

Université de Tlemcen Faculté des Sciences Département Informatique	Année Universitaire 2020-2021 Module Sécurité Informatique Promotion : L3
---	---

TD1 : Notions de base – Les besoins/services de sécurité

Exercice 1

Pour chacun des situations suivantes, indiquez le besoin de sécurité qui a été affecté par un attaquant :

- Formatage/endommagement totale de votre disque dur **Disponibilité**
- Lecture de vos emails sur serveur par une tierce personne **Confidentialité**
- Accès au réseau de l'université afin d'accéder à Internet par une personne ne disposant pas d'un compte (étudiant, enseignant, employé) **Authentification**
- Modification des notes d'examens des étudiants sans la connaissance/autorisation de l'administration/enseignant. **Intégrité**
- Un rançomware prend en otage ton pc (tes données). **Disponibilité**

Exercice 2

Vous voulez passer une communication textuelle numérique interactive (ex, fb) avec une personne distante via le réseau Internet. Vous avez deux besoins à satisfaire : (1) Vous voulez vous assurer qu'une tierce personne ne puisse pas comprendre votre conversation. (2) Vous souhaitez vous assurer que votre conversation est intacte.

Q1- Citez les services de sécurité dont vous aurez besoin pour satisfaire les deux besoins ci-haut **Confidentialité et Intégrité**

Q2- Avez-vous une garantie que l'autre personne au bout de la connexion est bien la bonne personne qu'elle prétend être ? Pensez-vous que les deux services précédents sont suffisants ? **On a aucune garantie de l'autre personne au bout de la connexion. Les deux services confidentialité et intégrité ne le permettent pas, il faut donc implémenter le service d'authentification**

Exercice3

Dans une entreprise, il y a Cinq type de données, dont l'accès est hiérarchique :

- Top secret : connues uniquement au PDG de l'entreprise (1)
- Secret : connues en plus aux DGs de l'entreprise (2)
- Confidentiel : connues en plus aux sous-directeurs et autres responsables (3)
- Classé : connues en plus au reste des employés des entreprises (4)
- Publique : connue au grand public (5)

Ces données sont stockées sur un ou plusieurs serveur, et accessible aux personnes appropriées depuis le réseau intérieur de l'entreprise ou depuis l'extérieur. Pour les 3 premiers types de données l'accès instantané est primordiale, en plus, pour l'accès en écriture/modification il est impératif de savoir l'identité de la personne, alors qu'en lecture seul il suffit de s'assurer que la personne fait partie des catégories (1, 2, 3). Pour les 2 derniers types de données, l'accès n'a pas un caractère urgent (des délais peuvent être tolérés voir même une indisponibilité temporaire).

Questions:

- **Q1:** Selon vous, est ce que la sensibilité des données de l'entreprise est la même? **les données n'ont pas la même sensibilité**

- **Q2:** Selon vous quels sont les besoin en sécurité qui s'appliquent à ces données? **Confidentialité, Intégrité, Disponibilité, Authentification et Non répudiation**

- **Q3:** On désire maintenant noter sur une échelle chacun des besoins identifiés ci-haut.

* Pour le besoin exprimant la nécessité de pouvoir accéder au bien au moment voulu, l'échelle sera : Fort Faible

* Pour le besoin qui nous garantit que les données sont intactes l'échelle sera: Fort Faible

* Pour le besoin exprimant la nécessité de protéger le bien contre les accès non autorisés l'échelle sera : Extrêmement Important, Très Important, Important, Moins Important, Faible

* On adoptera la même échelle précédente pour le besoin permettant de trouver les circonstances dans lesquelles un bien évolue

	Disponibilité	Intégrité	Confidentialité	Authentification et non répudiation
Top Secret	Fort	Fort	Extrêmement Important	L : Extrêmement Important E : Extrêmement Important
Secret	Fort	Fort	Très Important	L : Très Important E : Extrêmement Important
Confidentiel	Fort	Fort	Important	L : Important E : Extrêmement Important
Classé	Faible	Fort	Moins Important	L : Moins Important
Publique	Faible	Fort	Faible	L : Faible

- **Q4:** Selon vous, comment sera régulé l'accès aux données, pour savoir qui aura accès à quoi? **authentification + droit d'accès**

- **Q5** (en lien avec Q4): Supposant qu'un attaquant veut avoir un accès aux données, mais qu'il n'a pas les moyens pour pénétrer directement le/les serveurs hébergeant les données, dans ce cas à qui s'attaquera-t-il? et dans quel but ? **l'attaquant s'attaquera aux utilisateurs afin d'avoir un compte utilisateur**

- **Q6** (en lien avec Q5) Selon vous quel est la cible idéal de l'attaquant lui permettant d'avoir l'accès à toutes les données ? Comment cette attaque peut avoir lieu ? **cible idéal de l'attaquant est le PDG, moyen : le fishing**

- **Q7** Supposant qu'un des serveurs contenant les données soit physiquement volé, mais que l'accès à la machine est protégé par login/mot de passe robuste. Est-ce que dans cette situation, le besoin de confidentialité sera toujours assuré ? **Non**

- **Q8** (en lien avec Q7) selon vous est ce que les données de l'entreprises sont stockés et transmis sur réseau en clair (de façon lisible)? **Les données doivent être chiffrées**

- **Q9** Est ce que attribué un même login/mot de passe à l'ensemble des DGs pour accès au donnée risque d'affaiblir un des besoins en sécurité ? Si oui lequel ? **Non répudiation**