

PROJET : SEMESTRES 3 - 4

Chaines de caractères en langage C : vulnérabilités et performances

Peu de fonctions de la *bibliothèque standard C* (**glibc** sous *Linux*) auront cumulé autant de ratés (noms piégés, conception peu soignée, fonctionnement inconsistant, ambiguïté, sécurité défaillante) que les fonctions dédiées à la copie ou à la concaténation de chaînes de caractères.

Le projet se décomposera en deux parties. À partir de documents officiels relatifs aux bonnes pratiques de programmation en langage C, la première partie consistera à détecter (et corriger) les vulnérabilités présentes dans certains exemples de code C.

La deuxième partie sera consacrée à l'étude de performance des fonctions ***strncpy*, *strncat*, *strlcpy*, *strlcat*, *strntcpy* et *strntcat***.

1. Vulnérabilités

Les problèmes posés par les chaînes de caractères en langage C sont nombreux : leur copie ou concaténation peuvent provoquer un dépassement de tampon ou une perte de données (chaînes tronquées silencieusement), créer des chaînes mal formées (c'est-à-dire non terminées par un caractère ‘\0’).

La proposition [1] soumise à l'Open Group propose d'utiliser la fonction ***memccpy*** pour la copie(concaténation de chaînes de caractères. Ce document illustre son propos à l'aide de plusieurs bouts de code.

Le travail à réaliser sera de vérifier en situations anormales (chaînes mal formées, chaînes trop longues, etc.) la solidité du code présenté.

[1] <http://www.open-std.org/jtc1/sc22/wg14/www/docs/n2349.htm>

2. Performances

Les travaux à réaliser seront les suivants :

- comparer les temps d'exécution d'une copie(concaténation de chaînes en utilisant ***memccpy*, *strlcpy*/*strlcat* et *strntcpy*/*strntcat*** au sein de plusieurs programmes significatifs
- faire une analyse statistique de l'utilisation des fonctions ***strncpy*/*strncat*** présentes dans les commandes linux les plus utilisées (paquetage ***coreutils***)

- instrumenter le code source de certaines commandes linux choisies, en remplaçant les occurrences de **strncpy/strncat** par **memccpy** puis par **strntcpy/strntcat**, puis comparer les temps d'exécution des trois versions (commande linux originale, commande linux utilisant **memccpy**, commande linux utilisant **strntcpy/strntcat**)

- créer un paquetage permettant l'installation automatique des fonctions **strntcpy/strntcat**. On s'inspirera pour cela du paquetage *libbsd-dev* contenant les fonctions **strlcpy/strlcat**.