La sécurité des échanges sur les réseaux

1- Pourquoi et comment sécuriser ?

L'enjeu :

Afin d'éviter toute intrusion pirate sur un réseau ou bien l'implantation d'un virus, il est nécessaire de bien protéger son réseau. Cela passe notamment par la sécurisation des processus d'authentification, ceux-ci doivent être confidentiel et bien vérifier que la personne qui se connecte au réseau est la bonne. On peut aussi parler des programmes qui doivent certifier qu'ils ne sont pas infectés et qu'ils réalisent bien ce qu'ils sont censés faire et rien de plus.

Les objectifs :

Sécuriser son réseau veut dire chercher à atteindre plusieurs objectifs comme notamment :

La confidentialité : c'est-à-dire que lorsqu'une communication à lieu sur le réseau, celle-ci ne doit pas pouvoir être lu ou récupérés par une tierce personne. D'autant plus lorsque ce sont des données sensibles qui sont communiqués, celles-ci doivent être davantage sécurisés.
L'authentification : dans un réseau li faut toujours veiller à ce que les différentes entités qui communiques soient sur de l'identité de la personne avec qui ils échangent, notamment lorsqu'il s'agit de communications commerciales ou encore lors d'un échange enter un logiciel client et un logiciel serveur.
La non-répudiation : cela concerne la validité juridique des signatures, c'est-à-dire s'assurer qu'un contrat signer sur internet ne puisse être remis en cause par l'une des parties
Le contrôle d'intégrité : pour s'assurer de l'intégrité de l'information sur un réseau, il faut s'assurer que lors d'un transfert d'informations rien n'ai pu être altérer par une tierce personne.

2- Les moyens :

Nous allons maintenant voir les différentes manières disponible pour sécuriser au mieux les échanges sur un réseau :

Le Cryptage :

Pour le cryptage, 2 méthodes sont utilisées : les clés symétriques ou les clés asymétriques.

Les avantages de ces deux méthodes sont repris dans une solution intermédiaire : la clé de session.

Les clés symétriques ou privées : On utilise la même clé pour crypter et décrypter le message.

- Avantage : les algorithmes de cryptage et décryptage sont rapides.
- Inconvénient : il faut transmettre la clé privée sur le réseau ; or, cette clé peut être interceptée par une personne malveillante.

Les clés asymétriques ou publiques : On utilise deux clés : une pour crypter, l'autre pour décrypter. L'une est transmise sur le réseau : la clé publique, l'autre est conservée par son propriétaire : la clé privée.

- Avantage : seule la clé publique est transmise.
- Inconvénient : les algorithmes de cryptage et de décryptage sont lents.

La clé de session : Pour pallier la lenteur de l'algorithme à clés publiques, on va utiliser celui-ci pour déterminer une clé symétrique entre deux interlocuteurs. Cette clé sera elle-même cryptée par des clés asymétriques avant d'être transmise sur le réseau. Puis elle sera ensuite utilisée pendant l'échange à la place des clés asymétriques.

Le Hachage :

Une fonction de hachage va convertir des séquences de caractères de différentes longueurs en séquences de même longueur. Par exemple, la fonction de hachage confère à des mots de passe différents une quantité définie de caractères autorisés. Une conversion de la valeur de hachage dans le sens inverse, c'est-à-dire vers la séquence de caractères initiale, est exclue.

Il y a certaines caractéristiques exigé pour une fonction de hachage :

- Un sens unique de la fonction de hachage, c'est-à-dire qu'une valeur de hachage généré ne doit pas permettre de générer à nouveau le contenu des données utilisées en entrée.
- Une absence de collisions, c'est à dire qu'une même valeur de hachage ne doit pas pouvoir être attribuée à des données initiales différentes, lorsque c'est atteint on parle de fonction de hachage cryptographique. En somme, chaque valeur d'entrée doit générer une autre valeur de hachage.

Ces algorithmes couplés avec les algorithmes à clés asymétriques permettent de vérifier l'authenticité et l'intégrité.

Les Certificats :

Contenu :

Le certificat est un lien entre les données d'identification d'une personne et les données enregistrées et garanties par l'autorité de certification.

Le contenu d'un certificat est aujourd'hui normalisé par la norme X509, version 3. Elle contient les informations suivantes :

–la version du certificat délivré ;

–le numéro de série attribué par l'autorité de certification ;

–l’algorithme de signature utilisé par l’autorité de certification pour signer le certificat ;

–le code de l’autorité de certification ;

–la validité du certificat ;

–le nom du propriétaire du certificat ;

–la clé publique du propriétaire du certificat ;

–la signature du certificat par l’autorité de certification (emprunte numérique à l’aide d’une fonction de hachage).

Signature :

Une signature numérique est une manière d’assurer la non-répudiation d’un document ainsi que d’authentifier l’auteur. Elle a la même valeur aux yeux de la loi qu’une signature manuscrite d’un document cependant elle se différencie car elle n’est pas visuelle, elle est représentée par une suite de caractère.

Afin qu’une fonction de signature sois considérée comme valable, elle doit être :

- Authentique
- Infalsifiable
- Non réutilisable
- Inaltérable
- Irrévocable

Autorité de certification :

Il existe deux différents type d’autorité de certification :

- L’autorité de certification commerciale, qui fournit des certificats dans lequel des clients, ou des services externes à l’entreprise, ont confiance. On fait appel à une société dont l’activité est la gestion de certificats. Les plus connues sont Verisign, Thawte, Securenet, Globalsign, Certeurope.

- L’autorité de certification privée ou autonome qui génère des certificats internes au réseau de l’entreprise pour sécuriser ses échange

L’horodatage :

Prenant la forme d’un sceau électronique, l’horodatage de documents numériques peut servir de preuve irréfutable sur l’existence d’un fichier à une date et une heure précise, mais aussi de garantir la non-modification du document depuis cette date. L’horodatage électronique peut être utilisé comme une preuve devant les tribunaux ou d’autres instances légales en cas de litige. Le sceau électronique, faisant foi comme le cachet de la Poste, garantit la valeur probante des actes et documents électroniques tels que les factures, les contrats et autres documents administratifs.

Le RSA :

Le chiffrement RSA nommé d'après ses inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman est asymétrique : il utilise une paire de clés (des nombres entiers) composée d'une *clé publique* pour chiffrer et d'une *clé privée* pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne qui souhaite que lui soient envoyées des données confidentielles. Elle va rendre la clé publique accessible. Cette clé est utilisée par ses correspondants pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à l'émettrice, et lui permet de déchiffrer ces données.