Joshua Keifer

Maddy Preston

Anthony Ruvo

Professor Hardie

CSCI 360

17 October 2023

# Ticketing System Project Security

## 1. Technical Implications - Log In

Two additional security features will be implemented in the log in process. First, a captcha system will be implemented using Google's reCaptcha. This widget will prevent non-human actors from accessing the system. reCaptcha is available to Java web applications and only requires a JSON processing API. This will not significantly increase the program's complexity. Second, a two-factor authentication system will be implemented using the email associated with the account attempting to log in. A randomly generated token will be created and it will be sent to the aforementioned email address.

## 2. Technical Implications - Stolen Card

Three additional security processes will be implemented to prevent stolen or compromized cards from being used, two functions and one user process. The first function, checkCVV(), will ask the user to enter their CVV, it will then take it in as a string, ensure that it does not contain any invalid characters (non-numerical) and that it is of the proper length (3/4 digits), and convert it to an integer. The next function, verifyCVV(), will verify that the entered

CVV is valid - *shocking!* - by sending it to the bank. If the bank returns that the CVV is valid and associated with the card being used, the user will be able to complete the transaction. The additional user action will be inputting the CVV value at the time of purchase. This will not significantly add to the complexity of using the ticketing system or the complexity of its implementation.

3. Functional Implications - Log In

The functional implications of the additional security features in the process of logging in will ensure that the person using the system is a human and is not malicious. Two-factor authentication requires that the user can access their email to retrieve the code. This small security measure should not significantly alter the user experience. In addition to ensuring that the user trying to log in is a human, it will also prevent brute-force password cracking attempts. If someone were using a password cracker or some other way of gaining access to another user's account, the reCaptcha would stop it. The two-factor authentication will further make sure that the user has access to something else that exists outside of the system and belongs to the actual owner of the account being accessed.

4. Functional Implications - Stolen Card

In order to prevent malicious actors from using stolen or compromised cards to make unauthorized purchases, the user will need to enter the CVV associated with the card being used. Merchants are prohibited from storing CVVs, and while they are not required for card-not-present transactions, validating them will significantly increase the security of the

system and lower rates of fraudulent transactions. Users will either need to be in possession of the card or have the CVV memorized in order to complete the transaction. This implementation will not significantly alter the user experience as legitimate actors should be in possession of the card.