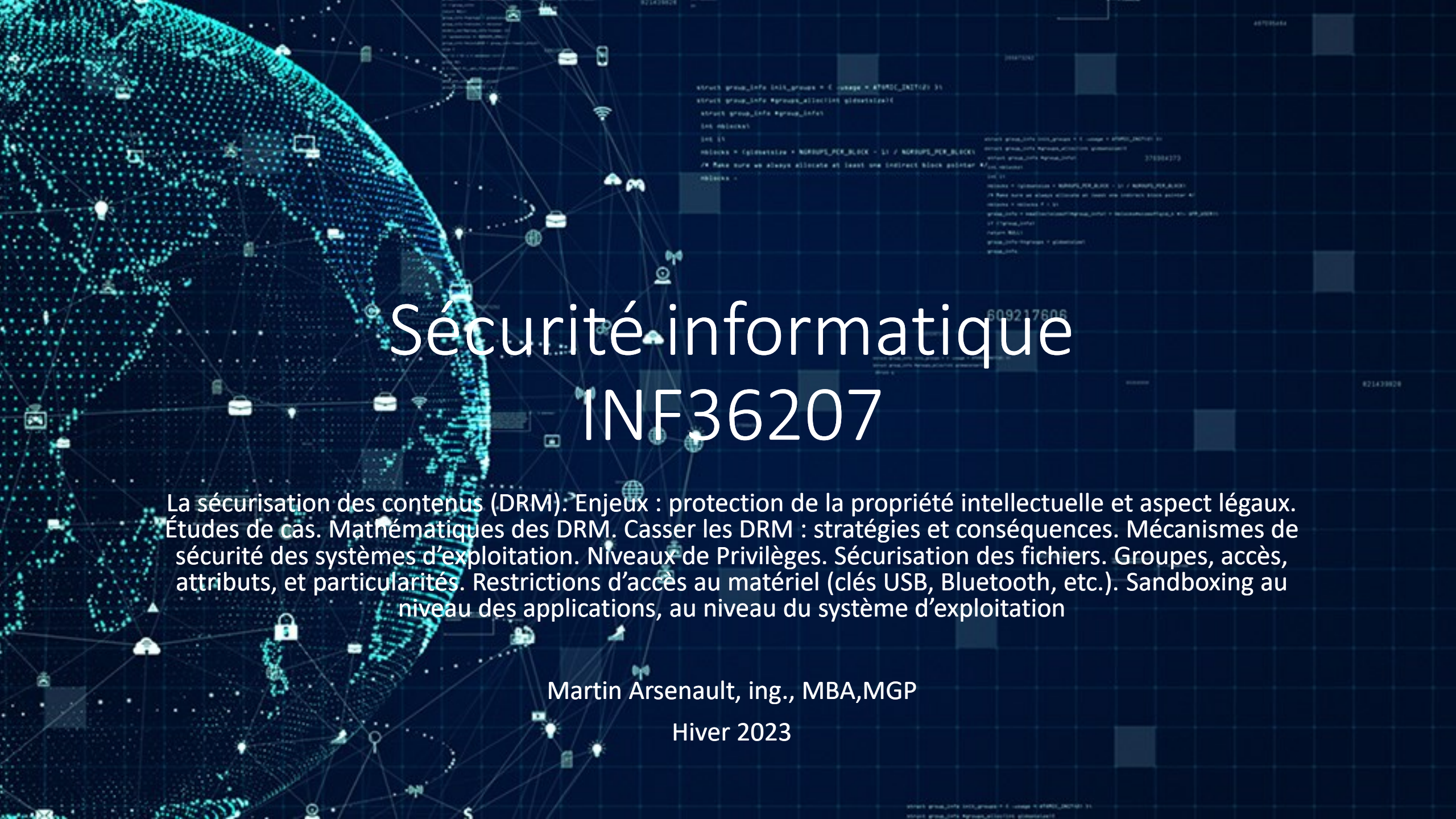


Sécurité informatique
INF36207

La sécurisation des contenus (DRM). Enjeux : protection de la propriété intellectuelle et aspect légaux. Études de cas. Mathématiques des DRM. Casser les DRM : stratégies et conséquences. Mécanismes de sécurité des systèmes d'exploitation. Niveaux de Privilèges. Sécurisation des fichiers. Groupes, accès, attributs, et particularités. Restrictions d'accès au matériel (clés USB, Bluetooth, etc.). Sandboxing au niveau des applications, au niveau du système d'exploitation

Martin Arsenault, ing., MBA,MGP

Hiver 2023

Qu’est-ce que la gestion des droits numériques ?

- La gestion des droits numériques, ou DRM, est un ensemble de normes technologiques qui permettent aux fabricants d'applications logicielles et de supports numériques d'appliquer des contrôles d'accès à leur(s) produit(s), tels que la restriction de l'utilisation, de la reproduction, de la modification et de la distribution du produit.
- Pourquoi ?
  - Les éditeurs de logiciels et les entreprises de médias numériques consacrent une grande partie de leur argent et de leur temps à la recherche, au développement et à la commercialisation de leurs produits.
  - À l'ère de la technologie et de la connectivité, il n'est pas difficile pour des éléments ayant des intérêts illégitimes de produire et de distribuer des copies non autorisées/piratées de l'application/du multimédia, qui ne pourraient autrement être utilisées qu'en les payant.
  - Le piratage entraîne une perte de revenus importante. Il existe plusieurs lois de protection du droit d'auteur (variant d'un pays à l'autre) qui interdisent de tels actes, mais même elles n'ont pas réussi à empêcher le piratage.
  - C'est exactement là que les DRM entrent en jeu. Les différentes technologies qui entrent dans cette catégorie établissent des mécanismes qui rendent extrêmement difficile, voire impossible, le vol du produit. Il empêche la copie, la distribution et l'utilisation non autorisées du produit, en raison du contrôle d'accès qu'il applique.

Qu’est-ce que la gestion des droits numériques ?

- L’objectif :
  - Empêcher ou limiter les utilisateurs de modifier ou de stocker leur matériel ou leurs produits, de les partager et de les transmettre, de les imprimer ou de capturer des captures d'écran.
  - Définir des dates d'expiration sur les médias pour interdire aux gens d'y accéder après cette date ou pour limiter le nombre de fois qu'ils peuvent le visionner.
  - Limiter l'accès aux médias à des appareils, des adresses IP ou des lieux géographiques spécifiés.
  - Ajoutez des filigranes aux documents et aux images pour affirmer la propriété et l'identité du contenu.

Cible ➔ Musique, Cinéma/vidéo, Jeux vidéo, Application (licences), Livres (eBook, PDF, etc.)

Avantages du DRM

- Avantages de la gestion des droits numériques :
  - **Assure la confidentialité :**
    - Chiffrer des documents critiques
    - Permet aux utilisateurs de restreindre l'accès aux fichiers, retracer les accès.
  - **Sécurisation de la propriété :**
    - Protéger les documents travail et interdit qu'ils soient modifiés, enregistrés, dupliqués ou imprimés.
  - **Empêcher toute utilisation non autorisée et involontaire. :**
    - Respect des licence qui régissent comment, quand et même où ils peuvent l'utiliser.
  - **Garantir un accès approprié au contenu :**
    - Limite le contenu à des publics ciblés et le restreint à certains publics.
  - **Confidentialité des fichiers :**
    - Sécuriser les fichiers sensibles et préserver leur confidentialité.

À quel endroit retrouve-t-on le DRM ?

- Le matériel DRM peut être trouvé dans une variété de types de médias numériques :
  - Musique, photos, films, livres électroniques, actifs propriétaires d'entreprise, abonnements à des bases de données et les logiciels.
- Entreprises de médias :
  - Permet de lutter contre l'utilisation illégale de leur produits.
- Entreprises technologiques :
  - 57 % des utilisateurs d'ordinateurs admettent avoir piraté des logiciels dans le passé. Assure une protection contre le piratage.
- Entreprise :
  - Couramment utilisé par les entreprises pour sécuriser les données sensibles (conception de produits, plans, contrat, stratégie d'affaires, etc.).

Selon Gartner, l'industrie du DRM vaudra plus de 330 millions de dollars d'ici la fin de 2026

Quelques méthodes pour le DRM

- Les différentes technologies de gestion des droits numériques sont les suivantes :
  - Activations d'installation limitées;
  - Authentification en ligne persistante;
  - Falsification de logiciels;
  - Clés de produit;
  - Gestion des droits numériques d'entreprise;
  - Système de brouillage de contenu;
  - DRM dans les services de streaming.

Quelques méthodes pour le DRM

- Activations d'installation limitées
  - Limite le nombre d'utilisateurs sur les systèmes desquels l'application logicielle ou le jeu vidéo peut être installé.
  - Cela se fait en exigeant une activation en ligne via le serveur du fournisseur, après l'installation du produit.
    - Exemple : Logiciel antivirus est limité à 4 utilisateurs uniquement.
- Authentification en ligne persistante
  - L'authentification en ligne persistante nécessite que l'utilisateur reste connecté au serveur en ligne pour pouvoir utiliser le produit.
  - Méthode populaire avec les jeux vidéo qui obligent l'utilisateur à se connecter au serveur pour jouer, même lorsque l'utilisateur joue en mode solo.
  - Cela a cependant un inconvénient majeur : le produit devient inutilisable en cas de problème de connexion internet.

Quelques méthodes pour le DRM

- Falsification de logiciels
  - Nombreux fournisseurs introduisent délibérément des bogues dormants dans leurs applications et jeux vidéo qui seraient activés chaque fois que le produit est suspecté d'être piraté.
  - Exemple : le jeu commencerait délibérément à planter dès que l'ordinateur serait connecté à Internet et que le produit établirait secrètement une connexion avec le serveur.
    - Microsoft Windows a également implémenté cette fonctionnalité dans Windows XP et Windows 7. Chaque fois que le système d'exploitation était piraté, le fond d'écran devenait noir et l'icône de volume était verrouillée.
- Clés de produit
  - Méthode la plus courante pour authentifier un produit. Lors de l'achat de l'application, l'utilisateur recevrait une clé de produit qu'il devrait mettre lors de l'installation de l'application.
  - Il serait ensuite vérifié par le serveur pour trouver une correspondance car chaque copie de l'application a une clé différente. Si une correspondance n’est pas trouvée, alors le produit n'est pas activé.
- Gestion des droits numériques d'entreprise
  - Il s'agit d'une combinaison de gestion des identités, d'accès et de chiffrement.
  - Le contenu est crypté et couplé à la protection qui permet différentes politiques d'accès et de modification pour différentes entités.
  - La protection est indépendante de l'appareil et du lieu d'accès. Il est principalement utilisé pour sécuriser des documents tels que des documents MS Word, PDF, des fichiers Autocad, etc.

Quelques méthodes pour le DRM

- Système de brouillage de contenu
  - Il s'agit d'un système de cryptage utilisé dans les disques multimédias produits dans le commerce pour les protéger contre la copie et la distribution non autorisées. Il utilise un algorithme de chiffrement de flux de 40 bits. Nous y reviendrons plus loin.
- DRM dans les services de streaming comme Netflix, Comcast, Amazon prime, etc. qui utilisent des produits tels que Microsoft PlayReady, Xfinity, etc., qui sont des technologies de prévention de la copie de fichiers multimédias (concept de domaine et de licence intégrée). Elles sont pour la plupart portables et indépendantes de la plate-forme.
  - Problèmes de connectivité Internet avec l'authentification en ligne
  - Méthodes de contournement pour le contenu audio et vidéo permettant l'extraction et la perte de protection par DRM
  - Courte durée de vie du produit pour les utilisateurs payants non transférable à d'autres technologies et plates-formes les rendant perdus à jamais suite à des mises à jour (DB, OS, etc.).
  - Suppression des filigranes via un logiciel tiers.
  - Matériel conçu à cet effet pour décrypter et montrer le contenu à l'utilisateur, ce qui est fait afin de protéger la clé de décryptage. Cependant, le système est susceptible de tomber en panne.

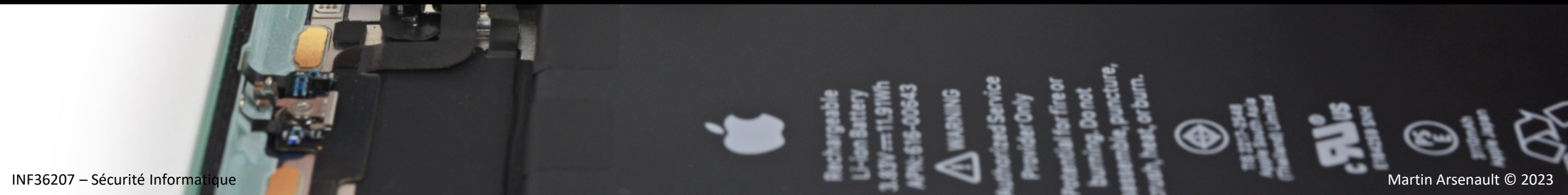
Techniques de DRM

- Techniques de DRM sont centrées sur :
  - L'authentification (utilisateur, machine)
  - L'autorisation (droits consentis à l'usage)
- Les méthodes pour la gestion des DRM se fait avec :
  - Logiciel/applications
  - Matériel

  ➔Caractéristiques communes : propriétaires, environnement fermé
- Exemple :
  - Matériel : iPhone, iPad, Mac, etc.
  - Logiciel/application : NetFlix, Amazon Prime TV, iTunes, Spotify, etc.
- Cette fermeture retire le contrôle des mains de l'utilisateur
- Cette fermeture rend également les DRM plus difficiles, mais pas forcément impossibles à casser;

Techniques de DRM

Possible d’y aller avec la méthode dure



Techniques de DRM

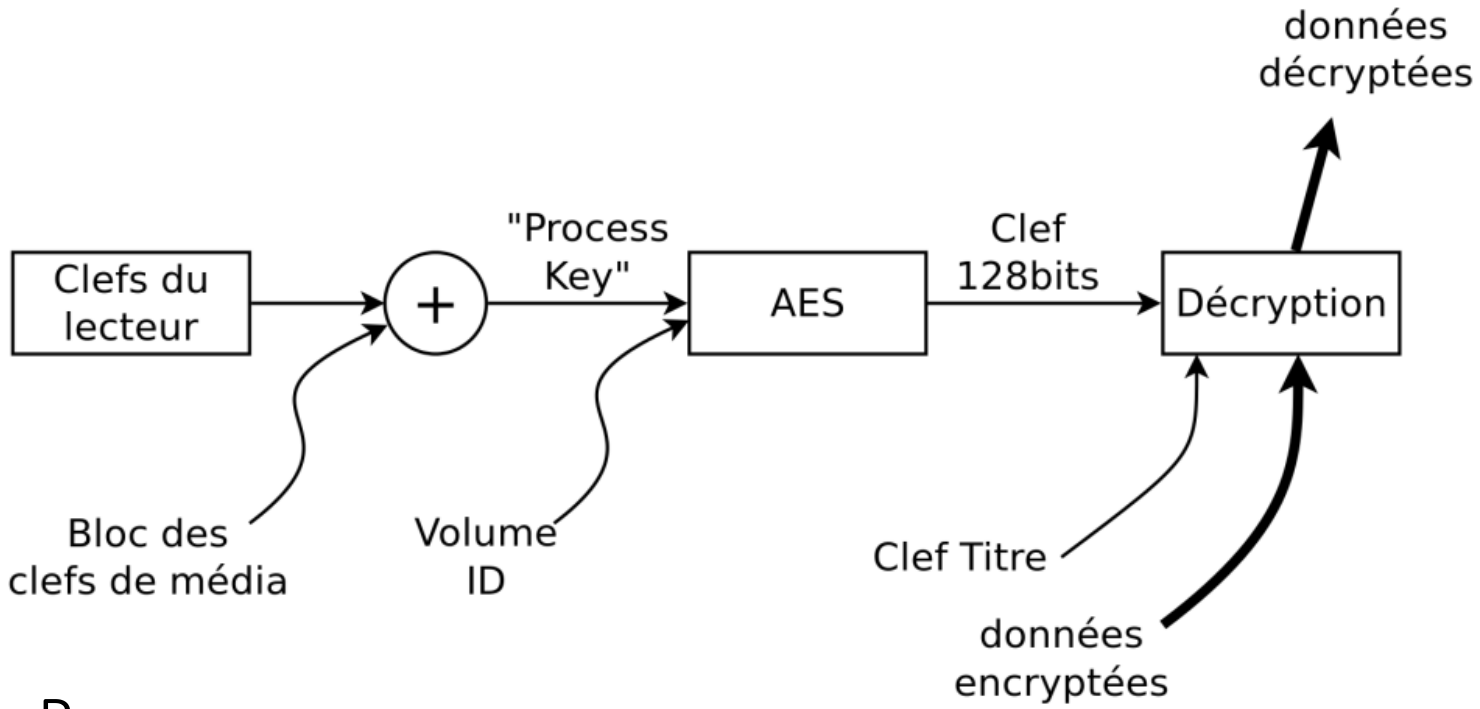
- Filigranes visible (watermarks)
  - Fond de pages
  - Logo dans un coin d'image
- Métadonnées insérées dans le fichier contenant l'identité du propriétaire
  - Blocs de données supportés par le type de fichier
  - Informations cachées par stéganographie

Techniques de DRM

- Pour les plate-forme fermées
  - Partitions encryptés contenant les clés d'accès au contenu DRM
  - Ou encore base de données encryptées
- Exemple : DVD et Blu-Ray
  - On présume un lecteur digne de confiance;
  - Cryptographie se fait avec le « hardware » et les données sur le disque;
  - Le lecteur contient une/des clés (clé secrète, code de région);
  - Le disque contient aussi des clés et une zone secrète contenant les clés d'encryption, le hash et le code de région;

DRM sur les DVD

- Les DVD utilisent l'algorithme CSS (Content Scrambling System) qui est propriétaire et qui utilise un clé de chiffrement de 40 bits;
- Il permet d'authentifier le lecteur autorisé avec la région et permettre le décodage du titre;
  - CSS est très faible comme algorithme
  - Se casse très rapidement avec `libdvdcss` qui est un logiciel OpenSource;
- Blu-Ray utilise un schéma assez compliqué :
  - Plusieurs jeux de clés,
  - Clés ont 128 bits,
  - Algorithme AES,
  - Le hardware participe de façon importante



DRM sur les Blu-Ray

- Les clés Blu-Ray :
  - Chaque lecteur a ses clés uniques (en principe);
  - Les clés du lecteur sont révocables (en principe);
  - Les clés du média se trouvent sur le disque;
  - Le volume ID est accédé par du hardware spécial;
  - La taille des clés est censée prévenir une attaque brute force.

Authentification/autorisation externe pour le DRM

- Méthodes proches des signatures numériques :
  - Obtenir un ticket du serveur pour activer des services,

    C'est une situation de login où on s'authentifie à un serveur et où on obtient des services (ex : Kerberos, etc.);
  - Utiliser un serveur pour s'authentifier et « barrer » des données à un appareil en particulier.

    C'est une situation de lock-in où on télécharge des données (disons de la musique) sur une machine en particulier et où on ne peut qu'accéder aux données à partir de cette machine en particulier, même si on copie les données ailleurs;

Autorisation d'accès DRM par la méthode avec Ticket

- Alice veut obtenir des service de Bob :
  - Alice envoie ID(Alice), H(password) à Bob dans un tunnel sécurisé;
  - Bob vérifie que H(password) et ID(Alice) concordent;
  - Bob crée un ticket T_B avec les autorisations, encrypté avec la clef secrète d'Alice, K_A, que Bob connaît;
  - Bob envoie T_B à Alice;
  - Alice décode T_B avec K_A et passe son contenu au logiciel;

Autorisation d'accès DRM à un appareil spécifique

- Alice veut obtenir de la musique de BobMusique, mais BobMusique veut ne lui permettre de l'écouter qu'à partir d'un appareil en particulier;
- BobMusique va vouloir authentifier Alice et l'appareil sur lequel elle veut conserver la musique;
- De plus, BobMusique va vouloir faire en sorte que la musique ne puisse plus être jouée qu'à partir de cet appareil en particulier;

1. Alice possède :
   - ID(Alice), son identificateur unique;
   - m, l'identificateur du média qu'elle demande;
   - u, l'identificateur unique de son appareil;
   - K_s, sa clé secrète;
   - K_p, sa clé publique

Autorisation d'accès DRM à un appareil spécifique

2. Alice envoie à Bob
   - T_a = (ID(Alice); E_{Ks} (u; m; ID(Alice)))

3. Bob reçoit Ta et avec Kp, calcule
   - E_{Ks}^{-1} (u; m; ID(Alice)) ;
   - Obtenant ainsi u, m, et confirmant ID(Alice).

4. Bob décide s'il autorise Alice ou non.

Autorisation d'accès DRM à un appareil spécifique

5. S'il autorise Alice pour m, Bob choisit s_m, un nombre aléatoire « grand », et calcule :
   - $K_m = f(u; s_m)$

6. Bob envoie à Alice :
   - $T_B = E_{Kp}(s_m); E_{Km}(M_m))$
   - où M_m représente les bits du média m demandé par Alice

Autorisation d'accès DRM à un appareil spécifique

7. Alice reçoit T_B et le décode avec K_s, et obtient s_m, et $EK_m(M_m)$.

   Alice stocke s_m de façon sécurisée, et $EK_m(M_m)$ n'importe où.

8. Pour écouter la musique, Alice (re)calcule $K_m = f(u; s_m)$, puis :
   - $E_{Km}^{-1}(E_{Km}(M_m)) = M_m$;
   - sans stocker M_m

Autorisation d'accès DRM à un appareil spécifique

- Si Alice prend $E_{Km}(M_m)$ et le copie sur une autre machine, elle ne pourra plus le décoder, même si elle transporte aussi s_m, parce que Km ne peut plus être calculé !
  - $K_m = f(u; s_m)$;
- mais si elle change de device, u', alors
  - $K_m = f(u; s_m) \neq f(u'; s_m)$
- Et Alice se retrouve avec un fichier qu'elle ne peut plus écouter !

Licence USB Dongle Key

- Un dongle de licence (également appelé clé de licence matérielle ou dongle licence USB) est un élément matériel électronique qui peut:
  - Déverrouiller une application par une licence logicielle;
  - Fournir une protection contre la copie pour un logiciel;
  - Déchiffrer le contenu d'une licence crypté.
- Un dongle est généralement utilisé dans des contextes où la protection physique contre le piratage et la distribution non autorisée est essentielle, ainsi que pour fournir une autre voie pour la monétisation des logiciels dans le cadre de la gestion des licences logicielles.
- Voici un aperçu du fonctionnement des dongles, comment ils agissent comme une défense physique pour empêcher toute utilisation non autorisée et un guide expliquant pourquoi ils sont maintenant en déclin.

Licence USB Dongle Key

- Un dongle fonctionne grâce à la protection électronique contre la copie.
- Il est programmé avec des clés de cryptage logicielles ou matérielles avec les informations de licence nécessaires pour déverrouiller le logiciel ou tout autre contenu de licence.
- Il protège généralement les applications de bureau, mais peut également protéger les systèmes Web ou infonuagiques.
- Le micrologiciel sur le dongle contient des informations qui autorisent l'accès au logiciel et définissent les conditions de licence indiquant comment et à quoi l'utilisateur final peut accéder.
- Il applique les conditions de licence, telles que les fonctionnalités disponibles, l'heure ou le lieu d'utilisation, et l'utilisateur final ne peut sécuriser l'accès à l'application logicielle que s'il dispose physiquement du dongle connecté à un port USB de son ordinateur.

Licence USB Dongle Key
(Inconvénients)

- Les dongles sont facilement perdus ou endommagés;
- Problèmes de compatibilité avec différents systèmes d'exploitation ou configurations réseau;
- Les dongles sont passés entre utilisateurs, portant atteinte à la sécurité d'accès ou d'utilisation;
- Augmentation des coûts de production, de stockage et de livraison des dongles, et coûts élevés de remplacement des licences;
- Le clonage matériel devient monnaie courante, laissant aux fournisseurs le soin de remédier aux violations de licence
- Problèmes de mise à niveau et de mise à jour des clés matérielles pour correspondre à la dernière version du logiciel ou à la modification des conditions de licence;
- Les pénuries de puces limitent la capacité de produire des dongles compatibles avec les nouvelles versions;
- Les avancées en matière d'authentification et contrôle des autorisation font en sorte que ce modèle est de plus en plus laissé de côté.

DRM et droit

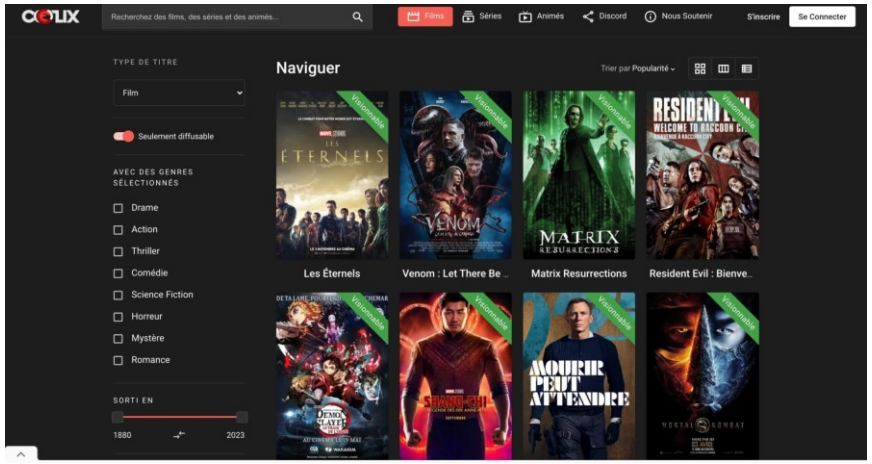
- On est en droit de se demander si les restrictions arbitraires imposées par les grands fournisseurs de contenus ne briment pas nos droits de consommateurs,
- Et si encore ils ne contreviennent pas à d'autres lois (comme, par exemple, les lois canadiennes sur le copyright)
- Il y a donc des groupes de lobbyistes qui militent pour des changements aux lois qui permettent les DRM (et les poursuites au criminel si on casse les DRM), et d'autres groupes qui militent contre les DRM et pour les libertés civiles.

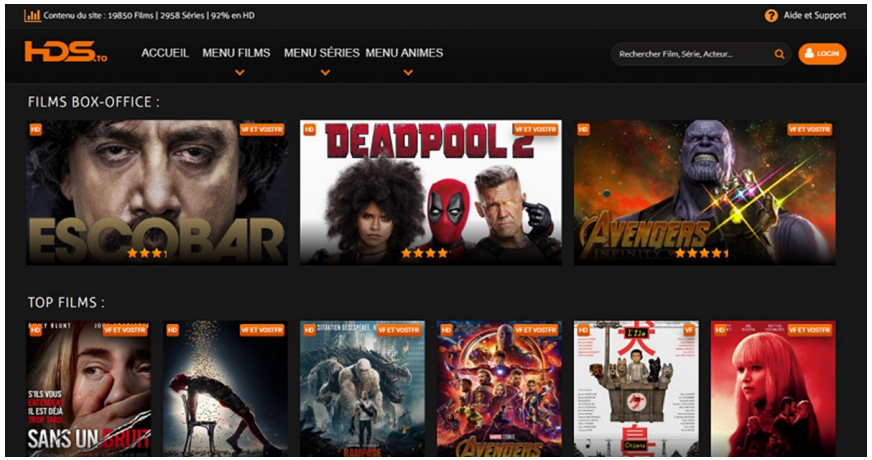
https://www.defectivebydesign.org https://www.fsf.org

DRM et droit

- On pourrait aussi argumenter qu'il y a des raisons légitimes pour contourner les DRM :
  - Assurer la survie d'un produit après la fin du support officiel (systèmes d'exploitation, jeux, etc.).
    - Qu'est-ce qui arrive quand un jeu cesse d'être supporté et que les serveurs sont éteints ?
  - Se protéger contre des révocations de licence arbitraires.
    - En 2009, Amazon a retiré le roman 1984 de George Orwell de ses lectrices Kindle sans le consentement des utilisateurs parce que l'éditeur du livre avait décidé de ne plus le vendre à travers Amazon.
  - Se protéger contre les changements de licence arbitraires.
    - Suite à un embargo commercial votre iPod devient inutilisable. Que faire ?
    - Exemple du iPhone en Russie.

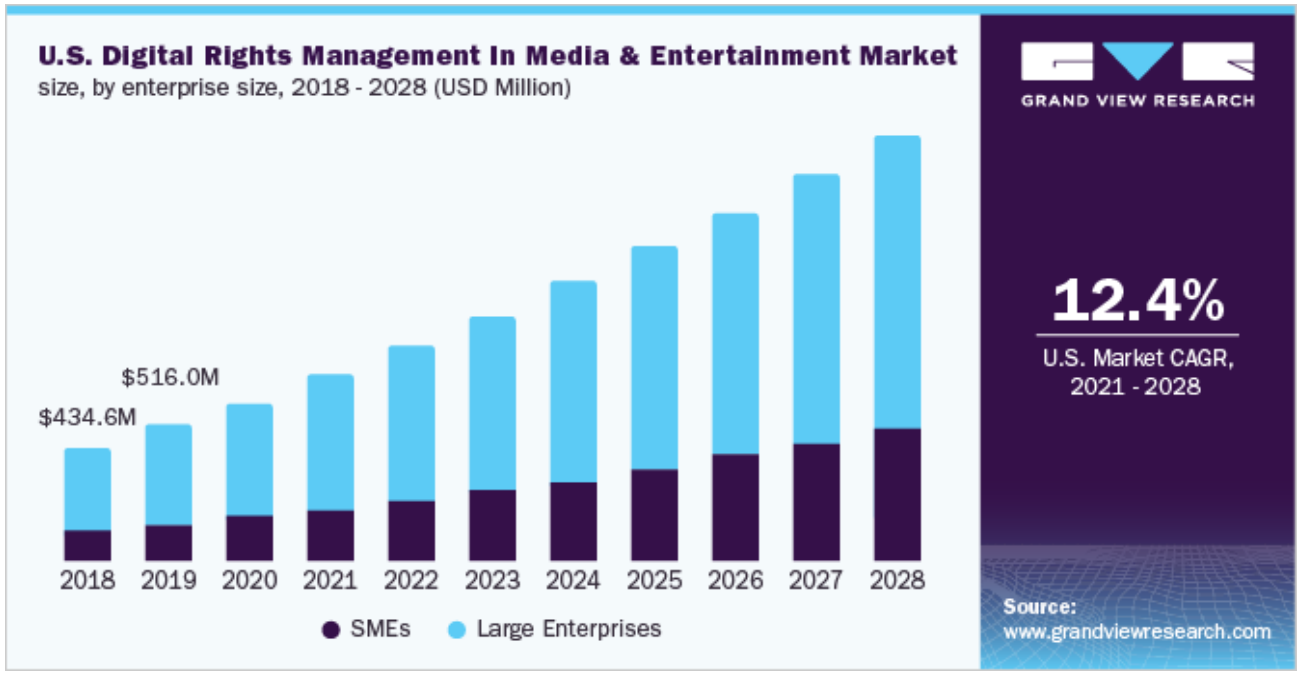
Contourner les DRM ?





- Les DRMs sont vulnérables à beaucoup d'attaques :
  - « analog hole » où on capture les signaux analogiques,
  - Ponts-convertisseurs :
    - par exemple HDCP/HDMI à DVI ou → Fichier MP4,
  - Logiciels modifiés :
    - hacker un driver (carte de son, vidéo).
    - Obtenir les clés;
    - Obtenir les données décodées;
    - Changer les routines d'autorisation;
  - Casser les clés;

Tout cela est probablement illégal dans certain pays!!

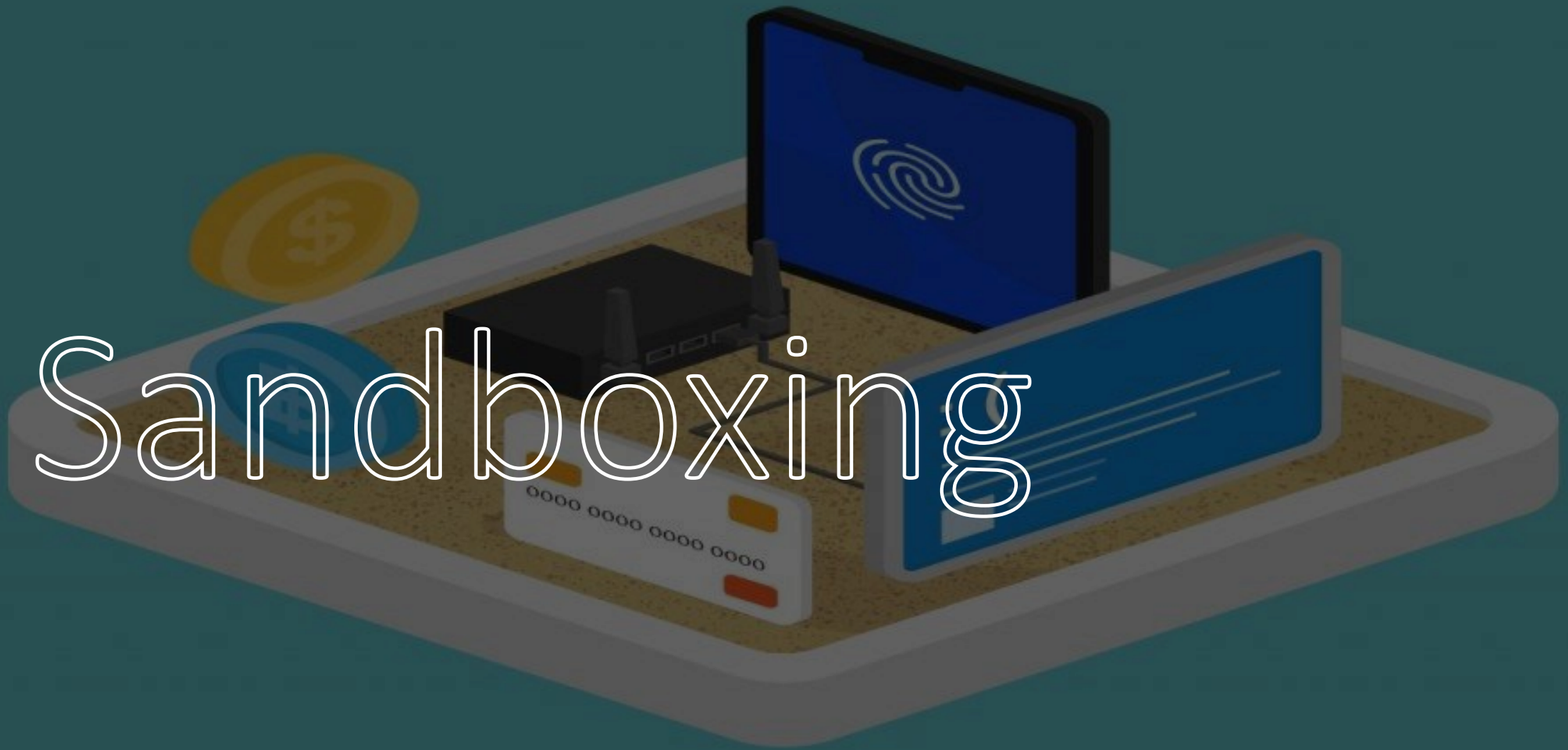


Source: Secondary Research, Expert Interviews, and MarketsandMarkets Analysis

CAGR : Compound Annual Growth Rate

En Français : Taux de croissance annuel composé

Sandboxing



Sandboxing

- En partant de l'observation que :

> *An application can do little harm if its access to the underlying operating system is appropriately restricted,*
>
> [Goldberg et al.]

- il devient clair que tous les processus devraient s'exécuter selon le principe de moindre privilège, c'est-à-dire s'exécuter avec des permissions et des accès **tout juste suffisants** pour qu'ils réalisent leur tâche

Qu’est-ce que le Sandboxing ? (Bac à sable)

- Approche de développement, de gestion de logiciels, d’infrastructure et de gestion d'applications mobiles qui limite les environnements dans lesquels certains codes peuvent s'exécuter;
- Le bac à sable d'application, comme le bac à sable d'un enfant, crée un environnement sûr pour exécuter et tester le code informatique qui protège les utilisateurs et les environnements de production.
- Chaque application logicielle se voit attribuer un environnement contrôlé et restreint pour exécuter des applications et du code.
- Cet environnement aide les développeurs à isoler et à protéger les ressources système contre les logiciels malveillants et autres types de cybermenaces.
- Les chercheurs utilisent également des bacs à sable pour identifier le comportement d'un logiciel et repérer tout logiciel malveillant ou tout autre élément de programme indésirable.

Conteneurisation (sandboxing)

- Objectifs :
  - Améliorer la sécurité en isolant et en protégeant l'application des intrus extérieurs ou des logiciels malveillants. Il est également utilisé lorsqu'il est nécessaire d'empêcher les ressources système ou d'autres applications d'interagir avec l'application protégée.
  - Ce type de séparation permet de créer un environnement sécurisé afin que l'application puisse s'exécuter sans risquer d'endommager l'ensemble du système.
  - L'approche est particulièrement utile pour exécuter ou tester des applications provenant de sources non fiables (par exemple, des développeurs inconnus), de sites Web ou encore d'étudiant développant du code ☺.
  - Augmente également l'intégrité des applications permettant aux développeurs d'envelopper l'application dans des politiques de sécurité ou d'isoler et de protéger l'application au sein de sa propre machine virtuelle.

Conteneurisation (sandboxing)

- Avantages :
  - Sécurité renforcée. En limitant l'environnement dans lequel les codes peuvent s'exécuter, les développeurs protègent l'application des influences extérieures, qu'il s'agisse de ressources système ou de bogues non malveillants, de logiciels malveillants ou de pirates .
  - Empêche les utilisateurs d'accéder à des environnements auxquels ils n'ont pas besoin d'accéder ou auxquels ils ne devraient pas accéder ;
  - Fournit une sécurité supplémentaire en cas d'erreurs causées par des bogues ou des vulnérabilités inattendus ; et
  - Les principaux éditeurs de logiciels comme Amazon, Microsoft et Google comptent sur ces avantages afin d’offrir des environnements d'application sécurisés aux utilisateurs.

Type de Sandbox

Jail

- L'OS emprisonne les applications :
  - OS de type préemptif
  - Mémoire et matériel protégés
  - Appels au système d'exploitation régis par des permissions de type MARC (Mandatory Access Control)

Cuckoo (pas un vrai sandbox)

- Instrumenter le code existant au niveau des appels systèmes
- Suivre l'exécution du code
- Suivre l'exécution des librairies
- https://cuckoosandbox.org/

Type de Sandbox

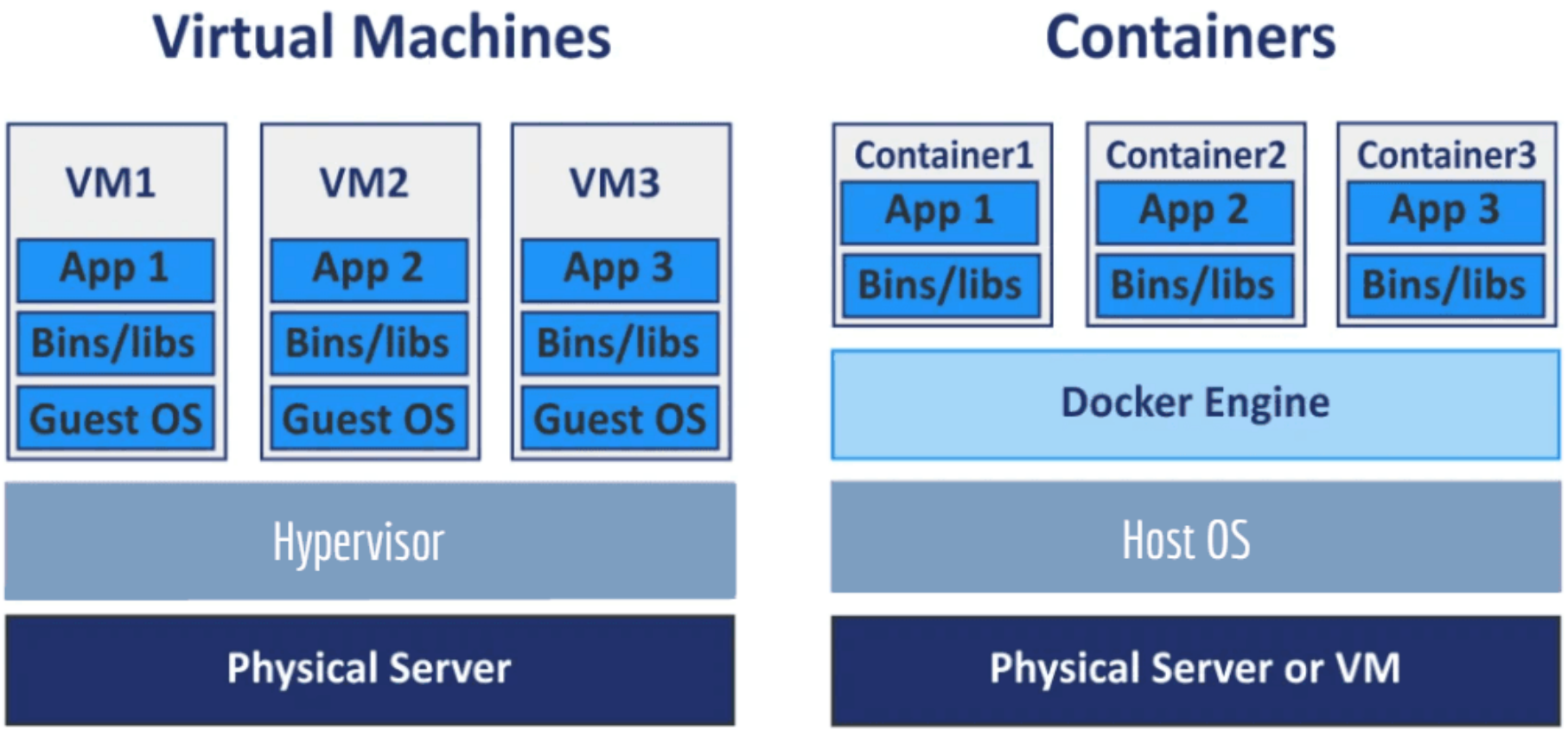
Machine Virtuelle (1)

- L'application s'exécute dans un environnement contrôlé, possiblement interprété;
- Les instructions possibles sont limitées par la machine virtuelle;
- La machine virtuelle expose l'API qu'elle veut bien exposer;
- La machine virtuelle peut-être exécuté avec les privilèges d'un utilisateur régulier;
- Exemple : Java et la JVM, C#, etc.

Machine Virtuelle (2)

- C'est la machine complète (y compris le système d'exploitation) qui se trouve isolée.
  - La machine invitée exécute tout son code dans une « bulle » fournie par l'hyperviseur;
  - La machine virtualisée n'est pas contrainte de façon explicite. Pour le programme, c'est une machine « ordinaire »;
  - La machine hôte exécute l'hyperviseur et alloue les ressources (mémoire, CPU, etc.) ; l'hyperviseur gère les accès externes (principalement réseau);
- Exemple : Windows 10 roulant dans VirtualBox, ou encore le « Sandbox » intégré dans Windows 11 exécutant une version bac à sable de Windows 11.

Virtual Machine VS Containers



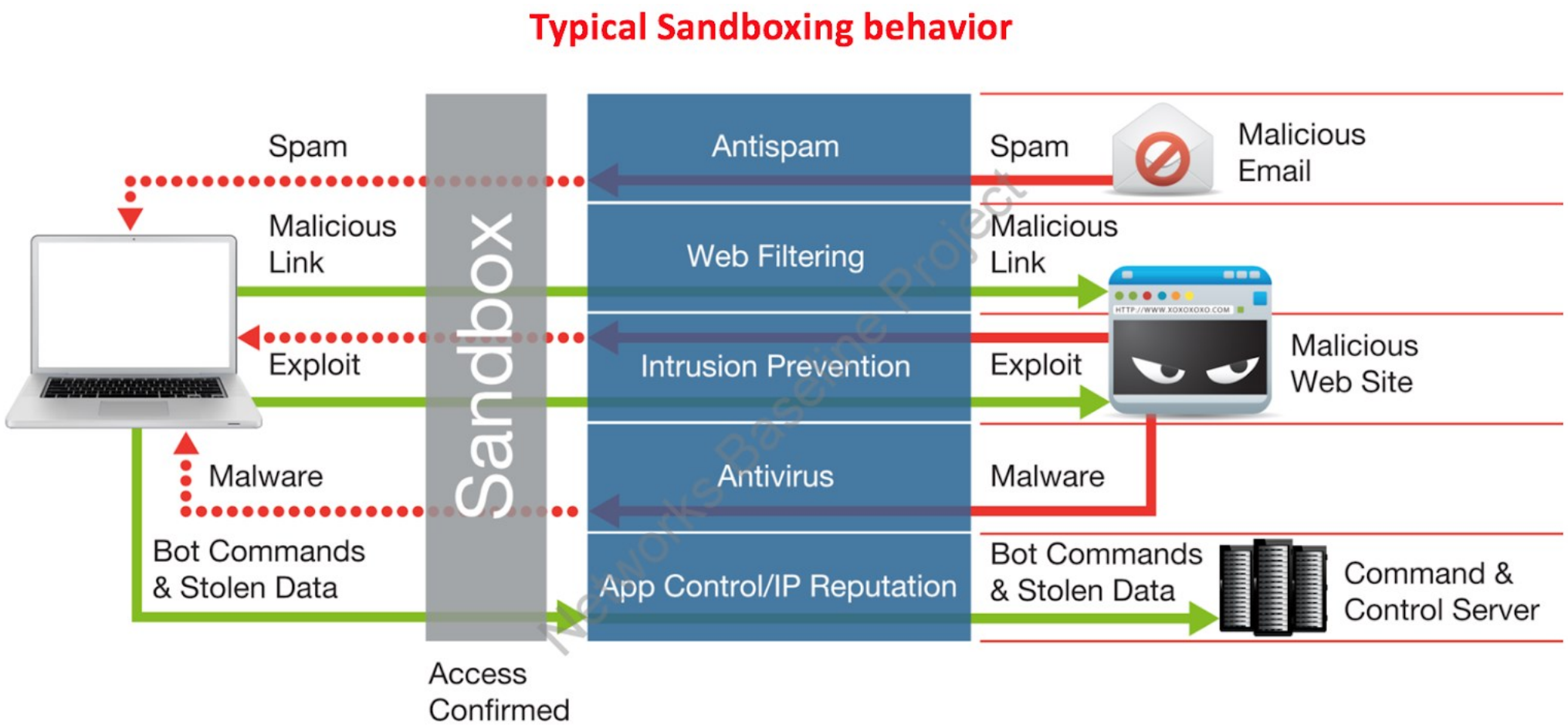
Virtualisation (Virtual Machine)

- Il peut s'agir d'une plate-forme matérielle informatique virtuelle, d'un stockage virtuel ou de ressources réseau virtuelles.
- Les conteneurs et les bacs à sable peuvent donc être des exemples de virtualisation.
- Aujourd'hui, l'utilisation la plus courante du terme virtualisation concerne les environnements dans lesquels le matériel physique a été virtualisé.
- Lorsque vous utilisez la virtualisation, vous utiliserez dans la plupart des cas une copie complète du même logiciel que vous exécuteriez autrement sur du matériel réel, la seule différence est que vous n'avez pas d'accès physique au matériel.
- Les systèmes tels que Hyper-v ou VMware sont des plates-formes populaires qui utilisent la virtualisation.

Conteneurisation (Container)

- La conteneurisation est une application plus récente de la virtualisation et est également connue sous le nom de « virtualisation au niveau du système d'exploitation ».
- Avec les conteneurs, le matériel sous-jacent n'est pas virtualisé, mais à la place, le système d'exploitation crée des environnements « d'espace utilisateur » isolés.
- Une application qui s'exécute dans un tel conteneur pensera qu'il s'agit de la seule application en cours d'exécution.
- Du point de vue de la sécurité, le fait que les applications ne puissent pas se voir est un avantage majeur.
- Un avantage supplémentaire à cela est que la surface attachée de l'application est plus petite que si elle ne s'exécutait pas dans un conteneur.
- Des logiciels comme Docker et Kubernetes utilisent ce type de virtualisation.
- Comme les conteneurs partagent le « noyau » sous-jacent, cela peut être un moyen très efficace de protéger les applications non approuvées les unes des autres.

Sandbox

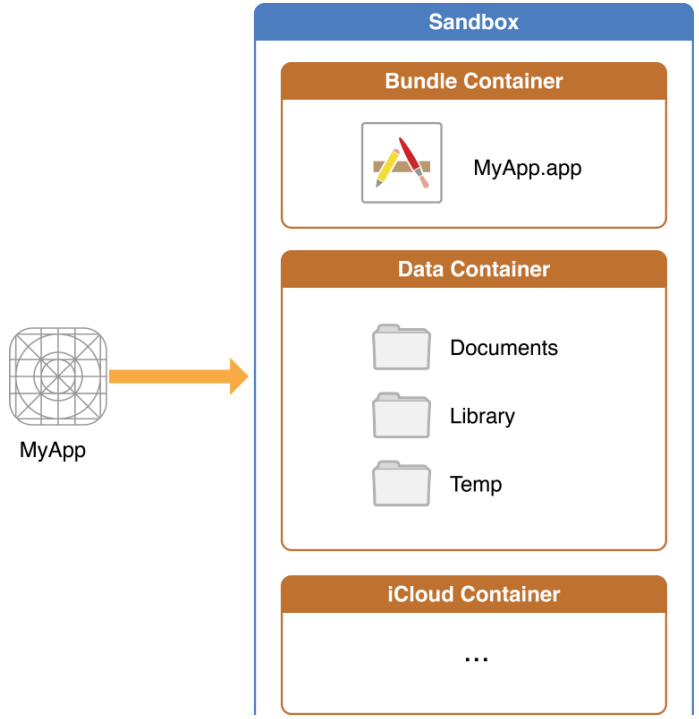


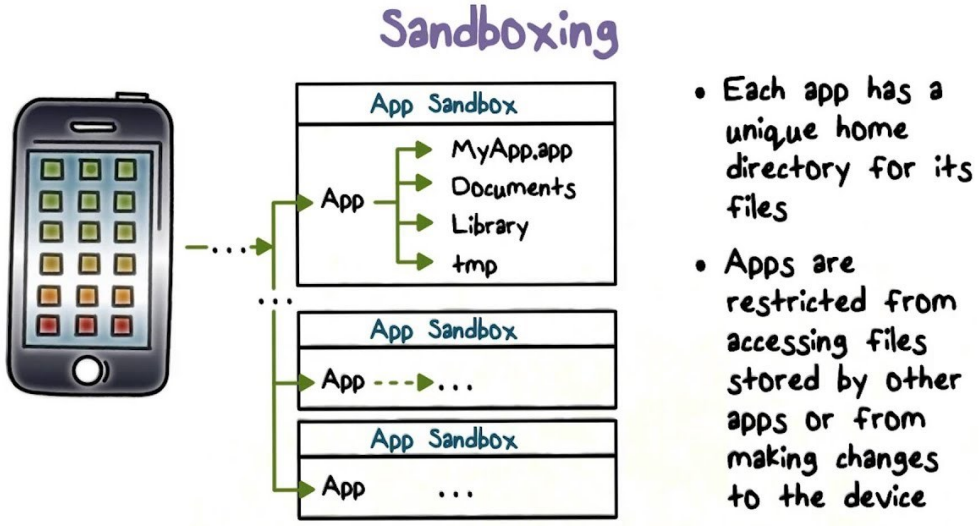
Bac à sable (Sandbox)

- Dans le domaine de la sécurité informatique, un bac à sable peut faire référence à au moins deux mécanismes / techniques connexes :
  - En ce qui concerne les systèmes d'exploitation, un bac à sable est un environnement dans lequel vous exécutez des applications afin que l'application ne puisse pas obtenir un accès complet à d'autres applications.
  - En ce qui concerne iOS et Android, ils ont chacun des formes légèrement différentes de bacs à sable mais fonctionnent essentiellement de la même manière : chaque application a une liste des ressources auxquelles elle souhaite accéder, que les utilisateurs doivent approuver, soit lors de l'installation de l'application ou lorsque la ressource est nécessaire.
  - Pour les pirates, le mécanisme de bac à sable du système d'exploitation est une cible tentante. Si leur logiciel malveillant peut échapper au bac à sable, l'impact sera grand.
- La deuxième manière, peut-être plus traditionnelle, d'utiliser le terme bac à sable est un environnement dans lequel un logiciel peut s'exécuter afin qu'il puisse être analysé pour des problèmes de sécurité.
  - Cela se fait en surveillant ce que fait l'application analysée afin que tout problème de sécurité potentiel puisse être découvert avant qu'elle ne soit autorisée à s'exécuter dans un environnement de production.

Exemple de sandbox au niveau de l'OS

- Apple iOS :
  - Le sandboxing est intégré dans iOS (iPhone, iPad, etc.) au niveau du noyau.
  - En principe, permet d'accorder des permissions avec une granularité fine basée sur le manifeste de l'application,
  - La structure de fichiers et de permissions de l'application est créée au moment de l'installation.
  - Pour en savoir plus : App Sandbox in Depth
- Android :
  - Comme pour iOS, le sandboxing est intégré au noyau (basé sur Linux) d'Android.
  - On a aussi les permissions à granularité fine.
  - Structures créées au moment de l'installation, à partir du manifeste de l'application.
  - Pour en savoir plus :
    - Android Virtualization Framework
    - Security in a virtual machine





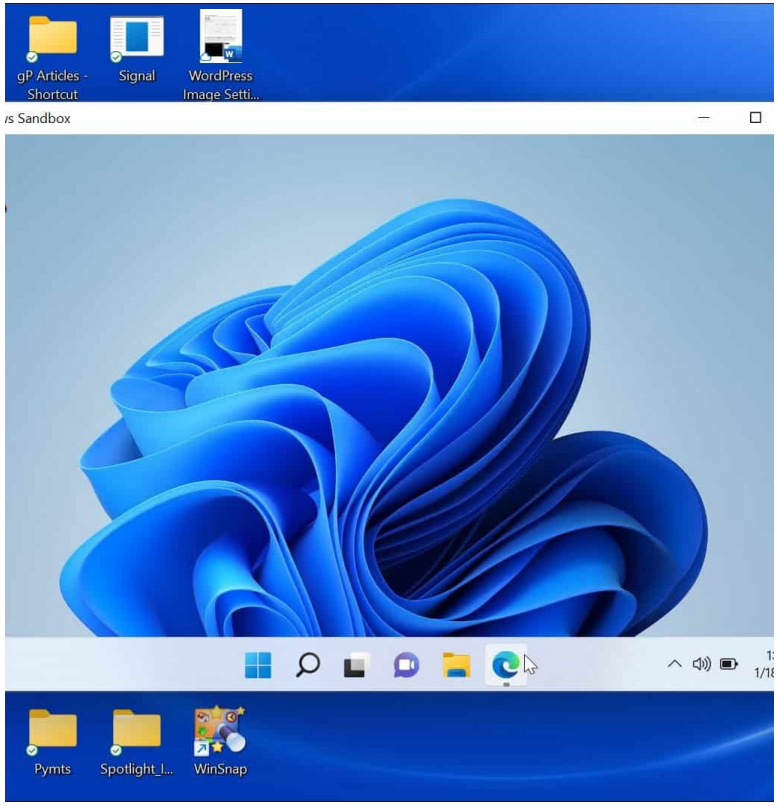
Bac à sable Windows

- Le Bac à sable Windows fournit un environnement de bureau léger pour exécuter des applications en toute sécurité de manière isolée.
- Les logiciels installés à l'intérieur de l'environnement Bac à sable Windows restent « en bac à sable » et s'exécutent séparément de l'ordinateur hôte.
- Le bac à sable est temporaire. Lorsqu'il est fermé, tous les logiciels et fichiers, ainsi que l'état, sont supprimés.
- Vous obtenez une nouvelle instance du bac à sable chaque fois que vous ouvrez l'application.
- Pour y avoir recours :
    1. Vérifiez que votre ordinateur utilise Windows 10 Professionnel ou Enterprise, build version 18305 ou Windows 11.
    2. Activer la virtualisation sur la machine.
        a) Si vous utilisez une machine physique, vérifiez que les fonctionnalités de virtualisation sont activées dans le BIOS.
        b) Si vous utilisez une machine virtuelle, exécutez la commande PowerShell suivante pour activer la virtualisation imbriquée :

        PowerShell :

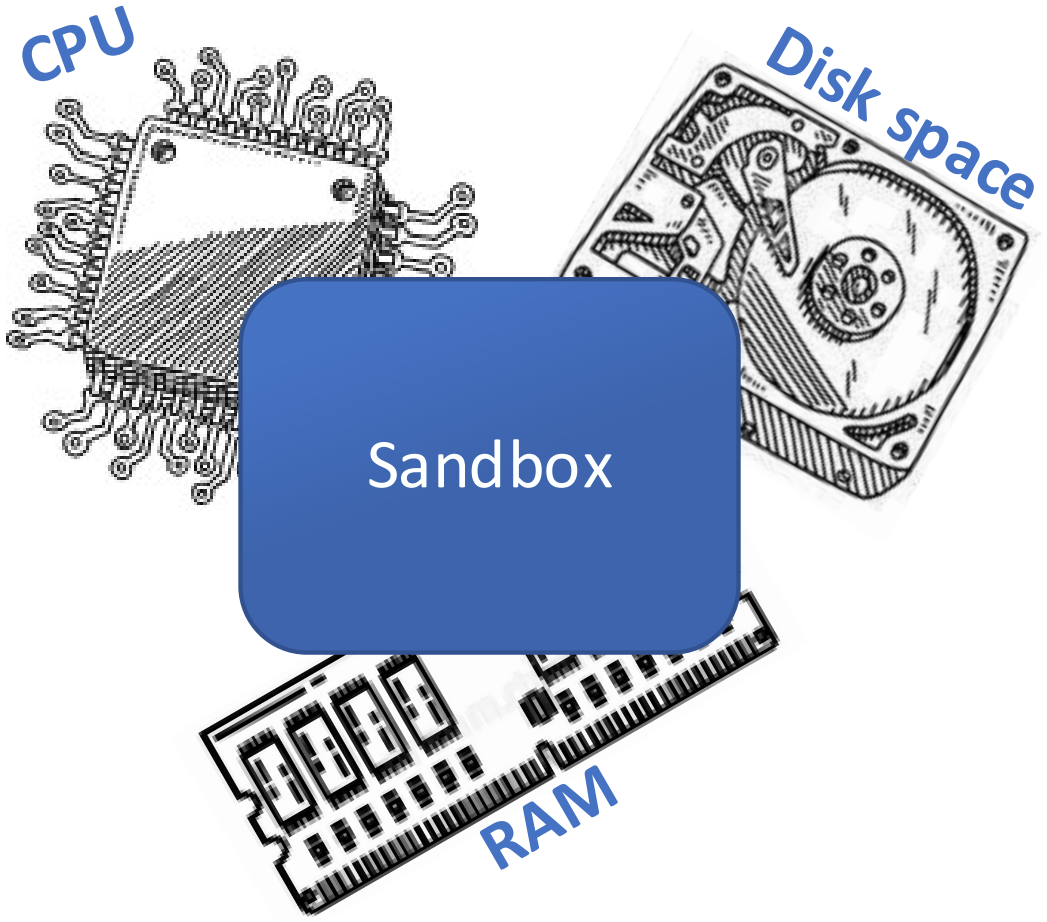
        ```
        Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
        ```

        Ou encore :
    3. Utilisez la barre de recherche de la barre des tâches et tapez **`Activer ou désactiver les fonctionnalités Windows`** pour accéder à l'outil Fonctionnalités facultatives Windows. Sélectionnez Bac à sable Windows, puis OK. Redémarrez l'ordinateur si vous y êtes invité.
- [Plus d'information sur le Bac à sable de Windows]



AppArmor

- AppArmor est un système de contrôle d'accès obligatoire (MAC) qui est une amélioration du noyau (LSM) pour limiter les programmes à un ensemble limité de ressources.
- Le modèle de sécurité d'AppArmor consiste à lier les attributs de contrôle d'accès aux programmes plutôt qu'aux utilisateurs.
- Le confinement AppArmor est fourni via des profils qui peuvent être assez fins, chargés dans le noyau, généralement au démarrage permettant de spécifier les librairies et accès.
- Les profils chargés en mode d'application entraîneront l'application de la politique définie dans le profil ainsi que le signalement des tentatives de violation de la politique (via syslog ou auditd).
- Pour en savoir plus : AppArmor

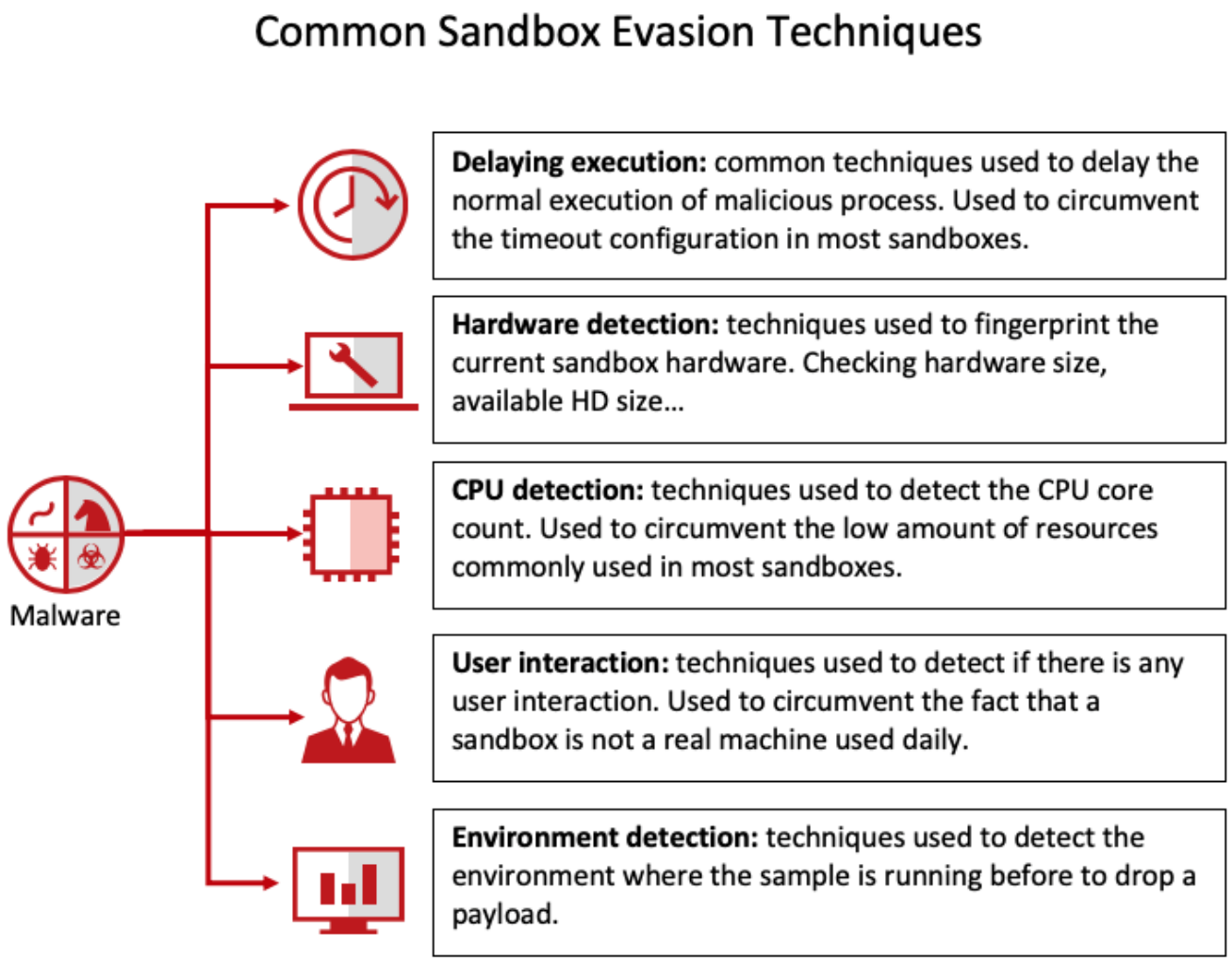


En conclusion pour le Sandboxing

- Pour être efficace, le sandboxing :
  - Être supporté par le jeu d'instruction du CPU;
  - Être intégré au noyau;
  - Être obligatoire (i.e., les applications doivent absolument être exécutées dans un environnement sandbox).

Est-ce quand même 100% efficace ?

- Selon McAfee, la détection anti-sandbox est de plus en plus en vogue du côté cybercriminel car les sandbox d'aujourd'hui deviennent le meilleur moyen pour obtenir une vue d'ensemble de la menace.
- Ils ont observé plusieurs souches de logiciels malveillants changer leurs tactiques pour garder une longueur d'avance au fur et à mesure que les bacs à sable devenaient plus sophistiqués et évoluaient pour vaincre les menaces.
- Le diagramme suivant montre l'une des astuces d'évasion de bac à sable les plus répandues



https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/