|  |  |  |
| --- | --- | --- |
| Threat | Property | Possible approach |
| Spoofing identity | Authentication | Passwords, login system |
| Tampering | Integrity | Digital signatures, checksums |
| Repudiation | Confirmation | Digital signatures, log-in system, log user activity |
| Information Disclosure | Confidentiality | Encryption |
| Denial of Service | Availability | reCAPTCHA |
| Elevation of Privileges | Authorisation | login system, verification |

In order to make the system secure, possible risks and dangers that come with the project were discussed. All goals, means and powers of an attacker were taken under consideration. Matters such as threat frequency and effect, preventive and corrective measures are examined in the next part of the document.

The threat of spoofing identity endangers the authentication property. A possible goal of the attacker might be to impersonate a different user. This is possible to achieve by preforming the man in the middle attack. The criminal can intercept the messages that the two users are exchanging and steal the signature of one of the users. A masquerade attack is an active type of attack usually performed by external attackers on the network. To overcome this threat implementing a login system and encrypting the signature can be a solution. This way the attacker won’t be able to get a hold of the user’s signature, nor send data as this specific user, because of the required password.

Tampering puts the integrity property in danger. A goal of such an attack is to modify the data while it is transferred from one user to another user. That means that the information a user is receiving is not the original that was sent. An external attacker can modify the message (which is an active attack) either online, offline or on the network. Mechanisms such as signing packets or checksums can prevent tampering. By signing we are sure that the message was sent from the right user, and thanks to checksums, once the information is coded it cannot be reverted. Because of that, the perpetrator either cannot access the data to modify it, or he cannot change the signature.

Repudiation threatens the confirmation property. In this case the attacker is denying the actions that they performed on the system. Such a violation can be performed in a system that is not keeping track of the user’s activity. Repudiation is an active attack that can be performed by an internal user, either offline, online or on the network. To prevent repudiation digital signatures or logging of user activity can be implemented. Thanks to such mechanisms the attacker will not be able to deny their action, because all his activity will be associated with themselves.

Information disclosure can be an attacker’s goal and threatens the confidentiality property of data used in our system. An attacker being able to disclose information means that they had access to data they should not have been able to see. This goal can be achieved by a number of attacks that our system may be vulnerable to. Some of those attacks could be passive, such as eavesdropping on the information sent, or active, for example blocking a message from arriving and then looking at the information. By using the EINOO model we can determine where and by whom our system could be attacked. External attackers could perform network attacks, such as the ones mentioned above, in order to gain access to unauthorized information and internal attackers which may be able to perform off-line attacks so that they could steal information. A feasible approach to this threat would be to use cryptographic encryption in order to secure the data in our system. This way if the data is intercepted by an external attacker using passive or active attacks or if an internal attacker carries out successfully an off-line attack the information they get is encrypted and therefore secure. However, if an attacker does manage to achieve information disclosure then the mistake we made would be at the Mechanism level, suggesting that the vulnerability comes from what encryption we use.

Denial of service type attacks represent a danger to the availability of the data used in our system. An attacker could be able to deny a user’s access to our system and such a goal could be accomplished through some attacks that the system may be vulnerable to. A denial of service attack is an active one and can be carried out by both external and internal attackers; such attacks usually occurring on the network. A login system is susceptible to DoS attacks by the use of bots that input wrong information for a large amount of times. In order to prevent this the system should ask the user to perform an action only a human would be able to before verifying the login credentials. The most widely used solution for this is the reCAPTCHA security service. However, attacks that have the goal of denying service to the user may take many forms and if such an attack does succeed we should take another look at the Threat Model and see what types of attacks we dismissed or we did not think of.

An attacker may also have elevation of privileges as his goal, such attacks resulting in them being able to receive higher rights in our system than they should. Attacks directed at achieving elevation of privileges could be active ones and may occur on the network; such attacks being most usually carried out by external attackers. In order to prevent unauthorized access a login system and verification of input may be useful in order to deter this threat. Another idea would be to ask for the user’s credentials again before authorizing them to perform an important action (e.g.: permanently deleting some files). Omissions in the Threat Model may, however, permit attackers to succeed in elevating their privileges.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat event | Incident likelihood | Incident consequence | Risk | Approach |
| Malicious human interference – masquerade attack  High | No log in system present, anyone can book a ticket.  High | All bookings are cancelled if not redeemed half an hour before the movie starts  Very Low | Low | No action needed |
| User/Attacker books every seat  High | No log in system present, anyone can book a ticket.  High | All bookings are cancelled if not redeemed half an hour before the movie starts  Low | Moderate | Monitor suspicious bookings |
| Malicious or accidental human interference – file deletions  High | There are no files or data stored locally on the user’s end  Low | All data is stored on a database  Low | Low | No action needed |
| Malicious human interference – DoS attack  High | No log in system or firewall present  High | Website will be unavailable  High | High | Configure a firewall with DoS mitigation |

The table above presents 4 of the most prominent threatening events that can occur on our system. Because anyone can access the Zinema website and book a ticket to a movie a few of issues are raised.

First of all, someone may book a ticket and give false information about themselves. The frequency of such a threat can be high as there is no authentication required to book a seat. However, there is a corrective measure put in place in order to ensure that the consequence of such an event is not that damaging; every booking expires of not claimed half an hour before the movie. Therefore, we decided that the risk of this particular threat event is low and no action should be taken.

Secondly, a user or attacker may book every seat and as a result make them unavailable for other users. Just like the previous threat the likelihood of this occurring is high but the consequence is low. However, we decided that the risk for this threat is moderate as the damage in terms of profit loss for the company is higher than the previous threat. A feasible approach to this would be to monitor for suspicious bookings and try to contact the person responsible about it. If there is no doubt that the intent of the person was malicious the booking should be cancelled.

Moreover, interference with files or data can occur on such a system quite frequently. As a preventive measure to reduce the likelihood of this event substantially, no files or other form of data are stored locally on the user’s end. If, however, data loss does occur in some way everything is stored in a database so the data can be retrieved, making the consequence of this threat low. As a result, the risk of this event is considered low and that no action is required.

Lastly, because the system uses a website to interact with the company’s clients and that anyone can access said website, DoS-type attacks can occur frequently. Coupling this with the fact that there is no firewall or log in system present results in a high likelihood for this to happen. What is more, the consequence of a DoS attack running successfully on our is system is also high, making the risk of this threat high as well. Therefore, a solution should be implemented to mitigate this risk and one of them would be to configure a firewall that can repel this type of attack.