Le Cadenas Numérique : TLS/SSL et Cybersécurité

Roxina Fmnd

Introduction : le cadenas numérique

Le petit cadenas dans la barre d’adresse

Symbole universel de sécurité

Mais que protège-t-il vraiment ?

Programme :

- Décryptage du cadenas
- Identification de la menace
- Technologie protectrice et évolution
- Recommandations des experts

Abréviations utilisées

- HTTPS : HyperText Transfer Protocol Secure → protocole HTTP sécurisé par chiffrement
- HTTP : HyperText Transfer Protocol → protocole de communication web classique
- TLS : Transport Layer Security → protocole de sécurité remplaçant SSL
- SSL : Secure Sockets Layer → ancien protocole de sécurité, obsolète
- MitM : Man in the Middle → attaque de l'homme du milieu
- PFS : Perfect Forward Secrecy → confidentialité persistante

HTTPS : Qu’est-ce que ça signifie ?

HTTPS = version sécurisée de HTTP

Le “S” = Secure → chiffrement des données sensibles

- Mots de passe
- Numéros de carte bancaire

Protection contre l’espionnage numérique

Les certificats HTTP/HTTPS

Lorsqu’un site utilise HTTPS au lieu de HTTP, il repose sur le protocole TLS qui chiffre les échanges entre le client et le serveur. Pour garantir la confiance, ce protocole utilise un certificat numérique.

Qu’est-ce qu’un certificat numérique ?

- Fichier électronique délivré par une Autorité de Certification (CA)
- Associe la clé publique d’un serveur à son identité
- Signé numériquement par la CA pour prouver son authenticité

Rôle d’un certificat HTTPS

Types de certificats

- DV (Domain Validation) : vérifie le domaine seulement
- OV (Organization Validation) : inclut la validation de l’organisation
- EV (Extended Validation) : validation poussée, affichait le nom de l’entreprise dans la barre d’adresse

Cycle de vie d’un certificat

1. Génération d’une clé privée et d’une CSR
2. Validation par l’Autorité de Certification
3. Délivrance du certificat signé
4. Installation sur le serveur web
5. Renouvellement régulier

Limites et risques

- Certificat obsolète : expiré ou algorithme faible
- Faux HTTPS : le cadenas ne garantit pas la fiabilité du site
- Absence/invalide : vulnérabilité MITM, perte de confiance

Comment reconnaître un faux HTTPS ?

- Vérifier attentivement l’URL
- Cliquer sur le cadenas pour consulter le certificat
- Se méfier des certificats DV pour sites sensibles
- Repérer fautes d’orthographe ou mise en page douteuse

Comment se protéger ?

- Vérifier l’orthographe exacte du domaine
- Utiliser un navigateur à jour
- Activer protection contre le phishing
- Ne jamais cliquer sur des liens douteux
- Pour organisations : utiliser HSTS et renouveler les certificats

Attaque de l’homme du milieu (MitM)

- Attaquant s’interpose discrètement
- Peut écouter ou modifier les messages
- Exemple : facteur malveillant ouvrant le courrier

De SSL à TLS

- SSL = protocole ancien et obsolète
- TLS = norme actuelle, plus robuste
- “Certificat SSL” reste courant mais TLS sécurise
- Authentification + chiffrement renforcé

Handshake TLS : la poignée de main

- Client et serveur se présentent
- Vérification mutuelle de l’identité
- Accord sur une clé secrète pour chiffrer la session
- Processus rapide et invisible

TLS 1.3 : la dernière version

- Mise à niveau majeure contre menaces modernes
- Supprime algorithmes faibles
- Réduction du handshake : 2 allers-retours → 1 seul
- Confidentialité persistante (PFS)

Chronologie TLS et vulnérabilités

- SSL 3.0 → Poodle
  - Ancienne version du protocole SSL
  - Vulnérabilité Poodle : permettait de déchiffrer des données sensibles
  - Obsolète et dangereux

Chronologie TLS et vulnérabilités

- TLS 1.0 / 1.1 → obsolètes
  - Faiblesses dans les algorithmes et le handshake
  - Navigateurs modernes les bloquent ou déconseillent

Chronologie TLS et vulnérabilités

- TLS 1.2 encore utilisé sous conditions strictes
  - Sûr si bien configuré
  - Nécessite désactivation des algorithmes faibles
  - PFS recommandé

Chronologie TLS et vulnérabilités

- TLS 1.3 recommandé
  - Supprime les algorithmes faibles et obsolètes
  - Handshake plus rapide
  - PFS obligatoire par défaut
  - Meilleure sécurité et performances

Tableau récapitulatif

Version	Statut	Points clés
SSL 3.0	Obsolète	Vulnérable (Poodle)
TLS 1.0/1.1	Obsolète	Failles connues, non recommandé
TLS 1.2	Acceptable si strict	Configurer avec PFS et cipher modernes
TLS 1.3	Recommandé	Sécurisé, handshake rapide, PFS obligatoire

Poodle : vulnérabilité SSL 3.0

- Découverte en 2014
- Affecte principalement SSL 3.0 et certaines configurations anciennes de TLS
- SSL 3.0 utilisait un mécanisme appelé padding pour remplir les blocs de données

Poodle : vulnérabilité SSL 3.0

- La faille Poodle permet à un attaquant de déchiffrer partiellement les données
- Exemple : cookies de session, mots de passe
- Connexion supposée sécurisée compromise
- Sites utilisant SSL 3.0 vulnérables
- Solution : passer à TLS 1.2 ou TLS 1.3 avec cipher suites modernes et PFS activé

Performances TLS 1.3

- Gain de vitesse handshake : jusqu’à 50 %
- Latence réduite → chargement pages web plus rapide
- Sécurité renforcée et optimisation simultanée

C’est quoi l’ANSSI ?

- Agence Nationale de la Sécurité des Systèmes d’Information
- Organisme français chargé de la sécurité informatique nationale
- Émet des recommandations et normes pour sécuriser les réseaux, logiciels et infrastructures
- Conseille les entreprises et administrations pour réduire les risques cyber

Recommandations ANSSI

- Utiliser TLS 1.3 ✓
- TLS 1.2 acceptable si configuré strictement ✓
- Désactiver TLS 1.0, 1.1 et SSL ✓
- Cipher suites validées uniquement
- Mettre à jour logiciels et composants TLS

Cipher suites et algorithmes recommandés

Cipher suites et algorithmes recommandés

Algorithmes asymétriques

- Établissent la clé secrète commune
- ECDHE → recommandé, rapide, PFS
- RSA → encore utilisé, clé 2048+ bits
- EdDSA → récent, performant, sûr

Algorithmes symétriques

- Chiffrent le trafic une fois la clé partagée
- AES-GCM → sûr, rapide avec matériel
- ChaCha20-Poly1305 → performant sur appareils mobiles/IoT

ChaCha20-Poly1305 : algorithme symétrique

- ChaCha20 : chiffrement moderne, rapide sur CPU sans accélération
- Poly1305 : fonction d’authentification cryptographique
- Avantages : rapide sur smartphones/IoT, sécurisé
- Usage : TLS/HTTPS

Fonctions de hachage

- Assurent intégrité des données
- SHA-2 → robuste
- SHA-1 → obsolète, vulnérable

Configuration TLS/HTTPS recommandée

- Échange de clés : ECDHE (PFS)
- Chiffrement symétrique : AES-GCM ou ChaCha20-Poly1305
- Hachage : SHA-2

Sécurité et protection des données

- Authentification serveur
- Confidentialité des données échangées
- Intégrité des données
- Protection contre le rejeu

Résumé : Le cadenas numérique aujourd’hui

- **Cadenas + TLS 1.3 = protection solide**
- Résultat de décennies d’amélioration
- Toujours vigilance : nouvelles menaces et informatique quantique