# Projet “Sécurité informatique”

**ou “The HE-Arc 2007 Security Challenge” ; – )**

## 1 Directives

Le projet sera réalisé en groupes de 3 ou 4 personnes. Il consistera en la réalisation d’un petit “Challenge” dans un domaine donné. Ce challenge sera soumis aux autres étudiants de la classe lors d’un cours.

Ce cours sera mené entièrement par les étudiants ayant conçu le challenge et se déroulera ainsi :

- Si nécessaire, petite introduction théorique par oral (max 15’)
- Distribution des documents décrivant le challenge et la manière de l’aborder
- Résolution du challenge par les autres étudiants, avec le soutien des concepteurs du challenge si nécessaire.

La résolution du challenge devra donc représenter 1h–1h15 de travail pour un étudiant moyen.

Quelques remarques :

- Si le sujet s’y prête, le challenge peut se présenter en partie comme une sorte de “tutorial”. Cependant, la résolution ne devrait pas pouvoir se faire simplement en suivant les instructions. Une participation active du “résolveur” est attendue.
- On peut imaginer un gros challenge, plusieurs petits challenges indépendants ou, plus amusant, un challenge “en chaîne” (la résolution du premier donne des indices pour le suivant, etc.)
- Si la réalisation du challenge nécessite un équipement spécial (machine dédiée, disque dur amovible, machine virtuelle, …), pensez à prendre contact assez tôt avec le professeur pour voir si cela est possible !

## 2 Sujets

La classe se partagera en 4 groupes qui se répartiront les 4 sujets suivant :

**Stéganographie** parmi des documents à l’air anodin se cachent des informations… comment les détecter ? comment les récupérer ?

**Débordements de tampon** comment détecter une faille, comment l’exploiter ?

**Injections SQL** comment récupérer des informations ou exécuter des actions non autorisées en “trafiquant” des requêtes SQL ?

**Crackme** les “crackmes” sont des petits programmes destinés à exercer les capacités d’ingénierie inverse. Confronté à un tel programme, comment retrouver un mot de passe, faire sauter une protection ?

Les sujets ci-dessous représentent le sujet principal du challenge… mais il n’est pas interdit de mélanger les genres si cela rend les choses plus intéressantes (stéganographie mélangée à un peu de cryptologie, injection SQL complétée de “crackage” de mots de passe, …)

## 3 Délivrables

À rendre par mail, à l'adresse `matthieu.amiguet@he-arc.ch` pour le **vendredi 11 mai 2007** au plus tard :

1. Les éléments constitutifs du challenge lui-même :
   - Code compilé du crackme/Documents stéganographiques/…
   - Documentation d'accompagnement destinée à être distribuée aux étudiants le jour du challenge
2. Un rapport sur l'élaboration du challenge
   - Brève présentation du sujet (1–2 page max.)
   - Techniques choisies, difficultés rencontrées
   - Codes sources, …
   - "Corrigé" du challenge

La partie 1. sera distribuée à vos collègues le jour du challenge, la partie 2. sera mise à disposition sur le serveur après le challenge.

## 4 Critères d'évaluation

| Critère | Coefficient |
|---|---|
| Maîtrise technique du sujet | 3 |
| Qualité des délivrables et de l'encadrement lors du challenge | 3 |
| Niveau de difficulté adéquat (ni trop difficile, ni trop facile ; temps de résolution adéquat ; intérêt du challenge ; …) | 2 |
| Originalité, engagement, quantité de travail, respect des consignes | 1 |

## 5 Calendrier

- semaine 14 : répartition des groupes et des sujets
- semaines 16–19 : préparation
- **vendredi 11 mai 2007** : date limite pour l'envoi des délivrables
- semaine 20 : Challenge "stéganographie"
- semaine 21 : Challenge "débordements de tampon"
- semaine 22 : Challenge "injections SQL"
- semaine 23 : Challenge "crackme"

## 6 Plagiat

Recopier des extraits significatifs de code, de texte, ou d'images sans le signaler clairement constitue du **plagiat** et sera considéré comme de la **tricherie**. Donc :

- De manière générale, n'oubliez pas de citer (toutes) vos sources !
- Recopier *une* phrase (ou *quelques lignes* de code) d'une source parce qu'elle est bien tournée est acceptable.
- Recopier un paragraphe entier est également acceptable, à condition que l'on *voie clairement* qu'il s'agit d'une citation et que la *source* soit *citée*.
- Rendre un rapport composé entièrement de couper-coller d'une ou deux sources *n'est pas acceptable* et constitue un cas de *tricherie*.

Le non respect de ces consignes pourra selon les cas réduire la note ou, dans les cas graves, résulter en un 1 de tricherie. Qu'on se le dise !

… Bonne préparation !