# PA2562-Secure Software Development

Assignment-3

Threat Modeling Assignment

Monica Gattupalli

*moga20@student.bth.se*

National id 19991130-T308

# I. Introduction of EVV System

Exam Verification Verifier is an application which is used to examine the students who are attending the exam, which helps the Exam Leader to identify the individual. Exam takers need to log in and then takes a picture of then, this picture is referred to a unique Hash Id which is taken by the Exam leader to verify the credentials of Exam taker.at the time of exam the Exam Leader will use to check the picture of Exam taker.

# II. Threat Modeling

Under Threat Modeling we roughly discuss about the Assets, Architecture overview, Decompose the software, dataflow, entry points, trust boundaries, Threat Categorization.

## Assets

Some of the assets in the EVV system provide protection to the systems. Server01, Server02, Server03, and Mobile application are the names of the servers.

1. Server01: Server01's primary responsibility is to provide web services to the application's REST API.

2. Server02: Server02's primary responsibility is to provide a backend service that is connected to the database and hosts the credentials.

3. Server03: The main task of Server03 is to provide a backend service that is linked to the Rest web services that are used for image storage and retrieval.

4. Mobile application: Works on both the student's and the Exam verifier's phones.

## Overview of the Architecture

1. The student and Exam Verifier should log in to the application, and Sever02 will verify the details/credentials.

2. To write the exam, students should snap a picture, which will be saved on the Server03.

3. The examinee will login to Server01 to validate the Hash Id created by the photograph.

## Decomposition of Software.

In Decomposition of the system, we analyze the system in a deeper view, and we divide the system as flow diagram, entry point and trust.

## Data Flow

1. The exam verifier and student must both register in the system, with the credentials being saved on the Server.
2. If the exam verifier and student both log in to the system, Server02 will validate the user by comparing the credentials in the server.
3. If the student is genuine, he or she is permitted to take a photograph, which is kept in Server03, and the code generated by the photograph assists the student in attending the exam.
4. The student's mobile application will use internal storage to store the picture and the phone camera to shoot the picture.

5. In the exam verifier mobile, there is a verification mode for checking the student picture.

6. If the student is valid, the image is forwarded to Server03 to obtain the image's code.

7. The code is delivered to server01, which contains the student's application.

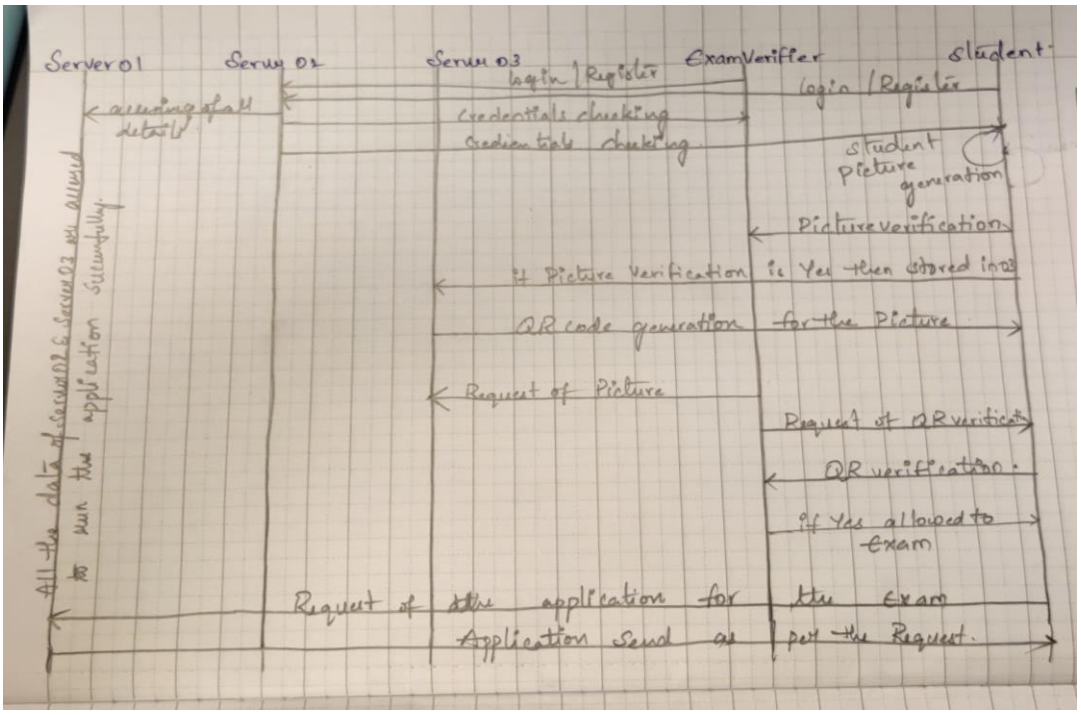


Figure-1 EVV system's dataflow diagram

## Entry point

The Entry point of the application deals with login part / scanning part in the system. In the given application there are 2 entry points

1. API entry point.

In the application on Server01 they are 2 entry points, The exam verifier and student should register and login to the mobile application by giving username/email and password, and these details are stored server02.

2. Application entry point

Student must login, if they want to attend the exam to do so they need to take picture of them and upload to the server03, that will generate a hash id which helps the student to write the exam and helps the Exam verifier to validate the student.

## Communication

To Fulfill purpose of the system properly there is a communication between

1. The Server01 and Server02 for checking the credentials of the of the student and exam verifier.
2. The server01 and server03 will have communication for getting the code and Hash ID which is used by the exam verifier and the student.

## Trust Boundaries

The only trust boundary in the EVV system is with the server, the student and exam verifier login/register which directly dealing with server02 without boundary, but when the student takes the picture to storage and the retrieval of then they need to communicate with server01 to access the server03 here where the trust boundaries arise.

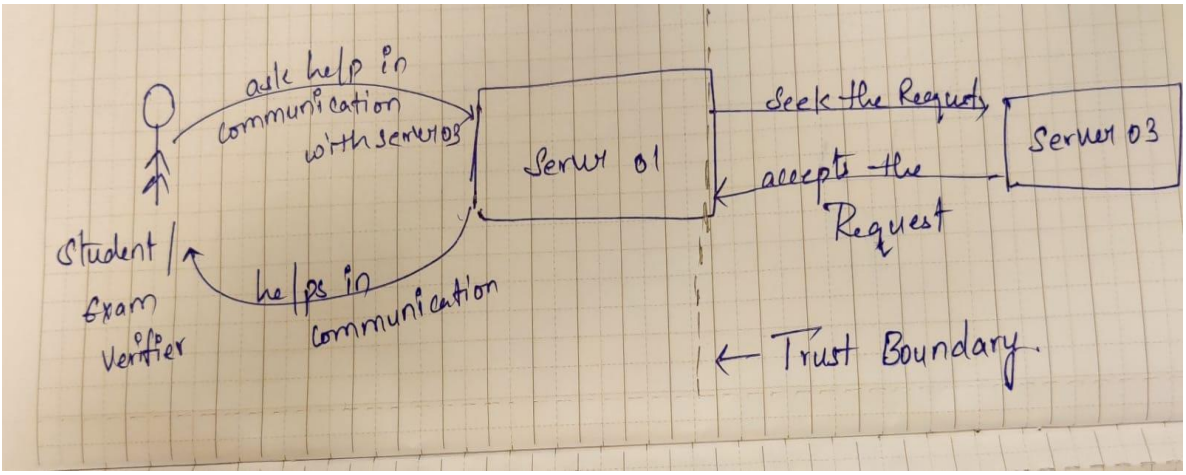


Figure 2: Trust Boundaries between server01 and server03

## III. Threat Categorization:

Threat categorization can be done using STRIDE method.

STRIDE

1. Spoofing: This threat deals with authentication of the user identity[1].
2. Tampering: This threat deals with the altering the personal data/ public data without knowing the admin/ authorized user[1].
3. Repudiation: This threat deals with the human trust, they will have the full authorized access to all part of the system. This type of attack is majorly seen in the when the bad person holds the highest authority in the organization[1].
4. Information Disclosure: This threat deals with the leakage of the data, this generally happens when an unauthorized user accesses the data. Sometimes accessing the source file when they are under backup by unauthorized users[2].
5. Denial of service: This threat happened when the intruder wants to access the personal details of the user without knowing the authorized user. This attack can be achieved by the interruption of the network[2].
6. Elevation of Privilege: This threat deals with the privilege of both authorized and unauthorized access of the data, this threat leads to different types of security allegation[2].

Below tables are the STRIDE categories of the different elements of the EVV system

Server-01

Security Challenges faced by server01 are Spoofing, tampering, Information Disclosure, Denial of service, Elevation privilege.

| Element | Spoofing | Tampering/ Information Disclosure | Denial of Service | Elevation of privilege |
|---|---|---|---|---|
| Server-01 | As server01 is mainly dealing with the REST API it can come across the Brute force attack to steal the credentials. It may also encounter the masquerading when the retrieval of the data from the server | Tampering can be experienced by the Server 01 when it undergoes Brute force attack the intruder my send the malicious files into the system, so that those files will cause any alternation in the data | Whenever the intruder what to disturb the flow of process then he will enter the network and down the server to the client. By doing this he can have the complete access of the client system with all passwords and the username | This security threat can be achieved in server 01 by just in cooperating different tools then making them as the authorized user to steal the data. |

Mitigations

| Element | Spoofing | Tampering | Denial of Service | Elevation of privilege |
|---|---|---|---|---|
| Server-01 | As, server01 deals with the running of the application, to access the application compatibly stopping the cookies acceptance and generating the OTP for every re-login into the server-01. | To Avoid tampering of data, we need to secure the private files by storing them under encrypted files are storing in the private access security files. | We can connect to the private Network of the organization, or security version of the IPV6 and IPV4, and limiting the access to the system at unused times. | Authorizing users at start of the session by implementing better security techniques, to avoid the unauthorized access to all users. |

## Server02

Security Challenges faced by server02 are Spoofing, tampering, Information Disclosure, Denial of service, Elevation privilege.

| Element | Spoofing | Tampering/Information Disclosure | Denial of Service/Elevation of Privilege |
|---|---|---|---|
| Server-02 | As Server-02 deals in storing the complete details of the student and exam verifier in this case spoofing can be done at by using IP address, for executing this the intruder should crack the session or he should use the session cookies | In this tampering comes at changing the password and username of user for ensuring this attack the intruder can alter the URL or he/she can use buffer overflow technique. BY altering the URL any information can be accessed without knowing the username and password | Denial of service can be done with same techniques as of server01, slowing down the server connection at any side of communication and stealing the details of the user for their personal use. |

Mitigations

| Element | Spoofing | Tampering/ Information Disclosure | Denial of Service/Elevation of Privilege |
|---|---|---|---|
| Server-02 | In the case of Server 02, the admin of the system should maintain the encrypted data like unique hash id and attaching better protocols in the network zone. | Hashing of data may help the server to avoid Tampering of user's personal data. We can also introduce the keys for every data to secure then and to store without losing then. | Choosing the better Firewall protection and making the firewall security level stronger to reduce the Denial-of-Service attack. |

## Server03

Security Challenges faced by server03 are tampering, Information Disclosure, Elevation privilege.

| Element | Tampering/Information Disclosure | Elevation of Privilege |
|---|---|---|
| Server-03 | By cracking the session cookies / cracking the network tampering and information disclosure can be done, just by inserting the malicious files or transferring the network packets. | This attack is done as same in server-02, can be achieved by using various tools, by getting user control of the system by manipulating of token. |

Mitigations

| Element | Tampering/Information Disclosure | Elevation of Privilege |
|---|---|---|
| Server-03 | Securing the IP information, observing the actives of the system and by reducing the access at the unused times. | To reduce the attack, we should employ some of the filtering techniques and reducing the remote-control session. |

## Mobile Application

Security Challenges faced by Mobile Application are Spoofing, Repudiation, Information Disclosure, Elevation privilege.

| Element | Spoofing | Repudiation | Information Disclosure | Elevation of Privilege |
|---|---|---|---|---|
| Mobile application | This can be achieved by DNS (Domain Name System) cracking, as this contains all the names, main domain, and the route path of the main system. And this allows spoofing of the credentials. | Everyone should have the self-control on them for not utilizing the given permission in a wrong way. | Owner of the mobile should take care that no other /unauthorized should use your mobile. They also should not have the access to the personal details like password, fingerprints, face detection etc. | As the system uses the internal storage and the memory for taking picture and storing it the owner of the mobile should take care about the permissions and the storage of the picture |

Mitigation

| Element | Spoofing | Repudiation | Information Disclosure | Elevation of Privilege |
|---|---|---|---|---|
| Mobile application | By using SSL (Secure sockets Layer) we can authenticate the user acceptance cookies in the mobile application, and filtering may help in reducing the attack of spoofing | Deny permission of personal and private file should be carried out for the users who are not known to the main user. | Accepting the different hashing techniques and employing different encryption techniques | This threat can be avoided by employing the techniques like taint tracking and history-based access control. |

## Exam verifier and Student

Security Challenges faced by Exam verifier and Student are Spoofing, Repudiation

| Element | Spoofing | Repudiation |
|---|---|---|
| Exam verifier and Student | This element can have the spoofing threat from 2 ways. First is, if the spoofing threat is occurred in the server01,02 and in the mobile application, in this case automatically the user will affect with threat. In the second case it affects directly by misusing the authorized credentials | User should take care about not performing any unethical things. |

Mitigations

| Element | Spoofing | Repudiation |
|---|---|---|
| Exam verifier and Student | Explain ever user about the different spoofing and how they will happen, circulate all safety measures to take care of spoofing. Better if they have any practical classes to know. | Make sure that all the participants are be limited about their permissions and the access to the authorized content. |

## Admin (Authorizing the credentials)

Security Challenges faced by Admin (Authorizing the credentials) are Tampering, Information Disclosure.

| Element | Tampering and Information Disclosure |
|---|---|
| Admin (Authorizing the credentials) | If the intruder entered the system either by DNS or by spoofing, he/she has the chance of Tampering of data of the credentials/ can also tamper any other data with has highly authorized. |

Mitigation

| Element | Tampering and Information Disclosure |
|---|---|
| Admin (Authorizing the credentials) | Admin must monitor the activities of the system proper checking must be done to secure the system from the Tampering and information. |

## Picture Verification and QR code generator

Security Challenges faced by Picture Verification and QR code generator are Spoofing, tampering, Denial of service.

| Element | Spoofing, Tampering | Denial of service |
|---|---|---|
| Picture Verification and QR code generator | As of the above (exam verifier and student) this can also be affected in the same way, the altering of QR code can be done and any another picture can be stored, and different picture can be sent to the exam verifier. This alteration can be done if the spoofing is happened in the system. | This attack led to take the clients currents session can change the picture and can also in cooperator of inserting of different malicious files, which leads to QR code generation. |

Mitigation

| Element | Spoofing, Tampering | Denial of service |
|---|---|---|
| Picture Verification and QR code generator | The mobile phone of the user should have secured file management and it should be able to find out the different threats without fail. | System should have the proper firewalls security so that, firewall defencer supports to not happen the attack. |

## Communication channel:

Security Challenges faced by communication channel are Spoofing, Tampering, Denial of service, Information Disclosure, Elevation of privilege.

| Element | Spoofing, Tampering, Information Disclosure | Repudiation | Denial of service | Elevation of Privilege |
|---|---|---|---|---|
| Mobile application | Intruder can come into the network and can interrupt the connection without knowing them and can spoof, tamper can be done. Information disclosure | Cracking the Network of the channel can lead to Reveal of complete data/ information, sometime this attack may give flexibility to the intruder to steal the data. | To steal the data at the time of communication the intruder can perform DOS technique. | The attacker will try to intercept the communication to identify the admin details. |

| Element | Spoofing, Tampering, Information Disclosure | Repudiation | Denial of service | Elevation of Privilege |
|---|---|---|---|---|
| Mobile application | Better to use organization network to avoid the spoofing and tampering, security protocols can reduce attack. | As this threat related to the network, better to employ better security protocols and filtering the network packets may help in reducing the risk. | As of above mitigation better to limit the rate of usage and using virtual private network may help in reducing the threat. | Maintain the firewall well and increasing the security of the database. Employing the self-network may help to reduce the attack |

## Reference


[1] "How to think about security and threats in your distributed application." https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model/ (accessed Mar. 12, 2022).

[2] "STRIDE Threat Modeling | What Is It? | Explanation and Examples | Read," *Software Secured*, Sep. 02, 2021. https://www.softwaresecured.com/stride-threat-modeling/ (accessed Mar. 12, 2022).