Dossier thématique n°12

Sécuriser les communications sur Internet de bout-en-bout avec le protocole DANE

Aujourd'hui, près de 2,5 milliards de personnes utilisent Internet pour communiquer et fournir/obtenir des informations. Lorsque la communication concerne des informations sensibles telles que des coordonnées bancaires, des numéros de cartes de crédit, des dossiers médicaux, etc., la méthode de communication doit être sécurisée. L'échange d'informations sur l'Internet n'est pas sécurisé par défaut, ce qui induit un risque variable d'attaques malveillantes telles que la corruption des données, l'usurpation d'identité, etc.

Avec l'évolution de l'Internet, de nouveaux mécanismes de sécurité sont devenus nécessaires, que ce soit en raison de l'émergence de nouveaux types d'attaques ou de l'identification de nouvelles failles de sécurité. Des solutions ont été proposées et déployées progressivement. Ces solutions comprennent entre autres IPSec (Internet Protocol Security) pour sécuriser la couche réseau (également appelée couche IP), TLS (Transport Layer Security) pour sécuriser la communication entre deux applications Internet, telles qu'un serveur Web et un navigateur Web, DNSSEC (Domain Name System Security Extensions) pour sécuriser le processus de résolution DNS, etc.

Ces dernières années, des attaques de haut niveau, ciblant l'infrastructure à clés publiques X.509 (PKIX) utilisée pour sécuriser les communications Internet, ont suscité un besoin urgent d'une technologie permettant de corriger la faille de sécurité présente dans l'écosystème PKIX. C'est dans ce contexte que la communauté IETF (Internet Engineering Task Force) a proposé le protocole/mécanisme DANE (DNS - based Authentication of Named Entities) qui s'appuie sur le DNS pour authentifier des entités applicatives.

Ce document explique le protocole DANE et comment DANE pourrait apporter la confiance nécessaire dans l'infrastructure du dernier kilomètre en s'appuyant sur DNSSEC. Ce document est destiné à un public ayant une certaine connaissance des protocoles d'Internet en général et du système de noms de domaine (DNS) en particulier. Ce document présente le protocole DANE et explique comment DANE corrige la faille de sécurité existant dans l'Internet tout en assurant une communication de bout-en-bout. Ce dossier thématique n'est pas suffisant pour permettre à un administrateur de domaine d'implémenter DANE.

La figure suivante illustre une communication Internet type, une navigation sur le Web :

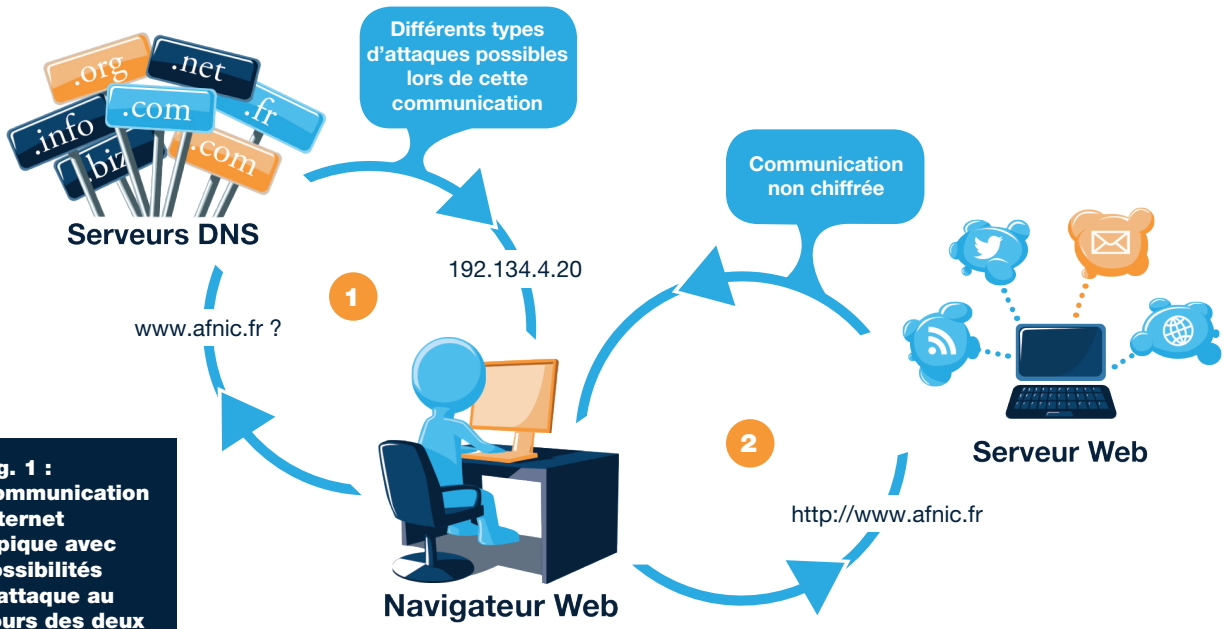


Fig. 1 : Communication Internet typique avec possibilités d'attaque au cours des deux opérations

Cette figure met en évidence deux opérations :

1. Étant donné que le cerveau humain n'est pas capable de mémoriser un grand nombre de numéros (adresses IP) à la fois, mais qu'il est bien équipé pour se souvenir de noms, des noms de domaine sont normalement utilisés lors de l'interrogation d'un service sur Internet. Mais, étant donné que les applications Internet ont besoin d'adresses IP pour communiquer entre elles, le DNS est utilisé comme «Annuaire de noms», généralement pour obtenir l'adresse IP associée à un serveur donné identifié par son nom.
2. L'adresse IP obtenue est ensuite utilisée par l'application (c.-à-d. le navigateur Web illustré en Figure 1) pour engager une communication Internet avec le serveur Web distant.

Les deux opérations mentionnées précédemment ne sont pas intrinsèquement sécurisées. Par défaut, lorsque des informations sont transmises au cours de la résolution DNS ou lors d'un accès au serveur pour échanger des données, aucune procédure d'authentification ou de chiffrement n'est appliquée. Il existe par conséquent au cours de ces opérations de nombreuses possibilités permettant à un attaquant de fournir de fausses informations, comme une adresse IP frauduleuse lors de la résolution DNS, et de rediriger ainsi l'utilisateur vers un serveur frauduleux.

En ce qui concerne la première opération (résolution DNS), la sécurisation de la communication peut être assurée par DNSSEC. Nous décrirons plus loin dans ce dossier comment DNSSEC améliore la sécurité. Pour la seconde opération (connexion entre le navigateur et le serveur Web), le protocole TLS vient à la rescousse en permettant au client et au serveur de s'authentifier mutuellement et de négocier un algorithme de chiffrement et des clés cryptographiques avant que les données ne soient échangées. TLS garantit que les données ne peuvent être lues ou altérées par un tiers lors du transfert, puisqu'elles sont chiffrées.

Le chiffrement et le déchiffrement des données dans le protocole TLS s'effectuent au moyen d'une paire de clés cryptographiques : une clé publique et une privée. Les données chiffrées avec une clé publique ne peuvent être déchiffrées qu'avec la clé privée correspondante, et vice versa. Cela permet d'avoir une communication sécurisée avec des utilisateurs inconnus. Par exemple, une banque publie sa clé publique et permet à quiconque de la télécharger. Titulaire d'un compte à la banque, Alice chiffre un message à l'aide de la clé publique et l'envoie à la banque. Seule la banque est en mesure de déchiffrer ce message avec sa clé privée. Ainsi Alice est sûre que son message ne sera pas lu par quelqu'un d'autre.

Dans une connexion TLS, le navigateur demande au serveur Web d'envoyer sa clé publique. La clé publique envoyée par le serveur Web au navigateur est sous la forme d'un certificat X.509, qui est expliquée plus en détail dans la section II.

1 Énoncé du problème

Infrastructure à clé publique X.509 (PKIX)

En revanche, il existe une possibilité qu'un imposteur publie sa clé publique et se fasse passer pour la banque d'Alice. Alice va chiffrer le message en utilisant la clé publique présentée par l'imposteur et l'envoyer à sa banque, où l'imposteur agit comme intercepteur ("man-in-the-middle") et copie le message. Étant propriétaire de la clé publique, l'imposteur possède également la clé privée lui permettant de déchiffrer et de lire le message. Pour faire une analogie avec la navigation sur le Web, n'importe qui peut créer une clé publique pour accéder à n'importe quel nom de domaine. En termes de sécurité, c'est une catastrophe, car un imposteur peut créer une clé publique pour des domaines tels que www.example.com, et tromper l'utilisateur en le faisant accéder à un serveur frauduleux.

Il est donc nécessaire d'établir un lien entre l'identité (le nom de domaine) et la clé publique. La norme X.509 proposée par l'UIT et l'ISO propose un mécanisme permettant de lier une clé publique particulière à une identité particulière. Cette liaison peut être établie de manière autonome par le titulaire du nom de domaine et l'on parle dans ce cas d'un certificat auto-signé. Si l'application qui, pour l'authentification, utilise le certificat auto-signé l'a obtenu auprès d'une source fiable, alors le certificat est accepté ; dans le cas contraire, il n'y a aucune garantie d'authenticité du certificat.

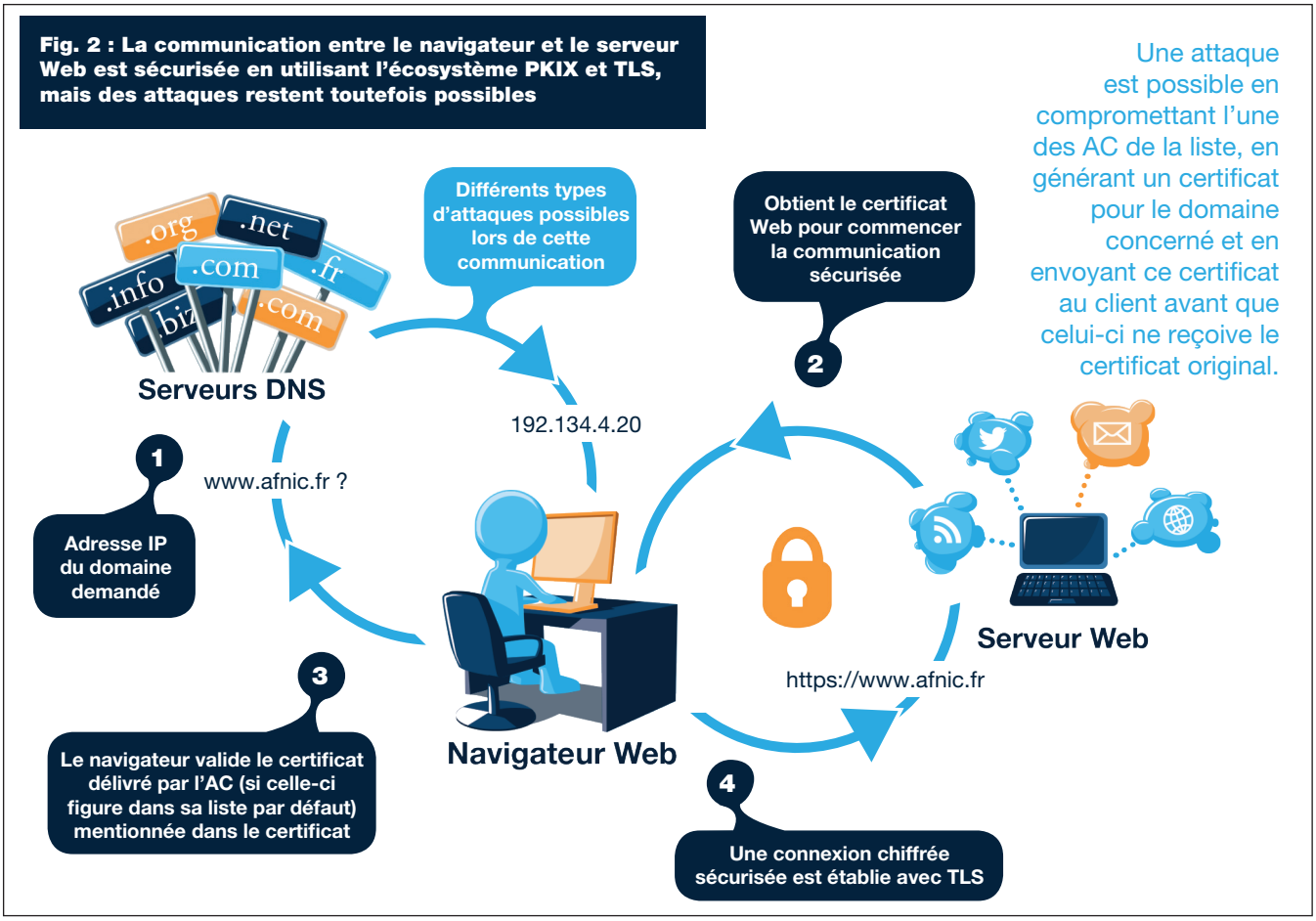
Rôle des Autorités de Certification (AC)

C'est là que la nécessité d'un tiers de confiance se pose. C'est comme dans le cas du passeport, où le tiers de confiance est le gouvernement qui a délivré le passeport. Dans un passeport, le gouvernement atteste que la personne sur la photo est identifiée par un nom et un prénom particuliers et d'autres informations d'identification.

Dans le cas de la navigation sur le Web, le certificat délivré fait office de passeport. Dans l'écosystème PKIX, le rôle du gouvernement est joué par des organisations appelées "AC". Un certificat émis par une AC associe le nom de domaine donné à des informations telles que l'entité ayant attribué le certificat, l'entité qui en a fait la demande, la période de validité du certificat, etc.

De la même manière qu'un passeport délivré par un gouvernement est accepté par d'autres gouvernements en tant que document valide permettant d'authentifier une personne, les éditeurs de navigateurs, tels que Firefox, Chrome, Internet Explorer, Safari, etc., acceptent les certificats numériques établis uniquement par certaines autorités de certification. Les éditeurs de navigateurs n'autorisent une organisation à devenir une AC qu'après s'être assurés que cette organisation est digne de confiance et qu'elle observe des principes et des procédures bien définis en ne délivrant des certificats qu'aux titulaires officiels de noms de domaine. Lorsque les éditeurs de navigateurs autorisent une organisation à devenir une AC, cette dernière est ajoutée à la liste des AC de confiance dans la bibliothèque du navigateur. Ainsi, lorsqu'un client utilisant un navigateur accède à un nom de domaine qui dispose d'un certificat numérique généré par l'une des AC figurant dans sa liste préinstallée, le certificat est automatiquement accepté comme le montre la Figure 2.

Fig. 2 : La communication entre le navigateur et le serveur Web est sécurisée en utilisant l'écosystème PKIX et TLS, mais des attaques restent toutefois possibles



Le problème des AC nombreuses

En bref, si l'on regarde la longueur de la liste des AC reconnues par les navigateurs les plus courants comme Chrome, Firefox, Internet Explorer, etc., celle-ci varie, mais est de l'ordre de plusieurs centaines. Par exemple, un navigateur tel que Firefox reconnaît 1 482 certificats d'AC (selon l'observatoire SSL[1] de l'EFF) fournies par 651 organisations. S'ajoute au problème l'existence d'une pratique, au sein de l'écosystème des AC, consistant pour une AC à autoriser d'autres organisations, ou ses succursales, à générer des certificats en son nom. Ces organisations ou succursales sont appelées des AC subordonnées. Un navigateur reconnaîtra également le certificat numérique créé par une AC subordonnée.

Même si une seule AC dans la liste des autorités de certification est compromise, ou ses subordonnées, elle peut générer un certificat pour un nom de domaine qui pourrait être authentifié par un navigateur tel que Firefox et compromettre ainsi la communication Web sécurisée d'un utilisateur final utilisant Firefox. Par exemple, deux AC différentes (dont l'une est compromise) peuvent émettre deux certificats différents pour le même domaine et ces deux certificats seront acceptés par le navigateur. La faille réside dans le fait que jusqu'à présent le titulaire d'un domaine n'avait aucun moyen d'indiquer au monde quels AC ou certificats devaient être utilisés pour authentifier la connexion au serveur d'un domaine particulier.

Nécessité d'une solution

L'utilisation de PKIX pour sécuriser les communications Web n'est pas nouvelle. Les éditeurs de navigateurs, utilisateurs et organismes de normalisation sont tous conscients du problème - «Problème des AC nombreuses». Il y a eu quelques tentatives d'atténuation du problème (Perspectives, ToFU (Trust on First Use), Channel ID, Certificate Transparency, etc.), mais ces tentatives sont devenues plus ciblées après les deux attaques de haut niveau sur les AC Comodo et DigiNotar.

La chronologie des événements est la suivante. Comodo a découvert que l'une de ses Autorités d'enregistrement[2] (AE) affiliées avait été compromise le 15 mars 2011 et que l'attaquant avait créé un compte utilisateur avec l'AE affiliée. Avec ce compte, l'attaquant a créé des Demandes de signature de certificat pour des sites Web de grande valeur tels que *login.live.com*, *mail.google.com*, *login.yahoo.com* etc. et l'on croit qu'il a obtenu au moins un certificat public X.509 pour ces sites (à partir de ses 9 demandes).

Sans entrer dans les aspects politiques de cette attaque, un attaquant ayant créé des certificats frauduleux, comme dans le cas de Comodo, pourrait agir comme intercepteur (Man-in-the-middle) et rediriger l'utilisateur vers un faux serveur ressemblant à celui du site d'origine (hameçonnage ou phishing). Les certificats fournis par le faux serveur seront acceptés par le navigateur, car ils sont générés par une AC reconnue par le navigateur. Tout ce que l'utilisateur lit ou écrit (nom d'utilisateur, mot de passe, email, etc.) peut être vu et copié par le faux serveur.

[1] https://www.eff.org/observatory

[2] Les AE recueillent et vérifient les informations d'identité provenant d'Abonnés Directs à l'aide de procédures mettant en œuvre les politiques de validation d'identité. Les AE créent les Demandes de Signature de Certificat pour soumission à une AC. L'AC signe les Demandes de signature de certificat et délivre les certificats publics X.509 aux abonnés directs.

Selon les rapports, le pirate qui a pénétré dans Comodo est également parvenu à s'introduire dans les systèmes DigiNotar. Bien que l'attaque ait été révélée au public à la fin août 2011, l'enquête montre que l'intrus accédait au système DigiNotar depuis le 17 juin 2011. Tout comme dans le cas de l'attaque Comodo, l'intrus a créé des certificats numériques frauduleux pour des sites Web prestigieux. L'enquête révèle également que les certificats générés ont été utilisés pour rediriger des utilisateurs vers de faux serveurs et obtenir leurs informations d'identification.

DigiNotar et Comodo n'étaient pas des entreprises ordinaires. Ce sont des sociétés de sécurité de haut niveau auxquelles de nombreuses organisations, y compris des gouvernements, et des millions d'utilisateurs accordent leur confiance. Les attaques ultérieures sur des sociétés de haut niveau ont montré qu'il ne suffit pas de renforcer la sécurité de l'infrastructure des AC, et ont souligné la nécessité de réduire la portée des attaques dans le modèle PKIX.

Quelles solutions pour réduire la surface d'attaque ?

Comme mentionné précédemment, le problème n'est pas la sécurité de la technologie PKIX. Mais avec une liste aussi longue d'autorités de certification acceptées par les navigateurs par défaut, il existe une plus forte probabilité de compromission lors de l'établissement d'une connexion TLS avec PKIX, que lors de la résolution d'adresses IP avec le DNS. Comme indiqué précédemment, avec le modèle PKIX actuel, un titulaire de nom de domaine n'a pas la possibilité d'indiquer au navigateur que toute connexion d'un utilisateur à son domaine doit être validée par un certificat délivré par une AC particulière.

Différentes techniques ont été proposées pour réduire la probabilité d'attaque au sein du modèle PKIX, telles que Trust on First Use (ToFU), Perspectives[3], Certificate Transparency[4] (CT), Certificate Authentication and Authorization (CAA)[5] et DANE.

Parmi les différentes technologies proposées pour limiter la surface d'attaque, ToFU est la plus facile à mettre en œuvre car il suffit d'installer un module de navigateur compatible ToFU. Perspectives et CT reposent sur un système de service de notarisation qui ne coexiste pas totalement avec le modèle PKIX actuel et nécessite des services supplémentaires agissant comme services de notarisation. CAA est comme une «bidouille» ne nécessitant aucune modification et qui semble à court terme une bonne solution pour réduire la surface d'attaque. Mais si l'on considère la sécurité de façon plus globale et la fourniture d'options supplémentaire aux utilisateurs (telles que des certificats auto-signés), DANE arrive en tête.

[3] http://perspectives-project.org/

[4] http://www.certificate-transparency.org/

[5] http://tools.ietf.org/html/rfc6844

2 Une solution permettant de déployer un dispositif de sécurité bout-en-bout : DANE

DANE - Augmenter la sécurité dans PKIX

Cette section explique de façon plus détaillée comment DANE réduit la portée d'une attaque dans l'écosystème PKIX, en s'appuyant sur une infrastructure DNS sécurisée grâce à DNSSEC[6]. Avec le protocole DANE, un titulaire de nom de domaine signe le certificat fourni par le serveur Web en fonction de différentes options (expliquées ci-dessous) et le publie dans la zone DNS du domaine (signée avec DNSSEC), offrant ainsi au titulaire du nom de domaine la possibilité d'informer l'application (p. ex. le navigateur) sur les moyens de valider le certificat provenant du serveur Web. Par exemple, si l'AC du domaine www.example.com est «X», avec le mécanisme DANE, le navigateur n'acceptera qu'un certificat de l'AC «X» pour authentifier le serveur, ce qui réduit ainsi la probabilité d'une attaque.

DANE a été conçu et normalisé par l'IETF. L'IETF a publié deux RFC concernant DANE :

1. RFC 6394 – Cas d'utilisation DANE
2. RFC 6698 - Protocole DANE.

Le RFC 6698 met l'accent sur la normalisation et l'utilisation de l'enregistrement de ressource TLSA. Cet enregistrement a pour rôle essentiel d'être publié dans une zone DNS et de fournir des informations de certificat correspondant à un service spécifique sur un port spécifique d'un nom dans cette zone.

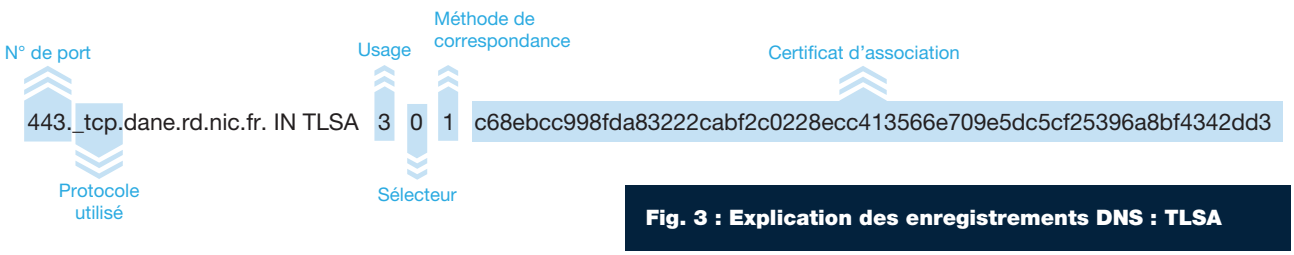


Fig. 3 : Explication des enregistrements DNS : TLSA

Comme le montre la Figure 3, l'enregistrement de ressource TLSA se compose de quatre champs : «utilisation du certificat», «sélecteur», «méthode de correspondance» et «certificat d'association». L'application doit établir la correspondance entre le «champ de données certificat d'association» de l'enregistrement de ressource (RR) TLSA et le certificat cible (c.-à-d. le certificat fourni par le serveur web du nom de domaine) sur la base des autres valeurs (utilisation du certificat, sélecteur et méthode de correspondance) figurant dans l'enregistrement de ressource TLSA.

Le champ «Utilisation du certificat» est brièvement résumé ici. Pour de plus amples informations sur les autres paramètres du RR TLSA, veuillez vous référer au RFC 6698

Utilisation du certificat 0/1: si le champ «utilisation du certificat» dans le RR TLSA a pour valeur '0 'ou '1 ', l'application doit valider le certificat cible utilisant l'infrastructure PKIX, c.-à-d. valider le certificat cible en utilisant l'écosystème des AC.

- '0' - Lors de la validation, le navigateur doit utiliser uniquement l'AC spécifiée dans le champ «Certificat d'association» du RR TLSA pour valider le certificat cible.
- '1' - Le navigateur doit valider le certificat cible uniquement avec le certificat mentionné dans le champ «Certificat d'association» du RR TLSA.

Il y a deux autres valeurs ('2' et '3') dans le champ «Utilisation du certificat», qui seront expliquées plus loin.

[6] Voir description de ce mécanisme plus loin

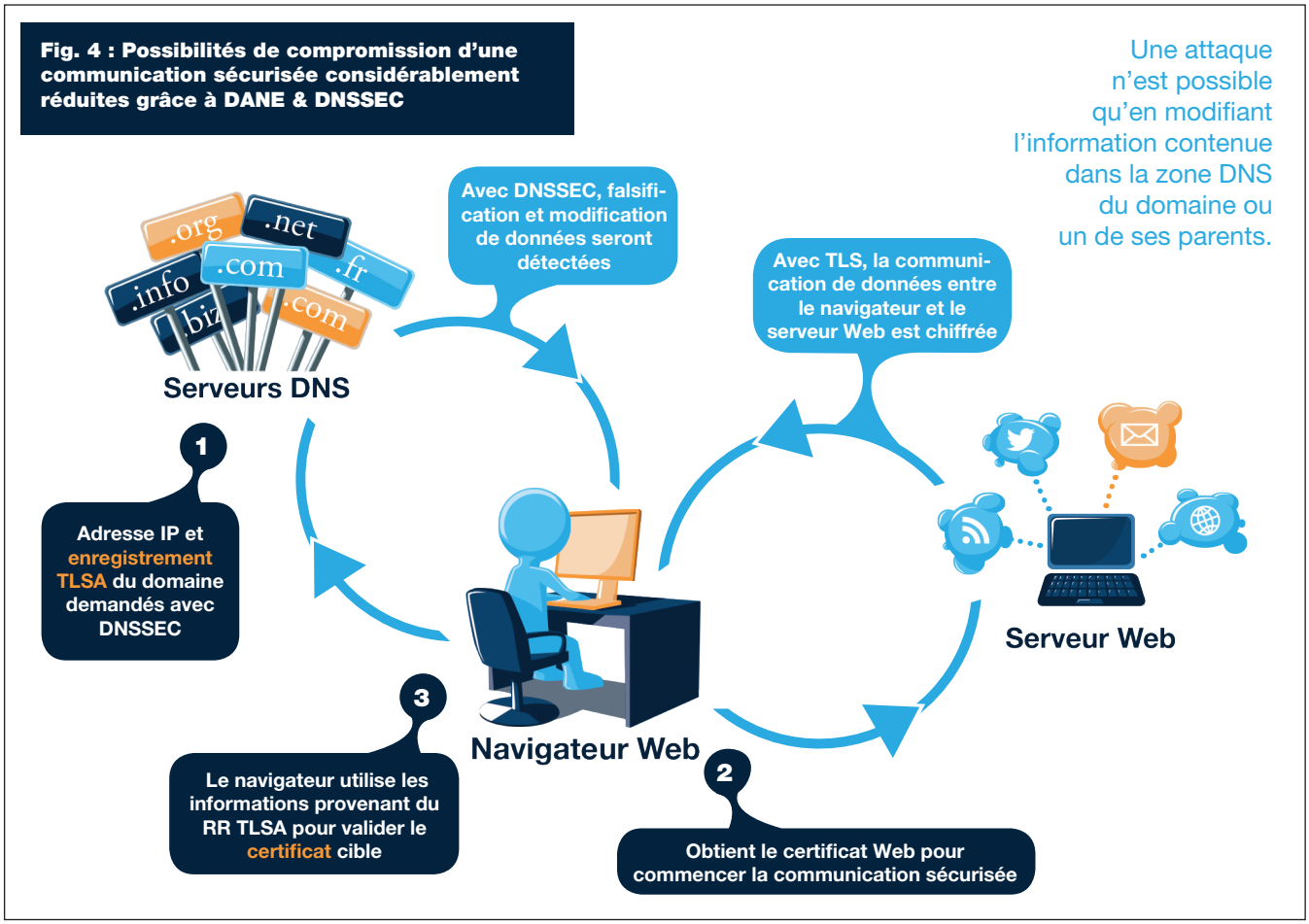
Pourquoi DNSSEC est-il vital pour DANE ?

Les valeurs '0' et '1' du champ «utilisation du certificat» indiquent comment la surface d'attaque peut être réduite au sein de l'écosystème PKIX en validant le certificat cible fourni par le serveur. Supposons que l'attaquant ait lancé une attaque de type «Man in the middle» lors de la résolution DNS («première opération» de la figure 3) et fourni une adresse IP frauduleuse pour le domaine demandé, le navigateur utilisera l'adresse IP obtenue pour accéder au serveur. Si l'attaquant crée un certificat numérique pour le faux serveur à partir d'une AC autorisée, l'attaquant peut convaincre le navigateur qu'un serveur choisi par l'attaquant lui-même représente légitimement le service de la victime.

DNSSEC[7] permet à un utilisateur de vérifier, sur la base d'une chaîne de confiance cryptographique, que les informations résultant d'une requête de résolution DNS proviennent de la zone DNS légitime correspondant au nom de domaine demandé. En d'autres termes, lorsqu'elles sont utilisées de bout-en-bout dans le processus de résolution DNS, les extensions DNSSEC empêchent que les données ne soient altérées lorsqu'elles redescendent jusqu'à l'utilisateur demandeur. Par conséquent, pour que DANE augmente la sécurité au sein du modèle PKIX existant, les informations obtenues lors de la résolution DNS doivent être validées avec DNSSEC. C'est pourquoi le RFC 6698 (protocole DANE) stipule que la zone DNS qui a un RR TLSA doit être signée par DNSSEC et que les applications qui interrogent le domaine pour validation du RR TLSA doivent utiliser un résolveur DNSSEC. Pour simplifier, DANE n'est efficace que s'il repose sur une infrastructure DNSSEC.

Ainsi DANE combiné à DNSSEC offre une sécurité de bout-en-bout aux deux étapes d'une communication Internet (comme le montre la Figure 4) : tout d'abord lors de la résolution DNS préliminaire, puis lors de la connexion établie avec le serveur du domaine.

Fig. 4 : Possibilités de compromission d'une communication sécurisée considérablement réduites grâce à DANE & DNSSEC



[7] http://tools.ietf.org/html/rfc6698/

DANE - Utilisation de DNSSEC comme PKI alternative

Jusqu'à présent, l'attention était portée sur une infrastructure à clés publiques (PKI) reposant sur des certificats numériques, à savoir le modèle PKIX. Le DNS complété par les extensions DNSSEC devient *de facto* une PKI.

Comme dans le cas du modèle PKIX, où la clé de l'AC est l'ancre de confiance, dans le cas du PKI DNSSEC, l'ancre de confiance est la clé de la racine du DNS.

Les valeurs '2' et '3' du champ «utilisation du certificat» indiquent comment une sécurité de la navigation sur le Web peut être instaurée de bout-en-bout sans que l'écosystème des AC entre en jeu. Autrement dit, un titulaire de domaine crée un certificat auto-signé et peut toutefois être authentifié par les éditeurs de navigateurs :

- '2' en cas d'utilisation indique qu'une organisation a prévu de créer sa propre AC et que tous les départements de cette organisation créent leurs propres certificats avec l'AC créée comme ancre de confiance de leurs sites Web respectifs. Lors de la validation, normalement le navigateur ne reconnaîtra pas le site Web des départements de l'organisation, car l'AC de l'organisation ne figure pas dans sa liste des AC de confiance. Mais, en recevant le RR TLSA dans la réponse après validation DNSSEC, il est certain que les données de l'enregistrement TLSA ne sont pas contrefaites, sauf si quelqu'un a accès à la zone DNS du domaine. Pour valider le certificat, le navigateur doit s'assurer que l'AC du certificat cible est la même que celle indiquée dans le champ «Certificat d'association» du RR TLSA.
- '3' en un cas d'utilisation indique que l'administrateur de domaine délivre le certificat auto-signé qui est stocké comme certificat cible sur le serveur web, et qu'une empreinte du certificat est ajoutée dans la zone DNS du domaine dans le champ «certificat d'association» du RR TLSA. Pour valider le certificat, le navigateur doit s'assurer que le certificat cible correspond au champ «Certificat d'association» du RR TLSA.

Ainsi, la technologie DANE renforce non seulement la sécurité de la navigation Web sur le dernier kilomètre en utilisant le modèle PKIX existant, mais fournit également une solution alternative consistant à n'utiliser qu'un DNS renforcé par DNSSEC et donc à contourner complètement le mécanisme de fourniture et de gestion des certificats X.509 via PKIX.

Mettre en œuvre DANE

La première étape vers la mise en œuvre DANE pour un nom de domaine est de créer un enregistrement TLSA pour le domaine, par l'administrateur du domaine. Il existe plusieurs outils disponibles pour générer un enregistrement TLSA. L'un d'eux est 'SWEDE[8]'. L'enregistrement TLSA généré est publié dans la zone DNS par l'administrateur du domaine, et la zone a été signée avec DNSSEC.

Au cours de résolution DNS, l'enregistrement TLSA devrait également être interrogé comme indiqué dans la Figure 4. Si le champ «utilisation de certificat» dans l'enregistrement TLSA a des valeurs '0' ou '1 ', l'application doit valider le certificat cible en utilisant l'infrastructure PKIX (voir III.1). Si le champ «utilisation de certificat» dans l'enregistrement TLSA a des valeurs '2 'ou '3', alors la validation est faite en utilisant l'infrastructure DNS renforcé par DNSSEC (voir III.3).

[8] https://github.com/pieterlexis/swede

3 En conclusion : DANE ou la pièce jusqu'à présent manquante au dispositif de sécurisation de bout-en-bout de l'Internet ?

DANE n'est pas réservé qu'à la navigation sur le Web

DANE a été conçu pour résoudre les problèmes relatifs à la navigation sur le Web. Des efforts ont été déployés à l'IETF au sein du groupe de travail DANE[9] pour en étendre l'utilisation à la sécurisation d'autres applications comme la messagerie électronique (s/MIME), la messagerie instantanée (XMPP), etc. Tous ces travaux se poursuivent et s'ils sont adoptés par l'IETF et publiés en tant que RFC, des implémentations suivront. DNSSEC est une infrastructure indispensable commune pour toutes ces implémentations.

Rôle de DANE dans l'accélération du déploiement de DNSSEC

Comme expliqué au début du présent document, une communication Internet type implique l'écosystème DNS pour résoudre l'adresse d'un nom de domaine particulier. DNSSEC permet de s'assurer que les données obtenues par résolution DNS proviennent de la zone légitime du nom de domaine (authentification de l'origine des données) et que les données ne sont pas altérées lors du transfert (intégrité des données). Ces extensions de sécurité font de DNSSEC une composante essentielle des communications Internet nécessitant un haut niveau de confiance dans l'infrastructure DNS.

Comme la plupart des technologies importantes (telles que IPv6), DNSSEC illustre le paradoxe de l'œuf et de la poule. De nombreux fournisseurs de services et d'infrastructure réseau adoptent une position attentiste à l'égard de DNSSEC. Les raisons invoquées sont variables et vont de la complexité de mise en œuvre de DNSSEC aux pannes injustifiées et incitations commerciales. Beaucoup d'entre eux sont prêts à attendre un scénario qui les obligera à déployer DNSSEC dans leur infrastructure réseau.

L'adoption lente de DNSSEC a souvent été attribuée à l'absence d'application phare utilisant DNSSEC comme base de la sécurité. Le potentiel commercial généré par une telle application peut induire une pression des consommateurs pour l'adoption de DNSSEC. Même si les applications construites autour de DNSSEC et du protocole DANE peuvent ne pas être des applications phares pour DNSSEC, leur mise en œuvre de manière transparente assurera la sécurité de millions d'utilisateurs utilisant Internet pour des communications sécurisées. L'utilisation même de ces applications par des millions d'utilisateurs exigeant une infrastructure réseau sécurisée par DNSSEC forcera les parties prenantes à déployer DNSSEC. Ainsi, DANE pourrait être un catalyseur accélérant l'adoption de DNSSEC

Retrouvez tous les dossiers thématiques de l'Afnic :
http://www.afnic.fr/fr/ressources/publications/dossiers-thematiques-7.html

[9] https://datatracker.ietf.org/wg/dane/charter/