Généralités à la Technologie Blockchain

Eugène C. Ezin & Nelson Saho

31 octobre 2024

Contenu

1. Bases de la technologie Blockchain
   - Les niveaux de sécurité et types de menaces
   - Les modèles de sécurité
   - Les objectifs de la sécurité informatique et les mesures de sécurité

Contenu

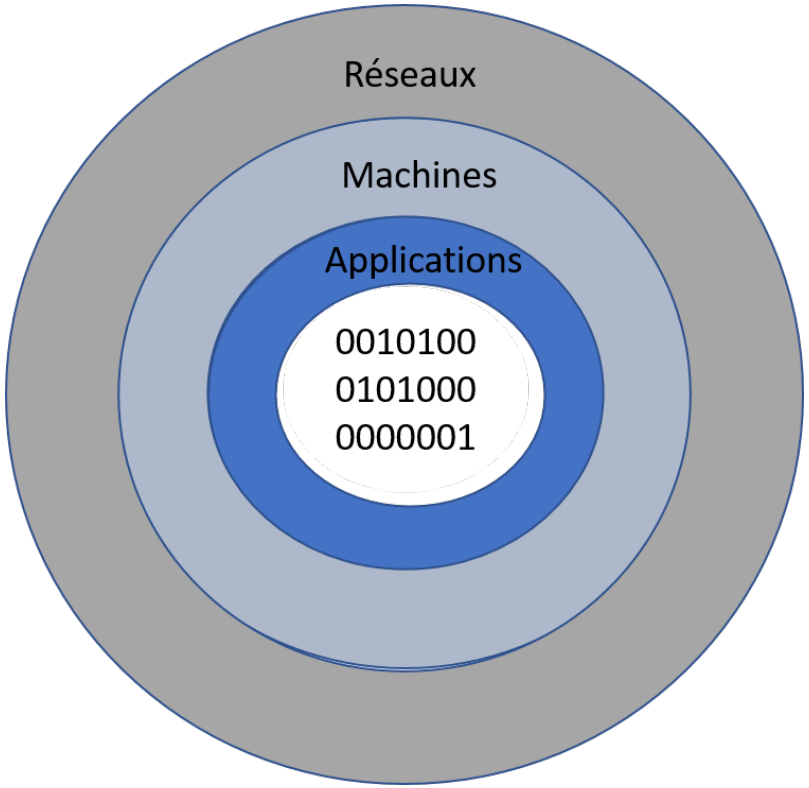
Les niveaux de sécurité

D'une manière générale, la sécurité est présente à plusieurs niveaux à savoir :

- au niveau physique (les locaux) ;
- au niveau des réseaux ;
- au niveau des machines ;
- au niveau des applications ; et
- au niveau des données ;

Les niveaux de sécurité (suite)

Cette figure illustre les différents niveaux de la sécurité d'un Système d'information.



Les types de menaces

Les menaces peuvent être vues comme des violations potentielles de la sécurité qui existent en raison des vulnérabilités du système. Les menaces envers un système informatique comprennent les éléments suivants :

- Destruction d'information et /ou d'autres ressources ;
- Corruption ou modification d'informations ;
- Vol, suppression ou perte d'informations et /ou d'autres ressources ;
- Divulgation d'informations ; et
- Interruption de service.

Les types de menaces (suite)

Avec la populatirité des réseaux, des échanges de données, et les transmissions entre individus, de nombreuses menaces émergent. En catégorisant les différentes menaces possibles, On peut citer :

- les menaces accidentelles ;
- les menaces intentionnelles ;
- les menaces passives ; et
- les menaces actives.

Les menaces accidentelles ou menaces intentionnelles peuvent être actives ou passives.

Les types de menaces : menaces accidentelles

Les menaces accidentelles sont celles qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles sont :

- les bugs de logiciels ;
- les pannes matériels ;
- les défaillances incontrôlables.

Les types de menaces : menaces intentionnelles

- Elles reposent sur l'action d'un tiers désirant s'introduire et relever des informations.
- On parle ici d'attaque de système informatique. D'où la notion d'attaquant. Les menaces intentionnelles peuvent aller de l'examen fortuit, utilisant des outils de contrôle facilement disponibles, aux attaques sophistiquées, utilisant une connaissance spéciale du système.
- Les menaces intentionnelles peuvent être passives ou actives. Par exemple
  - les virus comme les chevaux de troie ;
  - les hackers.

Les types de menaces : menaces passives

- Dans le cas d'une menace passive, l'intrus tente de dérober les informations par audit du système d'information sans modifier les fichiers et les éléments de ce système.
- Les menaces passives sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne changent.
- Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système.
- L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.

Les types de menaces : menaces actives

- Les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou du fonctionnement du système.
- Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable.
- Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données.
- Le résultat d'une attaque est soit une divulgation de l'information : violation de la confidentialité de l'objet, soit une modification des objets : violation de l'intégrité de l'objet, soit un déni de service : violation de la disponibilité.

Les types de menaces : menaces actives

On distingue donc quatre catégories de menaces actives :

- **Interruption** - il s'agit d'un problème lié à la disponibilité des données.
- **Interception** - il s'agit d'un problème lié à la confidentialité des données.
- **Modification** - il s'agit d'un problème lié à l'authenticité des données.
- **Fabrication** - provoque des attaques de déni de service (DOS) dans lesquelles l'attaquant s'efforce d'empêcher les utilisateurs d'accéder à certains services, auxquels ils sont autorisés ou, en termes simples, l'attaquant accède au réseau, puis verrouille l'utilisateur autorisé.

Contenu

Les modèles de sécurité

Il existe plusieurs modèles de sécurité notamment :

- le triangle CIA
- le protocole AAA
- le pentagone de confiance
- le modèle de Donn Parker
- le cube de McCumber

Les modèles de sécurité : Le triangle CIA

Il s'agit d'un modèle de sécurité introduit en 1987 qui définit les grands axes de la sécurité à savoir :

- la confidentialité (*Confidentiality*) - l'information n'est connue que des entitiés communicantes.
- l'intégrité (*Integrity*) - l'information n'a pas été modifiée entre sa création et son traitement et même pendant son transfert.
- la disponibilité (*Availability*) - l'information est toujours accessible et ne peut être perdue ni bloquée.

Le triangle CIA sert de base à la plupart des autres modèles.

Les modèles de sécurité : protocole AAA

Le contrôle d'accès (encore appelé le protocole AAA) se fait en quatre étapes :

- l'Identification - qui êtes-vous ?
- l'Authentification - prouvez-le !
- l'Autorisation - Avez-vous les droits requis ?
- Accounting/audit : Qu'avez-vous fait ?

On parle de protocole AAA simplement parce que les deux premières étapes sont fusionnées. Dans certains cas, la quatrième étape est scindée.

Les modèles de sécurité : protocole AAA

On parle d'accounting lorsque le fait de comptabiliser des faits sera demandé.

On parle d'audit lorsque des résultats plus globaux devront être étudiés.

L'authentification visant à prouver l'identité peut se faire de plusieurs manières(mot de passe, code PIN, carte magnétique, lecteur de carte, empreintes digitales, réseau rétinien, etc.)

Les modèles de sécurité : pentagone de confiance

Ce modèle a été défini par Piscitello en 2006 et précise la notion d'accès à un système. Ce modèle précise aussi la confiance que peut/doit avoir l'utilisateur en présence d'un système informatisé. Les cinq étapes de ce modèle de confiance sont :

- l'authentification (*Authentification*)
- l'autorisation (*Authorization*)
- la disponibilité (*Availability*)
- l'admissibilité (*Admissibility*)
- l'intégrité (*Authenticity - Integrity*)

La confiance se traduit par l'admissibilité. De façon plus précise, la machine sur laquelle nous travaillons, à laquelle nous nous connectons est-elle fiable ? Peut-on faire confiance à la machine cible ?

Les modèles de sécurité : Modèle de Donn Parker

Le modèle de Donn Parker encore appelé Parkerian Hexad est introduit en 1998 comporte la notion d'utilité en plus des notions de

- confidentialité ;
- intégrité ;
- disponibilité ;
- authentification ;
- contrôle ou possession.

Une information chiffrée pour laquelle on a perdu la clé de déchiffrement n'est plus d'aucune utilité bien que l'utilisateur y est accès, que cette information soit confidentielle, disponible et intègre.

Les modèles de sécurité : Modèle de Donn Parker

Figure 2 – Le modèle Parkerian Hexad [1]

1. http://...

Les modèles de sécurité : Le cube de McCumber

Le cube de McCumber est introduit en 1991 et inclut deux autres dimensions en plus des trois piliers de la sécurité (CIA). Les deux autres dimensions sont :

- l'état des données : le stockage, la transmission, l'exécution ;
- les méthodes : les principes et règles à adopter pour atteindre le niveau de sécurité souhaité.

Les modèles de sécurité : Le cube de McCumber

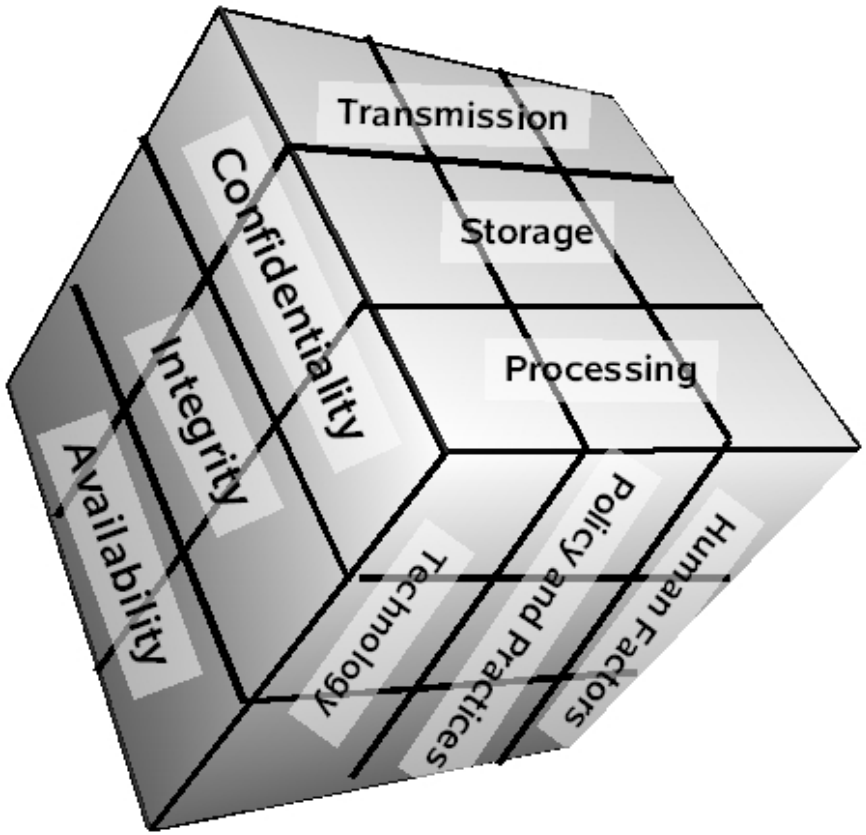


Figure 3 – Le cube de McCumber [2]

Notion de sécurité parallèle

On parle de sécurité en parallèle lorsque plusieurs mécanismes de sécurité protégeant un système possèdent le même rôle. Dans ce cas, le niveau de protection du système est équivalent à celui du mécanisme le moins sûr.
Comme exemple, on peut considérer un ordinateur portable que l'on peut déverrouiller par mot de passe, ou empreinte digitale.

Notion de sécurité en série

On parle de sécurité en série ou de défense en profondeur lorsque plusieurs mécanismes de sécurité protègent un système et ont des rôles différents.
Par exemple, le réseau d'une entreprise comportant un firewall hardware, les différentes machines équipées de firewall logiciel, les ordinateurs comportent des logiciels accessibles par mot de passe, etc.
Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Contenu

Les objectifs de la sécurité informatique

Les principaux objectifs de la sécurité informatique sont :

- la disponibilité ;
- l'intégrité ;
- la confidentialité des infrastructures informatiques (données, services, systèmes).

Les mesures de sécurité

Il existe plusieurs mesures de sécurité pour atteindre les objectifs de la sécurité informatique. Parmi elles, nous pouvons citer :

- le contrôle d'accès
- **le chiffrement des données ou mieux la cryptographie**
- la gestion des incidents ;
- la gestion des erreurs ;
- la gestion des dysfonctionnements ;
- la gestion des intrusions ;
- le cloisonnement d'environnements ;
- etc.

Vocabulaire

- **sûreté :** protection contre les actions non intentionnelles
- **sécurité :** protection contre les actions intentionnelles malveillantes
- **menace :** moyen potentiel par lequel un attaquant peut attaquer un système
- **risque :** prise en compte à la fois la probabilité d'une menace et de sa gravité si elle réussit

Cryptographie et sécurité informatique

La cryptographie est un outil fondamental de la sécurité informatique. En effet :

- la mise en oeuvre de la cryptographie permet de réaliser des services de confidentialité des données transmises ou stockées ;
- la mise en oeuvre de la cryptographie permet les services de contrôle et d'intégrité de données ;
- la mise en oeuvre de la cryptographie permet l'authentification d'une entité lors des transactions ou opérations.

Cryptographie et sécurité informatique

De par l'utilisation d'une clef, il existe deux branches en cryptographie : les cryptographie symétrique et la cryptographie asymétrique. Et c'est justement la sécurité de cette clef qui constitue la plupart du temps la faille des cryptosystèmes symétriques et asymétriques :

- Avec les cryptosystèmes symétriques, la sécurité autour de la clé secrète est un souci.
- Avec les cryptosystèmes asymétriques, la sécurité autour de la clé privée ne se pose pas tellement mais il y a insécurité tout de même.
- etc.

La clé est un souci majeur pour les cryptosystèmes. Une alternative est la technologie Blockchain.

Merci pour votre attention.
Commentaires ? Questions ?