Sécurité des réseaux

Sidi Biha

SupNum

2023-2024

Plan

Règles

- Présence obligatoire : les absents seront pénalisés!
- les TD et les TP sont notés.
- Il y aura des tests en classe et des tests à domicile.
- Les tests ont une deadline. Les retardataires seront pénalisés.
- Si vous arrivez 10 min après le début du cours, vous ne serez pas autorisé à entrer.

Organisation

- CM : 12 h (8 séances)
- TD : 12 h (8 séances)
- TP : 12 h (8 séances)
- Pour communiquer avec moi : sidi.biha@esp.mr

Plan

- **Rappels et Introduction**
- **Applications réseaux**
- **Sécurité des protocoles réseau**
- **Outils de sécurité réseau**
- **Authentification**
- **Sécurité Web et Email**

Rappels

Propriétés et modèles de menace

- Secret/confidentialité : des données secrètes peuvent-elles être divulguées à un attaquant ?
- Intégrité : le système peut-il être modifié par l'attaquant ?
- Authenticité : avec qui le système communique/interagit-il ?
- Disponibilité : le système est-il toujours en mesure de remplir sa fonction ?
- Nécessité de réfléchir aux modèles de menace (attaquant)

Rappels

Qu'est-ce que la sécurité réseau ?

- Confidentialité : seul l'expéditeur, le destinataire prévu, doit comprendre le contenu du message.
  - Méthode : chiffrer à l'expéditeur, déchiffrer au destinataire.
  - Un protocole qui empêche un adversaire de comprendre le contenu du message est censé assurer la confidentialité.
  - La dissimulation de la quantité ou de la destination de la communication s'appelle la confidentialité du trafic.
- Intégrité du message : l'expéditeur et le destinataire veulent s'assurer que le message n'est pas altéré (en transit ou après) sans détection.
  - Un protocole qui détecte la falsification des messages assure l'intégrité des données.
  - L'adversaire pourrait également transmettre une copie supplémentaire de votre message lors d'une attaque par relecture (replay).
  - Un protocole sécurisé doit détecter la falsification des messages.
  - Un protocole sécurisé les tactiques dilatoires.

Rappels

Qu'est-ce que la sécurité réseau ?

- Authentification : l'expéditeur et le destinataire veulent confirmer l'identité de l'autre.
  - Un protocole qui garantit que vous parlez vraiment à qui vous pensez parler est censé fournir une authentification.
  - Exemple : Attaque DNS [l'URL correcte est convertie en adresse IP malveillante].
- Accès et disponibilité : les services doivent être accessibles et disponibles pour les utilisateurs.
  - Un protocole qui assure un certain degré d'accès est appelé disponibilité.
  - Attaque par déni de service (DoS)/
  - Exemple : attaque SYN Flood (le client ne transmet pas le 3e message dans la poignée de main TCP à 3 voies, consommant ainsi les ressources du serveur).
  - Exemple : Ping Flood (l'attaquant transmet des paquets ICMP Echo Request.

Rappels

Que peut faire un "méchant" ?

- Écoute : intercepter les messages
- Insérer activement des messages dans la connexion
- Usurpation d'identité : peut falsifier (usurper) l'adresse source dans le paquet (ou n'importe quel champ dans le paquet)
- Détournement : "prendre le contrôle" de la connexion en cours en supprimant l'expéditeur ou le destinataire, en s'insérant à sa place
- Déni de service : empêcher l'utilisation du service par d'autres (par exemple, en surchargeant les ressources)

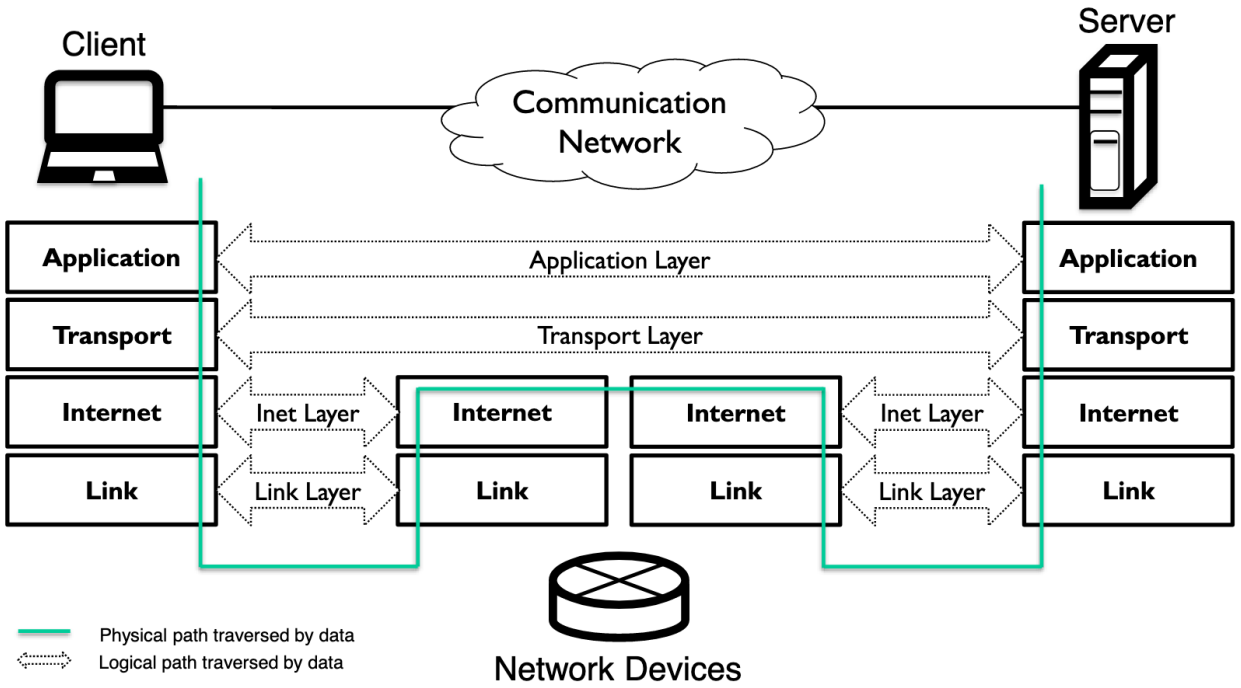
Rappels

Que peut faire un "méchant" ?

- Écoute : intercepter les messages
- Insérer activement des messages dans la connexion
- Usurpation d'identité : peut falsifier (usurper) l'adresse source dans le paquet (ou n'importe quel champ dans le paquet)
- Détournement : "prendre le contrôle" de la connexion en cours en supprimant l'expéditeur ou le destinataire, en s'insérant à sa place
- Déni de service : empêcher l'utilisation du service par d'autres (par exemple, en surchargeant les ressources)

Applications

Problème



- Les applications ont besoin de leurs propres protocoles.
- Les applications sont des protocoles réseau (au sens où elles échangent des messages avec leurs homologues sur d'autres machines).
- Les applications sont des programmes (au sens où elles interagissent avec le système d'exploitation, le système de fichiers et l'utilisateur).

Applications

Quelques applications réseau

- WEB
- Email
- Connexion à distance (ssh, RDP)
- Partage de fichiers (P2P, SMB)
- Jeux en réseau.
- Streaming vidéo (YouTube, Hulu, Netflix)
- Voix sur IP (par exemple, Skype)
- Visioconférence en temps réel (Google Meet)
- Réseaux sociaux
- Recherche

Applications

Création d'une application réseau

- Ecrire des programmes qui :
  - Exécuter sur des machines clients.
  - Communique sur le réseau.
  - Par exemple, un serveur Web (Apache) communique avec un navigateur (Chrome).
  - Pas besoin d'écrire de logiciel pour les périphériques réseau.
- La plupart utilisent le paradigme requête/réponse (les utilisateurs envoient des requêtes aux serveurs, qui répondent ensuite en conséquence).
- Il est important de faire la distinction entre les programmes d'application et les protocoles d'application : HTTP et Firefox, SMTP et Mail.

DNS

Définitions

- Personnes : nombreux identifiants (NNI, nom, passeport).
- Hôtes Internet, routeurs :
  - Adresse IP : utilisée pour l'adressage des datagrammes.
  - Nom : par exemple, www.yahoo.com utilisé par les humains.
- DNS: domain name system
  - Base de données distribuée implémentée avec une hiérarchie de plusieurs serveurs de noms.
  - Protocole de la couche application : les hôtes, les serveurs de noms communiquent pour résoudre les noms (traduction adresse/nom).

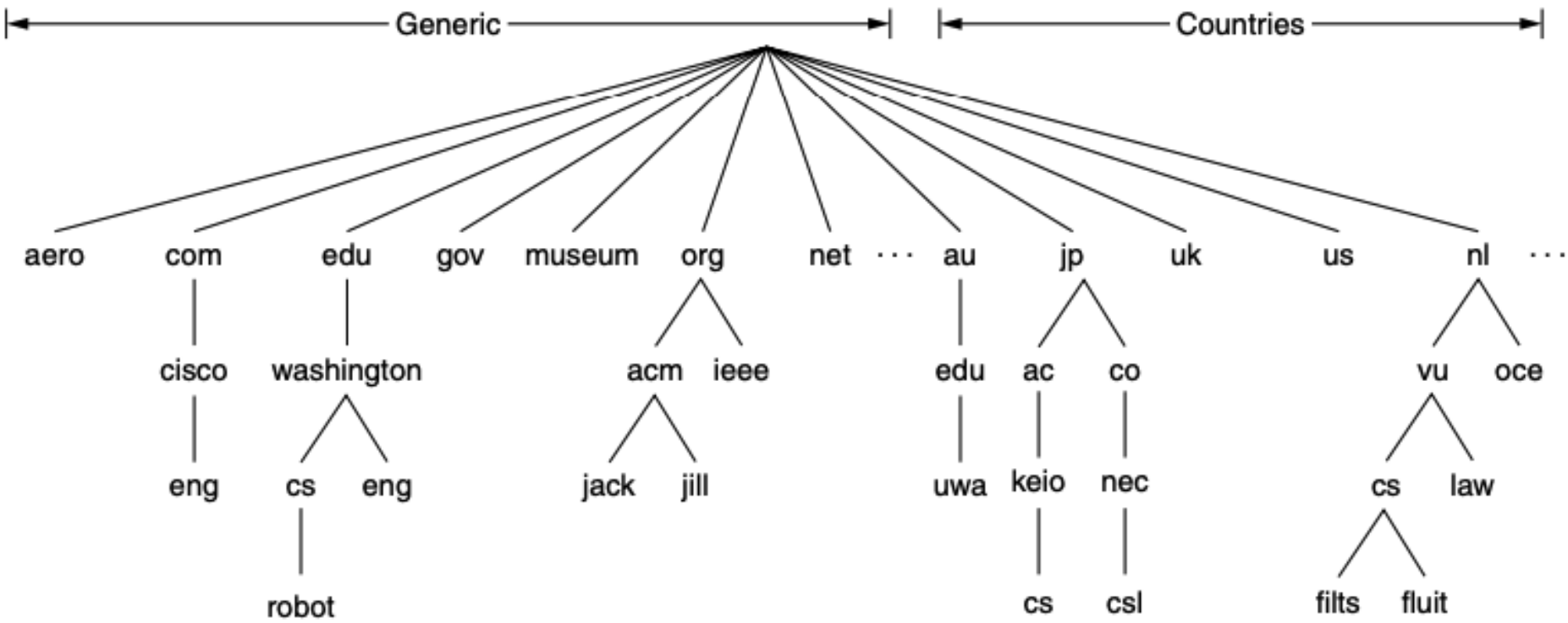
DNS

Services, Structure

- Services:
  - Traduction du nom d'hôte en adresse IP.
  - Alias d'hôte.
  - Alias de serveur de messagerie.
  - Fonctionne sur UDP et utilise le port 53.
  - Répartition de la charge, serveurs Web répliqués : plusieurs adresses IP correspondent à un même nom.
- Pourquoi ne pas centraliser le DNS?
  - Point de défaillance unique.
  - Le volume du traffique.
  - Maintenance.
  - Non évolutif (scale up!).

DNS

Hiérarchique



- Attribué en fonction de l'affiliation de l'institution.
- Racine : contacté par le serveur de noms local qui ne peut pas résoudre le nom.

DNS

Enregistrements/Records

- Base de données distribuée stockant les enregistrements.
- Format: `Domain TTL Class Type Value`

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

DNS

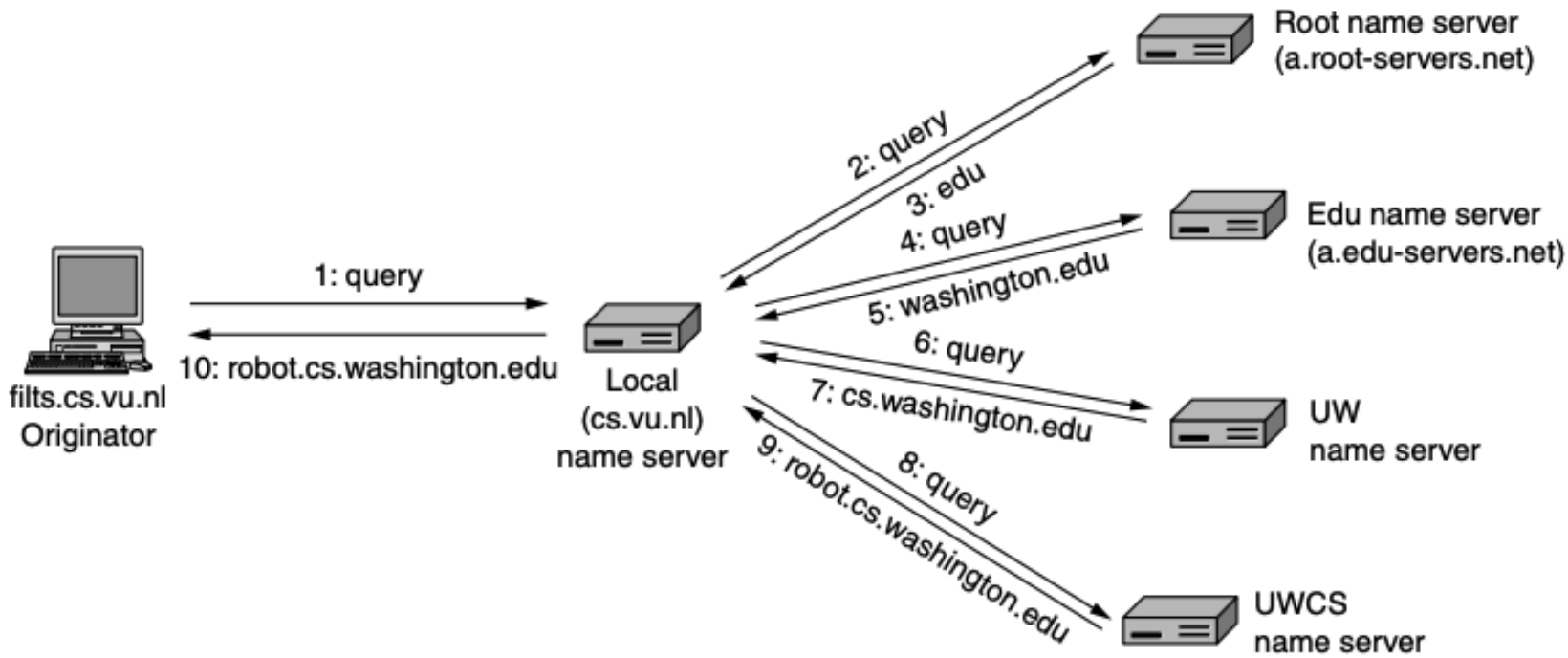
Enregistrements/Records

- Exemples:

cs.vu.nl.	86400	IN	SOA	star boss (9527,7200,7200,241920,86400)
cs.vu.nl.	86400	IN	MX	1 zephyr
cs.vu.nl.	86400	IN	MX	2 top
cs.vu.nl.	86400	IN	NS	star
star	86400	IN	A	130.37.56.205
zephyr	86400	IN	A	130.37.20.10
top	86400	IN	A	130.37.20.11
www	86400	IN	CNAME	star.cs.vu.nl
ftp	86400	IN	CNAME	zephyr.cs.vu.nl
flits	86400	IN	A	130.37.16.112
flits	86400	IN	A	192.31.231.165
flits	86400	IN	MX	1 flits
flits	86400	IN	MX	2 zephyr
flits	86400	IN	MX	3 top

DNS

Résolution



- Requête récursive.
- Chaque FAI (entreprise, université) possède un serveur DNS local.
- Lorsque l'hôte effectue une requête DNS, la requête est envoyée à son serveur DNS local.
- Une fois qu'un serveur de noms apprend le mappage, il le met en cache.

HTTP

Définitions

- HTTP: hypertext transfer protocol.
- Modèle client/serveur
  - Client : navigateur qui demande, reçoit (à l'aide du protocole HTTP) et affiche des objets Web
  - Serveur : envoie (à l'aide du protocole HTTP) des objets en réponse aux requêtes du client.

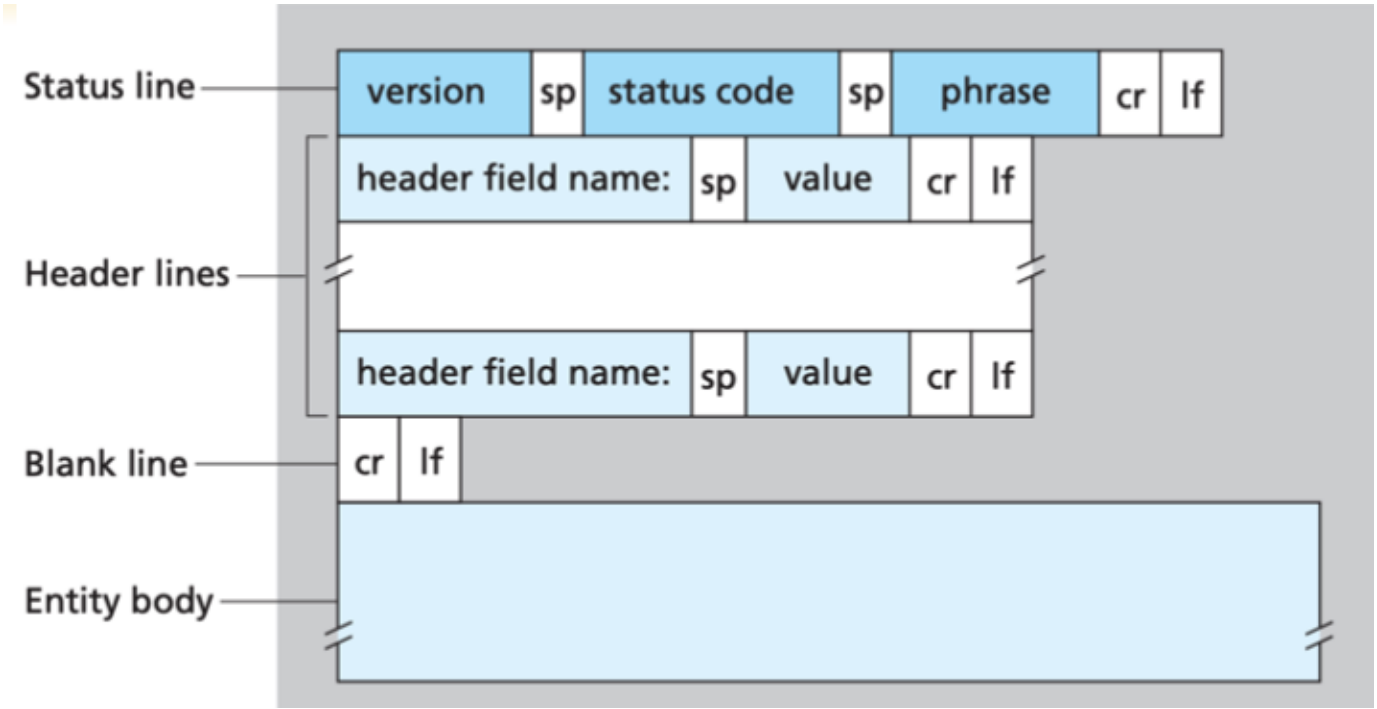
HTTP

Définitions

- Utilise TCP :
  - Le client initie une connexion TCP (crée un socket) au serveur, sur le port 80.
  - Le serveur accepte la connexion TCP du client.
  - Messages HTTP (messages de protocole de couche application) échangés entre le navigateur (client HTTP) et le serveur Web (serveur HTTP).
  - Connexion TCP fermée.
- HTTP est sans état: le serveur ne conserve aucune information sur les demandes passées des clients.
- HTTP est un protocole orienté texte.

HTTP

Message



- HTTP est un protocole de requête/réponse, où chaque message a la forme générale :

```
START_LINE <CRLF>
MESSAGE_HEADER <CRLF> <CRLF>
MESSAGE_BODY <CRLF>
```

HTTP

Requête/Réponse

- Opérations :

Operation	Description
OPTIONS	Request information about available options
GET	Retrieve document identified in URL
HEAD	Retrieve metainformation about document identified in URL
POST	Give information (e.g., annotation) to server
PUT	Store document under specified URL
DELETE	Delete specified URL
TRACE	Loopback request message
CONNECT	For use by proxies

- Réponse codes:

Code	Type	Example Reasons
1xx	Informational	request received, continuing process
2xx	Success	action successfully received, understood, and accepted
3xx	Redirection	further action must be taken to complete the request
4xx	Client Error	request contains bad syntax or cannot be fulfilled
5xx	Server Error	server failed to fulfill an apparently valid request

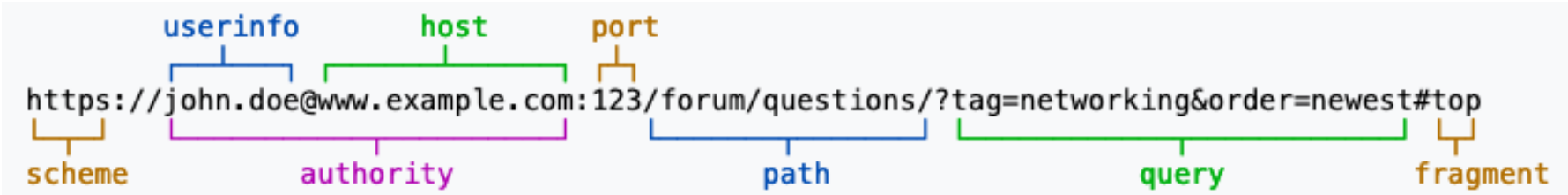
HTTP

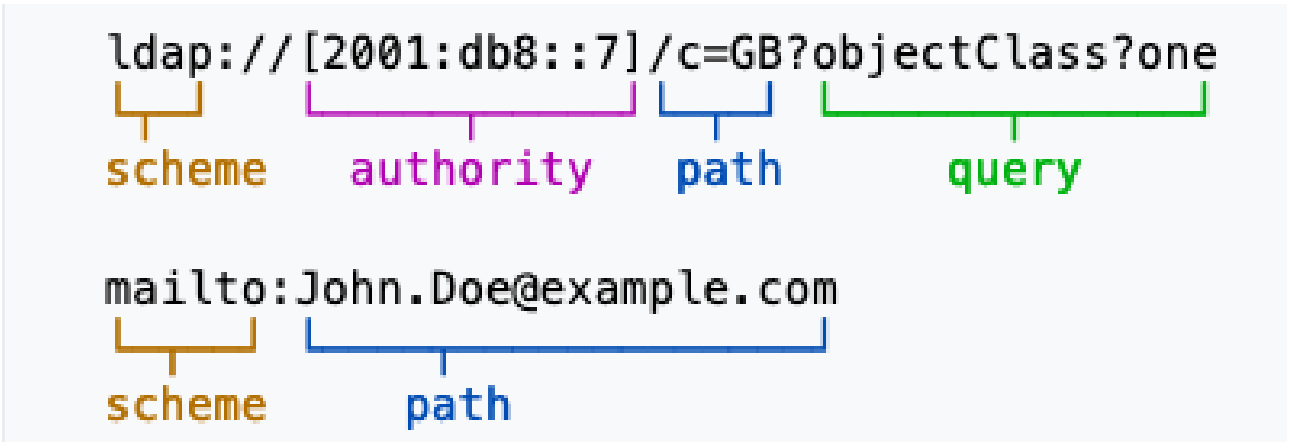
URI

- Uniform Resource Identifiers: Identificateurs de ressources uniformes.
- Utilisées par le HTTP comme adresses.
- Un URI est une chaîne de caractères qui identifie une ressource, où une ressource peut être un document, une image ou un service.
- La première partie d'un URI est un schéma qui nomme une manière particulière d'identifier un certain type de ressource.
- La deuxième partie d'un URI, séparée de la première partie par deux-points, est la partie spécifique au schéma.

HTTP

URI: exemples





HTTP

Cookies

- Ligne d'en-tête dans la réponse HTTP.
- Ligne d'en-tête dans la requête HTTP.
- Fichier conservé sur le système final de l'utilisateur et géré par le navigateur de l'utilisateur.
- Géré par la base de données du site Web.
- A quoi peuvent servir les cookies :
  - Autorisation
  - Paniers (commerce en ligne)
  - Recommandations
  - État de la session utilisateur (e-mail Web)

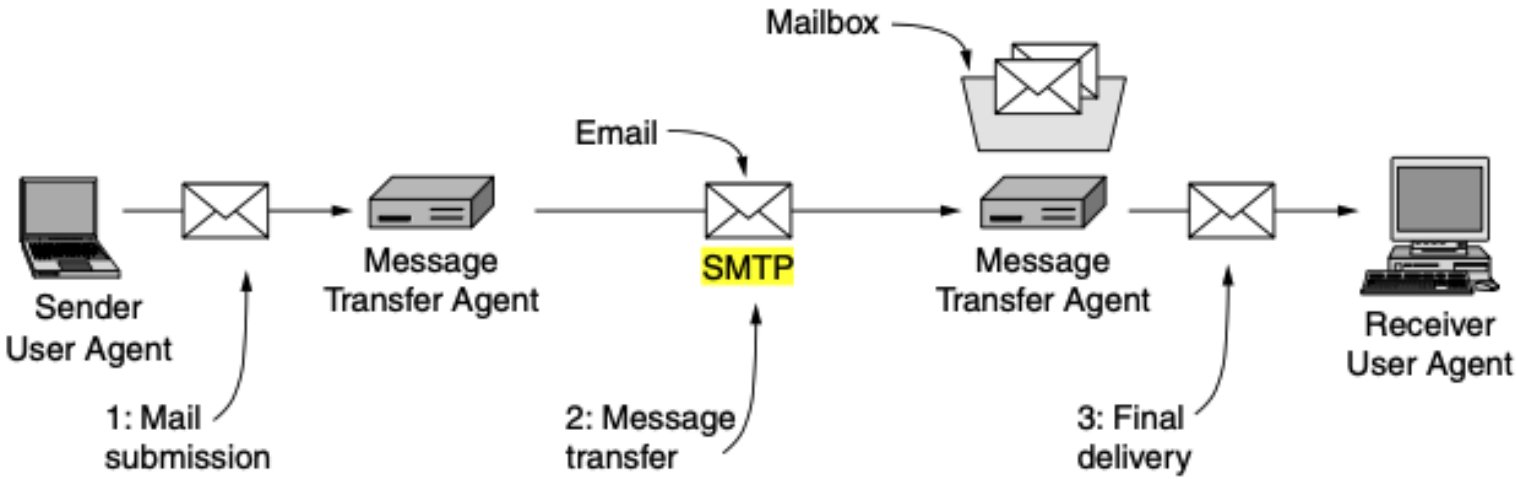
SMTP

Définitions

- Courrier électronique : Courriel/Email
- Trois composants majeurs :
  - Client (User Agent).
  - Serveurs de messagerie
  - Protocole de transfert de courrier simple : SMTP
- User Agent:
  - Lecteur de courrier comme navigateur pour HTTP.
  - Rédiger, éditer, lire des messages électroniques
  - Par exemple, Outlook, Thunderbird, client de messagerie iPhone
  - Messages sortants et entrants stockés sur le serveur
- Protocoles d'accès au courrier :
  - SMTP : livraison/stockage au serveur du destinataire
  - Protocole d'accès au courrier : récupération depuis le serveur
    - POP : Post Office Protocol : autorisation, téléchargement
    - IMAP : Internet Mail Access Protocol : plus de fonctionnalités, y compris la manipulation des messages stockés sur le serveur
    - HTTP : Gmail, Hotmail, Yahoo ! Courrier, etc...

SMTP

Architecture



- Client : machine d'envoi de messagerie.
- Serveur : serveur de réception du courrier.
- Utilise TCP pour transférer de manière fiable le message électronique du client au serveur, port 25.
- Transfert direct : serveur émetteur vers serveur récepteur.
- SMTP (push) vs HTTP (pull)

SNMP

Définitions

- SNMP - Simple Network Management Protocol.
  - Norme de l'industrie pour la surveillance des périphériques réseau.
  - Présent sur la quasi-totalité des équipements réseau.
- Basé sur le principe de Requête/Réponse : GET / SET.
- Hiérarchie arborescente.
- Requête avec les "identificateurs d'objet" (OID): une clé unique (au sein d'un appareil géré) pour une information.
- Concept MIB (Management Information Base) : standard et spécifique au fournisseur (Enterprise).
- Protocole UDP, port 161.
- Différentes versions:
  - V1: publiée en 1988.
  - V2: étend la V1, nouveaux types de données, meilleures méthodes de récupération
  - V3: avec sécurité.

SNMP

Terminologie

- Gestionnaire (le manager en charge de la surveillance).
- Agent (fonctionnant sur l'équipement/serveur).
- Requêtes typiques:
  - Octets In/Out sur une interface, erreurs.
  - Charge CPU.
  - Disponibilité.
  - Température ou autres OID spécifiques au fournisseur.
- Pour les hôtes (serveurs ou postes de travail):
  - Espace disque
  - Logiciels installés
  - Exécution de processus
- Windows et Linux/UNIX ont des agents SNMP

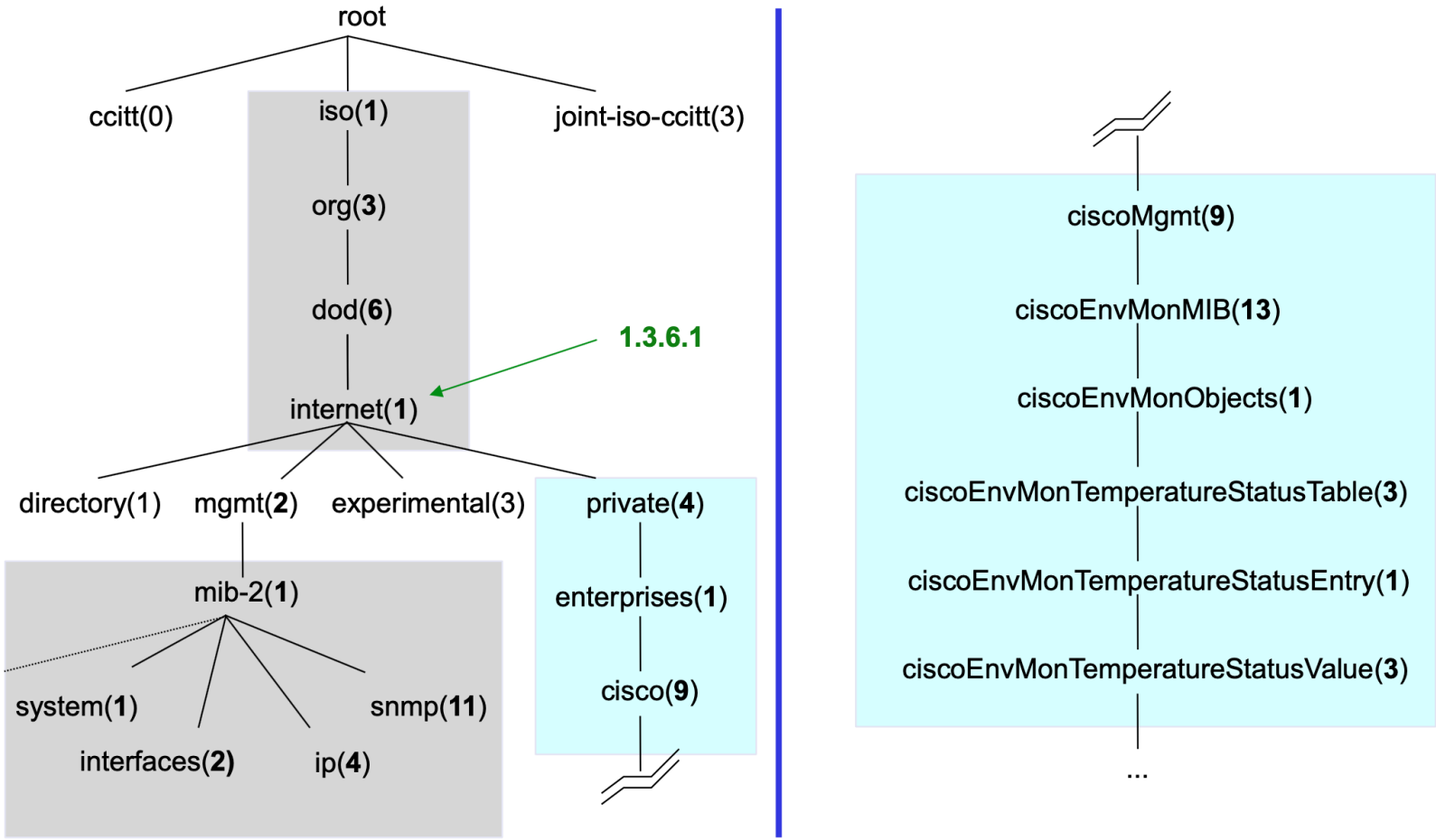
SNMP

Commandes de base

- **GET** (manager vers agent): requête pour une valeur.
- **GET-NEXT** (manager vers agent): Obtenir la valeur suivante (liste de valeurs pour une table).
- **GET-RESPONSE** (agent vers manager): réponse à GET/SET, ou erreur.
- **SET** (manager vers agent): définir une valeur ou effectuer une action.
- **TRAP** (agent vers manager): notification spontanée de l'équipement (ligne en panne, température au-dessus du seuil, ...).

SNMP

Arborescence MIB



- Naviguer dans l'arborescence vers le bas.
- OID séparés par "." : `1.3.6.1.4.1.9. ....`

Partage de fichiers

FTP

- Filte Transfer Protocol : Protocole de communication utilisé pour le transfert de fichiers informatiques d'un serveur vers un client sur un réseau informatique.
- Construit sur une architecture de modèle client-serveur utilisant des connexions de contrôle et de données séparées entre le client et le serveur.
- Les utilisateurs peuvent s'authentifier avec un nom d'utilisateur et un mot de passe, ou de manière anonyme si le serveur le permet.
- Pour une transmission sécurisée qui protège le nom d'utilisateur et le mot de passe et crypte le contenu, FTP est souvent sécurisé avec SSL/TLS (FTPS) ou remplacé par SSH File Transfer Protocol (SFTP).
- Les clients FTP sont généralement intégrés dans les navigateurs Web, où les serveurs de fichiers sont parcourus avec le préfixe URI `ftp://`

Partage de fichiers

SMB

- Server Message Block : protocole de communication.
- Permet le partage de fichiers, le partage d'imprimantes, la navigation sur le réseau et la communication inter-processus sur un réseau informatique.
- Sert de base à l'implémentation du système de fichiers distribués de Microsoft.
- S'appuie sur les protocoles TCP/IP pour le transport.
- Permet le partage de fichiers sur des réseaux complexes et interconnectés, y compris l'Internet public.
- Le composant serveur SMB utilise le port TCP 445.
- Sous Windows, le composant serveur utilise trois ports TCP ou UDP : 137, 138 et 139.

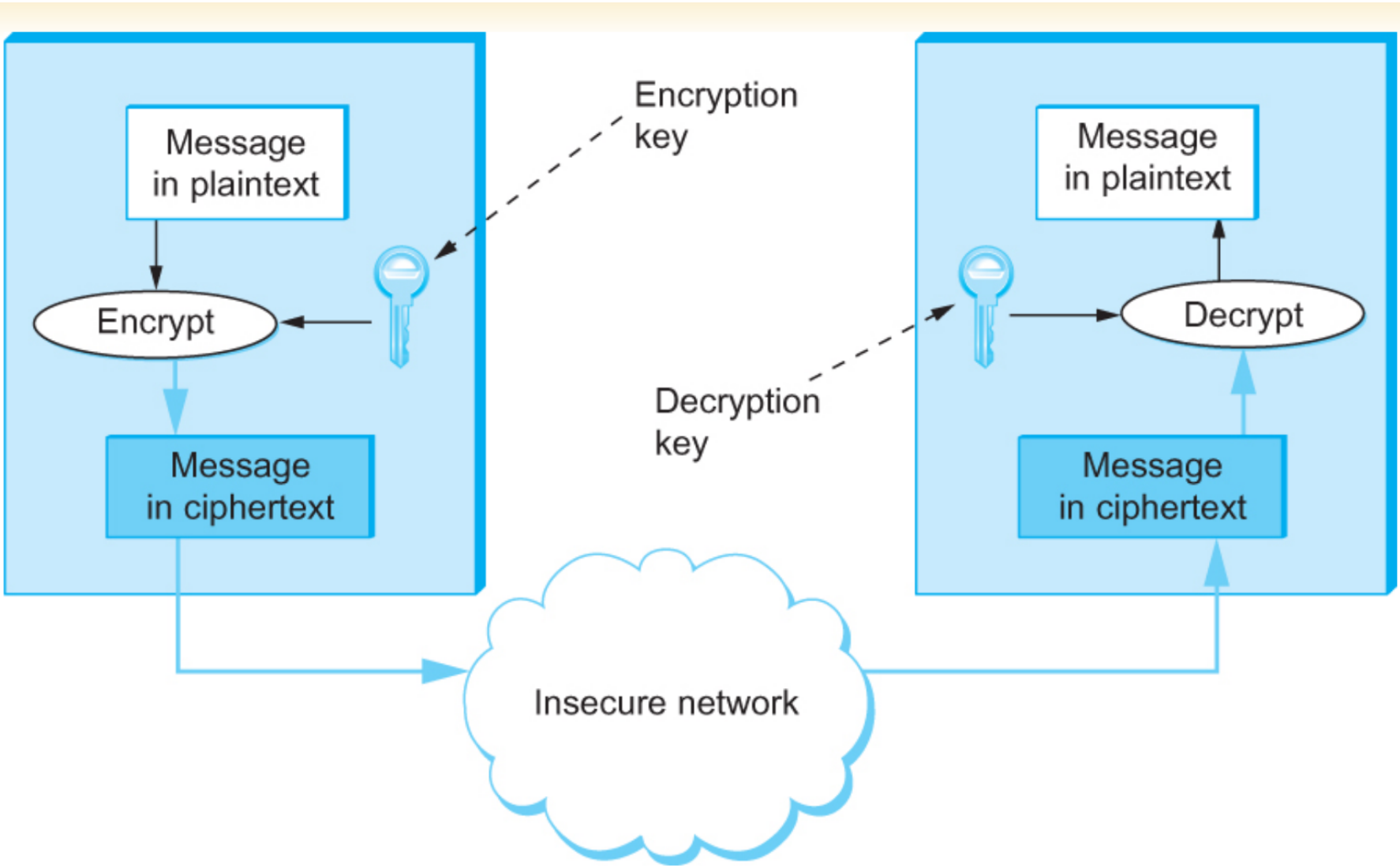
Partage de fichiers

NFS

- Network File System (NFS) un protocole de système de fichiers distribué.
- Permet à un utilisateur sur un ordinateur client d'accéder à des fichiers sur un réseau informatique de la même manière qu'un accès au stockage local.
- Souvent utilisé avec les systèmes d'exploitation Linux/Unix.
- NFS vs SMB :
  - NFS est plus approprié pour les utilisateurs de Linux, tandis que SMB est plus approprié pour les utilisateurs de Windows.
  - NFS est sensible à la casse, tandis que SMB n'est pas sensible à la casse.
  - NFS est plus rapide que SMB lorsque vous lisez ou écrivez plusieurs fichiers de taille moyenne ou petite. NFS est également rapide lors de la navigation.
  - NFS utilise un système de vérification basé sur l'hôte, tandis que SMB utilise un système de vérification basé sur l'utilisateur.

Cryptographie

Principes



Cryptographie

Principes

- Un algorithme cryptographique doit être sécurisé même si tout ce qui concerne le système, à l'exception de la clé, est publique.
- Même si l'adversaire connaît l'algorithme, il devrait être incapable de récupérer le texte en clair tant qu'il ne connaît pas la clé.
- Deux catégories:
  - Chiffrements par substitution.
  - Chiffrements par transposition.

Cryptographie

Catégories

- Chiffrement par substitution :
  - Chaque lettre ou groupe de lettres est remplacé par une autre lettre ou groupe de lettres pour le déguiser.
  - L'un des plus anciens chiffrements connus est le chiffrement de César.
  - Avec cette méthode, a devient D, b devient E, c devient F, . . . , et z devient C.
  - Par exemple:attaque devient DWWDFN.
  - Préservent l'ordre des symboles en clair mais les déguisent.

Cryptographie

Catégories

- Chiffrement par transposition:
  - Réorganise les lettres mais ne les déguise pas.
  - Exemple courant: la transposition en colonnes (voitre Image ci-dessous).
  - Le chiffrement est codé par un mot ou une phrase ne contenant aucune lettre répétée.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

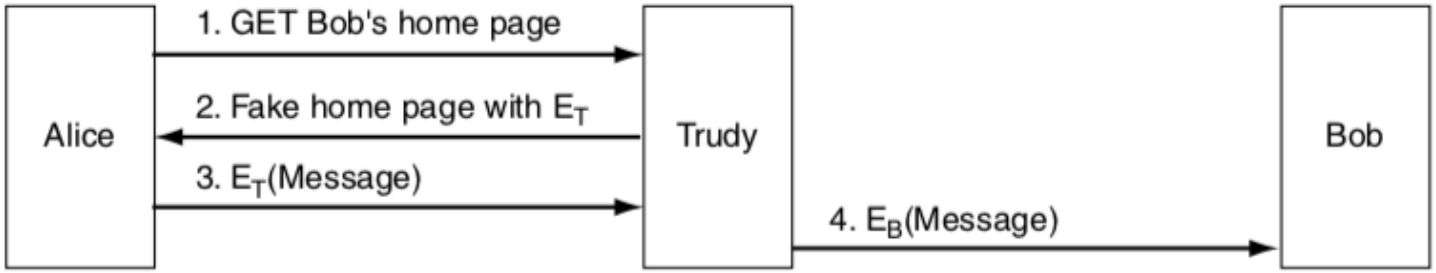
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Cryptographie

Block vs Stream Cipher

- Les chiffrements par blocs traitent les messages en blocs, dont chacun est ensuite chiffré/déchiffré.
  - 64 bits ou plus.
  - Exemple : DES, AES.
- Les chiffrements de flux traitent les messages un peu ou un octet à la fois lors du chiffrement/déchiffrement.
  - Exemple : WEP (utilisé dans 802.11)
- Une attaque par force brute est possible si peu de bits sont choisis.

Gestion des identités : problème



- Attaques de l'homme du milieu (MITM).
- Dans un environnement à clé publique, il est essentiel que vous soyez assuré que la clé publique à laquelle vous chiffrez les données est en fait la clé publique du destinataire prévu et non une falsification.

Certificats

Définition

un document contenant une déclaration certifiée, en particulier quant à la vérité de quelque chose.

- Un justificatif d'identité.
  - Exemples : votre passeport, votre CIN ou votre certificat de naissance.
- Certains certificats, tels que votre passeport, sont une confirmation suffisamment importante de votre identité que vous ne voudriez pas les perdre, de peur que quelqu'un ne les utilise pour se faire passer pour vous.

Certificats numérique

- Un certificat numérique : une donnée numérique qui fonctionne comme un certificat physique.
- Une information incluse dans la clé publique d'une personne/entité qui aide les autres à vérifier qu'une clé est authentique ou valide.
- Utilisés pour contrecarrer les tentatives de substitution de la clé d'une personne par une autre.

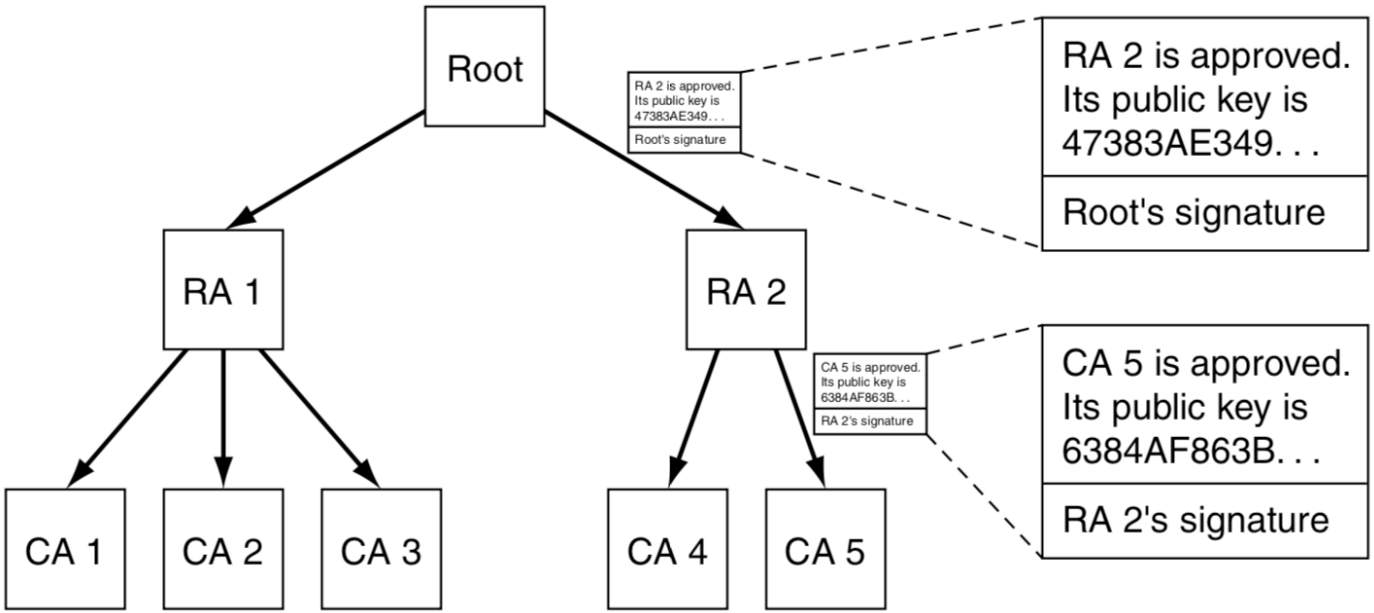
Certificats numérique

- Un certificat numérique se compose de trois éléments:
  - Une clé publique.
  - Informations sur le certificat (Informations d'identité sur l'utilisateur, telles que le nom, l'ID utilisateur, etc...)
  - Une ou plusieurs signatures numériques.
- Le but de la signature numérique sur un certificat est de déclarer que les informations du certificat ont été attestées par une autre personne ou entité.
- La signature numérique n'atteste pas de l'authenticité du certificat dans son ensemble; il atteste uniquement que les informations d'identité signées vont avec ou sont liées à la clé publique.
- Une organisation qui certifie les clés publiques s'appelle CA (*Certification Authority*) ou Autorité de Certification.

PKI : Public Key Infrastructures

- Autorité de Certification : Valide des identités et émet des certificats.
- Une infrastructure de clés publiques ou PKI permet d'organiser le processus de certification des clés publiques.
- Une PKI comprend plusieurs composants :
  - Autorités de certification.
  - Certificats.
  - Utilisateurs.
  - Instructions et procédures.
- Fournit un moyen de structurer ces composants et de définir des normes pour les divers documents et protocoles.

PKI : Hiérarchie



- Organisation hiérarchique des CA.
  - Racine auto-certifiée, supposée de confiance.
  - Chaque niveau inférieur est certifié par le CA du niveau supérieur.
- Clients ont des listes de CA de confiance.

PKI : Vérification

- *Alice* a besoin de la clé publique de *Bob* pour communiquer avec lui.
- Elle cherche et trouve un certificat le contenant, signé par **CA 5**.
- Mais *Alice* n'a jamais entendu parler de **CA 5**.
- Elle pourrait aller à **CA 5** et dire: Prouvez votre légitimité.
- **CA 5** répondra avec le certificat obtenu de **RA 2**, qui contient la clé publique de **CA 5**.
- Désormais armée de la clé publique de **CA 5**, elle peut vérifier que le certificat de *Bob* a bien été signé par **CA 5** et est donc légal.
- La prochaine étape est pour elle de demander à **RA 2** de prouver qu'il est légitime.
- La réponse à sa requête est un certificat signé par la racine et contenant la clé publique de **RA 2**.
- Vu que *Alice* connaît le CA racine, elle est sûre qu'elle a la clé publique de *Bob*.

PKI : Confiance

- Avec des certificats signés, nous pouvons facilement détecter toute tentative de falsification de leur contenu.
- Une chaîne de certificats remontant à la racine est parfois appelée **chaîne de confiance** (*chain of trust*) ou chemin de certification.
- La technique est largement utilisée dans la pratique.
- Problème : qui va administrer la racine.
- Une solution : ne pas avoir une seule racine, mais plusieurs racines.
- Les navigateurs et les systèmes d'exploitation sont préchargés avec les clés publiques pour plus de 100 racines, parfois appelées ancres de confiance.
- De cette façon, il est possible d'éviter d'avoir une seule autorité mondiale de confiance.