FOAD : Protection des accès distants

1 Ressource

— "Firewall Policies and VPN Configurations", ISBN : 978-1-59749-088-7 pages 246-289 (accessible sur Scholarvox cyberlibris)

2 Commentaire slides IPsec

Si une entreprise peut naître très discrètement dans un garage, elle a pour objectif de croître et de s'étendre. En effet, au fur et à mesure de son développement, elle va faire appel à de nouvelles compétences et services qui vont demander de l'espace. Dans le cas d'un FAI, par exemple, les services orientés "technique" ne seront pas colocalisés avec les services de ressources humaines ou la direction de l'entreprise : ces différents départements obéissent à des contraintes de sécurité et d'accessibilité différentes. Leur aménagement et les contrôles d'accès mis en oeuvre ne seront donc pas les mêmes.

Une fois stabilisée sur la région d'origine, l'entreprise va entrer dans une phase d'identification de nouveaux consommateurs de ses services. Pour accéder à ces nouveaux marchés, elle pourra commencer par l'envoi d'émissaires (le commercial) mais, selon l'ampleur de la collaboration, elle pourra mettre en place un point de présence (infrastructure et personnel). Parallèlement, l'entreprise permettra à certains employés de travailler de chez eux selon un horaire défini.

Ces différentes situations (entreprise répartie sur différents sites, travail à distance, travail en mobilité) ne font pas exploser l'entreprise en différentes entités indépendantes : ces acteurs accèdent à des ressources communes (fichiers, outils *legacy* etc...). Il est donc indispensable de se doter de moyens de communication adaptés.

La première piste consisterait à mettre en place une infrastructure dédié : un nouveau réseau serait donc déployé sous le contrôle exclusif de l'entreprise E. Les accès à la ressource étant contrôlés par des membres d'E, on peut croire que la sécurité est maximale sur tous les aspects. Malheureusement, les charges associées à l'installation (installer les antennes-relais, creuser pour faire passer les câbles...) et à la maintenance du système de communication retombent sur E qui peut ne pas être spécialiste du réseau. De plus, ce type de solution supporte mal la mobilité : pour chaque nouveau recruté, il faudrat s'assurer que son quartier d'habitation soit couvert par le réseau géré par son employeur.

Une fois la solution dédiée écartée, E peut envisager d'exploiter une infrastructure existante : cette approche libèrerait E du fardeau de la maintenance qui ne devrait se soucier que des droits d'accès/utilisation. S'il existe des solutions de type ligne louée (une partie de l'infrastructure d'un fournisseur de services est louée à E qui en a la jouissance quasi exclusive), la solution naturelle aujourd'hui est de passer par le réseau Internet : en plus d'être omniprésent, ce réseau a vu ses coûts d'accès devenir plus qu'abordables. Par contre, la question de la protection des données durant leur cheminement dans le réseau se pose : ce qui sera injecté correspond à la force vitale de l'entreprise : que se passe-t-il si un routeur vampire se trouve sur le chemin ? Ce type de réflexions a mené à la définition de réseaux privés virtuels (*Virtual Private Network*, VPN) : un tunnel est donc créé dans le réseau pour masquer les données. Masquer ici équivaut à confidentialiser donc à chiffrer pour rendre l'interprétation difficile. Deux familles de solutions sont souvent rencontrées : le VPN basé sur IPsec (niveau réseau) et le VPN basé sur SSL.

Le support d'IPsec se fait un niveau su système d'exploitation : l'OS est en charge du stockage des informations de configuration telles la *Security Policy Database* à laquelle nous reviendrons plus tard. Selon le positionnement de l'équipement et la politique d'entrerprise, ces fonctionnalités pourront être activées ou pas. Par exemple, sur la figure de la slide 6, un noeud du LAN n'a pas à supporter le protocole sécurisé car le routeur d'accès à Internet s'en charge. PAr contre, pour un utilisateur en mobilité désirant contacter son réseau d'origine, ces fonctionnalités doivent être activées.
Certaines configurations chiffrent l'intégratlité des données échangées, on parlera alors de *blanquet coverage*.

Deux protocoles sont utilisés pour la sécurité : *Authentication Heade*r (AH) et *Encapsulation Security Payload* (ESP). AH est le plus simple des deux : une en-tête supplémentaire est insérée entre IP et TCP. Cette en-tête comporte un hash du message permettant de contrôler son intégrité et son authenticité. L'ensemble du message n'est donc pas chiffré, ce qui est dommage lorsque la confidentialité est critique. AH sera donc exploité lorsqu'une autre technologie complémentaire aura mis en oeuvre le tunnel.

ESP prend en charge l'intégrité et la confidentialité en chiffrant la paylaod : le paquet entier étant chiffré, les informations d'adressage sont également masquées ; il est donc nécessaire d'encapsuler à nouveau le résultat avec les adresses IP des noeuds chargés de l'application du protocole.

Le fonctionnement d'ESP repose sur des *Security Associtaions* (SA) entre la source et la destination. Ces SA sont des liens unidirectionnels gérés par le système d'exploitation dans le contexte de la *Security Association Database* (SAD) : chaque entrée de cette liste correspond à un SA. En examinant le contenu de la ligne, l'équipement détermine l'identité de son interlocuteur et la manière de traiter les messages (quel algorithme de chiffrement, quel algorithme de contrôle d'intégrité etc...).

Dans le document, nous nous intéressons au mode tunnel d'ESP dans lequel la totalité du paquet est chiffrée car il permet justement de créer le tunnel. Dans ce mode, le paquet d'origine est donc chiffré avec un algorithme de chiffrement par bloc. On se souviendra que le message est découpé en blocs de taille fixe au début du traitement. Si la taille du paquet n'est pas un multiple de la taille de bloc, il sera nécessaire d'ajouter des bits de bourrage qui seront supprimés à la réception. A cet ensemble, on ajoutera une en-tête ESP indiquant la manière de traiter le contenu : une référence à une ligne de la SAD sera donc introduite par ce champ. Afin d'assurer que l'ensemble provient bien d'un noeud connu, un MAC est calculé et attaché à la fin du bloc. Le processus de création du MAC est rappelé en slide 13.

Avec ESP, les paquets circulant librement sur le LAN sont habillés d'une armure au moment de s'aventurer sur Internet. Cela implique que pour le noeud mobile (souvent appelé un *road warrior*), l'OS sera responsable de la mise en oeuvre du tunnel avec la passerelle distante et de la gestion des couches de protection du message.

IPsec autorise des combinaisons quasi infinies de solutions : par exemple, deux ordinateurs dans deux LAN séparés peuvent produire sur leurs LAN respectifs du trafic IPsec qui sera à nouveau encapsulé par la passerelle au moment de sortir du réseau local. Malheureusement les implémentations existantes ne sont pas tenues de supporter toutes les combinaisons possibles et imaginables car plus la solution proposée est flexible, plus elle se rapproche d'une usine à gaz (comprenez, elle devient complexe :)).

Dans IPsec, les solutions de chiffrement symétrique et asymétrique ont leur place. Les solutions asymétriques permettent d'assurer authenticité et confidentialité : elles seront donc exploitées lors de la création de lien entre passerelles avec des mécanismes de type DH. Par contre, pour les liens entre utilisateurs du service de la passerelle, les solutions utiliseront des algorithmes avec un coût computationnel réduit : en effet, plusieurs postes de travail peuvent dépendre de la même passerelle

donc un algorithme lourd affecterait la performance.

Un autre aspect du passage à l'échelle concerne le partage des clés publiques : si dans un réseau de faible taille, il est envisageable de pré-partager les clés (donc les renseigner manuellement), cette approche devient coûteuse quand les distances augmentent et/ou les noeuds se multiplient. Un protocole supplémentaire (IKE) prend e charge l'échange dynamique de clés sous forme de certificats, ce mode de fonctionnement permettant de sécuriser les échanges pour des noeuds qui ne se connaissaient pas antérieurement.

Finalement, il faut garder à l'esprit que tout le trafic géré par la passerelle n'a pas vocation à emprunter un tunnel IPsec. En effet, l'utilisateur peut être sur FB tout en communiquant avec le réseau central. Ce sera le rôle de la SPD de permettre d'orienter les messages vers les chaînes de traitement appropriées.

Les slides concernant SSL ne sont pas commentées puisque vues en cours en 4e année. Le schéma présenté pour le Secure SHell introduit la séance de TP correspondante et sera commentée à ce moment. Vous remarquerez que SSH fait appel (comme plusieurs autres solutions) à l'opérateur modulo. Dans ce contexte, une introduction à ce type d'espace vous est proposée sous forme de TD à remettre.

Pour votre culture personnelle, un lien vers la spécification d'un autre type de VPN vous est fourni à la fin de la présentation. Des points vous permettant d'en organiser votre compréhension vous sont proposés : les réponses ne sont pas à inclure dans votre compte-rendu.

3 Questions

Comparez en terme de protection des données, de coût financier et de complexité de mise en oeuvre (logiciel et matériel spécialisé ?) les solutions de transport de l'information sensible suivantes :

— infrastructure dédiée
— traversée libre du réseau Internet
— VPN IPSec
— VPN SSL

IPSec Quelle est l'utilité du champ MAC ESP dans le paquet IPSec ?

Rappelez la définition du passage à l'échelle. Comment IPSec prend-t-il en compte cette contrainte sur le partage des clés ?

4 TD

Les différents algorithmes vus en cours font appel à la fonction modulo et au Ou-Exclusif dans leur traitement de l'information. Cela revient à travailler dans un cors de Galois qui est un corps contenant un nombre fini d'éléments. Dans la suite, on considèrera que le corps comporte un nombre premier q d'éléments. Considérons l'ensemble Z/q des entiers relatifs modulo q. Pour tout élément e appartenant à Z/q, on peut écrire e = p.q + r

avec $0 \leq r \leq q - 1$.

Ex : Z/2 est un corps de Galois à 2 éléments : 0,1 Sur ce corps, on définira les opérations d'addition et de multiplication (et leurs opérations inverses) : 0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

0.0 = 0
0.1 = 0
1.0 = 0
1.1 = 1

L'addition est dont équivalente à un _ _ et la multiplication à un _ _.

Ex : Considérons Z/5 = 0, 1, 2, 3, 4. Complétez les tables suivantes, utilisées pour l'addition et la multiplication.

Addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	_	_	_	_
3	3	_	_	_	_
4	4	_	_	_	_

Multiplication

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	_	_	1	3
3	0	_	_	_	_
4	0	4	_	_	_

4.1 Extension de corps de Galois $\mathbf{Z}/2^m$

L'alorithme AES manipule des octets dans ses différentes opérations. Les résultats de ces opérations sont codés sur 8 bits ce qui signifie que le nombre d'éléments manipulables est fini. Par contre, il n'est pas premier (256 possibilités). Les manipulations seront donc différentes sur ces extensions de corps de Galois. Les éléments seront désormais des polynômes A(x) tels que :

$$A(x) = a_7x^7 + ... + a_1x + a_0 \tag{1}$$

a_i appartenant à Z/2.
Un tel polynôme peut être stocké sous la forme d'un vecteur de 8 bits (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0) : la position du bit permet d'associer le bon coefficient à la puissance de x.
Sur l'espace contenant ces polynômes, on définira les opérations d'addition et de soustraction en conjonction avec le concept de polynôme générateur. Le polynôme générateur P est irréductible (ne peut être factorisé) et d'ordre m pour $Z/2^m$.
Soient A(x) et B(x) deux polynômes de $Z/2^m$. La somme de A(x) et B(x) est calculée comme :

$$C(x) = A(x) + B(x) = c_ix \tag{2}$$

$c_i = a_i + b_i \bmod 2$.
Le produit de A(x) et B(x) est calculé comme :

$$D(x) = A(x).B(x) mod P(x) \tag{3}$$

P(x) étant le polynôme générateur.

- Rapprochez l'équation 3 de la table de multiplication et expliquez le rôle du polynôme générateur dans la multiplication.
- Calculez la somme de A(x) et B(x) dans $Z/2^4$ avec $P(x) = x^4 + x + 1$
  - $A(x) = x^2 + 1$; $B(x) = x^3 + x^2 + 1$
  - $A(x) = x^2 + 1$; $B(x) = x + 1$
- Calculez le produit de A(x) et B(x) dans $Z/2^4$ avec $P(x) = x^4 + x + 1$