CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Module 1 : notions de base

05/11/2015

Plan du module

1. Les enjeux de la sécurité des S.I.
2. Les besoins de sécurité
3. Notions de vulnérabilité, menace, attaque
4. Panorama de quelques menaces
5. Le droit des T.I.C. et l'organisation de la sécurité en France

1. Les enjeux de la sécurité des S.I.

a) Préambule
b) Les enjeux
c) Pourquoi les pirates s'intéressent aux S.I. ?
d) La nouvelle économie de la cybercriminalité
e) Les impacts sur la vie privée
f) Les infrastructures critiques
g) Quelques exemples d'attaques

1. Les enjeux de la sécurité des S.I.

a. Préambule

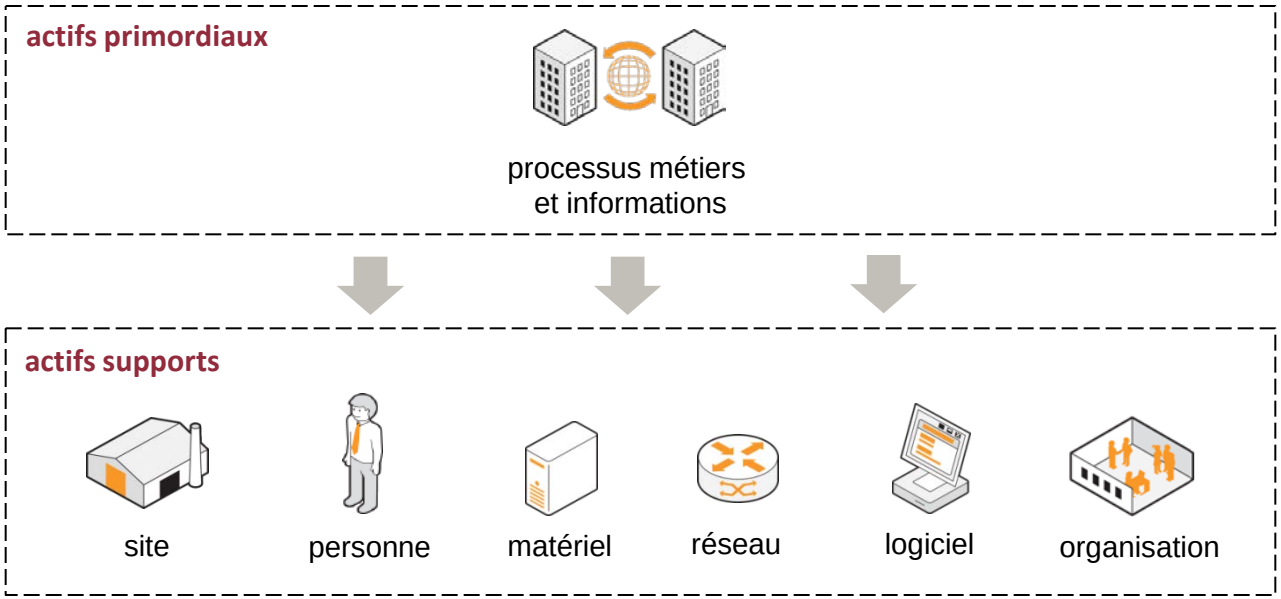
- Système d'Information (S.I.)
  - Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
  - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de l'organisation

1. Les enjeux de la sécurité des S.I.

a. Préambule

- Le système d'information d'une organisation contient un ensemble d'actifs :



ISO/IEC 27005:2008

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

1. Les enjeux de la sécurité des S.I.

b. Les enjeux

- La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations…

- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :

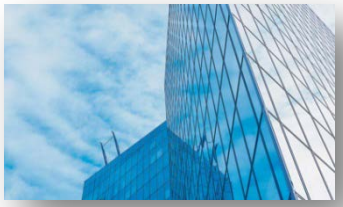
  – Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre

  – Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

1. Les enjeux de la sécurité des S.I.

b. Les enjeux

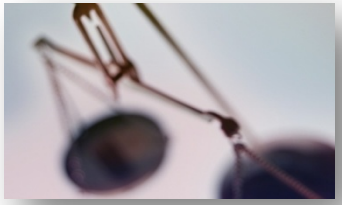
Impacts financiers



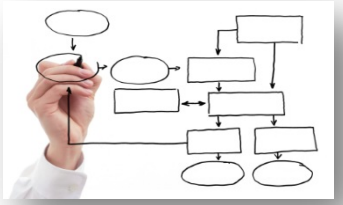
Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires



Impacts organisationnels



2. Les besoins de sécurité

a) Introduction aux critères DIC
b) Besoin de sécurité : « Preuve »
c) Différences entre sureté et sécurité
d) Exemple d'évaluation DICP
e) Mécanisme de sécurité pour atteindre les besoins DICP

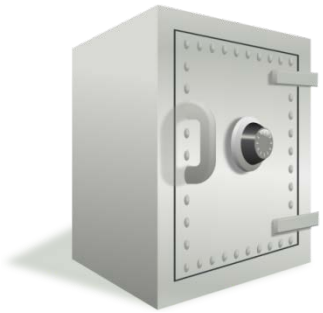
2. Les besoins de sécurité

a. Introduction aux critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?

- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger



Disponibilité

Propriété d'accessibilité au moment voulu des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité

Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité

Propriété des biens de n'être accessibles qu'aux personnes autorisées

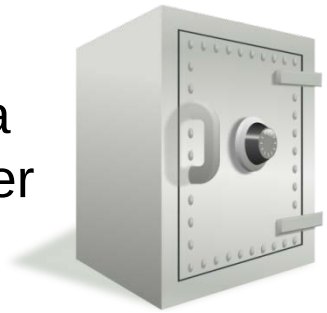
2. Les besoins de sécurité

b. Besoin de sécurité : « Preuve »

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?

- 1 critère complémentaire est souvent associé au D.I.C.

Bien à protéger



Preuve

Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe Notamment :

La traçabilité des actions menées
L'authentification des utilisateurs
L'imputabilité du responsable de l'action effectuée

2. Les besoins de sécurité

c. Différences entre sureté et sécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage…*

* Certaines de ces parades seront présentées dans ce cours

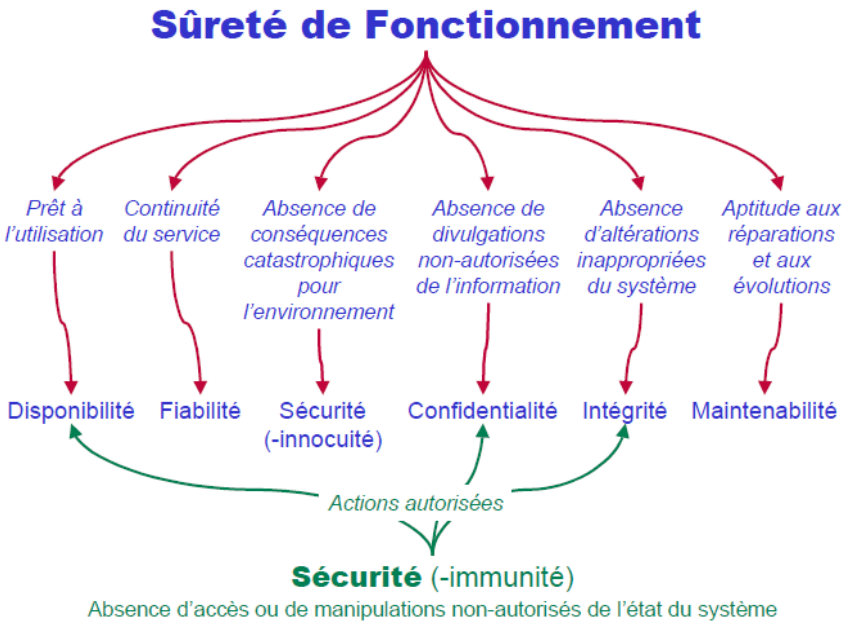
2. Les besoins de sécurité

c. Différences entre sureté et sécurité

Sûreté : ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité : ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Le périmètre de chacune des 2 notions n'est pas si clairement délimité dans la réalité : dans le cas de la voiture connectée on cherchera la sécurité et la sûreté.



On constate sur le schéma que la notion de sécurité diffère selon le contexte :

- sécurité ► innocuité
- sécurité ► immunité

2. Les besoins de sécurité

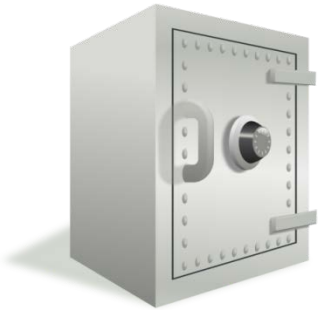
d. Exemple d'évaluation DICP

Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

L'expression du besoin attendu peut-être d'origine :

- **Interne** : inhérente au métier de l'entreprise
- ou **externe** : issue des contraintes légales qui pèsent sur les biens de l'entreprise.

Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :



Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible

Le bien bénéficie d'un niveau de sécurité adéquat

2. Les besoins de sécurité

d. Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site institutionnel simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

Disponibilité = **Très fort**

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaitre ses services au public

Intégrité = **Très fort**

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)

Serveur web

Confidentialité = **Faible**

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = **Faible**

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie :

		D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

		D	I	C	P
Capacité d'audit	Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.	✓	✓	✓	✓
Clauses contractuelles avec les partenaires	Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients	✓	✓	✓	✓
Formation et sensibilisation	Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I. Diffusion des bonnes pratiques de sécurité. Le cours actuel en est une illustration !	✓	✓	✓	✓

Certains de ces mécanismes seront présentés dans le cadre cette sensibilisation à la cybersécurité

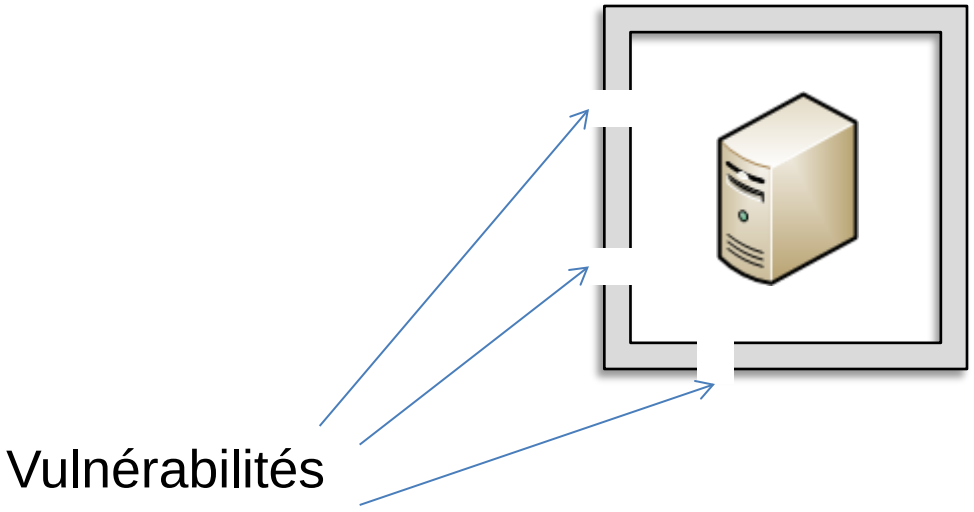
3. Notions de vulnérabilité, menace, attaque

a) Notion de « Vulnérabilité »
b) Notion de « Menace »
c) Notion d'« Attaque »
d) Exemple de vulnérabilité lors de la conception d'une application
e) Illustration d'un usage normal de l'application vulnérable
f) Illustration de l'exploitation de la vulnérabilité présente dans l'application

3. Notions de vulnérabilité, menace, attaque

a. Notion de « Vulnérabilité »

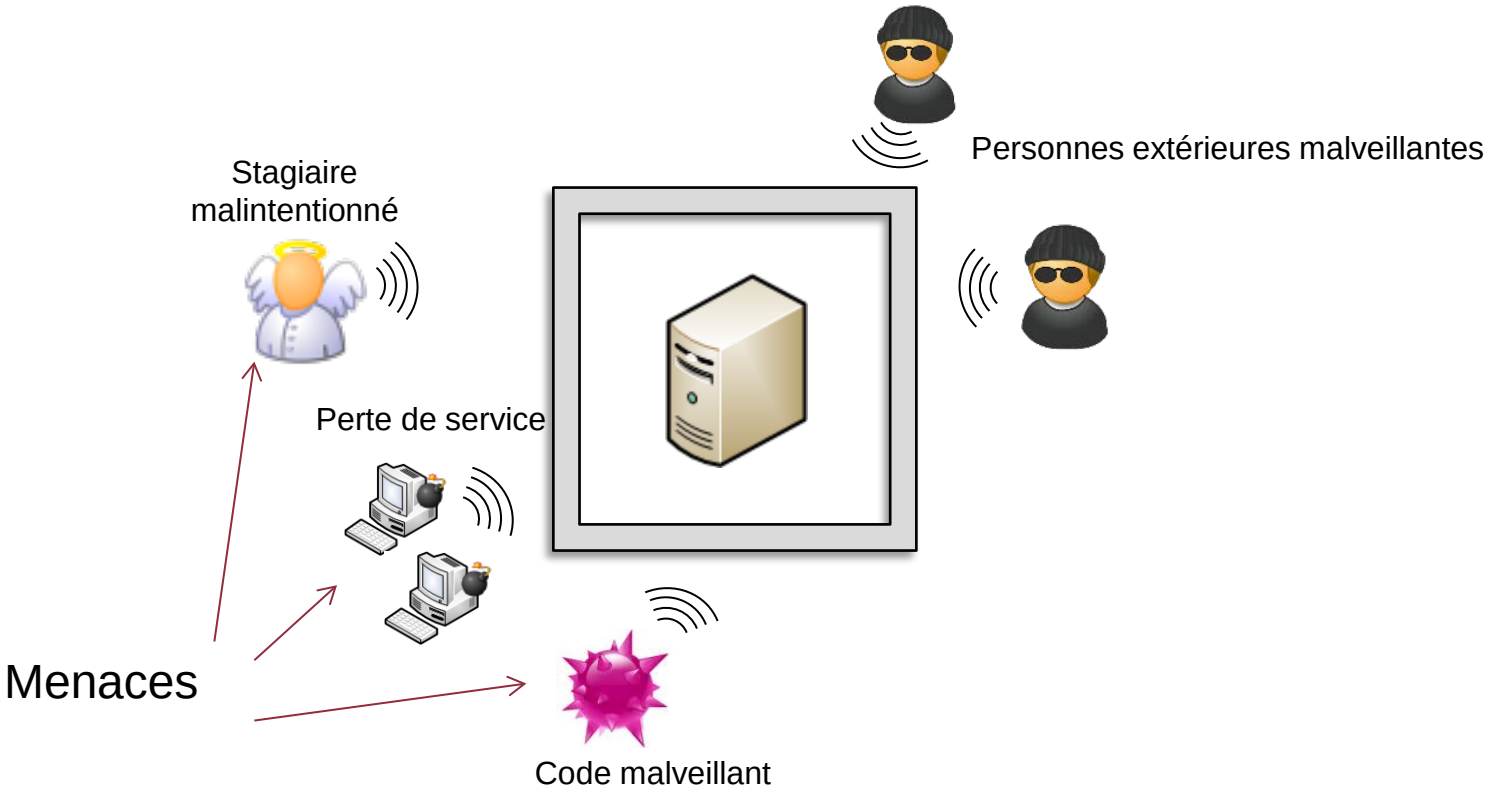
- **Vulnérabilité**
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



3. Notions de vulnérabilité, menace, attaque

b. Notion de « Menace »

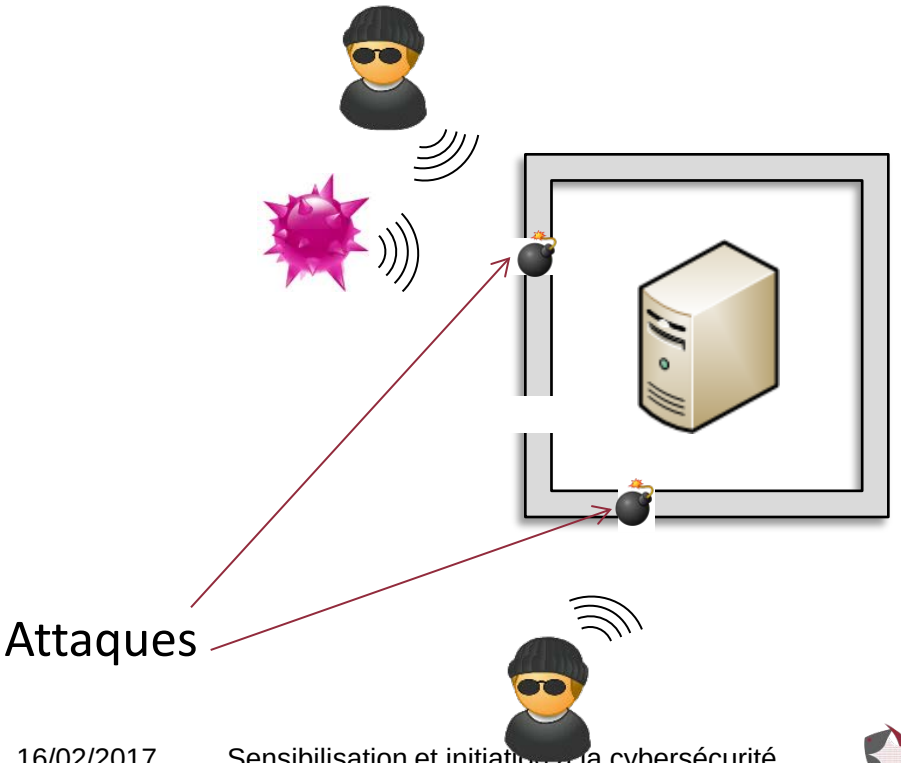
- **Menace**
- **Cause *potentielle* d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

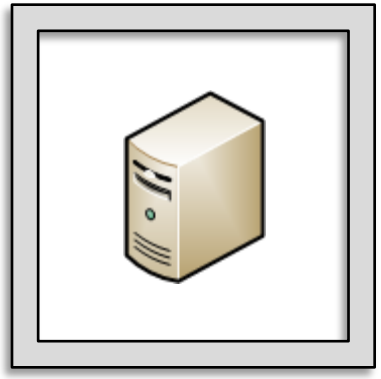
- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

- **Attaque**
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.



Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

3. Notions de vulnérabilité, menace, attaque

d. Exemple de vulnérabilité : Contournement de l'authentification dans l'application VNC

L'application VNC permet à un utilisateur de prendre en main sur une machine distance, après qu'il se soit authentifié.

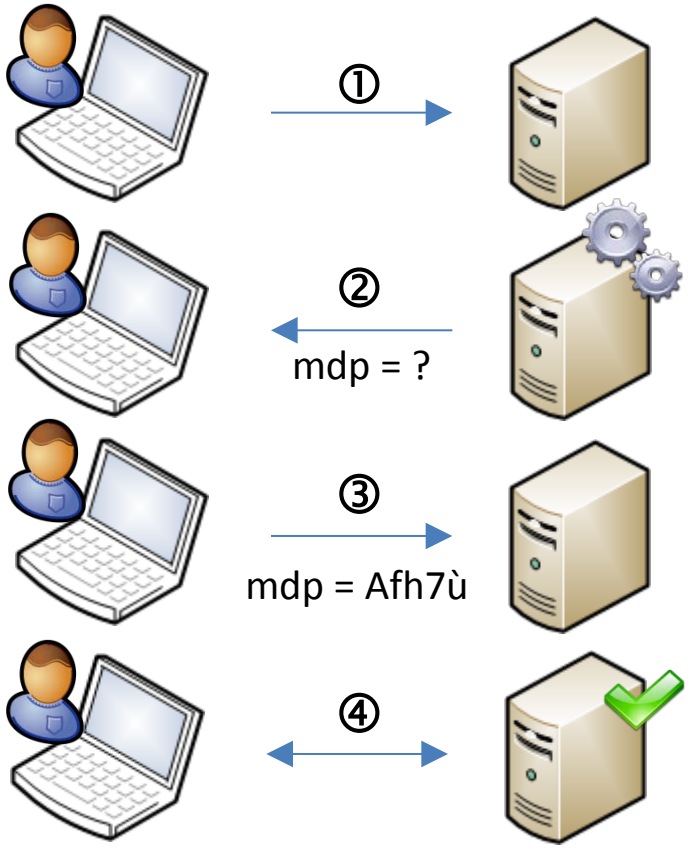
- La vulnérabilité décrite dans les planches suivantes est corrigée depuis de nombreuses années. Elle est symptomatique d'une **vulnérabilité dans la conception d'une application ;**
- L'application permet en temps normal à un utilisateur de se connecter à distance sur une machine pour y effectuer un « partage de bureau » (i.e. pour travailler à distance sur cette machine) ;
- En 2006, il est découvert que cette application – utilisée partout dans le monde depuis de très nombreuses années – présente une vulnérabilité critique : il est possible de se connecter à distance sur cette application **sans avoir besoin de s'authentifier** (i.e. tout utilisateur sur internet peut se connecter à distance sur les systèmes en question) ;
- Le diaporama suivant illustre la **vulnérabilité technique** sous-jacente à ce comportement.

3. Notions de vulnérabilité, menace, attaque

e. Illustration d'un usage normal de l'application vulnérable

Description du fonctionnement normal de l'application

L'utilisateur effectue une demande de connexion au serveur depuis son PC client



Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat*, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur

L'utilisateur s'authentifie selon la méthode choisie par le serveur

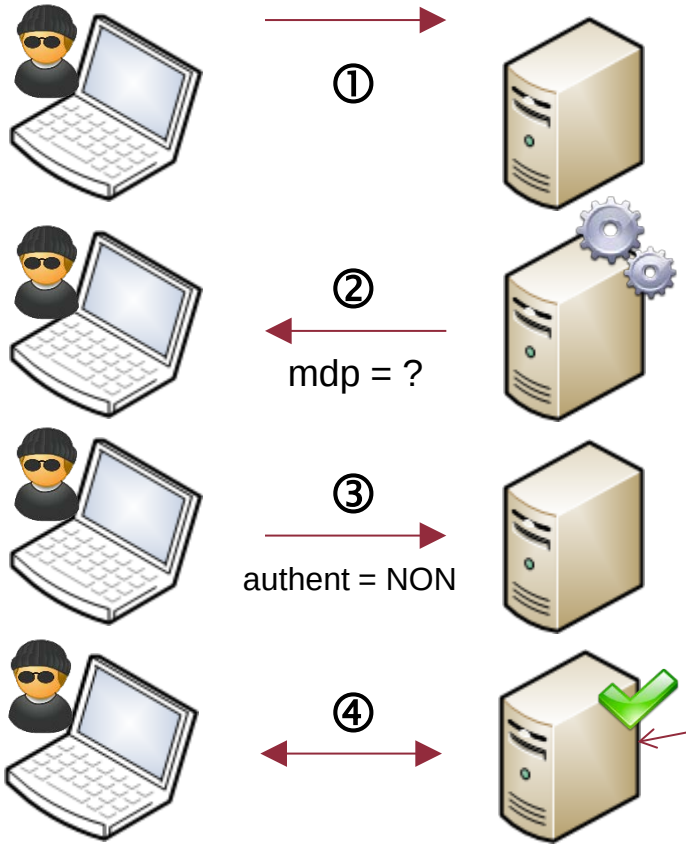
Le serveur valide l'authentification (si elle est correcte) et autorise donc la connexion

Référence : CVE-2006-2369

3. Notions de vulnérabilité, menace, attaque

f. Illustration de l'exploitation de la vulnérabilité présente dans l'application

L'attaquant effectue une demande de connexion au serveur depuis son PC client



Description du fonctionnement modifié par un attaquant

Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat*, etc.) et envoie cette demande d'authentification à l'utilisateur demandeur

L'attaquant choisit de s'authentifier avec le mécanisme de son choix, et non pas avec le mécanisme choisi par le serveur. Ici il choisit la méthode « pas d'authentification »

Le serveur valide l'authentification (car elle est valide i.e. aucune authentification est une méthode valide) et autorise donc la connexion

Référence : CVE-2006-2369

La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « authent = NON » est effectivement une authentification qui est toujours correcte)

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Merci de votre attention