PARTIE E. Faugeron - Examen attaques logicielles sur Java Card

4 pts, durée ~30 minutes

Répondre sur intercalaires !

1. Quels sont les deux principaux éléments de sécurité d'une javacard ? Les décrire brièvement. *0,5/4*

2. Qu'est-ce qu'une attaque combinée ? décrire brièvement un exemple d'attaque combinée. *0,5/4*

3. Le code suivant est présent dans le fichier JAVA/JCA d'une application : *2/4*

Fichier java :

```
public class Underflow_applet extends Applet {
      byte[] codeDump = {(byte)0x01, (byte)0x00, (byte)0x7D, (byte)0x80,
                         (byte)0x00, (byte)0x78};
      short myVar1 = 0x1111;
      short myVar2 = 0x1111;
      short myVar3 = 0x1111;
      short myVar4 = 0x1111;
      short myVar5 = 0x1111;

      [...]

      public void myFunction (short param)
      {
            short myLocal1 = (short)0xAAAA;
            short myLocal2 = (short)0xBBBB;
            short myLocal3 = (short)0xCCCC;
      }

      [...]
```

Fichier JCA :

```
.class public Underflow_applet 0 extends 0.3 {
// extends javacard/framework/Applet

      .fields {
                  byte[] codeDump 0;          // [B
                  short myVar1 1;       // S
                  short myVar2 2;       // S
                  short myVar3 3;       // S
                  short myVar4 4;       // S
                  short myVar5 5;       // S
      }

      [...]
```

```
        .method public myFunction(S)V 9 {
          .stack 1;
          .locals 3;
          L0:
                sspush -21846;
                sstore_2;
                sspush -17477;
                sstore_3;
                sspush -13108;
                sstore 4;
        }
        [...]
}
```

Ecrire le nouveau code de la fonction *myFunction* permettant de créer un underflow et de stocker les valeurs retrouvées dans les variables globales myVar1, myVar2, myVar3, myVar4, myVar5. Décrire l'effet de la modification effectuée et le but finale de l'underflow.

4. L'application contient les trois tableaux suivants : 1/4
   - byte[] myArray1 = new byte[10] ;
   - byte[] myArray2 = new byte[20] ;
   - byte[] myArray3 = new byte[30] ;

   Les adresses de ces tableaux sont les suivantes :
   - myArray1 : 0x8010
   - myArray2 : 0x801F
   - myArray3 : 0x8038

   Déterminer la taille de l'header du tableau (détailler le calcul). Quelles données peuvent être contenues dans cet header ? Quels types de manipulations peuvent être effectués sur cet header ?