Cryptographie
Attaques par canaux auxilliaires

December 18, 2023

1 Attaque temporelle du code PIN

Dans cette section nous intéressons à trois variations autour du code PIN. Pour une question de simplicité le programme permet à l'utilisateur de tester autant de codes qu'il le souhaite sans blocage.

1. Le programme `pin4` vérifie la validité d'un code à 4 chiffres. Réaliser une attaque temporelle *à la main* pour retrouver le code.

2. Le programme `pin16` vérifie la validité d'un code à 16 chiffres. Combien de temps prendrait une attaque par recherche exhaustive (voir figure 1)? Écrire un programme automatisant l'approche précédente pour retrouver le code. Quelle est sa complexité en fonction du nombre de chiffre du code PIN ?

3. Le programme `pin16a` est une variante du programme précédent qui vérifie la validité d'un code à 16 chiffres mais en testant les chiffres dans un ordre spécifique et secret déterminé par le tableau `perm` (voir figure 1). Écrire un programme permettant de retrouver le code secret. Quelle est sa complexité en fonction du nombre de chiffres du code PIN ?

```
//pin16
char pin[16] = {...};
...
int i,j,k=1;
for (i=0; i<16; i++){
  if (argv[1][i]!=pin[i]){
    return -1;
  }
}
```

```
//pin16a
char pin[16] = {...};
int perm[16] = {...};
...
int i,j,k=1;
for (i=0; i<16; i++){
  if (argv[1][perm[i]]!=pin[perm[i]]){
    return -1;
  }
}
```

Figure 1: Fragment du code source des programmes `pin16x`