Concordia Institute for Information Systems Engineering (CIISE)

Concordia University

INSE 6150: Security Evaluation Methodologies

Assignment 1

Submitted to:

Professor Jeremy Clark

Submitted By:

Devina Shah

Student ID - 40238009

Question 1: STRIDE

1. **Spoofing**:
   Quebec System: Spoofing is a concern with the Quebec System, as basic details are required to fetch the vaccine status QR code of an individual, that can either be found through a simple software or guessed as per the article referenced [1]. After scanning the QR Code, the digital message includes name, birthdate and their vaccinate status, but no photo which makes it easy to spoof. To combat spoofing, the government states that an individual has to show their photo ID as well as the vaccine passport to crosscheck identity. While this is a step towards preventing spoofing, there is still an option of Fake photo IDs which can match the details of vaccine passport presented, thereby leaving room for concern. There were also measures in place of a hefty fines if caught doing identity spoofing.

   Physical System: As the physical system is a government issued photo ID card with vaccination status, there is very less risk of spoofing except if somebody makes fake IDs like that.

   Online System: The online system is safe from spoofing as every individual requires a unique identity number to access their vaccine status which includes their photo as well.

2. **Tampering**:
   Quebec System: Tampering is a concern in Quebec System as there have been known cases of Fake Vaccine Passports, where in there were two doses of vaccine administered in incorrect intervals or at timings when the clinics were closed to public [2]. Tampering was also done by an internal worker who had access to the system by registering false information in the vaccine registry [3]. To prevent this a probe was started to investigate it and take action on it.

   Physical System: Tampering of data is not possible in the physical system as once the physical government issued card has been distributed then no changes can be made to it. Any changes, if made to the database later, will be not reflected on the physical card.

   Online System: Online system is also not secure from tampering like the Quebec System.

3. **Repudiation:**
   Quebec System: Repudiation is a concern in Quebec System as the system in prone to tampering which means the attacker can access system logs and activity logs as well. Erasing or altering the logs exposes the system to repudiation attack after which any actions can be performed without leaving any footprints to prove validity.

   Physical System: Repudiation is not a concern in physical system as data cannot be altered on it and physical presence of an individual in needed.

   Online System: Online system works like the Quebec system and is exposed to Repudiation Attack as well. Attacker can erase logs from the server leaving no proof of validity of any action performed.

4. **Information Disclosure:**

Quebec System: Quebec System is at a risk of information disclosure. [4] A computer security expert managed to create an application which can read any QR Code and access the information on it. While the information in itself may not be harmful but if collated with other databases, it can provide a significant risk. To combat it, it was under the advisory to only disclose the QR Code to authorised person only who is using government approved application. Any other application may collect the data after scanning the QR Code.

Physical System: Physical System is not at risk of information disclosure as the card does not have any confidential information on it. It cannot be recorded without consent as the individual can keep the card back after showing to the authorised personnel.

Online System: Online system is at a high risk of information disclosure because the data shows a lot of personal information such as name and address together which can cause a risk if it goes in the hands of someone which malicious intent.

5. **Denial of Service:**

Quebec System: Internet connection is required to download & update the app in accordance with new policies and to keep the QR Code updated, but once the setup is done the app does not communicate with internet [5] thus keeping the data protected and denial of service not a concern. An individual can setup their QR Code and go to any place, and they would be able to show their vaccine proof without any hassle of server being down. Denial of service is a concern while the setup is being done, and if there is more load on the server then the app may crash or fail to update.

Physical System: Denial of service is not a concern as a physical card is being used to verify vaccination status

Online System: Denial of service is a concern as QR Code is scanned by the app that queries a server run by the Quebec government using HTTPS. Which means multiple pings on the server may result in overload resulting in delay or denial of service.

6. **Elevation of Privilege:**

Quebec System: Elevation of Privilege is a concern in Quebec System as the govt apps uses SHC specification which involves the use of public and private keys for verification. During the implementation in Quebec System, the code to download a third party issued key was still a part of the application and once a public key is downloaded, it can be used to validate any other passport, without checking if it matches the content of the issuer field [6]. This gives unauthorised and elevated privilege to users. As the system is vulnerable to spoofing and tampering, the attacker has an elevated privilege.

Physical System: There is no risk of elevation of privilege as a physical card is used for verification

Online System: As the system is vulnerable to spoofing and tampering, the attacker has an elevated privilege which can be used to perform unauthorised activities.

Part II: Evaluation Frameworks

Question 2: Six Security Evaluation Criteria

S1. Resilient to Phishing

This criterion describes if the data can be accessed through any phishing methods.

- No Dot - Can obtain data or access through phishing such as through calls or text
- Full Dot - Cannot obtain data or access through phishing

S2. Resilient to Tampering

This criterion describes if the data can be added, deleted or modified by an individual.

- No Dot - Data can be easily accessed and altered by anyone
- Half Dot - Data can be altered by someone with some approved privileges in the system such as an individual from the medical team or the app maintenance team etc
- Full Dot - Data cannot be altered

S3. Resilient to Denial-of-Service Attack

This criterion describes if the app can be brought down (crashed) through a DOS attack resulting in delay or denial of service from the app.

- No Dot - The system can be easily brought down resulting in denial or delay of service
- Half Dot - The system can be brought down but may not affect users at the time of use.
- Full Dot - Denial of service is not possible.

S4. Identifying Attacks

This criterion describes if an attack can be identified by the system to prevent it.

- No Dot - The system cannot identify attacks before, during or after the system is compromised
- Half Dot - The system can identify and notify of attacks after the attack
- Full Dot - The system can identify and prevent any attacks and is completely secure.

S5. Resilient to Spoofing

This criterion describes if the identity of a user can be stolen and can be used by others

- No Dot - Identity of an individual can be stolen and used
- Half Dot - Identity of an individual can be stolen but not used
- Full Dot - Identity of an individual cannot be stolen

S6. Disclosure of Confidential Data

This criterion describes if the app requires disclosure of confidential data and if the app protects it.

- No Dot - The user needs to disclose confidential information which will be visible to all users and can cause security concerns
- Half Dot – The user needs to disclose confidential information to use the app but it is not visible during vaccine status verification
- Full Dot - The user does not have to disclose any confidential information

Question 3: Six Usability and Deployability Evaluation Criteria

Usability Evaluation Criteria

U1. Easy to Access and Setup

This criterion describes the easy availability of the system to the user.

- No Dot - The end user is unable to access the application through any app store
- Half Dot - The user is able to find the app but is restricted to operate through their smartphone
- Full Dot - The app is easy to find and operate on a smartphone

U2. User Friendly

This criterion describes if the application is easy to learn and operate for any user

- No Dot - The application is extremely complex and is difficult to use by the user
- Full Dot - The application is easy to use with a user interface that is easy to navigate

U3. No Internet Connection Required

This criterion describes if an internet connect is required to operate the application.

- No Dot - A high speed internet connection is required to operate the app
- Half Dot - Internet connection is needed for some parts of the system
- Full Dot - Internet connection is not required after application setup

U4. No Password Required

This criterion describes if a password is required to operate the application.

- No Dot - A password is required to access the application
- Half Dot - A password is required to access some parts of the application
- Full Dot - A password is not required to access the application

U5. Recovery from Loss

This criterion describes that in an event of loss the user can reset the application

- No Dot - If the phone is lost or damaged, the app setup is not possible
- Half Dot - If the phone is lost or damaged, ned to visit authorised centre for reset of app
- Full Dot - If the phone is lost or damaged, the app setup is possible without any hassle.

U6. Nothing to Carry

This criterion describes that an individual does not have to carry any documents or additional device for using the application.

- No Dot - The user needs to carry a government issued device specially for this application.
- Half Dot - The user needs to carry a photo ID and smartphone for this application.
- Full Dot - The user does not have to carry any photo ID or any device for this application

Deployability Evaluation Criteria

D1. Cost Effective

This criterion describes that the deployment of system does not incur very high cost per user.

- No Dot - The app is paid and new equipment is required for every user
- Half Dot - The app is paid but equipment can be re-used.
- Full Dot - The app is free, and infrastructure as well as equipment can be re-used.

D2. Cross Platforms Availability

This criterion states that the application can be used on different platforms such as ios, android etc and on different browsers.

- No Dot - The app is compatible to only one kind of platform and browser
- Full Dot - The application is available to use on any kind of platform or browser

D3. Application Maintenance

This criterion describes that the app has regular updates upon feedback to keep up with policy changes and to fix any vulnerability found.

- No Dot - The app has no updates and vulnerabilities are not fixed
- Half Dot - The application has infrequent updates
- Full Dot - The application has regular updates in accordance with policy changes and to fix any vulnerability found.

D4. Customer Service

This criterion describes if the application has a good customer service to fix any user issues.

- No Dot - The application had no customer service
- Half Dot - The application has slow customer service
- Full Dot - The application has effective and fast customer service

D5. Load balancing

This criterion describes the ability of an app to manage large scale deployments and multiple users

- No Dot - The application cannot handle multiple users
- Half Dot - The application can handle within 100,000 users
- Full Dot - The application can handle more than 100,000 users and is scalable

D6. Mature

This criterion describes that the application has been tested for vulnerabilities by security experts and previously deployed on a large scale.

- No Dot - The application is relatively new and still has vulnerabilities.
- Full Dot - The application is completely secure and has been implemented on several occasions on a large scale.

Question 4: Evaluation Framework for Quebec System

Serial No.	Criteria	Status	Dot State	Explanation
Security				
S1	Resilient to Phishing	No Dot	○	Social Engineering can be used to trick an individual into giving out their QR Code so Quebec System is not resilient to phishing
S2	Resilient to Tampering	No Dot	○	There was news for internal employee tampering with data and fake vaccine passports [2][3] concluding that tampering is possible.
S3	Resilient to Denial-of-Service Attack	Full Dot	●	As the app does not require internet to function after the initial setup, the user will not face denial of service at the time of use. [5]
S4	Identifying Attacks	Half Dot	◐	The system cannot identify the attacks but based on patterns and kind of attacks it can be made secure for future.
S5	Resilient to Spoofing	Half Dot	◐	Spoofing is a possibility in Quebec System but using a photo ID to cross check identity is one step towards combating it.
S6	Disclosure of Confidential Data	Half Dot	◐	The app uses confidential data to set up the QR Code of the user but during verification it shows only limited and required data.
Usability				
U1	Easy to Access and Setup	Full Dot	●	The app is readily available on App store from where it can be downloaded easily. The setup is also convenient.
U2	User Friendly	Full Dot	●	The application has a basic user interface which can be self-learnt and easy to use by any user.
U3	No Internet Connection Required	Full Dot	●	After the basic setup the app does not require an active internet connection to use, which enables the user to use it in a weak or no network areas as well. Internet is required to install updates
U4	No Password Required	Full Dot	●	The application does not require a password to access the QR Code which eliminates the need to memorise one.
U5	Recovery from Loss	Full Dot	●	The app setup is based on basic user info which enables the user to setup the app again in case of loss or damage to their phone
U6	Nothing to Carry	Half Dot	◐	The user has to carry a photo ID with them along with their smartphone with the QR Code in their app.
Deployability				
D1	Cost Effective	Full Dot	●	After the initial cost of infrastructure setup, the equipment can be re-used and there are no in-app purchases.
D2	Cross Platforms Availability	Full Dot	●	The app is available to use on different platforms such as ios, android etc and can be accessed through any browser.
D3	Application Maintenance	Full Dot	●	The app has regular updates to include the latest public health recommendations and to fix any vulnerabilities.
D4	Customer Service	Full Dot	●	There is a dedicated customer service line to assist with any app related issues and to find alternate solutions if the issue persists.
D5	Load balancing	Full Dot	●	The app was deployed for the use by every resident in Quebec which implied that it has excellent load balancing capability
D6	Mature	No Dot	○	This app is one of its kind implementations that started after 2020 post covid, which implies that it is relatively new, and as researched it had some vulnerabilities when deployed. The app uses SMART Health Card standard which other countries are using as well developed specifically for issuing vaccine passports. [6]

References: -

[1] https://www.theglobeandmail.com/canada/article-quebec-politicians-covid-19-vaccine-passport-qr-codes-allegedly-hacked/

[2] https://www.mtlblog.com/quebec-has-started-slapping-people-who-used-fake-covid-19-vaccine-passports-with-tickets

[3] https://www.cbc.ca/news/canada/montreal/quebec-vaccine-scam-investigation-charges-1.6574159

[4] https://www.lapresse.ca/actualites/covid-19/2021-08-26/passeport-vaccinal/les-applis-de-quebec-defoncent-le-palmares-d-apple.php

[5] https://www.quebec.ca/en/health/health-issues/a-z/2019-coronavirus/progress-of-the-covid-19-vaccination/covid-19-vaccination-passport/help-for-vaxicode

[6] https://www.welivesecurity.com/2021/08/31/flaw-quebec-vaccine-passport-vaxicode-verif-analysis/?web_view=true