

# M1

## Sécurité des systèmes d'informations

2023-2024

SESSION

Partie  
1



# Aujourd’hui : Session 2 : Notions de base

- Les détections des vulnérabilités
- Correction TP 1
  - Formulaire d’identification sécurisé
- Les enjeux de la sécurité des S.I.
- Besoin de sécurité : Preuve
- Les notions des vulnérabilités
- Les règles en France
- ...



- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

# Session 1



# Stéganographie : L'art de cacher les choses

Q : Trouver Une tête de pirate dans l'image





- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

# OWASP

- Open Web Application Security Project
- Organisme à but non lucratif mondial
  - Pour l'amélioration de la sécurité des logiciels.
- Crée en 2001
- Communauté, de plus de 45000 membres
- Objectif :
  - Informer
    - Les individus
    - Les entreprises
  - Sur les risques liés à la sécurité des systèmes d'information.
- Propose des guides et des livres blancs des bonnes pratiques.

# Productions

- Des outils
- Des API
- De la documentation
- Des guides
- Des conférences
- Des blogs
- Des contenus
  - Audio / Vidéo
  - Podcast





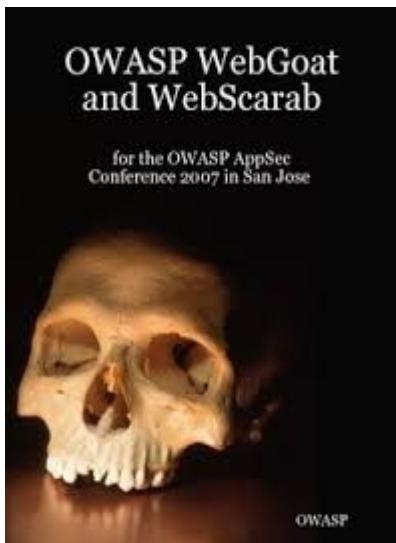
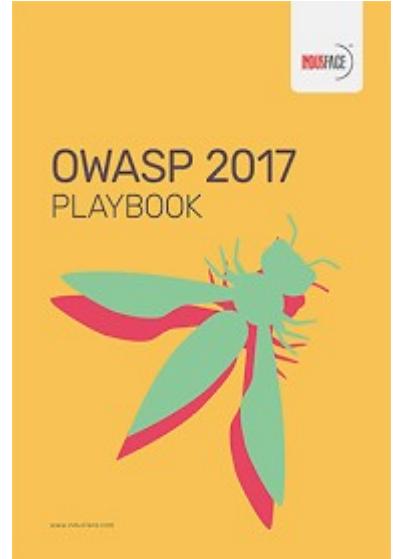
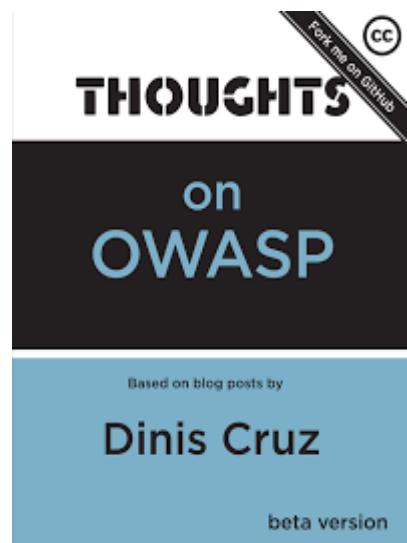
## OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks



<https://owasp.org>

This work is licensed under a  
[Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)

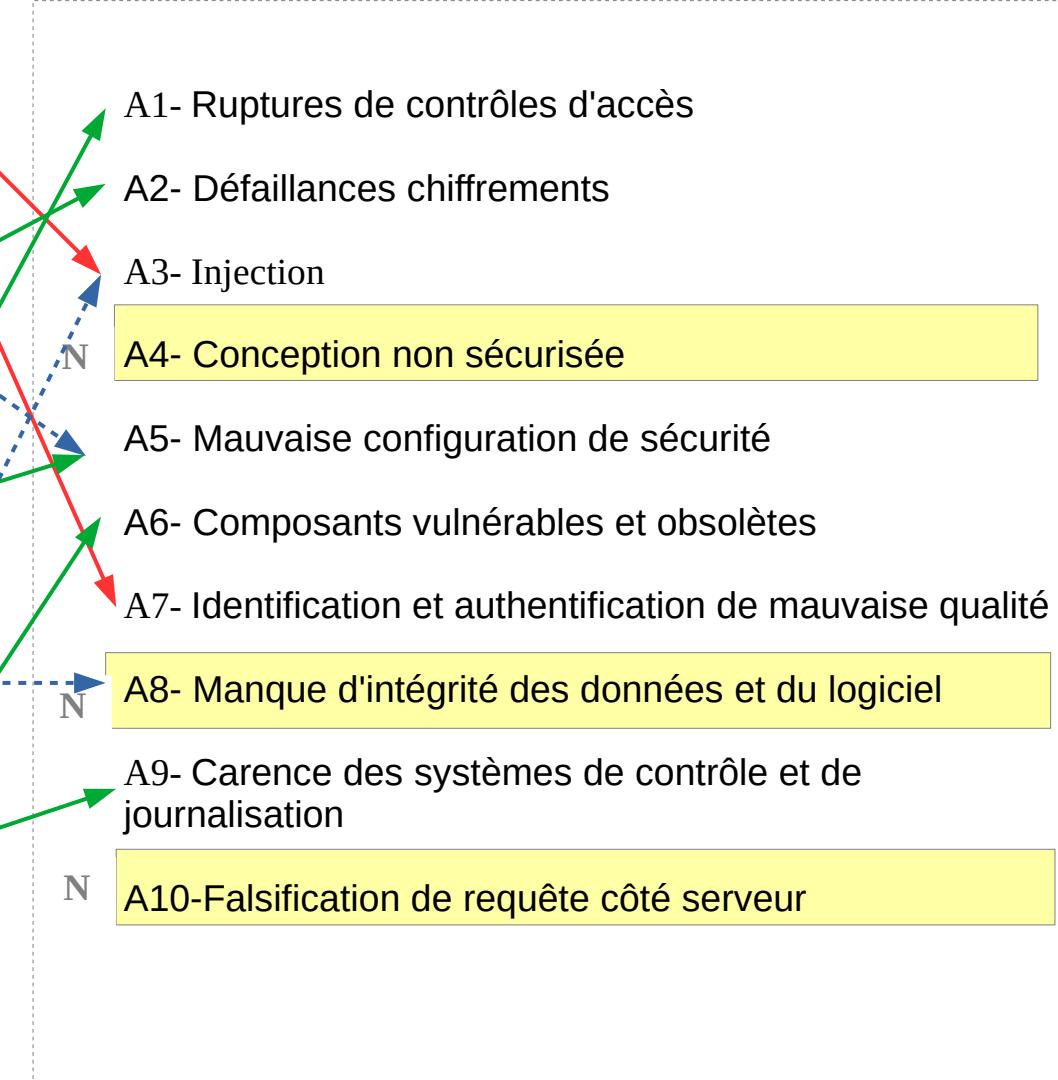
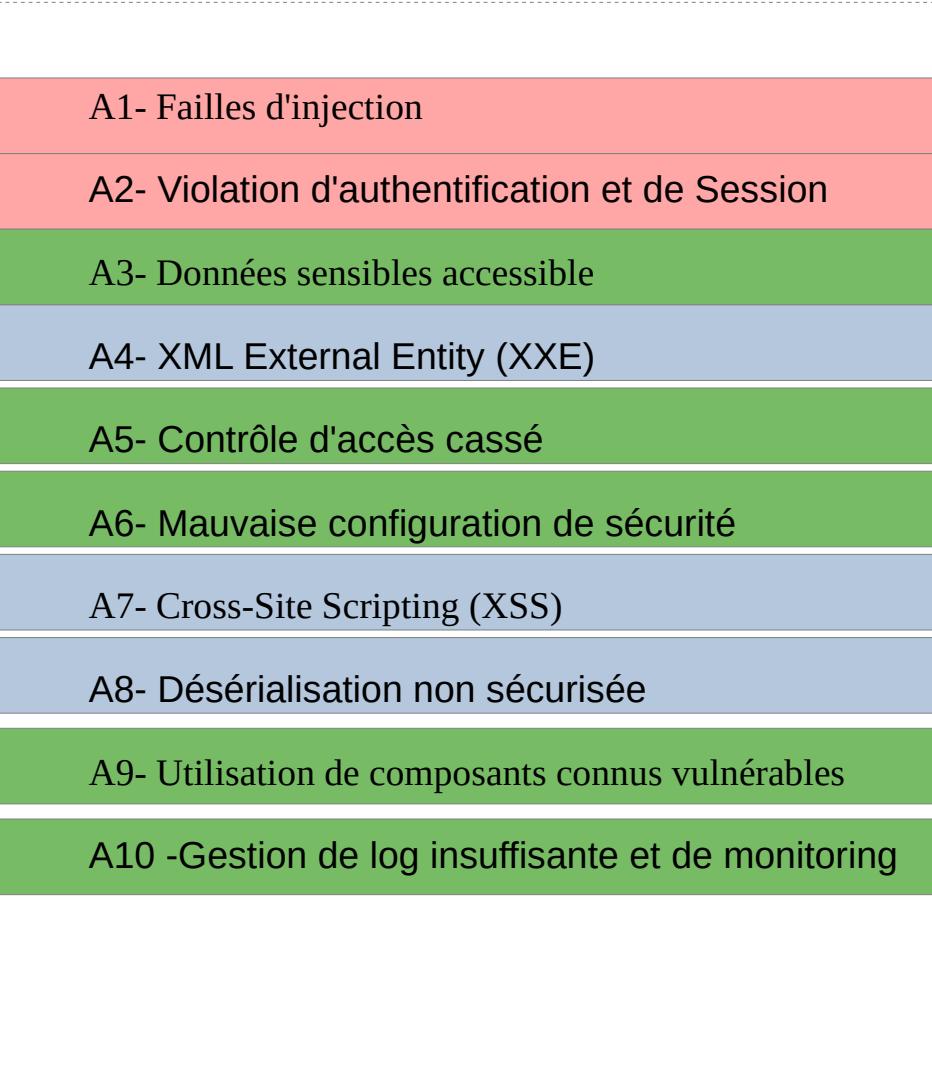


# Owasp : Les guides

- Guide de développement
  - [https://www.owasp.org/index.php/Projects/OWASP\\_Development\\_Guide](https://www.owasp.org/index.php/Projects/OWASP_Development_Guide)
- Guide des tests
  - [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
- Revue de code
  - [https://www.owasp.org/index.php/Category:OWASP\\_Code\\_Review\\_Project](https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project)
- Exemple d'application Webgoat
  - [https://www.owasp.org/index.php/Category:OWASP\\_WebGoat\\_Project](https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)
- Guide développeur
  - [https://www.owasp.org/index.php/OWASP\\_Guide\\_Project](https://www.owasp.org/index.php/OWASP_Guide_Project)

# TOP 10 : OWASP

2017



▲ Hausse

▼ Baisse

► Merge

■ Nouveau

# Rupture de contrôle d'accès

## Principe de l'attaque

- ✓ Absence de contrôle d'accès
- ✓ Défaillances affichent les données sensibles
- ✓ Ne pas accéder à des contenus précis
- ✓

## Conséquence

- ✓ Modification URL
- ✓ Manipulation de métadonnées
  - ✓ JSON, Token, CORS
- ✓ Forcer la navigation vers les pages authentifiées pour un anonym

# Défaillances de chiffrement

## Principe de l'attaque

- ✓ Transports données sensibles
- ✓ Chiffrement absent
- ✓ Hash faible
- ✓ Recherche des messages d'erreurs, ligne de débug
- ✓

## Conséquence

- ✓ Vol de mots passe, CB, données médicales, vie privée
- ✓ RGDP
- ✓ Effectué des opérations non prévues initialement

# Injection de ligne de commandes

## Principe de l'attaque

- ✓ Configuration non à jour
- ✓ Pas de maintenance
- ✓ Mise à disposition des fonctions
  - ✓ Exec
  - ✓ System

## Conséquence

- Autre manière de prise en main du système
- Serveur Zombie
-

# Injection SQL

## Principe de l'attaque

- ✓ Envoie du code SQL
  - ✓ Formulaire
  - ✓ GET / POST
  - ✓ Cookies
  - ✓ ...

## Conséquence

- ✓ Contournement authentification
- ✓ Récupération des données de la base
- ✓ Récupération de fichiers
- ✓ Exécution de codes

# Contrôle d'accès au niveau fonctionnel

## Principe de l'attaque

- ✓ Accéder à des pages non autorisés
- ✓ Modifier les droits
- ✓ XSS

## Conséquence

- ✓ Prise de contrôle du site
- ✓ Générer des actions non autorisés

# Exposition de données sensibles

## Principe de l'attaque

- ✓ Trouver
  - ✓ des données stockés / archivés en clair
  - ✓ Espace privée non partagée
  - ✓ Communication avec la banque
- ✓ Déterminer les algorithmes de cryptage faible

## Conséquence

- ✓ Cible principale
  - ✓ Mot de passe
  - ✓ Données sensibles non chiffrées
  - ✓ Carte bleu

# Conception non sécurisée

## Principe de l'attaque

- ✓ Validation des données
- ✓ Absence de contrôle
- ✓ Niveau contrôle faible

## Conséquence

- ✓ Sécurité effectuée à la fin du projet
- ✓ Copier / coller

# Mauvaise configuration de sécurité

## Principe de l'attaque

- ✓ Manque de sécurité élevé
- ✓ Présence d'erreur dans la pile
- ✓ Nettoyage faible
- ✓ Librairie ou logiciel obsolète

## Conséquence

- ✓ Listé le contenu d'un dossier
- ✓ Exposition des données sensibles
- ✓ Attaque par les entêtes
- ✓

# Composants vulnérables et obsolètes

## Principe de l'attaque

- ✓ Recherche des versions utilisées
- ✓ API non à jour
- ✓

## Conséquence

- ✓ Les librairies utilisées (JS)
- ✓

# Identification et authentification faible

## Principe de l'attaque

- ✓ Suivi des utilisateurs par SESSION ID
- ✓ Caractéristiques utilisateur stockées côté serveur par une variable de session
- ✓ Gestion des états : Cookies / Get / Post
- ✓ Chiffrement faible

## Conséquence

- ✓ Vol des données SESSION\_ID si elles ne sont pas cryptées
- ✓ Utilisation ailleurs

# Manque d'intégrité des données et du logiciel

## Principe de l'attaque

- ✓ Falsification de requêtes (CSRF)
- ✓ Modification du contenu d'une page
- ✓ But éviter de passer par le formulaire
- ✓ Token ou jeton de sécurité

## Conséquence

- ✓ Conduire l'utilisateur vers un site malveillant
- ✓ Lui forcer la main
  - ✓ Ex : download

# Carence des systèmes de contrôle et journalisation

## Principe de l'attaque

- ✓ Trouver
  - ✓ des données stockés / archivés en clair
  - ✓ Espace privée non partagée
  - ✓ Communication avec la banque
- ✓ Déterminer les algorithmes de cryptage faible
- ✓ Les logs sont disponibles

## Conséquence

- ✓ Voir les données en clair

# Falsification de requêtes côté serveur (SSRF)

## Principe de l'attaque

- ✓ Récupération de valeurs distance par une API
  - ✓ sans validation URL
- ✓ Absence de SSL, VPN, ACL
- ✓

## Conséquence

- ✓ Attaque Oauth
- ✓ WebServices

# En résumé

- Tous les détails
  - OWASP TOP 10
    - <https://owasp.org/Top10/fr/>
  - CWE
    - 2017 : top 10
      - <https://cwe.mitre.org/data/definitions/1026.html>
    - 2021 : Top 25
      - [https://cwe.mitre.org/top25/archive/2021/2021\\_cwe\\_top25.html](https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html)

# Correction TP 1 : Des idées supplémentaires ?





- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

# Détails

A (RE) Lire

Image / logo

identifiant

Mot de passe

Reset

Valider

Ajout  
Compte

Message :

Vous êtes  
connecté

Message :

Erreur.  
Recommencé

1 formulaire avec :

- 1 logo
- 1 champ identifiant
- 1 champ mot de passe
- 3 boutons
  - . Reset : Remise à zero des champs
  - . Ok : Message ok ou error
  - . Ajout compte : possibilité d'ajouter un identifiant en plus

## Réalisation Technique

- Tous langages (PHP, Python, JS, HTML,...)
- Framework / CMS : Tous
- Base de données (NoSQL, SQL, aucune...)

## Aucunes contraintes

## Dans le README.md

- écrire les informations techniques
- comment utiliser
- Identifiant/mot de passe si nécessaire

# Erreurs identifiés

- Absence d'image et/ou Base de données
- Mauvais dépôt
- Absence de fichier « index »
- Accents dans la base de données
- HS : Qualité de code (A revoir)



# Cacher le contenu des dossiers

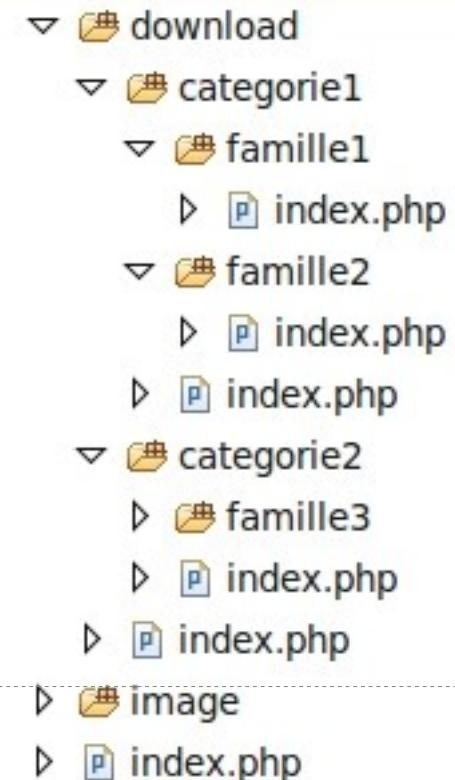
- Ex : `http://votreURL.com/nomDossier`

- Solution : fichier `index.php`

```
<?php  
header("Location: ../index.php");  
die();  
?>
```

- Autre solution :

- `Index.html`
- `URL Rewriting`
- `Fichier .htaccess`



# Pour se protéger des fichiers malicieux

- <?php Include (\$file) ; ?>
  - Ex : <http://votreURL.com/file=toto.php>
- Solution
  - <http://votreURL.com/toto.php>
- Ecraser le contenu de la variable
  - <http://urlPirate.com/hack.gif>
- Solution dans php.ini
  - `allow_url_fopen = off`

# Protection de base

- Verrouillez les dossiers
  - .htaccess
  - Chmod (444) ou 665 ou 775
- HTTPS / SSL

# Utilisation du SQL (1/3)

- Risque : Requête avec des simples quotes

```
SELECT * FROM 'users' WHERE 'username'='$login' AND 'password'='$pass'
```

- Saisie : \$login = hello \$pass = hello

```
SELECT * FROM 'users' WHERE 'username'='hello' AND 'password'='hello'
```

**TRUE**

# Utilisation du SQL (2/3)

- Risque : Requête avec des simples quotes

```
SELECT * FROM 'users' WHERE 'username'='$login' AND 'password'='$pass'
```

- Saisie : \$login = ' OR '1'='1' \$pass = ' OR '1'='1'

```
SELECT * FROM 'users'
```

```
WHERE 'username'=" OR '1'='1" AND 'password'=" OR '1'='1"
```

**TRUE**

# Utilisation du SQL (3/3)

- Risque : Requête avec des simples quotes

```
SELECT * FROM 'users' WHERE 'username'='$login' AND 'password'='$pass'
```

- Saisie : \$login = ' OR 1=1"); drop table users; \$pass =

```
SELECT * FROM 'users' WHERE 'username'=' OR 1=1"); drop table users;'  
AND 'password'='
```

**TRUE**  
*Sauf si BDD  
lecture*

# Se protéger contre injection SQL

- `addslashes()`

- Ajoute des *antislashes* dans une chaîne

*SELECT \* FROM 'users'*

*WHERE 'username'=' \' OR \'1\'='1\' '*

*AND 'password'=' \' OR \'1\'='1' '*

*mysqli\_real\_escape\_string()*

- Protège les caractères spéciaux
- `pdo_quote()`
  - Place des guillemets simples autour d'une chaîne entrée

les guillemets simples '  
les guillemets doubles  
"

les slashes /  
les caractères NULL

# Gestion des données entrées

## Principe de l'attaque

- ✓ Suivi des utilisateurs par SESSION ID
- ✓ Caractéristiques utilisateur stockées côté serveur par une variable de session
- ✓ Gestion des états : Cookies / Get / Post
- ✓ Chiffrement faible

## Conséquence

- ✓ Vol des données SESSION\_ID si elles ne sont pas cryptées
- ✓ Utilisation ailleurs

# Solution de contrôle (1/3)

- Prévoir la présence d'une clef de hashage caché (type honeypot)
  - Générer une clef cryptée de hachage
    - IP
    - Navigateur utilisé
    - Une durée de validité
    - ...
  - Différencier les formulaires
  - Eviter la protection en MD5 pour HASH

# Solution de contrôle (2/3)

- Remède contre Session ID
  - Cryptage par HASH
  - Eviter le MD5 avec la date de connexion
  - Contenu aléatoire
- Oublier les champs Hidden avec des caractéristiques utilisateur

# Solution de contrôle (3/3)

- Lors de l'envoie d'un formulaire, quelques bases
  - If `isset($_POST['string']) { /* ... */ }`
  - If `sizeof($_POST['string'])>0 { /* ... */ }`
- Attention aux superglobales  
`$_GLOBALS, $_SERVER, $_GET, $_POST, $_FILES, $_SESSION, $_REQUEST, $_ENV`
  - `$str=htmlentities($_COOKIE['string'],ENT_QUOTES);`

# La navigation en mode tranquille

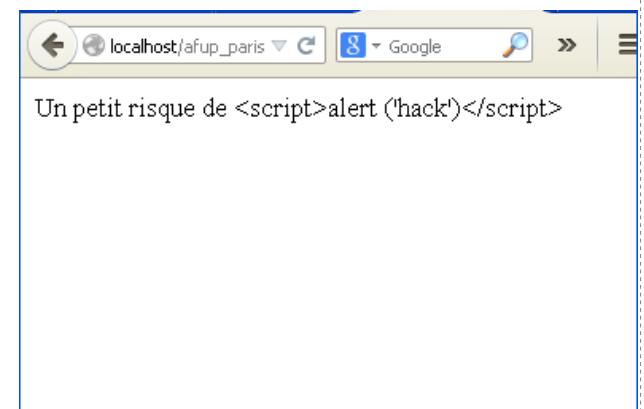
- Absence de protection

```
<?php  
echo "Un petit risque de  
<script>alert ('hack')</script>";  
?>
```



- Avec une protection

```
<?php  
echo htmlentities("Un petit risque de  
<script>alert ('hack')</script>");  
?>
```



# Solution contrôle d'accès

- Exemple
  - <http://urlSite.com/getpage>
  - http://urlSite.com/admin\_getpage
- Solutions
  - Vérifier le contrôle d'accès (principe identification)
  - Vérifier les URLs

# Expositions de données sensibles

- Identifiant de connexion
  - A la base de données dans les fichiers
- Mode Debug **TRUE**

# Imposer un comportement

- Créer un token ou un jeton de sécurité (toutes les pages)

## Passage 1

```

<?php
session_start();
$token = uniqid(rand(), true);      // jeton unique
$_SESSION['token'] = $token;        // stockage

// heure de création du jeton
$_SESSION['token_time'] = time();
?>
<html><body>
<form id="form" name="form" method="post"
action="traitement.php">
...
<input type="hidden" name="token"
id="token" value="<?php echo $token;?>"/>
...
</form>
</body></html>

```

## Passage 2 : traitement.php

```

<?php
session_start();
if(isset($_SESSION['token'])
  && isset($_SESSION['token_time'])
  && isset($_POST['token']))
{
  //Si jeton session = au formulaire
  if($_SESSION['token'] ==
    $_POST['token'])
  {
    // exécution du code
  }
}
// sinon erreur
?>

```

# Manipulation d'objets sensibles

```
class car [  
    public string color;  
}
```

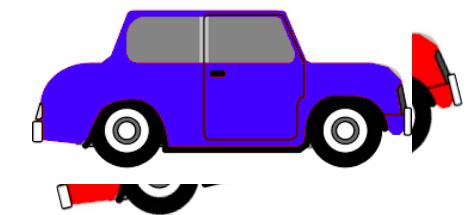
*Processus de  
sérialisation*

```
var redCarObj =new car();  
redCarObj.color = 'rouge';
```



redCarObj sérialisé

*processus de  
désérialisation*



redCarObj

Plus....

- Contrôle en direct

## En résumé

- Utilisez des outils disponibles pour valider son code :
  - LGTM
    - <https://lgtm.com>
  - Exakat (pour PHP)
    - <https://www.exakat.io>
  - Sonar
    - <https://www.sonarqube.org>
  - Mozilla Observatory
    - <https://observatory.mozilla.org/>
  - ...



- Détections vulnérabilités
- Correction TP 1
- Les enjeux de la sécurité
- Besoins de sécurité
- Notions des vulnérabilités
- Panorama des menaces
- Les règles en France

# Préambule

## Système d'Information (S.I.)

- Ensemble des ressources destinées à
  - **Collecter**
  - **Classifier**
  - **Stocker**
  - **Gérer,**
  - **Diffuser les informations**

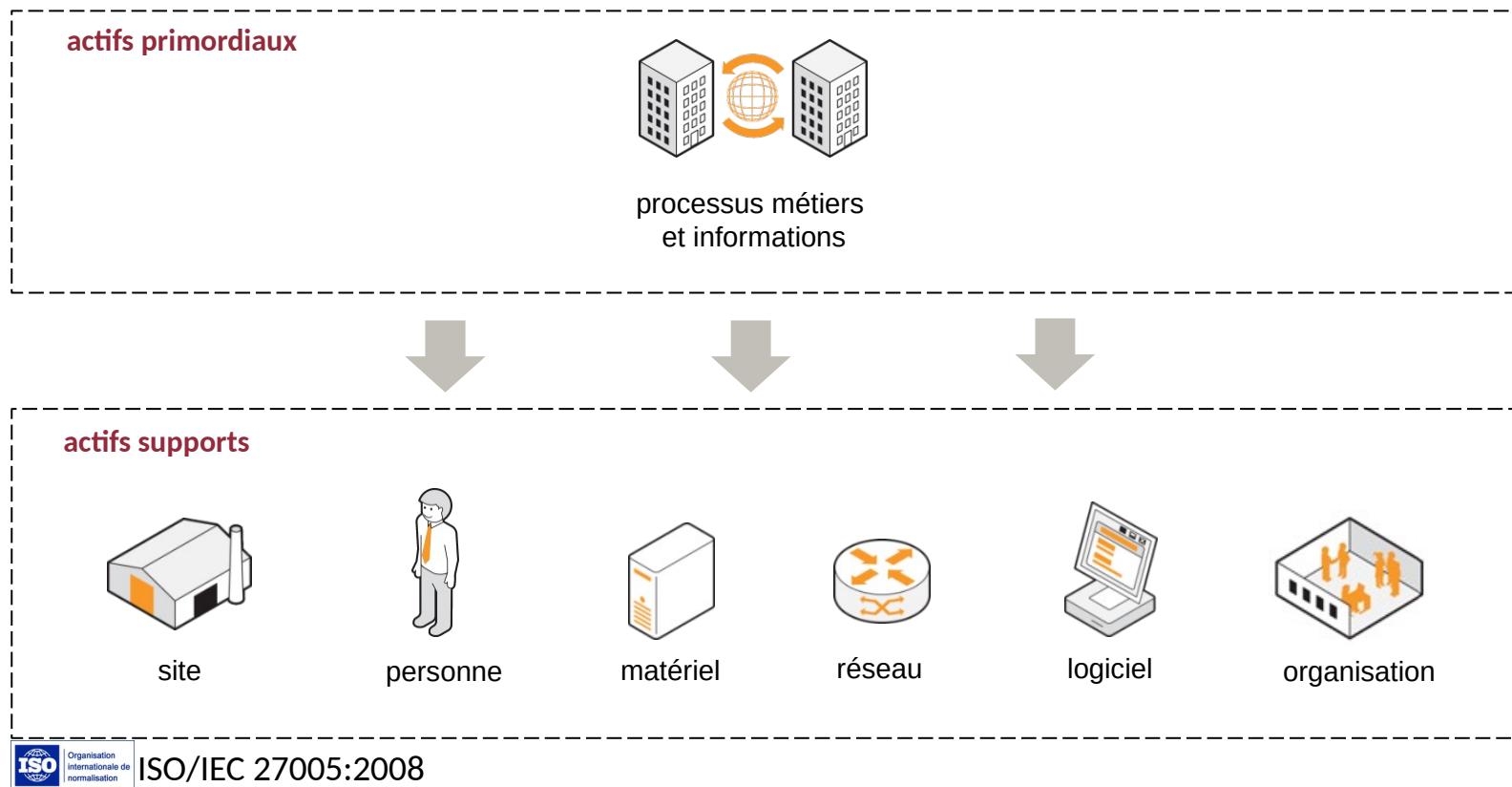
Au sein d'une organisation

- c'est le « nerf de la guerre »
- pour
  - Les entreprises,
  - Les administrations,
  - Les organisations,
  - etc.

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

# Organisation

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



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

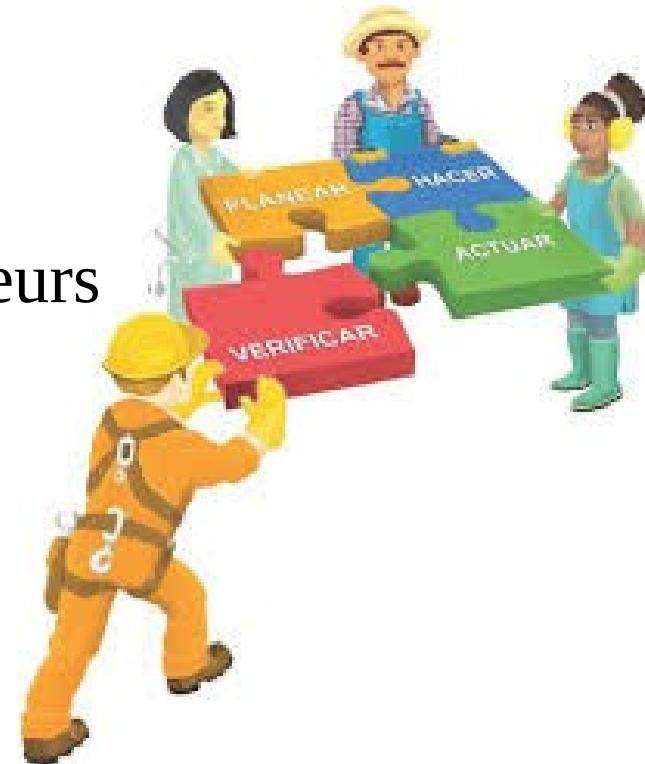
# Les enjeux (1/

- La sécurité a pour objectif
  - Réduire les risques
    - pesant sur le système d'information,
  - Limiter leurs impacts
    - sur le fonctionnement
    - les activités métiers des organisations...



## Les enjeux (2/

- 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
    - A 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



# Les impacts dans les enjeux



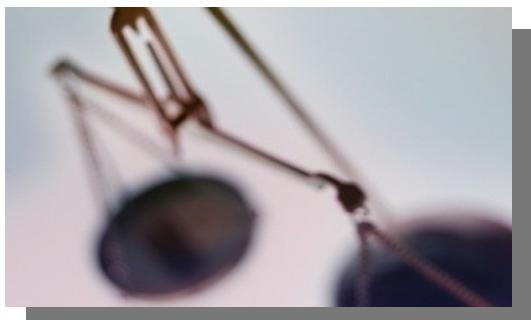
Impacts financiers



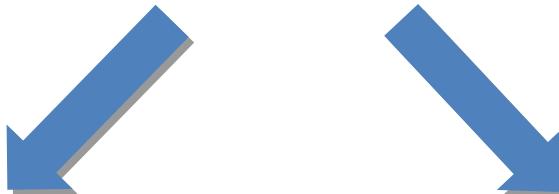
Impacts sur l'image  
et la réputation



Sécurité  
des S.I.



Impacts juridiques  
et réglementaires



Impacts  
organisationnels

# Vision des pirates

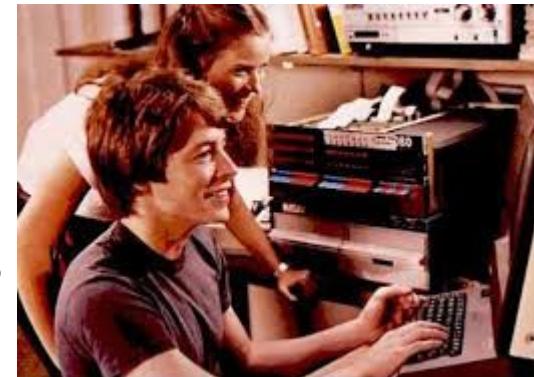


Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?



# Historiques des motivations

- Années 80 et 90
  - beaucoup de bidouilleurs enthousiastes



De nos jours :  
- Majoritairement  
des actions organisées  
et réfléchies

[https://fr.wikipedia.org/wiki/Les\\_Pirates\\_de\\_la\\_Silicon\\_Valley](https://fr.wikipedia.org/wiki/Les_Pirates_de_la_Silicon_Valley)

# TOP 8 des hackers les plus célèbres (1/2)

- **1983 Kevin Poulsen**
  - TRS-80 qu'il va s'introduire dans le réseau ARPAnet de l'Université de Californie
- **1988 Robert Tappan Morris**
  - écrit et lance Morris, un ver informatique
- **Adrian Lamo**
  - introduit plusieurs réseaux informatiques comme Microsoft, Yahoo! et New York Times
- **Steve Jobs et Steve Wozniak**
  - fabriquant des Blue Box qu'ils ont réussi à court-circuiter les standards téléphoniques

# TOP 8 des hackers les plus célèbres (2/2)

- **1987 Kevin Mitnick**
  - A réussi à accéder à la base de données des clients de Pacific Bell
  - Numéro de cartes de crédits téléphoniques
- **2001 Gary McKinnon**
  - accusé d'avoir infiltré 97 ordinateurs appartenant à l'US Army et à la NASA
- **1994 Vladimir Levin**
  - tenté de transférer 10 millions de dollars sur différents comptes à l'étranger
- **1992 Julian Assange**
  - publié pas moins de 77 000 documents confidentiels de l'armée américaine sur la guerre en Afghanistan

# Cyber délinquance

- Les individus attirés
  - 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
  - ...



# Quel but ?

- Gains financiers

47.89	+7.9%	543.23	500,000
45.34	+5.34%	254.23	120,000
17.34	-7.89%	321.56	320,000
34.89	+5.97%	100.08	430,000
34.89	+2.13%	564.23	900,000
16.45	+6.43%	765.90	600,000
23.67	-11.6%	120.34	380,000
34.64	+23.1%	893.23	120,000
43.69	+5.56%	128.98	320,000
43.69	-3.67%	432.12	750,000
12.78	+11.3%	765.23	150,000
12.78	+11.3%	432.24	120,000

- Utilisation de ressources



- Chantage



- Espionnage



# Quel but ? (1/4)

- Gains financiers
- Utilisations de ressources
- Chantage
- Espionnage

## 3 étapes :

- Accès à l'information
  - Monétisation
  - Vente
- Cible :
    - Utilisateurs, emails
    - Organisation interne de l'entreprise
    - Fichiers clients
    - Mots de passe,
    - N° de comptes bancaire
    - Cartes bancaires

# Quel but ? (2/4)

➤ Gains financiers

➤ Utilisation de ressources

➤ Chantage

➤ Espionnage

- Etapes :
  - Revente
  - Mise à disposition en tant que « service »
- Services :
  - Bande passante
  - Espace de stockage
    - hébergement
      - MP3, films...
    - Zombies (botnets)

# Quel but ? (3/4)

- Gains financiers
- Utilisations de ressources
- Chantage
- Espionnage

- Déni de service
- Modifications des données

# Quel but ? (4/4)

- Gains financiers
- Utilisations de ressources
- Chantage
- Espionnage

- Industriel / concurrentiel
- Étatique

# Actes de délinquance

- Majorité des actes de délinquance réalisés
  - sur Internet sont commis par :
    - Des groupes criminels organisés
    - Des professionnels
    - Impliquant de nombreux acteurs

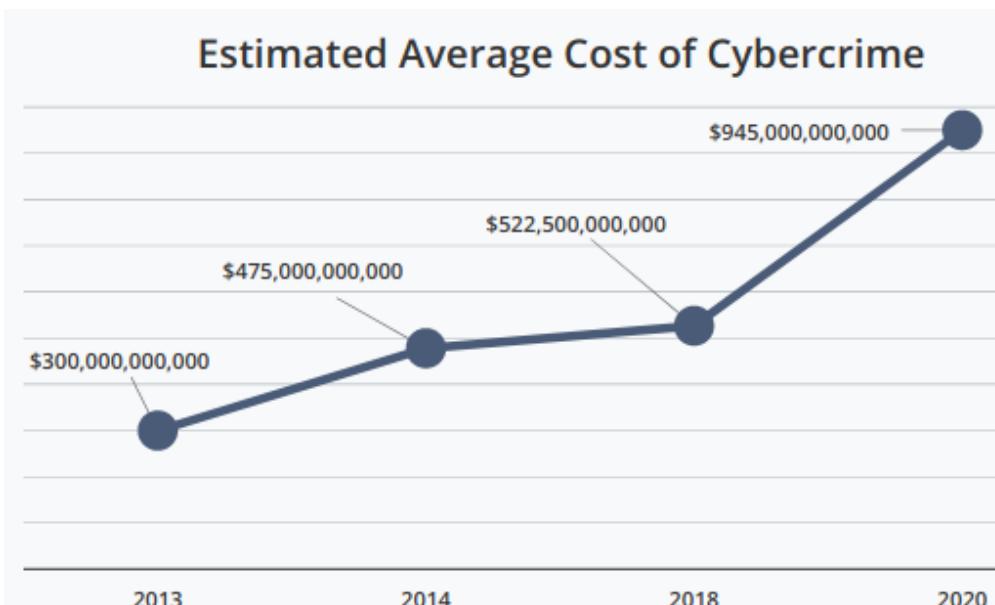


# Structure des groupes de délinquance

- 1 → Des groupes spécialisés
  - dans le développement de programmes malveillants et virus informatiques
- 2 → Des groupes en charge de l'exploitation
  - et de la commercialisation de services permettant de réaliser des attaques informatiques
- 3 → Un ou plusieurs hébergeurs
  - stockent les contenus malveillants,
    - soit des hébergeurs malhonnêtes
    - soit des hébergeurs victimes eux-mêmes d'une attaque
      - 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

# Quelques chiffres (2015)

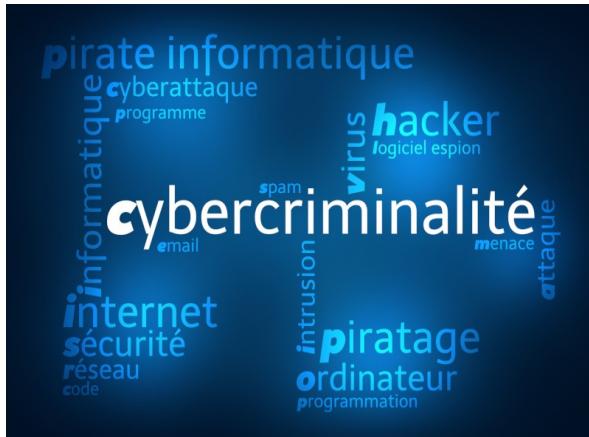
- Prix moyen des numéros de cartes bancaires
  - en fonction du pays et des plafonds **de 2 à 10 \$**
- Tarif moyen de location pour 1 heure d'un botnet, **5 \$** système permettant de saturer un site internet
- Prix de commercialisation du malware **2.399 \$**
  - permettant d'intercepter des numéros de carte bancaire



<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>

# Les impacts sur la vie privée

- Les Impacts



- Usurpation d'identité



- Perte définitive de données



- Impacts financiers



# Alors... Ce qu'on vient de voir



ne signifient pas qu'il  
ne faut pas utiliser  
Internet, loin de là !



Il faut :

- Apprendre à anticiper ces risques
- Faire preuve de discernement lors de l'usage d'Internet / smartphones

# Les impacts sur la vie privée (1/4)

## ➤ Les impacts

➤ Usurpation d'identité

➤ Perte définitive de données

➤ Impacts financiers

- Impact
  - sur l'image
  - le caractère
  - la vie privée
- Diffamation de caractère
- Divulgation d'informations personnelles
- Harcèlement cyber-bullying

# Les impacts sur la vie privée (2/4)

## ➤ Les impacts

### Usurpation d'identité

### ➤ Perte définitive de données

### ➤ Impacts financiers

- « Vol »
- Réutilisation de
  - Logins
  - Mots de passe
- But :
  - Effectuer des actions au nom de la victime

# Les impacts sur la vie privée (3/4)

## ➤ Les impacts

### ➤ Usurpation d'identité

### ➤ Perte définitive de données

### ➤ Impacts financiers

- Malware récents (rançongiciel) :
  - données chiffrées contre rançon
- Connexion frauduleuse à un compte « cloud »
- Suppression malveillante de l'ensemble des données

# Les impacts sur la vie privée (4/4)

## ➤ Les impacts

### ➤ Usurpation d'identité

### ➤ Perte définitive de données

### ➤ Impacts financiers

- N° carte bancaire usurpé
  - Réutilisé pour des achats en ligne
- Chantage
  - Divulgation
    - de photos
    - d'informations compromettantes
  - si non paiement d'une rançon

# Les impacts sur les infrastructures critiques

- Infrastructures critiques
  - Ensemble d'organisations parmi les secteurs d'activité listés
- L'État français considère
  - 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.



# Classement

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



# Exemples d'attaques



## Copé, Hortefeux, Dassault... leurs messageries Orange piratées

par Emilien Ercolani, le 07 mai 2013 15:04 ★★★★★

Les messageries des téléphones portables de plusieurs personnalités politiques (JF Copé, B Hortefeux) ou industrielles (la famille Dassault) ont été piratées plusieurs semaines durant. Des plaintes ont été déposées, alors qu'Orange a lancé une enquête interne.

Publié le 13 avril 2014 à 12h24 | Mis à jour le 13 avril 2014 à 12h24

## Le centre allemand de recherche spatiale cible d'une cyberattaque

Agence France-Presse

Le centre allemand de recherche aéronautique et spatiale (DLR) a été la cible il y a quelques mois d'une cyberattaque présumée par un service de renseignements étranger, affirme le magazine *Der Spiegel* dimanche.



[Derniers articles](#) | [Archives](#) | [Recherche](#)

Actualités > Société

## Une panne réseau a cloué au sol les avions d'American Airlines

Près de 670 vols ont été annulés hier, en raison d'un problème d'accès au système de réservation. La compagnie s'est appuyée sur les réseaux sociaux pour informer ses clients.



Gilbert Kallenborn, avec AFP | 01net | le 17/04/13 à 11h23 | [laisser un avis](#)

[Tweet](#) +1 5

## Panne informatique à l'hôpital de

En l'espace de deux jours, mercredi et jeudi, l'accueil aux urgences de a été très perturbé. Il a fallu diriger les patients vers d'autres hôpitaux.

Publié le 10.01.2009

## Ukraine : le mystérieux virus Snake infecte les ordinateurs du gouvernement

Publié le 08.03.2014, 16h50 | Mise à jour : 17h23

[Recommander](#) 52 personnes le recommandent. [Inscription pour ce que vos amis recommandent.](#) [Tweeter](#) 64 [G+1](#) [Share](#)



Illustration. Un mystérieux virus a été réactivé ces derniers jours et vise les ordinateurs ukrainiens. | LP/ Olivier Arandel



# Exemples d'attaques



## Bug informatique à La Poste : "Tout est rentré dans l'ordre"



par Caroline Piquet

le 30 juillet 2013 à 15h50, mis à jour le 30 juillet 2013 à 18h59.

**A la suite d'une panne informatique, les opérations de prélèvements et de virements bancaires accusent un retard de 24 heures. Ce mardi, les clients ne pouvaient accéder à leurs soldes sur Internet et il leur était impossible de retirer de l'argent aux distributeurs automatiques.**

## Hacker un pacemaker, c'est possible et c'est dangereux

10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info



Zoom

## Une panne informatique paralyse Wall Street pendant 3 heures

Édité par MYTF1News avec AFP  
le 23 août 2013 à 06h50, mis à jour le 23 août 2013 à 07h02.

Help! My fridge is full of spam and so is my router, set-top box and console  
Security company says it discovered spam and phishing campaign run over Christmas, which involved internet fridge

Charles Arthur  
[Follow @charlesarthur](#) [Follow @guardiantech](#)  
theguardian.com, Tuesday 21 January 2014 11.40 GMT  
[Jump to comments \(19\)](#)



## Gibraltar: un incendie interrompt des services de paris en ligne

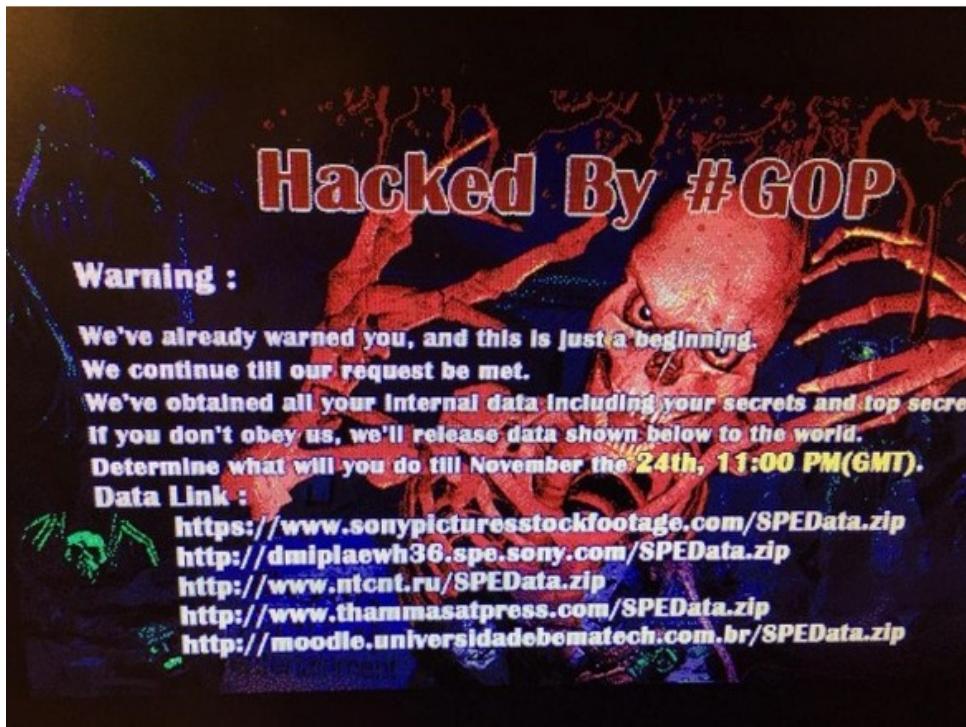
AFP, 20/04 23:31 CET



## Un avion espion « plante » le système informatique d'un aéroport

Par Pierre Dandumont 5 MAI 2014 12:30 - Source: NBC News | 0 COMMENTAIRE

# Exemple : Sony Pictures Entertainment



- GOP pour Guardian of Peace
- Des données internes ont été publiées contenant :
  - les numéros de sécurité sociale et les numérisations de passeport appartenant aux acteurs et directeurs.
  - des mots de passe internes
  - des scripts non publiés
  - des plans marketing
  - des données légales et financières
  - et 4 films entiers inédits
- La probabilité de vol d'identité est très forte désormais pour les personnes dont les informations ont été publiées.
- Les studios concurrents de Sony, ont une visibilité sur les plans stratégiques de Sony.

« Si vous n'obéissez pas, nous publierons au monde les informations suivantes ». Ce message était affiché sur plusieurs ordinateurs de Sony Pictures Entertainment le 24 nov 2014

**La source de l'attaque reste à déterminer.  
La Corée du Nord est soupçonnée d'être à l'origine de l'attaque.**

<http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html>

# Exemple : vol de données

- En 2018
  - 10 – Sacramento Bee : fuite de données de 19,5 millions de personnes
  - 9 – Ticketfly : fuite de données de 27 millions de personnes
  - 8 – Panera Bread, fuite de données de 37 millions de personnes
  - 7 – Facebook : fuite de données de plus de 200 millions de personnes
  - 6 – MyHeritage : fuite de données de 92 millions de personnes
  - 5 – Quora : fuite de données de 100 millions de personnes
  - 4 – Under Armour : fuite de données de 150 millions de personnes
  - 3 – Exactis : fuite de données de 340 millions de personnes
  - 2 – Marriott : fuite de données de 500 millions de personnes
  - 1 – Aadhaar : fuite de données de 1,1 milliard de personnes

<https://www.lebigdata.fr/fuites-de-donnees-2018-top>

# Fuites de données des utilisateurs

- Yahoo en août 2013
  - 3 milliards de comptes attaqués
- Alibaba en novembre 2019
  - 1.1 milliard de données volées
- LinkedIn en juin 2021
  - 700 millions d'utilisateurs touchés
- Facebook en avril 2019
  - 533 millions d'utilisateurs attaqués
- Adult Friend Finder en octobre 2016
  - 412,2 millions de comptes atteints

<https://www.lebigdata.fr/top-5-fuites-donnees-dutilisateurs>

# Quelques exemples d'attaques ciblant l'enseignement



## Espace étudiants

Ce Forum est un espace ouvert de communication entre étudiants, tuteurs, moniteurs et enseignants pour discuter des cours, des exercices, des travaux pratiques.

> Poster un nouveau message <

Liste des messages postés  
pages 1 2 3 4 5 6 7 8 9 10

# HACKED BY SWAN HACKED BY SWAN  
HACKED BY SWAN HACKED BY SWAN  
HACKED BY SWAN HACKED BY SWAN

## Défacement de site

### Vol de données personnelles

## TheWMURChannel.com

### Dartmouth Computer Hackers

POSTED: 4:07 PM EDT August 1, 2004

**HANOVER, NH** -- Hackers hit the computer system at Dartmouth College last week and got access to sensitive information about thousands of employees and students.

Larry Levine, Dartmouth's chief information officer, said he did not know for sure what the hackers' purpose was. He said one of the compromised computer servers contained information on college employees, retired employees and their families. Other servers involved contained research data and staff and student immunization information.

# Quelques exemples d'attaques ciblant l'enseignement

## Click2Houston.com

### Police: Student Installs Device On Teacher's Computer To Sell Tests

#### **Warnings Sent To Other School Districts**

POSTED: 5:23 pm CST February 1, 2005

UPDATED: 5:39 pm CST February 1, 2005

**HOUSTON** -- A high school student is facing criminal charges for allegedly hooking a device up to a teacher's computer to steal test information to sell to other students, Local 2 reported Tuesday.

The student attended [Clements High School](#), 4200 Elkins Dr., in the [Fort Bend Independent School District](#).

Officials said the 16-year-old boy hooked up a keystroke decoder to a teacher's computer and downloaded exams in November.

"Sometime in mid-December, we got a tip that this student was selling test exams that had apparently come from a teacher's computer, so that's when the investigation began," said Mary Ann Simpson, with the Fort Bend School District.

The student confessed when he was confronted, officials said.

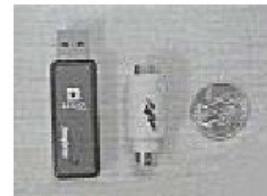
Note des lecteurs: **5.0/5**

**Exclusif : Tentative de fraude bancaire via le site de l'Union française des Professeurs de Physique et de Chimie.**

Un pirate informatique, spécialisé dans la fraude bancaire et l'[hameçonnage](#) a décidé de s'attaquer aux clients de la banque en ligne EGG. Pour ce faire, l'escroc a été installer son piège directement dans le site de l'Union des Professeurs de Physique et de Chimie (udppc.asso.fr). A première vue, eux aussi auront droit à des devoirs de vacances pour bien protéger leur site Internet. (iago)

**Vol de données professionnelles**

#### Video



[See How Keystroke Decoder Works](#)

**Rebond pour fraude externe**

# Attaques de locomotions

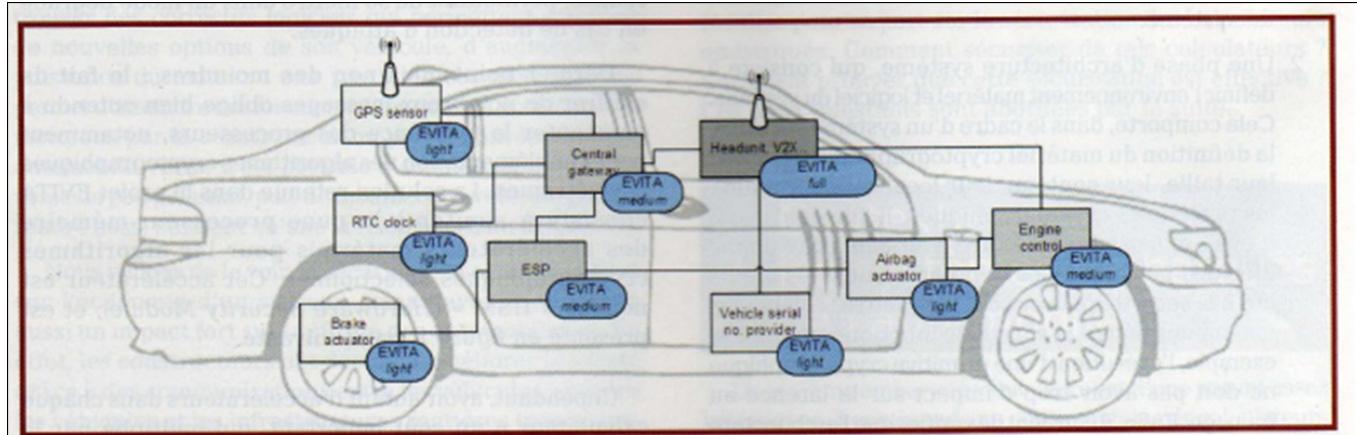
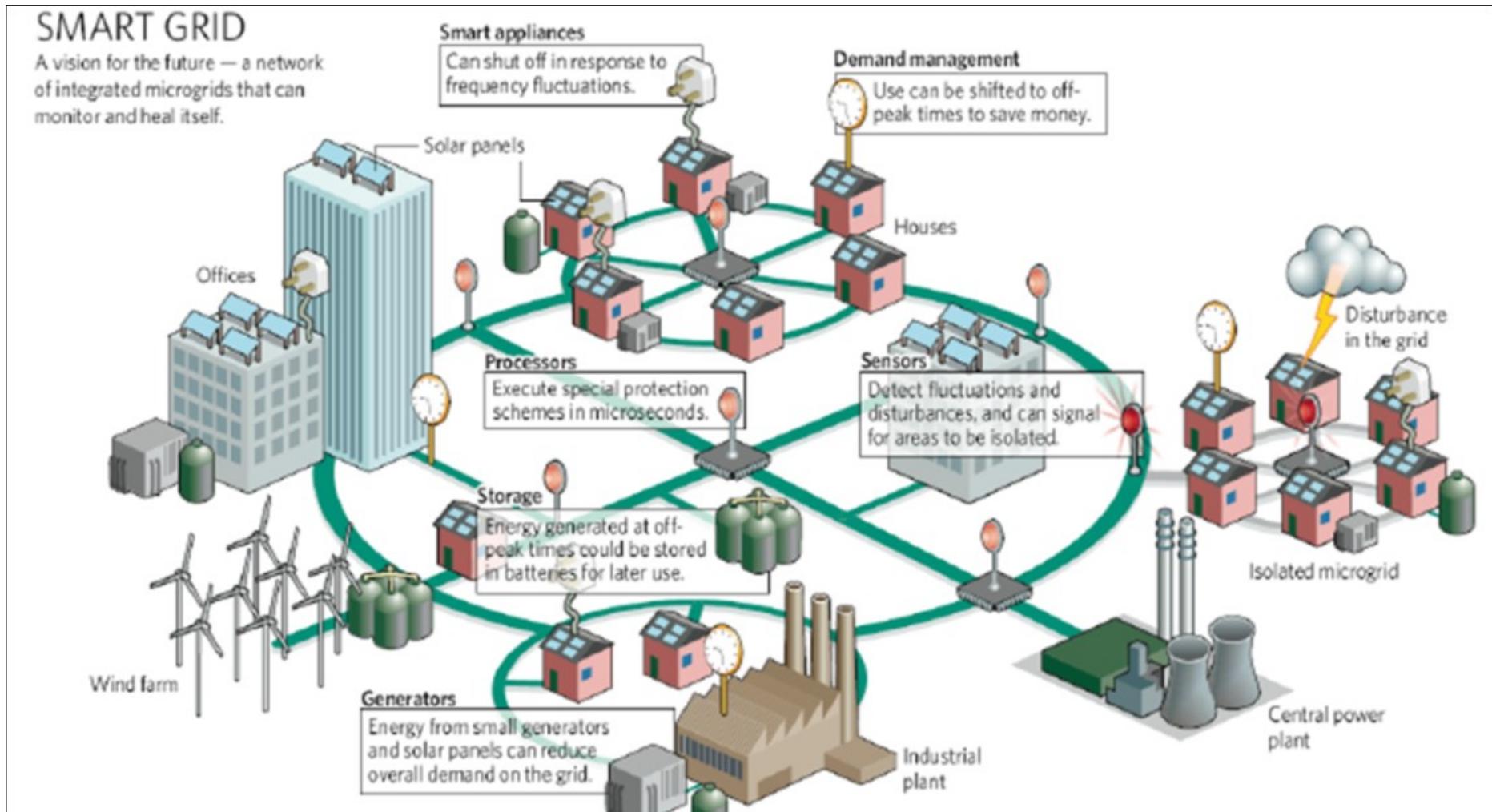


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout calculateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

Cyberattaques sur la voiture connectée envisagées  
Exemple : Prise de contrôle du système de frein

# Attaques CRE

## CRE : Réseaux intelligents



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

# Attaques sur les points de ventes

- Borne tactile dans un point de vente
  - Accélération récente de la digitalisation des commerces et services
- Un support pour augmenter les ventes
- Gagnez en rentabilité tout en maîtrisant vos coûts opérationnel
- Mais...



<https://www.zataz.com/pourquoi-installer-une-borne-tactile-dans-son-point-de-vente/>

# A retenir

- La sécurité de demain est
  - un enjeu important
    - qui doit commencer dès maintenant



**EXERCICE**

# La suite de la Session 2 ???

- La suite de cette partie
  - Rendez vous la semaine prochaine



## Exercice de Rattrapage

- A partir de l'exercice 1 :
  - Corrigé le formulaire d'identification sécurisé
    - Avec les informations vues aujourd'hui
    - Mettre à jour le dépôt GitHub
  - Notation :
    - Vous pouvez signaler la mise à jour du dépôt pour **refaire** noter l'exercice et obtenir une nouvelle note (ou meilleure note)
    - Si vous demandez pas une nouvelle notation, il n'y aura aucun impact dans la note déjà attribuée
- Deadline
  - Le 15 février 2023 23:59

# Rendez-vous au prochain cours

- Merci de votre attention

