Concordia Institute for Information System Engineering
(CIISE)

Concordia University

INSE 6150 – Security Methodology Evaluations

Assignment -1:

Submitted to:

Professor Jeremy Clark

Submitted By:

Sai Chandra Sekhar Reddy Dwarampudi
40139233

□

Systems:

Vaccine Passports Recently, Quebec has introduced a system for residents to prove they have been adequately vaccinated against COVID19. Consider a few possible designs for a vaccine passport system used by a customer at a restaurant.

The Quebec System: the Quebec government issues a digital message with: (1) a name, (2) a birthdate, and (3) indication of a fully vaccinated status. This message is signed with the government of Quebec's public key. The signed message is encoded into a QR code which can be displayed on paper or in a smartphone app by the customer, along with a piece of photo ID. The restaurant checks with the assistance of an smartphone app: (1) the photo on the ID matches the person, (2) the name/birthdate on the ID matches the QR code, (3) the QR code indicates the vaccination status, and (4) the QR code contains a digital signature by the Quebec government.

A Physical Card System: the Quebec government will take a photograph and issue a physical card (like a driver's license or health card) with a name, photo, and vaccination status on it. It will be mailed to people vaccinated in Quebec. A customer displays this card to the restaurant. The restaurant checks (1) the photo on the card matches the person, and (2) the card displays the vaccination status.

An Online System: the Quebec government gives each vaccinated person a unique identity number encoded into a QR code which can be displayed on paper or in a smartphone app by the customer. The restaurant scans the code from the back of the card with a smartphone app from the Quebec government that queries a server run by the Quebec government using HTTPS. The server responds with the customer's name, ID, address, photograph, and confirmation of their vaccination status. The restaurant checks with the assistance of an smartphone app: (1) the photo matches the person, and (2) the app displays the vaccination status.

Question 1:

STRIDE is one of the evaluation frameworks used to assess a solution. It is an extension for CIA (confidentiality, Integrity, and Availability). Evaluation in STRIDE is based on six categories Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege.

Spoofing:

Spoofing is impersonating something or someone else. Authentication property is violated by spoofing.

Quebec System:

Verification is done through scanning a QR code which includes the details of the person which are signed by the government public key. By simply knowing the key and the encryption mechanism we can add our own people to the system and generate the QR code. As per the article in the itsworldcanada.com the hackers were able to create vaxicode for fake people.

Physical Card System:

Spoofing in this system can be done very easily by simply creating a card which looks like the government issued. Since no chip is present in the card it can easily be spoofed.

Online System:

Here everything is digital, so by hacking into the system the details of the person can be changed and moreover since the traffic is sent through HTTPS, pointing the tunnel and man in the middle attacks can be done for spoofing.

Tampering:

Tampering is to change the original data or code to something the adversary is interested in. Integrity property is violated by tampering.

Quebec System:

It is possible to implement some malicious code into the QR code but since the QR code is encrypted it will be difficult to tamper and replace the existing QR with some malicious code which works the same.

Physical Card System:

A physical card can easily be tampered with, by creating an exact replica of the card with the new values by using a printer.

Online System:

All the HTTPS communication in this system is done through a tunnel, an adversary can change the values whenever the authorities request the data from the server by man in the middle attack or pointing the tunnel towards him.

Repudiation:

Repudiation is claiming to have not performed an action. It violates Non-Repudiation Property.

Quebec System:

If the logs in system can be deleted by the adversary leaving no digital signature, then Repudiation can be performed. Since Spoofing and Tampering can be done in the Quebec system the adversary can go into the system and remove the logs. The authorities can only identify if something big failure occurs.

Physical Card System:

Since the physical presence of the person is required it's not possible to repudiate using a physical card.

Online System:

Repudiation in Online System works like the Quebec System where an adversary can simply remove the logs from the system.

Information Disclosure:

Information disclosure is to expose the information to an unauthorized person. Confidentiality property is violated by information disclosure.

Quebec System:

By using a QR scanner and scanning the QR of a person, the details can easily be disclosed. According to the article in the itsworkdcanada.com a group of hackers were able to get the vaxination status of the ruling and opposition party people.

Physical Card System:

Stealing the card or taking the photo of the card can make the information on the card easily disclosed to other people.

Online System:

Adversary can break into the channel if it is not properly maintained and leak the information to the public.

Denial of Service:

Denial of Service simply means to deny or downgrade the service to the users. Availability property is violated here.

Quebec System:

As per the welivesecurity.com, the Quebec vaxicode system app failed to work initially due to deployment and production issues but not due to cyber-attack. It is possible to bring down the system by flooding it with large number of requests to create the QR codes.

Physical Card System:

DOS attack cannot be done in card system since everything is manual and once a card is given there is no need of the servers or protocols.

Online System:

It is similar to the Quebec system where the system can be flooded with large number of HTTPS requests, making the system reach the maximum limit and bringing it down.

Elevation of Privilege:

Elevation of Privileges is to gain capabilities without proper authorization. Authorization property is violated here.

Quebec System:

Akinox includes the public key of the Quebec government in VaxiCode and VaxiCode Verif. However, even if it is not necessary, the code to download third-party issuer keys remained in the program. This flaw makes anyone download the public key which can be used to validate the other persons QR, even though he is not authorized to.

Physical card System:

Elevation of privileges is not an issue in the physical card since a card is given to each user.

Online System:

Hackers can be able to interrupt and change the communication between the user and government by adding an anonymous user and giving special privileges to the user.

Question 2:

Security Evaluation Criteria:

Security Evaluation is the comparison between various alternatives. There are no solutions, just trade-offs. Deliverable is a simple chart where full, half and no dot are represented whether the alternatives can meet the specific deliverable. There is more to security than real security (security, usability and deploy ability)

6 Security Evaluation Criteria:

S1: Resilient to Theft

Dot Selection	Property
○	Adversary is completely able to access the system and its database
◑	Gaining access to the user data by using the vulnerabilities in the vaxi-code
●	Not able to access the application and its databases

S2: Resilient to Spoofing

Dot Selection	Property
○	Not able to restrict any cloned QR applications and scanners
◑	
●	Various security updates for the application which can detect and track cloned applications and QR scanner.

S3: Resilient to Phishing:

Dot Selection	Property
○	Adversary able to get the QR and other details of the user through phishing emails.
◑	Attackers can change the application and send some ecommerce suggestions and various other adds to the end user just like app notification.
●	The application is completely resilient to any attacks and is designed only to generate QR and the data of the user.

S4: Resilient to Elevation of Privilege

Dot Selection	Property
○	The entire application and the user data are accessible by anyone, even unauthorized people.
◑	Authorized people can escalate their privileges to see the sensitive data at higher levels.
●	Only the authorized people at respective levels can see the data at their respective levels.

□

S5: Resilient to Tampering

Dot Selection	Property
○	Attackers can manipulate the entire user data by hacking into the system.
◑	Attackers can add only new user data but not modify the older ones.
●	Application and user data cannot be changed at any cost.

S6: Identify the Threats

Dot Selection	Property
○	The system is not able to detect and identify the attacks or the security breaches.
◑	The system can detect an attack after some time and needs manual support to stop the attack and bring back the system to normal state.
●	The system is completely autonomous, able to detect and prevent attacks in a few milli seconds.

Question 3:

6 Usability Evaluation Criteria:

U1: Bug Free

Dot Selection	Property
○	Unavailability of the system is extremely high. The application is susceptible to errors with frequent downtimes.
◑	Program works with periodic downtime yet is resistant to failures.
●	The system works without any downtime and the application is error free.

U2: User Friendly

Dot Selection	Property
○	Application can be accessed by only skilled people; UI is difficult for normal people to access.
◑	Only a few important parameters can be accessible to the normal user and the application consists of complex features which require customer support to access.
●	The application is accessible to everyone. The User Interface is simple and easy to navigate.

U3: No Passwords

Dot Selection	Property
○	Users need to enter the login details every time they login. The login details are also chosen by the system which are complex.
◑	Users once entered the credentials in a session need not enter the login details again the current session.
●	The application remembers the login details when the user login for the first time and never asks for the later logins.

U4: No Training Support

Dot Selection	Property
○	Users need training sessions to understand and use the application.
◑	Users need to be given just some basic information about the use of QR and how to scan it.
●	No training or information need to be given to the user. They can access directly by just downloading the application.

U5: Nothing to Carry

Dot	Selection Property
○	A physical proof of vaxi-code like a print of vaxi-code on paper need to be carried always along with passport.
◑	General usage of an id like driving license is sufficient to carry along with QR code in the mobile phone.
●	No need for physical ID, just the QR code in the mobile application is sufficient.

U6: No Dependency on the Internet

Dot	Selection Property
○	Need of compulsory high-speed internet (Wi-Fi/ 5G/5G) to access the application every time the user to login and gets verified.
◑	General internet with low speed is sufficient for the user to get verified.
●	No need for any internet for the user to log in and get verified. Once the details of the user are entered in the application.

6 Deployability Evaluation Criteria:

D1: Negligible Cost

Dot	Selection Property
○	Lot of capital cost is required for initial setup.
◑	Requires only the cost of the QR scanning devices and the cloud storage.
●	No cost is required at the user and verifier end. They can login and scan the QR's directly on their mobile devices.

D2: Easy Installation

Dot	Selection Property
○	Application is not available on app store or play store and user also need to pay the money to access the application.
◑	Able to download the application by using links using the exact keyword to search.
●	App is directly available in app store and play store free of cost.

□

D3: Cross-Platform Support

Dot	Selection Property
○	Application is restricted to a single platform like works just on only type of operating system.

◑	
●	Application is supported in various operating systems like iOS, Android, windows, and Linux.

D4: Regular Product Updates

Dot Selection	Property
○	No further modifications to the application once it is released.
◑	Very few minor changes to the application and also not periodically.
●	Periodically updating the application-based user feedback and major improvement to the app related to the security.

D5: Application Control and Authority

Dot Selection	Property
○	Application is completely controlled by the private firm which has developed the application
◑	Control is shared between the client (government) and the developer (firm).
●	Entire application is controlled by the federal and the state government (the main responsible authorities)

D6: Customer Support Availability

Dot Selection	Property
○	There will be no immediate support to the user and the user needs to wait for weeks to get the response from the corresponding authority.
◑	Customer support and a call back is immediately done on the same day as user request.
●	Immediate customer support, which works 24/7, is available related to any issue with the application.

□

Question 4:

Evaluation of Quebec System:

Criteria	Dot Status	Deployability
D1- Negligible Cost	◑	Quebec system requires QR scanner which is given to the verifiers and cloud storage to store the data.
D2- Easy Installation	●	Quebec vaxi-passport app is available in the app store and play store free of cost and is easy to download.

D3- Cross Platform Support	●	Vaxi-passport app is compatible with all the available operating systems in the market.
D4- Regular Product Updates	●	As per the developer firm reports, the firm is continuously adding new features and improving security for the app.
D5- Application Control and Authority	◑	The vaxi-passport application support team, various tools are being implemented to prevent data flow downwards.
D6- Customer Support Availability	◑	Immediate support for the vaxi-passport is not available but authorities respond to the email within a day or two.

Criteria	Dot Status	Usability
U1- Bug Free	◑	Application is mostly error free and has scheduled downtime whenever there is an upgrade.
U2- User Friendly	●	Application is accessible anywhere and anytime and no special skills are required to operate it.
U3- No Passwords	●	Vaxi-code app does not ask the user for login details.
U4- No Training Support	●	No need of any specific training for the users of the app. The UI is very simple, and the app is easy to understand.
U5- Nothing to Carry	●	Users do not need to carry any physical ID, just the QR code is sufficient to enter most of the public places.
U6- No dependency on the internet.	●	To display the QR code the application does not need any internet connection.

Criteria	Dot Status	Security
S1- Resilient to Theft	◑	Various vulnerabilities in the application are being attacked by the attackers and the developer firm is proposing multiple fixes.
S2- Resilient to Spoofing	◑	Multiple cloned vaxi-code apps are available in the play store which are being downloaded by the end user.
S3- Resilient to Phishing	◑	vaxi code can be a victim of phishing since attackers use app notifications to reach the user and attempt to obtain access to their information.
S4- Resilient to Elevation of Privilege	◑	Several tools are being implemented by the application support team to prevent any flow of information downward and protect data integrity.
S5- Resilient to Tampering	●	As of now there is proof of tampering with the vaxi-code app. The application is mostly tampered proof.
S6- Identify the Threats.	◑	No information about this parameter is available on the internet, the system is mostly secure.