Résumé Complet du Cours d'Introduction à la Sécurité des Systèmes d'Information (IntroSSI)

La Cryptographie

Cryptographie Classique vs Moderne

- **Cryptographie classique** : Art d'écrire ou de résoudre des codes, initialement concentrée sur la communication privée entre deux parties utilisant des cryptages à clé privée.
- **Cryptographie moderne** : Conception, analyse et mise en œuvre de techniques mathématiques pour sécuriser les informations contre les attaques adverses. Champ d'application beaucoup plus large incluant l'intégrité des données, l'authentification, les protocoles, la communication de groupe.

Stéganographie

- Art de dissimuler un message dans un support innocent
- Différente de la cryptographie car le message secret est caché dans un contenu qui semble normal
- Exemples historiques : encre invisible, tatouages, micro-points
- Applications modernes : protection de droits d'auteur, distribution dissimulée de malwares, exfiltration de données
- **Technologies modernes de stéganographie** : codes d'identification des machines dans les imprimantes laser (points jaunes minuscules)

Principes Fondamentaux

- **Principe de Kerckhoff** (1883) : La sécurité d'un système cryptographique ne doit pas dépendre de l'algorithme mais uniquement de la clé. Pas de sécurité par obscurité.

Fonctionnement des Algorithmes de Chiffrement

- Deux composants principaux : une permutation et un mode d'opération
- **Permutation** : Fonction qui transforme un élément de manière à ce que chaque élément ait un inverse unique
- **Mode d'opération** : Algorithme utilisant une permutation pour traiter des messages de taille arbitraire

Chiffrements Classiques

1. **Chiffrement de César** : Déplace chaque lettre de trois positions dans l'alphabet
2. **Chiffrement de Vigenère** (16ème siècle) : Amélioration du chiffrement de César utilisant une clé composée de plusieurs lettres
3. **Null Cipher** (Chiffrement de dissimulation) : Technique cachant un message dans une grande quantité de données non pertinentes
4. **Dispositifs mécaniques historiques** : Cylindre de Jefferson, machine Enigma

Insécurité des Chiffrements Classiques

- Limités aux opérations manuelles (sur papier ou mentales)
- Facilement cassés par des programmes informatiques simples
- Ne peuvent utiliser qu'une petite fraction des permutations possibles

One-Time Pad (Masque Jetable)

- Chiffrement "parfait" avec secret absolu (théorisé par Claude Shannon)
- Utilise une clé aléatoire de même longueur que le message
- Opération XOR bit à bit : $C = P \oplus K$ (où C=chiffré, P=texte clair, K=clé)
- Inconvénient : chaque clé ne peut être utilisée qu'une seule fois
- Peu pratique car nécessite une clé aussi longue que le texte en clair
- Utilisations historiques : British Special Operations Executive (2ème Guerre mondiale), KGB, NSA

Cryptographie Moderne

Cryptographie Symétrique (à clé privée)

- Utilise une clé unique pour chiffrer et déchiffrer
- Nécessite un échange de clés entre l'expéditeur et le destinataire
- Exemples : DES, 3DES, AES, Twofish, Serpent, Blowfish, CAST5, RC6, IDEA

Cryptographie Asymétrique (à clé publique)

- Introduite par Martin Hellman et Whitfield Diffie en 1976
- Utilise deux clés : une publique (pour chiffrer) et une privée (pour déchiffrer)
- Principal avantage : pas besoin de distribuer une clé secrète
- Algorithmes : RSA, ECC (Cryptographie à courbe elliptique), ElGamal, Diffie-Hellman, DSS
- Applications : PGP, SSL, TLS

Fonctions de Hachage Cryptographiques

- Type de cryptographie sans clé
- Convertissent le texte en clair en une valeur unique et de longueur fixe (hash)
- Caractéristiques : fonction à sens unique, résistante aux collisions
- Bonnes fonctions : SHA-256, SHA-512, SHA-3
- Fonctions obsolètes : MD5, SHA-1

Signatures Numériques

- Utilisation d'algorithmes asymétriques pour créer des signatures
- Permettent de vérifier l'intégrité du message, d'authentifier l'expéditeur et d'assurer la non-répudiation
- Processus :
    1. L'expéditeur génère un hash du message et le chiffre avec sa clé privée
    2. Le destinataire utilise la clé publique pour déchiffrer la signature et vérifier le hash

Certificats Numériques

- Associent une clé publique à un individu

- Validés par une autorité de certification
- Utilisés comme forme d'identification électronique
- Infrastructure à clé publique (PKI) pour gérer les certificats à grande échelle

Protection des Données

- **Au repos** : Chiffrement intégral du disque (VeraCrypt, BitLocker, dm-crypt), sécurité physique
- **En mouvement** : SSL/TLS, VPN (SSL, IPsec)
- **En cours d'utilisation** : Chiffrement homomorphique, chiffrement interrogeable

Collecte de Données et Surveillance sur le Web

Services Collectant des Informations

- **Types d'informations collectées** :
    - Comptes et paramètres de configuration
    - Identité
    - Données d'achat
    - Stockage dans le cloud (fichiers, emails, photos, blogs, sites web)
    - Sites web visités (via cookies de suivi)
    - Centres d'intérêt et historique de navigation
- **Grandes plateformes** : Facebook, Google collectent ces données pour l'extraction de données et la publicité ciblée

Cookies sur le Web

- **Définition** : Données locales (name=value) stockées dans le navigateur et envoyées au serveur
- **Fonctions** : Éviter de se reconnecter, suivre sessions/panier d'achat/préférences
- **Types** :
    - **Cookies standard** : Associés au site (politique du "same-origin")
    - **Cookies de suivi (tiers)** : Intégrés via publicités/images 1x1 pixel, permettent le suivi inter-sites

    - Exemple : via les ressources intégrées, un site de tracking (suismoi.sn) peut collecter l'historique de navigation

Anonymat et Protection sur Internet

Navigation Privée

- **Fonctionnalités** :
    - N'envoie pas de cookies stockés
    - N'autorise pas la définition de cookies
    - N'utilise/n'enregistre pas les informations de remplissage automatique
    - Ne conserve pas d'informations sur le contenu téléchargé
    - Supprime les pages en cache et l'historique en fin de session
- **Limites** :
    - L'adresse IP reste visible pour les serveurs web
    - Les FAI connaissent toujours l'identité et les domaines accédés
    - Les serveurs DNS savent quelles adresses sont recherchées
    - Les proxies, pare-feux et routeurs enregistrent le trafic

Suivi des Appareils Mobiles

- Appareils mobiles recherchant les dispositifs Bluetooth et points d'accès Wi-Fi
- Diffusion d'adresses MAC pouvant être suivies
- Solution d'Apple : fournir une adresse MAC différente à chaque nouvelle connexion

Types de Web

- **Surface Web** : Contenu indexé par les moteurs de recherche traditionnels
- **Deep Web** : Contenu non indexé, souvent issu de pages générées dynamiquement (bibliothèques, bases de données gouvernementales)
- **Dark Web** : Partie intentionnellement cachée du Deep Web, nécessitant des logiciels spéciaux comme Tor
    - Utilise des pseudo-domaines .onion
    - Héberge des services légitimes et illicites

The Onion Router (Tor)

- Permet une navigation anonyme
- Utilise un réseau de relais mondiaux (~6 900) géré par des organisations à but non lucratif
- Environ 2 millions de clients, acheminant des centaines de Go/seconde
- Développé initialement par le U.S. Naval Research Laboratory (1995)
- Projet Tor fondé en 2006 avec le soutien de l'EFF
- Fonctionnement : routage en oignon avec cryptage en couches multiples

I2P (Invisible Internet Project)

- Alternative à Tor utilisant le "routage en ail" (Garlic routing)
- Combine plusieurs messages à un relais
- Tunnels unidirectionnels (vs circuits bidirectionnels de Tor)
- Services : I2PTunnel (connectivité TCP), chat IRC, BitTorrent, iMule, I2P-Bote (email décentralisé), Syndie (blogs, forums)
- Plus orienté vers l'hébergement anonyme de services (vs accès anonyme de Tor)
- Utilise une table de hachage distribuée (DHT) pour localiser les informations

Communication P2P Sans Internet

- Réseaux maillés pair à pair utilisant Bluetooth
- Messages passant de téléphone en téléphone
- Utile lors de manifestations (Hong Kong 2019) ou dans des zones sans infrastructure Internet

Applications et Implications

- **Utilisations légitimes de l'anonymat** :
    - Éviter les conséquences (sociales, politiques, juridiques)
    - Accéder à des contenus dans des gouvernements oppressifs
    - Protéger les dissidents politiques et dénonciateurs
    - Éviter les services basés sur la géolocalisation
    - Cacher l'activité des entreprises

    - Préserver la confidentialité des recherches personnelles (santé, crédit)
- **Problèmes du Dark Web** :
    - Recherche difficile et mauvais résultats
    - Sites changeant constamment d'adresse pour éviter les attaques DDoS
    - Nombreuses arnaques et honeypots des forces de l'ordre
    - Blocage par les FAI
    - Exemples de fermetures : Silk Road 2.0 (2014), Silk Road 3.0 (2017), AlphaBay (2017), Hansa Market (2017)