Organisation du Module d'Approfondissement « *Software Reverse Engineering and Protection* »

MSE HES-SO 2024-2025

Enseignant Le cours sera donné par Pascal Junod (modulo p SA).

Email: pascal+sre25@mod-p.ch
Site web: crypto.junod.info

Répartition des Heures de Cours

Type	**Nombre de périodes (heures)**
Cours	20 (15)
Laboratoires pratiques	22 (16)
Travail personnel	76 (59)
Total:	118 (90) = 3 ECTS

Documents Électroniques Les transparents et autres supports de cours seront publiés de manière régulière sur Moodle. Les exécutables des laboratoires seront publiés sur la page web `https://crypto.junod.info/sre25/`. Le nom d'utilisateur est `sre25` et le mot de passe sera donné en classe. De plus, un identifiant et un mot de passe individuels seront distribués en classe à chaque participant et permettront d'accéder à un répertoire personnel dans lequel seront déposés les exécutables des laboratoires ainsi que les évaluations.

Prérequis Pour pouvoir suivre ce cours dans les meilleures conditions possibles, il est recommandé de posséder les prérequis suivants:

- bonnes connaissances d'un langage de programmation système (par exemple, C, C++ ou Rust);
- bonnes connaissances d'un langage de script (par exemple Python);
- familiarité avec le système d'exploitation Linux;
- volonté avérée de « mettre les mains dans le cambouis ».

Cours et Laboratoires Pratiques Le cours sera donné sous forme *ex cathedra*, le support de cours étant formé par les transparents.

Les laboratoires pratiques forment le gros du volume de travail dans ce cours. Ils doivent permettre aux participants d'expérimenter et d'approfondir les concepts théoriques présentés en classe. Les laboratoires sont à effectuer essentiellement comme travail personnel, même si du temps sera consacré en classe pour les commencer. Les laboratoires, dont certains seront évalués, sont effectués individuellement ou en groupes d'au plus deux personnes.

Le cours est donné en français, mais tous les supports sont rédigés en anglais.

Évaluations La note finale est constituée à 50% par la note de laboratoire et à 50% par la note de l'examen écrit final.

Au total, 20 laboratoires seront proposés: 3 qui sont très faciles (VE), 5 qui sont faciles (E), 7 qui sont de difficulté moyenne (A), et 5 qui sont plus difficiles (D).

Chaque laboratoire validé donne un certain nombre de points: les laboratoires très faciles valent 1 point, les laboratoires faciles 5 points, les laboratoires de difficulté moyenne 10 points, et les laboratoires plus difficiles 30 points.

Les **laboratoires très faciles et faciles** doivent être validés **individuellement**. Les laboratoires de difficulté moyenne et difficile peuvent être effectués individuellement ou en groupes de deux personnes. Le temps à disposition pour effectuer les laboratoires très faciles et faciles est au minimum d'une semaine, au minimum de deux semaines pour les laboratoires de difficulté moyenne, et de trois semaines pour les laboratoires plus difficiles.

La note de laboratoire est calculée selon le processus suivant:

1. Chaque personne doit valider **au moins 90 points**; si cette condition n'est pas remplie, la note de laboratoire γ_{lab} sera fixée de la manière suivante, où n représente le nombre de points obtenus:

$$\begin{aligned} 80 \leq \quad n \quad &< 90 \quad \rightarrow \gamma_{\text{lab}} = \mathbf{3.5} \\ 70 \leq \quad n \quad &< 80 \quad \rightarrow \gamma_{\text{lab}} = \mathbf{3.0} \\ 60 \leq \quad n \quad &< 70 \quad \rightarrow \gamma_{\text{lab}} = \mathbf{2.5} \\ 50 \leq \quad n \quad &< 60 \quad \rightarrow \gamma_{\text{lab}} = \mathbf{2.0} \\ 40 \leq \quad n \quad &< 50 \quad \rightarrow \gamma_{\text{lab}} = \mathbf{1.5} \\ 0 \leq \quad n \quad &< 40 \quad \rightarrow \gamma_{\text{lab}} = \mathbf{1.0} \end{aligned}$$

2. Si et seulement si la première condition est remplie, deux laboratoires de difficulté moyenne et un laboratoire difficile sélectionnés par le participant ou le groupe seront évalués. Étant donné les trois notes γ_A, $\gamma_{A'}$ et γ_D, la note de laboratoire sera calculée avec la formule

$$\gamma_{\text{lab}} = \frac{\gamma_A + \gamma_{A'} + 2\gamma_D}{4}.$$

   La valeur finale de γ_{lab} sera arrondie à une décimale.

Un laboratoire sera considéré comme validé si et seulement si la personne ou le groupe envoie par courrier électronique à l'enseignant la valeur du secret à découvrir **dans le délai imparti**. L'évaluation d'un laboratoire se fondera sur un rapport, rédigé en français ou en anglais et livré sous forme de fichier PDF, d'au plus une page A4 recto-verso qui devra contenir:

- des réponses succinctes aux questions posées dans la description du laboratoire;
- une description synthétique des difficultés rencontrées et les solutions identifiées pour les contourner;
- une liste des outils utilisés;
- et en annexe, le cas échéant, le code source des outils implémentés par la personne ou le groupe pour résoudre le laboratoire.

Les critères d'évaluation des laboratoires sont les suivants:

- Qualité technique (80%)
  - Degré de complétude (50%)
  - Clarté des explications (25%)
  - Pertinence du choix des outils et des techniques (25%)
- Qualité rédactionnelle (20%)
  - Orthographe, grammaire et syntaxe (100%)

Calendrier Prévu Il est prévu que les séances en présentiel débutent par une ou deux périodes de cours. Le temps restant sera dédié à la présentation et à la discussion des laboratoires, ainsi qu'à débuter leur résolution.

Semaine	Date	Thème	Laboratoires
1	17/02/2025	Introduction	VE1 & E1 (6pts)
2	24/02/2025	x86 & ARM Architectures	VE2 & E2 (6pts)
3	03/03/2025	Structure & Life of an Executable	VE3 & E3 (6pts)
4	10/03/2025	Native & Interpreted Languages	E4 & A1 (15 pts)
5	17/03/2025	Debugging & Hooking	E5 & A2 (15 pts)
6	24/03/2025	Binary Instrumentation	
7	31/03/2025	Software Protection	A3 & D1 (40 pts)
8	07/04/2025	Code Obfuscation	A4 & D2 (40 pts)
9	14/04/2025	Code Tamperproofing	A5 & D3 (40 pts)
10	28/04/2025	Anti-Debug Tricks & Jailbreak Detection	A6 & D4 (40 pts)
11	05/05/2025	Advanced Reverse Engineering Tools	A7 & D5 (40 pts)
12	12/05/2025	Advanced Software Protection Techniques	
13	19/05/2025	Remote Attestation	
14	26/06/2025	Summary & Reserve	