Chap. I : Introduction à la sécurité informatique

Laurent Poinsot

UMR 7030 - Université Paris 13 - Institut Galilée

Cours " Sécrypt "

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs (examen systématique des candidats au cours de leur recrutement).
Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger fichiers et autres informations stockées est devenu évident. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de sécurité informatique.

Le second changement majeur qui affecte la sécurité est l'introduction de systèmes distribués et l'utilisation de réseaux et dispositifs de communication pour transporter des données entre un terminal utilisateur et un ordinateur, et entre ordinateurs. Les mesures de sécurité des réseaux sont nécessaires pour protéger les données durant leur transmission. On parle alors de sécurité des réseaux.

Il n'existe pas de frontières claires entre ces deux formes de sécurité. Par exemple, un des types d'attaque de systèmes d'information les plus médiatisés est le virus (informatique). Un virus peut être physiquement introduit dans un système via une disquette ou via Internet. Dans les deux cas, une fois le virus présent dans le système, des outils informatiques de sécurité sont nécessaires pour le détecter et le détruire.

Pour donner une idée des domaines couverts par la sécurité de l'information, considérons les exemples de violation de sécurité suivants :

- l'utilisateur *A* transmet un fichier à l'utilisateur *B*. Ce fichier contient une information sensible (par exemple, un projet de brevet) qui doit être protégée de toute divulgation. L'utilisateur *C*, qui n'est pas autorisé à consulter ce fichier, est en mesure de contrôler la transmission et de capturer une copie du fichier durant sa transmission ;
- une application de gestion de réseau D transmet un message à un ordinateur E sous son contrôle. Le message ordonne à l'ordinateur E de mettre à jour un fichier d'autorisation pour inclure l'identité de nouveaux utilisateurs devant avoir accès à cet ordinateur. L'utilisateur F intercepte le message, altère son contenu en ajoutant ou détruisant des entrées, et fait suivre le message à E, qui l'accepte comme issu du gestionnaire D et met à jour ses fichiers d'autorisation en conséquence ;

- plutôt que d'intercepter un message, l'utilisateur F construit son propre message avec l'entrée désirée et le transmet à E comme s'il venait du gestionnaire D. L'ordinateur E accepte le message et met à jour ses fichiers d'autorisation ;
- un employé est victime d'un licenciement qu'il juge abusif. Le responsable du personnel envoie un message à un serveur afin de supprimer son compte. Lorsque la supression est accomplie, le serveur poste une note à destination du dossier de l'employé pour confirmation de l'action. L'employé est en mesure d'intercepter le message, de le retarder et d'accéder au serveur afin d'y extraire une information sensible. Le message est ensuite réémis, l'action a lieu et la confirmation postée. L'acte de l'employé peut demeurer indétecté pendant un temps considérable ;
- un client envoie un message à un agent de change (un trader ?) avec l'instruction de diverses transactions. Par la suite, l'investissement perd de la valeur et le client nie avoir envoyé le message

Bien que la liste des exemples n'épuise pas tous les types possibles de violation de sécurité, elle illustre l'étendue des préoccupations en matière de sécurité des réseaux. La sécurité interréseau est tout à la fois fascinante et complexe, notamment pour les raisons suivantes :

- la sécurité impliquant communications et réseaux n'est pas aussi simple que pourrait le croire un novice. Les exigences semblent simples. En effet, celles concernant les services de sécurité peuvent se passer d'explication : confidentialité, authentification, non-répudiation, intégrité. Mais les mécanismes utilisés pour satisfaire ces exigences peuvent être très complexes (par exemple, les cryptosystèmes qui sont basés sur des propriétés mathématiques), et leur compréhension nécessiter des raisonnements subtiles ;

- en développant un mécanisme ou un algorithme de sécurité particulier, on doit toujours considérer les contre-mesures potentielles. Dans bien des cas, les contre-mesures sont conçues en considérant le problème différemment, par conséquent en exploitant une faiblesse inattendue du mécanisme ;
- du fait du point précédent, les procédures utilisées pour fournir un service particulier ne sont pas toujours intuitives. Il n'est pas évident, à partir d'une exigence donnée, de faire le lien avec les mesures compliquées nécessaires à sa réalisation. C'est seulement lorsque les contre-mesures sont considérées que la mesure utilisée prend tout sons sens ;
- une fois conçus divers mécanismes de sécurité, il est nécessaire de décider de leur utilisation. Cela est vrai tant en termes d'emplacement physique (par exemple, à quel point, dans un réseau, certains mécanismes de sécurité sont requis) que de sens logique (à quelle(s) couche(s) d'une architecture telle que TCP/IP placer certains mécanismes) ;

- les mécanismes de sécurité impliquent habituellement plus d'un algorithme ou protocole. Ils requièrent également que les participants soient en possession d'une information sécrète (par exemple, une clef de déchiffrement), ce qui soulève des questions concernant la création, la distribution et la protection de cette information secrète. Le degré de confiance dans les protocoles de communication, dont les comportements peuvent compliquer le développement de mécanismes de sécurité, est un autre souci. Par exemple, si le fonctionnement correct du mécanisme de sécurité requiert de préciser des limites temporelles sur le temps de transit d'un message, alors un protocole ou un réseau qui introduirait des délais variables ou imprévisibles peut rendre ces critères temporels caducs.

Ainsi, il y a beaucoup de concepts et d'idées à considérer. Ce chapitre fournit une vue générale des sujets principaux de la sécurité informatique. On commencera par un exposé des types d'attaques qui créent le besoin de services et de mécanismes de sécurité de réseau.

Attaques, servcices et mécanismes

Pour considérer efficacement les besoins de sécurité d'une organisation et évaluer et choisir les nombreux produits et politiques de sécurité, le responsable de la sécurité a besoin de moyens systématiques de définition des exigences de sécurité et de caractérisation des approches qui satisfont ces exigences. Une approche possible est de considérer trois aspects de la sécurité de l'information :

- services de sécurité : un service qui améliore la sécurité des systèmes informatiques et des transferts d'information d'une organisation. Les services sont conçus pour contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité ;
- mécanismes de sécurité : un mécanisme est conçu pour détecter, prévenir ou rattraper une attaque de sécurité.

- attaque de sécurité : une action qui compromet la sécuité de l'information possédée par une organisation.

Services (1/2)

On peut penser aux services de sécurité de l'information par analogie avec les types de fonctions associées aux documents physiques. La plupart des activité humaines, dans des domaines aussi divers que le commerce, la politique étrangère, les actions militaires, dépendent de l'utilisation de documents et de la confiance des deux partis en l'intégrité de ces documents. Les documents portent signatures et dates ; ils peuvent nécessiter une protection contre la divulgation, la falsification ou la destruction ; être attestés, enregistrés, etc. À mesure que les systèmes d'information deviennent plus diffus et essentiels à la conduite des affaires humaines, l'information électonique prend en charge bien des rôles traditionnellement dévolus aux documents papier. En conséquence, les fonctions associées aux documents papier doivent être accomplies sur des documents au format dématérialisé.

Services (2/2)

Plusieurs apsects propres aux documents électroniques font qu'assurer ces fonctions ou services est un défi :

- il est habituellement possible de distinguer entre un document papier original et sa photocopie. Cependant, un document électronique est purement une séquence de bits ; il n'y a pas de différence entre " l'original " et toutes ses copies ;
- une altération d'un document papier peut laisser des preuves physiques. Par exemple, un effacement peut laisser une tache ou une surface rugueuse. L'altération de bits dans une mémoire d'ordinateur ou un signal ne laisse a priori aucune trace ;

- tout processus de " preuve " associé à un document physique dépend des caractéristiques physiques du document (par exemple, la forme d'une signature manuelle ou un tampon de notaire). De telles preuves d'authenticité d'un document électronique doivent être basées sur des signes présents dans l'information elle-même.

Mécanismes

Un seul mécanisme ne peut fournir tous les services de sécurité. On peut noter qu'un élément particulier sous-tend la plupart des mécanismes de sécurité en usage : les techniques cryptographiques. Le chiffrement - ou des transformations similaires - de l'information est le moyen le plus courant pour fournir une sécurité. Ainsi, dans ce cours on insistera sur le développement, l'utilisation et la gestion de ces techniques.

Attaques

La sécurité de l'information traite de la prévention de la fraude, ou, à défaut, de sa détection dans des systèmes d'information à l'intérieur desquels l'information elle-même n'a pas d'existence physique significative. On verra dans les transparents suivants une liste d'exemples évidents de tricherie, qui se sont produits dans des cas réels. Ce sont des exemples d'attaques spécifiques qu'une organisation ou un individu peut avoir à affronter. La nature de l'attaque varie considérablement selon les circonstances. Heureusement, il est possible d'approcher le problème en examinant les types génériques d'attaques pouvant être rencontrées. Ce sera le sujet de la prochaine section.

Attaques : exemples

- Obtenir un accès non autorisé à l'information (c'est-à-dire, violer secret ou confidentialité) ;
- Usurper l'identité d'un autre utilisateur pour modifier ses attributs de responsabilité ou pour utiliser les droits de ce dernier dans le but de
  - diffuser une information frauduleuse ;
  - modifier une information légitime ;
  - utiliser une identité frauduleuse pour obtenir un accès non autorisé ;
  - faciliter des transactions frauduleuses ou en tirer partie.
- Refuser la responsabilité d'une information que le fraudeur a diffusée ;
- Prétendre avoir reçu de la part d'un autre utilisateur une information en fait créée par le fraudeur (par exemple, de fausses attributions de responsabilité ou de confiance).

- Prétendre avoir envoyé (à un moment donné) une information qui soit n'a pas été envoyée, soit l'a été à un autre moment ;
- Nier avoir reçu une information ou prétendre qu'elle a été reçue à un autre moment ;
- Étendre des droits d'un fraudeur (pour un accès à des informations) ;
- Modifier (sans autorisation) les droits d'autrui (les inscrire, restreindre ou élargir leurs droits, etc.) ;
- Dissimuler la présence d'information (la communication cachée) dans une autre information (la communication déclarée) ;
- S'insérer dans un lien de communication entre d'autres utilisateurs en tant que point de relai actif (et indétecté) ;
- Apprendre qui a accès à une information donnée (fichiers, etc.) et quand les accès sont réalisés, même si l'information elle-même reste cachée (par exemple, la généralisation de l'analyse de traffic de canaux de communication à des bases de données, des logiciels, etc.) ;

- Mettre en cause l'intégrité d'un protocole en révélant une information que le fraudeur est censé (selon les termes du protocole) garder secrète ;
- Pervertir la fonction d'un logiciel, en général par l'ajout d'une fonction cachée ;
- Faire qu'autrui viole un protocole en intoduisant une information incorrecte ;
- Saper la confiance en un protocole en causant des défaillances visibles dans le système ;
- Empêcher la communication entre d'autres utilisateurs, en particulier par des interférences afin que la communication authentique soit rejetée comme non authentique.

Attaques de sécurité

Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information. En général, il existe un flot d'information issu d'une source - un fichier ou une zone de la mémoire centrale -, vers une destination - un autre fichier ou utilisateur. Il existe quatre catégorie d'attaques : interruption, interception, modification, fabrication.

Attaques de sécurité : interruption

Un atout du système est détruit ou devient indisponible ou inutilisable. C'est une attaque portée à la disponibilité. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples.

Attaques de sécurité : interception

Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples.

Attaques de sécurité : modification

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon (presque) indétectable. Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.

Attaques de sécurité : fabrication

Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.

Attaques passives et attaques actives

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.

Attaques passives (1/2)

Écoutes indiscrètes ou surveillance de transmissions sont des attaques de nature passive. Le but de l'adversaire est d'obtenir une information qui a été transmise. Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic. La capture du contenu de messages est facilement compréhensible. Une conversation téléphonique, un courrier électronique ou un fichier transféré peuvent contenir une information sensible ou confidentielle.

Attaques passives (2/2)

La seconde attaque passive, l'analyse de trafic, est plus subtile. Supposons qu'un moyen de masquer le contenu des messages ou des informations soit à disposition (par exemple, un système de chiffrement), de sorte que les adversaires, même en cas de capture, ne pourront en extraire l'information contenue. Cependant l'adversaire pourra être en mesure d'observer le motif de ces messages, déterminer l'origine et l'identité des systèmes en cours de communication, et observer la fréquence et la longueur des messages échangés. Cette information peut être utile pour deviner la nature de la communication. Les attaques passives sont très difficiles à détecter car elles ne causent aucune altération des données.

Attaques actives (1/2)

La seconde catégorie d'attaques est l'attaque active. Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent être subdivisées en quatre catégories : mascarade, rejeu, modification de messages et déni de service. Une mascarade a lieu lorsqu'une entité prétend être une autre entité. Une attaque de ce type inclut habituellement une des autres formes d'attaque active. Par exemple, des séquences d'authentification peuvent être capturées et rejouées, permettant ainsi à une entité autorisée munie de peu de privilèges d'en obtenir d'autres en usurpant une identité possédant ces privilèges. Le rejeu implique la capture passive de données et leur retransmission ultérieure en vue de produire un effet non autorisé.

Attaques actives (2/2)

La modification de messages signifie que certaines portions d'un message légitime sont altérées ou que les messages sont retardés ou réorganisés. Par exemple, le message " autoriser X à lire le fichier confidentiel *comptes* " est modifié en " autoriser Y à lire le fichier confidentiel *comptes* ". Le déni de service empêche l'utilisation normale ou la gestion de fonctionnalités de communication. Cette attaque peut avoir une cible spécifique ; par exemple, une entité peut supprimer tous les messages dirigés vers une destination particulière. Une autre forme de refus de service est la perturbation d'un réseau dans son intégralité, soit en mettant hors service le réseau, soit en le surchargeant de messages afin de dégrader ses performances.

Une classification utile des services de sécurité est la suivante :

- confidentialité ;
- authenticité ;
- intégrité ;
- non-répudiation ;
- contrôle d'accès ;
- disponibilité.

Confidentialité

La confidentialité est la protection contre les attaques passives des données transmises. Plusieurs niveaux de protection de la confidentialité sont envisageables. Le service le plus général protège toutes les données transmises entre deux utilisateurs pendant une période donnée. Des formes restreintes de ce service peuvent également être définies, incluant la protection d'un message élémentaire ou même de champs spécifiques à l'intérieur d'un message. Un autre aspect de la confidentialité est la protection du flot de trafic contre l'analyse. Cela requiert qu'un attaquant ne puisse observer les sources et destinations, les fréquences, longueurs ou autres caractéristiques du trafic existant sur un équipement de communication.

Authentification

Le service d'authentification permet évidemment d'assurer l'authenticité d'une communication. Dans le cas d'un message élémentaire, tel un signal d'avertissement, d'alarme, ou un ordre de tir, la fonction du service d'authentification est d'assurer le destinataire que le message a bien pour origine la source dont il prétend être issu. Dans le cas d'une interaction suivie, telle une connexion d'un terminal à un serveur, deux aspects sont concernés. En premier lieu, lors de l'initialisation de la connexion, il assure que les deux entités sont authentiques (c'est-à-dire, que chaque entité est celle qu'elle dit être). Ensuite, le service dont assurer que la connexion n'est pas perturbée par une tierce partie qui pourrait se faire passer pour une des deux entités légitimes à des fins de transmissions ou de réceptions non autorisées.

Intégrité

À l'instar de la confidentialité, l'intégrité s'applique à un flux de messages, un seul message, ou à certains champs à l'intérieur d'un message. Là encore, la meilleure approche est une protection totale du flux. Un service d'intégrité orienté connexion, traitant un flot de messages, assure que les messages sont reçus aussitôt qu'envoyés, sans duplication, insertion, modification, réorganisation ou répétition. La destruction de données est également traitée par ce service. Ainsi, un service d'intégrité orienté connexion concerne à la fois la modification de flux de messages et le refus de service. D'un autre côté, un servide d'intégrité non orienté connexion, traitant des messages individuels sans regard sur un contexte plus large, fournit généralement une protection contre la seule modification de message.

Non-répudiation

La non-répudiation empêche tant l'expéditeur que le receveur de nier avoir transmis ou reçu un message. Ainsi, lorsqu'un message est envoyé, le receveur peut prouver que le messqge a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le receveur prétendu.

Contrôle d'accès

Dans le contexte de la sécurité des réseaux, le contrôle d'accès est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée, ou s'authentifier, de telle sorte que les droits d'accès puissent être adaptés à son cas.

Disponibilité

De nombreuses attaques peuvent résulter en une perte ou une réduction de la disponibilité d'un service ou d'un système. Certaines de ces attaques sont susceptibles d'être l'objet de contre-mesures automatiques, telle que l'authentification et le chiffrement, alors que d'autres exigent une action humaine pour prévenir ou se rétablir de la perte de disponibilité des éléments d'un système.

Bombe logique

Une Bombe logique est une partie d'un programme malveillant (virus, cheval de Troie, etc.) qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou encore que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein. Le virus Tchernobyl, qui fut l'un des virus les plus déstructeurs, avait une bombe logique qui s'est activée le 26 avril 1999, jour du treizième anniversaire de la catastrophe nucléaire de Tchernobyl.

Cheval de Troie

Un Cheval de Troie (trojan en anglais) est un programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime. La fonction illicite peut consister en la divulgation ou l'altération d'informations. Trojan.ByteVerify est un cheval de Troie sous forme d'une applet java. Ce cheval de Troie exploite une vulnérabilité de la machine virtuelle java de Microsoft permettant à un pirate d'exécuter du code arbitraire sur la machine infectée. Par exemple, Trojan.ByteVerify peut modifier la page d'accueil d'Internet Explorer.

Porte dérobée

Une porte dérobée (ou backdoor en anglais) est un moyen de contourner les mécanismes de contrôle d'accès. Il s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier). C'est donc une fonctionnalité inconnue de l'utilisateur légitime qui donne un accès secret au logiciel. Une porte dérobée a été découverte dans le SGBD *interbase* de Borland au début des années 2000. Il suffisait d'entrer le nom d'utilisateur " politically " et le mot de passe " correct " pour se connecter à la base de données avec les droits d'administrateur.

Virus

Un virus est un segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'une application), et qui devient ainsi un cheval de Troie. Puis le virus peut ensuite se propager à d'autres ordinateurs (via un réseau) à l'aide du programme légitime sur lequel il s'est greffé. Il peut également avoir comme effets de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. PsybOt, découvert en 2009, est considéré comme étant le seul virus informatique ayant la capacité d'infecter les routeurs et modems haut-débit.

Ver

Un ver est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer. Le ver a habituellement un objectif malicieux, par exemple :

- espionner l'ordinateur dans lequel il réside ;
- offrir une porte dérobée à des pirates informatiques ;
- détruire des données sur l'ordinateur infecté ;
- envoyer de multiples requêtes vers un serveur internet dans le but de le saturer.

Le ver Blaster avait pour but de lancer une attaque par déni de service sur le serveur de mises à jour de Microsoft.