3TI
Sécurité des réseaux informatiques
2015-2016

La sécurité des réseaux

V. Van den Schrieck

Table des matières

Protocoles et standards de sécurité Internet

- Couche réseau
- Couche transport
- Applications
  - HTTPS
  - Mail
  - DNS
- Authentification sur Internet

Références

Le contenu et les figures de ce slideshow sont principalement tirés de Stallings et Brown, « Computer Security, Principles and Pratice », 3rd edition, Ed. Pearson

Couche réseau

Brainstorming :

Quelles sont les menaces sur/utilisant le protocole IP?

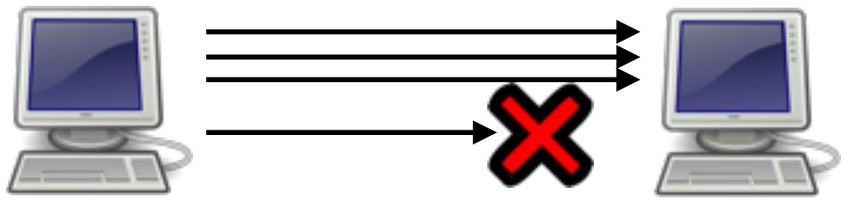
Couche réseau

But initial d'IP : Assurer, avant tout, la disponibilité de la communication

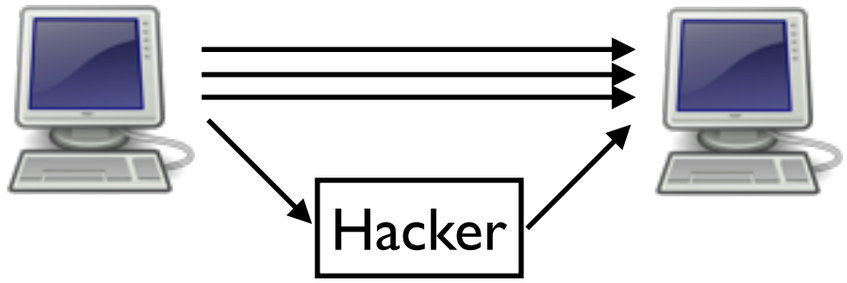
- Confidentialité?
- Intégrité des données?

Couche réseau

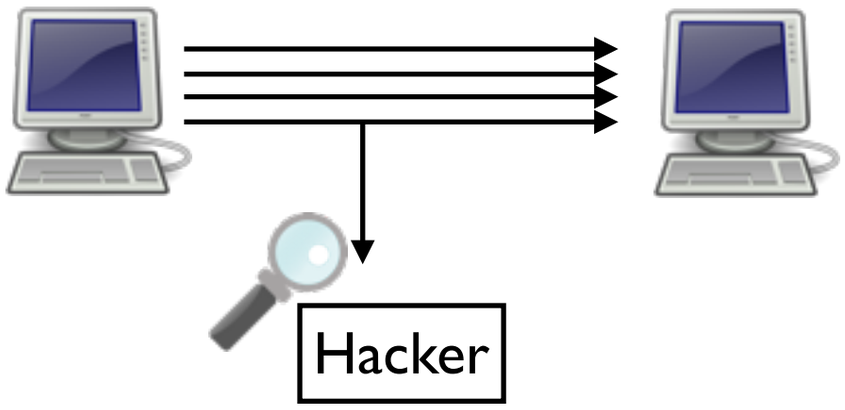
Types d'attaque :



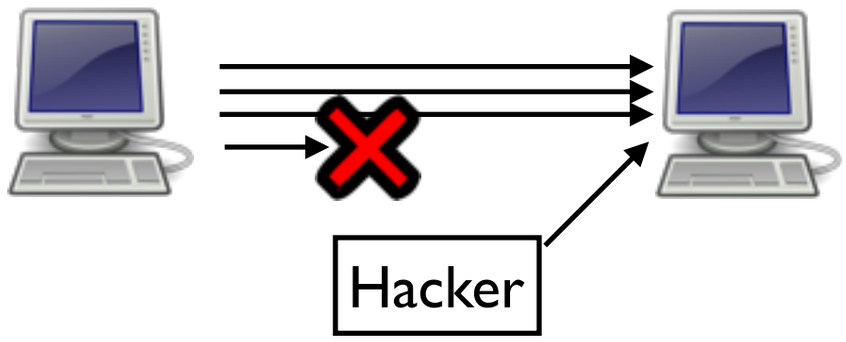
Interruption



Modification
(Man in the Middle)



Interception



Impersonnalisation

Attaques ICMP

- Host Unreachable : Provoque la déconnexion des sessions de la victime
- ICMP Redirect : Permet de dévier les paquets de la victime
- Ping flood
- Ping of Death : `ping -s 65510 <target>`
- Smurf : ping sur une adresse de broadcast avec une IP source spoofée

ARP Poisoning/Spoofing

- Interception, Man-in-the-Middle ou DoS
- Insérer des fausses informations dans les tables ARP pour dévier le trafic
- Gratuitous ARP : Trame ARP de broadcast
- ARP forgée : Trame ARP unicast envoyée à la victime

Attaques sur IP

Attaques sur la fragmentation IP :

- IP Fragment Overlap
- IP Fragmentation Buffer Full
- IP Fragment Overrun
- IP Fragment Too Many Datagrams
- IP Fragment Incomplete Datagram
- IP Fragment Too Small

Couche réseau : Contre-mesures

- Firewall : Filtrer les ICMP
- Valider les adresses sources en sortie du réseau
- Limiter l'usage des broadcast
- ARP : Static ARP, IDS, blocage des ARP gratuits, surveillance
- IP : Chiffrement avec IPSec

IPSec

- IPSec est un ensemble de protocoles permettant le transport de données sécurisées sur un réseau IP
  - Authentification
  - Chiffrement
- Il a été développé pour IPv6, puis adapté à IPv4
- Sécurisation au niveau 3 => utile, entre autres, pour les VPNs

IPSec

2 modes d'utilisation possibles :

- Mode tunnel : la totalité du paquet IP est chiffrée/ authentifiée, puis encapsulée dans un nouveau paquet IP avec une nouvelle en-tête
  - Utilisé pour les VPNs, traverse les NATs
- Mode transport : Uniquement le payload est chiffré/ authentifié. Le routage n'est donc pas impacté.
  - Utilisé d'hôte à hôte, ne traverse pas les NATs avec AH

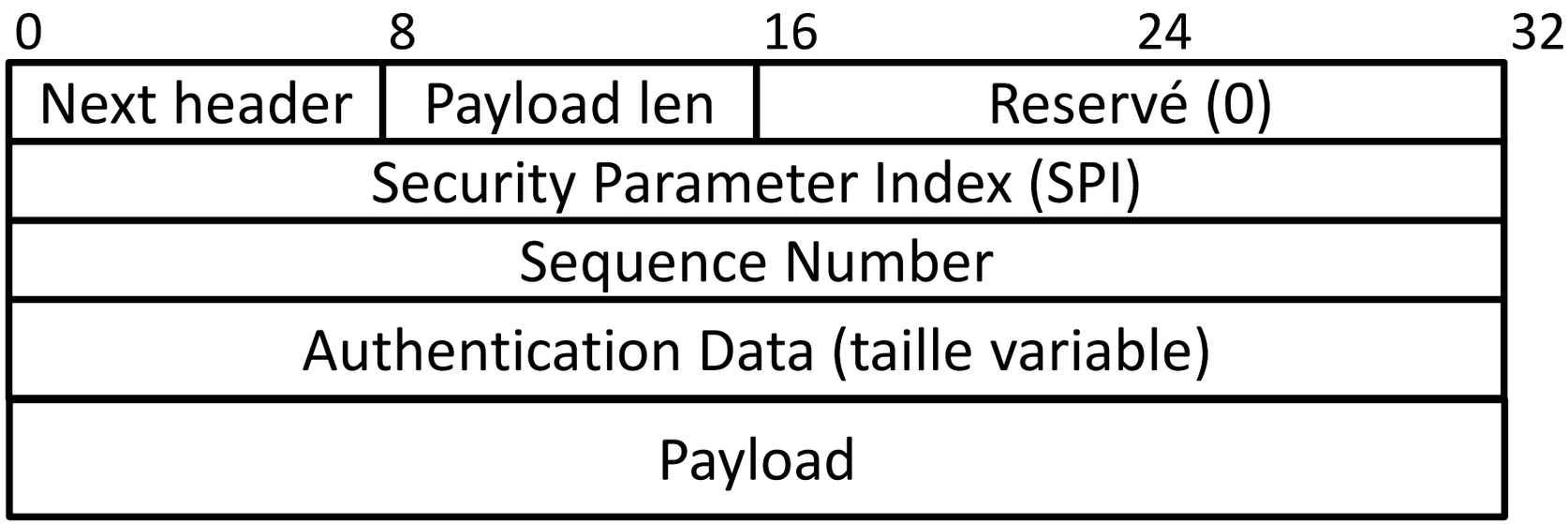
IPSec

Initiation d'une connexion logique IPSec : Security Association

- Authentification et échange de clés : Protocole IKE (Internet Key Exchange)
  - Authentification sur base d'un secret partagé
  - Ou sur base de crypto asymétrique
- Permet l'établissement d'une Security Association, définie par :
  - L'identifiant du protocole de sécurité (AH ou ESP)
  - L'adresse IP source
  - Un identifiant de 32 bits appelé SPI (Security Parameter ID), qui sera réutilisé dans tous les paquets de l'échange

Authentification Header Protocol

- AH garantit l'authentification de la source et l'intégrité des données, mais pas la confidentialité
- Après l'établissement de la SA, un entête AH est inséré entre le payload et l'en-tête du paquet IP

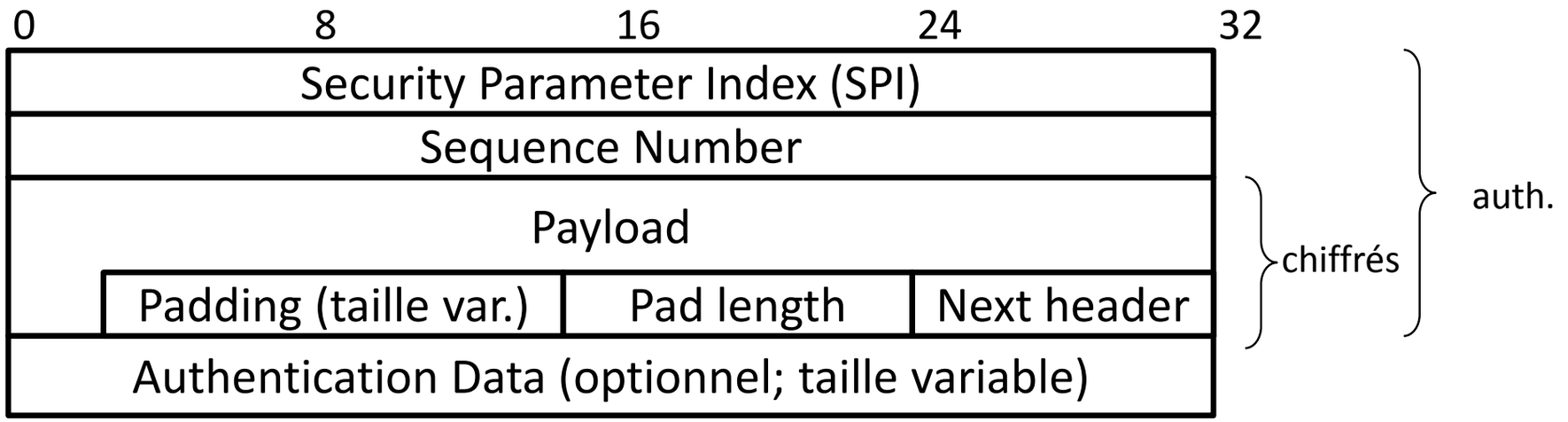


Attention : AH est à présent déprécié

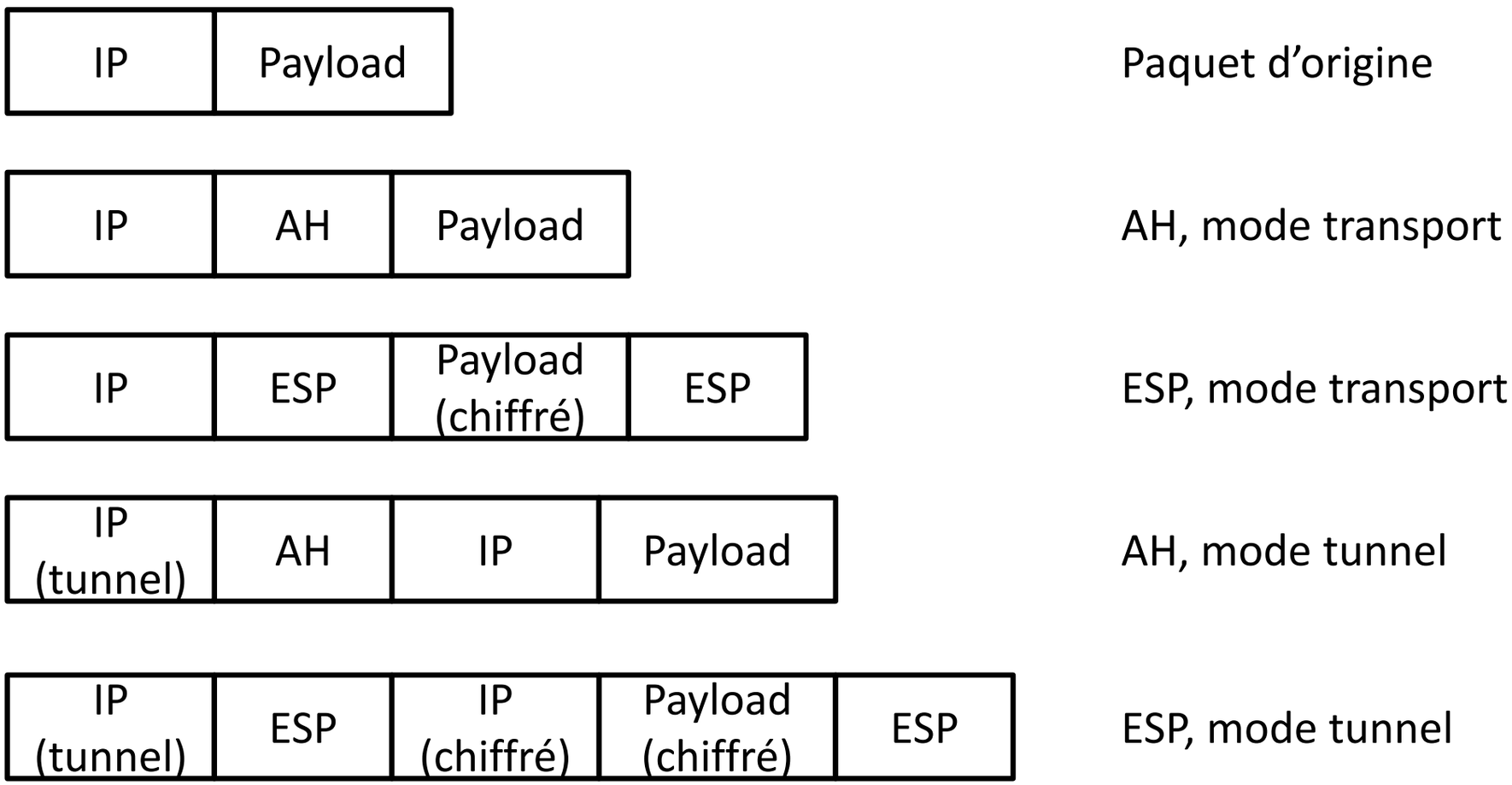
Encapsulating Security Protocol

- Comme AH, l'en-tête ESP s'insère entre l'en-tête et le payload IP. Il y a également un trailer ESP

- Certains champs de l'en-tête sont chiffrés



IPSec : Schémas des paquets



D'après I. Batugowski

Couche transport

Brainstorming :

Quelles sont les menaces sur/utilisant les protocoles de la couche Transport?

Attaques de la couche transport

- UDP Flood
- Land Attack : Adresse/port source idem que celles de destination (1997)
- SYN Flooding : Envoi de SYN spoofés
- Session Flooding : Etablissement d'un grand nombre de connexions TCP pour saturer la table
- TCP Sequence Guessing

Attaques de la couche transport

- Scans de port : Découvrir l'état des services d'un hôte, et/ou OS fingerprinting
  - open, close, drop
  - SYN scan : Ack reçu = service à l'écoute
  - ACK scan :
    - RST reçu : open
    - Pas de réponse ou Host Unreachable : Filtré
  - Aussi : FIN scan, UDP scan, …

Contre-mesures

- Contre le SynFlood :
  - SynCookies
  - IPSec
- Contre les scans : Firewall, IDS
- Sécurisation des connexions TCP : SSL/TLS

Transport Layer Security

- SSL : Netscape, années 90.
  - Plus fiable : Attaque POODLE, sept. 2014
- TLS : Standard IETF, basé sur SSL 3.0 (1996).
  - Actuellement : TLS 2.0, bientôt TLS 3.0
- Objectif : Utiliser TCP pour fournir un service sécurisé de bout-en bout

Architecture TLS

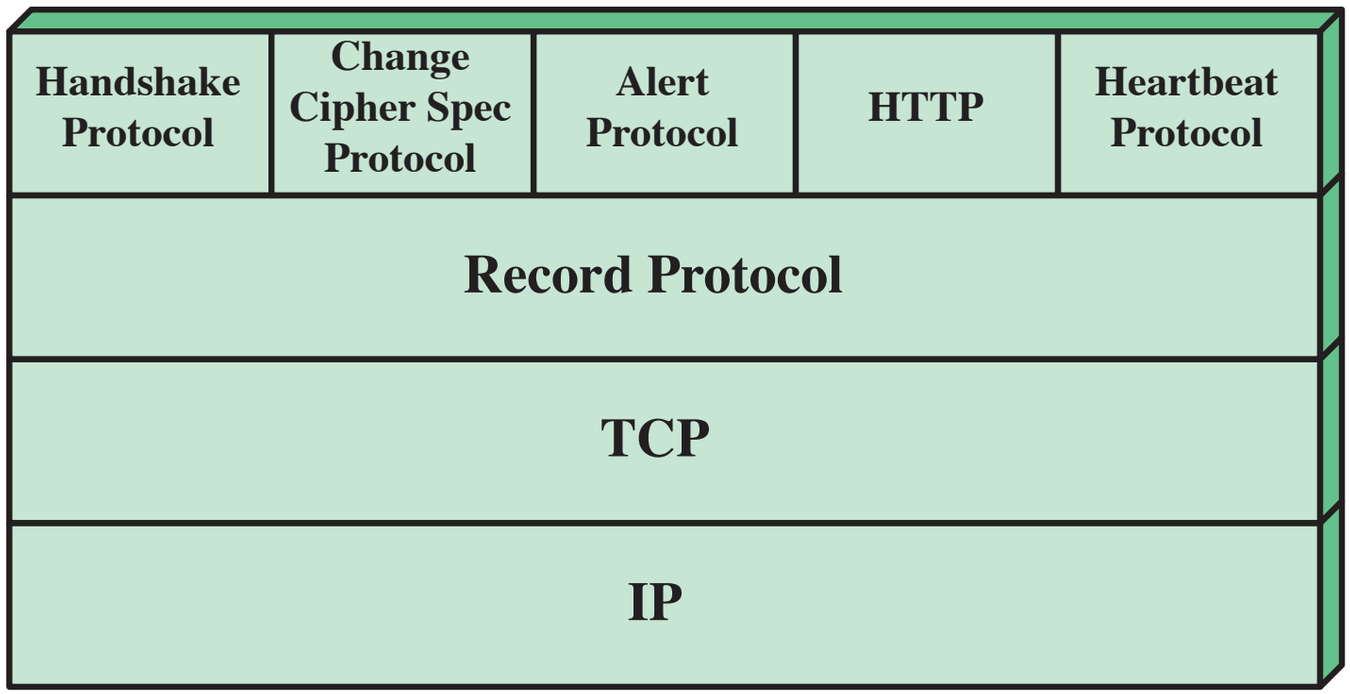


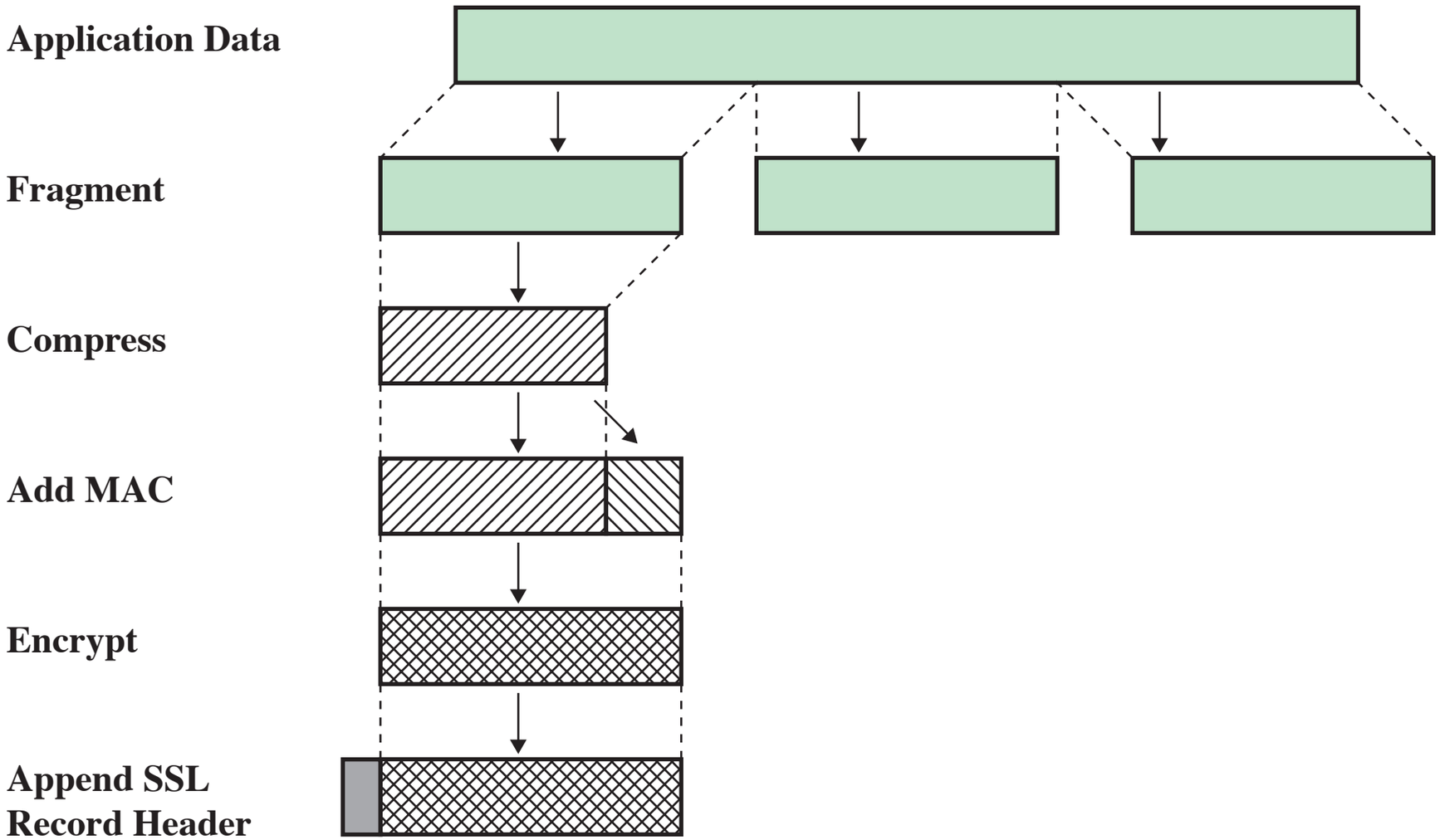
Figure 22.4 SSL/TLS Protocol Stack

TLS : Concepts de base

- **Connexion TLS** : Relation transitoire au niveau de la couche transport qui fournit un type de service. Une connexion est associée à une session
- **Session TLS** : Association entre un client et un serveur. Définit un ensemble de paramètres de sécurité cryptographique qui peuvent être partagés par plusieurs connexions.

Record Protocol

Fournit la confidentialité et l'intégrité des messages



Change Cypher Spec Protocol

- Fonctionne au dessus du Record Protocol
- Un seul message : Contient un octet de valeur 1
- Active la suite de chiffrement utilisée sur la connexion

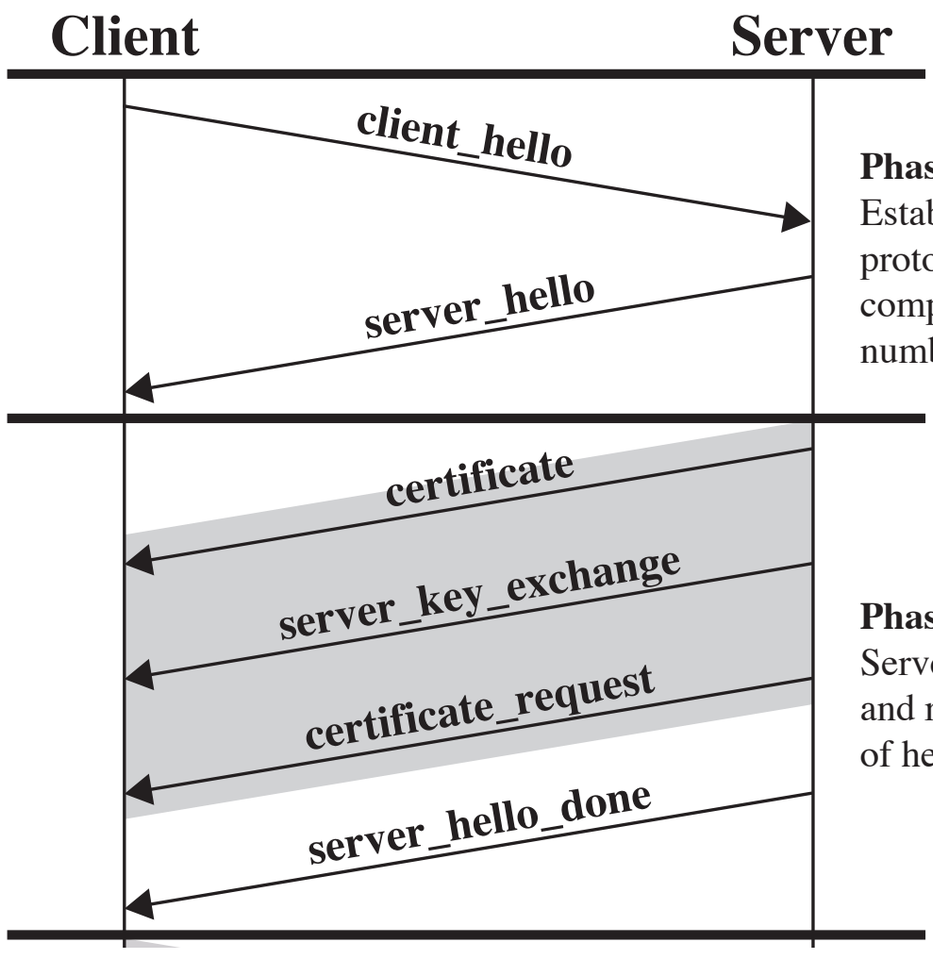
Alert Protocol

- Envoi de notification TLS au pair
- Contient deux octets
  - Le premier prend la valeur 1 (warning) ou 2 (fatal) pour indiquer la sévérité du message
  - Le second contient un code indiquant de quelle alerte il s'agit (ex : MAC incorrect, message close_notify)

Handshake Protocol

- Permet au client et au serveur de s'authentifier, de négocier les algorithmes MAC et de chiffrement, ainsi que les clés de chiffrement
- 4 phases:
  1. Initier la connexion logique et établir les capabilities de sécurité
  2. Le serveur peut envoyer un certificat, initier un échange de clé et demander un certificat au client
  3. Le client vérifie le certificat du serveur, et envoie ses propres informations
  4. Envoi des messages change_cipher_spec, et début de l'échange applicatif

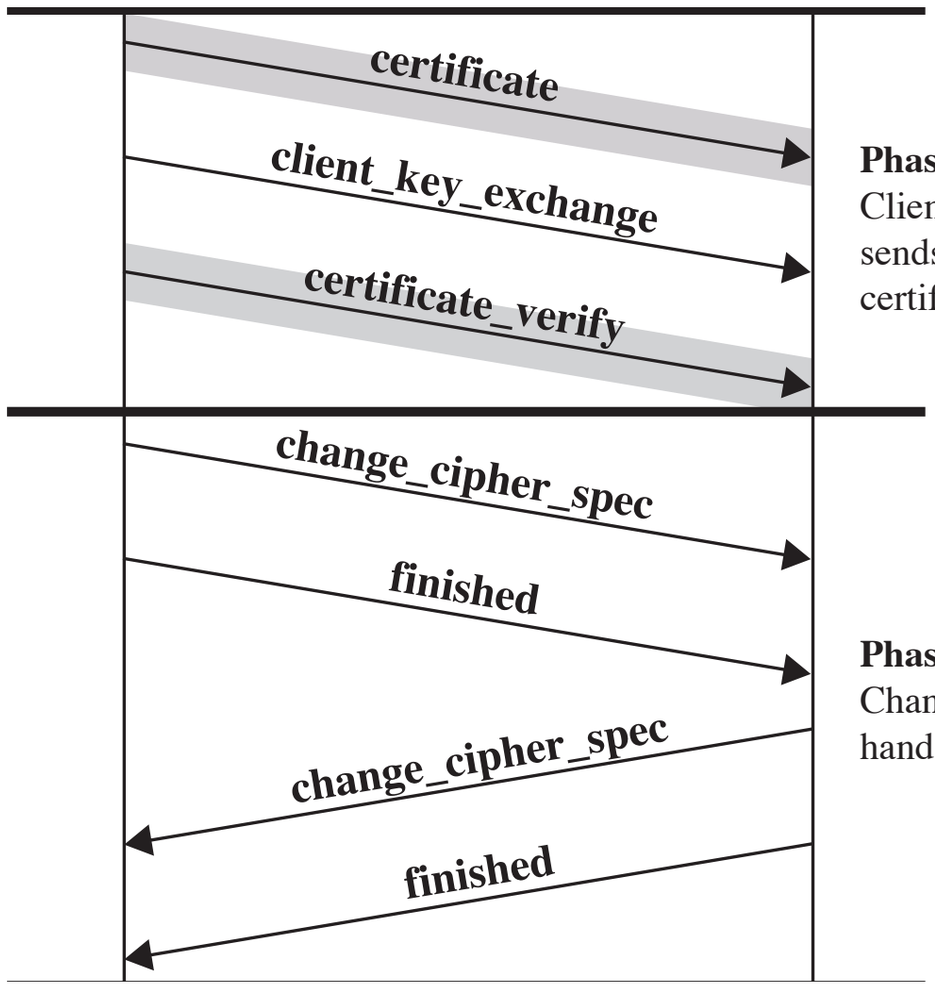
Handshake Protocol



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Handshake Protocol



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Heartbeat Protocol

- Utilisé pour surveiller la disponibilité des entités du protocole
- Défini en 2012 dans la RFC6250
- Deux messages : heartbeat_request et heartbeat_response
- Objectif :
  - S'assurer que le receveur est toujours actif
  - Générer de l'activité pendant les périodes d'inactivité pour éviter les timeouts dans les firewalls

Couche applicative

- Sécurité des applications :
  - Web
  - Mail
  - DNS

HTTPS

- Combinaison de HTTP et de SSL pour créer un canal de communication sécurisé entre un navigateur web et un serveur web.
- Utilisation de https:// et du port 443
- Trois niveaux de connexion :
  - Requête de connexion HTTP
  - Etablissement de session (et d'une ou plusieurs connexions) SSL/TLS
  - Etablissement de la connexion TCP
- Fermeture de connexion : Attention à bien gérer la fin e toutes les connexions

Sécurité DNS

- Attaque 1 : DNS Poisoning
  - Idée : Forcer un serveur DNS à mettre en cache des records malfaisants
    - Initialement : Pas de vérification du lien entre requête et réponse => facilite l'attaque
    - Actuellement, vérification
      - Mais possibilité de forcer des utilisateurs à effectuer la requête (ex : lien dans un email)
      - Ou : Deviner l'identifiant de la requête

Sécurité DNS

- Attaque 2 : DoS
  - Idée : Forcer un serveur à envoyer des réponses DNS vers une machine en envoyant des requêtes utilisant l'adresse IP de la cible comme source
    - Effet d'amplification : Les réponses DNS sont plus grandes que les requêtes.
      - Facteur d'amplification jusqu'à 60

Sécurité DNS

- Sécurisation du DNS : DNSSEC
  - Signature électronique : Authentification de la source des réponses
    - Prévention du cache poisoning
  - Pas de chiffrement
  - En cours de déploiement

Sécurité des emails

Menaces liées aux emails :

- Confidentialité (POP, IMAP et SMTP en clair)
- Intégrité
  - Usurpation d'identité à l'envoi ou durant le transit
- Spam
- Phishing

Un mot sur le spam…

- D'après Wikipedia : « *Le **spam, courriel indésirable** ou **pourriel** (terme recommandé au Québec par l'OQLF) est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.* »

Impact du spam

- Infrastructure : Bande passante et mémoire au niveau des serveurs et des mailboxes
- Productivité :
  - Tri des messages
  - Gartner : Cout du spam jusqu'à 1000$/an/employé
  - Sophos : 92% des emails sont du spam (premier trimestre 2008)
  - Coût global estimé : 100 milliards de dollars/an

Techniques de spam

- Adresse source : Typiquement spoofée
- Open relays
- Ouverture automatique de comptes email
- Botnets
- Collecte d'adresses destination : crawlers, achats, attaques par dictionnaire, hacking, virus/spyware, hoax/chaîne de lettres

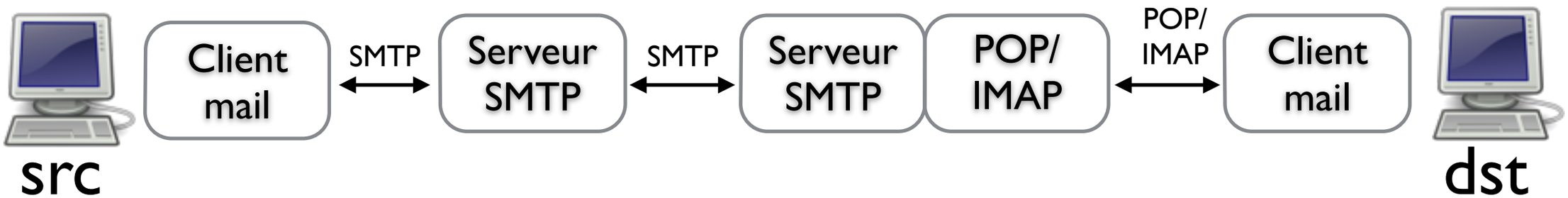
Protection contre le spam

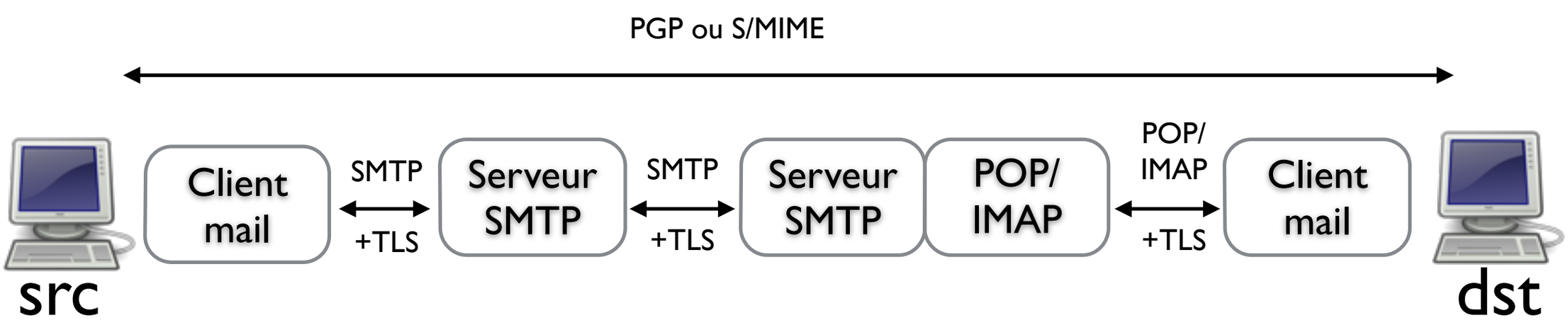
- Filtres :
  - Basés sur le format et sur le contenu du message
  - Attention aux faux positifs/faux négatifs
  - Ex : SpamAssassin
  - White/Black lists
- Législation
  - Plusieurs condamnations de « parrains du spam »

DKIM

- DomainKeys Identified Mail : Spécification permettant la signature cryptographique de messages, **par domaine**
- Protection efficace contre le spam et le phishing

Sécurité des emails

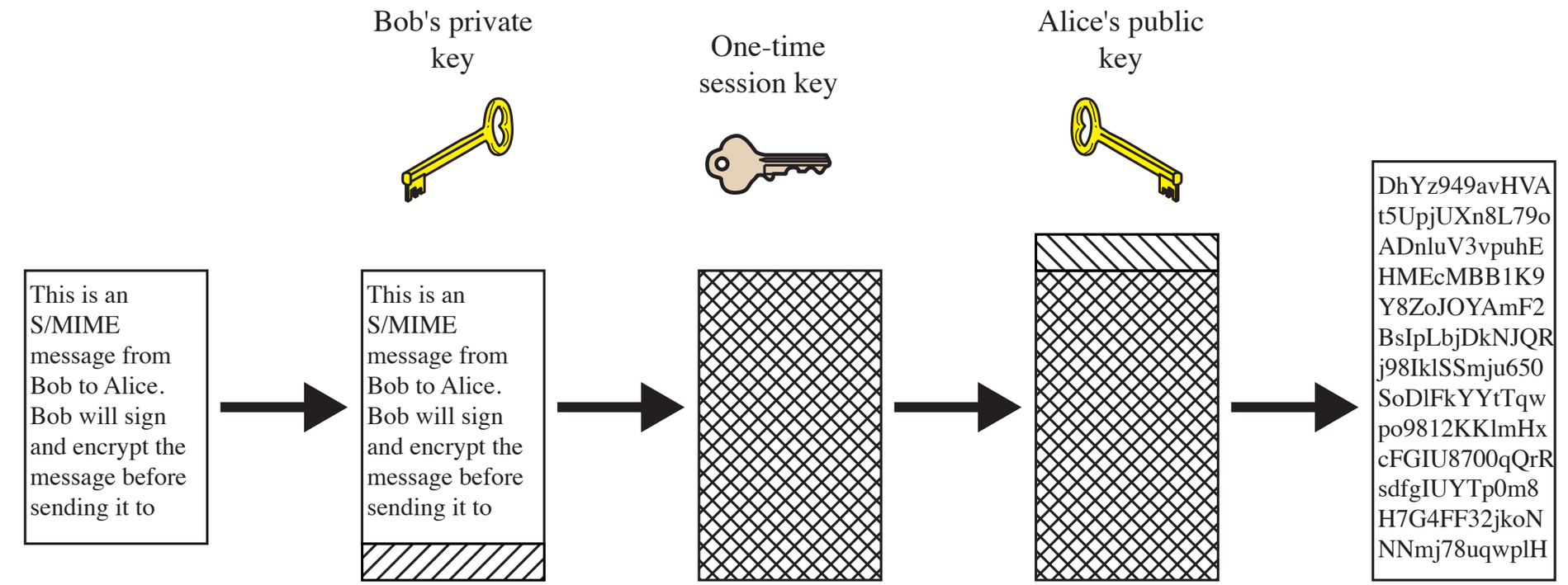




S/MIME

- Content-type MIME supplémentaire : S/MIME
- Fournit la possibilité de signer et ou de chiffrer des messages emails.
- 4 nouvelles fonctions :
  - Données sous enveloppe : Chiffrement
  - Données signées : Signature numérique, message encodé en base64
  - Données signées en clair : Signature numérique, message non encodé
  - Données signées et sous enveloppe
- Utilisation de la cryptographie asymétrique

S/MIME


Bob's private key
One-time session key
Alice's public key
This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to
This is an S/MIME message from Bob to Alice. Bob will sign and encrypt the message before sending it to
DhYz949avHVA
t5UpjUXn8L79o
ADnluV3vpuhE
HMEcMBB1K9
Y8ZoJOYAmF2
BsIpLbjDkNJQR
j98IklSSmju650
SoDlFkYYtTqw
po9812KKlmHx
cFGIU8700qQrR
sdfgIUYTp0m8
H7G4FF32jkoN
NNmj78uqwplH
Plaintext message (unisigned)
Digital signature added (DSS/SHA)
Message with signature encrypted with one-time session key (Triple DES)
Encrypted copy of session key added (El Gamal)
Document converted to Radix-64 format

PGP

- Pretty Good Privacy : Logiciel de cryptographie permettant de garantir la confidentialité et l'authentification des données
- Créé en 1991 par P. Zimmerman
  - Poursuivi par le gouvernement américain pour trafic d'armes…
- Utilisé pour la signature des données et le chiffrement des fichiers, partitions ou emails
- Suit le standard OpenPGP, cryptographie hybride (symétrique et asymétrique)

PGP

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Bonjour,

Blablabla

A bientôt!

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.14 (GNU/Linux)

iEYEARECAAYFAlRyzbEBCgkQ9D35xYOIvivOowCgxrCcDX2+VLk3m84g5SN6kJbG
tuYAoJ3QIevF1wgTqytsaKb09X1mWi2w0
=P8OR
-----END PGP SIGNATURE-----

Table des matières

Protocoles et standards de sécurité Internet

- Couche réseau
- Couche transport
- Applications
  - HTTPS
  - Mail
  - DNS
- **Authentification sur Internet**

Authentification sur Internet

- Pourquoi s'authentifier sur Internet?
- Comment? Quelles sont les moyens disponibles et sont-ils « efficaces » ?

Kerberos

Problème à résoudre : Authentifier des hôtes à travers un réseau non sécurisé

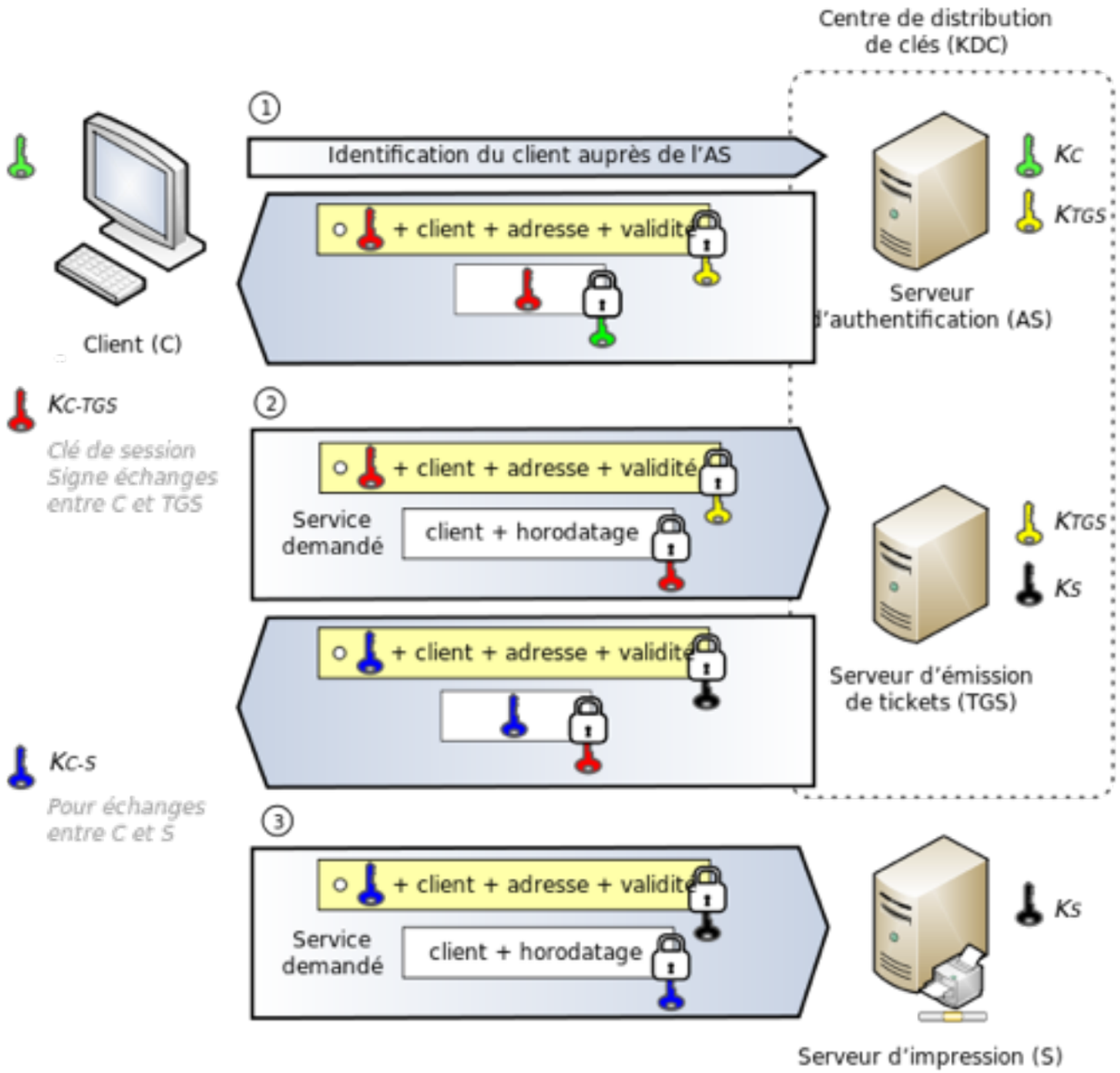
- One-time passwords (digipass, smart cards, …)
- Biométrique
- Logiciel d'authentification lié à un serveur d'authentification sécurisé

Kerberos

Kerberos : Protocole d'authentification réseau

- Authentification de communications client/serveur
- Authentification mutuelle
- Protège contre l'écoute (eavesdropping) et contre les attaques par rejeu
- Utilisation d'un **tiers de confiance** (serveur d'authentification)
- Utilisation de **tickets**

Kerberos : Principes



D'après http://fr.wikipedia.org/wiki/Kerberos_(protocole)

Public-Key Infrastructure

RFC4949 : « Une **infrastructure à clés publiques** ou ***Public Key Infrastructure*** (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériel type HSM ou encore des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) utilisés pour créer, gérer, stocker, distribuer et révoquer des **certificats numériques** sur base de la **cryptographie asymétrique**»

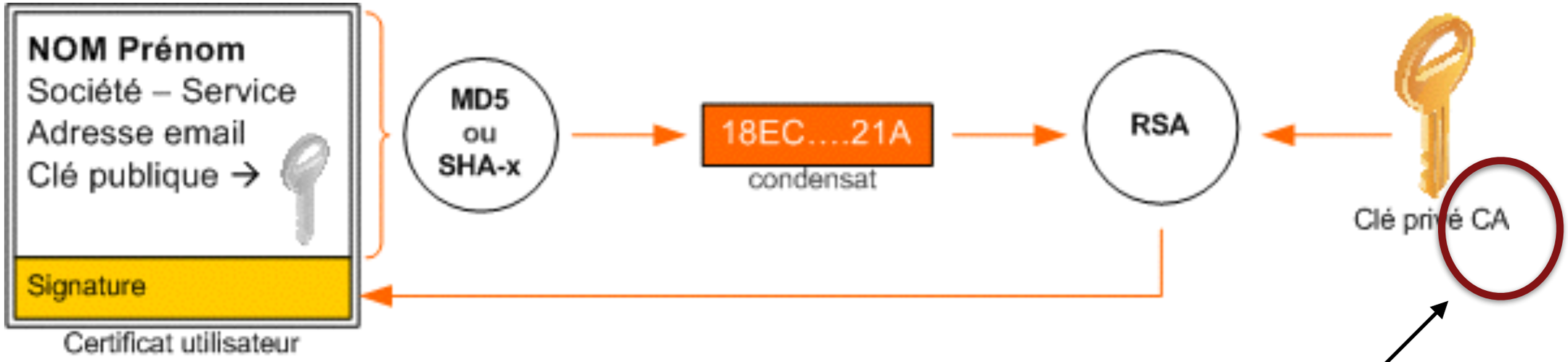
Public Key Infrastructure

Une PKI offre un ensemble de services :

- Enregistrement des utilisateurs ou des équipements
- Génération, publication, renouvellement ou révocation de certificats
- Publication de listes de révocation
- Identification et authentification des utilisateurs

Public Key Infrastructure

Certificat numérique :



Tiers de confiance!

Image d'après : http://fr.wikipedia.org/wiki/Certificat_électronique

Public Key Infrastructure

Les autorités de certification (CA) :

- Mission : Après vérification de l'identité du demandeur, le CA signe, émet et maintient :
  - Les certificats
  - Les listes de révocation
- Les CA doivent également être authentifiés
  - Ils disposent de leurs propres certificats, qui doivent aussi être signés par un CA => Hiérarchie
  - Au sommet de la hiérarchie : Certificats Racine
  - Les certificats racines sont inclus dans les navigateurs/OS

Public Key Infrastructure

Formats de certificat :

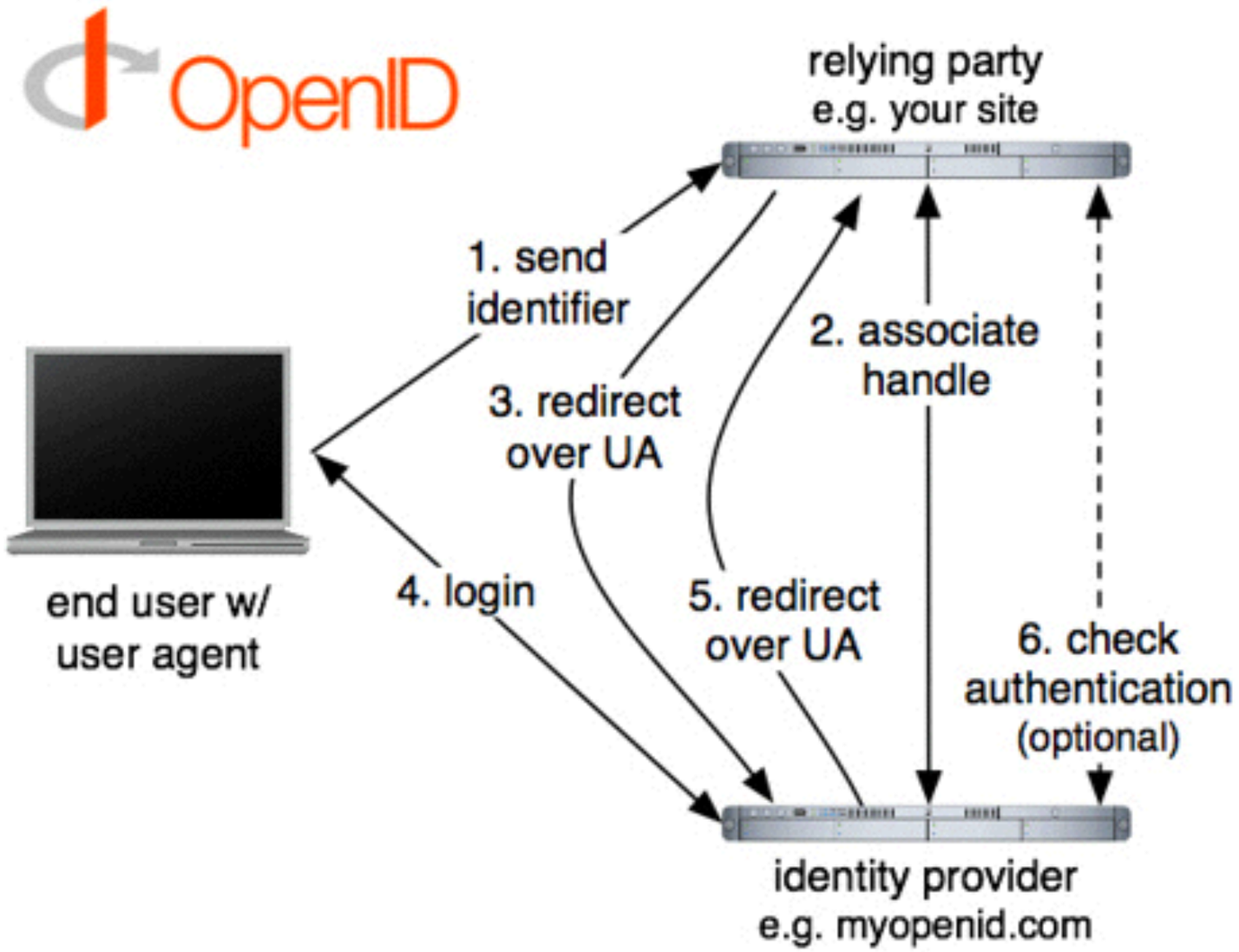
- X.509
- Open PGP

Open ID

Système d'authentification centralisée permettant l'authentification unique

1. Permet, pour un gestionnaire de site web, de déléguer l'authentification auprès d'un fournisseur d'identité, ou OpenID Provider
2. Le site Web et le fournisseur créent un secret partagé
3. L'utilisateur se loge auprès du fournisseur d'identité, et ce dernier lui fournit une preuve cryptographique de l'authentification
4. Le site web peut vérifier l'authentification grâce au secret partagé avec le fournisseur

Open ID



http://www.korben.info/wp-content/uploads/img147.imageshack.us/126/347821691_a13eac9e40.jpg