Sécurisation des communications

Assurer la sécurité des machines reliées à internet, c'est être sûr de l'identité de la machine distante, sécuriser les échanges et limiter l'accès à certaines données.
Un manque de sécurité expose les données d'une machines à des attaques. Ces attaques peuvent avoir plusieurs buts :

- ➔ **L'interception** qui vise la confidentialité des informations, c'est ce qui garantit aux utilisateurs qu'aucune donnée n'a pu être lue et surtout exploitée.
- ➔ **La fabrication** qui vise l'authenticité des informations, c'est ce qui garantit la provenance et donc la validité des messages reçus.
- ➔ **La modification** qui vise l'intégrité des informations, c'est ce qui permet de s'assurer qu'un message arrivera bien à destination sans avoir été modifié.
- ➔ **L'interruption** qui vise la disponibilité des informations, cette disponibilité peut être vital dans certains cas et un refus de service peut être un problème majeur pour le fonctionnement d'un système (par exemple le système de contrôle du trafic aérien ou des services d'urgence).

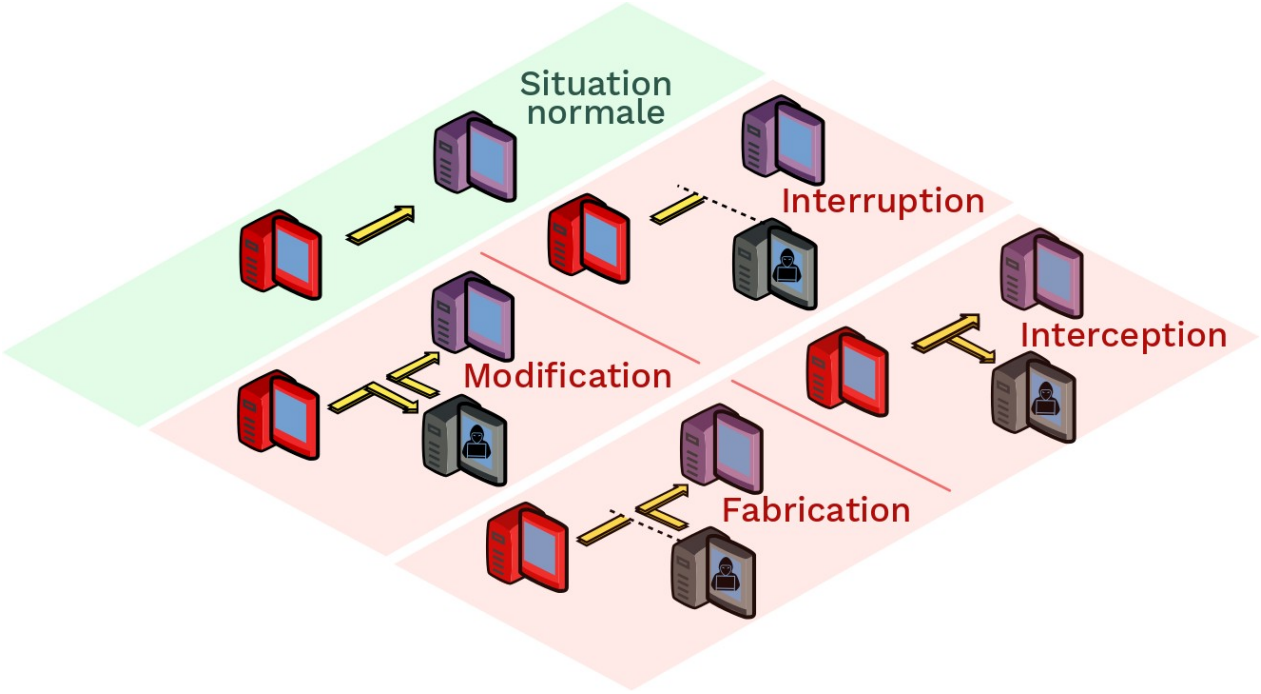

Figure 1: Types d'attaques

1. Sécurisation des échanges

Le principe de base de la sécurisation des échanges consiste à modifier la donnée qui doit être transmise (le chiffrement), de façon à ce que toute personne qui l'intercepterait ne pourrait pas en comprendre le sens. Seul le destinataire va pouvoir retrouver la donnée initiale (le déchiffrement) et la lire.
Les méthodes de chiffrement sont basées sur l'utilisation de clés (chaînes de caractères) qui vont, par l'application d'algorithmes spécialisés, permettre de chiffrer ou déchiffrer des messages.

2.Chiffrement symétriques

Cette technique consiste à définir une clé de chiffrement commune à l'ensemble des interlocuteurs. Cette clé va servir à chiffrer les données lors de leur envoi et de les déchiffrer à leur réception.
Une phase initiale de définition de la clé est nécessaire. Cette clé est ensuite communiquée à tous les ordinateurs susceptibles d'échanger des données.

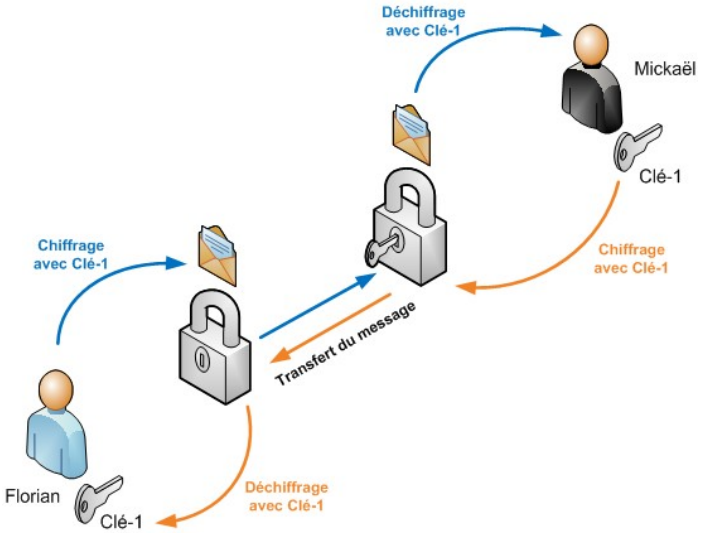

Figure 2: Principe d'un chiffrement symétrique

3.Chiffrement asymétriques

Le principe de chiffrement asymétrique est basé sur l'utilisation de deux clés :
Une clé publique est générée par le client puis diffusée à tous les postes distants
Une clé privée est définie et stockée de manière sécurisée sur le poste client.
Le transport sécurisé des données est ensuite assuré par leur chiffrement ; La clé publique sert à chiffrer et la clé privée est utilisée pour déchiffrer. Ce dispositif nécessite qu'un ordinateur possède les clés publiques de tous les postes susceptibles de lui envoyer un message.

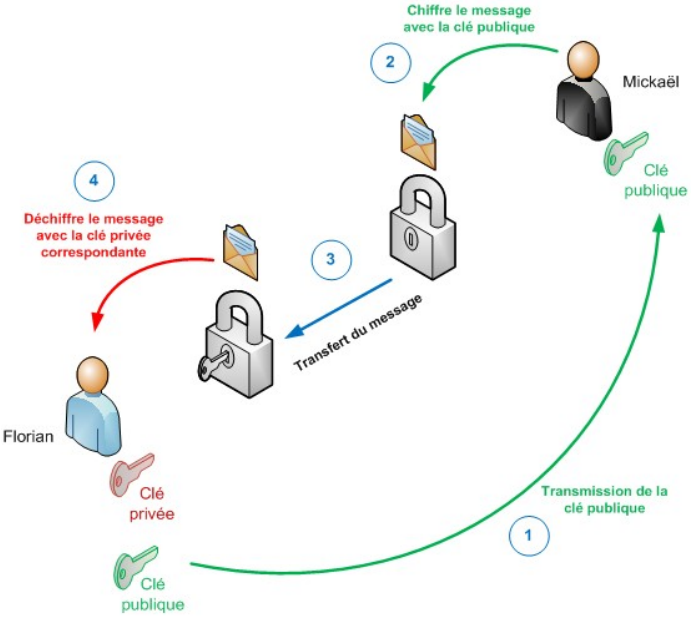

Figure 3: Principe d'un chiffrement asymétrique

4.Le protocole HTTPS

L'échange de données par le protocole HTTP présente plusieurs failles dont les principales sont :

- ➔ les données transitent en clair et peuvent se faire intercepter
- ➔ Un tiers peut se faire passer pour le serveur

Le protocole TLS (évolution du protocole SSL) apporte une couche supplémentaire (couche 5 du modèle OSI) afin de sécuriser les données.

L'association HTTP et TLS porte généralement le nom de HTTPS, ce protocole organise l'ouverture d'une session de la façon suivante :

- ➔ le client envoie une demande de connexion sécurisée. (1)
- ➔ Le serveur envoie alors la clé publique (chiffrement asymétrique) et un certificat d'authenticité. (2)
- ➔ Le client vérifie l'authenticité du certificat auprès d'un organisme de certification extérieur digne de confiance (sorte de notaire). (3 et 4)
- ➔ Après vérification que le serveur n'est pas frauduleux, le client génère une clé de chiffrement symétrique (AES), sa clé de session, et la chiffre avec la clé publique du serveur. (5)
- ➔ Le serveur reçoit la clé symétrique chiffrée et la déchiffre avec sa clé asymétrique.
- ➔ Client et serveur peuvent maintenant s'échanger les données en toute sécurité et rapidement en utilisant la clé de session AES (chiffrement symétrique).

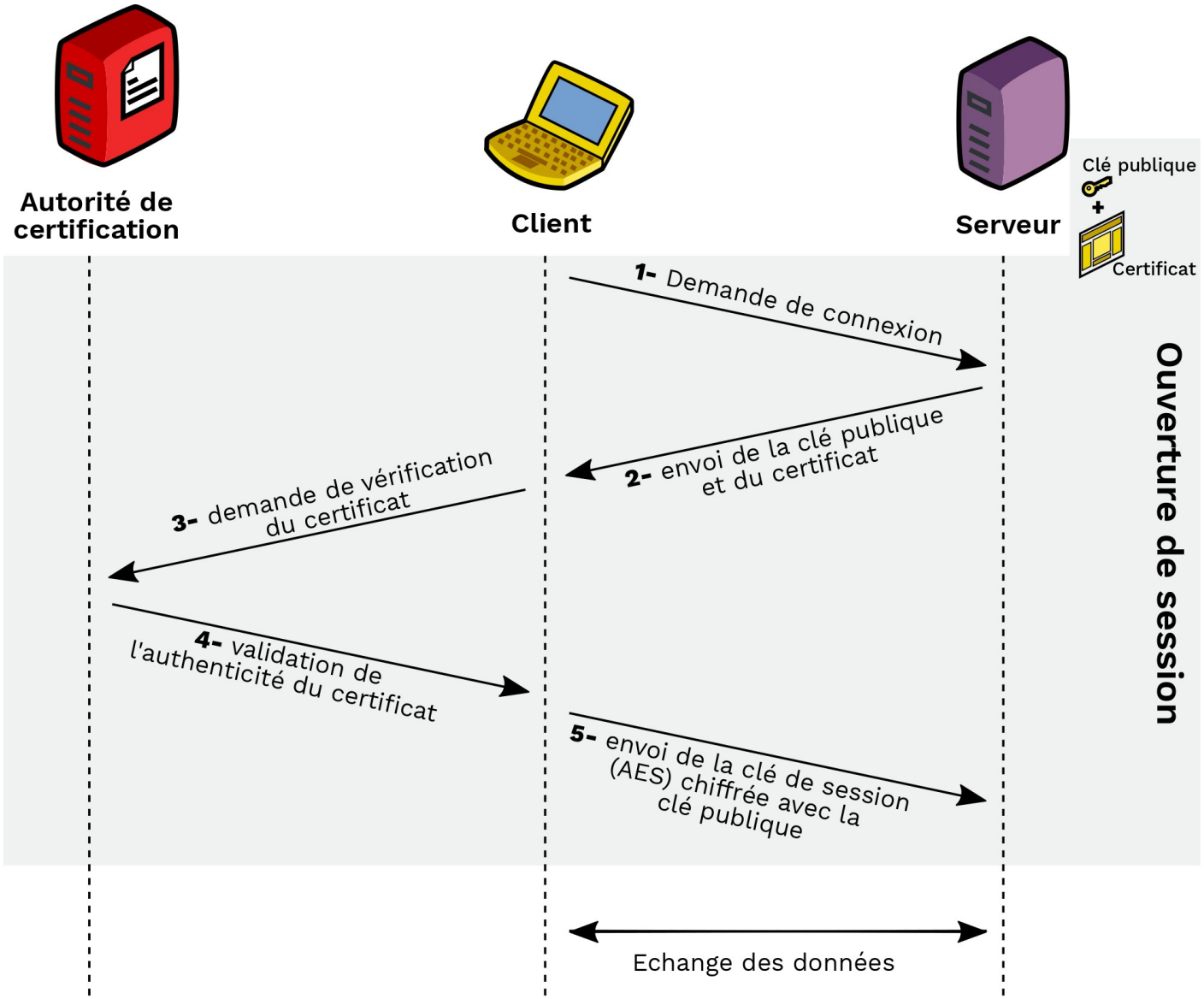

Figure 4: Principe du protocole HTTPS