

Critères de sécurité

Pour permettre une exécution sûre, le système doit contrôler 5 points :

1. La transmission du code doit être faite de manière sûre.

2. Les interactions entre l'environnement d'exécution et le système doivent être contrôlées.

3. L'exécution du code doit être sécurisée.

4. L'accès aux ressources lors de l'exécution doit être contrôlé.

5. Les codes s'exécutant en mémoire doivent être protégés les uns des autres. Les attaques auxquelles doit faire face le système sont principalement les suivantes :

- Les refus de services : le code bloque l'accès à un service de la machine, soit en le désactivant, soit en inondant de requêtes.

- La découverte d'informations confidentielles : le code outrepassa ses droits pour aller récupérer des informations auxquelles il ne devrait pas avoir accès.

- La destruction ou la modification de données : le code outrepassa ses droits pour aller modifier des informations.

- Attaques diverses : le but est de gêner les utilisateurs du système. Divers scénarios peuvent être imaginés : un « plug-in » d'affichage de vidéo à la demande qui parcourt discrètement le système de fichiers local à la recherche d'informations sensibles, un jeu en ligne qui met en place un cheval de Troie ou un programme invisible qui vient enregistrer l'activité du système.