Assignment 1

INSE 6150: Security Evaluation Methodologies

Due: **Wednesday Oct 13**. Upload on EAS by 15:00 (3:00 PM).

*Assignments are to be completed individually. Any reference to external material should be cited. Each student has available one slip day for use on one, and only one, assignment of his/her choosing. Using the slip day allows the assignment to be submitted at **noon** on the **Friday** that follows the due date without penalty. Late assignments will not otherwise be accepted (exceptions made for medical certificates).*

Assignments should be in a digital format (e.g., PDF) and uploaded to ENCS' EAS system under "Assignment 1." Please ensure you are registered for it well in advance of the deadline.

EAS: https://fis.encs.concordia.ca/eas/

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 the app displays the vaccination status.

STRIDE: Question 1 (12 marks)

Start with the Quebec system described above. Go through each of the 6 STRIDE categories. Starting with Spoofing, state what the Quebec system if spoofing is actually a concern with the system, what it does right to combat spoofing attacks and if any spoofing attacks might remain in the system. For each one, use no more than 4-5 sentences. Then state if the other systems (physical card and online) are different in terms of Spoofing and if so, how (using an additional 2-3 sentences maximum).

Repeat this for Tampering, Repudiation, Information Disclosure, Denial of Service, and Escalation of Privilege.

Part II: Evaluation Frameworks

This part of the assignment concerns the development of an evaluation framework for vaccine passports. For each part of the assignment, you should follow the tips and best practices described in class for making a useful framework. The criteria you develop should not fully overlap with the criteria used for evaluating passwords, as they are different topics (that said, if you feel some criteria applies to both, you are free to use it).

Question 2 (12 marks)

List 6 security evaluation criteria. For each criteria, say what is required to achieve a full dot, half dot, and no dot (max 2 sentences). You do not have to use a half dot if it is not appropriat. You may reuse parts of your answer to Question 1 in developing these criteria.

Question 3 (24 marks)

List 6 usability evaluation criteria and 6 deployability criteria. Once again, say (max 2 sentences) what is required to achieve a full dot, half dot, and no dot. Again, a half dot is optional.

Question 4 (36 marks)

You do *not* need to create an entire chart. Instead, do one evaluation of the “Quebec system” across your 18 criteria. For each, in a maximum of three sentences, say why you awarded a full dot, half dot, or no dot.

Useful Resources

Some examples of evaluation frameworks that might help you:

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf
https://oaklandsok.github.io/papers/unger2014.pdf
http://users.encs.concordia.ca/~clark/papers/2013_sp.pdf
http://users.encs.concordia.ca/~clark/papers/2015_usec.pdf
https://arxiv.org/pdf/1804.07706.pdf

Other Notes

The submitted PDF can be any reasonable page layout. Clearly mark the answers to each question.