Département Informatique
Master 1 RTIC
Année Universitaire 2022-2023

Chapitre 1

INTRODUCTION À LA SÉCURITÉ DES MULTIMÉDIA

Sommaire

- Introduction
- Cryptographie
- Stéganographie
- Tatouage
- Fingerprinting
- Digital Rights Management (DRM)

Introduction (1)

- La problématique liée à la sécurisation des communications répondait principalement à des besoins militaires et commerciaux.
-
- En effet, lorsque deux personnes géographiquement distantes veulent échanger une information confidentielle (comme un ordre martial), plusieurs questions se posent :

Introduction (2)

1. Comment être sûr qu'une personne mal intentionnée n'a pas eu accès au message pendant son transfert ?
2. Comment être sûr que le message n'a pas été modifié ?
3. Comment être sûr que la personne avec laquelle on communique est bien la bonne ?
4. Comment envoyer un message sans que l'adversaire puisse seulement se rendre compte qu'il y a eu transmission?
5. Comment s'assurer de la persistance du message dans le canal de transmission utilisé ?

Introduction (3)

- Afin d'illustrer ces différents scénarios, les cryptographes ont inventé un jeu de la sécurité qui a lieu entre trois personnages fictifs :

- X cherchera à transmettre une information à Y en cherchant à satisfaire un des points cités plus haut et l'adversaire Z essaiera de contourner cet objectif.

- Comme nous allons le voir par la suite,
  - la ***cryptographie*** permet de répondre aux trois premières questions,
  - la ***stéganographie*** à la quatrième,
  - et le ***tatouage*** à la cinquième.

Cryptographie

- ***La cryptographie*** obscurcit la signification d'un message de telle manière que le contenu devienne inintelligible et sans signification.
- La cryptographie se fonde sur la prétention que la protection est contrôlée par une clé secrète dont la valeur n'est pas connue aux attaquants.
- La cryptographie fonctionne aussi longtemps que l'attaquant n’est pas capable de savoir la clé secrète.

Stéganographie

- Si la *cryptographie* n'a pas pour but de cacher l'existence d'une communication entre deux individus ou entités,
- la ***stéganographie***, qui signifie « écriture cachée », est l'art de camoufler une information (message secret) dans une autre.
- L'information hôte peut ici désigner un autre message ou un contenu (image, audio, vidéo).
- toute personne n'ayant pas la clé secrète utilisée pour le camouflage des données ne pourra alors déceler la présence de ces données.

Tatouage

- Le tatouage (*watermarking*) est, comme la *stéganographie*, une technique permettant d'insérer une information de manière discrète dans un contenu.
- La *stéganographie* : discrétion de l'information cachée (une personne non autorisée n'est pas capable de déceler la présence de cette information).
- Le *tatouage :* discrétion imperceptible (non visible à l'oeil nu pour des contenus photos ou vidéos et non audible pour des sons).
- De plus, le but du tatouage ne sera pas de cacher l'existence d'une information cachée mais plutôt de protéger son insertion contre des manipulations du contenu.
- Le *tatouage* sert à étiqueter la propriété de l'auteur ou il peut être exploité à des fins de lecture sous-jacente parallèle par une machine annexe de façon que cette empreinte invisible ne gêne pas une lecture standard.

Fingerprinting

- **L'estampillage** ou traçage de traitres (*fingerprinting* ou *traitor tracing*) est une technique destinée à tracer les copies légales d'un contenu en insérant un identifiant propre au possesseur d'une copie.
- Si celle-ci est retrouvée sur un réseau d'échange (par exemple pair à pair), il sera alors possible d'identifier la personne responsable de sa diffusion.
- Le *fingerprinting* consiste à marquer les copies d'un contenu numérique que le distributeur veut fournir à ses utilisateurs.
- Chaque copie est marquée par le distributeur avec la séquence qui identifie un utilisateur spécifique,
- Un code est alors utilisé afin de tracer le responsable de la diffusion d'une copie non autorisée sur des réseaux d'échanges : téléchargement direct (Megaupload, Rapidshare, etc.) ou échange point à point (Emule, Torrents).

Gestion des droits numériques Digital Rights Management (DRM)

- Les DRM (*Digital Rights Management*) proposent des techniques afin de lutter contre la piraterie des oeuvres numériques.
- Ceux-ci permettent de limiter le nombre de copies qu'un utilisateur peut faire de son contenu acheté sur une plateforme légale
- ***DRM est une technologie qui protège et impose les droits liés à l'utilisation du contenu numérique, tel que les données de multimédia.***
- **Les fonctions les plus importantes de DRM sont:**
  - Empêcher l'accès non autorisé et la création des copies non autorisées du contenu numérique.
  - Fournir un mécanisme par lequel des copies peuvent être détectées et tracées (traçage du contenu).

fonctionnement du système DRM

Le fonctionnement global du système DRM est le suivant :

1. Le contenu est chiffré par le serveur de contenus à l'aide d'une clé (identifiant) avant l'envoi à l'utilisateur.
2. Le lecteur de contenus de l'utilisateur télécharge alors une licence après avoir vérifié que l'utilisateur a effectivement payé les droits.
3. La licence contient la clé secrète nécessaire à la lecture du contenu.

Utilisation du système DRM

- Parmi les sociétés utilisant des DRM sur leur plateforme de vente de contenus culturels, nous citerons par exemple *Apple*, *Microsoft* et *Adobe*.
- L'utilisation des DRM sur des contenus multimédia présente des défauts:
  - ✓ Chaque plateforme de contenus utilise son propre système de DRM, ceux-ci sont souvent non inter-opérables.
  - ✓ De plus, la valeur d'un contenu acheté dans un format propriétaire est discutable si ce format n'est pas lisible par les différents lecteurs de l'utilisateur. Ce