ENSIIE 1e année — Année 2009-2010
Systèmes

TP n° 11

1 Stack smash

On considère le programme suivant :

```
#include <stdio.h>
void muahaha()
{
    ...
}
int main()
{
    printf("Hello\n");
    muahaha();
    printf("World\n");
    return 0;
}
```

Le but est d'écrire le corps de la fonction `muahaha()` afin qu'elle modifie le contenu de la pile et change son adresse de retour : en particulier, on aimerait que cette fonction empêche le *second* appel à `printf()`.

1. Comment peut-on faire pour que la fonction `muahaha()` affiche le contenu de la pile ? Affichez par exemple 8*8 octets de la pile ?

   (Sur la machine Turing, le type `int` est de taille 4 octets, alors que `long int` est de 8 octets : utilisez ce dernier pour désigner les éléments de la pile.)

2. Utilisez la commande `objdump` pour déterminer l'adresse de retour de `muahaha()` (c'est-à-dire l'adresse de l'instruction de `main` qui suit celle qui appelle `muahaha`).

3. Utilisez les résultats des deux questions précédentes pour que la fonction `muahaha` reécrive son adresse de retour. A l'exécution, le programme doit afficher simplement `Hello`, et pas `World`.