COURSE PROJECT

Authenticating Humans

Instructions

The goal of this project is for you to apply the concepts we cover in this course to an example system. You should continue working on the same system as you used in the previous two courses.

In **Part One**, you will identify the human principals that need to be authenticated and how to do the authentication with passwords.

In **Part Two**, you will decide which humans should be authenticated with physical tokens and how to do that.

In **Part Three**, you will identify which humans should be authenticated with biometrics and how to do that.

Except as indicated, use this document to record all your project work and responses to any questions. At a minimum, you will need to turn in a digital copy of this document to your facilitator as part of your project completion. You may also have additional supporting documents that you will need to submit. Your facilitator will provide feedback to help you work through your findings.

Note: Though your work will only be seen by those grading the course and will not be used or shared outside the course, you should take care to obscure any information you feel might be of a sensitive or confidential nature.

Complete each project part as you progress through the course. Wait to submit the project until all parts are complete. Begin your course project by completing Part One below. A Submit Assignment *button can be found on the final course project assignment page online. Information about the grading rubric is available on any of the course project assignment pages online. Do not hesitate to contact your facilitator if you have any questions about the project.*

Part One

Authenticating With Passwords

The first step is to identify the human principals that need to be authenticated in your system. You must then decide which humans should be authenticated with passwords, and you should design a password-based authentication scheme for those humans. Be sure to consider how the passwords will be chosen, how the passwords will be stored, and how to recover forgotten passwords.

The system under study is an electronic voting system and the focus is on online voting system.

The human principals that need to be authenticated are

1. ***the voters*****,**
2. ***the system administrators,***
3. ***electoral commissioners***

An eligible voter will be require internet in order to provided get authenticated. The system administrators and the electoral commissioners will not require internet.

1. **The voters will be required to choose their own passwords**
   An eligible voter will need to visit an enrollment centre to be enrolled unto the voting system. A secure link will be sent by the electoral commission to the voter via email or sms after the enrollment/registration. The link will contain a temporary username and password which will expire after a certain period of time. Note that the username which is a voter ID will be given upon registration at the enrollment centre. The user is then required to visit the link and update the password.

Choosing the password

The voter will be required to chose a combination of alphabets (both upper and lower case), numbers and special character like “@, !, # , -, + etc.” to create the password. The system will ensure that the voter uses at least one of the characters in the three sets.

Storing the password

Each password $pass_i$ will be salted with $salt_i$ and peppered with pep_i. The result will be hashed with a hashing function; the final result is then stored in a database on the sever.

Authenticating an eligible voter

To access the voting system, a voter needs to provide the login credentials. The credential are sent over a secure channel. A hashed version of the password provided is compared against the stored version. If the two hash values match, a push button token is generated on the voters smart phone. Access to the system is granted once the voter hits the button..

Recovering forgotten password

To recover a password, the voter has to provide his or her user ID and email address when requesting for a password change. An email containing a secure link is then sent to the use to reset the password. It will be good to send an sms to the use to verify whether or not hi or she initiated the password change.

2. **The system administrators and the electoral commissioners**
   A system administrator and an electoral commissioner will also need to provide a user ID and a password for the purposes of maintenance and obtaining election results. We use the same method above. The only difference is that the he

passwords of administrators and commissioners will be set at the sever and given to the them. This will be done within the local network of the electoral commission.

Part Two

Authenticating With Physical Tokens

You now need to decide which humans should be authenticated with physical tokens (including humans that will be authenticated using multifactor authentication). You should design a token-based authentication scheme for those humans. Be sure to consider how the humans get their physical token, what authentication protocol the token uses, and how to handle lost tokens. Feel free to revise some of your designs from Part One, if appropriate.

In this part we will consider authenticating with physical tokens. The system administrators and the electoral commissioners will need to use physical tokens and passwords to access the server. We have assumed that the system server will be placed in a secure room.

The system administrators and electoral commissioners will need a plastic ID card that will be used together with a PIN to gain access to the secure room. The plastic card has a chip that stores user information and PIN. Also, they will need to use multi-factor authentication to gain access to the voting system for maintenance and obtaining the election results respectfully.

1. **Obtaining the plastic ID cards and PIN**

   The management of the will create a department that will handle the creation and distribution of plastic ID cards to administrators and the electoral commissioners. The cards will be created and given to them on the same day; they will also have to choose their PINs upon creation.

2. **Authentication protocol for the plastic card and PIN**
   A user will need to insert his or her plastic card in a device that is installed to lock the door of the secure room. This device contains the credentials of the administrators and electoral commissioners. The user will need to enter his or her PIN. IF there is a match, the door will be open; it will not open otherwise.
3. **Handling lost plastic cards.**
   If a plastic ID card is misplaces, the user need to report this to the department handling the issuance of the cards. It will then be disabled. A new card with different PIN is then issued.

In other to obtain election results the electoral commissioner will need to use a multi-factor authentication. A user will need to enter a user ID and a password. A push button associated with the election sever and user account will be generated by the user's smartphone if the stored credentials matches what the user provided (**See Authenticating with passwords**). Clicking the button for approval will grant access to the election results. Access will be denied otherwise.

Part Three

Authenticating With Biometrics

The final step is to identify which humans should be authenticated with biometrics (including humans that will be authenticated using multifactor authentication). You will then design a biometric-based authentication scheme for those humans. Be sure to include what biometric will be used, how you will handle false-positives and false-negatives, and how you might handle humans who have objections to using your chosen biometric (if applicable). Feel free to revise some of your designs from Part One and Part Two, if appropriate.

In this final part, we look at authenticating humans with biometrics. The humans that need to be authenticated with this form of authentication are the system administrators and electoral commissioners.

The fingerprints of the system administrators and elector commissioners will be used for

authentication. A device with for the biometric authentication will be used to lock the door of the room hosting the election servers. To have access to the servers, a user will first need to open the door. A user will need to place his or her five fingers on the device that stores the fingerprints of each administrators and commissioners. Note that both the backend and frontend will be put in the same device; this will make the communication channel secure. Three attempts will be allowed; if it fails to authenticate a user after exceeding the three limit attpempt, an alarm will sound. In addition, a security personal, as well as a security camera will be in place to check activities of users. This will prevent spoofing attacks.

Furthermore, In addition to multi-factor authentication, a biometric authentication will be incorporated into the election server to add extra layer of security.

We have learned a biometric authentication system can fail to authenticate an individual it should (***false reject***) and it can mistakenly authenticate an individual it should not (***false accept***). Due to the sensitive nature of an electronic system, it will be advisable to decrease false positives and increase false negatives. This will help prevent unauthorised access to the server room.

Measuring fingerprints is quite easy as compared to other biometrics, and using this form of authentication properly with make it difficult for attackers to compromise the system.

REFERENCE

The course materials

To submit this assignment, please refer to the instructions in the course.