NIST SP 800-30 – Évaluation des risques
Vulnérabilité
Faiblesse inhérente à un composant du système d'information.
Menace, Toute combinaison de circonstances et d'entités qui pourraient endommager les actifs informationnels.
Risque, Dépend à la fois de la vraisemblance de la menace et de son impact sur les actifs et les ressources.
Objectif
Initiation, Acquisition et développement, Implémentation, Opération et maintenance, Élimination, Évaluation des risques, Identification et évaluation des risques et de leurs impacts, Détermination des priorités de ces risques, Recommandation de contre-mesures, Atténuation des risques, Classement par ordre de priorité des contre-mesures, Implémentation des contre-mesures, Évolution et évaluation, Évaluation continue du système au cours de son évolution.
Neuf étapes
Caractérisation du système (Définir les limites du système à évaluer), *Identification des menaces* (menaces potentielles, motivations, moyens, aptitudes), *Identification des vulnérabilités*, *Analyse des fonctionnalités de sécurité* (Prévenir, Détecter, Réagir), *Détermination de la vraisemblance* (probabilité, nature, existence), *Analyse des impacts* (Mission, Criticité, Sensibilité, Rapport, Quantitatif, Quantitatif), *Détermination des risques (*vraisemblance, ampleur, aptitude, prevention*)*, *Recommandation des contre-mesures (*Efficacité, Compatibilité avec le système, Impact sur les opérations, Coûts, Politique organisationnelle, Loi et réglementation*)*, *Documentation* (Rapport, menaces, sources, moyen, motivation, vulnérabilités, priorité, risques, recommandations, sommaire, risques, principaux)
Accepter les risques, Éviter les risques, Limiter les risques, Planification, Transférer les risques
Moyens de contrôle
Vulnérabilité existe, Vulnérabilité peut être exploitée, Coût de l'attaquant est inférieur à son gain, La perte est trop grande.
Hiérarchisation des actions en fonction du niveau de risque.
Évaluation des contrôles proposés lors de l'évaluation des risques
Réalisation d'une analyse coût-bénéfice, Choix des moyens de contrôle, Assignation des responsabilités, Développement d'un plan d'implémentation, Implémentation des moyens de contrôle
Principe
Decomposition, liés
Simplicité: *Facilité la compréhension, Réduction des incohérences potentielles*
Restriction: *Limitation des interactions afin de minimiser les vérifications*
Architecture et conception
Abstractions simples (interfaces cohérentes), Mécanismes communs minimaux (dépendance mini), Modularité et Couches (efficace, structuré), Dépendances partiellement ordonnées (synchronisation, composant, gestion de dépendance, pas boucle), Accès assisté efficace et sécurisé (contrôle d'accès, limites, communs), Partage minimisé (nécessaire), Complexité Réduite (petite analyse), Évolutivité sécurisée (interconnexions, config), Composantes de confiance, Confiance hiérarchique, Seuil de modification inverse (proportionnel à sa fiabilité), Protection hiérarchique, Éléments sécurisés minimaux, Moindre privilège, Autorisation de prédicats, Fiabilité autonome, Composition distribuée sécurisée, Canaux de communication de confiance, Architecture ouverte
Moyens de sécurité et Comportements intrinsèques
Protection continue, Gestion sécurisée des métadonnées, Auto-Analyse, Imputabilité et traçabilité, Sécurité par défaut, Défaillance et recouvrement sécurisés, Coût-bénifice de la sécurité, Sécurité performante, Sécurité à facteur humain, Sécurité acceptable
Cycle de vie de sécurité
Procédures reproductibles et documentées, Rigueur procédurale, Modification sécurisée, Documentation suffisante
Développement de systèmes sécurisés fiables
Concept du moniteur de référence, Défense en profondeur, Isolation (logique ou physique)
Éviter les interfaces redondantes et inutilisées: *Simplicité des abstractions*
Éviter la dissimulation d'information: *Architecture ouverte, Simplicité des abstractions*
Si un noyau de système d'exploitation: Protection hiérarchique, Confiance hiérarchique
Les systèmes d'exploitation: *Modularité et couches, Dépendances partiellement ordonnées, Réduction de la complexité, Confiance hiérarchique, Composants de confiance, Protection hiérarchique, Éléments sécurisés minimaux, Architecture ouverte*
Need-to-know basis: *Principe du moindre privilège*
Deux personnes pour émettre un chèque: Autorisation basée sur des prédicats
Règles du pare-feu compte: *Principe du moindre privilège*
Éviter la surcharge sémantique des interfaces: Mécanismes communs minimaux, Simplicité des abstractions
WiFi Linux wpa_supplicant installe une clé de chiffrement tout zéro (TK) la vulnérabilité de clé de chiffrement tout zéro: *Protection continue, Échec sécurisé et récupération*
Mot de passe par défaut: Sécurité par défaut
Sudo wheel: Autorisation basée sur des prédicats
OSI: *Simplicité des abstractions, Modularité et couches, Dépendances partiellement ordonnées, Architecture ouverte*
Descripteur de fichier: *Accès assisté efficace et sécurisé*
Web no Certificat*: Sécurité à facteur humain*
Demande d'autorisation banque: *Autorisation de prédicats, Sécurité à facteur humain*
Protocole obsolète: *Évolutivité sécurisée, Protection continue, Défaillance et recouvrement sécurisés*
Rôles: *Moindre privilège*
Race condition*: Partage minimisé, Canaux de communication de confiance*
RSA 2048*: Sécurité performante, Sécurité acceptable*
Architecture Externe commun*: Sécurité performante, Sécurité acceptable*
Extra Keberos *: Architecture ouverte. Composantes de confiance, Éléments sécurisés minimaux*
Protection
Veille technologique=Connaissez bien vos ennemis.
Analyse des besoins=Connaissez-vous vous-même
Politique de sécurité (Prévention, Détection, Réaction)
Détecter l'occurrence d'une attaque: Reconnaissance, signatures d'attaques ou détection d'anomalie, modification aux informations sensibles
Système de détection d'intrusions (IDS): détecter en temps réel les tentatives d'intrusion et neutraliser ces attaques
IDS réseau (NIDS), IDS ordinateur hôte (HIDS), IDS application
Évènement (E-box): Netflow (trafic), Syslog(os log)
Analyse (A-box): Filtration, agrégation, corrélation
Base de données (BD-box): analyse post-mortem
Réaction (R-box): réponses malveillantes détectées
Méthodes de détection: DB mise à jour signature attaque, normal et malveillant, ver grand nombre de connexions
Fasse positive alarme: Détection d'une activité légitime comme une activité malveillante.
Fausse négative alarme: Activité malveillante acceptée comme une activité légitime.
Anti-virus: Scanneur de virus (pattern matching, only Virus connus)., Heuristiques (Rechercher code, false positive), Vérifieur d'intégrité (empreinte, après infection), Moniteurs de comportement (identifier le virus), Émulateurs(lent)
Signatures: Fuzzy Hashing, SSDEEP
Prévention: veille technologique, correctifs, architecture, Par défaut, bloquer tout trafic, bloquer signatures d'attaques, détection d'anomalie
Access Control List (ACL): Routeur (filtrer les paquets entrant ou sortant), Pare-feu (contrôle politique de sécurité) Source, IPSource, PortDest, IPDest, Port, Action, Trafic entrant (d'adresses illégales ou locales), IP spoofing, L'ordre des règles est important, Serveur SMTP et Serveur Web
Pare-feu à états: local → public, **table d'états:** filtrer TCP/IP (ou UDP/IP) avant le ACL
Connexions au pare-feu non filtrées par défaut, Présence de règles par défaut, Connexions au pare-feu non sécurité (p.ex., telnet), Gestion du pare-feu à partir de nombreux postes, Gestion du pare-feu à partir de postes externes, Connexions NetBIOS non filtrées! Souvent attaqués, Port RPC 111 non bloqué, Règles portant sur deux zones d'adresses IP, "Any" service on inbound, "Any" destination on outbound **Principe 1**: Sécurité par défaut, Règles précises pour accepter des flots données, Refuser tous les autres flots, **Principe 2**: Filtrer rapidement les protocoles les plus utilisés, Éviter de tester nombreuses règles inutilement
Configurations complexes: Cartographie réseau automatisée (prise en charge du cloud), Planification des politiques et gestion des règles, Orchestration automatisée des politiques, Découverte de connectivité / détection de périphérique, Coordination des politiques entre les pare-feu et l'infrastructure cloud, Surveillance des événements en temps réel, Console de surveillance unique
Service mandataire inverse: Le service agira aussi comme intermédiaire pour les communications chiffrées (TLS)
Analyse de flux: les paquets sont examinés en direct lors de leur passage dans un flux.
Pare-feu proxy: Ce dispositif devrait pouvoir interpréter les informations applicatives afin de pouvoir prendre une décision le plus juste possible. Par exemple, la reconstruction des paquets IP fragmentés. Le man-in-the middle autorisé!
Niveau circuit: OSI
Niveau applicatif: HTTP, Bloque l'accès, URL, commandes, js, SMTP, pièces jointes, analyse virus, Authentification, Contre performance, Bris de la communication
Zone démilitarisée: Zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le coupe-feu réseau intermédiaire regroupant des serveurs publics, connexion directe avec le réseau interne et de prévenir celui-ci de toute attaque extérieure depuis le Web. Moindre privilège, Séparation des privilèges, Protégé par défaut, Économie de moyen. **Externe** Cacher les adresses par le DMZ, Bloquer tout trafic illégitime, Offrir des proxys applicatifs. Économie de moyen, Séparation des privilèges, Protégé par défaut, **Interne:** Cacher les adresses par le DMZ, Bloquer tout trafic illégitime, Économie de moyen, Séparation des privilèges, Protégé par défaut
Proxy: Analyser les trafics applicatifs, Mettre en œuvre des filtres complexes (virus). Principaux dispositifs afin de mettre en œuvre la politique de sécurité.
Deep packet inspection: En plus de l'entête, analyse le contenu des paquets proxy pour les connexions chiffrées TLS, analyser les protocoles courants, authentifier (et autoriser) les usagers à accéder aux réseaux, analyser le trafic entrant et sortant
Threat Prevention, Service WildFire, URL Filtering, DNS Security, IoT Security
IEEE 802.1I: Usagers internes (authentifiés), Personnes externes, Usagers légitimes, Association, Données
Menaces: Confidentialité du service, Intégrité du service, Disponibilité du service, Usurpation du service
Beacon: paquet de gestion contenant diversesinformations permettant d'établir la communication MAC, SSID: Service Set Identifier, authentifier, associer
Robust Security Network (RSN): Mécanisme de gestion de clés – 4-way Handshake. Vérification de la clé commune (pairwise master key (PMK)), Synchronisation des clés de session, Confirmation des protocoles de chiffrement et d'intégrité
1 Découverte 802.11(WEP, TKIP, AES-CCMP), Authentification(IEEE 802.1x / EAP, EAPoW, RADIUS (Remote Authentication Dial In User Service), Master Session Key – MSK, Pre-Shared Key – PSK, EAP-TLS : authentification mutuelle basée sur les certificats à clés publiques, EAP-TTLS : authentification du serveur d'authentification (point d'accès)), Gestion de clés(Pairwise Master Key (PMK), Temporal Key, 4-way handshake)
Chiffré + Authentifié: Communication(AES-CCM, Compteur + Nonce, PTK), Terminaison
Key Reinstallation Attacks : Ne permet pas d'obtenir de clés, Mais la manipulation du flux de clés temporaires, AES-CCMP, broadcast
wpa_supplicant: Version 2.4 and 2.5 install an all-zero encryption key (TK) when receiving a retransmitted message 3. This vulnerability appears to be caused by a remark in the 802.11 standard that indirectly suggests to clear the TK from memory once it has been installed
Contre-mesures: already-in-use key is being installed, data-confidentiality protocol during a handshake execution
Payment Card Industry (PCI): SSL/TLS ou IPSEC pour sauvegarder les données des titulaires de cartes sensibles lors de leur transmission sur des réseaux publics ouverts
WEP: 24 bits – 224 possibilités, Paradoxe des anniversaires, Le standard permet réutilisé un même keystream pour 16 fragments. Avec beaucoup de SI Si l'attaquant près du point d'accès fragmente le paquet Si la première partie du paquet est connue Si le point d'accès envoie le paquet vers un site sous le contrôle de l'attaquant
Kerberos et SSL: Protocole distribué d'authentification, Fonctionne au dessus d'un réseau non sécurisé, Confidentialité des communications, Intégrité des données, Authentification mutuelle des deux participants à une communication, Protection contre le rejeu, clé symétrique
Key Distribution Center (KDC): tous les secrets et les clés cryptographiques permettant d'effectuer les diverses opérations,
Authentication Service (AS), **Ticket granting service** (TGS)
1. L'utilisateur saisit son identifiant et son mot de passe.
2. L'utilisateur utilise une fonction de hachage à sens unique pour produire sa clé secrète.
3. Le client envoie une requête au AS: « Usager X voudrait utiliser un service Y ». Pas de mot de passe ou de clé n'est envoyé.
as_req: <client, service, timeexp, timestamp>
4. L'AS vérifie que le client existe dans sa base de données. Si c'est le cas, l'AS renvoie deux messages au client :
Msg A: Clé de session entre le client et le TGS chiffrée.
as_rep A:[KeyClient-TGS, timestamp]KeyClient
Msg B: Ticket TGT
as_rep B:[client, address, validity, KeyClient-TGS]KeyTGS
5. Le client déchiffre Message A, vérifie si Timestamp correspond à celui envoyé à l'étape 3 et obtient sa clé pour communiquer avec le TGS. Le client ne peut pas déchiffrer le Ticket B destiné au TGS.
6. Pour accéder à srv, le client envoie une requête au TGS:
Msg C: Le Ticket TGT chiffré et le nom du service demandé.
tgs_req C: srv ,[client, address, validity, KeyClient-TGS]KeyTGS
Msg D: Authenticator - nom du client et du Timestamp chiffrés
tgs_req D: [client, timestamp]KeyClient-TGS
7. Le TGS déchiffre l'Authenticator et retourne au client
Msg E: Le Ticket Client-to-Server chiffré
tgs_res E: srv,[client,address,validity,KeyClient-Srv]KeySrv
Msg F: La clé de session client/serveur chiffrée
tgs_res F: [timestamp,KeyClient-Srv]KeyClient-TGS
8. Le client déchiffre Msg F, vérifie si Timestamp correspond à celui envoyé à l'étape 5 et obtient sa clé pour communiquer avec Srv.
9. Afin d'accéder à un service, le client envoie à Srv une requête de service:
Msg G: Le Ticket Client-to-Server et le nom du service demandé.
serv_req G: srv,[client,address,validity,KeyClient-Srv]KeySrv
Msg H: Authenticator composé du client et d'un nonce chiffré
serv_req H: [client, timestamp]KeyClient-Srv
10. Le service déchiffre le ticket et renvoie le time de Msg H incrémenté de 1 chiffré avec la clé de session client/serveur. **11.** Le client déchiffre Msg H et vérifie si Timestamp a été incrémenté. Si oui, le client peut faire confiance à Srv. **12.** Srv offre le service au client.
SSL - Secure Sockets Layer: Confidentialité, Couche transport, Intégrité, Authenticité. Successeur: Transport Layer Security (TLS)
Choisir une alg. de chiffrement, Certificat + Chaine de cert, Envoyer une clé publique, Envoyer clé de session chiffrée
GCM: Galois/Counter Mode
Attack: TLS utilise le cryptogramme du dernier bloc du message précédent comme IV pour le premier bloc du message suivant => prédictible Attaque avec message clair choisi, CBC Mode
We know ciphertext, we want plain text, we control plaintext end
Compression Ratio Info-leak Made Easy (CRIME)
Cherche à obtenir les cookies d'authentification Détournement de session
Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH)
Cherche à obtenir les mots de passe
Padding Oracle On Downgraded Legacy Encryption (Poddle)
Simplement désactiver SSLv3 sur le serveur
SSL v3 - mode de chiffrement CBC, supporter TLS v1.0
Degradation Revenir en arrière: un protocole non-sécuritaire au lieu de refuser une demande de connexion
Secure token, Cookie d'authentification, attack padding AES-CBC
HeartBleed: Permettre de garder un lien actif sans devoir renégocier à chaque connexion, Patch logiciel pour openssl
Sécurité de bout en bout
Vérification du certificat
Validation du Nom de domaine vs. Propriétaire du certificat
RFC 2818: Fully qualified DNS name vs. SubjectAltNames
Man-in-the-middle: routeur/commutateur, point d'accès WiFi, DNS, leur certificat SSL valide, Forger de faux certificats, Controller une

autorité de certification, Avoir accès aux clés privées du serveur attaqué

TLS v1.3 – Échange de clé: Chiffrement RSA, Obtenir la clé RSA du serveur (et son certificat), Valider la clé (et son certificat), Chiffrer une clé de session (nouvelle et « pseudo-aléatoire »).

Digression – Diffie-Hellman

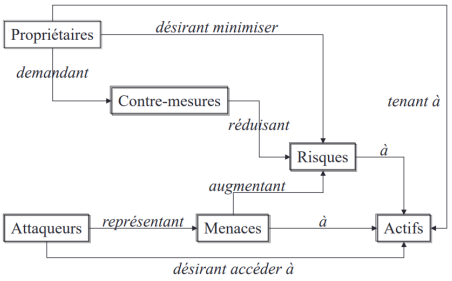
1. Alice choisit x au hasard. 1. Bob choisit y au hasard.
2. Alice envoie gx mod p à Bob. 2. Bob envoie gy mod p à Bob.
3. Après la réception du message de Bob, Alice calcule la (gy mod p)x mod p. 3. Après la réception du message d'Alice, Bob calcule la (gx mod p)y mod p.
4. La clé secrète peut être utilisée pour chiffrer un message. 4. La clé secrète peut être utilisée pour chiffrer un message.

Une clé de session grâce à DH, ils se doivent d'authentifier leur partenaire. DHE-RSA

MOTS DE PASSE: Facile à mettre en œuvre, révoquer ou changer, comprendre, Authentification rapide, Difficile mot de passe sécuritaire, rappeler, sécurité des systèmes d'information, bcrypt, Après trois tentatives infructueuses, Bloquer le compte, Ralentir la vérification, pas Réutilisation d'un mot de passe, 8 caractères, pas 4 fois char, minuscules, majuscules, chiffres, caractères spéciaux, Mots du dictionnaire, basic8, dictionnary8, comprenhensive8, blacklist, basic16,Indicateurs de sécurité, mots de passe choisis sont plus longs si un indicateur est présent, pas plus difficiles à mémoriser, Norme 1c12, Mauvais chiffrement md5, Base de données « salée », PBKDF2, bcrypt, rainbow tables, Liste des mots de passe les plus courants, éviter que le même SALT, algorithme lent, PBKDF2(PRF, Password, Salt, n, dkLen), fonction pseudo aléatoire telle que HMAC, nombre d'itérations de PRF, longueur de la clé générée. WiFi WPA2 – pre-shared key DK = PBKDF2(HMAC−SHA1, passphrase, ssid, 4096, 256). supportée après 90 jours

Contrôle d'accès: Identification: Identifier de façon unique un sujet grâce à un identifiant.(OpenID) **Authentification:** S'assurer que l'identité du sujet est bien celle qu'il prétend être.(Credential) (One-time password, Token device, GRID Cards: Défi / Réponse lors de l'authentification, One-time password) **Autorisation:** Déterminer si le sujet authentifié peut poser l'action désirée sur l'objet spécifié. (Discretionary Access Control DAC propriétaire d'un objet défini les droits ,Mandatory Access Control MAC hiérarchisation des sujets et des objets, Non discretionary Access Control RBAC).Tables de possibilités Le ticket de Kerberos utilise se principe. Listes de contrôle d'accès Très répandues. Systèmes d'exploitation, routeurs. Matrice de contrôle d'accès le modèle DAC

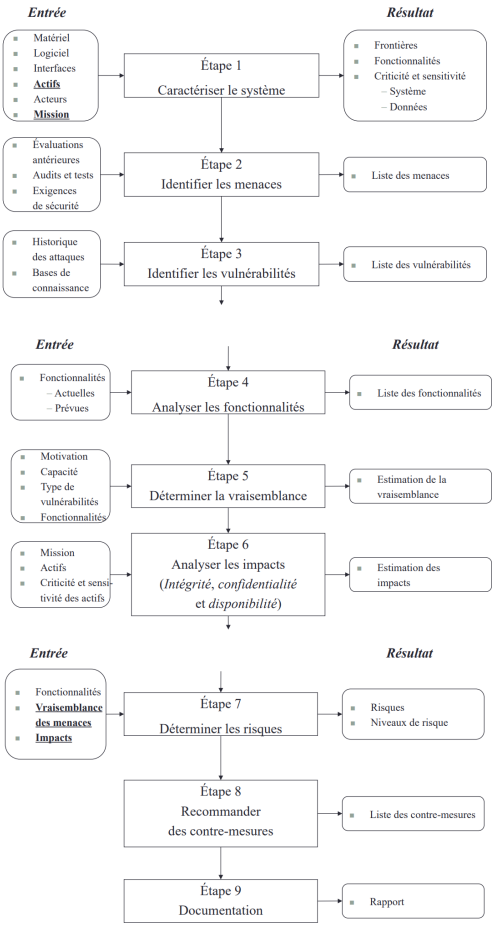
Imputabilité (Accounting): Attribuer un accès à un objet ou une opération à un sujet donné afin de s'assurer de la traçabilité de toute violation ou tentative de violation d'une règle de sécurité. La dernière étape est de s'assurer que les actions posées par les personnes dûment authentifiées et autorisées soient journalisées. Les fichiers journaux permettent d'imputer les actions aux personnes.



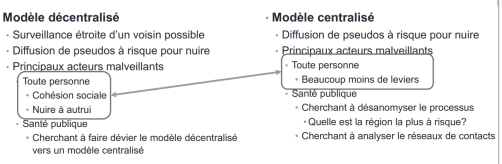
	Impact bas (10)	Impact moyen (50)	Impact haut (100)
Vraisemblance haute 1.0	**BAS** 10 x 1.0 = 10	**MOYEN** 50 x 1.0 = 50	**HAUT** 100 x 1.0 = 100
Vraisemblance moyenne 0.5	**BAS** 10 x 0.5 = 5	**MOYEN** 50 x 0.5 = 25	**MOYEN** 100 x 0.5 = 50
Vraisemblance basse 0.1	**BAS** 10 x 0.1 = 1	**BAS** 50 x 0.1 = 5	**BAS** 100 x 0.1 = 10

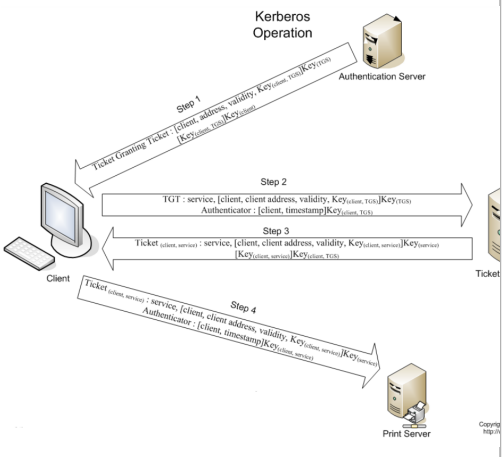
Étape 2 – Identification des menaces

Source	Motivation	Actions
Pirate (*hacker, cracker*)	▪Challenge ▪Ego ▪Rébellion	▪Piratage ▪Ingénierie sociale
Criminel informatique	▪Destruction d'information ▪Divulgation d'information ▪Altération d'information ▪Gain monétaire	▪Ingénierie sociale ▪Interception d'information ▪Intrusion de système ▪Chantage informatique ▪Cambriolage ▪Mystification (*spoofing*)
Terroriste	▪Destruction ▪Revanche ▪Idéologie	▪Bombe / terrorisme ▪Guerre de l'information ▪Attaque de systèmes (DDoS) ▪Intrusion de systèmes ▪Subordination de systèmes (*tampering*)
Espionnage industriel	▪Avantage compétitif ▪Appât du gain	▪Ingénierie sociale ▪Intrusion de système ▪Vol d'information
Employé ▪Malformé ▪Négligent ▪Malveillant ▪Malhonnête ▪Congédié	▪Curiosité ▪Ego ▪Renseignement ▪Appât du gain ▪Revanche ▪Non intentionnel et omission	▪Code malveillant ▫Cheval de Troie, Bombe logique ▪Accès à de l'information privée ▪Utilisation d'ordinateur abusive ▪Fraude et vol ▪Vente d'information personnelle ▪Sabotage de système ▪Intrusion de système



Semi-honnête ou Honnête-mais-curieux: Cherche à obtenir des informations mais sans polluer le système de fausses informations
Malhonnête: Aucune restriction





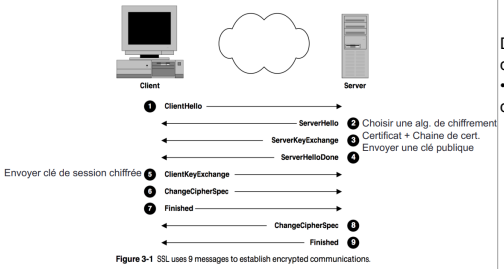
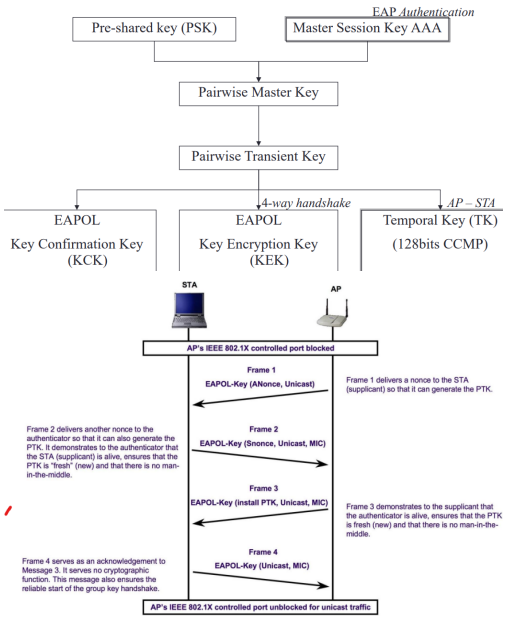


Figure 3-1 SSL uses 9 messages to establish encrypted communications.



Autorisation – Matrice de contrôle d'accès

- La matrice de contrôle d'accès est une matrice à deux dimensions indiquant pour chaque sujet quelles sont les actions que le sujet peut effectuer sur chaque objet.

Usager	Fichier 1	Fichier 2	Fichier 3
Alice	Lecture – Écriture	Lecture – Écriture – Exécution	Pas d'accès
Bob	Pas d'accès	Lecture	Lecture – Écriture – Exécution –
Charles	Lecture	Pas d'accès	Lecture

- Généralement utilisées pour le modèle DAC.

Autorisation – Listes de contrôle d'accès

- Vecteur de la matrice de contrôle d'accès donnant les droits des sujets pour un objet donnée.

Fichier 1
Alice: Lecture – Écriture
Bob: Pas d'accès
Charles: Lecture

- Très répandues. Systèmes d'exploitation, routeurs, …

Autorisation – Tables de possibilités

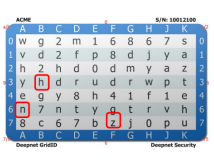
- Vecteur de la matrice de contrôle d'accès donnant les droits d'un sujet donné pour tous les objets.

Alice	Fichier 1: Lecture – Écriture	Fichier 2: Lecture – Écriture – Exécution	Fichier 3: Pas d'accès

- Le ticket de Kerberos utilise se principe.

Les GRID Cards

Défi / Réponse lors de l'authentification
- Coordonnés du défi: (A,6), (B,3), (F,7)
- Réponses: n, h, z
- Probabilité: 1 sur 363 ou 1 sur 46656



One-time password
- Pré-requis: l'usager définit un patron
  - Vertical / **Horizontal**
  - Longueur (max. 4, par exemple)

Le serveur vérifiera s'il trouve une séquence horizontale de longueur 4 correspondante – recherche exhaustive.

Durée variable • 8 à 30 caractères • Vérification avec le dernier mot de passe • Trois catégories • Lettres minuscules • Lettres majuscules • Chiffres • Symboles • Dictionnaire de chaines • Réduisant la durée de vie