

Lecture et fusion de fichiers ELF

Adrian Amaglio
Mohamed-Karim Boussedra
Benjamin Gontard
Maxence Grand
Quentin Rozand

13 Janvier 2017

Contents

1	Executables produits	2
2	Structure du code	2
2.1	Organisation des sources	2
2.2	Principe de fonctionnement	2
3	Fonctionnalités implémentées et manquantes	3
3.1	Implémentées	3
3.2	Manquantes	3
4	Bogues	3
5	Tests effectués	3
6	Journal de bord	4

1 Executables produits

L'executable `phase1` comprend toutes les fonctionnalités d'affichage du fichier ELF. Il s'utilise de la même manière que le programme `readelf` [1]:

`phase1 [-sShr] [-x <num|nom>] <fichier>`

`-s` Affiche la table des symboles.

`-S` Affiche la table des en-têtes de sections.

`-h` Affiche l'en-tête ELF.

`-x <num|nom>` Affiche le contenu de la section numéro `<num>` ou nommée `<nom>`, en hexadécimal et en ASCII lorsque c'est possible.

`-r` Affiche la table des réallocations.

Toutes ces options s'appliquent au fichier passé en dernier paramètre. L'executable `phase2` prend trois noms de fichiers en paramètre. Il fusionnera les deux premiers dans le troisième.

2 Structure du code

2.1 Organisation des sources

Le code est disponible sur [github](#)[2] dans sa version finale. Le code fonctionnel est sur la branche `master`.

getelf.h Structure `elf_t` représentant un fichier ELF en mémoire.

getelf.c Fonctions de lecture d'un fichier ELF et de remplissage de la structure `elf_t`. Son "api publique" n'est composée que de la fonction `initElf(elf_t elf, str *filename, int mode)` qui s'occupe d'ouvrir et charger le fichier.

display.c Affichage d'informations contenues dans une structure `elf_t`.

phase1.c Lecture d'un fichier ELF avec les fonctions de `getelf.c` et appel des fonctions de `display.c` en fonction des arguments.

fusionelf.c Fonctions de fusion de deux structures `elf_t`.

writeelf.c Écriture d'un fichier ELF à partir d'une structure `elf_t`.

phase2.c Lecture de deux fichiers ELF avec les fonctions de `getelf.c`, fusion avec `fusionelf.c` et écriture d'un fichier résultat avec `writeelf`.

2.2 Principe de fonctionnement

Le contenu de chaque fichier ouvert en lecture est copié en mémoire dans une structure organisée. La récupération des informations se fait dans ces structures pour l'affichage ou la fusion. Dans l'idéal, l'opération de fusion ne devrait pas écrire dans un fichier mais seulement dans une structure. L'écriture sur le disque serait alors prise en charge par une fonction dédiée.

3 Fonctionnalités implémentées et manquantes

Toutes ces fonctionnalités concernent l’affichage et la fusion.

3.1 Implémentées

- Table des symboles
- Table des en-tetes de sections,
- En-tete elf
- Contenu d’une section
- Table des réallocations

3.2 Manquantes

- Section des symboles dynamiques
- Sections unwind
- Sections de notes
- En-tetes de programmes

4 Bogues

Le fichier fusionné final, une fois compilé, n’est pas executable.

5 Tests effectués

Un script bash effectue automatiquement une série de tests et écrit le résultat dans des fichiers textes.

6 Journal de bord

	Adrian	Mohamed-Karim	Benjamin	Quentin	Maxence
03/01/17	Lecture doc, Étapes 1, 2, 3, mise en place du dépôt git				
04/01/17	Récupération des noms de sections		Suite 1, 2 & 3		
05/01/17	Ajout de la structure elf_t		Étapes 4&5		
06/01/17	Refactorisation de la phase 1		Début de la phase 2		
09/01/17	Extention de elf_t		Etape 6&7		
	Récriture des fonction d'affichage				
10/01/17	réécriture des fonction d'affichage		Etape 8&9		
11/01/17	Structuration des fichiers Début du rapport		Correction bug etape 8 et 9		Tests
12/01/17	Restructuration du projet Correction des erreurs et fuites				

References

- [1] <https://linux.die.net/man/1/readelf>
- [2] <https://github.com/AdrianUGA/fusion>