IFT-3275
Devoir 2
Évaluation de cas

SCÉNARIO A

Dans ce scénario, il faut assumer que la probabilité d'attaque est très élevée. Étant donné que l'information qui parvient jusqu'aux agents a probablement une valeur très importante aux yeux des autres agences de renseignement, il faut s'assurer que cette information est bien cryptée. Il faut aussi s'assurer que l'information est bien authentifiée car on veut être sûr que les agents ont reçu les bons ordres de mission et inversement que le CSE reçoive des information valide des agents. On veut également minimiser l'exposition des données aux adversaires, car même si la donnée est cryptée, une accumulation importante ou la possibilité de travailler longtemps dessus pose un risque accru. On parle dans ce scénario de se défendre d'une attaque visant à obtenir le contenu du portable ou carrément du serveur du CSE. Il faut également tenir en compte le *Denial of Service attack* qui peut-être utile pour un adversaire belliqueux.

En premier lieu, il faut inconditionnellement chiffrer le message. Peu importe ce qui est transmis, un message non chiffré constitue une brèche de sécurité majeure, puisque même s'il est sans importance, il transmet inévitablement de l'information sur le fonctionnement du système. Dans le cas qui nous intéresse, il faut utiliser un chiffre sûr et éprouvé. Et idéalement, un chiffre qui ne repose pas sur des difficultées technologique actuelle (comme RSA). Puisque les messages risquent fort probablement d'être intercepté par des agences étrangères, on doit assumer que ces agences déploiront tous les efforts nécessaire pour lire le fichier. Le chiffrement RSA est peut-être sûr aujourd'hui, mais dans dix ans, ce sera probablement facile pour une agence de sécurité de craquer un clef datant de 2016. Cependant, on peut utiliser RSA pour le *handshake* étant donné que cette information n'as aucune valeure une fois la transmissions terminée. Cela implique de changer de clef RSA de temps en temps, mais cela s'incorpore facilement au processus de maintenance.

Mainenant traitons de la connexion que le système devra établir avec le portable. Idéalement, cette connexion serait effectuée sur un canal secret, de sorte que la probabilité d'être écoutée reste basse, mais il faut toujours assumer que le canal est surveillé. Le plus important au moment d'établir la connexion est l'authentification. On place évidemment un pare-feu sur le système du CSE et on veut que le pare-feu n'accepte de transmettre que les connexions qui sont authentifiée comme provenant des agents. C'est la même chose du côté des agents; les portable ne doivent accepter que les transmissions provenant du CSE. Il serait d'ailleur utile de limiter toute connexion autre que celle avec le CSE sur les portable; en allant sur internet les agents exposeraient leur portable aux virus ce qui est dangereux particulièrement dans le cas d'un cheval de troie, mais nous y reviendrons. Finalement, il est important que le pare-feu soit prêt à contenir une attaque de type dénis de service d'envergure importante. En effet, supposons que le CSE veut faire parvenir de l'information critique à ses agents (ou

l'inverse) le serveur doit impérativement resté fonctionnel.

Sur les machine comme telles, l'authentification biométrique est a privilégier afin d'éliminer toute trace de mot de passe. Même si l'ordinateur ne télécharge pas les fichiers, il les aura quand même en mémoire, il faut donc que la représentation des fichiers en mémoire soit également encryptée. Au point de vue conception, on pourrait créer un ordinateur sans disque dur (seulement avec RAM à l'exception d'un *boot drive*) de sorte que dès que l'ordinateur est fermé toute l'information disparait. Il serait également pertinent de l'équiper d'un dispositif de “self-destruct” qui détruit toutes les composantes qui pourraient compromettre le CSE quand le portable détecte une attaque ou quand l'agent le spécifie. Par exemple, le portable pourrait effacer le programme qui effectue la connexion quand il détecte qu'un usager accède au dossier contenant sa source.

Finalement, du côté du CSE, le système se doit d'être inattaquable. Même si la connexion est chiffrée puis authentifiée, il doit assumer qu'elle n'est pas sûre. Quand le pare-feu reçoit une connexion d'un agent, il doit envoyer un message au serveur principal, lui demandant de transférer tous les fichiers auquel l'agent a accès sur un ordinateur tampon. La table de droit d'accès doit être mise à jour souvent pour chaque agent afin que la quantité de fichiers transférés sur l'ordinateur tampon soit raisonnable, et pour s'assurer que ledit agent n'a accès qu'à ce dont il a besoin. Quand ce sera fait, la connexion sera coupée avec le serveur, puis le pare-feu relayera l'information à l'ordinateur tampon. De cette façon, aucune connexion n'est effectuée avec le serveur depuis l'extérieur. Une fois que l'agent à terminé ce qu'il a à faire, si il n'y a aucune modification, le contenu de l'ordinateur tampon est supprimé en entier, sinon il doit passer par une “scrubbing-station” avant que les fichiers ajoutés ou modifiés soit incorporés au serveur.

Cette dernière étape est très importante, car avec un cryptage sûr et une authentification sûre, la seule option pour un éventuel attanquant est d'infiltrer le système par un cheval de troie. Il faut donc passer chaque document envoyé par l'agent en revue afin de s'assurer qu'ils ne contienne pas de code exécutable. Tel que mentionné précédemment, la meilleure manière de s'assurer que les portables des agents n'aient pas accès au réseau internet. Les connexions entre les ordinateurs doivent également suivre un modèle de protection strict. D'ailleurs au gouvernement il est interdit de connecter un média avec un certain niveau d'accès à un media de n'importe quel autre niveau sans que celui-là ne passe par un examen approfondi, donc une clef USB marquée PROTÉGÉ B, ne peut qu'être branchée dans les ordinateurs PROTÉGÉ B. C'est en quelque sorte l'intersection entre Bell-Lapadula et Biba. Il est primordial que ce protocole soit respecté car les clefs USB sont probablement, après internet, la source la plus probable d'infection par un trojan. Il est donc important de conscientiser tous les employés du CSE à la politique de sécurité.

Dans le cas présent, presque toute les attaques sont probables et doivent être envisagées. Évidemment, le serveur du CSE n'est pas connecté sur le Wi-Fi et on n'y installe pas de backdoor, mais toutes les autres attaques sont des menaces réelles pour lesquelles il faut être prépraré.

IFT-3275 Philippe Caron
Devoir 2 26 avril 2016

SCÉNARIO B

Contrairement au cas précédant, dans le cas d'un démarreur à distance, l'information a très peu d'importance. Tous le monde sait que le message transmis par le démarreur est “démarrer”. La protection des communications avec le téléphone est également de faible importance dans la mesure ou celui-ci ne génère par de *feedback*. On doit donc concentrer les efforts sur l'authentification du téléphone au yeux du véhicule. Si on veut que le démarrage semble instantanné, il faut que le nombre de caractère envoyer à la voiture reste en bas de 160, de sorte à n'envoyer qu'un seul texto, ce qui élimine d'emblée l'authentification par RSA. L'attaque la plus probable pour un tel scénario dont il faut absolument se prémunir est le *packet sniffing*. À l'échelle du réseau cellulaire, on est certain que les ondes voyagent au moins une cinq centaine de mètre avant de se dissiper; pour un pirate c'est la situation idéale, car il peut commettre ses méfaits à bonne distance, dans l'anonymat total, avec très peu de probabilité d'être détecté.

Pour ce qui est du *feedback*, la solution est simple, le téléphone ne répond pas au messages qui lui sont envoyés. En effet, dans le cas d'un démarreur, la relation est purement unidirectionnelle, toutes les informations que la voiture peut répondre, comme “démarré avec succès!” sont des informations que quiconque regarde la voiture peut obtenir.

Afin de se protéger contre les attaquants qui *sniffent* les paquets, il faut que le message change à chaque fois d'une manière qui ne donne pas d'information sur le code comme tel. Le plus simple serait d'initialiser un *block cipher* style CBC ou CTR avec un block de taille 160 caractère dans la voiture, et de faire la même chose dans le téléphone. Le téléphone chiffre un bloc, l'envoie à la voiture, la voiture chiffre un bloc et compare les résultats. Si les blocs correspondent, elle démarre. La différence entre cette méthode et une méthode qui consisterait à envoyer une séquence prédéterminée de nombres aléatoires est qu'avec cette méthode on peut faire tourner le fichier source en rond et les séquences produites seront toujours différentes, alors qu'avec la séquence aléatoire non cryptée, le pirate peut trouver le *pattern*.

Le pirate pourrait voler le fichier source dans la voiture, mais rendu là autant voler la voiture tout de suite. On pourrait également envisager une attaque de type *Denial of Service* ou *Bruteforce*, mais il suffit de bloquer la réception de tout message provenant d'un numéro envoyant plus de 10 textos en 5 secondes par exemple. Et dans le pire des cas, il suffit de placer un *breaker* dans l'application qui saute quand celle-ci se sent menacé, et qui peut-être réinitialisé manuellement par l'usager. La conséquence de devoir démarrer sa voiture en utilisant les méthodes conventionnelles est négligeable et ne justifie par une système bien plus complexe.

IFT-3275 Philippe Caron
Devoir 2 26 avril 2016

SCÉNARIO C

Il y a plusieurs angles d'approche pour un attaquant dans ce scénario. On peut tenter de masquer l'émission des RFID pour voler du matériel, on peut tenter de voler l'identité d'une des cartes de paiement, et on peut plus simplement tenter d'utiliser les clients comme intermédiaires; c'est-à-dire placer de la marchandise qu'il n'ont pas acheter dans leur panier, et la leur reprendre à leur insu à la sortie.

Une manière de réduire le risque de façon considérable est de s'assurer que les clients doivent effectuer un geste avec la carte, ou au moins qu'ils prennent conscient du moment de l'achat. Une carte à puce conventionnelle est parfaite pour la situation. Quand les clients sortes du magaisin, un écran s'allume et leur annonce le montant qu'ils ont a payer, il n'ont qu'a approcher leur sac ou leur porte-monaie du lecteur pour que celui-ci effectue la validation. Exactement comme lorsque l'on prend le métro.

Hormis les méthodes physiques, (ex: construire une cage de farad dans son sac a main, ou y placer un *degausser*), il ne reste plus que deux options aux pirates, attaquer la carte ou attaquer le système. Pour le cas présent, nous ne traiterons pas de l'attaque au système car des pirates qui parviendraient à s'introduire dans un système informatique de magasin n'irait certainement pas se compromettre en volant de la marchandise, et se concentrerait probablement plus sur les numéros de cartes de crédits, ce qui est bien plus facile et bien plus rentable. Mais ce cas en est un autre, nous allons émettre l'hypothèse pour le cas présent que le système informatique de la compagnie est sûr. À ce moment, tous le problème reviens à l'authentification. En effet, la carte ne fait qu'échanger l'identité du client avec le lecteur, aucune autre information n'est transmise.

Dans ce cas, l'attaque la plus plausible est une attaque par *sniffing*. Dans le temps des bandes magnétiques, les malfaiteurs installaient de petites extensions sur les fentes qui semblaient faire partie du guichet, ainsi ils pouvaient lire les cartes des utilisateurs. C'est à peu près le même genre d'attaque qui risque de se produire ici. Un client enregistré fait semblant de payé et il dépose un petit récepteur sur le gichet en même temps. Dans ce contexte, il est important de sensibiliser le gardien de sécurité à cette éventualité.

Vu que le lecteur ne risque pas d'être connecté directement à l'internet, on devrait distribuer au client des cartes à authentification dynamique. On pourrait même ,si le commerçant est prudent, distribuer des cartes à authentifications combinées. Cependant, puisqu'on spécifie que le système de surveillance est à la fine pointe de la technologie. En pratique, on pourrait se contenter de cartes à authentifications statique, il suffit que le lecteur tienne un log des paiements. Quand une activité suspecte est détectée, on regarde la vidéo à l'heure de l'achat et on identifie immédiatement le coupable. Il n'y a pas grand avantage pour les pirates à clôner des cartes si les chances qu'ils se fassent prendre sont importantes.

La technologie de carte à puce est plus qu'éprouvée et omniprésente, il est donc impensable que des gens qui voudraient la craquer dépensent autant d'effort pour voler une paire de chaussure. Ce scénario ne semble pas comporter de risque notable.