University of khenchela
Department MI

Computer security

Dr. Hichem Rahab

L3 ISIL

2022 - 2023

Chapter 1: Computer security / Information security

Overview

Introduction (1)

- La sécurité informatique constitue l'ensemble de moyennes mises en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.
- L'objectif de la sécurité informatique est d'assurer que les ressources (**Assets**) matérielles et/ou logicielles d'un parc informatique sont uniquement utilisées dans le cadre prévu et par des personnes autorisées.

Introduction (2)

- La sécurité d'un système est modélisée par une chaine où on mesure la sécurité de cette chaine entière à la sécurité de son maillon le plus faible.
- Si tout un système est sécurisé techniquement mais que le facteur humain, souvent mis en cause, est défaillant, c'est toute la sécurité du système qui est remise en cause.

Figure: Chaine de sécurité

Risk

Le risque (**Risk**) en sécurité est donné par la formule suivante :

$$Risk = \frac{Threat \times Vulnerabily}{Counter\_mesures}$$

- **Risque (Risk)**: C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- **Vulnérabilité (Vulnerability):** C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier.
- **Menace (Threat):** c'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.
- **Contre-mesure (Counter mesures):** c'est l'ensemble de moyens mises en place pour faire face aux risques dans une organisation.

Conséquences de la formule:

- Plus on augmente les contre-mesures (**Counter mesures**); plus on réduise les risques possibles **(Possible risks)**.
- Le plus sont les vulnérabilités (**Vulnerabilities**) et les menaces (**Threats**) contre le système ; le plus le risque (**Risk**) est important.

Security objectives

Il convient d'identifier les exigences fondamentales en sécurité informatique, qui caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques au regard de la sécurité :

1. L'authentification (**Authenticity**).
2. Le contrôle d'accès (**Acces control**).
3. La confidentialité (**Confidentiality**).
4. L'intégrité (**Intergrity**)
5. La disponibilité (**Availibility**).
6. La non-répudiation (**Non repudiation**)

1. Authenticity

- L'authentification permet de limiter l'accès aux personnes autorisées.
- Elle exige d'assurer de l'identité des utilisateurs avant l'échange de données.
- Dans le cas d'un seul message, tel qu'un signal d'avertissement ou d'alarme, la fonction du service d'authentification est d'assurer au destinataire que le message provient de la source qu'il prétend être.

Figure: Authenticity

1. Authenticity (2)

- Dans le cas d'une interaction continue, comme la connexion d'un terminal à un hôte, deux aspects sont impliqués:
  1. Au moment de l'initiation de la connexion, le service garantit que les deux entités sont authentiques, (chacune est l'entité qu'elle prétend être).
  2. Le service doit s'assurer que la connexion n'est pas entravée de telle sorte qu'un tiers peut se faire passer comme l'une des deux parties légitimes aux fins d'une transmission ou d'une réception non autorisée.

Figure: Authenticity

2. Acces control

- Le contrôle d'accès (**Acces control**) constitue une précaution prise contre l'utilisation non autorisée d'une ressource;
- Le contrôle d'accès permet de limiter et de contrôler l'accès aux systèmes et aux applications via les liaisons de communication.
- Pour ce faire, chaque entité qui tente d'accéder doit d'abord être identifiée ou authentifiée, de sorte que les droits d'accès peuvent être adaptés à l'individu.

Figure: Acces control

3. Confidentiality

- Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.
- Seules les personnes habilitées doivent avoir accès aux données.
- Toute interception ne doit pas être en mesure d'aboutir, les données (**data**) doivent être cryptées, seuls les acteurs de la transaction possèdent la clé (**key**) de compréhension.
- La confidentialité (**Confidentiality**) doit assurée que l'information est inintelligible à d'autres personnes que les seuls acteurs de la transaction.

Figure: Confidentiality

3. Confidentiality (2)

- La confidentialité est également un principe éthique associé à plusieurs professions, notamment dans les domaines de l'enseignement, la médecine, du droit, de la vente, de l'informatique, de la religion, du journalisme, etc.
- En éthique et en droit, certains types de communication entre une personne et un de ces professionnels sont dites " privilégiées ", et ne peuvent être discutées avec, ou divulguées à des tierces parties.
- Dans certaines juridictions où la loi assure une telle confidentialité, des sanctions sont habituellement prévues dans les cas d'infraction.

4. Integrity

- Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.
- Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication.
- L'intégrité des données (**Data integrity**) doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- Un service d'intégrité axé sur la connexion, qui traite d'un flux de messages, assure que les messages sont reçus comme envoyés, sans: duplication, insertion, modification, réorganisation ou répétition.

5. Availibility

- C'est la propriété d'être accessible et utilisable sur demande par une entité autorisée.
- Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment.
- La disponibilité d'un équipement (**Asset availibility**) se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.
- Ce service répond aux problèmes de sécurité soulevés par les attaques de déni de service(**Denial of Service DoS attacks**).

$$Disponibilite = \frac{Duree\_durant\_laquelle\_cet\_equipement\_est\_operationnel}{Duree\_durant\_laquelle\_il\_aurait\_du\_etre\_operationnel}$$

6. Non repudiation

- Une transaction ne peut être niée par aucun des correspondants.
- La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues.
- La non répudiation empêche l'émetteur ou le récepteur de refuser un message transmis.
- Ainsi, lorsqu'un message est envoyé, le destinataire peut prouver que l'expéditeur présumé a en effet envoyé le message.
- De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le récepteur a effectivement reçu le message.
- Cela se fait par le biais de certificats numériques grâce à une clé privée (**Private key**).

Levels of threat (1)

FIPS 199 a défini trois niveaux d'impact sur les organisations ou les les individus :

1. **Bas (Low) :** L'attaque peut avoir une effet limité sur les opérations de l'organisation, ses biens (**Assets**) ou personnes. Un effet adversaire limité signifie par exemple, une perte de confidentialité (**confidentiality**) , (**integrity**) , (**availability**), peut:
   - (i) Causer une dégradation dans les capacités de fonctionnement (**mission capability**) à une niveau et durée que l'organisation est capable d'accomplir ces fonctions principales, mais l'efficacité des fonctionnalités est visiblement réduite.
   - (ii) Résulte en un dommage minimale dans les bien de l'organisation (**organizational assets**);
   - (iii) Résulte en une perte financière minimale (**minor financial loss**);
   - (iv) Résulte en un mal minimal aux individus (**Minimal harm to individuals**).

Levels of threat (2)

FIPS 199 a défini trois niveaux d'impact sur les organisations ou les les individus :

1. **Modéré (Moderate)**: La perte (**loss**) est prévu d'avoir un effet adversaire sérieux sur les opérations de l'organisation (**organizational operations**), ses biens (**organizational assets**), ou ses individus (**individuals**). Un effet adversaire sérieux signifie, par exemple:
   - (i) Une dégradation significative dans les capacités de fonction (**mission capability**) à un niveau et une durrée que l'organisation est capable d'accomplir ses fonction de base (**primary functions**), mais l'efficacité des fonctions (**the effectiveness of the functions**) est réduite de manière significative;
   - (ii)Un dommage significatif dans les biens de l'organisation (**significant damage to organizational assets**);
   - (iii) Une perte financière significatif (**significant financial loss**); ou
   - (iv) Un mal significatif au individus qui n'implique pas une perte de vie (**loss of life**) ou des blessures sérieuses qui menacent la vie (**serious life-threatening injuries**).

Levels of threat (3)

1. **Haut (High:)** La perte est prévue d'avoir un effet adversaire sévère ou catastrophique sur les opération de l'organisation (**organizational operations**), ses biens (**organizational assets**), ou individus (**individuals**).La menace peut :
   - (i) causer une dégradation sévère ou perte dans les capacité de fonction (**mission capability**) à un niveau et une durée que l'organisation est incapable d'accomplir une ou plusieurs de ses fonctions vitales (**primary functions**);
   - (ii) Résulte en un dommage majeur dans les biens (**organizational assets**);
   - (iii) Résulte en une perte financière majeur (**major financial loss**); ou
   - (iv) Résulte en un mal catastrophique aux individus qui provoque une perte de vie (**loss of life**) ou des blessures menacent la vie (**serious life-threatening injuries.**)

Examples

Confidentiality

- Les notes des étudiants sont des données dont la confidentialité a une **haute** importance pour les étudiants (**high confidentiality level**). Dans les EUs, les notes des étudiants ne doivent être disponibles qu'aux étudiants, leurs parents, et les employés qui nécessitent ces notes pour leur travail.
- Les informations d'enregistrement des étudiants peuvent avoir une niveau de confidentialité **modéré** (**moderate confidentiality level**). Ces informations peuvent être vus par
- Le fichier des informations, les listes des étudiants d'un département par exemple, peut avoir un degré de confidentialité **bas** (**low confidentiality level**). Cette information est librement disponible au public dans le site web de l'université ou du département.

Integrity

- Several aspects of integrity are illustrated by the example of a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now, suppose an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital. The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible. Patient allergy information is an example of an asset with a **high** requirement for integrity. Inaccurate information could result in serious harm or death to a patient, and expose the hospital to massive liability.

Integrity (2)

- An example of an asset that may be assigned a **moderate** level of integrity requirement is a website that offers a forum to registered users to discuss some specific topic. Either a registered user or a hacker could falsify some entries or deface the website. If the forum exists only for the enjoyment of the users, brings in little or no advertising revenue, and is not used for something important such as research, then potential damage is not severe. The Webmaster may experience some data, financial, and time loss.
- An example of a **low** integrity requirement is an anonymous online poll. Many websites, such as news organizations, offer these polls to their users with very few safeguards. However, the inaccuracy and unscientific nature of such polls is well understood.

Availability

The more critical a component or service is, the higher will be the level of availability required.

- Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks. The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss. Such system has a **high** availability requirement.
- An example of an asset that would typically be rated as having a **moderate** availability requirement is a public website for a university; the website provides information for current and prospective students and donors. Such a site is not a critical component of the university's information system, but its unavailability will cause some embarrassment.

Availability (2)

- An online telephone directory lookup application would be classified as a **low** availability requirement. Although the temporary loss of the application may be an annoyance, there are other ways to access the information, such as a hardcopy directory or the operator.

The end