Chapitre 6 : Mesurer la sécurité

SÉcurité et Cryptographie
2013-2014

Sup Galilée INFO3

Le livre orange

Le livre orange surnom du TCSEC (Trusted Computer System Evaluation Criteria) est paru en 1983 aux États-Unis.

LeTCSEC décrit comment un système donné peut être affecté à un niveau et une classe de sécurté par la vérification d'un ensemble de critères d'évaluation.

Le niveau de sécurité est noté par une lettre A, B, C ou D, D étant le niveau de moindre sécurité.

La classe est donnée par un nombre 1, 2, 3. Le niveau de sécurité est d'autant plus élevé que le nombre est grand.

Les critères relèvent de quatre catégories : politique de sécurité, imputabilité (notion juridique), assurance et documentation.

Objectifs du TCSEC

- Fournir un instrument d'évaluation de la confiance que l'on peut accorder à un système donné.

- Fournir un guide de qu'il faut réaliser pour répondre aux exigences de confiance des utilisateurs.

- Servir de référence claire.

Niveau D : Sécurité minimale

Cette catégorie regroupe tous les systèmes qui ont échoué à être classé ailleurs.

Niveau C : Contrôle d'accès discrétionnaire

En classe C1, la sécurité est relativement primaire. Cette classe ne suppose pas fondamentalement de différences d'habilitation parmi les usagers. Les caractéristiques de systèmes de cette classe tendent en fait à empêcher les utilisateurs de commettre des erreurs qui pourraient nuire au système ou aux autres utilisateurs.

Les deux caractéristiques principales de la classe C1 sont :
- Les mots de passe pour identifier et authentifier un usager du système.
- Une protection discrétionnaire des fichiers (le propriétaire des fichiers peut choisir les droits d'accès des autres utilisateurs à ceux-ci).

La plupart des sytèmes de la famille UNIX sont C1.

Classe C2

En plus un système classé C2 doit fournir :

- Une surveillance des utilisateurs (fichiers de logs).

- Contrôle d'accès au niveau utilisateur (et non groupe).

- L'assurance qu'aucune donnée laissée en mémoire dans le système ne peut devenir accidentellement accessible à un autre utilisateur.

Niveau B : Contrôle d'accès obligatoire

Les systèmes de la classe B1 doivent proposer au moins l'étiquetage des fichiers et des utilisateurs (tout fichier et tout utilisateur possède une habilitation : pour un fichier il s'agit du niveau d'habilitation minimal requis pour un usager afin d'y accéder).

Ils doivent avoir une architecture séparant rigoureusement la gestion de la sécurité des autres fonctionnalités.

La documentation du système doit décrire un modèle de politique de sécurité (non nécessairement prouvé mathématiquement).

Classe B2

Les systèmes de classe B2 renforcent les caractéristiques existantes.

Le livre orange spécifie que les systèmes de classe B2 doivent être relativement résistant à la pénértration.

L'étiquetage est étendu à toutes les entités gérées par le systèmes, y compris les périphériques.

Un chemin de confiance est un moyen d'assurer l'usager qu'il a bien affaire au système (c'est la contrepartie de l'identification de l'utilisateur).

La politique de sécurité doit reposer sur un modèle formel mathématique.

Classe B3

- Un administrateur sécurité doit être désigné.

- Il doit être prouvé que la sécurité du système n'est pas remise en cause en cas de défaillance de celui-ci.

Classe A

Seule la classe A1 est définie.
La seule caractéristique différenciant un système de classe A1 d'un système de la classe B3 est que la preuve mathématique que le système est conforme à ses spécifications en matière de sécurité doit être apportée.

Défauts du TCSEC

- Il se focalise sur la confidentialité au détriment de l'intégrité et de la disponibilité.

- Il met l'accent sur le contrôle des accès externes, alors qu'il existe de nombreuses attaques internes.

- Il ne prend pas en compte la sécurité des interconnexions de systèmes.

Le livre rouge

Le livre rouge ou TNI (Trusted Network Interpretation) est un extention du livre orange.

Son objectif est de tenter de combler les lacunes du livre orange.

Il distingue deux types de réseaux sécurisés :
- Le réseau formé d'un ensemble de systèmes, chacun de ceux-ci ayant un niveau de sécurité déterminé par le TCSEC.
- Le réseau considéré comme un système, avec sa politique de sécurité, son architecture et sa conception propre.

Contenu du livre rouge

Il est constitué de deux parties :

1. La première reprend chacune des exigences du TCSEC et en donne l'interprétation pour un réseau.

2. La seconde décrit des services de sécurité additionnels qui peuvent être fournis : intégrité des communications (les services de cette catégorie assure que les communications ne sont ni fabriquées, ni manipulées, ni répudiées par l'émetteur ou le récepteur), la continuité de service (ces services garantissent la disponibilité du réseau; ce qui signifie qu'il existe des méthodes pour se protéger des menaces comme l'engorgement), non compromission (ces services assurent la confidentialité des transmissions).

L'Union européenne a également produit un document standardisant la sécurité des systèmes d'information : les ITSEC (Information Technology Security Evaluation Criteria).