing mechanism: In ASM, we are using a minimum configurable server and it is not configured to balance high load traffic.

Vulnerable Objects

- Input Fields
- URLs interacting with the database.
- Large file upload

2.5.2 THREATS

- **XSS**: In several client-side web pages, if any Javascript code inserted it will be run at browser.
- **Brute force attack**: Hacker can make brute force attack to guess the password of students or teachers. In AMS we did not provide any request rate limit to users to protect brute force attack.
- **Phishing**: Hacker can clone my web page and can steal user privacy data.
- **SQL injection attack**: In ASM we did not filter SQL script in the request parameter. And some parameter comes from URL. So, it is vulnerable to SQL injection attack.
- **Man in the Middle Attack:** In AMS the connection is not secured and it does not have any secured certificate. So, there can be Man in the middle attack.
- **DOS/DDOS:** As there is no firewall or traffic monitoring from the server side, a DOS/DDOS attack can occur anytime.

2.6 Asset Mapping

In this step the list of assets is checked to determine if all the assets have been included. It is important also determining the variance of the assets and the risk that the owner of the assets is willing to accept, and based on these values prioritizing them. To assign a value to the assets is not easy because the value can be personal and the priorities of the people can be different, nevertheless here it has been suggested three different values.

- High, assets with this value have to be protected with a high level of security; they are directly linked to the control of the system, with services that require highly secure level, or that have a big financial value.
- Medium, assets linked to access to common services, not critical, but still important with an intermediate financial value.
- Low value for assets of minor importance.

In AMS, database, file, server are considered to be highly valued assets. The public information of AMS are considered to be lowly valued assets. CSS/Javascript templates, Cache files, Cookie files are medium valued assets.

2.7 Ranking of Threats

2.7.1 Rating Procedure

Threat rating procedure involves three steps -

- Calculation of severity value.
- Calculation of probability.
- Calculation of threat factor.

2.7.2 Calculation of Severity Value

Severity is the amount of damage or harm a hazard could create and it is often ranked on four points scale as follows:

- **Catastrophic (4)**: System loss, thereby requiring immediate cessation of the unsafe activity or operation.
- **Critical (3)**: System damage thereby requiring immediate corrective action.

- **Marginal (2):** Systems damage such that can be counteracted or controlled without severe injury, illness or other system damage.
- **Negligible (1):** System damages which will result in no, or less than minor, illness, injury.

2.7.3 Calculation of Occurrence Index

Occurrence is the likelihood of the hazard occurring and it is often ranked on a five point scale:

- **Frequent (5):** Likely to occur often in the life of an item
- **Probable (4):** Will occur several times in the life of an item
- **Occasional (3):** Likely to occur sometime in the life of an item.
- **Remote (2):** Unlikely but possible to occur in the life of an item.
- **Improbable (1):** So unlikely, it can be assumed occurrence may not be experienced.

2.7.4 Calculation of Threat Factor value

Threat factor value is calculated as,

Threat factor value = Severity value*Occurrence index

Table 1: Threat Ranking

Threat name	Severity value	Occurrence index	Threat factor value	Threat Rank	Mitigation
XSS	4	4	16	2	Filter URL parameters and validate

Brute Force Attack	4	2	8	5	Introduce Request Limit and Firewall
Phishing	3	4	12	3	Establish Secure connection
SQL Injection	3	2	6	7	Checking input parameters
Man in the Middle Attack	2	2	4	8	Use secured protocol-suite
DOS/DDOS	4	5	20	1	Introduce firewall, request limit and load balancing

2.8 Risk Management

Risk management helps to balance the acceptability and the ability. The details on which vulnerability poses the highest risk quality can be derived from the list of threats and vulnerabilities. To assess risks, the effects, damage to the property if the hazard happens, the extent of the fault and the possibility that the danger attempts to materialize are factors that need to be taken into consideration. The highly valued assets are given most importance for risk managements. After that, the medium valued assets are given importance and finally the low valued assets.

Conclusion

In this report, we went through the AMS project and tried to identify the risks and threats of the project. We identified some major threats and planned some mitigation procedures. Web projects are more vulnerable than other projects as these expose to more users concurrently. So, caution is required while handling them.