Chapitre 10
Sécurité

M1

Introduction

- Des mécanismes de protection des activités informatiques sont intégrés au SE.
- Les Fichiers, les périphériques et la mémoire doivent être protégés des accès abusifs et les processus doivent être des interférences indésirables avec les autres processus.
- Des mécanismes mettent en œuvre des politiques de protection.
- Dans certains cas, la politique est intégrée dans le SE, mais elle peut également être définie par l'administrateur système.
- Ainsi, une politique de protection détermine les processus qui sont autorisés à mettre fin à d'autres processus.
- Les mécanismes de protection servent à faire respecter cette politique. Cependant des politiques trop strictes dans ce domaine ne vont pas dans le sens de concept de partages des fichiers et de commodité d'accès. Il faut donc trouver un juste équilibre entre les objectifs concurrents

Introduction

- Un niveau de sécurité de système correspond au degré de protection des ressources en fonction de ses politiques de protection.
- Les mécanismes de sécurité s'efforcent d'accroitre le niveau de sécurité d'un système cependant les mécanismes qui atteignent des niveaux de sécurité élevés ont tendance à rendre le système moins souple d'utilisation. Là encore, un équilibre doit l'être trouver entre la protection du système er la commodité d'accès.
- Les mesures de sécurité essaient de traiter les menaces susceptibles de mettre en péril les politiques de protection du système.
- Les principaux composants de la sécurité sont : l'authentification, la prévention, la détection, l'identification et la correction.

Authentification de l'utilisateur

- Des nombreuses politique d'autorisation sont basées sur l'identité de l'utilisateur associé à un processus. Les SE ont besoin des mécanismes pour authentifier un utilisateur qui interagit avec l'ordinateur
- La technique d'authentification la plus fréquemment utilisée consiste à demander à l'utilisateur de fournir une ou plusieurs informations connues de lui seul
- Les sources d'information sur lesquelles peut reposer l'authentification comprend le numéro d'un compte, le NNI, le nom de jeune fille, de la mère ou la date de naissance, etc. Cependant, pour ces exemples, l'utilisateur n'est probablement la seule personne en mesure de répondre à ces question. Ainsi la connaissance de ces info n'identifie pas uniquement l'individu.
- L'authentification est généralement plus précise si elle se repose sur un mot de passe (une combinaison de symboles créée dans l'unique but de fournir une authentification).

Authentification de l'utilisateur

- On peut aussi utiliser des systèmes physiques comme la biométrie ou des cartes à puces.
- Les mots de passe sont fragiles : de nombreux logiciels permettent de cracker les mots de passe. Les principes qu'ils utilisent sont les suivants :
  - Utiliser des dictionnaires standards
  - Utiliser le contenu du fichier de mots de passe pour générer des mots de passe potentiels, comme le login
  - Utiliser le nom de l'utilisateur et toutes ses données associées
  - Utiliser un langage de description de modifications permettant de définir les transformations des mots de passe potentiels
  - Construire des statistiques à propos de la constitution des mots de passe déjà cassés.

Fragilité des mots de passe

- Temps de craquage par force brute (40M essais/seconde : PC)

	Taille du mot de passe	6	7	8	10
Type de mot de passe	Lettres seules (maj et min)	8 mn	7 h	15 j	114 ans
	Lettres (maj et min) et chiffres	24 mn	1 j	63 j	665 ans
	Plus caractères spéciaux (+28)	3 h 41 mn	19 j	2,5 ans	27600 ans

NB : - Les mots les plus probables sont testés en premier →temps beaucoup plus court
- Ces temps peuvent être divisés en utilisant des machines en réseau ou des circuits spécialisés (GPU, DSP) ou un superordinateur (1 million fois plus rapide 27600 ans → 10 j).

Sécurité des mots de passe

- **sous Windows**
  - Les mots de passe sont placés dans le fichier SAM (Security Accounts Manager)
  - Il sont cryptés par deux algorithmes différents (LANMAN et NTLM)
  - Le 1er crypte par DES le mot de passe mis en majuscules et complété par de 0 pour atteindre 14 caractères puis séparé en 2 moitiés
  - Le 2ème crypte le mot de passe exprimé en UNICODE (le résultat est sur 16 octets).
- **Sous LINUX**
  - A la création on ajoute au mot de passe un code sur 12 bits (salt) aléatoire
  - Le mot de passé est concaténé au salt et sont cryptés
  - Ces codes et les salts sont placés dans le fichier /etc/shadow qui n'est accessible que par root

Sécurité du système de fichiers

- Le contrôle d'accès est discrétionnaire en ce sens que le propriétaire d'un objet (fichier, répertoire …) peut en modifier les permissions d'accès.
- Principe de droits :
  - UNIX utilisait rwx (read/write/execute) avec les notions de utilisateur /groupe / autres
  - MSDOS et Windows 3.1 utilisaient (read/write/caché) sans notion d'utilisateur ni de groupe
  - Windows NT définit des droits pour chaque utilisateur et/ou chaque groupe. Mais un utilisateur peut apparaître en tant que tel puis en tant qu'appartenant à plusieurs groupes. Dans ce cas Windows combine les droits => on a les droits de chacun des groupes + ceux de l'utilisateur
- Exception : si dans l'un des groupes l'utilisateur n'a aucun droit c'est ce qui prend le dessus.

Principes de sécurité par ACL (Windows et Linux)

- La liste de contrôle d'accès ACL (Access Control List) spécifie pour chaque fichier qui, quels utilisateurs et groupes ont accès à ce fichier.
- Chaque entrée d'une ACL assigne à un utilisateur ou à un groupe un ou plusieurs des niveaux d'accès suivants aux fichiers :
  - **Aucun** n'accorde aucun accès au fichier.
  - **Lire** autorise l'affichage des données du fichier
  - **Écrire** autorise la modification des données du fichier
  - **Exécuter** autorise l'exécution du fichier programme.
  - **Supprimer** autorise la suppression du fichier.
  - **Modifier** les autorisations autorise le changement des autorisations sur le fichier.
  - **Appropriation** autorise l'appropriation du fichier.

Principes de sécurité par ACL

- La liste de contrôle d'accès ACL (Access Control List) spécifie pour chaque répertoire qui, quels utilisateurs et groupes ont accès à ce répertoire.
- Un jeu de privilèges similaire est défini sur les répertoires :
  - **Aucun** n'accorde aucun accès au répertoire.
  - **Lire** autorise l'affichage des noms de fichiers et de sous-répertoires
  - **Écrire** autorise l'ajout de fichiers et de sous-répertoires
  - **Exécuter** autorise la modification des sous-répertoires
  - **Supprimer** autorise la suppression de sous-répertoires.
  - **Modifier** les autorisations autorise le changement des autorisations du répertoire
  - **Appropriation** autorise l'appropriation du répertoire.

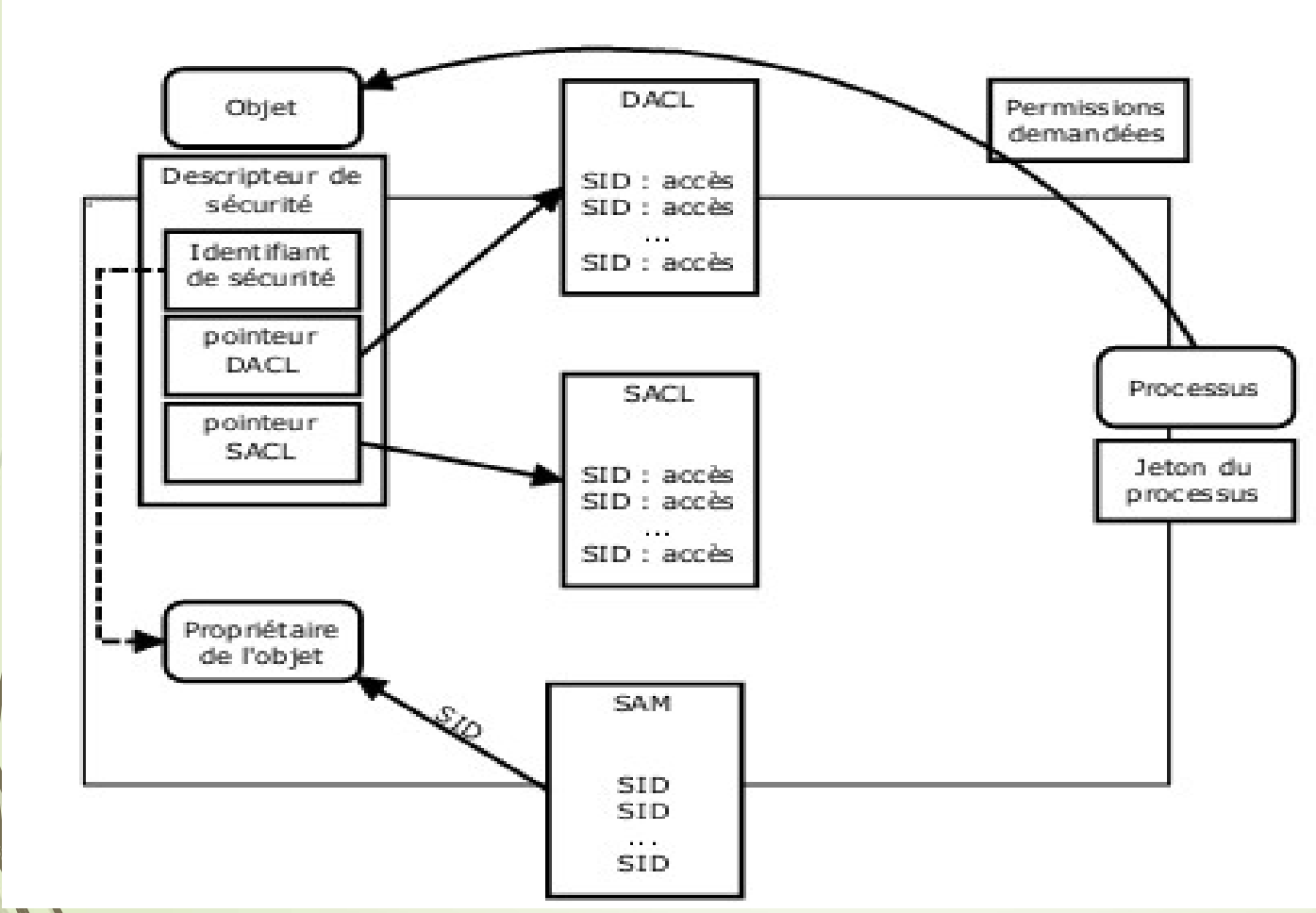
Modèle de sécurité de Windows

- Sous Windows, toutes les ressources sont gérées sous forme d'objets (les fichiers, les processus, les clés de la base de registres ...).
- Chaque objet du système est protégé par un descripteur de sécurité (SD) (Security Descriptor), qui définit quels types d'accès sont autorisés de la part de quelles entités.
- Chaque processus dispose d'un contexte de sécurité lui permettant d'accéder ou non à des objets. Cette structure, attachée à tout processus, porte le nom de jeton d'accès (AC) (access token).

Modèle de sécurité de Windows

- A tout objet est associé un descripteur de sécurité (SD), qui contient trois informations principales :
  - l'identifiant de sécurité (SID) du propriétaire de l'objet,
  - sa liste de contrôle d'accès discrétionnaire (DACL)
  - la liste de contrôle d'accès système (administrateur) (SACL)
- Un propriétaire est identifié par son SID placé dans la base de données de sécurité du système SAM (Security Account Manager) qui fait partie de la base d'enregistrement (base de registre : HKEY_LOCAL_MACHINE)

Modèle de sécurité de Windows



Modèle de sécurité de Windows

- La DACL est simplement une liste d'entrées de contrôle d'accès listant quels accès sont possibles à quels SID. Chaque entrée peut accorder un type d'accès ou le refuser.
- La SACL joue le même rôle pour le système (administrateur).
- Lorsque le processus veut accéder à un objet, le masque de permissions représente le type d'accès demandé

Modèle de sécurité de Windows

- Un jeton d'accès (AC) est attaché à chaque processus et définit son contexte de sécurité. En particulier par :
- identité et attributs d'autorisation :
  - SID du propriétaire du processus
  - Liste des SID des groupes locaux (au niveau du système local) dont le propriétaire fait partie.
  - Liste des SID des groupes globaux (au niveau du domaine)
  - SID indiquant le type de session de connexion (par exemple, interactive)
  - SID identifiant la session de connexion.
- sécurité par défaut pour les nouveaux objets créés

Modèle de sécurité de Windows

- L'algorithme utilisé pour le contrôle d'accès utilise trois éléments :
  - le masque de permissions représentant le type d'accès demandé
  - le descripteur de sécurité représentant la protection de l'objet
  - le jeton du processus, contenant les attributs d'autorisation
- L'algorithme utilisé est le suivant :
  - Si les permissions implicites sont suffisantes, l'accès est autorisé
  - Sinon chaque entrée de la DACL est examinée. Si elle autorise certaines permissions d'accès pour l'un des SID contenu dans le jeton, ces permissions sont ajoutées.

Modèle de sécurité de Windows

- L'algorithme se poursuit jusqu'à ce que l'un des trois événements suivants se produise :
  - Toutes les permissions présentes dans le masque de permissions spécifié lors de l'accès ont été accumulées, auquel cas l'accès est autorisé
  - Une entrée de la DACL refusant un accès à un SID contenu dans le jeton est rencontrée, auquel cas l'accès est refusé
  - La fin de la DACL est atteinte sans que toutes les permissions aient été accumulées, auquel cas l'accès est également refusé.

Quelques Ménaces du SE : LES VIRUS

- **Un virus** est un programme capable "d'infecter" d'autres programmes en les modifiant de façon à inclure une copie de lui-même, potentiellement évoluée » Frederick B. Cohen 1972
- Généralement les virus sont cachés dans un logiciel parfaitement fonctionnel
- Actuellement, l'objectif est de gagner de l'argent :
  - Vol d'informations bancaires
  - Appel de n°de téléphone
  - Spam
  - Bots pour le déni de service
  - Rançon (virus police, virus hadopi, …)

Les types de virus

On distingue les types de virus suivants :

- Les vers (worms) : se copient eux-mêmes et de se propagent à travers un réseau
- Les chevaux de Troie (trojans) : installent d'autres applications afin de pouvoir contrôler l'ordinateur qu'ils infectent depuis l'extérieur.
- Les bombes logiques : se déclenchent suite à un événement particulier (date système, activation distante, ...)
- Les Rootkits : dissimulent des objets sur les ordinateurs (processus, fichiers ...). Ils sont souvent utilisés par d'autres virus pour se cacher
- Les Exploits : exploitent une faille de sécurité dans un logiciel, un système d'exploitation ou un protocole de communication
- Les Adwares : affichent des publicités
- Les Spywares : collectent et transfèrent des informations

Les formes de virus

- On distingue cinq formes de virus :
- Les virus mutants : virus réécrits afin d'en modifier le comportement ou la signature (pratiquement tous)
- Les virus polymorphes : virus dotés de fonctions de chiffrement et de déchiffrement de leur signature
- Les rétrovirus : virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants
- Les virus de secteur d'amorçage : virus capables d'infecter le secteur de démarrage d'un disque (MBR master boot record)
- Les virus trans-applicatifs (virus macros) : virus situés à l'intérieur d'un banal document et exécutant une portion de code à l'ouverture de celui-ci.

Les antivirus

- Un antivirus est un programme capable de détecter la présence de virus et, dans la mesure du possible, de désinfecter ce dernier.
- On parle ainsi d'éradication de virus pour désigner la procédure de nettoyage de l'ordinateur.
- Il existe plusieurs méthodes d'éradication :
  - La suppression du code correspondant au virus dans le fichier infecté (pas toujours possible)
  - La suppression du fichier infecté
  - La mise en quarantaine du fichier infecté : le déplacer dans un emplacement où il ne pourra pas être exécuté (permet de le restaurer si on est sûr qu'il n'est pas dangereux, fausse alerte).

Les antivirus (détection de virus connus)

- L'antivirus s'appuie sur la signature (portion de code exécutable ajoutée par le virus au fichier infecté) propre à chaque virus.
- Il s'agit de la méthode de recherche de signature (scanning), la plus ancienne méthode utilisée par les antivirus. Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus et de toutes leurs variantes (mutants).
- Les virus polymorphes, dotés de capacités de camouflage, échappent à cette méthode. On utilise alors les méthodes génériques qui recherchent la partie du code du virus qui n'est pas modifiée mais ce n'est pas toujours efficace.

Les antivirus (détection de virus non connus)

- **Utilisation d'un contrôleur d'intégrité** pour vérifier si les fichiers ont été modifiés. Le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.
- **Surveillance du comportement des processus.** Pas exemple un processus qui modifie la base de registre ou accède à des fichiers système. Mais cela peut lever de fausses alertes

Les antivirus (détection de virus non connus)

- **Méthodes heuristiques** qui consistent à analyser le début du code d'un processus pour détecter soit une auto modification du code soit une tentative de trouver d'autres exécutables (pour les infecter) . Mais cela peut lever de fausses alertes
- **Méthode du bac à sable** consiste à exécuter le programme douteux dans un émulateur du système d'exploitation puis à analyser ce qu'il a modifié. L'émulateur évite les risques de modification réelle du système mais c'est lent.

Tester la présence d'un antivirus

- Test mis au point par le comité d'experts EICAR (European Institute for Computer Antivirus Research : http://www.eicar.org/) spécialistes de la sécurité informatique
  - Pour tester qu'un antivirus est actif, créer un fichier texte.
  - Tapez-y la ligne suivante :

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

- **Lors de l'enregistrement du fichier l'antivirus devrait réagir en signalant la présence du virus Eicar-Test-Signature ou Eicar-AV-Test**

la prévention

- la fonction la plus recherche d'un système de sécurité est d'empêcher que des intrus ne pénètrent dans le système.
- Les mesures préventives doivent être mises en place.
- Elles comprennent notamment :
- - Restreindre les nouveaux mots de passe pour ne conserver que ceux qui passent une série de test de qualité.
- - Demander à ce que les mots de passe soient changés régulièrement
- - Crypter les données soit lors de leur transmission, soit lors de leurs stockages.
- Des programmes tels que SSH PERMETTENT DE CRYPTER LES COMMUNICATION EN PARTANCE ET EN DESTINATION d'un site

la prévention

- - Désactiver des services inutilisés ou dupliqués.
- - Mettre en oeuvre un pare-feu interne. Des programmes comme tcpwrapper peuvent être configurés pour refuser l'accès réseau, en fonction de l'emplacement distant du service auquel on essaie d'accéder
- - Suivre les conseils de sécurité et mettre à jour les informations relatives aux logiciels et à la configuration comme il convient. Des groupes comme CERT et BugTraq fournissent des informations sur les vulnérabilités des sécurité et indiquent comment y remédier.

la correction

- Après qu'un système a été pénétré, il est souvent nécessaire d'entreprendre une action corrective :
- - Des sauvegardes périodiques doivent être effectués afin qu'un système puisse être ramené à un meilleur état antérieur. Les sauvegardes peuvent être stockées hors ligne et hors site, afin d'accroitre la probabilité que la sauvegarde ne soit pas endommagée au cours d'une attaque.
- - Si une sauvegarde n'existe pas ou que son intégrité est inconnu, un nouveau chargement du système entier peut se révéler nécessaire. Un enregistrement de tous les logiciels actuellement installés et des mises à jour simplifient l'effort de restauration.

la correction

- - il peut s'avérer nécessaire de changer toutes les informations de sécurité résidentes. Tous les utilisateurs peuvent être sollicités afin de modifier leur mot de passe.
- - la vulnérabilité ayant permis la pénétration du système doit être réparée. Cela peut inclure la désactivation d'un servie, l'installation d'un correcteur de bogue ou la modification du système de configuration.

L'identification

- Les programmes auxquels on accède par l'intermédiaire d'un réseau peuvent enregistrer l'adresse de l'ordinateur qui se connecté. Il est possible de remonter à l'origine des attaques relayées sur une série d'ordinateurs.
- Tous les services peuvent être configurés pour exiger une identification de l'utilisateur. Par exemple, un serveur mail peut refuser des servies mail à tout client non autorisé. Si ce serveur est utilisé pour relayer les virus par email, les informations d'authentifications peuvent être utiles à l'identification de la source.

L'identification

- Afin de décourager les intrus, il est recommandé d'identifier la source d'une attaque.
- L'indentification est généralement la tâche de sécurité la plus difficile.
- Des traces de contrôle peuvent fournir des informations d'identification intéressantes.
- Mais, en fonction de la nature de l'attaque et de l'emplacement du journal des erreurs, des informations contenues dans ce journal peuvent être modifiées par l'intrus.