Editions ENI

PKI
sous Windows Server 2016
Sécurité, cryptographie et certificats

Collection
Epsilon

Extrait

Chapitre 3
Cryptographie

1. Introduction

Les techniques cryptographiques font partie des éléments de base du fonctionnement d'une PKI (*Public Key Infrastructure* ou infrastructure de clé publique). Ce sont ces technologies qui seront concrètement utilisées pour fournir :

– La confidentialité, qui correspond au chiffrement des données de façon à ce qu'elles soient illisibles.
– L'authentification de l'utilisateur ou de l'ordinateur.
– L'intégrité des données qui assure que les données resteront non modifiées durant leur transit.

L'objectif de ce chapitre est de fournir les bases essentielles qui vous permettront de comprendre clairement le rôle de la cryptographie dans une infrastructure de PKI, et particulièrement son lien avec l'autorité de certification et les services/applicatifs utilisant des certificats.

Les ateliers de ce chapitre de mise en place du système EFS (*Encrypting File System*) dans un environnement de groupe de travail (Workgroup), illustreront les techniques de chiffrement.

2. Chiffrement des données (confidentialité)

Le chiffrement des données repose sur l'utilisation d'algorithmes mathématiques et des certificats. Deux types de chiffrement peuvent être utilisés, le chiffrement symétrique et le chiffrement asymétrique.

Remarque

Certaines documentations utilisent également le terme de cryptage symétrique ou cryptage asymétrique. Afin de ne pas prêter à confusion, nous utilisons uniquement dans ce livre le terme équivalent de chiffrement (cipher en anglais).

2.1 Chiffrement symétrique

Le chiffrement symétrique utilise des algorithmes mathématiques (tels que Des, 3Des ou Aes…) pour chiffrer les données.

Étant donné que ces algorithmes mathématiques sont publiquement connus, un attaquant pourrait, en renversant l'algorithme, retrouver les données en clair. C'est pour cela qu'un élément aléatoire doit être introduit dans le calcul mathématique, une valeur, généralement codée sur 128 ou 256 bits, qui permet de rendre le résultat aléatoire et donc très difficilement réversible. Pour retrouver le texte en clair il faudrait essayer l'algorithme mathématique avec toutes les combinaisons possibles de clés aléatoires. Pour une clé codée sur 256 bits qui représente la norme actuelle, les temps de calcul seraient trop importants et humainement impraticables.

Cette clé, tirée aléatoirement avant chaque chiffrement, est appelée clé symétrique. Le terme symétrique vient du fait que c'est la même clé qui, associée à l'algorithme mathématique, permet aussi bien le chiffrement que le déchiffrement des données.

Prenons un exemple…

Nous souhaitons envoyer un fichier chiffré à l'utilisateur Bob (un mail ou tout autre ensemble de données…).

Imaginons un algorithme mathématique simple qui pour chiffrer un texte décalerait les lettres de trois positions dans l'ordre alphabétique. On décale alors la lettre B de trois positions selon l'ordre alphabétique pour obtenir la lettre E, puis on décale alors la lettre suivante, o, de trois positions selon l'ordre alphabétique pour obtenir la lettre r, puis on décale à nouveau la lettre suivante n de trois positions selon l'ordre alphabétique, pour obtenir la lettre q et ainsi de suite…

Le mot Bonjour après chiffrement devient alors le mot Erqmrxu.

Dans notre exemple, l'algorithme mathématique est un décalage de lettre dans l'ordre alphabétique et la clé symétrique aléatoire qui fait varier le résultat est la valeur 3. Lors d'une prochaine utilisation, on pourrait choisir une clé aléatoire symétrique différente, 8 par exemple, pour décaler d'un nombre de positions différent dans l'ordre alphabétique.

Nous pouvons ensuite envoyer le texte chiffré à Bob avec la clé de chiffrement symétrique. Bob utilisera cette même clé (3), pour décaler en sens inverse chaque lettre de trois positions dans l'ordre alphabétique. Il pourra ainsi déchiffrer le texte.

L'algorithme de chiffrement décale les lettres dans l'ordre alphabétique d'un nombre de positions fixé par la clé de chiffrement symétrique (ici 3).

Il ne s'agit bien sûr que d'un exemple pédagogique, dans la réalité les algorithmes de chiffrement (Des, 3DES et AES) sont bien plus robustes et complexes.

2.2 Chiffrement asymétrique

Dans le chiffrement asymétrique, deux clés sont utilisées (et non plus une seule comme dans le chiffrement symétrique) : la clé publique et la clé privée.

Où sont stockées ces clés ?

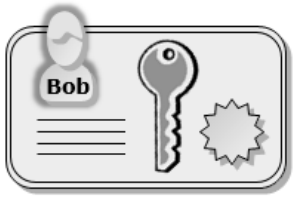
La clé publique est liée au certificat, elle est incluse dans le certificat. En donnant mon certificat, je donne aussi ma clé publique. La clé privée, elle, est stockée à l'extérieur du certificat, dans un emplacement protégé de l'ordinateur.

La taille standard de clés privées/publiques est actuellement de 1024, 2048 ou 4096 bits.

Qu'est-ce qu'un certificat ?

Un certificat est un fichier binaire qui contient (entre autres) :

– La clé publique !
– Des informations en clair sur le propriétaire des clés, leur durée de vie, les utilisations possibles…



Clé Publique de Bob

Le point capital à comprendre ici est que, ces deux clés, publique et privée, sont liées par un rapport mathématique de 1 à 1. Ce qui veut dire en clair que ce qui est chiffré avec l'une des deux clés ne peut être déchiffré que par l'autre clé correspondante. Nous n'allons pas démontrer ce point, il nous faudrait rentrer dans des mathématiques pures (les deux clés sont, pour vulgariser à l'extrême, le résultat de la factorisation de deux nombres premiers). Nous n'avons heureusement aucun besoin de démontrer ce lien mathématique de 1 à 1. C'est un fait, admettons le comme tel.

Mathématiquement, une clé publique ne correspond qu'à une (et une seule) clé privée, et inversement.

Avec laquelle des deux clés va-t-on chiffrer ?

Quelqu'un va souhaiter chiffrer un document pour vous l'envoyer. Il doit utiliser l'une de vos deux clés. Par convention il utilisera la clé dite publique. Comme son nom l'indique, elle peut être fournie à tout service/applicatif extérieur en charge du chiffrement.

Avec quelle clé va-t-on déchiffrer ?

Vous utiliserez votre clé dite privée. Comme son nom l'indique, vous conserverez cette clé de façon privée et vous serez la seule personne à l'utiliser pour déchiffrer le document.

■Remarque

Comme les clés privées/publiques sont liées par un rapport mathématique d'une à une, seule votre clé privée (correspondant à votre clé publique) pourra déchiffrer les données chiffrées !

Prenons un exemple…

Nous voulons envoyer des données chiffrées à Bob. Nous allons utiliser sa clé publique (celle de Bob) pour chiffrer les données. Une fois les données reçues par Bob, lui seul pourra déchiffrer les données avec sa clé privée (à cause du lien mathématique d'un à un entre les clés privée et publique).

On utilise la clé publique du destinataire pour chiffrer, le destinataire utilise sa clé privée pour déchiffrer.

2.3 Comparatif chiffrement symétrique et asymétrique

Nous avons vu qu'il existait deux types de chiffrement (symétrique et asymétrique). Quel est le plus couramment utilisé dans la pratique cryptographique ?

Effectuons une comparaison entre les deux types de chiffrement…

– Le chiffrement symétrique : il n'utilise qu'une seule clé pour chiffrer et déchiffrer. La clé étant de petite taille (256 bits par exemple), il est donc beaucoup plus rapide (100 fois ou plus) que le chiffrement asymétrique qui utilise deux clés de taille plus conséquente (2 048 bits par exemple).

L'inconvénient majeur du chiffrement symétrique est que les deux parties doivent déjà disposer d'un moyen sécurisé pour échanger la clé symétrique utilisée pour le chiffrement. De plus, avec quelques siècles, et en testant toutes les combinaisons clés symétriques, il serait possible … théoriquement … de déchiffrer les données.

Editions ENI

Sécurité informatique Ethical Hacking

Apprendre l'attaque pour mieux se défendre

(5e édition)

Collection
Epsilon

Extrait

Chapitre 8
Les failles web

1. Rappels sur les technologies du Web

1.1 Préambule

Il n'est pas concevable de se former à la sécurité des sites web sans avoir une bonne connaissance des mécanismes qui sont mis en jeu lors de la consultation de pages sur Internet. Nous allons rappeler dans ce chapitre les principales technologies du Web en expliquant les processus qu'elles mettent en place. Si vous pensez que vos connaissances sont déjà bien avancées dans ce domaine, vous pouvez passer directement à la section Généralités sur la sécurité des sites web de ce chapitre.

1.2 Le réseau Internet

Internet est un vaste réseau d'ordinateurs sur lequel transitent des millions d'informations quotidiennement. Ces données sont de différentes natures (e-mail, page web, chat, flux RSS...) et plusieurs méthodes sont utilisées pour les acheminer (HTTP, SMTP, FTP...). Chaque type de données et chaque méthode d'acheminement peuvent présenter des failles de sécurité.

Deux très importants types de données sont principalement utilisés sur le réseau Internet : les pages web et les e-mails. Dans ce chapitre nous développerons les bases des techniques d'attaque des sites web et expliquerons les principaux réflexes qu'il faut avoir pour s'en prémunir. Mais avant de commencer à développer les attaques possibles sur un site web il faut dans un premier temps bien comprendre les mécanismes qui sont mis en place lors de la consultation d'un site.

1.3 Qu'est-ce qu'un site web ?

Un site web est un ensemble de données cohérentes et ordonnées, comprenant plusieurs types de médias (texte, image, son, vidéo...). La consultation de ces informations s'effectue par un logiciel que l'on nomme navigateur. Les données sont transmises au navigateur, à sa demande, par un serveur. Un site web met donc en jeu une relation client/serveur. Les protocoles principalement utilisés pour l'échange des informations entre ces deux ordinateurs sont HTTP (*HyperText Transfer Protocol*) et HTTPS (*HyperText Transfer Protocol Secure*). Le mot *Secure* signifie sécurisé, mais nous verrons que c'est loin de garantir une sécurité totale et que bien souvent il donne un faux sentiment de sécurité. Les langages les plus utilisés pour la description des pages sont le HTML et le XHTML.

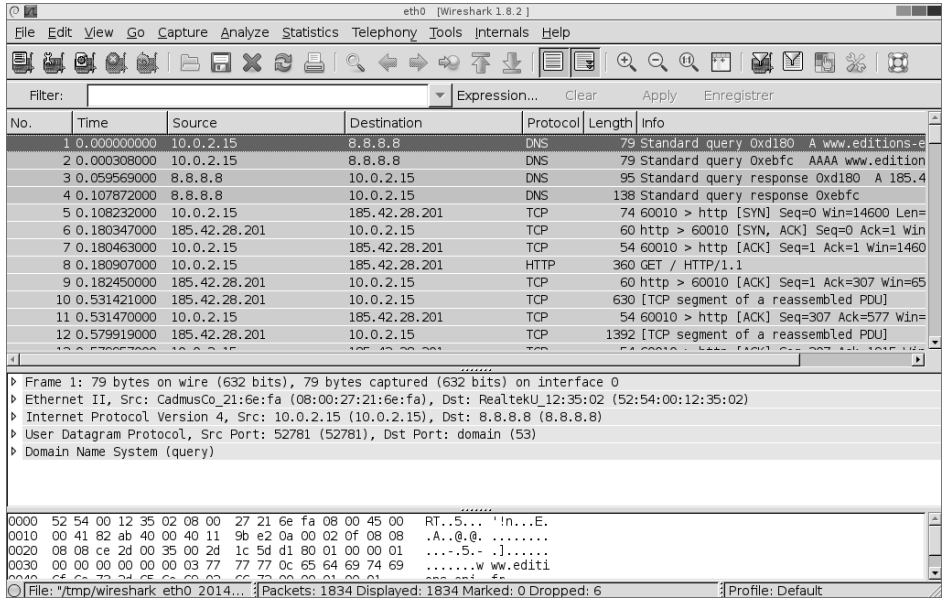
1.4 Consultation d'une page web, anatomie des échanges client/serveur

Lorsque nous souhaitons consulter un site web avec notre navigateur nous commençons par lui fournir l'adresse du site, son URL (*Uniform Resource Locator*) ou plus largement son URI (*Uniform Resource Identifier*). Nous emploierons ici le terme URL car il est le plus utilisé pour désigner l'adresse d'un site web. Supposons que nous voulions consulter le site http://mapage.com :

- Nous fournissons à notre navigateur l'adresse http://mapage.com.
- Notre machine va dans un premier temps chercher à résoudre le nom du site afin d'obtenir l'adresse IP du serveur qui l'héberge. Cette résolution de nom se fait grâce à une requête DNS (*Domain Name System*).
- Une fois l'IP obtenue, notre navigateur va envoyer une requête HTTP, sur le port 80, en utilisant la méthode GET sur la racine du site.
- Le serveur va alors nous répondre en renvoyant les données correspondant à la page d'accueil du site. Si des médias sont présents dans la page, plusieurs requêtes seront nécessaires afin d'aller chercher chacun d'eux.

Illustrons cet échange par un exemple concret en consultant le site des Éditions ENI. Pour cela, nous utiliserons un logiciel permettant de capturer l'ensemble des échanges entre notre ordinateur et le réseau Internet : Wireshark.

Nous obtenons le résultat présenté ci-dessous :



Nous constatons bien des requêtes DNS sur les six premiers échanges afin de résoudre l'adresse du site. Puis notre machine établit une connexion TCP avec le serveur par l'échange de trois paquets bien connus SYN, SYN/ACK et ACK. Le navigateur envoie alors la requête GET suivante : **`GET / HTTP/1.1`**

Mais ce n'est pas la seule information que notre navigateur envoie. Il fournit aussi beaucoup d'informations nous concernant afin que le serveur web puisse renvoyer la réponse la plus appropriée à notre situation. C'est ce que nous appelons les informations de l'en-tête HTTP, que voici dans notre cas :

```
GET / HTTP/1.1
Host: www.editions-eni.fr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0)
Gecko/20140722 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Nous trouvons dans cet en-tête des informations sur notre navigateur, notre système d'exploitation, le langage utilisé, le codage des caractères que nous acceptons, etc. Il est intéressant de noter que rien qu'avec cet en-tête, les serveurs web peuvent établir un bon nombre de statistiques.

Remarque

Pour mieux voir l'échange des données entre le client et le serveur dans Wireshark, il faut faire un clic droit sur le paquet TCP/SYN de la liaison client/serveur et demander ***Show TCP Stream****.*

Après la réception de ces données, le serveur web répond en conséquence. Il renvoie aussi un grand nombre d'informations. Dans un premier temps un en-tête :

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Transfer-Encoding: chunked
Expires: -1
Date: Tue, 09 Sep 2014 06:28:36 GMT
Content-Type: text/html; charset=iso-8859-1
Server: Microsoft-IIS/6.0
X-Generated-By: SW-IIS12
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=a2pxamtv35uv4lmep5dicppa; path=/; HttpOnly
Set-Cookie: CSM=Session=981f22a6-8afa-4aba-bd79-3bbd01b78e46&BNPro=;
expires=Fri, 19-Sep-2014 06:28:36 GMT; path=/; HttpOnly
Cache-Control: no-cache
Pragma: no-cache
Content-Encoding: gzip
Vary: Accept-Encoding
```

Nous ne détaillerons pas toutes les informations renvoyées mais seulement les principales. La première ligne indique que la page que nous demandons est disponible. Nous avons ensuite des informations sur le type de contenu, ici du *text/html*, ainsi que l'encodage des caractères utilisé dans la page, ici iso-8859-1. Les données suivantes sont très intéressantes, nous trouvons le type de serveur (Microsoft-IIS) et sa version (6.0). Vient ensuite le langage utilisé pour réaliser les pages, ici ASP.NET. Un dernier élément intéressant est l'envoi d'un cookie de session.

Nous reviendrons sur l'utilisation possible de toutes ces données mais pour le moment concentrons-nous sur la suite de la page. Dans la fenêtre **Follow TCP Stream** de Wireshark la suite de la page n'est pas lisible car une compression « gzip » est activée permettant de limiter la quantité de données transférées entre le serveur et notre navigateur. Pour voir le code source de la page il faut donc utiliser le navigateur. Dans Firefox la combinaison des touches [Ctrl] U permet d'ouvrir une fenêtre avec ce code source.

```
<!DOCTYPE html>
<html id="ctl00_html" xmlns="http://www.w3.org/1999/xhtml" lang="fr">
<head id="ctl00_Head1"><title>
         Editions ENI est &#233;diteur de livres informatique et
vid&#233;os de formation
</title>
```

```
    <a href="https://plus.google.com/112326652557810849753"
rel="publisher"></a>
    <link rel="stylesheet" type="text/css"
href="/Styles/fontface/bundle_62884021E11FF315AD657A74C0FA5C15.css" />
<script type="text/javascript" src="http://www.editions-eni.fr/scripts/
jquery-1.10.2.min.js"></script><script defer type="text/javascript" src="/
scripts/bundle_C91ADA28F43D216E5FEBF02F329BC084.js"></script><meta http-
equiv="Content-Type" content="application/xhtml+xml;charset=iso-8859-1" />
<meta http-equiv="description" content="Editions ENI est éditeur de livres
informatique, supports de cours et de formation, CD-Rom de formation,
formation en ligne accompagnée ou non par un formateur, solution e-learning
MEDIAplus. Vente en ligne." /><meta http-equiv="keywords" content="ENI,
éditions ENI, mediaplus, livres informatique, e-learning, e-learning
bureautique, supports de formation informatique, supports de cours
informatique, livres bureautiques, cd-rom de formation, guides informatique,
ouvrages informatique, autoformation, formations en ligne bureautiques,
formation logiciels microsoft, examen mos, mcas, certification microsoft" />
<meta http-equiv="lang" content="fr" /><meta http-equiv="abstract" content=
"vente en ligne des livres informatique des éditions ENI" /><meta http-
equiv=" publisher" content="Editions ENI" /><meta http-equiv="reply-to"
content="editions@edieni.com" /><meta http-equiv="contactcity"
content="Nantes" /><meta http-equiv="contactzipcode" content="44021" />
<meta http-equiv="contactstate" content="France" /><meta http-equiv=
"identifier-url" content="http://www.editions-eni.fr" /><meta http-equiv=
"copyright" content="Editions ENI" /><meta http-equiv="category"
content="Computing/General" /><meta http-equiv="distribution" content=
"global" /><meta http-equiv="rating" content="general" /><meta http-
equiv="vs_defaultClientScript" content="JavaScript" /><meta http-equiv=
"alexaVerifyID" content="bpVtOKMRHP2TIOOyork9G3gGP-M" /><meta http-equiv=
"Robots" content="Index, Follow" /><meta http-equiv="Cache-Control" content=
"no-cache" /><link rel="shortcut icon" type="image/x-icon" href="http://
www.editions-eni.fr/favicon.ico" /><link rel="canonical" href="http://
www.editions-eni.fr/livres-et-videos/.9a306885eaae816a50aefe4d3d676107.
html" /><script type="text/javascript">
   var RootPath = "http://www.editions-eni.fr/";
   var IdLNG = 1;
   var TypeEspace = 'Livres';
   var StateEspace = 1;
   var RefPartner = '';
</script><script type="text/javascript">
   var plug_inpage_Url = '//www.google-analytics.com/plugins/ga/
inpage_linkid.js';
   var _gaq = _gaq || [];
   _gaq.push(['_require', 'inpage_linkid', plug_inpage_Url]);
   _gaq.push(['_setAccount', 'UA-1499179-1'],
   ['_setSiteSpeedSampleRate', 100]);
   _gaq.push(['_setDomainName', 'www.editions-eni.fr'],
   ['_setCustomVar', 1, 'Espace', 'Livres', 3],
   ['_setCustomVar', 2, 'AccountType', 'NotLogged', 2],
   ['_trackPageview']);
```

```
   (function () {
       var
ga=document.createElement('script');ga.type='text/javascript';ga.async=true;
       ga.src=('https:' == document.location.protocol ? 'https://' :
'http://') +
'stats.g.doubleclick.net/dc.js';
       var s=document.getElementsByTagName('script')[0];
s.parentNode.insertBefore(ga, s);
   })();
</script></head>
<body class="MainBody ColorsBody" onload="">
    <form method="post" action="http://www.editions-eni.fr/Livres_rayon.
aspx?idspace=d9bd8b5e-f324-473f-b1fc-b41b421c950f&amp;idrayon=3a6222cf-b921
-41f5-886c-c989f77ba994&amp;idlng=1&amp;iditf=0" id="aspnetForm">
<div class="aspNetHidden">
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value=
"/wEPDwUKMTY4NjA0MjMyMmRkZfHXjM/kp5hvO5MdzzgsWKdXBuY=" />
</div>
<script type="text/javascript">
```

Nous nous limitons volontairement au début de la page pour ne pas remplir la totalité du livre avec du code HTML, ce qui n'est pas l'objectif. La première ligne de la page est très intéressante car elle informe le navigateur sur le langage utilisé pour décrire la page. Ici le langage de description de page utilisé est du XHTML. Nous constatons aussi que la page contient des fonctions en JavaScript.

Si nous poursuivions la lecture des échanges pour l'affichage de cette page nous constaterions que d'autres requêtes sont nécessaires : la demande de la feuille de style, la demande des images, etc.

1.5 Comment sont réalisées les pages web ?

Comme nous l'avons déjà évoqué, un site web est un ensemble de médias rassemblés de façon cohérente. Les pages disponibles sur un serveur peuvent être statiques ou dynamiques.

Dans le cas de pages statiques, le code HTML/XHTML de la page est simplement enregistré dans un fichier que le serveur se contentera de renvoyer au navigateur à sa demande. Il y a autant de fichiers que de pages consultables. Il en est de même pour les médias. Ce type de site n'est pas simple à maintenir car toute modification entraîne une édition du code de la page. Cette technologie a pratiquement disparu de la surface de l'Internet faisant place aux sites dynamiques. Le seul avantage est qu'un site statique présente bien souvent moins de failles de sécurité qu'un site dynamique.