



Ecole d'ingénieurs et d'architectes de Fribourg
Hochschule für Technik und Architektur Freiburg

CAHIER DES CHARGES

CODE OBFUSCATOR

Semestre d'hiver 2010/11

Professeurs : Schuler Jean-Roland, Kilchoer François

Etudiants : Franz Robin, Derbel Amine

1. GÉNÉRALITÉS

1.1 Contexte

Dans le cadre d'un projet de recherche, le groupe de compétences IT Security veut rendre difficile le reverse-engineering d'un programme exécutable.

En effet des utilitaires comme objdump ou IDAPro permettent facilement de trouver le code assembleur et de là retrouver des algorithmes industriels qui sont peut-être des secrets de fabrications d'une entreprise.

1.2 Objectifs du projet

Pour faire ceci, il faudra :

- Interpréter le code machine d'un programme
- Créer un obfuscateur de code qui permet de changer la structure du programme initial pour le rendre inintelligible sans changer sa sémantique

2. DÉVELOPPEMENT DU PROJET


2.1 Avancement du projet dans le temps :


1. Recherche d'information
 - structures des executables et codage elf
 - techniques d'obfuscation en assembleur
 - langage assembleur ARM
2. Développement d'un obfuscator simplifié
 - proposition de solutions
 - essais sur des boucles : if, while
 - tests
3. Développement du programme final
 - ajout de fonctionnalités
 - évaluation des performances
 - tests
4. Rendu final

2.2 Planning du projet et répartition des tâches

Semaine	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
Préparation cahier des charges														
Rendu du cahier des charges														
Présentation du cahier des charges														
Recherche information :														
Structures des executables et codage elf														
Techniques d'obfuscation en assembleur														
Langage assembleur ARM														
Développement d'un obfuscator simplifié:														
Proposition de solutions														
Essais sur instruction if														
Essais sur instruction while														
Jalon 1														
Tests if														
Tests while														
Développement du programme final														
Ajout de fonctionnalités														
Jalon 2														
Evaluation des performances														
Tests														
Rédaction du rapport final														
Rendu du rapport														

 Travail en commun

 Travail effectué par Amine

 Travail effectué par Robin

3. JALONS

Les jalons représentent une étape importante dans le développement du projet, nous avons choisi d'en fixer deux comme montré sur le planning, ils nous aideront à nous repérer dans le temps et de bien atteindre les buts que nous avons fixés.

Jalon 1 : fixé à la semaine A11, nous présenteront un prototype fonctionnel d'un obfuscateur simple que nous pouvons opérer sur des instructions if et while.

Jalon 2 : fixé à la semaine A14, nous présenteront le programme final deux semaines avant le rendu final pour vérifier les dernières modifications à rajouter.

4. CAHIER DES CHARGES

- Comprendre le langage assembleur des processeurs ARM
- Comprendre la structure elf
- Essayer le reverse-engineering : obtenir le code assembleur à partir d'un exécutable
- Maitriser quelques techniques d'obfuscation
- Ecrire un programme qui permet d'obfusquer l'exécutable d'un programme simple
- Ecrire un programme qui permet d'obfusquer le code assembleur d'un programme simple
- Comparaison des deux méthodes