Computer Security & Privacy

Assignment #1 (à rendre pour le mardi 2 février 2016 avant minuit)

Envoyez vos réponses à Tara Whalen à l'adresse tjwhalen@gmail.com

Question #1: Ecrire un avis d'introspection de sécurité

L'objectif principal de ce cours est de faire en sorte que vous commencez à penser le monde d'une manière différente - de développer une "security mindset" (~mentalité sécurité). Dans ce but, il est utile de travailler sur l'introspection de sécurité avec des exercices conçus pour vous faire réfléchir de manière basique sur le sujet, et dans des contextes où vous ne pensez pas forcément à la sécurité.

Votre objectif dans cette introspection est d'évaluer les problèmes potentiels de sécurité et de confidentialité dans les nouvelles technologies, d'évaluer l'âpreté de ces problèmes, et de discuter de la façon dont ces technologies peuvent potentiellement résoudre (ou se protéger contre) ces problèmes de sécurité et de confidentialité.

Vous pouvez choisir la technologie que vous voulez évaluer - cela peut être votre propre idée. Il peut s'agir de quelque chose que vous avez lu ou entendu dans les journaux, ou quelque chose que vous utilisez (c'est l'exemple de la Jeep connectée à un réseau et de la machine de vote électronique qui ont été vues en cours). Vous trouverez ci-dessous une liste de suggestions si vous ne parvenez pas à trouver un sujet par vous-même. Idées possibles pour une introspection de sécurité (vous pouvez cependant choisir votre propre idée):

- Le thermostat de Nest, une manière brillante d'éconimiser de l'énergie (https://nest.com/thermostat/meet-nest-thermostat/)
- Le produit Fitbit, une version sophistiquée d'application de fitness (https://www.fitbit.com/)
- Applications mobiles de services bancaires pour smartphones (Application qui vous permet de vous connecter à votre banque et de faire des transactions à l'exemple de Zenith Bank App) https://play.google.com/store/apps/details?id=com.zenithBank.eazymoney&hl=en)
- La connexion internet sur téléviseurs (Il en existe plusieurs types; https://en.wikipedia.org/wiki/Smart_TV)
- L'Audi A7 qui s'auto-conduit (http://www.dailymail.co.uk/sciencetech/article2259558/Audi-A7-The-incredible-self-parking-car-come-meet-youre-shopping.html)
- The Canary home-monitoring device (https://canary.is/)

Votre introspection sur le sujet doit contenir:

- Un résumé de la technologie que vous évaluez. Ce résumé doit être d'un niveau élevé, et doit faire un ou deux paragraphes. (L'idée est d'expliquer brièvement en qu'est cette technologie et/ou ce qu'il fait.) Statuez sur les aspects pertinents de cette technologie qui sont pertinents par rapport à vos observations ci-dessous. Si vous avez besoin de faire des hypothèses sur un produit, alors il est extrêmement important que vous statuez sur ce que sont ces hypothèses.
- Identifier au moins deux actifs (éléments ou informations -de différents types- qui doivent être protégés) et les objectifs de sécurité pour ces actifs, le cas échéant. Expliquer pourquoi l'objectif de sécurité est important. Cela doit tenir sur environ une ou deux phrases par actif/objectif. Exemple: "Un atout d'une machine de vote électronique est que les votes ont besoin d'être protégés; un objectif de sécurité est la confidentialité des votes afin que personne ne sache comment une personne a voté. Le vote d'une personne doit être gardé secret car dans le cas échéant, une personne pourrait être contraint à voter pour des candidats spécifiques."
- Identifier au moins deux menaces possibles, une menace étant définie comme une action par un adversaire qui vise à compromettre un atout. Donner un exemple adversaire pour chaque menace. Cela doit tenir sur environ une ou deux phrases par menace/adversaire.
- Statuez sur au moins deux faiblesses potentielles. Justifier votre réponse en utilisant une ou deux phrases par faiblesse. Pour le cadre de cette introspection de sécurité, vous n'avez pas besoin de complétement vérifier si ces potentielles faiblesses sont des réelles. (Vous pouvez trouver un certain chevauchement entre votre réponse avec celle que vous aviez donnée ci-dessus.)
- Statuez sur des défenses possibles. Décrire les défenses potentiels que le système pourrait utiliser ou peut-être utilise déjà pour remédier aux faiblesses potentielles que vous avez identifiées dans au point précédent.
- Évaluer les risques liés aux actifs, menaces et potentielles faiblesses que vous décrivez. De manière informelle, à quel point pensez-vous que sont importants cette combinaison d'actifs, de menaces et de faiblesses potentielles? (par exemple : Est-il peu probable que cela se produise, mais serait très dangereux si cela ce produit ? S'agit-il d'un problème mineur avec très peu d'impact?)

Conclusions: Donnez quelques conclusions basées sur vos précédentes discussions. Dans vos conclusions, vous devriez tenir compte « thoughtfully » (~de manière pensive) vos résultats ci-dessus. Si vous le souhaitez, vous pouvez élargir la discussion en incluant des problématiques d'une envergure plus grande (l'éthique, les possibilités d'évolutions futures de la technologie, ainsi de suite).

Cette introspection sur la sécurité doit être courte (environ 2 à 3 pages). Vos commentaires peuvent être sous la forme de liste à puces (comme celle utilisée précédemment - résumé, actifs, etc.)

- Si vous le souhaitez, vous pouvez écrire vos réponses en anglais ☺
- Si vous voulez un outil pour vous aider à réfléchir sur ces problèmes, vous pouvez essayer d'utiliser la «Security Cards» de l'Université de Washington (http://securitycards.cs.washington.edu/cards.html), il s'agit de «remue-méninges» sur la sécurité.
- Si vous voulez présenter quelque chose qui n'est pas vraiment une technologie (par exemple une sorte de système qui utilise une sécurité physique mais qui ne comporte aucune compilation en son sein), parlez-en avec moi pour voir s'il s'agit d'une idée convenable.

Question #2: Défense contre le « Stack Overflow » (en deux parties)

A. Comme nous l'avons vu en cours, Il y'a plusieurs manières de se prémunir d'un "Stack Overflow". Expliquez (brièvement) deux manières de prévention de votre choix, et préciser pour chacune :
    - Pourquoi cela fonctionne (en quoi cela arrête l'attaque?)
    - Quelles sont les limitations de cette méthode (pourquoi est-elle une solution imparfaite?)

B. Supposons que j'écris une partie de code pour un logiciel qui a besoin de pouvoir être exécuté rapidement (qui doit présenter de bonnes performances). Je m'inquiète aux attaques de type "Stack Overflow" sur mon logiciel. Existent-elles des méthodes de prévention qui ne constituent pas un bon choix pour ce cas particulier où je dois tenir compte de mes exigences de performances. Si oui qu'elles sont ces méthodes et pourquoi sont-elles probablement de mauvais choix. (Notez qu'il y'a plusieurs bonnes réponses possibles pour cette question ; je m'attends par conséquent à ce que vous justifiez votre raisonnement).