Sécurité des réseaux

M. Jean DIOKH

Les concepts généraux

- Les objectifs de la sécurité
- Les principes de la sécurité
- Les moyens de la sécurité
- Les politiques de sécurité

Sécurité

Les attaques

- Le sniffing
- L'usurpation d'adresse IP - IP Spoofing
- Man-in-the-Middle - ARP Poisoning
- DNS Spoofing
- Déni de service – DoS

Sécurité

Architecture sécurisée des réseaux

Contrôle d'accès au réseau : port-security, Rogue DHCP

Liste de contrôle d'accès (ACLs), Translation d'adresses (NAT, PAT)

Sécurité des applications: SSH, DNS, WEB, Messagerie, VoIP

Les pare feux : Iptables, Firewalld, PortSentry, Fail2Ban

Les concepts généraux

Sécurité
Introduction à la sécurité

Les objectifs de la sécurité

La sécurité des systèmes d'information vise les objectifs suivants:

- **la confidentialité** : Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

- **l'intégrité**: Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante.

- **la disponibilité**: Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

Sécurité
Introduction à la sécurité

Les objectifs de la sécurité

D'autres aspects peuvent aussi être considérés comme des objectifs:

- **la traçabilité(ou « Preuve»)** : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

- **l'authentification**: L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

- **la non-répudiation**: Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Sécurité

Introduction à la sécurité

Les principes de la sécurité

Sécurité
Introduction à la sécurité

Les principes de la sécurité

Sécurité
Introduction à la sécurité

Les principes de la sécurité

- Le secret
- L'isolation
- L'authentification
- L'accréditation et la classification des documents (Top Secret, secret, confidentiel,….)
- Plusieurs lignes de défense
- La minimisation (moins il y a de portes dans une base secrète, plus elle est facile à garder)

Sécurité
Introduction à la sécurité

Les principes de la sécurité

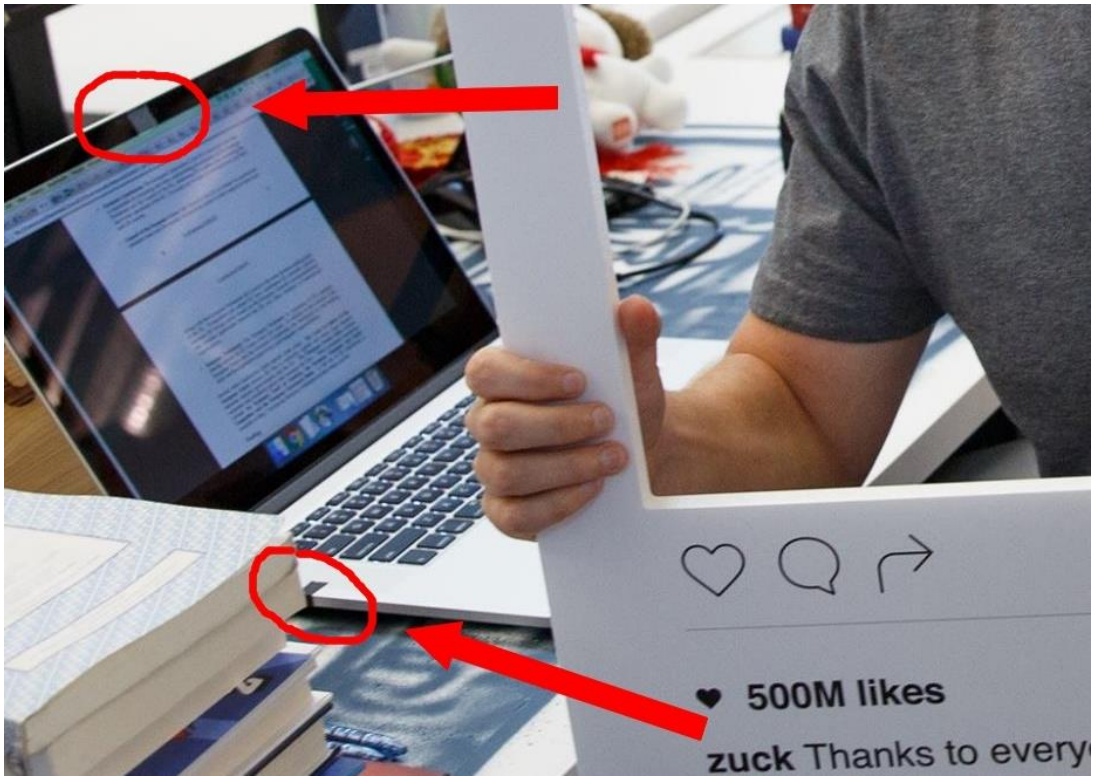
- La surveillance
- La formation, l'information, les sanctions

Sécurité
Introduction à la sécurité

Les moyens de la sécurité

Sécurité
Introduction à la sécurité

Les moyens de la sécurité



Sécurité
Introduction à la sécurité

Les moyens de la sécurité

- La sécurité physique
- Les systèmes d'authentification
- Les droits, privilèges
- La cryptologie

Sécurité
Introduction à la sécurité

Les moyens de la sécurité

- Les sommes de contrôle
- Les sauvegardes
- L’audit des principaux évènements

Les politiques de sécurité

- Identifier ce qu'il faut protéger
- Analyser les risques (faire l'audit, des essais d'intrusion)
- Pondérer les risques
- Evaluer les contraintes
- Choisir les moyens

Sécurité
Introduction à la sécurité

Les politiques de sécurité

- Adopter la politique de sécurité
- Tester (faire l'audit)