

Threat-Model-of-a-message-board-application

Giovanni Rosas-Marin



September 4, 2024

GCU

SWE-550

Assessment Description

The student should show the ability to represent an application using data flow diagrams and identify/analyze the threats associated with various components in the diagram using a common threat assessment model.

Write an essay overview of the threats identified in the threat model and include a screenshot of the completed data flow diagram. Describe the impact of the open source authentication component toward possible threats. Select one of the threats identified in the model and explain the best choice of action to address the risk from the following:

* Do Nothing
* Inform
* Mitigate
* Accept
* Transfer

The diagram needs to include elements representing the client, the open source authentication component, the application, and the database. Data flows should be shown to represent the authentication request, message of the day retrieval and display, and comment submission. All of these elements will need to be represented by the store, data flow, process, and actor icons, and a trust boundary should be provided.

A diagram with red lines and black text

Description automatically generatedIdentify 5 threats to the system and describe what could be negatively affected in the system if exploited, referring to the threat type using the STRIDE model. The threats identified should cover at least 4 parts of the STRIDE model, and at least one should involve the open source authentication component.

Threat Model Overview  
The data flow diagram for the threat model created for the message board application includes the components that where requested that is integrating Client/ User, Open Source authentication that I did an example to test with AWS Cognito for the login and registration and Authentication, the Main Application, Message-of-the-day after login authentication is approved, User would be able to comment on the message of the day and store the comment to the local database for the application. The Data flow represents the user requests, authentication validation and access message retrieval from the local database and gave permission to the user to comment and that will be stored in the local database and provided trust boundary for the main application, third party authentication and the local database that would normally be also stored in the cloud.  
The impact of using a third party authentication as AWS Cognito for the login and registration and login Authentication system. AWS offers security measures and the vulnerability within AWS Cognito if the plan selected has all the top tiers for authentication and for verification user 2 factor authentication. The potential breaches for data leaks and unauthorized access would be the main admin account and breach between the API connection. Regular monitoring to this AWS Cognito can help detect user that have not validated their user and be able to remove access if needed. Also having the option for encryption integrated to AWS for storing personal data and avoiding Tampering with user credentials.

5 Threats to this Message board Application

1. Spoofing:
   1. Description: An attacker will try to get a user’s credential to gain access to the application and this would go through the third-party service AWS Cognito
   2. Impact: This would compromise account would give access to unauthorized users to the data from the user and from there can create a breach the over data in the user database.
2. Repudiation:
   1. Description: User that are not approved will be denied access see messages and comment.
   2. Impact: If the account has issues in the authentication and been able to authenticate and the main database does not have the user register our an account issue it will need to track the user actions.
3. Elevation of Privilege:
   1. Description: The Message board app would have normal user and the admin and unauthorized users could gain elevated privileges.
   2. Impact: This access can cause data leaks and system manipulation that can cause over application closure by the attacker.
4. Denial of Service:
   1. Description: A hacker can cause deny service user by removing users accounts from database
   2. Impact: Users will not be able to recover messages and comments if account is deleted and will affect in the main experience and trust of the application and will not try to make new account.
5. Information Disclosure:
   1. Description: Data collected from the user that should be minimal due to more risks and vulnerabilities and because the application is a message board app and does not need sensitive information.
   2. Impact: But if there is a breach if would still get emails, names and get the app reliability and reputation damaged.

The Threat Modeling Diagram is crucial for having security and integrity for this Message Board Application and having an external authentication service integrated can create external vulnerabilities and risks that can have implementation for security and having the diagram trust boundaries can help identify the risk and where the information connection and data are routing and having the correct boundaries can protect vulnerabilities and risk.

Reference:

* Ransome, J. & Misra, A. (2014). *Core software security: Security at the source*. CRC Press. ISBN-13: 9781466560963.
* Aufner, P. (2020). The IoT security gap: a look down into the valley between threat models and their implementation.*International Journal of Information Security, 19*(1), 3-14. <https://doi.org/10.1007/s10207-019-00445-y>