

**RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE**

N° 650/DISSI/SCSSI le 28 Mars 1994

**LA MENACE
ET LES ATTAQUES INFORMATIQUES**

Délégation Interministérielle pour la Sécurité des Systèmes d'Information

SERVICE CENTRAL DE LA SÉCURITE DES SYSTEMES D'INFORMATION

Ce document présente les menaces d'origines interne et externe qui pèsent sur les systèmes d'information, ainsi que les attaques informatiques dont ceux-ci sont l'objet.

Il a été élaboré et rédigé sous l'égide de la sous-commission "système" de la commission interministérielle pour la sécurité des systèmes d'information.

1. Introduction

- 1.1 - Causes
- 1.2 - Conséquences
- 1.3 - Définitions
 - 1.3.1. - Actifs ou biens
 - 1.3.2. - Menace
 - 1.3.3. - Attaque
 - 1.3.4. - Vulnérabilité
 - 1.3.5. - Risque

2. Origine de la menace

- 2.1 - Généralités
- 2.2 - Accidents
- 2.3 - Menaces intentionnelles
 - 2.3.1. - Caractère stratégique
 - 2.3.2. - Caractère idéologique
 - 2.3.3. - Caractère terroriste
 - 2.3.4. - Caractère cupide
 - 2.3.5. - Caractère ludique
 - 2.3.6. - Caractère vengeur
- 2.4 - Conclusion sur le caractère de la menace

3. Catégories de menace

- 3.1 - Présentation
- 3.2 - L'espionnage
- 3.3 - La perturbation
- 3.4 - Le vol
- 3.5 - La fraude physique
- 3.6 - Le chantage
- 3.7 - Le sabotage
- 3.8 - Les accès illégitimes

4. Attaquants

- 4.1 - Motivations
- 4.2 - Profils
- 4.3 - Pirates
- 4.4 - Fraudeurs
- 4.5 - Espions
- 4.6 - Terroristes
- 4.7 - Aptitudes et classes d'attaque
- 4.8 - Ressources nécessaires

5. Techniques d'attaque

- 5.1 - Attaques physiques
 - 5.1.1. - Interception
 - 5.1.2. - Brouillage
 - 5.1.3. - Écoute
 - 5.1.4. - Balayage
 - 5.1.5. - Piégeage
- 5.2 - Attaques logiques
 - 5.2.1. - Fouille
 - 5.2.2. - Canal caché
 - 5.2.3. - Déguisement
 - 5.2.4. - Mystification
 - 5.2.5. - Rejeu
 - 5.2.6. - Substitution
 - 5.2.7. - Faufilement
 - 5.2.8. - Saturation
 - 5.2.9. - Cheval de Troie
 - 5.2.10. - Salami
 - 5.2.11. - Trappe
 - 5.2.12. - Bombe
 - 5.2.13. - Virus
 - 5.2.14. - Ver
 - 5.2.15. - Asynchronisme
 - 5.2.16. - Souterrain
 - 5.2.17. - Cryptanalyse

6. Conclusion

7. Références

1. - Introduction

Les Systèmes d'Information (SI) reposent en partie sur des machines qui stockent, traitent et transmettent de l'information [8]. Ces machines peuvent être, pour les plus sophistiquées, des ordinateurs mais aussi des périphériques informatiques, des téléphones, des télécopieurs, des télex... Elles sont souvent reliées par des réseaux locaux à l'intérieur de leur organisme d'appartenance, mais, dans de nombreux cas, elles permettent de communiquer avec l'extérieur. Certains SI offrent des services sur lesquels reposent l'économie des États et des entreprises. Ainsi de multiples informations, hier confinées dans les armoires, sont accessibles de presque n'importe quel point du globe alors que la dépendance vis-à-vis des services fragilise aussi bien leurs fournisseurs que leurs utilisateurs.

L'information est une ressource stratégique, une matière première, elle est un atout supplémentaire pour ceux qui la possèdent. La protection de ce patrimoine contre les malveillances doit par conséquent être un souci permanent.

• 1.1 - Causes

Les SI gèrent des informations qui peuvent être convoitées par des individus dont le spectre s'étale du simple potache qui cherche à occuper son temps, jusqu'au professionnel chevronné du renseignement en passant par le criminel de droit commun. En proposant de nouveaux services et en traitant toutes sortes d'informations les SI forment de nouvelles cibles qui ne sont pas toujours l'objet d'attentions particulières de la part de leurs propriétaires, qui vont parfois jusqu'à sous-estimer ou ignorer l'importance de leur capital.

La concentration des données et leur disponibilité sur un réseau permettent d'obtenir rapidement, dans la discrétion et parfois dans l'anonymat le plus complet, une grande quantité d'information qu'il était auparavant difficile de se procurer. Pour leur part, les services facilitent les échanges entre les acteurs économiques et permettent de traiter des problèmes de façon plus efficace et plus sûre.

Neumann et Parker [9] proposent trois raisons qui permettent d'expliquer que la menace pesant sur les SI est permanente et ne peut descendre en dessous d'un seuil incompressible :

- - il existe un fossé technologique entre ce qu'un système d'information est capable de faire et ce que l'on attend de lui ;
- - la loi, la réglementation et l'éthique sont toujours en retard sur la technique. Ceci vaut pour de nombreux domaines en dehors du traitement de l'information ;
- - les individus se comportent rarement comme on l'attend : un utilisateur jugé intègre par ses pairs peut dans certaines circonstances abuser de ses droits. Le comportement d'un individu confronté à des situations inhabituelles et critiques est imprévisible.

• 1.2 - Conséquences

Les menaces qui pèsent sur les SI sont de deux natures : interne et externe. Au delà de cette évidence, force est de constater que la menace interne représente plus de 70 à 80% des cas connus. Quand ce type de menace se concrétise par des attaques ou des fraudes, l'utilisateur, qui possède un accès légitime au SI et des services qu'il offre, tente d'obtenir ou de falsifier des informations, de perturber le fonctionnement du SI, en abusant de ses privilèges ou en les

accroissant. Réciproquement, la menace externe est le fait d'individus qui n'ont pas un accès légitime au SI et qui essaient de briser les barrières de sécurité lorsqu'elles existent.

Que la menace soit interne ou externe, l'information et les services fournis par le SI peuvent subir des préjudices qui se traduiront par une perte de confidentialité, d'intégrité ou de disponibilité [5]. Il en résulte une divulgation, une modification ou une destruction des données ou encore une impossibilité d'obtenir une information ou un service. Par ailleurs, les effets induits et non directement mesurables peuvent s'avérer catastrophiques pour l'entreprise ou l'organisme victime : atteinte à l'image de marque ou suppression d'emplois si le sinistre touche l'outil de production ou le produit vendu dans le cas d'un service par exemple.

- **1.3 - Définitions**

- **1.3.1 - Actifs ou biens**

Dans un SI, toutes les informations et tous les composants n'ont pas la même valeur. Celles et ceux qu'il est important de protéger parce que représentant un certain capital ou étant indispensables au bon fonctionnement d'un système sont généralement désignés par les termes actifs ou biens.

- **1.3.2 - Menace**

Nous reprendrons une terminologie usuelle qui définit la menace comme étant une *violation potentielle de la sécurité* [7]. D'une façon générale nous distinguerons les types de menace suivants, bien que pouvant se recouvrir :

- - la menace accidentelle : *menace d'un dommage non intentionnel envers le SI* [7]. Cette menace peut découler d'une catastrophe naturelle (incendie, inondation, tremblement de terre,...), d'une erreur dans l'exploitation du SI (manipulation, saisie, ...) ou de pannes qu'elles soient de matériel ou de logiciel. Nous ne traiterons pas cette catégorie de menace dans ce document ;
 - - la menace intentionnelle ou délibérée : par opposition à la précédente, elle est le fait d'un acte volontaire ;
 - - la menace active : *menace de modification non autorisée et délibérée de l'état du système* [7]. Si elle venait à se concrétiser, le SI, ou ses informations, subiraient un dommage ou une altération bien réelle ;
 - - la menace passive : *menace de divulgation non autorisée des informations, sans que l'état du système soit modifié* [7]. Une écoute de ligne ou une lecture de fichier sont des exemples de menaces passives ;
 - - la menace physique : menace qui pèse sur l'existence même et sur l'état physique du SI. Ce peut être une destruction après un sabotage, un incendie, un détournement ou un vol..

Les menaces sont permanentes et certaines ne peuvent être totalement supprimées.

- **1.3.3 - Attaque**

Une attaque est une action de malveillance consistant à tenter de contourner les fonctions de sécurité d'un SI [7]. Nous complétons cette définition en l'étendant aux mesures de sécurité et non pas uniquement aux fonctions.

- **1-3.4 - Vulnérabilité**

Une vulnérabilité peut se définir comme une faiblesse ou une faille dans les procédures de sécurité, les contrôles administratifs, les contrôles internes d'un système, qui pourrait être

exploitée pour obtenir un accès non autorisé à un SI, à un de ses services, à des informations ou à la connaissance de leur existence et permettre de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité du SI et de ses informations.

Dans certains cas le terme vulnérabilité est défini comme étant l'inverse de la quantité d'effort à fournir pour atteindre une information ou un bien.

Une classification des vulnérabilités est fournie dans [14].

- **1.3.5 - Risque**

Un risque est un danger, un inconvénient plus ou moins probable auquel on est exposé pour un système d'information, il est généralement admis que le risque est une fonction de la menace et des vulnérabilités.

2.- Origine de la menace

- **2.1 - Généralité**

La connaissance de l'origine de la menace est l'un des éléments qui va permettre au défenseur d'évaluer la force et les moyens de son agresseur potentiel. En comprenant les motivations de ce dernier, le défenseur pourra éventuellement adapter sa politique de sécurité et anticiper les actes malveillants. Un SI sera d'autant plus menacé que les informations qu'il possédera auront une valeur et pour leur propriétaire et pour d'autres entités. Il ne faut pas pour autant conclure qu'un SI ne gérant pas d'information de valeur n'est sujet à aucune menace : son rôle peut être primordial pour assurer un service.

Les origines que nous proposons sont celles de la Fiche d'Expression Rationnelle des Objectifs de Sécurité [3] *que nous avons complétées avec de nouveaux éléments*. Nous présentons ainsi le caractère stratégique, idéologique, terroriste, cupide, ludique ou vengeur de la menace. Cette liste n'est pas exhaustive car les composantes de la menace évoluent dans le temps. Pour un système gouvernemental par exemple la menace change selon que l'on est en temps de paix, de crise ou de guerre. Les effets de mode peuvent aussi influencer momentanément sur la prédominance d'une menace par rapport à une autre. Ajoutons que la menace est généralement composite ce qui rend plus difficile sa détermination pour le défenseur.

- **2.2 - Accidents**

Cette catégorie de menaces regroupe d'une part tous les événements naturels à caractère catastrophique comme les inondations, les incendies, les tremblements de terre et autres, mais aussi tous les types d'erreurs que l'on peut imaginer. Les erreurs, de saisie, de transmission, etc., seront le plus souvent provoquées par l'inattention ou le manque de formation des utilisateurs.

Notons que les conséquences des accidents seront le plus souvent les mêmes que celles dues aux malveillances.

- **2.3 - Menaces intentionnelles**

- **2.3.1 - Caractère stratégique**

Pour un Etat, la menace stratégique s'intéresse par essence à toutes les informations concernant le secret de Défense et la Sûreté de l'État, mais également à celles appartenant au patrimoine national, qu'il soit d'ordre scientifique, technique, industriel, économique ou diplomatique ; la menace stratégique, peut également attenter à la disponibilité de systèmes

d'information, dont le fonctionnement continu est nécessaire au fonctionnement normal des institutions. Elle est généralement le fait d'organismes gouvernementaux ou para-gouvernementaux structurés et organisés pour la recherche du renseignement et disposant de moyens financiers et techniques très importants leur permettant d'envisager tous types d'attaque sur un système.

Pour une entreprise ou une société, la menace d'origine stratégique aura pour but obtenir toute information sur les objectifs et le fonctionnement de celle-ci, pour récupérer des clients prospectés, des procédés de fabrication, des résultats de recherche et de développement et de porter atteinte à sa capacité de réaction. Elle sera principalement le fait de concurrents dont les moyens peuvent être proches de ceux d'un État.

- **2.3.2 - Caractère idéologique**

Les motivations idéologiques peuvent être les moteurs d'actes les plus extrêmes. Le combat pour les idées est incessant. Si la menace née des antagonismes est-ouest semble quelque peu diminuer, il ne faut pas pour autant négliger les confrontations qui pourraient résulter des divergences nord-sud ou entre l'orient et l'occident sur le plan des idées, de la culture ou de la religion.

D'autres idéologies, raciales ou religieuses, resurgissent à la faveur d'une situation économique tendue. Cette menace peut s'appliquer aux nombreux fichiers informatiques constitués dans le monde et comportant des informations à caractère privé sur les individus.

Enfin, il existe des courants de pensée qui mettent en avant le fait que l'information doit être libre et ne peut en aucun cas être la propriété d'une personne, d'un groupe, d'une organisation ou d'un État. Cette vision du monde est partagée par de nombreux pirates [1].

- **2.3.3 - Caractère terroriste**

On définira la menace terroriste comme regroupant toutes les actions concourant à déstabiliser l'ordre établi ; les actions entrant dans cette catégorie peuvent avoir un caractère violent (destruction physique de systèmes) ou plus insidieux (intoxication et désinformation par détournement ou manipulation d'informations, sensibles ou non, perturbations engendrées dans un système et susceptibles de déclencher des troubles sociaux présents à l'état latent...). Mais leurs auteurs recherchent en général un résultat spectaculaire et les effets médiatiques qui l'accompagnent. Ce mode d'action est l'arme privilégiée des minorités.

Les groupes, susceptibles de commettre ce genre de forfaits, disposent généralement de moyens financiers importants et complicités au niveau international, leur permettant d'envisager pratiquement tous types d'attaque sur un système. Cette menace peut aussi être brandie par un État qui veut mener une action de déstabilisation.

- **2.3.4 - Caractère cupide**

Cette nouvelle forme de délinquance, engendrée par l'apparition des procédés de traitement de l'information, et parfois dite en col blanc, peut avoir deux différents buts, parfois concomitants :

- - le premier se traduit par un gain pour l'attaquant ; ce gain peut être financier (détournement de fonds), lié à un savoir-faire (vol de brevet, concurrence déloyale...), ou de tout autre ordre ;

- - le second occasionne une perte pour la victime qui se traduira par un gain pour l'agresseur (parts de marché, accès au fichier des clients, à des propositions commerciales...) ; ce peut être la destruction de son système ou de ses informations, une perte de crédibilité ou de prestige (image de marque) vis-à-vis d'une tierce personne, etc.

Il est difficile de caractériser, même succinctement, le profil type du fraudeur, tant les applications susceptibles d'être attaquées sont multiples. Néanmoins, les statistiques à ce sujet permettent de souligner que dans un grand nombre de cas, la menace a été initiée et mise en oeuvre à l'intérieur même de l'organisme abritant le système et a été le fait d'employés, dont les antécédents ne permettaient pas de supposer qu'ils commettraient un forfait de ce type. Les victimes figurent en général parmi les organismes qui détiennent l'argent : banques, compagnies d'assurances, etc.

Pour sa part le concurrent déloyal est plus facile à identifier : il figure parmi les concurrents, pour peu qu'ils soient connus !

Nous ajouterons dans cette catégorie le crime organisé qui pourrait prendre de l'importance dans un futur proche s'il s'avère qu'il est plus facile - moins coûteux et moins risqué - de détourner les fonds de manière électronique qu'en pillant une banque.

• **2.3.5 - Caractère ludique**

Les nouvelles techniques de traitement de l'information (micro-ordinateurs, modem, minitel...) ont créé cette menace, qui procède d'avantage, dans l'esprit de ceux qui en sont les auteurs, d'un jeu ou d'un loisir que d'un réel forfait (intrusion dans des systèmes, développement de virus ou de vers informatiques...). Animés d'un désir de s'amuser ou bien d'apprendre, ces auteurs sont souvent des adolescents et des étudiants possédant de bonnes connaissances techniques [1].

Motivée par la recherche d'une prouesse technique valorisante destinée à démontrer la fragilité du système plutôt que par souci de nuire, elle recrute ses auteurs parmi les jeunes soucieux de s'affirmer, et ses victimes dans les organismes à forte notoriété sur le plan technique ou réputés inviolables. Les moyens financiers et techniques dont disposent les personnes, agissant souvent isolément, qui commettent de telles actions, sont généralement modestes, et seule leur bonne connaissance du système visé leur permet de s'y introduire de façon efficace.

• **2.3.6 - Caractère vengeur**

La vengeance peut être la motivation de l'employé brimé, qui se sent mal utilisé par rapport à ses capacités, qui vient d'être licencié ou qui sait qu'il va être. Il faut alors craindre des actes destructeurs et souvent non corrélés avec leur cause dans le temps.

Les résultats consécutifs à une vengeance se verront ou se comprendront parfois bien après qu'ils aient été initiés.

• **2.4 - Conclusion sur le caractère de la menace.**

Les aspects de la menace évoqués dans ce paragraphe ne constituent pas une classification exhaustive, mais ces origines sont parmi les plus courantes. La menace n'est pas monolithique ; elle est souvent composite comme l'illustre le cas tristement célèbre du Chaos Computer Club où certains pirates ont mis leurs talents aux services d'organismes de renseignement dans un but purement lucratif.

3.- Catégories de menace

- **3.1 - Présentation**

Nous avons déjà dit que la concrétisation d'une menace peut se traduire par une perte de confidentialité, d'intégrité ou de disponibilité pour les informations et les services. Les pertes peuvent être, partielles ou totales avec les conséquences qui en découlent : divulgation d'informations stratégiques pour un État ou une entreprise, avec éventuellement mise en cause de son avenir pour cette dernière, perte d'argent, de marché...

Des menaces différentes peuvent avoir les mêmes effets. Nous proposons, comme dans les autres paragraphes, une liste non exhaustive de catégories de menaces parmi les plus courantes.

- **3.2 - L'espionnage**

Principalement d'origine étatique cette menace concerne particulièrement les informations stratégiques d'une nation. Les renseignements d'ordre militaire, diplomatique, mais aussi, économiques, industriels, technologiques, scientifiques, financiers et commerciaux seront recherchés en priorité.

S'il est moins fréquent, mais surtout non avoué que des entreprises ou des sociétés aient recours à l'espionnage, nous pouvons imaginer l'intérêt que cela représente pour leur activités en gain de temps et d'investissement. Les techniques restent les mêmes et la différence se fera sur l'ampleur des moyens utilisés. Il est concevable de penser que des États utilisent leurs services de renseignement pour fournir des informations à leurs industriels. Il est aussi de notoriété publique que des sociétés privées offrent leur services pour obtenir des renseignements.

L'espionnage va tenter d'enfreindre les mesures de sécurité qui protègent la confidentialité des informations.

- **3.3 - La perturbation**

L'agresseur va essayer de fausser le comportement du SI ou de l'empêcher de fonctionner en le saturant, en modifiant ses temps de réponse ou en provoquant des erreurs. L'agresseur veut désorganiser, affaiblir ou ralentir le système cible.

La perturbation va influencer sur la disponibilité et l'intégrité des services et des informations d'un SI.

- **3.4 - Le vol**

Le vol, visible quand l'objet du délit est matériel, est difficile à détecter quand il s'agit de données et encore plus de ressources informatiques. En effet une simple copie suffit pour s'approprier une information. Cette opération n'est pas toujours facile à déceler.

Le vol de données va permettre d'enfreindre les mesures de sécurité protègent la confidentialité des informations. Le vol de ressources est plus insidieux, car il se peut qu'il soit réalisé sans porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des informations et des services.

- **3.5 - La fraude physique**

Elle peut consister à récupérer les informations oubliées ou non détruites par l'adversaire ou le

concurrent. l'attaquant portera une attention particulière aux listages, aux supports physiques usagés (bandes magnétiques, disquettes, disques classiques ou optiques...), et s'intéressera aux armoires, aux tiroirs et aux dossiers des organismes visés.

Comme l'espionnage, la fraude physique va tenter d'enfreindre les mesures de sécurité qui protègent la confidentialité des informations.

- **3.6 - Le chantage**

Soutirer de l'argent à un organisme ou à une personne est d'autant plus tentant que de nombreuses données concernant la vie privée des personnes ou les activités d'une organisation sont gardées sur des ordinateurs.

Le chantage peut aussi porter sur une menace de sabotage à l'encontre des installations d'une organisation.

La chantage peut mettre en cause aussi bien la confidentialité, l'intégrité, que la disponibilité des informations et des services.

- **3.7 - Le sabotage**

Plus fort que la perturbation, le sabotage a pour but de mettre hors service un SI ou une de ses composantes.

Le sabotage porte atteinte à l'intégrité des informations mais surtout à la disponibilité des services.

- **3.8 - Les accès illégitimes**

Cette menace est le fait d'une personne qui se fait passer pour une autre en usurpant son identité. Elle vise tout particulièrement l'informatique.

Les accès illégitimes portent atteinte à la confidentialité des informations.

4. - Attaquants

- **4.1 - Motivations**

Les motifs de l'agresseur sont nombreux et variés ; ils évoluent dans le temps. Il n'est pas possible de dresser une liste exhaustive des motivations des criminels en col blanc mais quelques exemples permettront de saisir la personnalité de quelques uns d'entre eux. Les actes intentionnels, qui nous intéressent ici, comprennent : l'espionnage, l'appât du gain, la fraude, le vol le piratage, le défi intellectuel, la vengeance, le chantage, l'extorsion de fonds. Nous compléterons cette liste par celles des actes non intentionnels mais qui constituent une menace pour le SI [9] : la curiosité, l'ennui, la paresse, l'ignorance, l'incompétence, l'inattention...

- **4.2 - Profils**

Bien qu'il n'y ait pas de portrait robot de l'attaquant, quelques enquêtes et études ont montré que les criminels en informatique étaient majoritairement des hommes ayant un travail peu gratifiant mais avec d'importantes responsabilités et un accès à des informations sensibles [10]. L'avidité et l'appât du gain sont les motifs principaux de leurs actes, mais il apparaît que les problèmes personnels ainsi que l'ego jouent un rôle primordial en influant sur le comportement social [11].

- **4.3 - Pirates**

Nous proposons les deux profils de pirate les plus souvent identifiées :

- - *hacker* : individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement et possède souvent un code d'honneur et de conduite [1]. Plutôt jeune, avec des compétences non négligeables, il est patient et tenace ;
- - *cracker* : plus dangereux que le hacker, cherche à nuire et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

Les pirates possèdent rarement des moyens importants : assez fréquemment il s'agira d'un micro-ordinateur associé à un modem ou à un minitel, sauf s'ils utilisent des relais pour pénétrer leurs attaques.

Leur population, tend à s'accroître car les compétences en informatique se répandent et les SI sont de plus en plus nombreux. Les pirates communiquent par l'intermédiaire de revues spécialisées et vont jusqu'à s'organiser en clubs comme le Chaos Computer Club.

- **4.4 - Fraudeurs**

Les fraudeurs se répartissent en deux catégories avec des compétences similaires :

- - le fraudeur interne : possédant de bonnes compétences sur le plan technique, il est de préférence informaticien et sans antécédents judiciaires. Il pense que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur. Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Pour parvenir à ses fins il possède les moyens mis à sa disposition par son entreprise qu'il connaît parfaitement.
- - le fraudeur externe : bénéficiant presque toujours d'une complicité, volontaire ou non, chez ses victimes, il cherche à gagner de l'argent par tous les moyens. Son profil est proche de celui du malfaiteur traditionnel. Parfois lié au grand banditisme, il peut attaquer une banque, falsifier des cartes de crédit ou se placer sur des réseaux de transfert de fonds, et si c'est un particulier il peut vouloir fausser sa facture d'électricité ou de téléphone.

- **4.5 - Espions**

Ils travaillent pour un État ou pour un concurrent. Choisis pour leur sang-froid et leur haut niveau de qualification, il sont difficiles à repérer.

- - l'espion d'État : professionnel, entraîné, rompu à toutes les techniques, il dispose de nombreux moyens d'attaque et d'une importante puissance de calcul. Il peut aller jusqu'à acquérir, légalement ou non, une copie du système qu'il veut attaquer pour l'analyser et l'étudier sous toutes ses coutures. Il est patient et motivé. Il exploite les vulnérabilités les plus enfouies d'un SI car elles seront les plus difficiles à détecter et il pourra les utiliser longtemps. Il sait garder le secret de sa réussite pour ne pas éveiller les soupçons et continuer son travail dans l'ombre [12].
- - l'espion privé : souvent ancien espion d'État reconverti, il a moins de moyens mais une aussi bonne formation.

- **4.6 - Terroristes**

Moins courant, le terroriste est aidé dans sa tâche par l'interconnexion et l'ouverture des réseaux.

- - le terroriste : très motivé, il veut faire peur et faire parler de lui. Ses actions se veulent spectaculaires.

- **4.7 - Aptitudes et classes d'attaque**

Le succès d'une attaque dépend en partie de la compétence et de l'entraînement de son auteur. Le niveau de l'attaquant varie de l'expert au novice. Les domaines de connaissance seront cependant presque toujours l'informatique en général et en particulier la programmation, les systèmes d'exploitation, les communications mais aussi le matériel (routeurs, commutateurs, ordinateurs...). Selon Neumann et Parker [9], nous pouvons classer les méfaits en trois niveaux pour la compétence requise :

- - compétence technique faible ou nulle pour dénaturer une information, observer, fouiller physiquement, voler, abîmer un équipement, perturber un SI, entrer des données fausses, se mettre de connivence avec un étranger à l'organisation...
- - compétence technique moyenne pour balayer un SI et chercher des information, fouiller logiquement, inférer, faire des agrégats, surveille le trafic ou une activité, écouter, faire fuir de l'information, se faire passer pour quelqu'un d'autre, rejouer une transaction, abuser de ses droits, exploiter une trappe...
- - compétence forte pour modifier le système, exploiter un cheval de Troie, fabriquer une bombe logique, un ver ou un virus, réaliser une attaque asynchrone, modifier le matériel, décrypter...

Ces compétences sont souvent présentes dans un organisme et parfois à l'insu des dirigeants qui connaissent mal les capacités de leur personnel. Cette méconnaissance peut aussi expliquer le nombre d'attaques internes, les politiques de sécurité étant inadaptées ou sous-estimant les agresseurs potentiels.

- **4.8 - Ressources nécessaires**

Les ressources requises vont de pair avec les compétences et dépendent des techniques utilisées. Un attaquant voulant s'emparer d'informations chiffrées disposera d'importants moyens de calcul, ou de complicités internes, pour ensuite briser l'algorithme de chiffrement.

Notons tout de même que ce cas est extrême et concerne la menace d'origine stratégique. L'attaquant classique possédera probablement un ou des ordinateurs plus modestes, mais puisera sa connaissance dans la documentation technique et la littérature ouvert. Il se procurera les logiciels nécessaires à l'accomplissement de ses méfaits sur des serveurs publics ou les développera lui-même.

5.- Techniques d'attaque

Nous présentons quelques types d'attaque génériques et par ailleurs très connus. Remarquons à nouveau qu'il n'est pas toujours besoin d'être un spécialiste de l'informatique pour s'emparer de façon illicite d'informations intéressantes.

Les attaques peuvent porter entre autres sur les communications, les machines, les traitements, les personnels et l'environnement. Nous les classons en deux catégories : attaques physiques, attaques logiques.

- **5.1 - Attaques physiques**

Nous plaçons ici les attaques qui nécessitent un accès physique aux installations ou qui se servent de caractéristiques physiques particulières. La destruction pure et simple ou la coupure d'une ligne ne sont pas évoquées car non spécifiques à l'informatique.

- **5.1.1 - Interception**

L'attaquant va tenter de récupérer un signal électromagnétique et de l'interpréter pour en déduire des informations compréhensibles. L'interception peut porter sur des signaux hyperfréquences ou hertziens, émis, rayonnés, ou conduits. L'agresseur se mettra ainsi à la recherche des émissions satellites, et radio, mais aussi des signaux parasites émis par les SI, principalement par les terminaux, les câbles et les éléments conducteurs entourant les SI. Les techniques d'interception seront très variées pour les différents cas évoqués.

Pour se protéger, le défenseur pourra sécuriser ses transmissions (TRANSEC) en utilisant des appareils à saut de fréquence et diminuer le nombre et l'intensité des signaux parasites compromettants de ses SI (utilisation de matériels dits TEMPEST). Il devra en outre vérifier ses matériels pour éviter tout piégeage ou altération dans le temps. Pour cela, il lui faut avoir l'assurance que ses matériels sont conformes à ce qu'il en attend et vérifier que les procédures de maintenance ne viennent pas les altérer.

- **5.1.2 - Brouillage**

Utilisée en télécommunication, cette technique rend le SI inopérant. C'est une attaque de haut niveau, car elle nécessite des moyens importants, qui se détectent facilement. Elle est surtout utilisée par les militaires en temps de crise ou de guerre. Le défenseur se protégera avec des techniques TRANSEC.

- **5.1.3 - Écoute**

L'écoute consiste à se placer sur un réseau informatique ou de télécommunication et à analyser et à sauvegarder les informations qui transitent. De nombreux appareils du commerce facilitent les analyses et permettent notamment d'interpréter en temps réel les trames qui circulent sur un réseau informatique.

Des protections physiques, pour les réseaux informatiques, ou le chiffrement (COMSEC), pour tous types de réseaux, offrent une protection adéquate pour faire face à ce type d'attaque.

- **5.1.4 - Balayage**

Le balayage consiste à envoyer au SI un ensemble d'informations de natures diverses afin de déterminer celles qui suscitent une réponse positive. L'attaquant pourra aisément automatiser cette tâche et déduire par exemple les numéros téléphoniques qui permettent d'accéder à un système, le type dudit système et pourquoi pas le nom de certains utilisateurs ainsi que leur mot de passe. Cette technique est analogue à celle qui consiste à balayer une gamme de fréquences pour trouver un signal porteur.

- **5.1.5 - Piégeage**

L'agresseur tentera d'introduire des fonctions cachées, en principe en phase de conception, de

fabrication, de transport ou de maintenance, dans le SI. Seule une évaluation de la sécurité du SI donnera au défenseur une certaine assurance [5], [6].

- **5.2 - Attaques logiques**

- **5.2.1 - Fouille**

La fouille informatique, par analogie avec la fouille physique, consiste à étudier méthodiquement l'ensemble des fichiers et des variables d'un SI pour en retirer des données de valeur. Cette recherche systématique d'informations est en général grandement facilitée par la mauvaise gestion des protections classiques qu'il est possible d'attribuer à un fichier. Quand on se déplace dans les divers répertoires d'un système informatique, il est courant de constater que des fichiers et des répertoires ont des protections insuffisantes contre des agresseurs potentiels, uniquement par manque de connaissance, dû le plus souvent à l'insuffisance de formation, de l'utilisateur. Ainsi, est-il bien utile de donner un droit de lecture à ses fichiers pour l'ensemble des utilisateurs du système ?

Si l'attaquant est quelque peu entraîné, il aura recours à une attaque plus subtile. Pour s'emparer de certaines informations il va lire la mémoire, centrale ou secondaire, ou les supports de données libérés par les autres utilisateurs. Une parade efficace consiste à effacer physiquement toute portion de mémoire ou tout support libéré. En contrepartie, les performances du SI seront moindres.

- **5.2.2 - Canal caché**

Ce type d'attaque est de très haut niveau et fait appel à l'intelligence de l'attaquant. Il permet de faire fuir des informations en violant la politique de sécurité. Knod propose de classer les canaux cachés en quatre catégories [15] :

- - les canaux de stockage qui permettent de transférer de l'information par le biais d'objets écrits en toute légalité par un processus et lus en toute légalité par un autre ;
- - les canaux temporels qui permettent à un processus d'envoyer un message à un autre en modulant l'utilisation de ses ressources système afin que les variations des temps de réponse puissent être observées ;
- - les canaux de raisonnement qui permettent à un processus de déduire de l'information à laquelle il n'a pas normalement accès ;
- - les canaux dits de "fabrication" qui permettent de créer de l'information en formant des agrégats qui ne peuvent être obtenus directement.

Ces attaques sont perpétrées dans le système ou les bases de données à plusieurs niveaux de confidentialité.

- **5.2.3 - Déguisement**

Forme d'accès illégitime, il s'agit d'une attaque informatique qui consiste à se faire passer pour quelqu'un d'autre et obtenir les privilèges ou des droits de celui dont on usurpe l'identité.

Un utilisateur est caractérisé par ce qu'il est, (empreintes, digitales ou palmaires, rétiniennes, vocales, ou toute autre authentifiant biométrique), ce qu'il possède (un badge, une carte magnétique, à puce, un jeton, un bracelet...) et ce qu'il sait (un mot de passe, sa date de naissance, le prénom de ses parents...). Pour se faire passer pour lui, un agresseur doit donc s'emparer d'un ou plusieurs éléments propres à l'utilisateur. Si le contrôle d'accès au SI se fait par mot de passe, l'attaquant tentera de le lire quand l'utilisateur le rentrera au clavier ou quand il le transmettra par le réseau. Si le contrôle d'accès se fait avec une carte à puce, l'attaquant cherchera à

en dérober ou en reproduire une. Si le contrôle d'accès est biométrique, la tâche de l'attaquant sera plus difficile mais pas impossible comme le montre ce cas où un dirigeant d'entreprise a été enlevé par des malfaiteurs qui lui ont sectionné un doigt afin de tromper un système de contrôle d'accès.

Sans arriver à des solutions lourdes et coûteuses, le défenseur pourra combiner des méthodes d'identification et d'authentification comme carte et mot de passe pour renforcer sa sécurité.

- **5.2.4 - Mystification**

Dans ce cas, l'attaquant va simuler le comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son nom et de son mot de passe. Un exemple type est la simulation de terminal et le comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son nom et de son mot de passe. Un exemple type est la simulation de terminal.

Un protocole d'authentification de la machine de destination permettra à un utilisateur d'être sûr de son interlocuteur.

- **5.2.5 - Rejeu**

Le rejeu est une variante du déguisement qui permet à un attaquant de pénétrer dans un SI en envoyant une séquence de connexion effectuée par un utilisateur légitime et préalablement enregistrée à son insu.

- **5.2.6 - Substitution**

Ce type d'attaque est réalisable sur un réseau ou sur un SI comportant des terminaux distants. L'agresseur écoute une ligne et intercepte la demande de déconnexion d'un utilisateur travaillant sur une machine distante. Il peut alors se substituer à ce dernier et continuer une session normale sans que le système note un changement d'utilisateur.

Un cas bien connu est celui des ordinateurs sur un réseau local qui ne sont déclarés que par leur adresse Internet. Un attaquant peut alors attendre qu'une machine soit arrêtée pour se faire passer pour elle en usurpant l'adresse de la machine éteinte.

Les techniques et outils de détection d'intrusion pourront contribuer à identifier ce type d'attaque.

- **5.2.7 - Faufilement**

Par analogie avec le faufilement physique où une personne non autorisée franchit un contrôle d'accès en même temps qu'une personne autorisée, on dira qu'il y a faufilement électronique quand, dans le cas où des terminaux ou des ordinateurs ne peuvent être authentifiés par un SI, un attaquant se fait passer pour le propriétaire de l'ordinateur ou du terminal.

- **5.2.8 - Saturation**

Cette attaque contre la disponibilité consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser. Il en résultera un déni de service.

- **5.2.9 - Cheval de Troie**

Subterfuge employé par les grecs pour prendre Troie, en informatique un cheval de Troie est un programme qui comporte une fonctionnalité cachée connue de l'attaquant seul. Elle lui permet de contourner des contrôles de sécurité en vigueur. Cependant un cheval de Troie doit

d'abord être installé et ceci n'est possible que si les mesures de sécurité sont incomplètes, inefficaces ou si l'agresseur bénéficie d'une complicité.

Un cheval de Troie doit être attirant (nom évocateur) pour être utilisé, posséder l'apparence d'un authentique programme (un utilitaire par exemple) pour inspirer confiance et enfin ne pas laisser de traces pour ne pas être détecté. La simulation de terminal, dont le but est de s'emparer du mot de passer d'un utilisateur, est un cheval de Troie.

En conséquence, identifier la présence d'un cheval de Troie n'est pas aisée et une bonne connaissance du système et des applications installées est nécessaire.

- **5.2.10 - Salami**

La technique du salami permet à un attaquant de retirer des informations parcellaires d'un SI afin de les rassembler progressivement et de les augmenter de façon imperceptible. Cette technique est utilisée par de nombreux fraudeurs pour détourner subrepticement des sommes d'argent soit en s'appropriant de faibles sommes sur de nombreux comptes, soit en faisant transiter d'importantes valeurs sur des périodes courtes mais sur des comptes rémunérés leur appartenant.

- **5.2.11 - Trappe**

Une trappe est un point d'entrée dans une application généralement placé par un développeur pour faciliter la mise au point des programmes. Les programmeurs peuvent ainsi interrompre le déroulement normal de l'application, effectuer des tests particuliers et modifier dynamiquement certains paramètres pour changer le comportement original. Il arrive quelquefois que ces points d'entrée en soient pas enlevés lors de la commercialisation des produits et qu'il soit possible de les utiliser pour contourner les mesures de sécurité.

Un exemple connu est celui de l'exploitation du mode *debug* du programme *sendmail* utilisé par Robert T. Morris lors de son attaque par un ver sur Internet [2].

- **5.2.12 - Bombe**

Une bombe est un programme en attente d'un événement spécifique déterminé par le programmeur et qui se déclenche quand celui-ci se produit. Ce code malicieux attend généralement une date particulière pour entrer en action. Les conséquences peuvent être bénignes comme l'affichage d'un message, d'une image ou d'un logo mais aussi dommageables, comme la destruction de données et plus rarement la destruction du matériel. Les effets visuels et sonores sont fracassants.

- **5.2.13 - Virus**

Nommé ainsi parce qu'il possède de nombreuses similitudes avec ceux qui attaquent le corps humain, un virus est un programme malicieux capable de se reproduire et qui comporte des fonctions nuisibles pour le SI : on parle d'infection. Le virus dispose de fonctions qui lui permettent de tester s'il a déjà contaminé un programme, de se propager en se recopiant sur un programme et de se déclencher comme une bombe logique quand un événement se produit.

Ses actions ont généralement comme conséquence la perte d'intégrité des informations d'un SI et/ou une dégradation ou une interruption du service fourni.

- **5.2.14 - Ver**

Un ver est un programme malicieux qui a la faculté de se déplacer à travers un réseau qu'il cherche à perturber en le rendant indisponible. Cette technique de propagation peut aussi être utilisée pour acquérir des informations par sondage.

Parmi les vers célèbres nous pouvons citer :

- - Christmas Tree sur Bitnet en 1987 [13] ;
- - Father Christmas sur DECnet en 1988 [4] ;
- - le ver Internet en 1988 [2], [13] ;
- - WANK sur Easynet en 1989.

- **5.2.15 - Asynchronisme**

Ce type d'attaque évoluée exploite le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation. Les requêtes concernant de nombreux périphériques sont mises en file dans l'ordre des priorités puis traitées séquentiellement. Des tâches sont ainsi endormies puis réveillées lorsque les requêtes sont satisfaites. A chaque fois qu'une tâche ou qu'un processus est ainsi endormi, son contexte d'exécution est sauvegardé pour être restitué en l'état lors du réveil. En outre de nombreux processus s'exercent sur les périodes très longues. Pour éviter de perdre le bénéfice des calculs effectués depuis le début de l'application en cas de panne, il est nécessaire de définir des points de reprise sur incident. Les sauvegardes de contexte contiennent donc des informations propres à l'état du système et un attaquant averti peut les modifier afin de contourner les mesures de sécurité.

- **5.2.16 - Souterrain**

La technique du souterrain est un type d'attaque qui évite de s'attaquer directement à une protection mais qui tente de s'en prendre à un élément qui la supporte. Une telle attaque exploite une vulnérabilité d'un système qui existe à un niveau d'abstraction plus bas que celui utilisé par le développeur pour concevoir et/ou tester sa protection. Nous retrouvons ce type d'attaque dans le cas où un détenu veut s'évader de prison : il préférera creuser un souterrain dans la terre plutôt que tenter de percer un mur d'enceinte en béton.

- **5.2.17 - Cryptanalyse**

L'attaque d'un chiffre ne peut se faire que lorsqu'on a accès aux cryptogrammes qui peuvent être interceptés lors d'une communication ou qui peuvent être pris sur un support quelconque. Cette attaque nécessite en général d'excellentes connaissances en mathématiques et une forte puissance de calcul. Elle est principalement le fait de services de renseignement.

6 - Conclusion

Notre société est confrontée à des mutations sociales et technologiques constantes. Le domaine du traitement de l'information est particulièrement sujet à des bouleversements. Les États et les entreprises confient leurs informations à des systèmes de plus en plus performants et complexes. Leurs qualités dues principalement à la miniaturisation et à l'abaissement des coûts des équipements s'améliorent au détriment de la sécurité en partie à cause d'une grande ouverture pour faciliter les échanges, d'une grande hétérogénéité des matériels et des procédures et de la complexité croissante des produits.

Pour un SI donné, la menace n'est pas unique mais le plus souvent composite du fait de la diversité des systèmes et des informations gérées. Il en va de même pour les attaques. Un

agresseur utilisera généralement plusieurs techniques, ou des combinaisons, pour arriver à ses fins en exploitant les vulnérabilités d'un SI.

De son côté, le défenseur doit être capable de déterminer ce qu'il veut protéger et contre qui. Connaissant ses propres vulnérabilités, une analyse de risque lui permettra d'identifier les scénarii d'attaques réalistes et par conséquent de mettre en place les parades nécessaires à la protection de ses informations.

7 - Références

[1] Concerning Hackers who Break into Computer Systems, Dorothy Denning, proceedings of the 13th National Computer Security Conference, 1990.

[2] M.W. Eichen and J.A. Rollis, With Microscopes and Tweezers : An Analysis of The Internet Virus of November 1988, 1989 IEEE Computer Society Symposium on Security and Privacy.

[3] [Fiche d'Expression Rationnelle des Objectifs de Sécurité](#), 150/SGDN/DISSI/SDSSI.

[4] The Father Christmas Worm James L. Green and Patricia L. Sisson, proceedings of the 12th National Computer Security Conference, 1989.

[5] [Information Technology Security Evaluation Criteria](#), Version 1.2, June 91, Commission of the European Communities.

[6] [Information Technology Security Evaluation Manual](#), Version 1.0, October 1993, Commission of the European Communities.

[7] ISO-7498-2-89.

[8] Information System Security : A Comprehensive Model, captain John R. McClumber, proceedings of the 14th National Computer Security Conference, 1989.

[9] A Summary of Computer Misuse Techniques, Peter G. Neumann and Donn B. Parker, proceedings of the 12th National Computer Security Conference, 1989.

[10] Espionnage and Computer, Lonnie Moore, présentation à l'US DoE 11th Computer Security Group Conference, may 1988.

[11] Computer Crime and Espionnage : Similarities and Lessons Learned, Lloyd F. Reese, proceedings of the 12th National Computer Security Conference , 1989.

[12] Computers at Risk, System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, US National Research Council, National Academy Press, 1991.

[13] An Epidemiology of Viruses & Network Worms, Clifford Stoll, proceedings of the 12th National Computer Security Conference, 1989.

[14] A Taxonomy of Vulnerabilities, John F. Clayton, 4th annual Canadian Computer Security

Symposium, Ottawa, may 1992.

[15] A Covert Channel taxonomy for Trusted Database Management Systems, Ronald B. Knode, 4th annual Canadian Computer Security Symposium, Ottawa, may 1992.