

Présenté par INDIA3

CYBER SECURITY

GF4GZ3W/HSEKGYK2IJXI9+3/LPFWW7AFT3+HOXJTSN4=





PLAN

- C'EST QUOI LA SÉCURITÉ ?
- POURQUOI LES SYSTÈMES SONT VULNÉRABLES ?
- POURQUOI LA SECURITE EST IMPORTANTE ?
- DEFINITION DE SECURITE, PROTECTION ET DISSUATION
- STRATEGIE DE SÉCURITÉ
- WHOIS : LE SERVICE DE RECHERCHE
- MENACES DE SÉCURITÉ COURANTE

C'EST QUOI LA SÉCURITÉ ?

La sécurité est un concept complexe et multidimensionnel qui englobe la protection contre les menaces, les dangers et les risques. Elle peut s'appliquer à de nombreux domaines de la vie, notamment la sécurité personnelle, la sécurité informatique, la sécurité alimentaire, la sécurité routière, la sécurité nationale, la sécurité environnementale, et bien d'autres.

En général, la sécurité vise à réduire ou à prévenir les dangers potentiels et à minimiser les risques pour les individus, les communautés ou les systèmes. Elle implique souvent la mise en place de mesures, de protocoles, de réglementations et de pratiques visant à garantir un environnement ou une situation plus sûre.



SÉCURITÉ VS SÛRETÉ

Sûreté :

1. Se concentre sur la prévention des actes intentionnels et malveillants.
2. Implique des mesures spécifiques pour contrer le terrorisme, le sabotage, etc.
3. Souvent associée à des domaines comme la sûreté aérienne ou nucléaire.

Sécurité :

1. Englobe une protection plus large contre les menaces et les risques, qu'ils soient accidentels ou intentionnels.
2. Peut s'appliquer à de nombreux domaines, y compris la sécurité informatique, alimentaire, routière, etc.
3. Vise à minimiser les dangers potentiels en général.



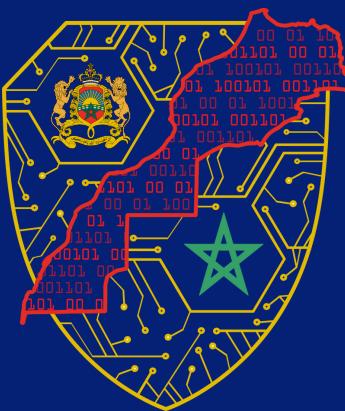
POURQUOI LES SYSTEMES SONT-ILS VULNERABLES ?

- Failles de logiciels
 - Injection SQL
 - Déni de service (Denial of Service, DoS)
- Évolution des menaces
- Utilisation de logiciels tiers
 - Navigateurs Web
- Mauvaise gestion des correctifs
 - Mise à jour
- Vulnérabilité matérielle
 - 👉 Porte d'entrée physique
 - 👉 Objets technologiques personnels
- Mauvaise gestion des privilèges (segmentation)
- Risque humain
 - 👉 Fishing
 - 👉 Mot de passe faibles
 - 👉 Non-respect des règles de sécurité
- IP Spoofing

NB : Faille distante VS Faille locale

IMPORTANTE

- Adoption croissante des technologies numériques au Maroc.
- Dépendance du secteur public et privé à l'égard de ces technologies numériques.
- Interdépendance des infrastructures critiques, augmentant la vulnérabilité.
- Risque potentiel pour la pérennité des institutions et la souveraineté nationale.
- Nécessité de répondre de manière adéquate aux besoins de sécurité des infrastructures numériques et des utilisateurs.
- Considération des dimensions humaine, juridique, économique et technologique dans la réponse à ces besoins de sécurité.
- Objectif : instaurer la confiance dans le numérique.
- Potentiel pour stimuler le développement économique bénéfique pour tous les membres de la société.



ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

DGSSI, CNDP

المملكة المغربية
٢٠١٨ | ٥٤٠٤٣٦
Royaume du Maroc



اللجنة الوطنية لمراقبة حماية المعلومات ذات الطابع الشخصي
CNPD | CNCDP | CNODC | CNCC | CNCDI
Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel

Définition de la sécurité, protection et dissuasion



DEFINITIONS

1

SÉCURITÉ DES SYSTÈMES D'INFORMATION

La sécurité des systèmes d'information est une discipline qui cherche à prévenir et à gérer les menaces et les risques qui pèsent sur les systèmes informatiques et les données. Elle repose sur trois principes fondamentaux : Confidentialité , Intégrité , Disponibilité.



PROTECTION DES SYSTÈMES D'INFORMATION

La protection des systèmes d'information englobe les pratiques et les technologies visant à renforcer la sécurité des systèmes contre une variété de menaces, notamment les logiciels malveillants, les attaques par déni de service (DDoS), les intrusions, etc.

Voici quelques aspects de la protection : Technologies de sécurité, Politiques de sécurité, Formation et sensibilisation



DISSUASION DANS LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

La dissuasion vise à rendre les attaques moins attrayantes pour les attaquants potentiels en créant un environnement où le risque et les conséquences sont élevés. Voici quelques stratégies de dissuasion :

Affichage des mesures de sécurité ,Démonstration de capacités de défense, Avertissements juridiques.



**comment une organisation peut-elle
élaborer et mettre en œuvre une
stratégie efficace pour protéger ses
données et ses systèmes informatiques ?**



Sennouni Dina

STRATEGIE DE SECURITE

- **Évaluation des Risques et des Vulnérabilités:**

La première étape est une évaluation minutieuse des risques et des vulnérabilités. L'organisation doit identifier les actifs critiques, tels que les données sensibles et les systèmes essentiels, et évaluer les menaces potentielles auxquelles elle est exposée. Cette analyse de risque permet de hiérarchiser les priorités en matière de sécurité.

Exemple : Prenons l'exemple d'une institution financière. Elle identifie comme risque potentiel les attaques de phishing visant à voler les informations bancaires de ses clients.



Sennouni Dina

STRATEGIE DE SECURITE

- Développement de Politiques de Sécurité:

Une fois les risques identifiés, l'organisation doit élaborer des politiques de sécurité claires et adaptées à ses besoins spécifiques. Cela comprend la définition de règles pour la gestion des mots de passe, la classification des données, l'accès aux systèmes, la protection physique des équipements, etc. Ces politiques servent de cadre pour la mise en place des mesures de sécurité.



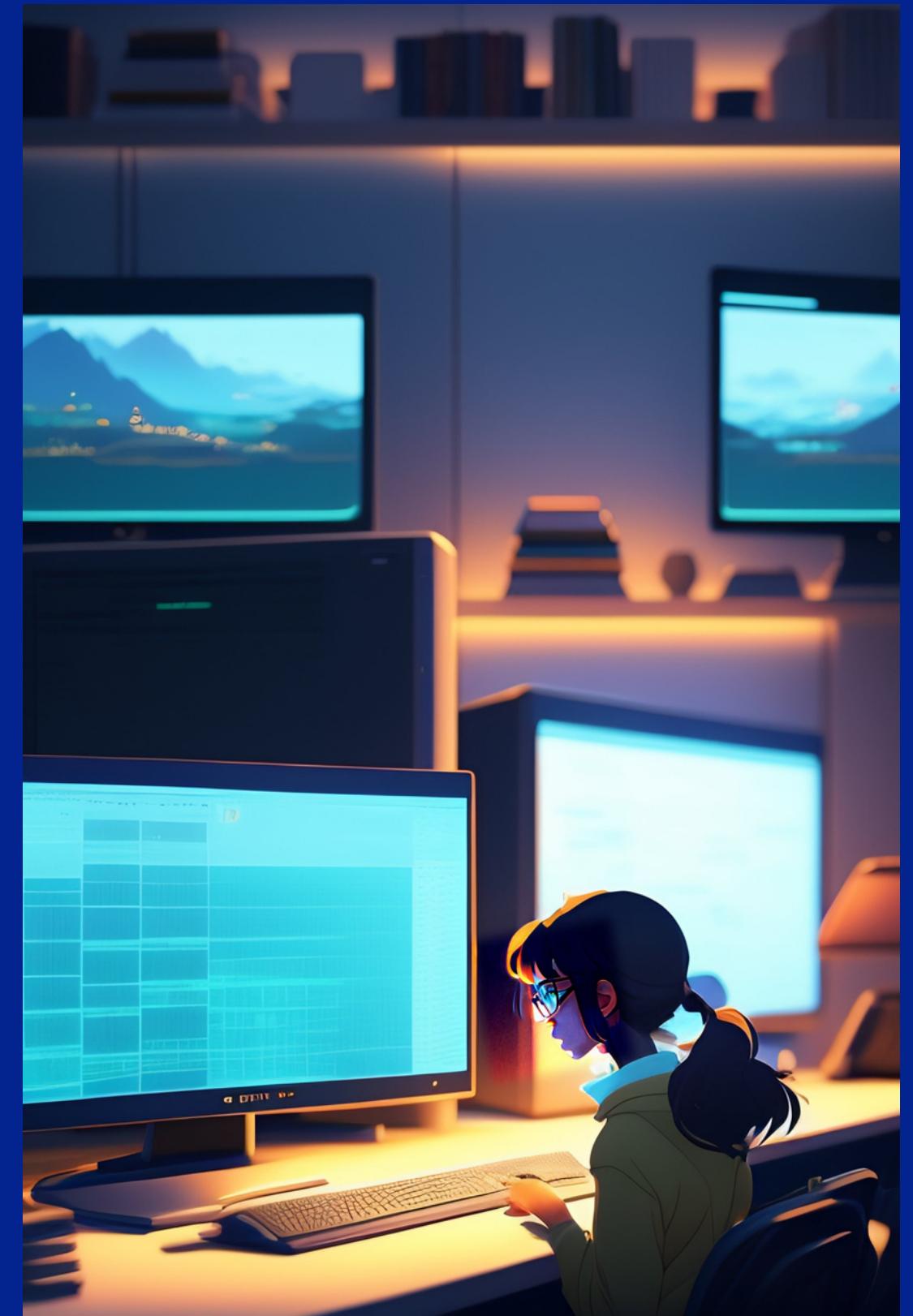
Sennouni Dina

STRATEGIE DE SECURITE

- Mise en Place de Mesures de Protection :

Les politiques de sécurité ne sont efficaces que si elles sont mises en pratique. L'organisation doit mettre en place des mesures de protection techniques, telles que les pare-feu, les antivirus, les systèmes de détection d'intrusions, ainsi que des mécanismes de contrôle d'accès et de chiffrement des données. Ces mesures contribuent à prévenir les attaques et à réduire les risques.

Exemple : Notre entreprise de cloud computing décide d'implémenter une combinaison de pare-feu pour bloquer les attaques DDoS et de chiffrement des données pour protéger les informations sensibles stockées sur ses serveurs.

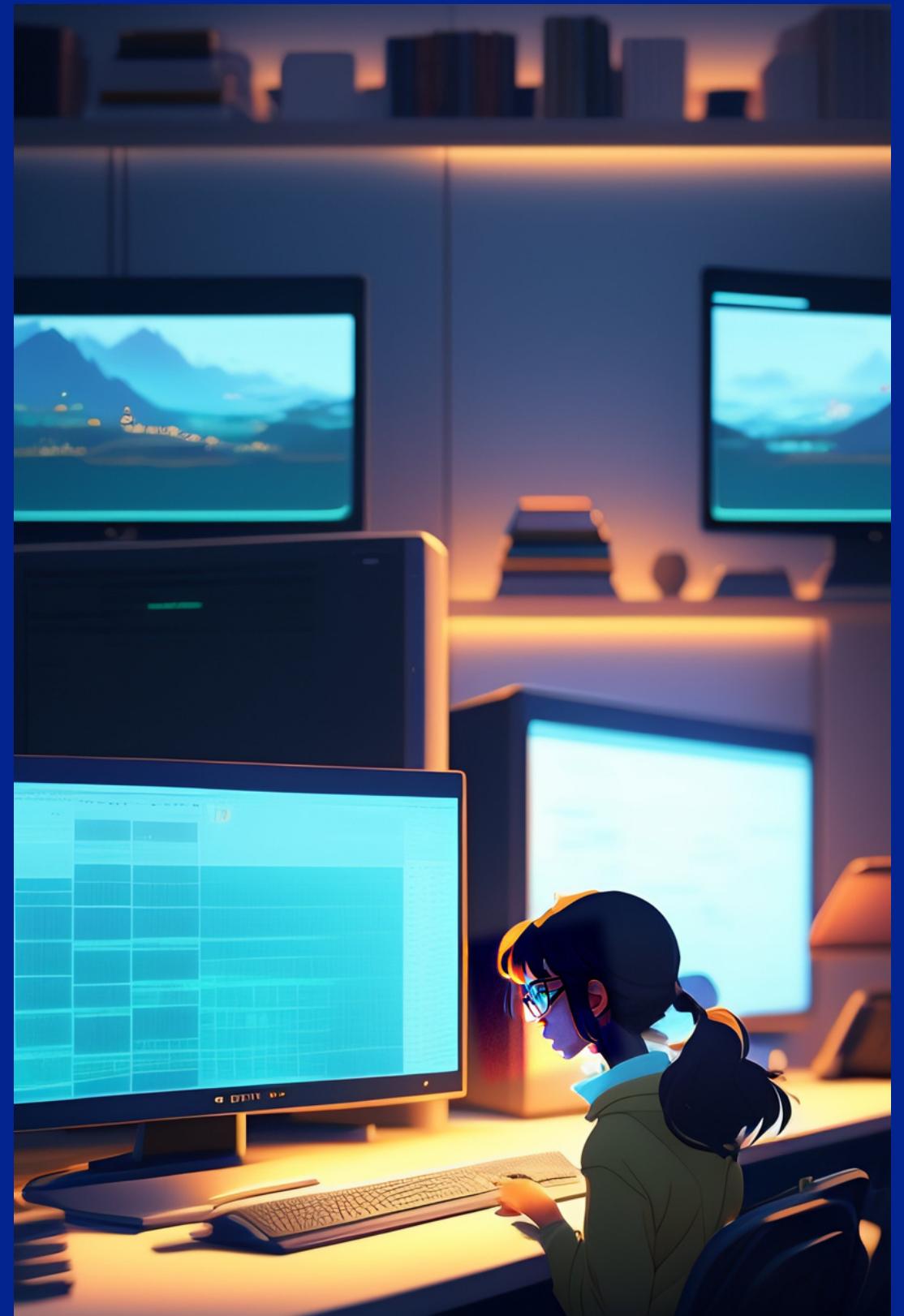


Sennouni Dina

STRATEGIE DE SECURITE

- Sensibilisation et Formation des Employés :

Les employés sont souvent la première ligne de défense contre les menaces à la sécurité. Il est donc essentiel de les sensibiliser aux risques et de les former pour qu'ils puissent reconnaître les signes d'attaques potentielles et adopter des pratiques sécurisées. Un personnel bien informé est un atout précieux pour renforcer la sécurité.

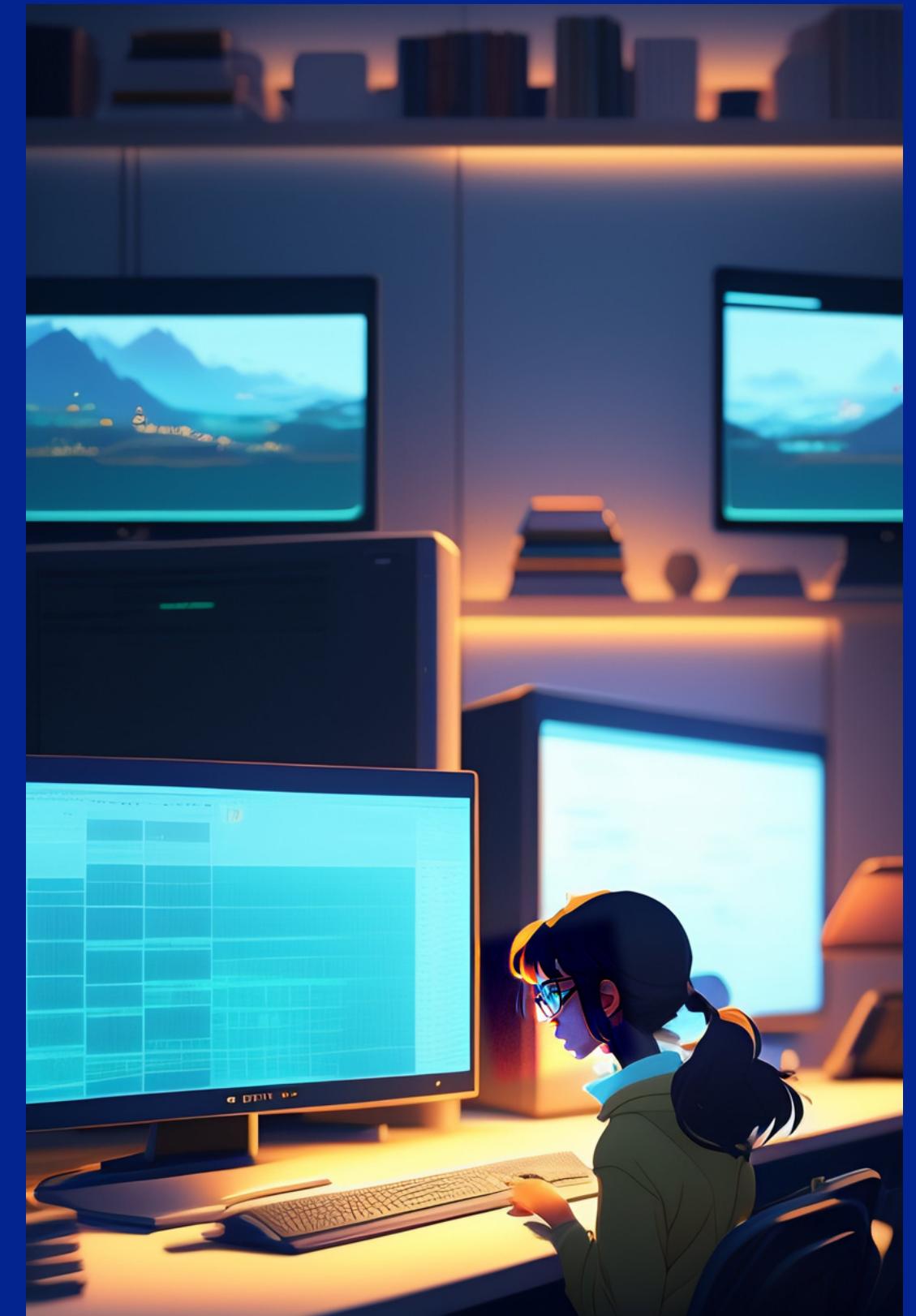


Sennouni Dina

STRATEGIE DE SECURITE

- Évolution et Adaptation Continue :

Enfin, la sécurité des systèmes d'information n'est pas un processus statique. Les menaces évoluent constamment, de nouvelles vulnérabilités sont découvertes, et les technologies changent. Par conséquent, une organisation doit continuellement évaluer et adapter sa stratégie de sécurité pour rester efficace face aux menaces émergentes.



Sennouni Dina

WHOIS : LE SERVICE DE RECHERCHE

DEFINITION

Whois est un service Internet qui permet aux utilisateurs d'obtenir des informations détaillées sur les noms de domaine, les adresses IP et d'autres ressources en ligne. Il joue un rôle essentiel dans la gestion, la sécurité et la transparence d'Internet. Cette définition approfondie vous guidera à travers son fonctionnement, ses utilisations et son importance.

```
~ $ whois 91.198.174.2
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '91.198.174.0 - 91.198.174.255'

inetnum:          91.198.174.0 - 91.198.174.255
netname:          WIKIMEDIA-EU-NET
descr:            Wikimedia Foundation Inc.
country:          NL
org:              ORG-WFI1-RIPE
admin-c:          MBE96-RIPE
tech-c:           MBE96-RIPE
tech-c:           RT744-RIPE
status:           ASSIGNED PI
mnt-by:           RIPE-NCC-HM-PI-MNT
mnt-lower:        RIPE-NCC-HM-PI-MNT
mnt-by:           WIKIMEDIA-MNT
mnt-routes:       WIKIMEDIA-MNT
mnt-domains:      WIKIMEDIA-MNT
source:           RIPE # Filtered
```

HISTORIQUE

- Le besoin de Whois est né avec la création d'Internet dans les années **1960** et **1970**.
- Les premiers systèmes Whois étaient manuels, gérés par un réseau restreint de chercheurs d'informations sur les noms de domaine.
- En **1982**, le RFC 812 de l'Internet Engineering Task Force (IETF) a formalisé le protocole Whois, établissant un standard pour la recherche d'informations sur les ressources Internet.
- En **1993**, l'InterNIC (Network Information Center) a été créé pour gérer la distribution des noms de domaine de premier niveau (TLD) et a mis en place un service Whois centralisé pour ces domaines.
- Avec l'expansion rapide d'Internet, la demande de services Whois a augmenté de manière exponentielle, nécessitant une amélioration constante du service.
- En **1998**, l'InterNIC a été privatisé, et de nombreuses entreprises privées ont commencé à offrir des services Whois concurrents.
- Au fil des ans, diverses réglementations ont été mises en place pour protéger la vie privée des titulaires de noms de domaine tout en fournissant un accès public aux informations Whois.
- De nos jours, les services Whois évoluent constamment pour s'adapter aux besoins changeants de la communauté Internet et pour se conformer aux réglementations de protection des données.

FONCTIONNEMENT

Whois est un protocole de recherche d'informations sur les noms de domaine, les adresses IP et d'autres ressources Internet.

- Interrogation de bases de données :
 - Les utilisateurs envoient des requêtes Whois aux serveurs Whois appropriés en utilisant le protocole TCP/IP sur le port 43.
- Données fournies :
 - Les informations disponibles via Whois incluent le nom du propriétaire, les coordonnées de contact, les serveurs de noms, la date de création et d'expiration du domaine, etc.
- Bases de données Whois :
 - De nombreuses bases de données Whois sont gérées par des registraires de noms de domaine, des registres nationaux et d'autres entités.
- Protocole standardisé :
 - Whois est basé sur un protocole standard, ce qui garantit la cohérence et la compatibilité des résultats.

UTILISATION

```
WHOIS(1)                                     Debian GNU/Linux

NAME
    whois - client for the whois directory service

SYNOPSIS
    whois [ { -h | --host } HOST ] [ { -p | --port } PORT ] [ -a
    ATTR[,ATTR]... ] [ -s SOURCE[,SOURCE]... ] [ -T TYPE[,TYPE]...
        whois -q KEYWORD
        whois -t TYPE
        whois -v TYPE
        whois --help
        whois --version

DESCRIPTION
    whois searches for an object in a RFC 3912 database.

    This version of the whois client tries to guess the right server
    can be made it will connect to whois.networksolutions.com for N
    and network names.

OPTIONS
    -h HOST, --host=HOST
        Connect to HOST.
    Manual page whois(1) line 1 (press h for help or q to quit)
```

- Recherche de propriétaires de domaines : Vérifier et mettre à jour les informations associées à les domaines.
- Gestion de la sécurité : Surveiller les activités suspectes, lutter contre la fraude en ligne et détecter le cybersquatting.
- Résolution de litiges :Identifier les propriétaires en conflit.
- Vérification de la disponibilité des domaines : vérifier si un nom de domaine est disponible à l'enregistrement.
- Conformité réglementaire : garantir la conformité des opérateurs de domaines aux règles et réglementations établies.

CONCLUSION

Whois demeure un pilier de l'infrastructure d'Internet, offrant un accès précieux aux informations essentielles concernant les noms de domaine, les adresses IP et d'autres ressources en ligne.

Bien que son rôle évolue pour respecter les normes de protection de la vie privée, il reste un outil indispensable pour la gestion, la sécurité et la transparence du monde numérique.

Menaces de sécurité informatique courantes

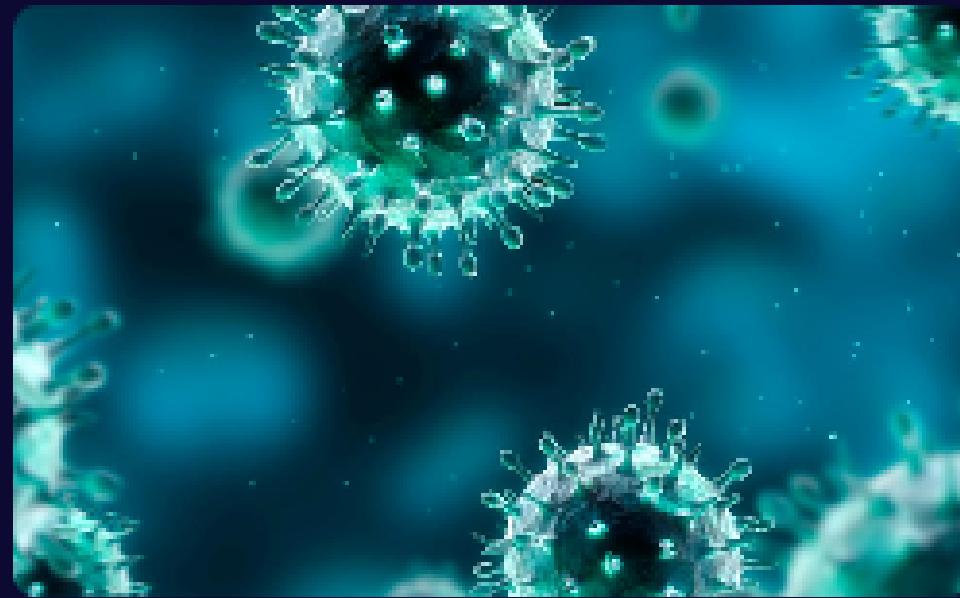
La sécurité informatique est l'un des enjeux les plus importants de notre époque. Dans cette présentation, nous allons explorer les menaces les plus courantes, les attaques réussies ainsi que les moyens de se protéger contre ces menaces.

Présenté par:

- EL HAJJI MAROUANE
- DAH ABDALLAHI



Les types courants de menaces



Virus

Un programme malveillant qui s'installe sur votre ordinateur pour endommager le système et vos données personnelles.



Phishing

Une technique qui consiste à tromper les utilisateurs pour qu'ils fournissent des informations sensibles telles que des mots de passe ou des numéros de carte de crédit.



Ransomware

Un type de logiciel malveillant qui bloque l'accès à vos fichiers et réclame une rançon pour débloquer l'accès.

Comment les attaquants exploitent les vulnérabilités

Ingénierie sociale

Les attaquants utilisent des tactiques de manipulation psychologique pour tromper les utilisateurs et leur faire divulguer leurs informations personnelles.

Vulnérabilités des logiciels

Les attaquants exploitent les failles dans les programmes ou les systèmes d'exploitation pour accéder aux informations sensibles.

Mot de passe faible

Les attaquants tentent d'accéder aux comptes en utilisant des mots de passe courants ou devinant les mots de passe faibles.

Les exemples de cyberattaques réussies



Sony Pictures Entertainment

En 2014, les données de Sony Pictures Entertainment ont été piratées, révélant des informations sensibles sur les employés et les partenaires commerciaux.



Equifax

En 2017, Equifax, l'une des principales agences d'évaluation du crédit, a été piratée, compromettant les informations personnelles de millions de personnes.



Yahoo

En 2013 et 2014, Yahoo a subi deux cyberattaques massives, exposant les informations personnelles de plus de 1 milliard d'utilisateurs.

Les conséquences des violations de données

1

Pertes financières

Les entreprises subissent souvent des coûts considérables pour réparer les dommages causés par les violations de données.

2

Réputation ternie

Les violations de données peuvent avoir des répercussions sur la réputation d'une entreprise, ce qui peut affecter la confiance des clients et des partenaires commerciaux.

3

Impact personnel

Les individus peuvent subir des préjudices tels que l'usurpation d'identité et le vol de données personnelles.

Comment se protéger contre les cybermenaces

Mettre à jour régulièrement les logiciels

Les mises à jour comprennent souvent des correctifs pour les vulnérabilités connues.

Utiliser des mots de passe forts et uniques

Les mots de passe doivent être suffisamment complexes pour résister aux attaques de devinettes.

Naviguer en toute sécurité

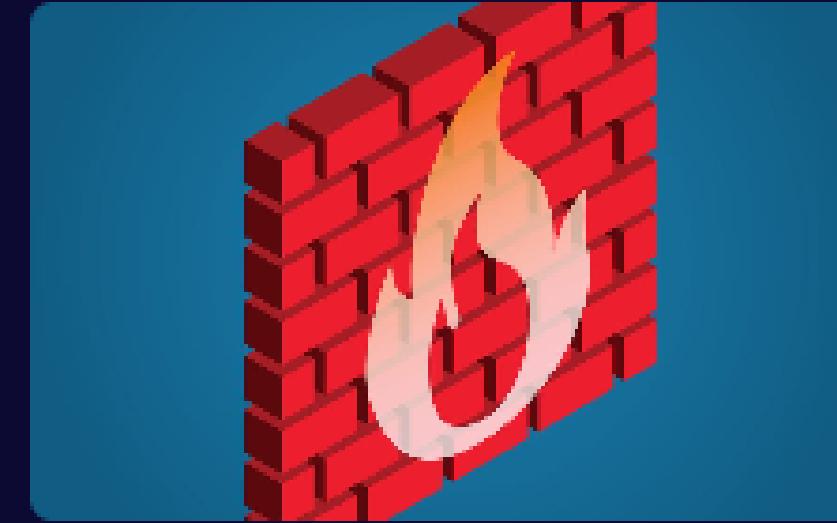
Les utilisateurs doivent être conscients des menaces potentielles, telles que les sites de phishing, et utiliser un logiciel antivirus de qualité.

Les meilleures pratiques de sécurité informatique



Authentification à deux facteurs

Une méthode de sécurité supplémentaire pour les comptes qui nécessitent une deuxième forme d'identification, tel qu'un code envoyé par SMS.



Pare-feu

Un pare-feu peut aider à bloquer les attaquants en empêchant l'accès non autorisé à un réseau.



Sauvegarde de données

Les données critiques doivent être sauvegardées régulièrement pour minimiser les effets potentiels des violations de données.

Conclusion et résumé des points principaux

- 1 Les types courants de menaces de sécurité informatique**
- 2 Comment les attaquants exploitent les vulnérabilités**
- 3 Les exemples de cyberattaques réussies**
- 4 Les conséquences des violations de données**
- 5 Comment se protéger contre les cybermenaces**
- 6 Les meilleures pratiques de sécurité informatique**

La sécurité informatique reste un enjeu majeur pour les entreprises et les utilisateurs. En prenant des mesures préventives pour protéger vos informations, vous pouvez réduire les risques de violations de données et les répercussions qui s'en suivent.

Présenté par INDIA3

TD 2 :

GF4GZ3W/HSEKGYK2IJXI9+3/LPFWW7AFT3+HOXJTSN4=





PLAN

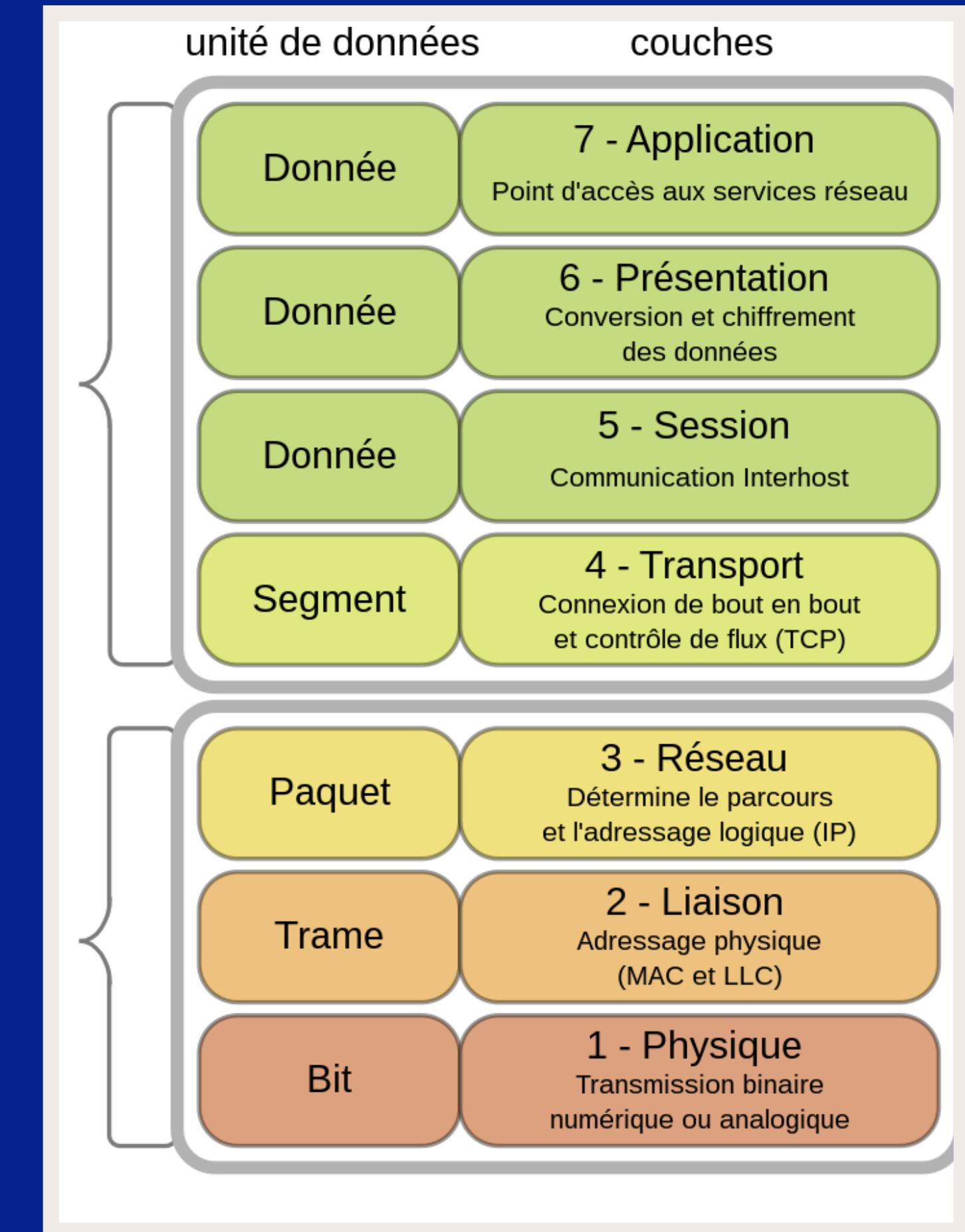
- ARCHITECTURE DE SECURITE OSI
- LES SERVICES DE SECURITE
- LES MECANISMES DE SECURITE
- MODELE DE SECURITE RESEAU
- DOCUMENTS RECOMMANDES



ARCHITECTURE OSI

Norme de communication, en réseau, **de tous les systèmes informatiques**, qui décrit les **fonctionnalités nécessaires à la communication et l'organisation de ces fonctions**

Proposé par l'**ISO (Organisation internationale de normalisation)** et conçu en 1970



LES FONCTIONS DES DIFFERENTES COUCHES

	PDU	Couche		Fonction
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment / Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit / Symbole	1	Physique	Transmission des signaux sous forme numérique ou analogique

VULNERABILITES

Couche	Vulnérabilités
7 Application	- Vulnérabilités logicielles - Attaques par injection SQL
6 Présentation	- Attaques par injection de code - Attaques de déchiffrement
5 Session	- Vol de session - Interruption de session
4 Transport	- Attaques de déni de service (DoS) - Séquence d'attaque TCP/IP
3 Réseau	- Attaques par déni de service (DoS) - Attaques de détection d'adresse IP
2 Liaison	- Empoisonnement ARP - Attaques d'usurpation d'adresse MAC
1 Physique	- Interception de signal - Accès physique non autorisé

MÉCANISMES ET PROTOCOLES DE SÉCURITÉ OSI

Protocoles de sécurité :

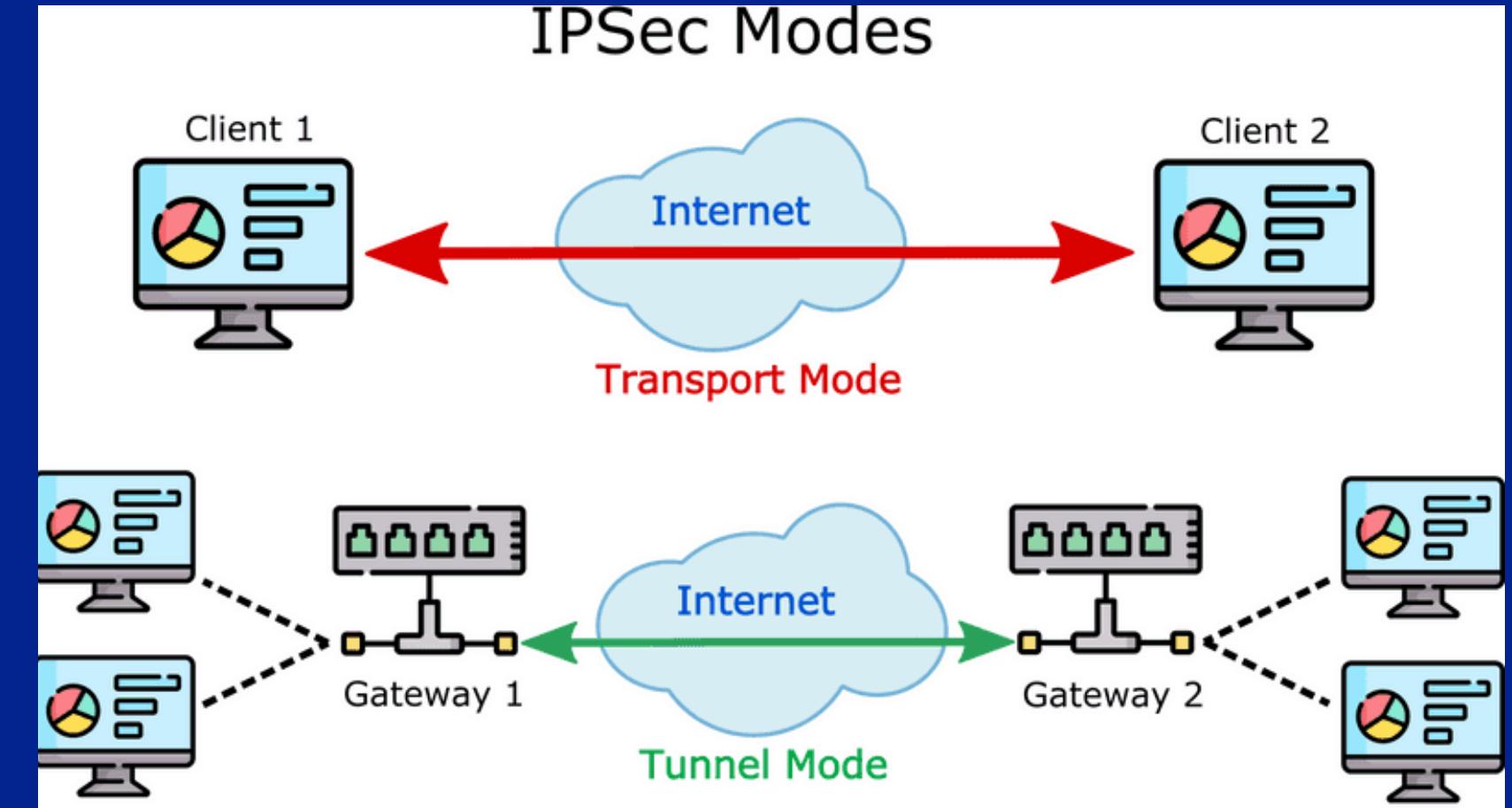
AU NIVEAU DE LA COUCHE RÉSEAU

IPsec, ou Internet Protocol Security :

- Ensemble de protocoles et de normes de sécurité utilisés pour sécuriser les communications sur des réseaux IP (Internet Protocol).

Un VPN, ou Virtual Private Network :

- Service ou une technologie qui vous permet de créer une connexion Internet sécurisée et privée, même lorsque vous utilisez un réseau public, comme une connexion Wi-Fi dans un café ou un aéroport.



HOW A VPN WORKS



MÉCANISMES ET PROTOCOLES DE SÉCURITÉ OSI

Protocoles de sécurité :

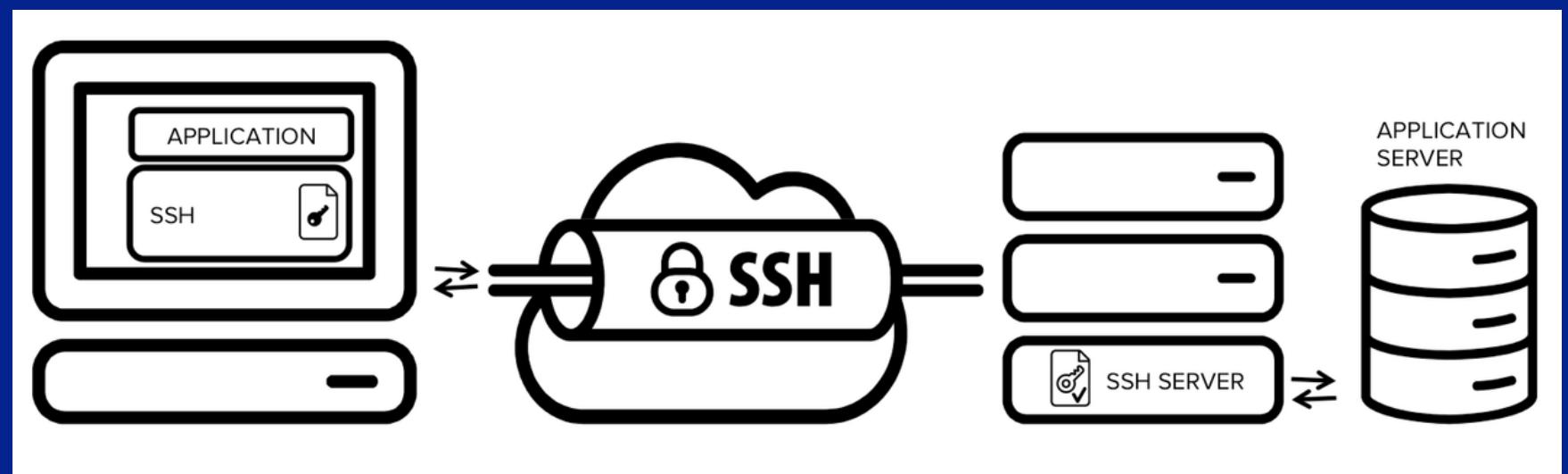
AU NIVEAU DE LA COUCHE TRANSPORT

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

- Une technologie de cryptage utilisée pour sécuriser les communications sur Internet, en particulier les transactions en ligne et les échanges de données sensibles, comme les informations de carte de crédit.

SSH (Secure Shell) :

- Un protocole de sécurité utilisé pour établir des connexions sécurisées avec des serveurs distants, généralement pour l'administration à distance d'ordinateurs ou de serveurs.



MÉCANISMES ET PROTOCOLES DE SÉCURITÉ OSI

Gestion de la Sécurité OSI

GESTION DES CLÉS

La gestion des clés est essentielle pour assurer la confidentialité des données.

Lorsque des données sont chiffrées pour être protégées pendant leur transmission, elles sont converties en un format illisible sans la clé appropriée.

- Génération des clés.
- Stockages des clés sécurisé.
- Distribution des clés contrôlée.
- Mis à jour des clés régulièrerie.



MÉCANISMES ET PROTOCOLES DE SÉCURITÉ OSI

Gestion de la Sécurité OSI

SURVEILLANCE ET AUDIT

La surveillance et l'audit sont des activités de surveillance visant à détecter toute activité anormale ou non autorisée sur le réseau ou dans les systèmes. Cela permet de repérer rapidement les éventuelles menaces à la sécurité.

- Surveillance continue.
- Audit régulier.
- Alertes et réponses.



MÉCANISMES ET PROTOCOLES DE SÉCURITÉ OSI

Normes et Organisations de sécurité OSI

ISO / IEC

**Organisation internationale de
normalisation et d'électrotechnique :**

Organisations internationales indépendantes, collaborent pour établir des normes techniques, y compris dans les domaines de la sécurité des systèmes informatiques et des réseaux.



MÉCANISMES ET PROTOCOLES DE SÉCURITÉ OSI

Normes et Organisations de sécurité OSI

ITU-T

**Union internationale des
télécommunications - Secteur de la
normalisation des télécommunications :**

L'ITU-T, agence de l'ONU, normalise les technologies de l'information et des communications à l'échelle mondiale, avec un accent sur les télécommunications, l'interopérabilité des systèmes et les protocoles de communication.



Les services de sécurité informatique



Présenté par:

- EL HAJJI MAROUANE
- CHAHIR BILAL

LES SERVICES DE SÉCURITÉ

- **Définition :**

La sécurité informatique est essentielle pour protéger nos données et prévenir les cyberattaques. Découvrez les différents services disponibles pour garantir l'**authentification, le contrôle d'accès, la confidentialité, l'intégrité des données, la non répudiation, le service de disponibilité.**



L'authentification

- Identification

L'authentification permet de vérifier l'identité d'un utilisateur ou d'un système.



- Facteurs

Les méthodes d'authentification peuvent inclure des mots de passe, des empreintes digitales, ou des cartes d'accès.

- Renforcement

Les technologies telles que la double authentification renforcent la sécurité des systèmes.



Le contrôle d'accès



Politiques

Le contrôle d'accès définit les politiques qui permettent de restreindre l'accès aux ressources sensibles.



Technologies

Les technologies telles que les lecteurs de cartes et les claviers sécurisés garantissent un accès autorisé.



Attributs

Les attributs, tels que les rôles et les niveaux d'autorisation, déterminent les droits d'accès.

LA CONFIDENTIALITÉ DES DONNÉES



- **Cryptage**

Le cryptage des données protège leur confidentialité en les rendant illisibles sans clé de déchiffrement.

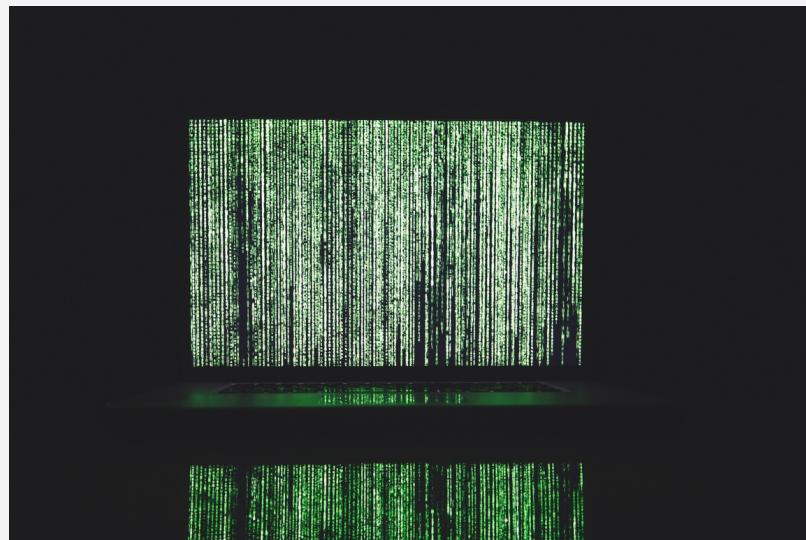
- **Règles de partage**

Les règles de partage des informations définissent qui peut accéder et partager les données.

- **Protection des communications**

Les protocoles sécurisés, tels que HTTPS, garantissent la confidentialité des échanges de données sur le réseau.

Intégrité des Données



Hachage

Les fonctions de hachage vérifient l'intégrité des données en générant une empreinte unique pour chaque fichier.

Contrôles d'intégrité

Les mécanismes de contrôle d'intégrité détectent toute altération non autorisée des données.

Sauvegardes

La création régulière de sauvegardes permet de restaurer les données en cas de perte ou de corruption.

NON-RÉPUDIATION

- Autorisation

L'autorisation garantit que les utilisateurs ne peuvent pas nier avoir réalisé une action.

- Systèmes de suivi

Les journaux d'activité et les signatures électroniques fournissent des preuves pour résoudre les litiges.

- Certificats numériques

Les certificats numériques permettent de valider l'identité d'une personne lors d'une transaction en ligne.



Disponibilité

- La disponibilité en sécurité informatique fait référence à la garantie que les systèmes, les services et les données sont accessibles et fonctionnent lorsque cela est nécessaire, sans interruption indue.
- La disponibilité en sécurité informatique peut être compromise par divers facteurs, tels que les attaques par déni de service (DDoS) visant à saturer les ressources d'un système



LES MÉCANISMES

DE SÉCURITÉ

Réaliser par:

RACHMOUN Khadija
BOUDEBZA Fatima



LES MÉCANISMES DE SÉCURITÉ

La sécurité informatique est un domaine essentiel pour protéger les systèmes informatiques, les données et les informations sensibles contre les menaces et les attaques.



LES MÉCANISMES DE SÉCURITÉ



Authentification :

L'authentification est le processus de vérification de l'identité d'un utilisateur ou d'un système. Les mécanismes d'authentification comprennent les mots de passe, les cartes à puce, les certificats numériques, les empreintes digitales, etc.

Autorisation :

L'autorisation détermine les actions qu'un utilisateur ou un système est autorisé à effectuer une fois qu'il est authentifié. Les systèmes utilisent des listes de contrôle d'accès (ACL) ou des rôles pour définir les autorisations.

LES MÉCANISMES DE SÉCURITÉ



Chiffrement :

Le chiffrement consiste à convertir des données en un format illisible sans une clé de déchiffrement appropriée. Il garantit la confidentialité des données lors de leur stockage et de leur transmission.

Pare-feu :

Un pare-feu est un dispositif matériel ou logiciel qui contrôle le trafic réseau entrant et sortant pour empêcher les intrusions et les attaques.

LES MÉCANISMES DE SÉCURITÉ



Détection d'intrusion :

les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) surveillent le trafic réseau et les activités du système pour détecter les activités suspectes et les attaques.

Gestion des journaux :

La collecte et l'analyse des journaux d'audit permettent de détecter les activités anormales et les tentatives d'intrusion.

LES MÉCANISMES DE SÉCURITÉ



Sécurité physique :

Protégez l'accès physique aux équipements informatiques en utilisant des serrures, des systèmes de surveillance et des contrôles d'accès.

Sensibilisation à la sécurité :

Éduquez les utilisateurs et le personnel sur les meilleures pratiques en matière de sécurité, y compris la création de mots de passe forts, la protection des informations sensibles et la détection des attaques par phishing.

LES MÉCANISMES DE SÉCURITÉ



Gestion des identités et des accès (IAM) :

La gestion des identités et des accès définit et contrôle les niveaux d'accès des utilisateurs aux systèmes et aux données.

Sécurité des applications:

Protégez les applications contre les vulnérabilités en utilisant des pratiques de développement sécurisé, telles que la validation des entrées, la protection contre les injections SQL et la gestion des sessions.

LES MÉCANISMES DE SÉCURITÉ



Sauvegarde et récupération :

Mettez en place des mécanismes de sauvegarde réguliers pour garantir la disponibilité des données en cas de défaillance ou de perte de données.

Sécurité des réseaux :

Protégez les réseaux contre les attaques en utilisant des techniques de segmentation, de surveillance du trafic et de cryptage.

DOCUMENTS RECOMMANDÉS



Réaliser par:

RACHIQ Ali

CHAKRANE Ismail

Tehranipoor, M., & Wang, C. (2011). Introduction to hardware security and trust. Springer Science & Business Media

Fournit les bases de la compréhension de la sécurité matérielle et de la confiance, qui sont devenues des préoccupations majeures pour la sécurité nationale au cours de la dernière décennie.

La couverture comprend les problèmes de sécurité et de confiance dans tous les types de dispositifs et systèmes électroniques tels que ASIC, COTS, FPGA, microprocesseurs / DSP et systèmes embarqués. Cela constitue une référence inestimable à la recherche de pointe qui revêt une importance cruciale pour la sécurité et la confiance dans les infrastructures soutenues par la microélectronique de la société moderne.

Mohammad Tehranipoor · Cliff Wang
Editors

Introduction to Hardware Security and Trust

 Springer

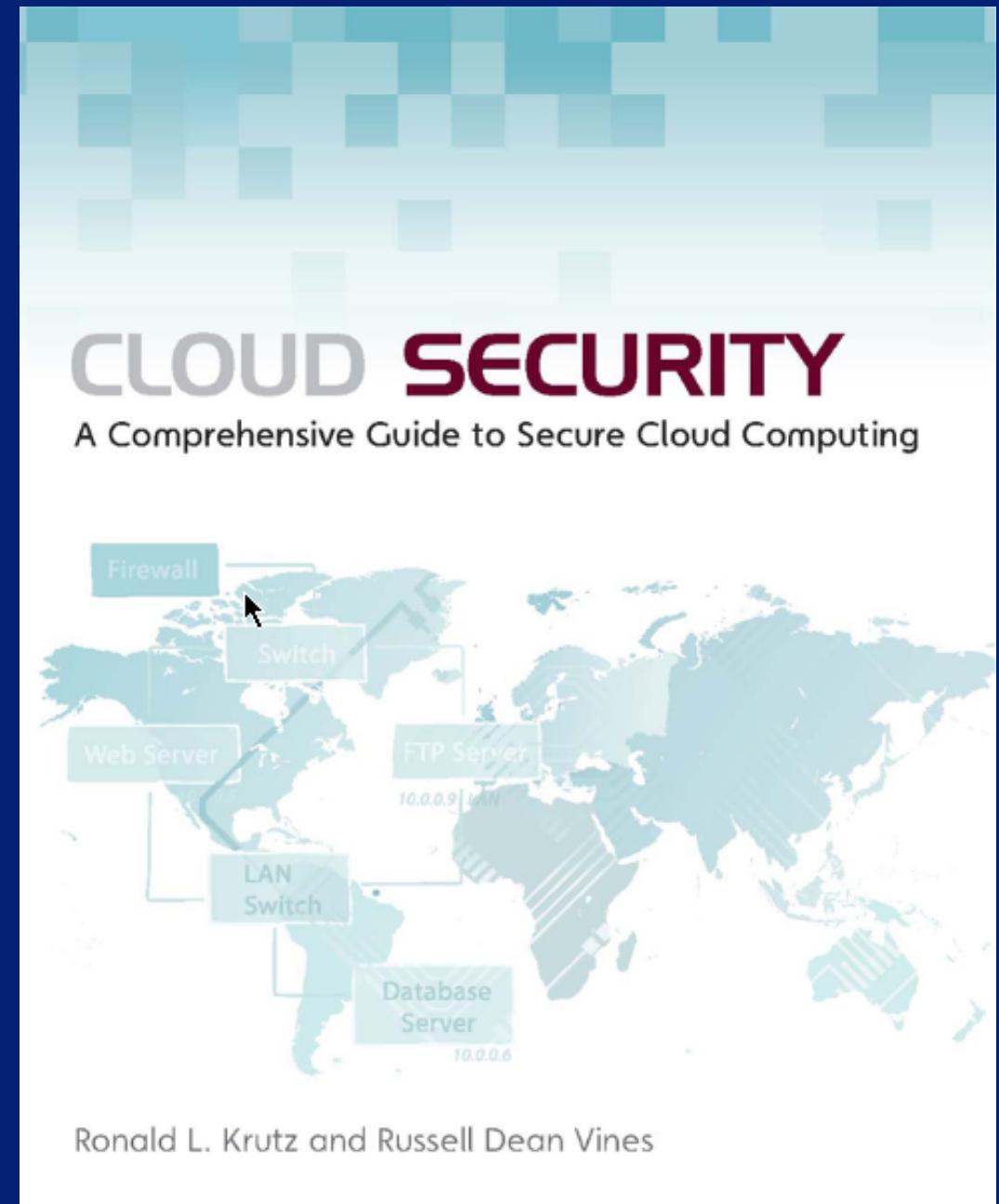
Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing
Wiley Publishing

Est intéressant si vous êtes impliqué dans n'importe quel aspect du cloud computing. Il offre une analyse approfondie des enjeux de sécurité liés à l'informatique en nuage.

Ce livre couvre une gamme diversifiée de sujets, de l'identification des menaces à la mise en œuvre de solutions de sécurité robustes dans le contexte du cloud computing.

Les auteurs mettent en lumière les meilleures pratiques, les techniques de chiffrement, les politiques de gestion des accès et bien d'autres aspects cruciaux pour garantir la protection des données et des systèmes dans un environnement cloud en constante évolution.

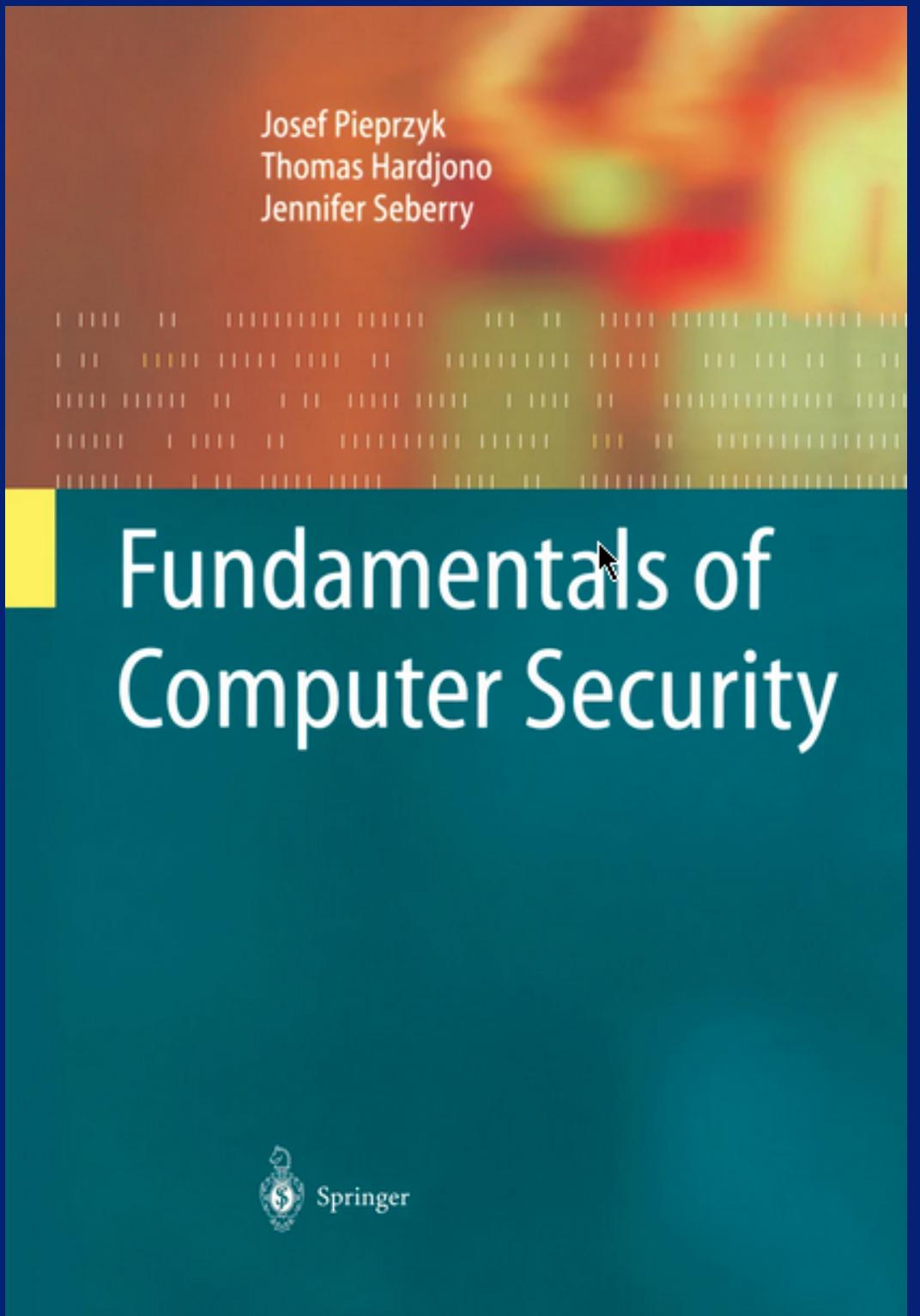
Ce guide sert de ressource précieuse pour les professionnels de la sécurité informatique, les administrateurs de systèmes, ainsi que pour tous ceux qui s'intéressent à la sécurisation des infrastructures cloud.



Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). Fundamentals of computer security
Springer Science & Business Media

Présente des concepts modernes de sécurité informatique. Il introduit l'arrière-plan mathématique de base nécessaire pour suivre les concepts de sécurité informatique.

Les développements modernes en cryptographie sont examinés, à partir du cryptage de clé privée et de clé publique, en passant par le hachage, les signatures numériques, l'authentification, le partage secret, la cryptographie axée sur le groupe, la pseudo-émanation, les protocoles clés d'établissement, les protocoles de connaissance zéro et l'identification.

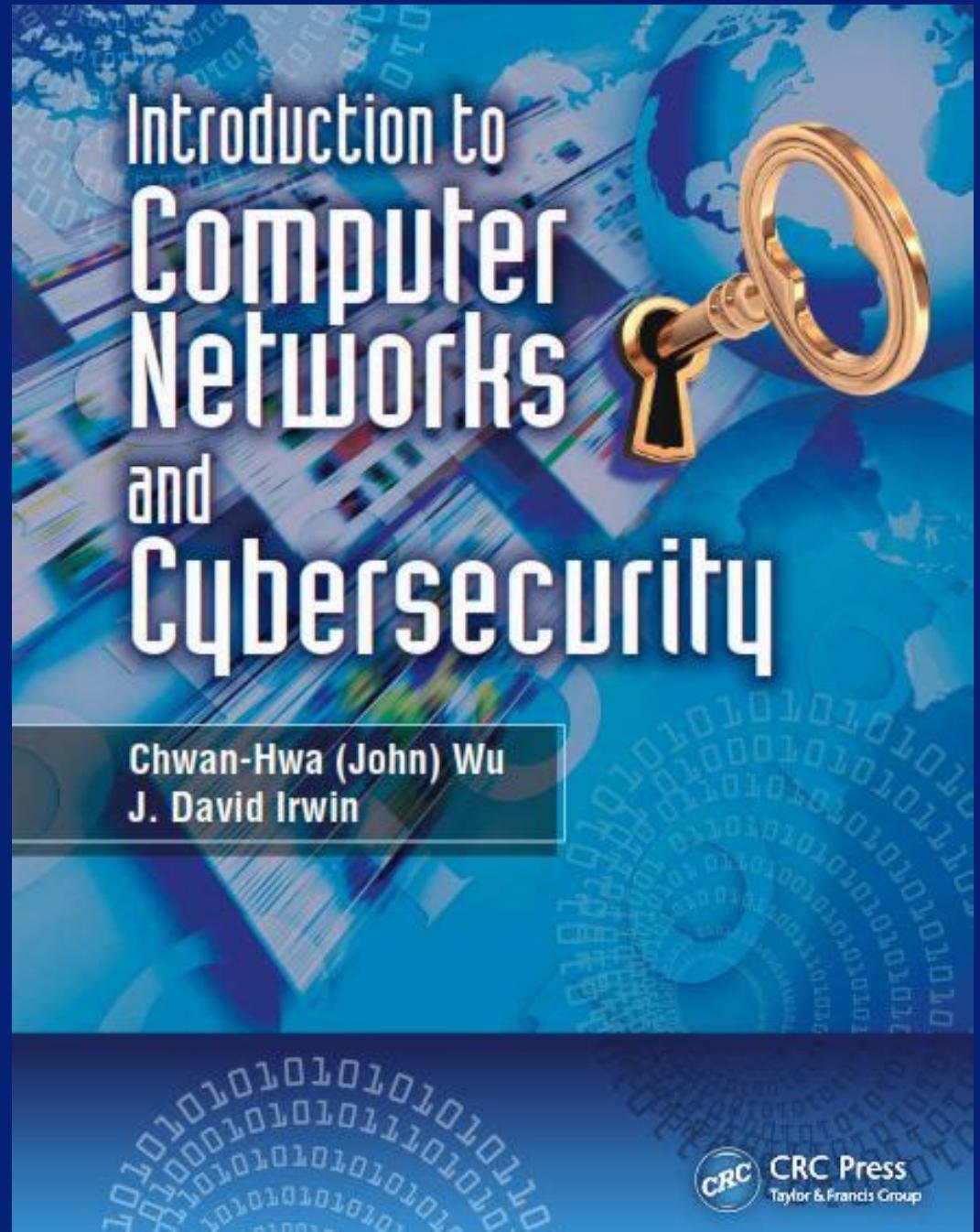


Wu, C. H. J., & Irwin, J. D. (2016). *Introduction to computer networks and cybersecurity*
CRC Press

Vous guide dans les principes fondamentaux, en commençant par la façon dont la plupart des personnes rencontrent d'abord des réseaux informatiques - à travers l'architecture Internet. La partie 1 couvre les applications Internet les plus importantes et les méthodes utilisées pour les développer.

La partie 2 traite du bord du réseau, composé d'hôtes, de réseaux d'accès, de réseaux locaux et de médias physiques utilisés avec les couches physiques et de liaison.

La partie 3 explore le noyau du réseau, y compris les commutateurs de paquets / circuits, les routeurs et le backbone Internet, et la partie 4 examine le transport fiable et la gestion de la congestion du réseau.



MERCI