Comment mesurer la sécurité informatique ?

Yves Deswarte

Directeur de recherche au CNRS

LAAS, Laboratoire d'Analyse et d'Architecture des Systèmes, CNRS

1 Introduction

La sécurité informatique, ou plutôt la sécurité des systèmes d'information, est généralement définie comme la combinaison de trois propriétés [ITSEC 91] :

- la confidentialité, qui empêche la divulgation d'information à des personnes non autorisées à la connaître,
- l'intégrité, qui empêche l'altération d'information, et
- la disponibilité, qui assure que les personnes autorisées peuvent accéder à l'information lorsqu'elles en ont besoin.

Notons que ces définitions qui se rapportent à l'*information* pourraient tout aussi bien se rapporter au *service* fourni aux utilisateurs, comme dans les définitions liées à la sûreté de fonctionnement [Laprie 96]. Ainsi la disponibilité peut se définir de façon équivalente comme la capacité du système informatique à être prêt à délivrer le service.

Les travaux en sûreté de fonctionnement ont conduit à développer des techniques pour estimer ou *mesurer* la disponibilité, soit de façon statistique (par exemple, on dira qu'un système est disponible 99% du temps), soit de façon probabiliste (probabilité qu'à un instant donné le système soit prêt à délivrer le service). De telles mesures quantitatives ne sont pas aussi faciles à définir pour la confidentialité et l'intégrité.

La première difficulté vient de la nature des phénomènes à considérer : la sûreté de fonctionnement s'intéresse principalement (mais pas exclusivement) à des causes accidentelles (qu'on appelle *fautes accidentelles*), alors que la sécurité des systèmes d'information se préoccupe principalement (mais pas exclusivement non plus) des malveillances (ou *fautes délibérées, créées dans l'intention de nuire*). Dans le cas de fautes accidentelles, il est assez naturel de considérer que les événements sont indépendants et plus ou moins uniformément distribués dans le temps, ce qui se représente facilement par des processus stochastiques. Dans le cas des malveillances, il est plus difficile de considérer les attaques comme des phénomènes aléatoires, puisqu'elles résultent directement de la volonté

de quelqu'un qui pourra choisir un moment propice, lancer plusieurs attaques en même temps ou même coordonner ses actions avec celles de complices.

Une seconde difficulté tient à la détection des atteintes à la confidentialité, qui peuvent ne pas laisser de trace (les données divulguées ne changeant pas de valeur). Il en est souvent de même pour les attaques réussies contre l'intégrité, où généralement l'attaquant fait en sorte que la fausse information qu'il introduit apparaisse authentique. Il est donc difficile d'identifier des états de défaillance vis-à-vis de la confidentialité et de l'intégrité, et il est encore plus difficile d'identifier les instants de défaillance correspondants.

Ces difficultés font qu'il n'est pas possible d'appliquer directement à la sécurité des systèmes d'information les méthodes d'évaluation de la sûreté de fonctionnement. Trois approches ont été proposées pour évaluer la sécurité des systèmes d'information : l'analyse de risques, les critères d'évaluation et l'évaluation quantitative de la sécurité opérationnelle. Ces trois approches seront développées dans les prochaines sections.

2 Analyse de risques

On peut appliquer aux systèmes d'information des analyses de risques analogues à celles utilisées dans le domaine des risques vis-à-vis de catastrophes naturelles ou industrielles.

Il existe plusieurs méthodes globales d'évaluation de la sécurité d'une installation informatique basées sur l'analyse de risques (*Risk Assessment*), et prenant en compte aussi bien des risques liés à des accidents ou des phénomènes naturels (incendie, inondation, bogue de logiciel ou erreur de saisie, etc.) que ceux liés à la malveillance (terrorisme, fraude, extorsion de fonds, etc.). En France, les méthodes les plus utilisées ont été MARION [Lamère 1985], développée et soutenue par le CLUSIF (Club de la sécurité informatique français) et l'APSAD (Assemblée Plénière des Sociétés d'Assurances Dommages), et MELISA développée pour le compte de la Délégation Générale pour l'Armement et commercialisée par la société CF6, jusqu'à son absorption par la société Telindus. Plus récemment, le CLUSIF a développé la méthode MEHARI (MÉthode Harmonisée d'Analyse de RIsques). On peut également citer la méthode CRAMM, couramment utilisée en Grande-Bretagne, et le projet européen CORAS[1].

Pour ces méthodes, les entraves à la sécurité des systèmes informatiques sont généralement classées en menaces, vulnérabilités et risques :

---

1 <http://www.nr.no/coras/>

- Les *menaces* sont caractérisées par les possibilités et les probabilités d'attaque (au sens large) contre la sécurité. Elles sont définies par la source (interne au système ou externe), par la motivation des attaquants, par le processus d'attaque, par la cible et par le résultat (conséquences de la réussite d'une attaque).
- Les *vulnérabilités* sont les fautes de conception ou de configuration, intentionnelles ou accidentelles, qui favorisent la réalisation d'une menace ou la réussite d'une attaque.
- Les *risques* sont le résultat de la combinaison des menaces et des vulnérabilités. Les risques doivent être évalués, soit pour obtenir le meilleur compromis possible entre sécurité et coût pour un système donné, soit simplement pour calculer le montant des primes d'assurance pour couvrir ces risques.

L'identification des menaces conduit à les classer en menaces physiques (incendie, dégâts des eaux, défaillances d'équipements, etc.), ou logicielles (bogues, spécificités de certaines versions qui pourront conduire à des incapacités d'évolutions, etc.), maladresses de certains utilisateurs, opérateurs ou personnels de maintenance (erreurs de saisie, mauvaises configurations, etc.), et malveillances (terrorisme, chantage, extorsion de fonds, fraude, piratage de données ou de logiciels, etc.). Les malveillances peuvent être d'origine externe (par des individus non autorisés à utiliser le système d'information) ou interne (par des utilisateurs autorisés, voire des concepteurs ou des administrateurs du système d'information).

Les conséquences des incidents peuvent être des dégâts en terme de matériel ou de données, ou des coûts liés à l'arrêt ou la dégradation de l'exploitation, ou encore des atteintes à l'image de marque de l'entreprise.

Les vulnérabilités sont des fautes de conception au sens large, c'est-à-dire qu'elles peuvent être introduites durant le développement du système, son installation, son exploitation ou sa maintenance. Ce sont des fautes dormantes dans le sens qu'elles ne produisent pas d'erreurs par elles-mêmes, mais elles peuvent être exploitées par des fautes externes accidentelles ou des attaques. On peut généralement identifier des vulnérabilités dans la gestion des incidents (plans de secours, organisation des sauvegardes, etc.), dans la sécurité physique (contrôle des accès aux locaux, matériel de lutte contre l'incendie, etc.), ou dans la sécurité logique (définition de la politique de sécurité, mécanismes d'identification et d'authentification, gestion des droits d'accès, journalisation des événements de sécurité, protection des communications, etc.).

Pour obtenir des mesures quantitatives, il convient alors d'estimer la fréquence de réalisation des menaces (par exemple, une inondation est dite centenaire si elle survient en

moyenne tous les cent ans) susceptibles d'exploiter les vulnérabilités identifiées (par exemple, le fait qu'une digue soit étudiée pour résister à des inondations dont la fréquence est supérieure à une par siècle), ainsi que les coûts des conséquences des incidents correspondants. Des méthodes de calcul, basées sur les principes des espérances mathématiques permettent d'évaluer le montant des primes d'assurances contre ces risques, ou de justifier ou non le coût des parades (réduction des vulnérabilités ou protections pour réduire les conséquences des attaques).

Néanmoins ces mesures quantitatives restent sujettes à caution, car il est généralement impossible d'estimer les paramètres avec précision (absence de statistiques plausibles) et de garantir la complétude des menaces et des vulnérabilités. La qualité de l'analyse de risques repose donc en grande partie sur la compétence de ceux qui la mènent. C'est souvent aussi une démarche lourde et coûteuse. Enfin, elle ne représente qu'un cliché à un moment donné, et elle devrait être refaite en fonction de l'évolution du système et de son environnement.

En résumé, l'analyse de risques est une démarche utile, mais plus pour ses effets collatéraux (sensibilisation et motivation des personnels et de la hiérarchie aux problèmes de sécurité) que comme instrument de mesure de la sécurité.

3 Critères d'évaluation

Des *critères d'évaluation* qualitative ont été développés pour comparer la capacité de divers systèmes informatiques à faire face à des malveillances.

Les premiers critères ont été définis par la défense américaine (DoD) dans ce qui est couramment appelé le *Livre Orange* ou TCSEC ("*Trusted Computer System Evaluation Criteria*") [TCSEC 1985], ainsi que dans les livres de diverses couleurs qui l'accompagnent, comme le *Livre Rouge* ou TNI ("*Trusted Network Interpretation of the TCSEC*") [TNI 1987]. Ces critères, basés à la fois sur des listes de fonctions de sécurité à remplir et sur les techniques employées pour la validation, conduisent à classer les systèmes en 7 catégories (dans un ordre croissant de sécurité : D, C1, C2, B1, B2, B3, A1). Les critères portent à la fois sur la doctrine de sécurité (par exemple, un contrôle d'accès discrétionnaire ou obligatoire), sur la responsabilité (par exemple, la journalisation des opérations liées à la sécurité), l'assurance (c'est-à-dire les méthodes de validation employées) et sur la documentation.

Ces critères visaient à satisfaire d'abord les besoins du DoD, c'est-à-dire qu'ils privilégient la confidentialité plutôt que l'intégrité qui est le souci principal des systèmes dits "commerciaux". Ainsi, pour les système de niveau B1 ou supérieur, un modèle de sécurité multi-niveau est imposé, le modèle de Bell-LaPadula. Dans ce modèle, une classification est

attachée à chaque information, et une habilitation est assignée à chaque utilisateur. Chaque classification et chaque habilitation est identifiée par un niveau (par exemple, non-classifié, à diffusion restreinte, confidentiel, secret, très secret) et un compartiment qui est un ensemble de catégories (par exemple, nucléaire, cryptologie, télécommunications, etc.). Les différentes classifications et habilitations sont donc ordonnées partiellement dans un treillis, c'est-à-dire qu'une classification ou habilitation A domine une autre classification ou habilitation B si et seulement si à la fois le niveau de A est supérieur ou égal à celui de B et si le compartiment de B est inclus dans celui de A. Pour éviter toute fuite d'information, dans ce modèle, deux règles sont imposées :

- *Règle simple* : un sujet (utilisateur, processus, …) ne peut lire un objet (information) que si son habilitation domine la classification de l'objet.
- *Règle étoile* : un sujet ne peut à la fois lire un objet O_1 et écrire un objet O_2 que si la classification d'O_2 domine celle d'O_1.

Par la suite, des critères *harmonisés* européens ont été proposés [ITSEC 1991], visant à surmonter les limites apparues dans l'utilisation du Livre Orange : évaluation de systèmes plutôt que de produits, prise en compte aussi bien de l'intégrité et de la disponibilité que de la confidentialité, séparation entre les aspects fonctionnels et les aspects de validation. "À titre d'exemple", 10 classes de fonctionnalités sont prédéfinies, dont les 5 premières reprennent les fonctionnalités des catégories C1 à B3 du Livre Orange (les fonctionnalités A1 sont identiques à celles de B3, et pour la catégorie D, rien n'est exigé puisqu'elle correspond aux systèmes n'ayant pas obtenu le niveau d'évaluation visé). 5 autres classes de fonctionnalités sont définies pour les systèmes à haute intégrité, à haute disponibilité, à haute intégrité pour les transmissions, à haute confidentialité pour les transmissions et enfin pour les réseaux à hautes intégrité et confidentialité. Mais d'autres combinaisons de fonctionnalités peuvent être définies si le besoin s'en fait sentir pour un système ou une application particuliers. D'autre part, sont définis également 6 niveaux d'assurance *de conformité*, c'est-à-dire de validation, notés de E1 à E6. Des critères d'*assurance d'efficacité* sont également définis pour évaluer la pertinence et la cohésion des fonctionnalités, la résistance des mécanismes, la vulnérabilité de la construction ainsi que des critères liés à l'exploitation : facilité d'emploi et vulnérabilité en exploitation. Un manuel d'évaluation des ITSEC est paru sous une forme provisoire [ITSEM 1992].

Plus récemment, une collaboration internationale (menée par le NIST et la NSA aux Etats-Unis, le Canada, la France, la Grande-Bretagne et l'Allemagne) a permis de définir des *critères communs*, qui forment la norme ISO/IEC 15408. Fortement inspirés des ITSEC dont

ils reprennent la séparation entre classes de fonctionnalités et niveaux d'assurance, ils se caractérisent par la définition de *profils de protection* spécifiques pour des types de produits ou d'applications (par exemple, les pare-feux, les cartes à puces, etc.). Un profil de protection est défini par des fonctionnalités, un niveau d'assurance de conformité et des critères d'assurance d'efficacité adaptés au type de produit ou d'application. Cette notion de profil de protection doit permettre de comparer plus facilement différents produits évalués, mais aussi de réduire les coûts d'une évaluation.

Globalement, les critères dévaluation sont un excellent guide pour le développement de systèmes à haute sécurité, et ils peuvent justifier des arguments « marketing » par la comparaison qu'ils offrent entre différents produits. Cependant, une telle évaluation est coûteuse, surtout pour des niveaux d'assurance visés élevés, et elle n'est valable que pour une version spécifique du produit ou du système. Toute évolution doit conduire à une nouvelle évaluation. Par ailleurs, comme pour l'analyse de risques, une évaluation par les critères communs ne donnent qu'une vision statique de la sécurité : on évalue comment le système a été conçu plutôt que comment il est utilisé au jour le jour. Enfin, une telle évaluation étant essentiellement qualitative, les critères d'évaluation ne peuvent pas être considérés comme un instrument de mesure précis de la sécurité.

4 Évaluation quantitative de la sécurité opérationnelle

Les sections précédentes ont montré que les méthodes classiques d'évaluation de la sécurité par analyse de risques ou par critères d'évaluation se prêtent mal à des exigences pratiques que l'on retrouve dans bon nombre de systèmes actuels : modification fréquente de la politique de sécurité, évolution rapide des configurations et des applications, ouverture sur des systèmes ou des utilisateurs inconnus, etc. Dans de tels systèmes, il convient surtout d'obtenir un bon compromis entre sécurité et facilité d'utilisation, de partage de l'information et de coopération entre les utilisateurs. Ceci nous a conduit à proposer une nouvelle approche pour une évaluation quantitative de la sécurité.

Jusqu'à récemment, l'évaluation quantitative de la sécurité était limitée à quelques aspects particuliers, comme l'évaluation de la bande passante des canaux cachés (exigée à partir du niveau B2 du Livre Orange) ou l'application de la théorie de l'information à l'évaluation de l'efficacité des mécanismes cryptographiques ou de la fragmentation des traitements par tranches de bits [Trouessin 1991].

Pourtant une évaluation quantitative présente de nombreux avantages :

- Elle permet de surveiller les évolutions de la sécurité en fonction des modifications de configuration et d'usage.
- Elle permet d'identifier quelles modifications pourraient avoir le meilleur impact sur la sécurité.
- Elle permet de négocier avec les utilisateurs un meilleur compromis sécurité/facilité d'utilisation.

La mesure quantitative de la sécurité que nous proposons représente la robustesse du système, c'est-à-dire sa capacité à résister à de possibles attaques. La robustesse est une caractéristique du système à un moment donné, elle est indépendante de la probabilité que le système soit attaqué. Ceci nécessiterait, en effet, une modélisation de la population d'attaquants et de leur stratégie de choix d'une cible, ce qui nous semble – à l'heure actuelle – irréalisable. Au contraire, notre étude ne s'intéresse qu'au système informatique et à ses protections, mises en œuvre effectivement par les utilisateurs, toutes choses pour lesquelles on peut disposer de données tangibles. Cette approche est analogue à l'analyse de couverture dans les systèmes tolérant les fautes, où plutôt que d'estimer les taux de défaillance des composants, on évalue leurs possibles effets sur le fonctionnement global du système.

4.1 Graphe des privilèges

Notre démarche repose sur une modélisation du système informatique sous forme d'un *graphe des privilèges*, modèle abstrait que nous avons conçu en 1994 [Dacier 1994]. Dans ce graphe, les nœuds représentent des ensembles de droits (ou privilèges), et les arcs des transferts de privilèges : il existe un arc (étiqueté *M*) allant de *X* à *Y* s'il est possible, ayant les privilèges représentés par le nœud *X* d'acquérir les privilèges du nœud *Y*, en utilisant la méthode *M*. Cette méthode peut être un transfert licite de privilège (l'utilisateur *Y* fait confiance à *X*), ou un transfert implicite (*Y* est un sous-ensemble de *X*), ou encore une attaque élémentaire. Un poids peut être affecté aux différentes méthodes, selon la difficulté pour un possible attaquant d'exploiter la méthode ou selon le temps nécessaire pour réaliser l'attaque. Ce graphe peut être analysé pour identifier les possibilités de mettre en défaut la politique de sécurité du système. En effet, à partir de la politique de sécurité, il est possible d'identifier des attaquants potentiels (intrus externes, ou utilisateurs pouvant tenter d'étendre leurs privilèges ou d'abuser de leurs privilèges), et des cibles potentielles (ensembles de droits d'accès à des informations sensibles). La politique de sécurité peut être mise en défaut s'il existe (au moins) un chemin depuis l'ensemble des privilèges d'un attaquant potentiel jusqu'à une cible.

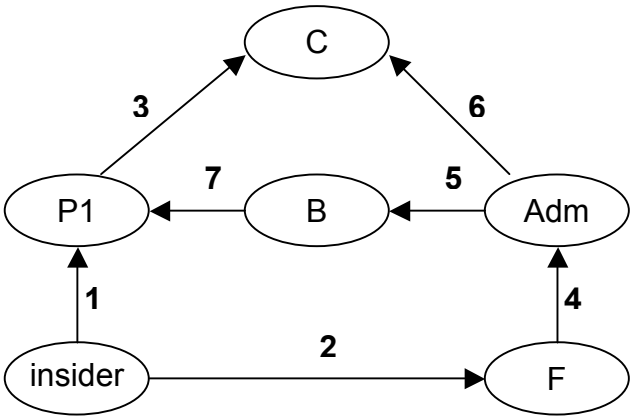

Figure 1 : exemple de graphe de privilèges

La figure 1 donne un exemple de graphe de privilèges. Dans cet exemple, le nœud « insider » représente les privilèges minimaux de n'importe quel utilisateur autorisé du système. Les nœuds « B », « C » et « F » représentent les privilèges de trois utilisateurs particuliers, alors que « Adm » représente les privilèges du groupe des administrateurs du système (dont F est membre) et « P1 » est un utilisateur virtuel correspondant à un projet. Dans cet exemple, les méthodes 1, 2 et 3 correspondent à des négligences des utilisateurs P1, F et C ; alors que les méthodes 4 à 7 correspondent à des transferts de privilèges volontaires (justifiés par la confiance des utilisateurs entre eux).

Le graphe des privilèges peut être généré automatiquement, par exemple en analysant la configuration d'un système Unix (ou d'un ensemble de machines Unix interconnectées) pour en déterminer les vulnérabilités (en fonction d'une liste de méthodes d'attaque connues). De même, à partir d'une description formelle de la politique de sécurité, il est possible d'identifier les nœuds correspondants à des attaquants potentiels (dans l'exemple, le nœud « insider »), et ceux correspondant à des cibles potentielles (dans l'exemple, le nœud « C »). Les arcs peuvent être affectés d'un poids représentant la difficulté pour un attaquant potentiel possédant les privilèges du nœud origine de l'arc d'obtenir les privilèges du nœud destination en utilisant la méthode *M*.

4.2 Calcul des mesures

À partir du graphe pondéré, on peut évaluer la difficulté pour chaque attaquant potentiel d'atteindre chaque cible potentielle. Pour ce faire, le graphe des privilèges est transformé en une chaîne de Markov correspondant aux processus d'attaque possibles. Les poids donnés aux arcs en fonction des méthodes d'attaque et du type de cible deviennent des

taux de succès correspondant à l'effort et au temps que l'attaquant doit dépenser pour réussir cette attaque : le taux sera d'autant plus petit que l'effort nécessaire à la réussite sera grand [Dacier 1996].

Il est alors possible de calculer des mesures significatives (effort moyen et temps moyen pour qu'un attaquant atteigne une cible) pour tous les couples (attaquant, cible) et ainsi d'estimer sous forme quantitative la sécurité du système. Nous avons développé ÉSOPE (outil d'Évaluation de la Sécurité OPÉrationnelle), prototype de suite logicielle, qui rassemble et enchaîne un ensemble d'outils permettant d'automatiser toutes ces phases : définition interactive de la politique de sécurité, création du graphe de privilèges par analyse du système de fichiers Unix, génération des chaînes de Markov et calcul des mesures. Ce prototype a été utilisé pour évaluer la sécurité du réseau du LAAS pendant plusieurs années, principalement dans le but de valider la pertinence des différentes mesures qu'il est possible d'obtenir [Ortalo 1999a].

Avec ÉSOPE, il est ainsi possible de calculer automatiquement, par exemple une fois par jour, des mesures pertinentes de la sécurité d'un système informatique et ainsi de suivre au jour le jour l'évolution de ces mesures, en fonction des modifications de configuration ou de la façon dont les utilisateurs mettent en œuvre les mécanismes de protection. En cas d'évolution défavorable des mesures, il est possible d'identifier automatiquement les modifications qui ont provoqué l'évolution, ce qui donne des arguments aux administrateurs systèmes pour discuter avec les utilisateurs et tenter de les convaincre de corriger leur façon de travailler.

5 Conclusion

La méthode d'évaluation quantitative de la sécurité opérationnelle a aussi été appliquée avec succès à des systèmes d'information prenant en compte non seulement le système informatique mais aussi l'organisation de ses utilisateurs, leurs relations hiérarchiques et leur confiance mutuelle. Ceci a conduit à développer une méthode de description des politiques de sécurité adaptées aux besoins des entreprises, en liaison avec une évaluation quantitative de la sécurité des systèmes d'information correspondants. Cette méthode a été validée par une expérimentation sur une agence bancaire, organisation réelle de taille significative [Ortalo 1999b]. Néanmoins ce type d'application n'est pas aussi facilement automatisable que pour un système informatique.

6 Références

[Dacier 1994]

Marc Dacier et Yves Deswarte, "Privilege graph: an extension to the Typed Access Matrix model", *European Symposium on Research in Computer Security (ESORICS 94)*, Brighton (UK), novembre 1994, Lecture Notes in Computer Science 875: Computer Security, ISBN 3-540-58618-0, 1994, Springer-Verlag, pp. 319-334.

[Dacier 1996]

Marc Dacier, Yves Deswarte, Mohamed Kaâniche, "Models and tools for quantitative assessment of operational security", *12th International Information Security Conference (IFIP/Sec'96)*, Samos (Grèce), 21-24 mai 1996, dans «Information Systems Security», Chapman & Hall, Ed. S.K. Katsikas and D. Gritzalis, 1996, pp.177-186.

[ITSEC 1991]

Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC), Office des publications officielles des communautés européennes, L-2985 Luxembourg, ISBN 92-826-3005-6

[Lamère 1985]

J.M. Lamère, *La sécurité informatique : approche méthodologique*, Dunod Informatique, ISBN 2-04-016503-7 (1985).

[Laprie 1996]

J.-C. Laprie *et al.*, *Guide de la sûreté de fonctionnement*, Cépaduès Éditions, 1996, 370p., ISBN 2.85428.382.1, seconde édition.

[Ortalo 1999a]

Rodolphe Ortalo, Yves Deswarte et Mohamed Kaâniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security", *IEEE Transactions on Software Engineering*, Vol.25, N°5, pp.633-650, septembre/octobre 1999.

[Ortalo 1999b]

Rodolphe Ortalo et Yves Deswarte, "Quantitative Evaluation of Information System Security Experimented in a Bank Organization", *2nd International Conference on Information System Security in the Financial Sector*, Bratislava (Slovaquie), 24-25 mars 1999, pp.38-47.

[TCSEC 85]

TCSEC, *Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Department of Defense, USA, December 1985.

[TNI 87]

TNI, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-005, National Computer Security Center, 31 July 1987.

[Trouessin 1991]

Gilles Trouessin, "Quantitative evaluation of confidentiality by entropy calculation", *IEEE Computer Security Foundation Workshop IV*, Franconia (USA), 18-20 juin 1991, pp.12-21.