UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Securité System et Réseau

Sommaire

- Fondamentaux de la sécurité informatique
- Sécurité des systèmes d'exploitation
- Sécurité réseau
- Cryptographie et gestion des clés
- Gestion des vulnérabilités et des risques
- Sécurité des applications et du développement
- Conformité et normes de sécurité

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Fondamentaux de la sécurité informatique

Fondamentaux de la sécurité informatique

Definition

- L'architecture logicielle se réfère à la structuration fondamentale d'un système logiciel.
- Elle consiste en la définition des différents composants logiciels (ou modules), les relations qu'ils entretiennent entre eux, et les principes de conception qui guident leur organisation et leur intégration au sein du système.
- Imaginez l'architecture logicielle comme le plan d'un bâtiment, décrivant non seulement les pièces (composants logiciels) mais aussi comment elles sont connectées (communications) et où elles sont placées (déploiement).

Fondamentaux de la sécurité informatique

Les enjeux et les risques

Enjeux de la sécurité informatique

1. ***Protection des données sensibles :***

- Protéger les informations personnelles, financières et professionnelles contre les accès non autorisés et les fuites de données.
- Garantir la confidentialité, l'intégrité et la disponibilité des données.

2. ***Maintien de la continuité des activités :***

- Assurer la disponibilité des systèmes et des réseaux pour éviter les interruptions de service qui peuvent entraîner des pertes financières et de réputation.
- Mettre en place des plans de reprise après sinistre et de continuité des activités.

Fondamentaux de la sécurité informatique

Les enjeux et les risques

Enjeux de la sécurité informatique

3. ***Conformité réglementaire :***

- Respecter les lois et les régulations en matière de protection des données et de cybersécurité (ex. RGPD, HIPAA).
- Éviter les amendes et les sanctions liées à la non-conformité.

4. ***Préservation de la réputation :***

- Éviter les incidents de sécurité qui peuvent nuire à la confiance des clients et des partenaires.
- Protéger la réputation de l'organisation en montrant un engagement envers la sécurité.

Fondamentaux de la sécurité informatique

Les enjeux et les risques

Enjeux de la sécurité informatique

5. ***Innovation et compétitivité :***

- Protéger les innovations et les propriétés intellectuelles contre l'espionnage industriel et le vol.
- Maintenir un avantage concurrentiel en sécurisant les informations stratégiques.

Fondamentaux de la sécurité informatique

Les enjeux et les risques

Risques de la sécurité informatique

1. ***Cyberattaques :***

- **Malware** : logiciels malveillants comme les virus, les ransomwares et les chevaux de Troie qui peuvent endommager ou compromettre les systèmes.
- **Phishing** : tentatives de fraude pour obtenir des informations sensibles en se faisant passer pour des entités de confiance.
- **Attaques DDoS** : attaques par déni de service distribué visant à rendre un service ou un réseau indisponible en le submergeant de trafic.

Fondamentaux de la sécurité informatique

Les enjeux et les risques

Risques de la sécurité informatique

2. ***Vulnérabilités et exploits :***

- **Failles de sécurité :** vulnérabilités dans les logiciels et les systèmes qui peuvent être exploitées par des attaquants.
- **Zero-day :** failles inconnues des développeurs et des utilisateurs, mais exploitées par les cybercriminels.

3. ***Insider threats :***

- **Menaces internes :** employés ou partenaires ayant des accès privilégiés qui abusent de leurs droits pour compromettre les systèmes ou voler des données.

Fondamentaux de la sécurité informatique

Les enjeux et les risques

Risques de la sécurité informatique

4. ***Perte de données :***

- **Fuites de données :** exfiltration d'informations sensibles vers des entités non autorisées.
- **Destruction de données :** perte définitive de données critiques à cause de malwares ou d'erreurs humaines.

5. ***Non-conformité réglementaire :***

- **Sanctions légales :** amendes et poursuites judiciaires en cas de non-respect des régulations en matière de sécurité et de protection des données.
- **Perte de confiance :** diminution de la confiance des clients et des partenaires en cas de non-conformité.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Principales Menaces

1. ***Malware (Logiciels malveillants) :***

- **Virus :** Programmes qui se répliquent en infectant d'autres fichiers exécutables et peuvent causer des dommages variés.
- **Trojans (Chevaux de Troie) :** Logiciels déguisés en applications légitimes, mais qui exécutent des actions malveillantes à l'insu de l'utilisateur.
- **Ransomware :** Logiciels qui chiffrent les fichiers de la victime et exigent une rançon pour fournir la clé de déchiffrement.
- **Spyware :** Logiciels qui espionnent les activités de l'utilisateur et collectent des informations sensibles.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Principales Menaces

2. ***Phishing :***

- **Emails de phishing :** Tentatives de fraude par email visant à obtenir des informations sensibles comme des mots de passe ou des informations de carte de crédit.
- **Spear phishing :** Attaques ciblées sur des individus spécifiques, souvent bien documentées et personnalisées.

3. ***Attaques par déni de service (DoS) et déni de service distribué (DDoS) :***

- **DoS :** Attaques visant à rendre un service ou un réseau indisponible en le surchargeant de requêtes.
- **DDoS :** Attaques similaires à DoS, mais lancées à partir de multiples systèmes infectés par des malwares.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Principales Menaces

4. ***Menaces internes :***

- Insider threats : Employés ou partenaires internes ayant accès aux systèmes et données, qui peuvent abuser de leurs privilèges pour des gains personnels ou par mécontentement.

5. ***Attaques par force brute :***

- Tentatives de deviner des mots de passe en essayant systématiquement toutes les combinaisons possibles.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Principales Vulnérabilités

1. ***Vulnérabilités logicielles :***

- **Failles zero-day :** Vulnérabilités non connues des développeurs du logiciel au moment de leur exploitation par les attaquants.
- **Failles de sécurité non corrigées :** Vulnérabilités pour lesquelles des correctifs existent, mais qui n'ont pas été appliqués par les utilisateurs.

2. ***Erreurs de configuration :***

- **Mauvaise configuration des pare-feux :** Politiques de sécurité trop permissives ou incorrectement configurées.
- **Paramètres par défaut non modifiés :** Utilisation de mots de passe ou de configurations par défaut, souvent bien connus des attaquants.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Principales Vulnérabilités

3. ***Problèmes d'authentification et de gestion des accès :***

- **Mots de passe faibles :** Utilisation de mots de passe simples et faciles à deviner.
- **Absence de multi-factor authentication (MFA) :** Dépendance uniquement sur les mots de passe pour la sécurité des comptes.

4. ***Vulnérabilités réseau :***

- **Sniffing de réseau :** Interception de données sensibles transmises en clair sur le réseau.
- **Man-in-the-Middle (MitM) :** Interception et modification des communications entre deux parties sans qu'elles en soient conscientes.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Principales Vulnérabilités

5. ***Problèmes de sécurité physique :***

- **Accès physique non sécurisé :** Accès non contrôlé aux équipements informatiques, permettant des manipulations matérielles ou des vols de données.

6. Scripts et injections :

- **SQL injection :** Insertion de code SQL malveillant dans des requêtes pour accéder ou manipuler des bases de données.
- **Cross-site scripting (XSS) :** Insertion de scripts malveillants dans les pages web vues par d'autres utilisateurs.

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Cartographie des attaques

https://cybermap.kaspersky.com/fr

https://threatmap.checkpoint.com/

https://threatmap.fortiguard.com/

https://www.digitalattackmap.com/

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Attaques importantes recentes

- **NOTPETYA** -> Attaque du 27 Juin 2017
- **WANNACRY** -> Attaques des 12 et 13 mai 2017
- **SONY** -> Attaque de Novembre 2014

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Statistiques des attaques

Concernant les particuliers

- Source https://silicon.fr
- 3 minutes en moyenne pour pirater un nouvel objet connecté
- 1,1 million de victimes de fraude à la carte bancaire par an
- 83% des smartphones infectés au 2eme semestre 2016
- 65 vols de données par seconde
- 41% de succès lors d'attaque par RansomWare
- 201 jours en moyenne pour découvrir une cyberattaque

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Statistiques des attaques

Concernant les entreprises

- 77% des organisations mondiales ont été victimes d'au moins une cyberattaque réussie en 2017
- https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge2018-CDR.pdf
- 23% des entreprises de type PME ont eu un incident de sécurité à cause d'objets connectés (IoT)
- https://keepersecurity.com/fr_FR2017-State-Cybersecurity-SmallMedium-Businesses-SMB.html
- 95% des attaques web comportent de l'ingénierie sociale
- https://www.proofpoint.com/sites/default/files/pfpt-fr-tr-thehuman-factor-2018.pdf

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Statistiques des attaques

Concernant les entreprises

- 5 à 10% du budget d'une entreprise est consacré à la cybersécurité
- https://experiences.microsoft.fr/business/confiance-numeriquebusiness cybersecurite-chiffres-cles/
- 800 000€ de coût en moyenne lors d'une violation de sécurité
- https://experiences.microsoft.fr/business/confiance-numeriquebusinesscybersecurite-chiffres-cles/
- 35% des incidents de cybersécurité sont dus à des collaborateurs
- https://experiences.microsoft.fr/business/confiance-numeriquebusiness/cybersecurite-chiffres-cles/

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Autres sources

- https://experiences.microsoft.fr/articles/cybersecurite/cybersecurite-chiffres-cles/
- https://cyberedgegroup.com/cdr/

Fondamentaux de la sécurité informatique

Principales menaces et vulnérabilités

Mesures de Protection

- **Mises à jour régulières et correctifs de sécurité** : Maintenir tous les logiciels et systèmes à jour.
- **Politiques de mot de passe robustes** : Exiger des mots de passe complexes et utiliser l'authentification multi-facteurs.
- **Configuration sécurisée** : S'assurer que les systèmes sont correctement configurés et sécurisés.
- **Sécurité physique** : Protéger les équipements et les données par des contrôles d'accès physiques.
- **Formation des employés** : Former et sensibiliser régulièrement les employés aux menaces de sécurité.
- **Chiffrement des données** : Utiliser des techniques de chiffrement pour protéger les données sensibles.
- **Contrôles d'accès** : Implémenter des contrôles d'accès stricts basés sur les rôles et les besoins.
- **Surveillance et journalisation** : Mettre en place des systèmes de surveillance et de journalisation pour détecter et répondre aux incidents de sécurité.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

Confidentialité, intégrité et disponibilité (CIA)

- Le modèle de sécurité CIA (Confidentialité, Intégrité et Disponibilité) est un cadre fondamental utilisé pour guider les politiques de sécurité de l'information au sein d'une organisation.
- Chacun de ces trois piliers vise à protéger différents aspects des informations et des systèmes informatiques.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

1. *Confidentialité (Confidentiality)*

- **Définition :** La confidentialité consiste à garantir que les informations ne sont accessibles qu'aux personnes autorisées et à prévenir tout accès non autorisé.
- **Objectif :**
  - Protéger les données sensibles contre les intrusions, le vol et la divulgation non autorisée.
  - Assurer que seules les personnes ayant les droits nécessaires peuvent consulter ou manipuler les informations.
- **Mécanismes de protection :**
  - **Chiffrement :** Utilisation de techniques de cryptographie pour rendre les données illisibles pour les utilisateurs non autorisés.
  - **Contrôle d'accès :** Mise en œuvre de systèmes d'authentification et d'autorisation pour vérifier les identités et limiter l'accès aux informations sensibles.
  - **Politiques de confidentialité :** Établir des règles strictes sur qui peut accéder aux informations et sous quelles conditions.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

2. *Intégrité (Integrity)*

- **Définition :** L'intégrité vise à maintenir la précision et la complétude des données tout au long de leur cycle de vie.
- **Objectif :**
  - Empêcher la modification non autorisée ou non détectée des données.
  - Garantir que les informations sont fiables et exactes.
- **Mécanismes de protection :**
  - **Contrôles de version :** Suivre les modifications apportées aux données et permettre la restauration des versions antérieures en cas de besoin.
  - **Sommes de contrôle et hachage :** Utiliser des fonctions de hachage pour vérifier que les données n'ont pas été altérées.
  - **Journalisation et audits :** Enregistrer les modifications et les accès aux données pour pouvoir détecter et analyser les actions suspectes.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

3. *Disponibilité (Availability)*

- **Définition :** La disponibilité garantit que les systèmes, les services et les données sont accessibles en temps voulu par les utilisateurs autorisés.
- **Objectif :**
  - Assurer un accès continu aux informations et aux systèmes nécessaires aux opérations.
  - Minimiser les temps d'arrêt et les interruptions de service.
- **Mécanismes de protection :**
  - **Redondance :** Utiliser des systèmes et des chemins de communication redondants pour éviter les points de défaillance uniques.
  - **Plans de reprise après sinistre (DRP) :** Établir des procédures pour restaurer les systèmes et les données après un incident.
  - **Maintenance régulière et surveillance :** Effectuer des vérifications et des maintenances préventives pour détecter et corriger les problèmes avant qu'ils n'affectent la disponibilité.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

Importance du Modèle CIA

Le modèle CIA est essentiel car il offre une approche équilibrée pour sécuriser les systèmes d'information.

- **Confidentialité :** Empêche les fuites d'informations et protège la vie privée.
- **Intégrité :** Assure que les informations sont exactes et fiables, évitant les erreurs et les fraudes.
- **Disponibilité :** Garantit que les services et les informations sont disponibles lorsque nécessaire, supportant la continuité des activités.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

Authentification, Autorisation et Audit (AAA)

- Le modèle AAA, qui se compose de l'Authentification, de l'Autorisation et de l'Audit, est un cadre fondamental utilisé pour gérer et renforcer la sécurité des systèmes d'information et des réseaux.
- Chacun de ces trois composants joue un rôle crucial dans la protection des ressources informatiques et la garantie de leur utilisation appropriée.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

1. *Authentification (Authentication)*

- **Définition :** L'authentification est le processus de vérification de l'identité d'un utilisateur, d'un système ou d'un service.
- **Objectif :**
  - Garantir que seules les entités légitimes peuvent accéder aux systèmes et aux données.
  - Prévenir l'accès non autorisé en vérifiant l'identité des utilisateurs ou des systèmes.
- **Mécanismes de protection :**
  - **Mots de passe :** Utilisation de mots de passe forts et uniques pour authentifier les utilisateurs.
  - **Biométrie :** Utilisation de caractéristiques physiques (empreintes digitales, reconnaissance faciale) pour l'authentification.
  - **Cartes à puce et tokens :** Dispositifs matériels utilisés pour authentifier les utilisateurs.
  - **Authentification multi-facteurs (MFA) :** Combinaison de plusieurs méthodes d'authentification (par exemple, mot de passe + token).

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

2. *Autorisation (Authorization)*

- **Définition :** L'autorisation est le processus de détermination des ressources et des services auxquels un utilisateur, un système ou un service authentifié a accès.
- **Objectif :**
  - Assurer que les utilisateurs ont accès uniquement aux ressources nécessaires pour accomplir leurs tâches.
  - Prévenir l'accès non autorisé aux ressources sensibles.
- **Mécanismes de protection :**
  - **Contrôle d'accès basé sur les rôles (RBAC) :** Attribution des permissions en fonction des rôles des utilisateurs dans l'organisation.
  - **Listes de contrôle d'accès (ACL) :** Définition des permissions spécifiques pour les utilisateurs ou les groupes d'utilisateurs.
  - **Cartes à puce et tokens :** Dispositifs matériels utilisés pour authentifier les utilisateurs.
  - **Politiques de sécurité :** Établissement de règles claires concernant l'accès aux ressources.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

2. *Audit (Accounting)*

- **Définition :** L'audit, ou l'accounting, est le processus de suivi et d'enregistrement des actions et des accès des utilisateurs, des systèmes et des services.
- **Objectif :**
  - Fournir une traçabilité des actions pour l'analyse des incidents de sécurité et la conformité réglementaire.
  - Permettre la détection et l'analyse des comportements suspects ou des violations de sécurité.
- **Mécanismes de protection :**
  - **Journaux d'audit (log files) :** Enregistrement détaillé des accès, des actions et des modifications apportées aux systèmes et aux données.
  - **Systèmes de gestion des informations et des événements de sécurité (SIEM) :** Collecte et analyse centralisée des journaux d'audit pour détecter les incidents de sécurité.
  - **Rapports et alertes :** Génération de rapports réguliers et envoi d'alertes en cas d'activités suspectes.

Fondamentaux de la sécurité informatique

Concepts de base en sécurité

Importance du Modèle AAA

Le modèle **AAA** est essentiel pour la gestion de la sécurité des systèmes d'information et des réseaux.

- **Authentification :** Empêche l'accès non autorisé en vérifiant l'identité des utilisateurs, ce qui est la première ligne de défense contre les intrusions.
- **Autorisation :** Assure que les utilisateurs authentifiés n'ont accès qu'aux ressources nécessaires, minimisant le risque d'abus ou de compromission des données sensibles.
- **Audit :** Fournit une traçabilité complète des actions et des accès, facilitant la détection des comportements anormaux, l'analyse des incidents et la conformité réglementaire.

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Sécurité des systèmes d'exploitation

Sécurité des systèmes d'exploitation

La Définition ?

La sécurité des systèmes d'exploitation (OS) fait référence à un ensemble de pratiques, de mesures et de technologies visant à protéger les systèmes d'exploitation contre les menaces potentielles, telles que les accès non autorisés, les attaques de logiciels malveillants, les vulnérabilités de sécurité et les erreurs de configuration.

Sécurité des systèmes d'exploitation

Les aspects essentiels

- Authentification et autorisation
- Protection contre les logiciels malveillants
- Mises à jour de sécurité
- Chiffrement des données
- Surveillance et journalisation
- Gestion des vulnérabilités
- Sécurisation des configurations
- Sécurisation des réseaux
- Éducation et sensibilisation

Sécurité des systèmes d'exploitation

Mises à jour régulières

1. **Utilisation de gestionnaires de paquets :**
   - Sur les distributions comme Ubuntu, utilisez `apt` pour mettre à jour les paquets système :

```
sudo apt update
sudo apt upgrade
```

   - Sur les distributions comme CentOS/RHEL, utilisez `yum` ou `dnf` :

```
sudo yum update
```

   ou

```
sudo dnf update
```

Sécurité des systèmes d'exploitation

Mises à jour régulières

2. **Configurer les mises à jour automatiques :**
   - Vous pouvez configurer votre système pour qu'il vérifie et installe automatiquement les mises à jour de sécurité. Par exemple, sur Ubuntu, vous pouvez utiliser `unattended-upgrades`.
3. **Vérifier régulièrement les mises à jour :**
   - Planifiez un horaire régulier pour vérifier les mises à jour disponibles et les appliquer. Par exemple, configurez une tâche cron pour exécuter `apt update` et `apt upgrade` toutes les semaines.

Sécurité des systèmes d'exploitation

Mises à jour régulières

4. **Mises à jour des applications tierces :**
   - Si vous utilisez des logiciels tiers ou des applications non incluses dans les dépôts officiels de votre distribution, assurez-vous de suivre les instructions de mise à jour fournies par les développeurs de ces applications.
5. **Surveillance des annonces de sécurité :**
   - Abonnez-vous aux listes de diffusion de sécurité de votre distribution Linux pour être informé des nouvelles vulnérabilités et des correctifs disponibles.
6. **Utilisation de gestionnaires de version pour les environnements de développement :**
   - Si vous développez ou utilisez des applications basées sur des environnements comme Python, Node.js, etc., utilisez des gestionnaires de version comme `pip` ou `npm` pour gérer les mises à jour des bibliothèques et des dépendances.

Sécurité des systèmes d'exploitation

Utilisation de comptes avec privilèges minimaux

Les principes de moindre privilège sont des principes de sécurité informatique visant à limiter les droits et les privilèges des utilisateurs, des applications et des processus au niveau minimum nécessaire pour accomplir leurs tâches spécifiques.

Sécurité des systèmes d'exploitation

Utilisation de comptes avec privilèges minimaux

1. **Privilèges administratifs restreints :**

- Limitez l'accès administratif aux seules personnes et aux seules ressources nécessaires pour effectuer des tâches administratives spécifiques. Évitez de donner des droits d'administration complets à des utilisateurs qui n'en ont pas besoin.

2. **Contrôle d'accès basé sur le rôle (RBAC) :**

- Utilisez le RBAC pour attribuer des droits d'accès en fonction des rôles spécifiques des utilisateurs dans l'organisation. Cela garantit que chaque utilisateur a uniquement les permissions nécessaires pour accomplir ses responsabilités.

Sécurité des systèmes d'exploitation

Utilisation de comptes avec privilèges minimaux

3. **Principe du besoin de savoir :**

- Appliquez ce principe en limitant l'accès à l'information uniquement aux personnes qui ont besoin de connaître cette information pour effectuer leur travail.

4. **Examen des privilèges :**

- Passez régulièrement en revue les privilèges accordés aux utilisateurs et aux applications pour vous assurer qu'ils restent pertinents et nécessaires.

Sécurité des systèmes d'exploitation

Utilisation de comptes avec privilèges minimaux

5. **Privilèges par défaut :**

- Configurez les systèmes et les applications avec les privilèges par défaut les plus bas possibles, puis accordez des privilèges supplémentaires au cas par cas, si nécessaire.

6. **Surveillance et audit :**

- Surveillez l'utilisation des privilèges et auditez régulièrement les activités des utilisateurs et des applications pour détecter toute anomalie ou utilisation abusive.

Sécurité des systèmes d'exploitation

Utilisation de comptes avec privilèges minimaux

Sécurité des systèmes d'exploitation

Contrôle des accès

- Les modèles de contrôle d'accès sont essentiels pour gérer et restreindre l'accès aux ressources d'un système informatique.
- Les principaux modèles de contrôle d'accès : Discretionary Access Control (DAC), Mandatory Access Control (MAC) et Role-Based Access Control (RBAC).

Sécurité des systèmes d'exploitation

Contrôle des accès

1. Discretionary Access Control (DAC)

Définition:
Le modèle de contrôle d'accès discrétionnaire (DAC) est un modèle où les propriétaires de ressources ou d'objets ont le pouvoir de décider qui peut accéder à leurs ressources et avec quels privilèges.

Caractéristiques:

- **Flexibilité** : Les utilisateurs ont la liberté de partager leurs ressources avec d'autres.
- **Contrôle par l'utilisateur** : Le contrôle d'accès est basé sur les identités des utilisateurs et les permissions définies par les propriétaires des ressources.
- **Permissions basées sur les fichiers** : Les permissions sont souvent gérées par les propriétaires des fichiers et des répertoires.

Sécurité des systèmes d'exploitation

Contrôle des accès

Exemple:
Environnement UNIX/Linux où les propriétaires de fichiers peuvent définir les permissions d'accès pour leurs fichiers en utilisant des commandes comme `chmod`.

```
chmod 755 fichier.txt
```

Sécurité des systèmes d'exploitation

Contrôle des accès

2. Mandatory Access Control (MAC)

Définition:
Le modèle de contrôle d'accès obligatoire (MAC) est un modèle où l'accès aux ressources est contrôlé par des politiques de sécurité centralisées définies par l'administration système et non par les propriétaires des ressources.

Caractéristiques:

- **Centralisation** : Les décisions d'accès sont prises par un administrateur central et non par les utilisateurs individuels.
- **Labels de sécurité** : Les objets (fichiers, données) et sujets (utilisateurs, processus) sont assignés des labels de sécurité.
- **Politiques strictes** : Les politiques de sécurité sont strictes et non modifiables par les utilisateurs.

Sécurité des systèmes d'exploitation

Contrôle des accès

Exemple:
SElinux (Security-Enhanced Linux) est un exemple de mise en œuvre de MAC où les politiques de sécurité sont définies par l'administrateur et appliquées strictement.

```
sestatus
```

Sécurité des systèmes d'exploitation

Contrôle des accès

3. Role-Based Access Control (RBAC)

Définition:
Le modèle de contrôle d'accès basé sur les rôles (RBAC) est un modèle où les permissions sont associées à des rôles spécifiques et les utilisateurs se voient attribuer ces rôles. Les utilisateurs obtiennent les permissions en fonction de leurs rôles.

Caractéristiques:

- **Rôles et Permissions** : Les permissions sont assignées à des rôles plutôt qu'à des utilisateurs individuels.
- **Gestion simplifiée** : La gestion des permissions est simplifiée en attribuant ou retirant des rôles aux utilisateurs.
- **Séparation des responsabilités** : Facilite la séparation des responsabilités et la conformité réglementaire.

Sécurité des systèmes d'exploitation

Contrôle des accès

Exemple :

- Pour des contrôles d'accès plus fins que ceux offerts par les permissions de base (rwx), utilisez les ACL pour définir des permissions sur des fichiers et des répertoires spécifiques.
- Cela permet de limiter l'accès en fonction des besoins spécifiques des rôles.

Utilisation de setfacl pour ajouter des ACL :

```
setfacl -m u:utilisateur1:rw fichier.txt
```

Sécurité des systèmes d'exploitation

Contrôle des accès

Sécurité des systèmes d'exploitation

Désactivation des services inutiles

La désactivation des services inutiles et la fermeture des ports non utilisés sur Linux sont des pratiques essentielles pour renforcer la sécurité et réduire la surface d'attaque de votre système

Sécurité des systèmes d'exploitation

Désactivation des services inutiles

- **Principes de la désactivation des services inutiles :**
  - **Moins de services** en cours d'exécution signifie moins de points d'entrée potentiels pour les attaquants.
  - Chaque service ou processus actif représente une surface d'attaque supplémentaire pour des vulnérabilités potentielles.
  - En désactivant **les services non essentiels**, vous réduisez la probabilité qu'un service mal configuré ou non mis à jour soit exploité pour compromettre votre système.

Sécurité des systèmes d'exploitation

Désactivation des services inutiles

Sécurité des systèmes d'exploitation

Chiffrement des données

- Le chiffrement est une technique essentielle en sécurité informatique pour protéger les données contre l'accès non autorisé.
- Il existe deux principaux types de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Sécurité des systèmes d'exploitation

Chiffrement des données

Définition:
Le chiffrement symétrique utilise une seule clé pour chiffrer et déchiffrer les données. Cette clé doit être partagée entre les parties communicantes de manière sécurisée.

Caractéristiques:

- **Clé Unique** : La même clé est utilisée pour le chiffrement et le déchiffrement.
- **Rapidité** : Les algorithmes de chiffrement symétrique sont généralement plus rapides et nécessitent moins de ressources que les algorithmes asymétriques.
- **Sécurité de la Clé** : La sécurité repose entièrement sur le secret de la clé. Si la clé est compromise, les données chiffrées le sont également.

Sécurité des systèmes d'exploitation

Chiffrement des données

Définition:
Le chiffrement symétrique utilise une seule clé pour chiffrer et déchiffrer les données. Cette clé doit être partagée entre les parties communicantes de manière sécurisée.

Caractéristiques:

- **Clé Unique** : La même clé est utilisée pour le chiffrement et le déchiffrement.
- **Rapidité** : Les algorithmes de chiffrement symétrique sont généralement plus rapides et nécessitent moins de ressources que les algorithmes asymétriques.
- **Sécurité de la Clé** : La sécurité repose entièrement sur le secret de la clé. Si la clé est compromise, les données chiffrées le sont également.

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Sécurité des réseaux

Sécurité des systèmes d'exploitation

C'est quoi ?

La sécurité des réseaux est un domaine essentiel en informatique qui vise à protéger les données et les infrastructures contre les menaces et les accès non autorisés.

Sécurité des systèmes d'exploitation

Protocoles de sécurité (HTTPS, SSL/TLS, IPsec)

HTTPS (HyperText Transfer Protocol Secure)

- **Fonctionnement :** HTTPS combine le protocole HTTP avec SSL/TLS pour chiffrer les données échangées entre le client et le serveur, assurant ainsi la confidentialité et l'intégrité des informations.
- **Exemple pratique :** Lorsque vous accédez à un site bancaire en ligne, la connexion utilise HTTPS pour protéger vos informations financières.

Sécurité des systèmes d'exploitation

Protocoles de sécurité (HTTPS, SSL/TLS, IPsec)

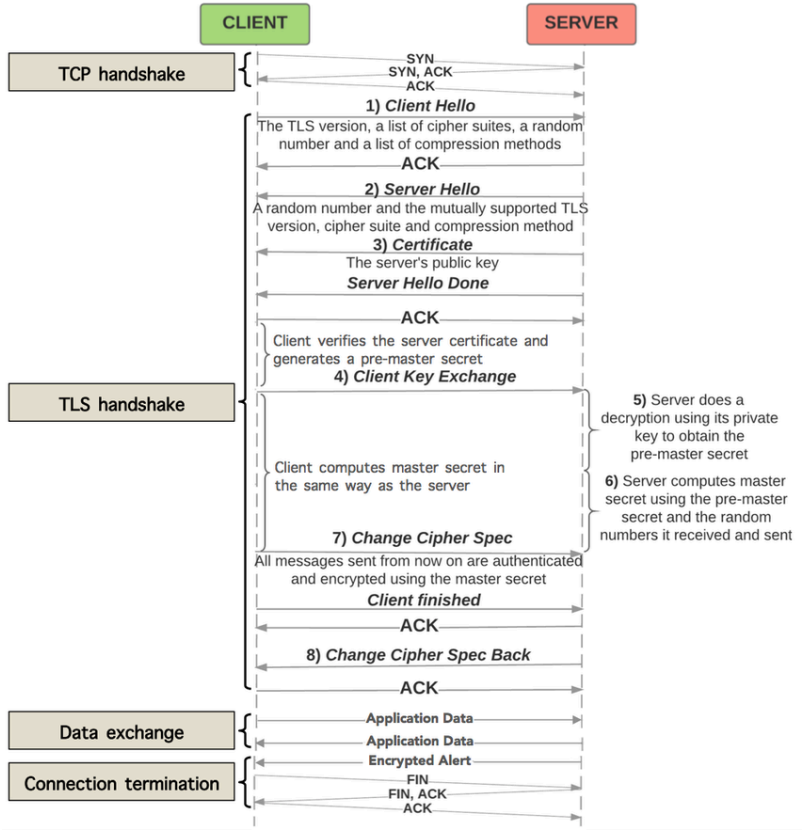
SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- **Fonctionnement :** SSL/TLS établit une connexion sécurisée en utilisant des certificats et des clés de chiffrement pour sécuriser les communications.
- **Exemple pratique :** Les sites web qui affichent un cadenas dans la barre d'adresse du navigateur utilisent SSL/TLS pour sécuriser la connexion.

Sécurité des systèmes d'exploitation

Protocoles de sécurité (HTTPS, SSL/TLS, IPsec)

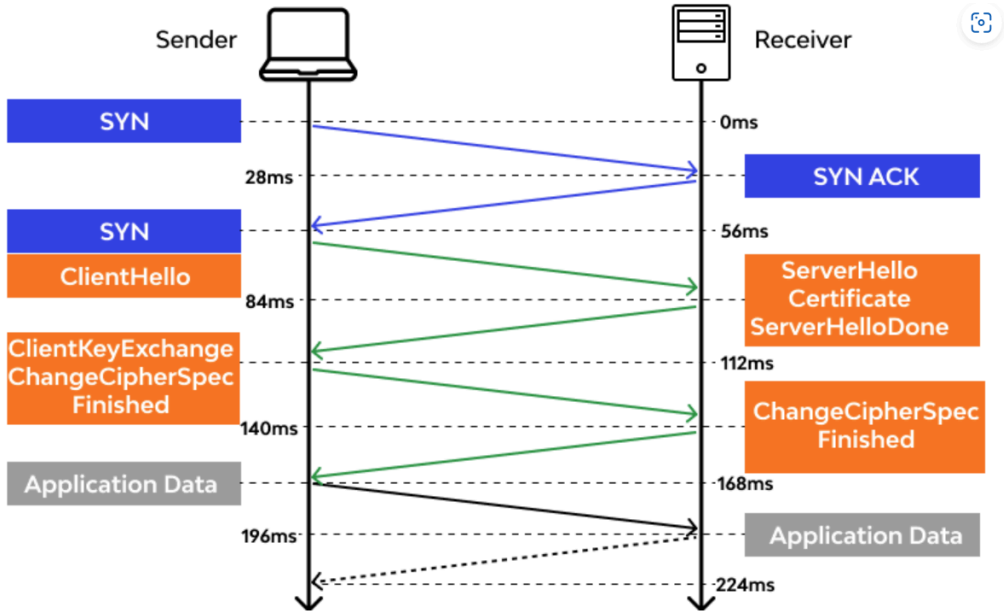
SSL/TLS (Secure Sockets Layer / Transport Layer Security)



Sécurité des systèmes d'exploitation

Protocoles de sécurité (HTTPS, SSL/TLS, IPsec)

SSL/TLS (Secure Sockets Layer / Transport Layer Security)



Sécurité des systèmes d'exploitation

Protocoles de sécurité (HTTPS, SSL/TLS, IPsec)

IPsec (Internet Protocol Security)

- **Fonctionnement :** IPsec sécurise les communications au niveau du réseau en chiffrant et en authentifiant chaque paquet de données.
- **Exemple pratique :** IPsec est souvent utilisé pour créer des réseaux privés virtuels (VPN), permettant aux employés de se connecter de manière sécurisée aux réseaux de l'entreprise à distance.

Sécurité des systèmes d'exploitation

Protocoles de sécurité (HTTPS, SSL/TLS, IPsec)

IPsec (Internet Protocol Security)