ISI - Sécurité Informatique

Leonard Cseres - Mars 2024

Loi Suisse

A.143 *Soustraction de données* : Appropriation intentionnelle et frauduleuse de données protégées.

A.143bis *Accès indu à un système informatique* : Accès non autorisé à des systèmes protégés, avec circulation de données punissable.

CIA Préservation de la confidentialité, intégrité et disponibilité de l'information

- **Confidentialité** : Seule les personnes autorisées peuvent accéder à l'information
- **Intégrité** : Protéger l'exactitude et la complétude de l'information
- **Disponibilité** : L'information est accessible par les personnes autorisées

SSI *Prévention*, *Détection*, *Réaction* (analyse et confinement), *Récupération*

3 domaines Sécurité physique, organisationnelle, technique

5 Couches (1) *Physique*, (2) *Réseau*, (3) *Protocoles*, (4) *Hosts* (systèmes d'exploitation), (5) *Application*

Contrôle d'accès - AAA Authentification (identité), Autorisation (droits), Accounting/audit (traçabilité)

Dommages Perte de CIA

5 Principles fondamentaux (1) Sécurité globale autant que le maillon le plus faible, (2) Sécurité parfaite impossible, (3) Sécurité processus pas un produit, (4) Sécurité complexité inversement proportionnelle, (5) Participation des utilisateurs

9 Règles fondamentales (1) Interdiction par défaut, (2) moindre privilège, (3) défense en profondeur, (4) séparation des fonctions, (5) segmentation (diversification), (6) économie de mécanismes (simplicité), (7) goulet d'étranglement (centralisation), (8) interruption/erreur sûre, (9) éviter la sécurité (transparence)

Types de menaces *Accidentelles*, *Environnementales*, *Délibérées*

Types de vulnérabilités *Matérielles*, *Logicielles*, *Réseaux*, *Personnelles*, *Physiques*, *Organisation*

Craquage de mot de passe *Brute force*, *Dictionnaire*, *Heuristique* (variations d'un dictionnaire), *Pré-génération*

$$N = \text{Alphabet}^{\text{Taille}} \qquad T_{moy} = \frac{N}{2}$$

Rainbow table Table de hachage pré-calculée (évite les collisions et optimise la probabilité de succès et le stockage)

Windows `c:\Windows\system32\config\SAM`

Linux `/etc/passwd` et `/etc/shadow` (root), sous forme `$type$salt$hash`

LM/NTLM Protocole d'auth. de Microsoft (pas salé) (1) **LAN & LM**: Win 9x/ME, (2) **LM & NTML**: Win NT/2K/XP/2003, (3) **NTLM**: Win Vista/7/8/10/11

Protection messagerie Utiliser des protocoles sécurisés (TLS), utiliser la messagerie sécurisée (PGP, GPG)

Maliciel Logiciel malveillant

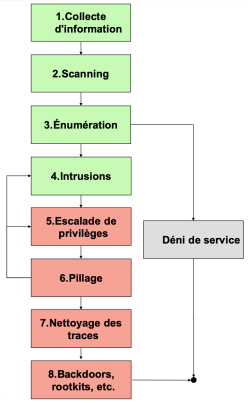
- **Virus** S'attache à d'autres programmes ou fichiers, on besoin de l'intervention de l'utilisateur pour se propager
- **Ver** Se propage via les réseaux et tout seul
- **Spyware** Collecte des informations sur l'utilisateur
- **Trojan** Se fait passer pour un logiciel légitime
- **Ransomware** Crypte et demande une rançon

Protection maliciels Vérification sur VirusTotal, antivirus, patch, backups, éducation

Pillage Vol d'informations et/ou d'argent

Backdoor Programme qui permet à des personnes non autorisées d'accéder à un système (introduit par un exploit, virus, ver, trojan, etc.)

RootKit Maliciel qui modifie le système d'exploitation pour cacher sa présence



Protocoles HTTP

```
GET /index.html HTTP/1.1
Host: www.example.com
HTTP/1.1 200 OK
Content-Type: text/html
```

Communication *Basique* (port TCP/UDP), *Évoluée* (canal caché + chiffré comme ICMP ping ou DNS), *Avancée* (injecte DLL et passe par IE pour aller chercher périodiquement ses ordres)

Attaques Web (1) Parcours d'arborescence, (2) Contournement côté client (cookies), (3) XSS (Cross-Site Scripting) *Reflected*: injecté dans l'URL, *Stored*: injecté dans la base de données, *DOM-based*: injecté dans le DOM, (4) Injection SQL, (5) CSRF (Cross-Site Request Forgery) forcer actions indésirées, (6) Clickjacking

Prévention

- Utilisation de requêtes préparées (prepared statements)
- Échappement des caractères spéciaux dans les entrées utilisateur (sanitation)
- Limitation des permissions des comptes de base de données utilisés par l'application
- Utilisation d'en-têtes de sécurité (e.g., Content Security Policy)
- **SAST** Static Application Security Testing (ex: *Semgrep*)
- **DAST** Dynamic Application Security Testing (ex: *ZAProxy*)

Sécurité OWASP

- **Top 10** (1) Broken Access Control (2) Cryptographic Failures (3) Injection (4) Insecure Design (5) Security Misconfiguration (6) Vulnerable and Outdated Components (7) Identification and Authentication Failures (8) Software and Data Integrity Failures (9) Security Logging and Monitoring Failures (10) Server-Side Request Forgery
- **Juice Shop** Un environnement vulnérable pour s'entraîner

---

Cryptographie Apporte la *Confidentialité*, *Authenticité*, *Intégrité* (pas de modification), *Non-répudiation* (ne peut pas nier de qui vient l'information)

- Cryptanalyse (décrypter une information sans connaître a priori la clé)
- Cryptologie (étude de la cryptographie et de la cryptanalyse)

Principe de Kerchhoff La sécurité d'un système cryptographique doit reposer sur la confidentialité de la clé et non sur celle de l'algorithme (sécurité par l'obscurité)

Algorithme de chiffrement/déchiffrement

- Cipher (clé symétrique/secrète)
- PK (clé asymétrique/publique)

Confidentialité parfaite L'adversaire ne peut rien apprendre de l'information chiffrée (jamais vrai en pratique)

Block Cypher Permutation mathématique d'un bloc de données en un autre bloc de même taille (opération inversible)

Stream Cypher Chiffrement bit à bit (opération non-inversible)

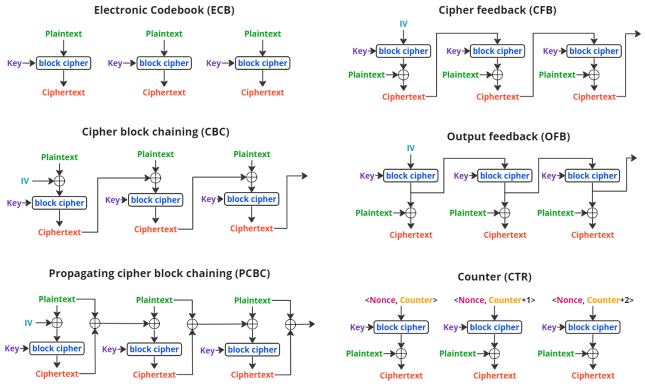
DES Block cypher de 64 bits avec une clé de 56 bits

Faiblesse 2^{56} clés possibles, trop facile à casser

3key-TDES $DES \rightarrow DES^{-1} \rightarrow DES$ (-1 garde la rétro-compatibilité)

AES Block cypher de 128 bits avec une clé de 128, 192 ou 256 bits

Modes de chiffrement



- *ECB*: Electronic Code Book, chaque bloc est chiffré séparément
- *CBC*: Cipher Block Chaining, chaque bloc est chiffré avec le bloc précédent (vecteur d'initialisation requis)
- *GCM*: Galois/Counter Mode, chiffrement par blocs avec authentification

Limitations chiffrement symétrique

- **Distribution des clés** Problème de distribution sécurisée des clés.
- **Nombre de clés** Nécessité d'une clé unique pour chaque paire de correspondants.
- **Sécurité des clés** Protection des clés nécessaire contre le vol ou la compromission.

Diffie-Hellman Échange de clés sans les échanger (clé publique) $f(x) = g^x \mod p$ avec g et p publics. x et y est choisi aléatoirement par chaque participant.

Chiffrement Asymétrique RSA, ECC (Elliptic Curve Cryptography)

- Moins performant que le chiffrement symétrique
- Repose sur la difficulté de certains problèmes mathématiques (factorisation pour RSA)

RSA Basé sur la difficulté de factorisation. Connaître une clé ne donne pas d'information sur l'autre clé (clé publique et privée)

- **Clé Publique** : (N, e)
- **Algorithme** :
  - Choisir deux nombres premiers aléatoires p et q de $\frac{l}{2}$ bits avec l la taille du modulus RSA.
  - Calculer $N = p \cdot q$ et $\phi(N) = (p-1)(q-1)$.
  - Trouver e tel que $1 < e < \phi(N)$ et e premier avec $\phi(N)$.
  - Calculer d tel que $d \cdot e \equiv 1 \pmod{\phi(N)}$.
  - **Chiffrement** : $c = m^e \mod N$
  - **Déchiffrement** : $m = c^d \mod N$

  e: exposant public, d: exposant privé, N: modulus, m: message, c: message chiffré

Note: e ne doit pas avoir de facteur commun avec $\phi(N)$

Authenticité et Intégrité

MAC code taille fixe généré par une fonction de hachage (HMAC), permet de prouver origine (authenticité) et vérifier l'intégrité

Non-répudiation Preuve d'origine et de livraison, l'expéditeur ne peut pas nier avoir envoyé le message

Signature Comme MAC avec non-répudiation

Intrusions Logicielles

Memory Overflow (1) Stack Overflow écrasement de variables locales, (2) Stack Smashing écrasement avec exécution de code, (3) Stack off-by-one dépassement d'un seul caractère, (4) Heap Overflow écrasement du tas

Manipulation d'entiers (1) Over/Underflow (Dépassement), (2) Signed/Unsigned (Conversion)

Format String Utilisation de la fonction `printf` pour lire ou écrire dans la mémoire

Contournement des protections mémoire

- **Return-to-libc** Exécution de code en appelant des fonctions de la libc
- **Return-oriented programming** Exécution de code en utilisant des fragments de code existants

Prévention Stack/heap non-exécutable, randomisation des adressage mémoire (ALSR), libraries sécurisées

---

Types ICMP : **0** => réponse echo ; **3** => destination inaccessible ; **5** => redirection ; **8** => echo ; **11** => temps dépassé.

Collecte d'informations (techniques ou non ; « examiner les lieux ») => créer un profil de l'organisation à attaquer. Ingénierie sociale (noms, tél., emails, rôles) ; Internet/Intranet (noms de domaine, DNS, IP) ; Accès à distance (VPN, WIFI) ; Extranet (partenaires, type/origine/destination des connexions).

Whois : service permettant d'obtenir des informations sur IP et noms de domaine ; interrogation des registres Internet. *whois heig-vd.ch*
Interrogation DNS : nslookup ; **Informations de transfert de zone / sur des hôtes non-accessibles** (serveur mail) : host, dig (questionnement des serveurs DNS => adresses IP, serveurs emails, serveurs DNS ; *dig "heig-vd.ch" ANY*). **Reconnaissance réseau** : traceroute/tracrt.
Protections : minimiser les informations sur le Web, rendre l'info inutilisable pour l'attaquant (infos générales dans les fichiers de config., noms génériques pour les contacts (info@organisation.com), désactiver les services inutiles) ; analyse de ce qui se trouve sur Internet.

Scanning : frapper les murs pour trouver toutes les fenêtres et portes (déterminer les machines, les services et les protocoles).
Machines : ping (messages ICMP souvent filtrés…) => envoi de paquets pour scanner les IP sur les ports.
Services : **1.** envoi d'un datagramme UDP à destination du port à scanner ; pas de réponse => port ouvert ; réponse « destination port unreachable » => port fermé ; *nmap -sU* ; **2.** TCP => si port ouvert : SYN => SYN-ACK => ACK ou RST ou Rien ; si port fermé : SYN => RST-ACK ; *nmap –sT* ou *nmap –sS* (pour le rien). Envoi à un port d'une application spécifique pour obtenir des infos : *nmap –sV*.
Envoi de **paquets forgés** pour interagir avec certaines caractéristiques (TTL) pour déterminer les systèmes ; *nmap –O*.
nmap –v –A 193.134.218.10 : commande tout-en-un.
Protections : màj, filtrages des messages ICMP, utilisation de pare-deux, utilisation de proxys inverses; évaluation de son propre système.
Enumération des ressources/utilisateurs/applications/vulnérabilités.

Intrusions : **Sniffing** (écoute du traffic ; infos sensibles ; promiscuous => écoute plus large, facile sur hubs,moins sur switchs), **Spoofing** (falsification d'identité (IP, MAC) ; facile pour UDP ; moins pour TCP (nécessite les bons numéros de séquence), **man-in-the-middle** (attaque ARP (IP/MAC) ; requêtes forgées => attaque Gratuitous ARP (remplissage du cache ARP => ne pas mettre à jour son cache lorsqu'une requête est reçue) et DNS à l'aide de **poisoning** (altération des données), **session hijacking**.