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

PROCÈS VERBAL DE LA SÉANCE NR.11 DU 19.01.2011

Intervenants

Etudiants	Amine Derbel, Robin Franzi
Professeur	François Kilchoer
Lieu et date	Salle D2007, 19.01.2011
Heure	9h00
Durée	20’

Contenu de la séance

- Présentations des méthodes réalisées pour l’obfuscation comme indiqué par le document présenté pendant la séance précédente :
    - Fonction obfuscateCMP : le code obtenu fonctionne à l’inverse de ce qu’il est censé faire → il faudra contrôler quels registres sont modifiés sur ARM lors des instructions OR et CMP
    - Fonction obfuscateMOV : change « MOV <registre>,0 » en « RSB <registre>,<registre> », fonctionne correctement.
    - Fonction obfuscateSUB : change l’instruction SUB en RSB, ADD, RSB, le principe général est : x-y = -(y+(-x)), elle ne fonctionne pas, on obtient une erreur de segmentation.
    - Fonction obfIncPC : le principe de base était d’incrémenter le PC de 2 bytes et d’insérer 2 bytes juste après, comme ça le processeur fonctionne normalement mais si on fait un dump les instructions n’auront aucun sens, mais le processeur n’accepte pas cela, message d’erreur : « illegal instruction ».

  <u>Pour la prochaine séance :</u>

- Essayer de faire fonctionner les deux fonctions obfuscateCMP et obfuscateSUB, en vérifiant les registres et les pointeurs.
- Appliquer le programme sur un vrai exécutable qui existe déjà sur ARM et faire des tests de fonctionnement et observer les performances.