

# **Sécurité de l'information**

## **Chapitre 1. Introduction à la**

# **Sécurité de l'information**

**Mohammed Mehdi Bouchene**

**Département Electronique et Télécommunications**

**Université 8 mai 1945 Guelma**

# Définitions

- L'information peut être considérée comme une signification véhiculée par une séquence de symboles. Les symboles peuvent être alphabétiques, c'est-à-dire des caractères, des nombres, des signes de ponctuation, etc. Ou il peut s'agir par exemple d'une séquence génétique et peut être physique ou logique (un livre ou quelque chose sur un ordinateur)
- L'information peut être mesurée, une discipline appelée théorie de l'information qui s'est développée à partir des travaux de Claude Shannon dans les années 40.

# Définissions

- Des aspects supplémentaires entourent la définition des informations notamment: exactes, opportunes, contextualisées et pertinentes, utiles, spécifiques et pouvant être organisées. Précieuses, car nous pouvons le monétiser. Nous pouvons accroître la compréhension, réduire l'incertitude et cela peut affecter les décisions et les résultats du comportement.
- La sécurité a plusieurs significations. Celui que nous utiliserons ici est le fait d'être à l'abri de tout **danger** ou **menace**. Il peut être appliqué à des scénarios physiques et logiques. Vers un actif vulnérable ou un atout précieux(N).

# Définitions

- D'après Wikipédia, la sécurité des informations est définie comme la pratique consistant à défendre les informations contre tout accès, utilisation, divulgation, perturbation, modification, inspection, enregistrement ou destruction **non autorisés**. Il s'agit d'un terme général qui peut être utilisé indépendamment de la forme que les données peuvent prendre, qu'elles soient physiques ou sur un ordinateur. Nous utilisons souvent la sécurité de l'information dans le contexte des systèmes informatiques. Ces dernières années, le terme de **cybersécurité** a été inventé.

# Définitions

- ACM(Association of computer machinery) dispose d'un groupe de travail conjoint qui définit la cybersécurité. Ils le définissent comme une discipline basée sur l'informatique impliquant la technologie, les personnes, les informations et les processus pour permettre le fonctionnement assuré d'une organisation. Elle implique la création, l'exploitation, l'analyse et le test de systèmes informatiques sécurisés (N).

# CIA TRIAD

- (N) Le modèle classique utilisé pour décrire les concepts clés de la sécurité de l'information est appelé le CIA TRIAD. (N).



# Le modèle CIA

- **Confidentialité:** Un système doit garantir que seuls les utilisateurs autorisés accèdent aux informations. Cela passe par l'application de technologies et de processus. Nous allons commencer à enquêter sur certaines d'entre elles grâce à notre introduction à la cryptographie, à la sécurité des réseaux et des ordinateurs.

# Le modèle CIA

- **Intégrité:** un système doit garantir l'exhaustivité, la précision et l'absence de modifications non autorisées de tous ses composants. Autrement dit, nous pouvons déterminer qu'un élément d'information est fourni comme demandé et nous pouvons vérifier sa provenance. Si une entité essaie de modifier cette information, elle ne peut le faire que si elle est autorisée.



# Le modèle CIA

- **Disponibilité** : Un système et tous les composants du système sont disponibles et opérationnels en cas de besoin, comme demandé par un utilisateur autorisé. Un système doit donc être fiable dans une certaine mesure et résilient à l'échec ou à une attaque (N).

# **Nous devons probablement définir certains termes!**

- Utilisateur autorisé - un utilisateur (personne ou système) qui a été authentifié. Une fois authentifié, un utilisateur dispose d'un certain niveau d'autorisation (par exemple, la capacité de visualiser, modifier, supprimer, administrer / gérer, etc.) qui est identifié et vérifié par le système.
- Authentification - un mécanisme (un protocole) par lequel un utilisateur est identifié et utilise un jeton pour prouver qui il est. L'authentification peut prendre de nombreuses formes, y compris la biométrie (c'est-à-dire l'utilisation de caractéristiques biologiques telles que le visage, l'iris, les empreintes digitales, etc.).

- Nous utilisons la cryptographie comme base pour cacher la signification des informations aux personnes ou aux systèmes qui n'ont pas la clé de déchiffrement (une information, généralement numérique, qui n'est connue que de l'utilisateur ou du système autorisé, et qui est tenue par eux de accéder aux informations). Dans ce cours, nous fournissons une introduction à la cryptographie au cours du Chapitre 2. Notez que, souvent, les données stockées dans un ordinateur ou sur disque sont appelées "données au repos" et les données transmises sont appelées "données en mouvement".

- Nous devons être sûrs que les informations ou les données auxquelles nous accédons sont valides, ce qui est obtenu par divers mécanismes d'intégrité. Notre définition identifie «l'absence de modifications non autorisées», cela implique plusieurs choses; (i) que le système suit (souvent appelé journalisation) quel utilisateur y a accès et que cet utilisateur a suivi les processus d'authentification appropriés, (ii) qu'il vérifie qu'un utilisateur doit avoir un accès en écriture avant de pouvoir effectuer une modification et enregistrer les modifications - et peut également conserver une sauvegarde des modifications ainsi que des informations d'audit, (iii) qu'un utilisateur autorisé peut afficher, modifier, supprimer, etc. uniquement les informations pour lesquelles il a l'autorisation, et (iv) le système peut être constitué d'un certain nombre de composants et donc l'authentification, l'autorisation, l'audit peuvent être quelque chose qui est partagé à travers un système.

Par conséquent, pour l'intégrité, nous devons authentifier et vérifier les niveaux d'autorisation, enregistrer les informations selon les besoins afin qu'un futur audit puisse identifier ce qui a eu lieu et, enfin, nous devons avoir la certitude que les informations ou les données que nous consultons sont correctes ou que la transaction que nous voulons entreprendre (par exemple, transfert d'argent ou paiement) est valide - c'est quelque chose que nous pouvons prouver mathématiquement / logiquement et nous en discutons brièvement au cours de la semaine 2. Ce dernier commentaire sur les transactions est important car nous devons considérer la non-répudiation (N).

Pour la disponibilité, nous cherchons à construire des systèmes fiables et capables de fournir des services dans un large éventail d'états de fonctionnement. Nous craignons qu'un système reste accessible aux utilisateurs autorisés pour une gamme de conditions de fonctionnement, par exemple en cas d'attaque ou d'utilisation intensive. Par exemple, un système connecté à Internet (ou à un autre réseau tel qu'un serveur sur un réseau cellulaire) peut être attaqué afin de refuser l'accès aux utilisateurs légitimes - un déni de service.

# QUIZ

## Question 1

Quel est le terme qui décrit le mieux ce qui suit: un expéditeur ne peut pas refuser d'envoyer un message, par ex. un e-mail ou un SMS.

- Non-répudiation des messages
- Confidentialité des messages
- Disponibilité des messages
- Intégrité du message

# QUIZ

## Question 2

Un message est intègre si:

- Il n'est pas modifié de façon vérifiable
- Il contient la vérité
- Il contient la signature manuscrite de l'expéditeur



# Les facettes qui composent le sujet de la sécurité de l'information

(N) Aujourd'hui, l'étendue de la cybersécurité informationnelle est encore en cours de définition. Il existe un certain nombre d'efforts internationaux qui cherchent à déterminer ce qui devrait être dans le programme d'études du premier cycle ou d'un Master en cybersécurité. Un effort majeur vient de l'ACM, qui a lancé un groupe de travail conjoint en 2015, composé de plusieurs grandes sociétés informatiques. Il est né du Cyber Educational Program aux États-Unis. L'IFIP, la Fédération internationale pour le traitement de l'information, qui a un groupe de travail sur l'éducation à la sécurité de l'information, est l'une des sociétés qui étudie ce domaine depuis longtemps. Ce programme existe depuis 1991 et son objectif est de promouvoir l'éducation à la sécurité de l'information et la formation au niveau universitaire ainsi qu'au sein du gouvernement et de l'industrie (N).

# Les facettes qui composent le sujet de la sécurité de l'information

1. Le premier est la cyberdéfense, qui comprend des aspects tels que la cryptographie, la sécurité informatique, la sécurité des réseaux et l'assurance de l'information.
2. Ensuite, les cyber opérations, qui couvrent les cyberattaques et les tests de pénétration. Dans les tests de pénétration, nous jouons l'attaquant, afin de comprendre ce qui peut être fait pour un système. Nous incluons également ici l'ingénierie inverse et la cryptanalyse.
3. Vient ensuite la criminalistique numérique, qui comprend la criminalistique matérielle et logicielle sur les hôtes et les services, les appareils mobiles, jusqu'aux systèmes embarqués, tels que les décodeurs. Ici, nous cherchons à identifier les incursions dans nos systèmes par des attaquants. Dans ce domaine, nous considérons également la réponse aux incidents, la cybercriminalité et la cyber application des lois comme faisant partie du programme.

# Les facettes qui composent le sujet de la sécurité de l'information

4. Les systèmes cyber-physiques, tels que le contrôle de supervision et l'acquisition de données, appelés systèmes SCADA, l'Internet des objets et les systèmes de contrôle industriels nous font sortir du bureau et de l'usine. Et c'est un élément essentiel de la cybersécurité, car beaucoup de valeur est créée en usine.

5. Le prochain est le développement de logiciels sécurisés, et cela inclut un certain nombre de facteurs différents tels que la conception de systèmes sécurisés, codage, déploiements et maintenance sécurisés du système. Et surtout, la convivialité d'un système sécurisé. Nous souhaitons bien sûr que tous les logiciels soient sécurisés et utilisables, mais ce n'est bien sûr pas le cas.

# Les facettes qui composent le sujet de la sécurité de l'information

6. La cyber-politique Il existe une gamme de réglementations qui s'appliquent aux cyber systèmes et aux opérations. Et, bien sûr, les cyber-lois sont très importantes pour nous en tant qu'individus, ainsi que pour des organisations telles que la loi sur la protection des données.

7. La gestion des cyber-risques comprend la cyber-résilience et l'assurance. Par exemple, nous devons penser à la reprise après sinistre et à la continuité des activités en tant qu'organisation. Comment y parvenir en cas d'attaque ou de défaillance d'un système. En cela, nous avons également des évaluations de sécurité.

8. Et nous devons considérer la cyberéconomie comme une partie intégrante.

# Les facettes qui composent le sujet de la sécurité de l'information

9. Le dernier domaine de connaissances concerne les comportements humains liés aux cyber systèmes et aux opérations. Comme l'ingénierie sociale par des attaquants qui utilisent les réseaux sociaux pour infiltrer nos organisations. De plus, l'expérience utilisateur et non le comportement organisationnel sont essentiels pour comprendre et développer des systèmes sécurisés.

# Le modèle RMIAS

- (N) Le RMIAS Le modèle de référence de l'assurance et de la sécurité de l'information proposé en 2013. et a combiné un certain nombre de points de vue différents, ou modèles, qui s'étendent sur la CIA (N).

# A Reference Model of Information Assurance & Security (RMIAAS)

