Exposé sous le thème :

HTTP/HTTPS : Protocole du web et importance de la sécurité

Élaboré par:
Christy Gérys LAMBERT
Donsam Jean Gabard NOEL

INTRODUCTION

Aujourd'hui , chaque clic que nous faisons sur le web déclenche une série d'échanges invisibles entre notre appareil et des serveurs à travers le monde. Mais comment ces échanges fonctionnent-ils? Et surtout comment sont-ils sécurisés? Dans cette présentation, nous allons plonger au cœur des protocoles HTTP et HTTPS, les piliers de la communication sur Internet, nous verrons comment ils permettent aux sites web de nous répondre, et pourquoi la sécurité, grâce au chiffrement, est devenue une exigence incontournable.

DEFINTION DES PROTOCOLES

HTTP

Hyper Text Transfer Protocol

C’est un protocole de transfert hypertexte qui permet à un navigateur d’obtenir des ressources d’un serveur .Il a été conçu pour permettre aux éléments intermédiaires du réseau d'améliorer ou de faciliter la communication entre clients et serveurs.

HTTPS

Hyper Text Transfer Protocol Secure

C’est la version sécurisée de HTTP, qui bloque certains types d’activités des pirates informatiques. Concrètement, ce protocole de transfert hypertexte sécurisé garantit que les informations échangées (formulaires, mots de passe, coordonnées bancaires …) sont chiffrées et protégées des regards extérieurs.

HISTORIQUE

Le protocole HTTP a été créé en 1990 par Tim Berners-Lee et a évolué à travers plusieurs versions majeures : HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2 et HTTP/3. Chaque version a apporté des améliorations en termes de performance, sécurité et fonctionnalités.

Version	Année	Caractéristiques
HTTP/09	1990	Première version très simple, utilisée uniquement pour transférer des fichiers HTML
HTTP/1.0	1996	Introduction des en-têtes HTTP, permettant plus de flexibilité dans les requêtes.
HTTP/1.1	1997	Amélioration des performances avec la persistance des connexions et la gestion du cache.
HTTP/1.2	2015	Multiplexage des requêtes, compression des en-têtes, meilleure efficacité réseau.
HTTP/1.3	2022	Utilise le protocole QUIC basé sur UDP pour réduire la latence et améliorer la sécurité.

HISTORIQUE

Le protocole HTTPS a été introduit en 1994 par Netscape. Il a évolué avec les avancées en cryptographie et les exigences croissantes en matière de sécurité. HTTPS est un standard incontournable pour protéger les données en ligne. Il utilise généralement TLS ou SSL pour chiffrer l'intégralité des communications entre un client et un serveur.

Période	Évènement clé	Détails techniques
1994	Création de SSL 2.0 par Netscape	Première version du protocole de sécurisation des échanges HTTP
1996	SSL 3.0	Amélioration majeure, base de TLS
1999	TLS 1.0 remplace SSL	Standardisation par l'IETF, meilleure sécurité
2006	TLS 1.1	Protection contre certains attaques
2008	TLS 1.2	Support des algorithmes modernes
2010s	Adoption massive de HTTPS	Navigateurs maquent les sites HTTP comme 'non-sécurisés'
2016	Lancement de Let's Encrypt	Certificats SSL gratuits et automatisés
2018	TLS 1.3	Chiffrement plus rapide, suppression des algorithmes obsolètes
2020s	HTTPS devient la norme universelle	La majorité du trafic web est chiffré, intégration dans les plateformes cloud et mobiles

SSL (Secure Sockets Layer) est un protocole de sécurité qui permet de chiffrer les communications sur Internet, garantissant la confidentialité, l'intégrité et l'authentification des données échangées. Il est le précurseur de TLS (Transport Layer Security), qui est aujourd'hui le standard moderne.

TLS (Transport Layer Security) est le protocole de sécurité qui protège les communications sur Internet. Il a remplacé SSL et est aujourd'hui la norme pour sécuriser les sites web, les emails, les applications bancaires et bien plus.

FONCTIONNEMENT

HTTP : l'envoie des données est vulnérable aux interceptions

HTTPS : établit une connexion chiffrée via SSL/TLS avant l'échange de données.

Le certificat **SSL/TLS** est l'élément-clé qui rend la connexion **HTTPS** sécurisée. Délivré par une autorité de certification (comme Let's Encrypt, Sectigo, etc.), ce certificat authentifie le site web et chiffre les échanges entre le serveur et le navigateur.

Concrètement

- ✓ Quand un internaute arrive sur un site HTTPS, son navigateur demande au serveur de s'authentifier.
- ✓ Le serveur envoie son certificat SSL/TLS, qui contient une clé publique.
- ✓ Le navigateur vérifie l'authenticité du certificat.
- ✓ Si tout est valide, une connexion chiffrée s'établit (protocole TLS), garantissant que personne ne pourra lire les données échangées.
- ✓ Sans ce certificat, le site ne peut pas proposer de HTTPS.

Le protocole SSL a été remplacé par TLS, plus moderne et plus sécurisé, mais on continue souvent à parler de "certificat SSL" par habitude.

Le port de communication diffère HTTP utilise le port 80 par défaut, HTTPS utilise le port 443.

L'indication visuelle dans le navigateur affiche un cadenas fermé vert/gris pour HTTPS contre un avertissement « non sécurisé » pour HTTP.

La configuration serveur est plus complexe pour HTTPS nécessitant l'installation et la gestion de certificats SSL/TLS.

Le coût des certificats varie selon le type et le fournisseur,bien que des options gratuites existent (Let's Encrypt).

Types de certificats

Les certificats **DV(Domain Validated)** vérifient uniquement la propriété du domaine ,offrant un niveau de validation basique.

Les certificats **OV(Organization Validated)** confirment l'existence légale de l'organisation en plus de la propriété du domaine.

Les certificats **EV(Extended Validation)** nécessitent une validation approfondie de l'identité organisationnelle et affichent le nom dans la barre d'adresse.

Les certificats **wilcard** protègent un domaine principal et tous ses sous-domaines avec un seul certificat.

Les certificats **multi-domaine**s sécurisent plusieurs domaines différents dans un certificat unique pour simplifier la gestion.

Conclusion

HTTP a permis l'essor du web en facilitant la communication entre serveur et navigateurs, mais il reste vulnérable car les données y circulent en clair.

HTTPS, est devenu la norme incontournable grâce au chiffrement TLS et aux certificats numériques, permettant de garantir la confidentialité, l'authenticité et l'integrité des échanges.

Dans un monde où les cyberattaques se multiplient, adopter HTTPS n'est plus une option, mais une responsabilité pour toute organisation qui publie sur le web.

Références

https://developer.mozilla.org/fr/docs/Web/HTTP

https://developer.mozilla.org/fr/search?q=HTTPS

https://aws.amazon.com/fr/compare/the-difference-between-https-and-http/

https://en.wikipedia.org/wiki/HTTP

https://en.wikipedia.org/wiki/HTTPS