CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Module 1 : notions de base

08/04/2020

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 Europe
6. … en France
7. … dans le monde

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

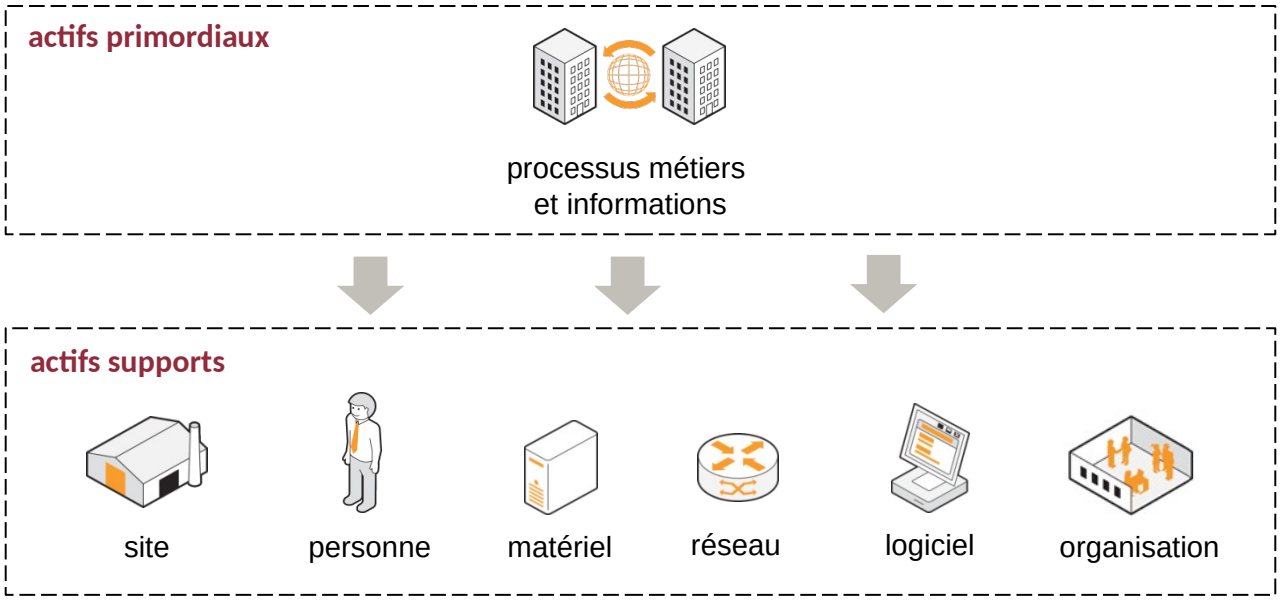
- Système d'Information (S.I.)
  - Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
  - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

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 :

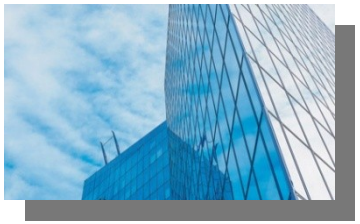
  - Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre

  - 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

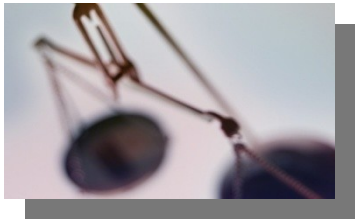
Impacts financiers



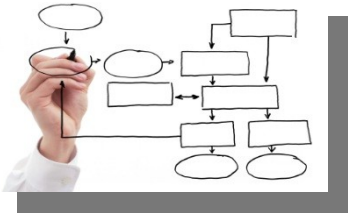
Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires



Impacts organisationnels



1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- Les motivations évoluent
  - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
  - De nos jours : majoritairement des actions organisées et réfléchies

- Cyber délinquance
  - Les individus attirés par l'appât du gain
  - Les « hacktivistes »
  - Motivation politique, religieuse, etc.
  - Les concurrents directs de l'organisation visée
  - Les fonctionnaires au service d'un état
  - Les mercenaires agissant pour le compte de commanditaires
  - …

1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires

- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)

- **Chantage**
  - Déni de service
  - Modifications des données

- **Espionnage**
  - Industriel / concurrentiel
  - Étatique

- …

1. Les enjeux de la sécurité des S.I.

d. La nouvelle économie de la cybercriminalité

- Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs

des groupes spécialisés dans le **développement de programmes malveillants** et virus informatiques

des groupes en charge de l'**exploitation et de la commercialisation** de services permettant de réaliser des attaques informatiques

un ou plusieurs **hébergeurs** qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates

4 des groupes en charge de la **vente des données volées**, et principalement des données de carte bancaire

5 des **intermédiaires financiers** pour collecter l'argent qui s'appuient généralement sur des réseaux de **mules**

1. Les enjeux de la sécurité des S.I.

e. Les impacts de la cybercriminalité sur la vie privée (quelques exemples)

- **Impact sur l'image / le caractère / la vie privée**
  - Diffamation de caractère
  - Divulgation d'informations personnelles
  - Harcèlement / cyber-bullying
- **Usurpation d'identité**
  - « Vol » et réutilisation de logins/mots de passe pour effectuer des actions au nom de la victime
- **Perte définitive de données**
  - malware récents (rançongiciel) : données chiffrées contre rançon
  - connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données
- **Impacts financiers**
  - N° carte bancaire usurpé et réutilisé pour des achats en ligne
  - Chantage (divulgation de photos ou d'informations compromettantes si non paiement d'une rançon)

Ces impacts – non exhaustifs – ne signifient pas qu'il ne faut pas utiliser Internet, loin de là !

Il faut au contraire apprendre à anticiper ces risques et à faire preuve de discernement lors de l'usage d'Internet/smartphones…

1. Les enjeux de la sécurité des S.I.

e. Les impacts de la cybercriminalité sur les infrastructures critiques

- Infrastructures critiques = un ensemble d'organisations parmi les secteurs d'activité suivants, et que l'État français considère comme étant tellement critiques pour la nation que des mesures de sécurité particulières doivent s'appliquer
  - Secteurs étatiques : civil, justice, militaire…
  - Secteurs de la protection des citoyens : santé, gestion de l'eau, alimentation
  - Secteurs de la vie économique et sociale : énergie, communication, électronique, audiovisuel, information, transports, finances, industrie.

- Ces organisations sont classées comme **Opérateur d'Importance Vitale (OIV).** La liste exacte est classifiée (donc non disponible au public).

1. Les enjeux de la sécurité des S.I.

Quelques exemples d'attaques, ce qui pourrait arriver

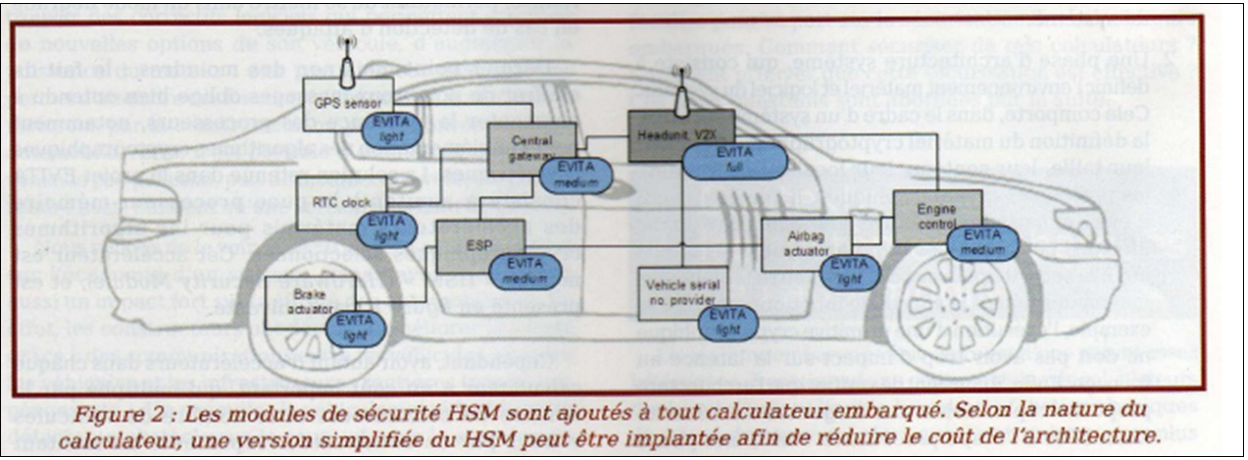
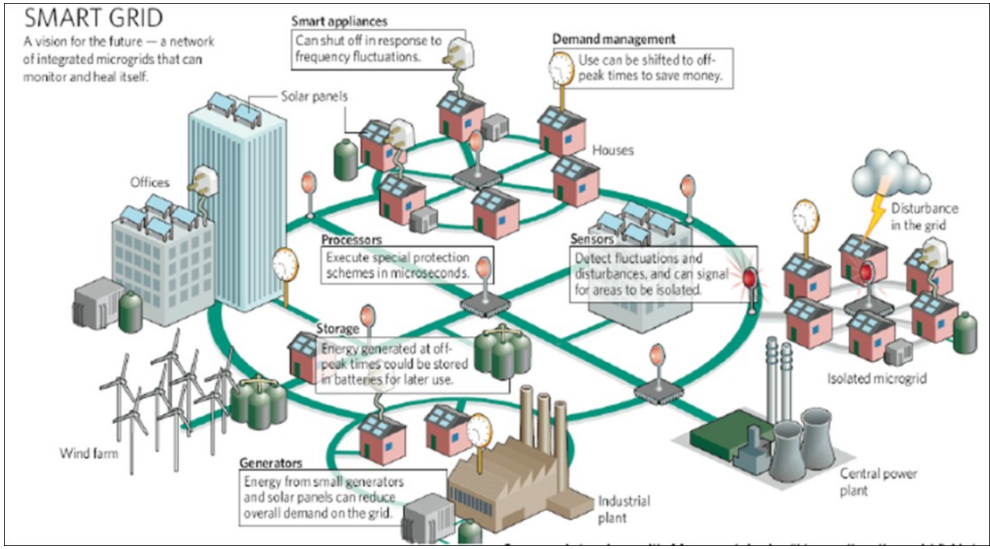


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout calculateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

Cyberattaques sur la voiture connectée envisagées à l'horizon 2020
Exemple : Prise de contrôle du système de frein

Déploiement des smart grid prévu à l'horizon 2030
Exemple : Blackout sur une grille.



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

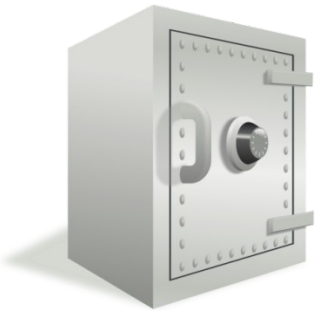
2. Les besoins de sécurité

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

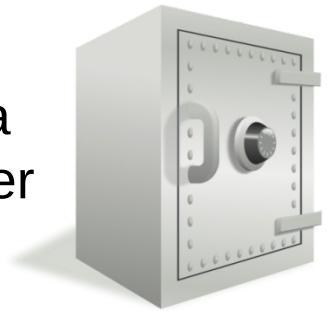
2. Les besoins de sécurité

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

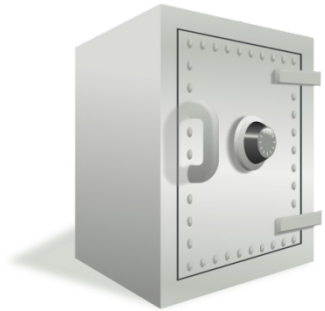
d. Exemple d'évaluation DICP

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

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Merci de votre attention