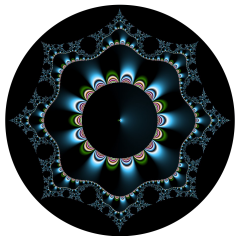
Sécurité des applications

Introduction

Thibaut et Corinne HENIN



www.arsouyes.org
@arsouyes

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Question 1

Bug = ?

Question 2

Vulnérabilité = ?

Sécurité

Triptyque sacré

Biens, Confidentialité, intégrité, disponibilité

Bien

- *Ressource qui doit être protégée*

- Exemples :
    - *Donnée*
    - *Fonctionnalité*
    - *…*

Confidentialité

- ***Confidentialité :***
    - *La ressource n’est accessible qu’à ceux qui y sont autorisés*

Intégrité

- ***Intégrité :***
  - *La ressource n'est modifiée que par des actions légitimes*

- ***Authenticité :***
  - *Idem en cryptographie*

Disponibilité

- ***Disponibilité :***
    - *La ressource est accessible lorsque l'utilisateur en as besoin*

D’autres définitions

Identification *vs.* Authentification

- **Identification :** dire qui on est
    - *E.g. fournir un pseudonyme à un formulaire*

- **Authentification :** prouver qui l'on est
    - *E.g. fournir le mot de passe correspondant*

Traçabilité

- ***Traçabilité :***
    - *Capacité à retrouver qui a fait quoi quand*
- ***Non Répudiation :***
    - *Idem en cryptographie, notion de preuve de la trace*
- ***Déni plausible :***
    - *Impossibilité de pouvoir retrouver et/ou prouver une trace*

La politique de sécurité

Et l’analyse des risques

But

« Plan d'actions définies pour maintenir un certain niveau de sécurité »

Source: wikipedia

PSSI 1/4

- Identifier les biens à protéger
    - Fonctionnalités,
    - Données utilisateur,
    - Données de l’application,
    - Code source, code machine de l’application,
    - …

PSSI 2/4

- Lister les propriétés de sécurité souhaitées
    - Confidentialité,
    - Intégrité,
    - Disponibilité
    - Traçabilité,
    - …

PSSI 3/4

- Lister les risques
    - Des événements *et leur vraisemblance*
    - Des conséquences *et leur gravité*
- *Méthodes :*
    - *Mehari, Ebios, …*

PSSI 4/4

- Lister les moyens pour couvrir les risques
    - Authentification,
    - Contrôle d’accès,
    - Cryptographie,
    - Obfuscation,
    - Qualité Logicielle,
    - …

Vulnérabilité

Définition

Gestion des risques

- **Point faible :**
    - « si je tape là, ça fait très mal »
- **Fragilité :**
    - « dois-je taper fort ? »

Informatique

- **Point faible :**
  - « si j’envoie plein de requêtes, le service ne répond plus »
- **Fragilité :**
  - « Est-ce facile à effectuer ? »
  - « Combien de paquets sont nécessaires ? »
- **Exploit :**
  - Programme qui utilise la vulnérabilité automatiquement

Criticité

Score CVSS - Common Vulnerability Scoring System

Somme de 6 métriques

Métriques d’exploitation

- Vecteur d’accès
- Complexité d’accès
- Authentification

Métriques d’impact

- Confidentialité
- Intégrité
- Disponibilité

Vecteur d’accès

- **Local**
  - *Accès physique ou un compte local*

0,395 pts

- **Réseau local**
  - *Accès réseau immédiat (couche 2)*

0,646 pts

- **Réseau**
  - *Accès via routage (couche 3 et +)*

1,000 pts

Complexité d’accès

- **Haute**
  - *Conditions très spécifiques pouvant être détectées*

0,350 pts

- **Moyenne**
  - *Conditions probables pouvant être rencontrées*

0,610 pts

- **Basse**
  - *Inconditionnelle*

1,000 pts

Confidentialité, Intégrité, Disponibilité

- **Aucune**
  - *Pas d'impact*

0,000 pts

- **Partielle**
  - *Impact modéré, partiel.*

0,275 pts

- **Complet**
  - *Perte totale de la propriété*

0,660 pts

Authentification

- **Multiple**
  - *Au moins deux authentifications sont nécessaires*

0,450 pts

- **Simple**
  - *Une authentification est nécessaire*

0,560 pts

- **Aucune**
  - *Libre accès*

1,000 pts

Publication

CVE - Common Vulnerability and Exposure

Registre des vulnérabilités

- **CVE :** Common Vulnerability and Exposure
  - Identifiant unique de vulnérabilité (CVE-AAAA-NNNN)
  - Description succincte
  - Liens « en savoir plus »

  - Edité par le MITRE :
    - https://www.mitre.org/
    - https://cve.mitre.org/

- **0day :**
  - vulnérabilité non publique (parfois : pas de correctif)

Full vs. No Disclosure

- **Full disclosure :**
    - Publier la vulnérabilité pour forcer les éditeurs à corriger
- **No Disclosure :**
    - Ne pas publier pour éviter une utilisation incontrôlée
- **Responsible Disclosure :**
    - Avertir l’éditeur, laisser un délai, puis publier

Et maintenant ?

Rapports de forces

Côté défense

- **Objectifs :**
    - Empêcher les contournements
    - Maintenir en condition opérationnelles
- **Risques :**
    - Image de marque
    - Dommages et intérêts

Côté attaque

- **Objectif :**
    - Trouver une vulnérabilité
    - Exploitable si possible
- **Gains :**
    - Image de marque
    - Primes et/ou valorisation

Dissymétrie

Côté attaque

- Pour gagner :
  - Suffit d’une erreur

Côté défense

- Pour ne pas perdre :
  - Tout doit être parfait

Quelle attitude ?

Autruche optimiste

- Ça marche, tout va bien
- On verra plus tard
- Qui voudrait nous attaquer ?

Perfectionniste paranoïaque

- Tout doit être parfait
- Une vulnérabilité est preuve d’incompétence
- Il reste toujours un risque

Humilité constructive

- Où sont les faiblesses
- Comment les corriger
- Amélioration continue

« Ce n’est pas parfait, mais on y travaille »

Objectif du cours

But

1. Sécurité pour les applications
2. Vulnérabilités dans les applications
3. Bonnes pratiques

Contenu du cours

1. Authentification et contrôle d’accès
2. Injections
3. Débordements
4. Gestion mémoire
5. Gestion des ressources
6. Cycle de développement