Systems Security

Course Project

Instructions

The goal of this project is for you to apply the concepts we cover in this course to an example system.

In **Part One**, you will choose your example system from a set of four possible categories.

In **Part Two**, you will identify threats of concern to your system.

In **Part Three**, you will come up with a set of security goals for your system.

In **Part Four**, you will consider how your security goals might be enforced.

In **Part Five**, you will examine how your system could have an effect on existing laws or social values.

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 course facilitator if you have any questions about the project.*

Part One

Choosing a System

The first step is to choose a system that you will later use as the object of your project work. Consider the four possible systems described below, and select one that best matches your interests.

1. **Secure anonymous communication:** This system enables users to communicate with one another secretly, accurately, and anonymously. Users can specify what information other users may learn about them and their communications.

2. **Electronic voting system:** This system enables users to privately express their preferences about some issue. The system produces a verifiably correct aggregate of all the users' preferences.

3. **Grade management system:** This system allows student grades to be stored by course staff, which may include TAs and professors, and to be retrieved by students. Grade information is stored in a back-end file system.

4. **Password manager:** This system allows users to create and store usernames and passwords for other systems. Users can manage their passwords across different devices.

Functional Requirements

For the system of your choice, define its intended behavior in further detail. To do so, invent a list of functional requirements. (See previous Read page for details about how "functional requirements" should be interpreted in the context of this course.)

A ***voting system***, is a set of rules that govern how elections are conducted and how the results will be determined. An ***election*** is a process by which people vote to choose a leader of a business, community or a country. An ***electronic voting system*** is a voting system in which the casting and counting of votes are done with the aid of electronic devices such as electronic voting machines or smart phones and computers connected to a main server via the internet.

In this project, our electronic voting system will consist of a standard web-application framework. A voting program will be sent from a server, hosting the voting system, via the internet to voters who can then access it from web browsers on their electronic devices. When users cast their votes, the information about the votes are sent to the server to be processed. Note that users are requires to register before they can use the system. We will assume the system will be used to elect the president of a democratic country.

Below is a table of the functional requirements of the electronic voting system.

User Type	Assets	User Story
Electoral Commissioner	Elections, the voting system	As an electoral commissioner, I can, together with my team, organise and conduct an election, per the constitution of a country. The elections will be held using an electronic voting system
Candidates	Electoral roll of eligible voters	As a candidate, I can access the electoral roll to verify its authenticity.
Voters	Registration, username and password, votes,	As a voter, I can register on the system to be added to an electoral roll of eligible voters. I can be provided with credentials such as a username and password in order to access the voting system on the election day. I can open the voting system on a computer connect to the internet using the credentials provided. I can cast my ballot by selecting my preferred candidate and then submit my ballot to the a server hosting the voting system to be counted.
Candidates	Collated ballots, election results	As a candidate, I view the election results and I can challenge any inconsistencies based on the collated ballots.
Electoral Commissioner	Collated ballots, election results	I can announce the election results from the collated ballots and declare the winner of the election.
Software developers	Election software	As the developers of the election software, we need to make sure the software is safe and secure.

Part Two

Threat Model

In this part of the course project, you will identify threats of concern to your system.

Against what kinds of attackers will your system defend? What are their motivations, resources, and capabilities? Don't just list vague, generic threats; make them specific to your system and its functionality.

One of the main difficulty in using an electronic voting system, in our case, an online voting system is ensuring the security of the system against attackers.

Attackers that the electronic voting system will defend against include the following:

1. Since the electronic voting system requires users to register before they can vote, attackers may want to ***misinform*** users about the registration and voting processes and also deny candidates the platform to encourage their followers to vote for them. These attackers use the media, including social media to misinform the public. Some of these misinformation are deliberate, whiles others are due to ignorance. Misinformation can lead to denying people their right to vote, confusion and mistrust.
2. Since the system processes users data, there are attackers who may want to hijack the data. These type of attacker's use a software called ***ransomware*** to attack the system which has the capability of encrypting the votes cast or the voters register and demand money to restore access.
3. Attacker who may want users of the system to loose confidence in the system, tarnish the integrity of the system. The motive of these attackers is to perform unauthorized process that will affect the election results. The confidentiality and integrity of the system will therefore be question. They use a ***malware,*** which is a software that can perform unauthrised processes in the voting system.
4. Attackers who may not want the voting system to be available online. These attackers may use malware and other tools to cause the system not to be available on the day of elections. Again the integrity of the system may be questioned by the users.
5. Attackers who may want to alter the election results. The motive of these attackers is to cause a particular candidate to win the election. The try to read the votes and alter the choices to of voters. This kind of attack is very dangerous and can cause chaos in the country.
6. Attackers who may want to steal passwords and usernames of voters. They may send emails to eligible voters; these emails may direct users to the wrong website of the voting system to collect personal details of users. Their intent is to do the voting themselves or disenfranchise eligible voters.

Attackers	Motivation	Resources	Capabilities
Misinforms	To misinform	Social Media	Disenfranchise, Cause mistrust
Hijackers	Gain money	Ransomware	It has the potential to encrypt the votes cast and the results of the election.
Attackers who want	To tarnish the integrity	Malware	The malware can perform unauthorised

users to loose confidence in the voting system.	of the voting system. To make voters loose confidence in the system		processes like encrypting election data stored in a database.
Attackers who may not want the voting system to be available online.	To tarnish the integrity of the voting system. To make voters loose confidence in the system	Malware	Cause the voting system to be unavailable.
Attackers who may want to change election results.	Alter election results in favour of a particular candidate.	Malware	Alter a voter's choice.
Attackers who steal user credentials.	To vote themselves or change users information to disrupt the voting process.	Emails, Malware	Changing user information.

If there are any non-threats, you should identify them as well. For example, you may wish to assume that some system components execute on hardware that is located in a physically secured machine room reachable only by trustworthy system operators.

We will assume that the server hosting the voting system cannot be tempered with physically or stolen due to heavy security presence.

Part Three

Security Goals

In this part of the course project, you will identify the assets and stakeholders involved with your system. This step should be easy because you already identified assets and users for each functional requirement. For each asset, identify its value to stakeholders.

The assets of the system are

1. The voting system
2. Elections
3. Election result
4. Electoral roll
5. Voter's credentials which include username and password

The stakeholders of the system include the following

1. The Electoral commissioner
2. The candidates
3. Voters
4. Attackers

First of all, an organised election is important to all stakeholders since without which there will be no president.

Next, the electronic voting system is one that will be used by the Electoral commission to collect the cast ballots, process the ballots and determine the winner of the election. The electoral commission need to make sure the system is safe and secure for the election to be free and fare.

The Election result is the decider; it determines who becomes the next president . It is very import to, first the candidates, since it determines their fate. Next, it import to the voters, since it is that which will let them get their choice.

The electoral roll or list of eligible voters is also very import to the electoral commission; it is the means by which voters are verified to be eligible to vote. It is also very import to attackers; if they are able to have access to it and, depending on their motive, the election with be disrupted. Note that getting the election disrupted will be their achievement. It is also import to the voters, since without which they will be disenfranchised.

Usernames and passwords are very import to the voter, since it is the means by which they get verified and then get the change to make their choice. They is also important to attackers, since they may use this to disenfranchise eligible voters.

Perform a harm analysis on assets; that is, identify all the things that might go wrong. You may find it helpful to use the template “Performing *action* on/to/with asset could cause *harm*.” (Although you are encouraged to rewrite statements made with that template into more naturally flowing English.) Be as thorough and creative here as possible; this is the step at which you’re most likely to overlook something that’s important and relevant to security.

A ***harm*** is a negative consequence to the assets of a system. Normally, attackers attack system to cause harm c**onfidentiality, Integrity** and **availability.** Using the proposed template, below are the actions and harm that may befall the voting system.

1. Power outages could cause the voting system to shut down or crush and make it unavailable. This may interrupt the voting process.
2. Erasing the electoral roll from the database could cause loss of eligible voters.
3. Overloading the server with client requests could slow down the internet and this may cause the system to be unavailable.
4. Over voting could cause the election result to be inaccurate.
5. Tempering with voters credentials in the database of the voting system could cause the them to be disenfranchised.

Now transform the harms you’ve identified into security goals using the template “The system shall prevent/detect *action* on/to/with *asset*.” Label each goal as being exactly one of confidentiality, integrity, or availability. Examine the feasibility of each goal in light of your threat analysis; if necessary, relax goals so that it is feasible to achieve them.

1. The system shall have a back up power to prevent power outages and crushes.
2. The system shall prevent erasing of electoral roll in the the database.
3. The system shall detect resources and client requests that slow down the server.
4. The system shall prevent over voting.
5. The system shall detect unauthorised user activities and prevent tempering with user credentials.

Part Four

Enforcement

For each security goal, explain how you might enforce it. Consider whether it would be best enforced by prevention, recovery, or deterrence. Attenuate your goals where appropriate to ensure that they can be met by the corresponding security mechanism.

For each of your recovery goals, identify which principals will need to be authenticated, what those principals are authorized to do, and what actions or states would need to be audited to enable recovery or deterrence.

Below are the explanations on how to enforce each security goals.

1. **The system shall have a back up power to prevent power outages and crushes:** There is the possibility for power outage. The electoral commission must provide a backup power like a generator or other sources of power to prevent the server hosting the electronic voting from shutting down or crushing should there be power outage.
2. **The system shall prevent erasing of electoral roll in the the database**: Attackers may send malicious programs to the server in an attempt to erase the database so that data about the eligible voters may be lost. Provide additional storage devices to back up or recover data collected from the voters. Also, provide an end-to-end encryption of data so that the attackers may not be able to understand the data. Finally, ensure that unauthorised people are unable to write to files on the server.

   Principals that need authentication are the voters. The voters are only authorised to register or vote. The database need to be audited to check requests from users to enable recovery of data.

3. **The system shall detect resources and client requests that slow down the server:** The system shall have monitors that detect processes that slow down the server and functions that free stop those processes.
4. **The system shall prevent over voting:** The system shall use functions to authenticate users before they have access to the system to vote. After voting the system will record the voter's vote to prevent over voting.
5. **The system shall detect unauthorised user activities and prevent tempering with user credentials.** The system shall use strong and updated encryption methods for voters credentials to prevent hacking.

Part Five

Public Policy

Discuss any ways your system could intrude on existing laws or affect social values.

There is no doubt that an electronic voting system provides increased efficiency, improved accuracy and greater voter turnout as compared to the traditional paper base voting. However, there are some disadvantages when implementing one.

First of all, opting for an electronic voting system as against paper based voting requires the amendment of existing laws to accommodate its implementation. In a democratic country where the opposition parties normally finds fault with the ruling party, there will always be mix feelings and trust issues about the implementation of the electronic voting system.

Going for an electronic voting system in an election requires the building of a safe and secure system. The trustworthiness of the system cannot be questioned. The confidence, integrity and availability of the system must not be compromised. Building such a system requires a lot of money which comes from tax payers money, meaning, it is very expensive to opt for this system.

When to use an electronic voting system is a question that depends on whether or not the majority of people support it or not. In the case where majority of the people do not trust the polling agents of a paper based voting system, then it will be good to implement an electronic voting system.

The question of privacy is also very important when using an electronic voting system. People normally shy away from giving their information when security and surveillance increases.

References

1. Electronic voting system, Wikipedi: https://en.wikipedia.org/wiki/Electronic_voting
2. Lecture notes
3. The European Union Agency for Cybersecurity, ENISA THREAT LANDSCAPE 2021, April 2020 to mid-July 2021

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