Protégez votre site Internet avec Always On SSL

Développer et préconiser les meilleures pratiques à adopter contre les menaces à l'encontre de la confidentialité, de l'identité et de la sécurité des services en ligne, des agences gouvernementales, des organisations et des consommateurs, et ainsi améliorer la confiance et l'assurance en ligne.

Mise à jour du 16 mars 2012

Table des matières

Résumé

La confiance et l'assurance du client constituent les bases sur lesquelles Internet a été fondé. Les plus grandes entreprises commerciales et les sociétés financières internationales utilisent depuis déjà longtemps les technologies du SSL/ TLS (Secure Socket Layer and Transport Layer Security) pour sécuriser les transactions et les communications de leur clientèle. Ce modèle de sécurité est utilisé depuis plus de dix ans pour assurer la confiance envers les navigateurs Internet, les appareils mobiles, les e-mails et autres applications Internet, et il reste aujourd'hui une valeur sûre. Les sites Internet et toute tierce partie utilisatrice utilisent le protocole SSL/ TLS pour protéger les informations confidentielles, telles que les mots de passe et les numéros de cartes bancaires. Le nombre de sites qui utilisent le SSL/ TLS a plus que doublé depuis 2005, et, aujourd'hui, on estime qu'il existe plus de 4,5 millions de sites Internet protégés par des certificats SSL émis par une Autorité de Certification.[1]

Mais avec le développement du Web 2.0 et des réseaux sociaux, les utilisateurs d'Internet passent de plus en plus de temps en ligne et sur des sessions privées, et communiquent bien davantage que leurs numéros de carte bancaire. De nombreuses personnes utilisent Facebook, Gmail et Twitter comme moyen de communication principal. Le paysage mondial de la menace a également évolué avec la prolifération des botnets, des malwares, de la perte de données, de faux e-mails, de la fraude en ligne et autres défis pour la sécurité et la confidentialité. Malheureusement, les pratiques de sécurité du Web n'ont pas toujours été en phase avec ces changements. De nombreuses organisations utilisent le protocole SSL/ TLS pour crypter les processus d'authentification lorsqu'un utilisateur se connecte à un site, mais les pages suivantes dans la session d'utilisateur ne sont pas incluses dans la démarche de cryptage. Cette pratique est risquée car les utilisateurs du site restent vulnérables aux attaques malveillantes en ligne, ce qui peut causer l'exposition des informations de milliers d'utilisateurs inconscients des dangers encourus par une simple visite sur un site de confiance.

L'OTA (Online Trust Alliance) fait appel aux mondes de la sécurité, des affaires et de la publicité interactive, afin de travailler ensemble et protéger les consommateurs de tout danger. Il incombe à chaque partie concernée de faire le nécessaire pour protéger la confiance et l'assurance des clients en adoptant des pratiques de sécurité qui sont indépendantes, faciles d'intégration et mondialement accessibles. L'une de ces pratiques est l'AOSSL (Always On SSL), une approche qui consiste à utiliser le protocole SSL/ TLS sur l'intégralité d'un site afin de protéger les utilisateurs grâce à une sécurité continue, et ce de l'ouverture de session jusqu'à sa fermeture. Always On SSL est une mesure fiable et pratique qui devrait être intégrée sur tous les sites Web sur lesquels les utilisateurs partagent ou accèdent à des données confidentielles.

Ce Livre Blanc met en lumière le besoin impératif d'intégrer Always On SSL, ainsi que les étapes à entreprendre pour offrir une protection totale aux utilisateurs de sites. Il comprend également des comptes-rendus de quatre organisations, Facebook, Google, PayPal et Twitter, qui ouvrent la marche avec Always On SSL dans un effort commun pour rendre Internet encore plus sécurisé.

[1] Enquête Netcraft de février 2012 SSL

L'OTA souhaite mentionner l'implication du OTA Steering Committee et de ses membres, tels que AllClear, DigiCert, Epsilon, IID, Intersections, LashBack, MarkMonitor, Message Systems, Microsoft, PayPal, Pitney Bowes, Publishers Clearing House, Return Path, Secunia, Star Marketing Group, Symantec, TrustSphere, VeriSign, Inc et GlobalSign.

Parmi ces remerciements, l'OTA souhaite également adresser une mention spéciale à Alex Rice de Facebook, Adam Langley de Google, Andy Steingruebl de PayPal, Quentin Lui et Rick Andrews de Symantec et Bob Lord de Twitter pour leur contribution et leur collaboration à ce projet.

Toute mise à jour de ce rapport sera mise en ligne sur https://otalliance.org/aossl.htm. Pour tout commentaire, merci d'envoyer un e-mail à staff@otalliance.org.

Le besoin d'une protection continue

Les utilisateurs d'aujourd'hui ont accès à une variété plus grande encore de services grâce à Web 2.0 qui leur offre une expérience riche, interactive et personnalisée, tandis qu'ils effectuent des recherches, échangent des données ou font du shopping en ligne. De nombreux services utilisent les cookies des navigateurs pour rendre de telles expériences possibles, en créant des sessions sécurisées continues. Lorsqu'un utilisateur ouvre une session sur un site, il doit généralement indiquer son nom d'utilisateur et son mot de passe pour garantir son identité. Le serveur Web génère ensuite une identité unique d'utilisateur et la transmet au navigateur qui la cache dans un cookie. Le navigateur renvoie le contenu caché du cookie vers le serveur Web à chaque fois que l'utilisateur connecté se sert du site, et le cookie reste actif jusqu'à son expiration ou son élimination.

HTTP et cookies non sécurisés rendent l'utilisateur vulnérable aux attaques

De nombreux site Internet utilisent le protocole HTTPS pour transmettre des informations de connexion sur un canal crypté par du SSL, mais c'est le protocole HTTP de base qui est ensuite utilisé pour le reste de la session. Ce système protège le mot de passe de l'utilisateur, mais le cookie, y compris l'identité de la session, est transmis en texte brut lorsque le navigateur envoie des demandes continues vers le nom de domaine, ce qui rend l'utilisateur vulnérable aux attaques de piratage informatique. Ce système peut également donner à l'utilisateur une fausse sensation de sécurité car il pense à tort que l'intégralité de sa session est protégée, alors que seule l'ouverture de session est cryptée.

Certaines organisations utilisent le protocole HTTPS sur l'intégralité de leur site, mais elles omettent de sécuriser les cookies. Ceci représente également un risque car souvent l'utilisateur n'entre qu'une partie de l'URL (sans entrer « https:// » par exemple), et les cookies sont alors exposés lors de cette première demande, avant même d'être redirigé vers une page sécurisée par le protocole HTTPS. Un pirate surveillant un réseau ouvert n'a besoin de récupérer qu'une seule demande non cryptée pour voler le cookie de sa victime et pirater son compte.

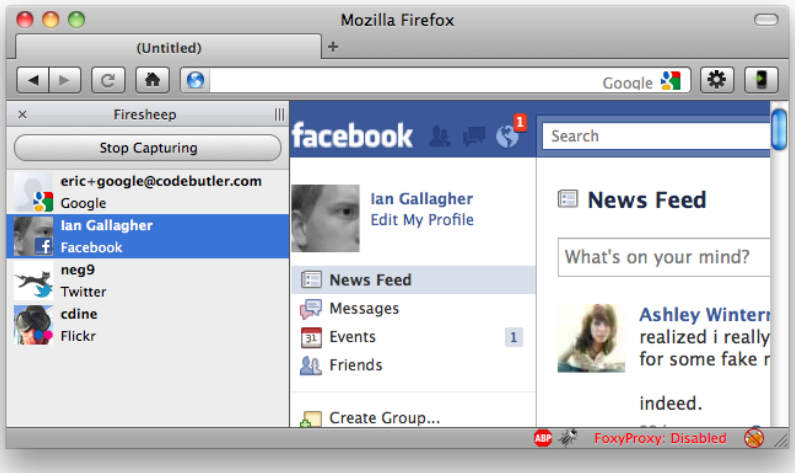
Ces problèmes ne sont pas nouveaux et peuvent affecter tout site Internet qui utilise des cookies de session. Même les moteurs de recherche qui répètent les termes de demande des utilisateurs sont vulnérables à de telles attaques. Les organisations ne peuvent plus se permettre de rester si confiantes, et l'information préventive à l'égard des utilisateurs n'est plus suffisante. L'industrie du Web a atteint un point critique et se doit de changer pour préserver la confiance et l'assurance des consommateurs.

Le piratage de sessions est désormais une tâche facile

Le piratage de session n'est pas un problème nouveau, mais le lancement récent d'un nouveau plugin de Firefox, « Firesheep », rend les utilisateurs et les pirates d'autant plus conscients des risques inhérents aux connexions HTTP non sécurisées (et aux réseaux Wi-Fi ouverts). Développé par Eric Butler et Ian Gallagher, Firesheep facilite énormément la tâche du pirate de base dans la récupération des données d'utilisateurs sur de nombreux sites populaires est simple comme bonjour. Firesheep trouve des réseaux ouverts qu'il rejoint, tels que les connexions Wi-Fi non cryptées dans les cafés et les bibliothèques, et il utilise ensuite un analyseur de paquets pour récupérer des cookies non sécurisés. Dès qu'une personne visite un site sur ces réseaux non sécurisés connus de Firesheep, le programme affiche son nom d'utilisateur et le service auquel elle est connectée. Le pirate peut alors double-cliquer sur le nom de sa victime et entrer directement sur son compte.

Firesheep est innovant d'un point de vue de l'intégration des fonctionnalités et de la facilité d'utilisation. Cependant, comme l'ont affirmé Butler et Gallagher, Firesheep met en lumière la gravité et l'envergure du problème, contre lequel les experts en sécurité ont mis en garde depuis de nombreuses années. Des outils, tels que « Hamster », « Ferret » et « CookieMonster » ont été présentés bien avant Firesheep, et permettent également aux pirates d'analyser les réseaux ouverts, de voler des cookies et pirater les sessions HTTP non cryptées avec facilité.

Figure 1. Firesheep en action



Avec ces outils, un pirate peut exploiter cette vulnérabilité afin d'obtenir un accès partiel ou intégral au compte de sa victime. Certains sites prennent des précautions pour éviter un piratage intégral de session (en demandant, par exemple, d'entrer un ancien mot de passe lorsque l'utilisateur tente d'en créer un nouveau), mais dans de nombreux cas, le pirate réussit à pirater complètement le compte de sa victime, à changer son mot de passe et, éventuellement, à pirater d'autres services connectés au compte de la victime.

Un problème global

Certaines personnes pensent que le piratage de session n'est qu'un problème de « bibliothèque », et que la solution consiste simplement à éviter d'utiliser les réseaux Wi-Fi non cryptés. Malheureusement, cette perspective est bien loin de la réalité, car les outils, tels que Firesheep, peuvent être utilisés pour intercepter n'importe quel trafic réseau, avec ou sans fil, sur lequel des cookies sont envoyés sur des sessions non protégées. Le risque pour les entités gouvernementales et les organisations qui utilisent des sites de réseaux sociaux, la messagerie Web et les applications Web 2.0 est un autre aspect pris en compte dans cette situation. Si un employé accède à un site non sécurisé et que sa session est piratée, le pirate peut utiliser son compte pour distribuer du malware, ou éventuellement pour accéder à des biens confidentiels et causer une atteinte à la sécurité. Les dégâts possibles pouvant résulter d'une telle atteinte seraient d'une gravité considérable.

L'information préventive seule ne suffit pas

Dans un effort de prévention et afin de combattre les dangers du piratage de session, l'EFF (Electronic Frontier Foundation) a créé sa propre extension Firefox, HTTPS-Everywhere, qui force Firefox à utiliser uniquement une connexion HTTPS pour certains sites. De plus, l'EFF et Access, une organisation de protection des droits du Web à but non lucratif, ont également créé HTTPS Now, une campagne d'information internationale dont le but est de créer une vraie prise de conscience et de pousser à l'adoption globale de Always on SSL comme niveau de sécurité minimum pour les navigateurs Web. La campagne comprend un site Internet sur lequel les utilisateurs peuvent se rendre pour chercher et donner des informations sur la façon dont les sites Web utilisent le protocole HTTPS. HTTPS-Everywhere est perçu comme un outil qui fonctionne très bien sur certains sites définis, mais il ne protègera pas l'utilisateur s'il visite d'autressites. Par ailleurs, HTTPS-Everywhere ne fonctionne pas sur Chrome, Safari ou Internet Explorer, et sa valeur sera limitée tant que les navigateurs principaux ne l'incluront pas comme fonction par défaut.

Le travail effectué par l'EEF est considérable, mais l'information préventive, ainsi que les outils développés à l'intention des utilisateurs ne seront pas suffisants pour mettre fin à la vulnérabilité de la gestion des sessions Internet, et il est peu probable que les réseaux non protégés des cafés, bibliothèques et aéroports ne soient un jour plus utilisés. Les opérateurs de sites Internet devraient protéger les données de leurs utilisateurs, peu importe le navigateur ou le type de réseau utilisé. En prenant des mesures de protection avant qu'une attaque de piratage de session ne se produise, les organisations s'assurent de garder leur clientèle et évitent ainsi les coûts exorbitants associés aux procédures légales et à la publicité nécessaire pour assumer le contrecoup d'un impact si négatif.

Assurer une protection intégrale de l'expérience d'utilisateur avec Always On SSL

Always On SSL est une mesure de sécurité abordable et indispensable qui offre une protection intégrale aux visiteurs de site Web. Ce n'est pas un produit, un service ou un système de remplacement pour un certificat SSL déjà existant, mais plutôt une approche à la sécurité qui reconnaît les besoins de protéger la session entière de l'utilisateur, et pas seulement l'ouverture de session. Always On SSL commence avec l'utilisation du protocole HTTPS sur l'intégralité du site, mais il nécessite également la configuration d'un drapeau sécurisé pour tous les cookies de session, afin d'éviter que leur contenu ne soit envoyé vers des connexions HTTP non cryptées. Des mesures supplémentaires, telles que les certificats EV SSL à validation étendue, et le HSTS, peuvent renforcer davantage une infrastructure contre les attaques pirates.

> *« A Symantec, nous pensons que Always On SSL est une façon assez simple et abordable de se protéger contre la plupart des menaces de réseaux. Les expériences des leaders de l'industrie Internet évoquées dans ce Livre prouvent sa faisabilité et sa valeur. Nous préconisons fortement aux propriétaires de sites Web d'adopter Always On SSL le plus rapidement possible. »*
>
> *– Quentin Liu, Symantec*

Tout le monde le fait, à votre tour

Tandis que les attaques en ligne deviennent de plus en plus fréquentes et faciles d'exécution, les organisations dans le monde entier sont constamment scrutées pour assurer que les transactions en ligne contenant des données confidentielles sont sécurisées. Les agents gouvernementaux ainsi que les groupes de protection de la vie privée poussent les organisations à utiliser Always On SSL.

En janvier 2011, en réponse aux rapports sur le piratage de SSL, le sénateur Charles Schumer (D-N.Y.) a envoyé une lettre à Yahoo!, Twitter et Amazon afin qu'ils retirent le « paillasson de bienvenue pour les pirates en herbe » que représente le protocole HTTP, et leur a demandé de rapidement intégrer Always On SSL.

Aujourd'hui, certains des sites les plus importants et les plus fiables, tels que Facebook, Google, PayPal et Twitter, ont intégré Always on SSL, et implémentent le protocole HTTPS pour crypter toutes les communications envoyées depuis et vers leurs sites, y compris les données commerciales et non confidentielles. Ces organisations reconnaissent l'importance grandissante de la protection continue, et travaillent dur pour offrir une expérience sécurisée pour les utilisateurs du Web.

Facebook

Site le plus visité du Web, Facebook comptait 845 millions d'utilisateurs actifs à la fin du mois de décembre 2011, avec en moyenne 483 millions d'utilisateurs actifs sur un même mois. Facebook s'est engagé dans la protection de l'information, et ses équipes de sécurité ont développé des systèmes sophistiqués de protection contre les spams, le hameçonnage, le malware et autres menaces de sécurité. En janvier 2011, dans un effort considérable pour renforcer la sécurité de sa plate-forme, Facebook a commencé à intégrer Always On SSL en offrant à ses utilisateurs la possibilité de se connecter sur une session HTTPS. Les utilisateurs ont répondu plus que favorablement à ce changement, avec plus de 19% d'utilisateurs actifs de Facebook optant pour une connexion sécurisée.

Mettre en place la migration de millions d'applications

Facebook a dû faire face à un défi encore plus difficile lorsqu'il lui a fallu déplacer son écosystème composé de plus d'un million de développeurs vers le HTTPS et OAuth 2.0, une norme ouverte créée par Yahoo, Twitter, Google et bien d'autres encore. Ceci représentait un problème majeur. En effet, de nombreuses applications étaient bloquées lorsque les utilisateurs se connectaient en HTTPS, car ces applications n'étaient pas conçues pour fonctionner avec ce protocole. En conséquence, les utilisateurs recevaient des messages de contenu mixte prêtant à confusion. Pour aider les développeurs à effectuer cette transition, Facebook a proposé un plan sur six mois dans sa « Developer Roadmap » (feuille de route pour ses développeurs) afin de faciliter la migration des sites et des applications vers le HTTPS. [2]

La transition a été rapide pour les développeurs qui avaient conçu leurs applications de façon à ce qu'elles fonctionnent sur une connexion sécurisée, mais pour ceux ayant un grand nombre d'applications à leur actif, cette migration a demandé beaucoup plus de temps et de ressources pour trouver et réécrire le code nécessaire, et pour effectuer les améliorations indispensables sur leurs infrastructures..

> *"Nous avons beaucoup plus d'assurance dans notre capacité à offrir un service de confiance sécurisé sur des réseaux où la confidentialité de nos clients auraient sinon pu être en danger."*
>
> – Alex Rice, Facebook

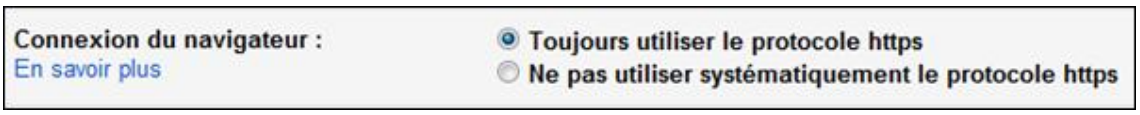
[2] https://developers.facebook.com/blog/post/497/

Pour Facebook, la transition vers une approche Always On SSL vaut bien l'effort qui a été requis pour la mettre en place. La société n'a désormais plus qu'une seule norme pour l'authentification et pour les applications utilisées à travers le HTTPS, ce qui leur permet d'offrir une plate-forme plus simple, plus sécurisée et plus fiable. Cette première étape terminée, Facebook se concentre à présent sur l'expansion d'infrastructures internationales pour réduire la latence à un niveau tolérable. Ceci représente une composante critique pour Facebook, dans la mesure où près de 80% de ses utilisateurs actifs sont situés en dehors de l'Amérique du Nord.

Google

Bien que Google ait commencé comme un moteur de recherche qui traitait surtout de l'information publique, la société s'est considérablement développée et offre désormais une expérience d'utilisateur personnalisée. Google a depuis longtemps cerné l'importance de la protection de la confidentialité des informations personnelles. Lorsque Google a lancé Gmail et Google Apps, son but était d'offrir des produits de qualité si solides qu'ils représenteraient une part importante dans le développement de la société, et Gmail et Google Apps ont donc été conçus pour fonctionner avec une connexion HTTPS dès leur lancement. Au début, le protocole HTTPS était utilisé pour la protection des données des utilisateurs. Puis, en juillet 2008, Google a lancé une fonction offrant à tous les utilisateurs de Gmail et Google Apps la possibilité de *toujours utiliser HTTPS*.

Figure 2. Option HTTPS dans Gmail et Google Apps



En Janvier 2010, Google a décidé d'établir le protocole HTTPS par défaut pour Gmail et Google Apps afin de faciliter la protection des e-mails des utilisateurs entre leur navigateur et Google à tout moment. Cette transition n'a demandé aucune machine supplémentaire ou équipement particulier, et l'impact sur la performance n'a été que très minime. Les chercheurs de Google ont découvert que le SSL/ TLS ne compte que pour moins de 1% de la charge du processeur de leurs machines de production, soit moins de 10KB de mémoire par connexion, et moins de 2% du réseau entier.

Favoriser une recherche sécurisée

Offrir une expérience de recherche sécurisée représentait une tâche plus complexe. En mai 2010, Google a lancé une option de recherche cryptée permettant à l'utilisateur d'effectuer des recherches à l'abri de la curiosité d'un tiers parti. Plus récemment encore, Google a commencé à utiliser le HTTPS par défaut pour tout utilisateur connecté à sa session. Ce changement permet le cryptage des demandes de recherche et des pages de résultats Google. L'avantage de cette approche d'un point de vue sécurité est clair : l'utilisateur bénéficie d'une expérience de recherche plus sécurisée et plus confidentielle grâce au cryptage intégral entre son ordinateur et Google. Mais l'écosystème autour de la recherche, notamment l'analyse du Web et l'optimisation des moteurs de recherche, a représenté un problème complexe.

Lorsque l'utilisateur clique sur le résultat d'une recherche Google et accède à un site, un drapeau de « référence » est fourni par le navigateur pour indiquer si la demande provient d'un lien Google. De nombreux spécialistes en optimisation des moteurs de recherche et en analytique utilisent cette information pour effectuer des statistiques d'utilisation ou pour mesurer

l'impact de leurs efforts de marketing en ligne. Cependant, lorsqu'un utilisateur effectue une recherche sécurisée, ses termes de demande sont protégés. Pour les sites recevant des clics à partir des résultats Google, cela signifie qu'ils pourront toujours savoir que les utilisateurs se sont servis de Google pour leurs recherches, mais ils ne recevront pas d'informations sur chaque demande individuelle.

Cependant, comme le fait remarquer Google, les sites peuvent toujours recevoir une liste complète sur les 1000 recherches les plus populaires qui ont augmenté le trafic vers leurs pages sur la période des 30 jours précédant leur demande, et ce grâce aux outils Google Webmaster. Ces informations aident les créateurs de sites à garder des statistiques toujours plus justes et précises sur le trafic vers leur site, tout en continuant à protéger la confidentialité des utilisateurs individuels qui se connectent avec HTTPS. De plus, lorsqu'un utilisateur choisit de cliquer sur une publicité qui apparaît sur les pages de recherche Google, son navigateur continue d'envoyer la demande correspondante sur le réseau afin que les publicitaires puissent mesurer l'efficacité de leurs campagnes et améliorer leurs publicités, ainsi que leurs offres.

Google prévoit d'améliorer à l'avenir la fonctionnalité de Always On SSL sur leurs produits, et ses chercheurs continue à publier des informations et des conseils sur le SSL/ TLS. Google recommande aussi fortement un effort beaucoup plus intense de la part de l'industrie du Web afin d'intégrer le SSL de manière plus générale et plus efficace, avec comme intention de protéger tous les contenus légitimes sur Internet pour assurer une expérience sécurisée et sans problème pour les utilisateurs.[3]

PayPal

Depuis 1998, PayPal est le leader mondial des solutions de paiement en ligne, et a été un des premiers à adopter le protocole SSL/ TLS. En 2000, la société sécurisait déjà toutes les pages au-delà de l'ouverture de session avec le protocole HTTPS, et utilise ce protocole pour l'ouverture de session elle-même depuis 2006. PayPal a aussi été l'une des premières organisations à utiliser les certificats EV SSL à validation étendue et a commencé à sécuriser toutes ses pages de connexion avec des EV SSL dès 2007.[4]

PayPal a dû faire face à des défis uniques par rapport à sa performance à cause de la nature transactionnelle de ses services. A la différence des sites sur lesquels l'utilisateur passe un certain temps sur une seule session, PayPal offre un large pourcentage de sessions courtes. Et dans la mesure où l'implémentation du SSL/ TLS requiert beaucoup de temps, PayPal avait conscience qu'il lui fallait surveiller et gérer avec attention les impacts possibles sur la performance de l'expérience utilisateur. Cependant, dans certains cas, la conversion vers HTTPS a en fait accéléré la vitesse d'exécution du site car il était possible de présenter du contenu depuis les mêmes serveurs à travers des connexions vers le navigateur.

[3] http://googleblog.blogspot.com/2011/10/making-search-more-secure.html
[4] https://otalliance.org/resources/EV/index.html

Les équipes de sécurité de PayPal savaient parfaitement que leur site constituait une cible particulièrement attirante pour les cybercriminels, et elles ont commencé à prendre des mesures extraordinaires afin de protéger leurs clients et leur réputation. Leur but était de contrecarrer les outils d'attaque pirate et de fraude, tels que SSLStrip (différent de Firesheep qui est un outil passif qui espionne mais ne déroute pas ou ne modifie pas les paquets de réseau).[5]

Ces efforts ont atteint leur point culminant avec le lancement de la spécification HTTP Strict Transport Security, créée en collaboration avec Jeff Hodges, ingénieur sécurité à PayPal. Cette spécification définit la façon dont les sites Web peuvent se déclarer accessibles par une connexion sécurisée uniquement. Aujourd'hui HSTS fonctionne avec Google Chrome et Mozilla Firefox, et des sites tels que PayPal.com qui utilisent HSTS informent explicitement les navigateurs qu'ils n'envoient et n'acceptent que des communications cryptées, évitant ainsi à l'utilisateur de visiter accidentellement une page HTTP ou d'être redirigé vers une page HTTP à travers une attaque SSLStrip ou une tentative de hameçonnage.

Twitter

Réseau d'information en temps réel, Twitter a été à l'origine de nombreux évènements évoqués par la presse, notamment dans les zones du monde où la liberté d'expression est limitée. Bien que Twitter ait été la cible de quelques incidents de sécurité, la société a effectué de nombreuses démarches pour améliorer la sécurité de Twitter.

Twitter fonctionnait déjà avec HTTPS pour ses sites, les Smartphones, les sites Web mobiles, ainsi que pour les fonctionnalités telles que le bouton Tweet. Mais la société a fait un pas en avant lorsqu'elle a intégré Always On SSL. En mai 2011, Twitter a annoncé qu'il offrait désormais l'option d'utiliser HTTPS en continu grâce à une configuration spécifique. La réponse des utilisateurs a été considérablement positive et a poussé Twitter à accélérer le déploiement du protocole pour tous ses utilisateurs en janvier 2012 en faisant de HTTPS l'option par défaut.

Twitter a surmonté quelques défis uniques en adoptant Always On SSL. La société sous-traite certaines parties de son trafic auprès de réseaux CDN, et il était prioritaire d'assurer que les réseaux CDN aient la capacité de gérer la charge grandissante de SSL. Préserver la capacité à suivre les références et l'analytique était aussi important pour Twitter et ses partenaires, et les ingénieurs de Twitter ont réécrit le code pour travailler sur des problèmes spécifiques aux contenus mixtes.

Leçons retenues

Les experts en sécurité de Facebook, Google, PayPal et Twitter ont récolté des informations de valeur qu'ils ont ensuite partagées avec l'OTA, service publique qui aide les opérateurs de sites Internet à se protéger et à protéger leurs utilisateurs contre les attaques de piratage de session. Ces informations majeures aident à comprendre la nécessité d'intégrer Always On SSL sur les sites Web.

[5] http://www.thoughtcrime.org/software/sslstrip/

Le SSL, un produit abordable

Certaines organisations sont réticentes à l'idée de mettre en place Always On SSL, parce qu'elles pensent que cela nécessiterait davantage de frais. Les certificats SSL/ TLS issus par une Autorité de Certification ne sont pas gratuits, mais ils n'ont pas de prix fixes, et il n'est pas nécessaire de remplacer un certificat déjà existant. Pour sécuriser plusieurs noms de domaine, il est possible d'ajouter des sous-domaines (SANs) à l'achat d'un certificat.

Hormis le prix du certificat SSL, la question des exigences informatiques et du besoin éventuel d'acheter des équipements supplémentaires se pose dans la gestion de la charge additionnelle requise pour le processeur.

Sur les gros sites populaires, il semble raisonnable de penser que le calcul additionnel nécessaire au cryptage et au décryptage des paquets de réseaux pourrait causer une augmentation des exigences en équipements informatiques. Cependant, ceci ne semble pas être le cas pour de nombreuses organisations.

Des chercheurs à Google, par exemple, ont effectué des recherches poussées sur la charge de calcul associée au système Always On SSL, et ont découvert qu'il ne requiert aucun équipement supplémentaire pour son implémentation dans leur environnement informatique. La plupart des preuves montre que les avancées technologiques ont minimisé l'impact informatique du SSL/ TLS, mais il est bon de définir la performance du serveur Web afin de déterminer les conséquences que cela implique sur l'environnement.[6]

> *"Si vous arrêtez de lire maintenant, rappelez-vous d'une seule chose : le SSL/ TLS a désormais un coût numérique peu élevé. Il y a dix ans, ce n'était pas forcément le cas, mais maintenant c'est un fait. Vous aussi vous pouvez vous permettre d'offrir une connexion HTTPS à vos utilisateurs."*
>
> *– Adam Langley, Google*

La latence d'un réseau représente un défi de performance

L'utilisation du protocole intégral HTTPS engage une certaine latence d'un réseau, notamment à cause des aller-retour nécessaires entre le client et le serveur pour compléter le handshake SSL/ TLS. Ceci est particulièrement épineux sur de longues distances, notamment pour les utilisateurs internationaux dans les zones où la bande passante du réseau est limitée, ou pour les sites sur lesquels un grand nombre d'utilisateurs commence des sessions SSL/ TLS plutôt courtes. La latence n'est pas un problème simple à résoudre. Cependant, l'impact sur la performance peut être géré grâce à une bonne organisation, et les sociétés de services financiers ont déjà montré qu'elles offrent une expérience de navigation riche et à faible latence tout en appliquant un cryptage intense par défaut. De plus, les chercheurs de Google testent de nouvelles technologies, telles que le « Faux Départ » (False Start) qui semble réduire la latence associée au handshake du SSL/ TLS de 30%.[7]

Le développement d'un Internet sécurisé rend la transition plus facile

[6] http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html
[7] http://googleonlinesecurity.blogspot.com/2010/05/extending-ssl-to-google-search.html

Des pratiques de développement sécurisé, si elles sont suivies dès le début, permettent d'obtenir des sites et des applications Web sécurisés qui engendrent les mêmes coûts pour leur développement, mais s'avèrent beaucoup plus rentables sur le long terme. Trouver et réécrire le code peut avoir un coût et demande du temps, notamment pour les grosses organisations qui possèdent de nombreux produits. Tous les sites créés aujourd'hui devraient systématiquement utiliser le HTTPS par défaut et immédiatement rediriger les connexions HTTP vers le protocole HTTPS, notamment pour tout ce qui est formulaire Internet. Il existe de nombreux aspects à prendre en considération, les ressources, telles que MozillaWiki, et les groupes, tels que l'OWASP (Open Web Application Security Project), fournissent des instructions complètes qui peuvent être suivies pour développer des applications et des services Internet sécurisés.[8]

Le contenu mixte, origine de la complexité

Le contenu mixte est un problème compliqué qui provient de la nature même du Web qui se compose de milliards d'hyperliens. La plupart des sites affichent des contenus issus de plusieurs sources, souvent de tiers partis. Si l'un de ces contenus redirige sur un lien HTTP, cela pourrait compromettre un site, à la base sécurisé, en permettant à un pirate actif d'exploiter le chargement du CSS ou du code JavaScript. De la même manière, lorsqu'une page HTTPS charge une image, une iframe ou une police vers une page HTTP, un pirate peut intercepter la ressource HTTP. De plus, les sites, tels que Facebook, commencent à requérir l'utilisation du SSL/ TLS pour éviter les contenus mixtes, et bloqueront toute application et tout contenu qui n'utilise pas le protocole HTTPS. Pour s'épargner de tels problèmes, les sites Internet doivent éviter d'appeler des fichiers dans leur code à travers le HTTP. Ceci comprend les éléments suivants (liste non exhaustive) :

- Les fichiers image et leurs liens dans la balise <img>
- Les fichiers CSS externes (.css)
- Les fichiers JavaScript (js.)
- Les contenus incrustés et les contenus iframe (Flash, etc.)
- Les URLs dans DOCTYPE ou les balises <html>
- Les appels vers des API et des kits de développement logiciels externes (le kit de Facebook par exemple)

Les liens relatifs sont une façon d'éviter les problèmes de contenu sécurisé et non sécurisé mixtes car ils ne précisent pas s'il s'agit de HTTP ou de HTTPS. Cependant, les liens relatifs peuvent être exploités pour du spamming de moteur de recherche ou des attaques de détournement d'URLs, il est donc important de considérer chaque besoin avec attention avant de décider comment et où utiliser les liens relatifs. [9]

[8] https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines
[9] http://www.dummies.com/how-to/content/prevent-someone-from-hijacking-your-web-sites-sear.html

Intégrer Always On SSL sur un site Web

Les sociétés qui accordent une importance primordiale à la protection de leur réputation et de leurs clients finiront par implémenter Always On SSL. L'OTA a esquissé des instructions de mise en place d'Always On SSL pour protéger les utilisateurs de sites Web. Le niveau de protection et d'assurance qui peut être offert dépend des fonctions de sécurité choisies pour l'implémentation (voir tableau ci-dessous).

Tableau 1. Mesures de sécurité Always On SSL

Fonctions de sécurité	Bonne	Mieux	Meilleure
HTTPS continu	✓	✓	✓
Cookies configurés avec drapeau sécurisé	✓	✓	✓
HTTPS continu avec EV SSL (à validation étendue)		✓	✓
HSTS			✓

HTTPS continu sur toutes les pages Web

Avant tout, Always On SSL consiste à faciliter l'utilisation systématique du HTTPS pour les visiteurs d'un site, peu importe la page sur laquelle ils sont. Le protocole HTTPS est un protocole basé sur du texte tout comme HTTP, seulement il ne fonctionne que sur une session cryptée. Voici les quelques étapes à suivre pour intégrer le protocole HTTPS :

- Installer un certificat SSL/ TLS issu par une Autorité de Certification
- Changer les connexions au serveur depuis Port 80 à Port 443
- Préciser la force de cryptage (128 bit par exemple)

Il est possible de rendre ces options optionnelles, cependant, sur le long terme, il est recommandé de faire du protocole HTTPS l'option par défaut, et d'offrir aux utilisateurs la possibilité de le désactiver si nécessaire. En mettant en place un système de HTTPS intégral, le niveau de sécurité minimum est ainsi assuré et garantit la sécurité et la confidentialité aux utilisateurs d'un site.

S'assurer de la bonne installation d'un certificat SSL

Pour activer le HTTPS, il est nécessaire d'installer un certificat SSL/ TLS valide émis par une Autorité de Certification (AC). Alors qu'un certificat auto-signé permettra de crypter les communications entre l'utilisateur et le site, seul un certificat émis par une AC assurera l'utilisateur que l'identité du nom de domaine a été vérifié par une source fiable. Si la connexion utilise un certificat auto-signé, le navigateur peut le percevoir comme un danger potentiel et afficher des messages d'erreur qui avertissent l'utilisateur que le site n'est peut-être pas sécurisé. Choisir la bonne Autorité de Certification est très important.

Il est nécessaire de s'assurer que l'AC choisie suit des pratiques de sécurité strictes pour la validation des certificats, et qu'elle offre une garantie de remboursement appropriée en cas d'activité frauduleuse qui pourrait résulter directement d'une transaction d'un client avec un site sécurisé par un certificat SSL valide.

De plus, il faut également s'assurer que le certificat SSL comprend tous les certificats intermédiaires de la chaîne de confiance. Des problèmes avec le certificat peuvent pousser les navigateurs à bloquer l'accès à un site, ou à afficher des messages d'avertissement. Des sites, comme Facebook, qui exigent une validation stricte, peuvent aussi bloquer le contenu d'un site si sa chaîne de certificat présente un problème. Il existe plusieurs outils d'analyse SSL disponibles qui peuvent être utilisés pour vérifier l'installation d'un certificat SSL/ TLS et réparer d'éventuelles erreurs.

Configurer le drapeau sécurisé pour tous les cookies de session

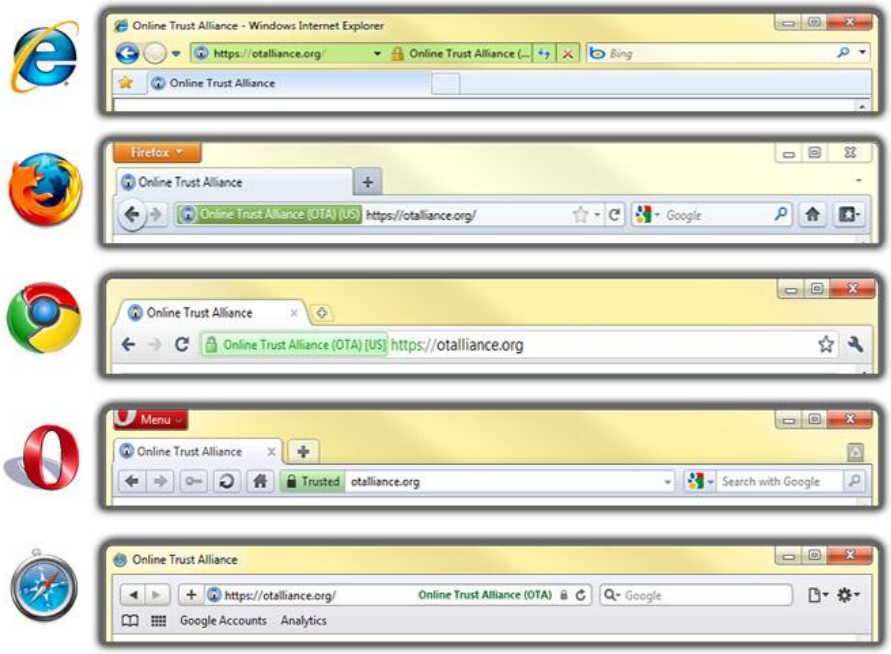
Un cookie de session peut être configuré avec un drapeau sécurisé optionnel qui demande au navigateur de contacter le serveur d'origine en utilisant uniquement le protocole HTTPS à chaque fois qu'il renvoie ce cookie. Cette option devrait être conseillée pour indiquer qu'il est dans l'intérêt de la session de protéger le contenu des cookies. Cette mesure permet d'empêcher le renvoi de cookies vers une connexion HTTP, même si l'utilisateur envoie par mégarde une demande au serveur à travers le protocole HTTP.

Améliorer la confiance avec un certificat à validation étendue (EV SSL)

Pour une meilleure protection contre les exploits, tels que SSLStrip, l'OTA recommande aux propriétaires de sites Web d'utiliser des certificats SSL à validation étendue (EV). Les sites sécurisés par de l'EV SSL sont soumis à un processus de vérification strict établi par le CA Browser Forum, une collaboration de plus de trente Autorités de Certification et de distributeurs de logiciels leaders du marché.

Ce processus de vérification confirme l'identité et l'existence d'un opérateur de site, et ce en utilisant des sources fiables de tiers partis. Les visiteurs d'un site sécurisé avec un certificat EV SSL peuvent voir le nom de l'organisation apparaître dans la barre d'adresse qui elle-même devient verte, ce qui offre une garantie visuelle de l'identité de l'opérateur du site.

Figure 3. affichage des caractéristiques visuelles du certificat EV SSL dans les navigateurs



L'OTA recommande que les organisations responsables utilisent un certificat EV SSL sur chaque site qui requiert une connexion sécurisée. Les services informatiques devraient aider leur direction ainsi que les utilisateurs de sites à comprendre qu'un certificat EV SSL protège la sécurité de l'utilisateur et réduit la vulnérabilité de l'organisation aux attaques pirates. Tout utilisateur devrait choisir un navigateur sur lequel les certificats EV SSL sont reconnus, et chaque site Web effectuant des transactions en ligne devrait considérer les certificats EV SSL dans leur stratégie de sécurité et de protection de leur marque.

Intégrer HSTS pour éviter les attaques actives

Les connexions HTTPS commencent généralement lorsqu'un visiteur est redirigé depuis une page HTTP ou lorsqu'il clique sur un lien (tel que le bouton de connexion) qui le dirige vers un site HTTPS. Cependant, il est possible de lancer une attaque pirate pendant la transition de la connexion non sécurisée à la connexion sécurisée, soit passivement, soit en piègeant la victime en la faisant cliquer sur un lien http vers un site légitime (en utilisant un e-mail de hammeçonnage par exemple).

Le moyen de défense le plus efficace contre ces types d'attaque consiste à intégrer le HSTS (HTTP Strict Transport Security) sur tous les sites Web. Cette spécification définit la façon dont les sites avertissent qu'ils ne sont accessibles que par une connexion sécurisée, et expliquent comment les utilisateurs peuvent naviguer sur ces sites à travers une connexion sécurisée. HSTS fonctionne sur Google Chrome et Mozilla Firefox, et des sites comme PayPal.com qui utilisent HSTS signalent de façon explicite aux navigateurs qu'ils n'envoient et ne reçoivent que des communications cryptées. L'utilisation de HSTS aide à empêcher les pirates de voler les cookies de session lorsque les utilisateurs sont redirigés vers une connexion HTTPS depuis une connexion HTTP, et il s'agit du moyen de défense le plus efficace contre les tentatives de hameçonnage et les attaques HDM.

Conclusion

Dans le passé, de nombreux experts ont conseillé aux développeurs et aux opérateurs de sites d'utiliser le SSL/ TLS pour protéger l'authentification des utilisateurs, les transactions financières et toute autre activité clé, mais beaucoup d'organisations étaient réticentes à l'idée de crypter leur site entier pour des soucis de coûts, de performances et d'autres problèmes. Cependant, Internet est arrivé à un point critique où il est évident que l'utilisation sélective du protocole HTTPS n'est plus adaptée pour protéger les utilisateurs d'aujourd'hui qui sont constamment connectés et en mouvement. Le SSL/ TLS constitue toujours une base solide, mais Firesheep a sonné l'alarme pour les opérateurs de sites afin qu'ils protègent l'expérience des utilisateurs dans son intégralité, et non plus seulement la page d'ouverture de session et le panier d'achat. En bref, le SSL est comme une ceinture de sécurité dans une voiture : il devrait toujours être utilisé.

Always On SSL n'est pas une « balle d'argent » qui arrêtera les pirates, et il doit être intégré dans une stratégie générale de sécurité afin de protéger les visiteurs d'un site. Cependant, il constitue une approche efficace contre le piratage de session et autres attaques HDM, et ne représente plus un coût exhorbitant pour la plupart des organisations. Tout comme Facebook, Google, PayPal, Twitter et bien d'autres l'ont prouvé, il est tout à fait possible, même pour les sites les plus importants et les plus complexes, d'offrir une expérience d'utilisateur riche grâce au HTTPS. Des problèmes, tels que la latence et les contenus mixtes, peuvent représenter des défis, mais les instructions et les pratiques décrites dans ce livre blanc aideront tout individu à gérer ces problèmes et optimiser la performance pour tout utilisateur.

Plus important encore, Always On SSL peut aider à protéger la confiance des utilisateurs pour un site. Protéger la confiance et l'assurance du client est un problème très délicat qui nécessite bien plus que des moyens purement techniques. A certains niveaux, les utilisateurs doivent simplement faire confiance au système, et, comme l'a dit Ken Thomson, l'un des auteurs principaux de UNIX, « il est peut-être plus important encore de faire confiance aux personnes qui ont écrit le programme ». Adopter l'approche Always On SSL peut aider à assurer aux utilisateurs d'un site que son propriétaire prend leur sécurité et la protection de leurs données au sérieux, et qu'il prend les dispositions nécessaires pour les protéger.

A propos de l'OTA

L'OTA (Online Trust Alliance) est une organisation indépendante à but non lucratif dont la mission est de développer et préconiser les meilleures pratiques et politiques publiques en vue de réduire les menaces grandissantes contre la confidentialité, l'identité et la sécurité des services en ligne, des organisations et de leurs consommateurs, et ainsi améliorer la confiance et l'assurance des transactions en ligne. En facilitant un dialogue ouvert avec l'industrie du Web, les entreprises et les agences gouvernementales pour travailler en collaboration, l'OTA fait des progrès dans la gestion des abus, des menaces et des pratiques qui menacent d'ébranler la confiance en ligne et augmentent le besoin de règlementations.

https://www.otalliance.org/

