Project Members:
Sujeet Deshmukh(476359)
Nidhi Pokhriyal(476361)
Surendra Kumar Yadav(476364)

PROJECT : SMART CARD TLS
PHASE IV

1. The applet code **eapengine.java** file was changed as under for testing using JCProfiler:-

```
case INS_VERIFY:   // retrieve the PIN data for validation.
        apdu.setIncomingAndReceive();
        if (P2 == (byte)0x01)
        {       PM.check(PMC.TRAP_methodName_0);
                verify(OperatorPin,buffer);
                if(OperatorPin.isValidated()) UserPin.resetAndUnblock();
                PM.check(PMC.TRAP_methodName_0);
        }
        else
        {
                PM.check(PMC.TRAP_methodName_0);
                verify(UserPin,buffer);
                PM.check(PMC.TRAP_methodName_0);
        }
        break;

case INS_CHANGE_PIN:   // retrieve the PIN data for validation.
        PM.check(PMC.TRAP_methodName_0);
        len= apdu.setIncomingAndReceive() ;
        if (len != (short)16)
        ISOException.throwIt(ISO7816.SW_WRONG_LENGTH);
        buffer[4]=(byte)8;

        if (P2 == (byte)0x01)
        {       verify(OperatorPin,buffer);
                OperatorPin.update(buffer,(short)13,(byte)8);
        }
        else
        {       verify(UserPin,buffer);
                UserPin.update(buffer,(short)13,(byte)8);
        }
        PM.check(PMC.TRAP_methodName_0);
        break;
```

2. All files related to eapengine applet were copied to
..\JCProfiler-master\demo\templates\input_applet_files folder

3. JCProfiler.jar tool was used to personalized the traps using the command

```
java -jar JCProfiler.jar --setTraps --baseDir demo --methodBaseName methodName --
trapIDStartConst 7770
```

The screenshot of the output is shown as under:-

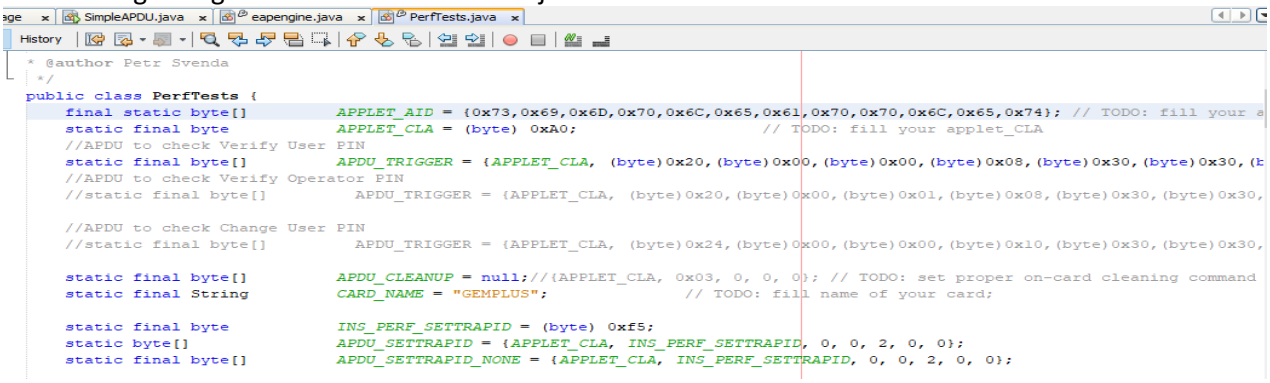
```
INFO: Processing file 'demo/target/profiler_applet/auth.java.orig'
  No template performance traps found in file 'demo/target/profiler_applet/auth.java.orig'
INFO: Processing file 'demo/target/profiler_applet/credentialpsk.java.orig'
  No template performance traps found in file 'demo/target/profiler_applet/credentialpsk.java.orig'
INFO: Processing file 'demo/target/profiler_applet/credentialtls.java.orig'
  No template performance traps found in file 'demo/target/profiler_applet/credentialtls.java.orig'
INFO: Processing file 'demo/target/profiler_applet/eapengine.java.orig'
  OK: Total '7' traps found in file 'demo/target/profiler_applet/eapengine.java.orig'
INFO: Processing file 'demo/target/profiler_applet/methodpsk.java.orig'
  No template performance traps found in file 'demo/target/profiler_applet/methodpsk.java.orig'
INFO: Processing file 'demo/target/profiler_applet/methodtls.java.orig'
  No template performance traps found in file 'demo/target/profiler_applet/methodtls.java.orig'
INFO: Transforming file 'demo/target/profiler_applet/PMC.java' for trapID constants.
  OK: '//### PLACEHOLDER PMC CONSTANTS' found and replaced
INFO: Transforming file 'demo/target/profiler_client/src/jcprofiler/PerfTests.java' for code with trapID to send.
  OK: '//### PLACEHOLDER PERFTRAPS INIT' found and replaced
INFO: Transforming file 'demo/target/profiler_client/src/jcprofiler/PerfTests.java' for code with mapping between name and trapID.
  OK: '//### PLACEHOLDER PMC MAPPINGS' found and replaced


#######################################
INFO: The personalized profiler generation is now finished.
Directory 'demo/target/profiler_applet/' contains your applet's transformed files with numbered performance traps.
Now you need to:
1. Copy applet files (together with PMC.java and PM.java) back to your applet structure.
2. Open PM.java and PMC.java and update package to your applet's package name.
3. Open PM.java and *move* specified part of code (INS_PERF_SETSTOP) at the end of file to process() method of your applet.
4. Convert your applet and upload to target card as usual.

Directory 'demo/target/profiler_client/' contains client-side code of the profiler.
Now you need to:
1. Open PerfTests.java and correct APPLET_CLA, APPLET_AID according to your applet.
2. Open PerfTests.java and set proper apdu APDU_TRIGGER which will trigger (let execute) the method you like to profile (method which now have 'PM.check(PMC.TRAP_' inse
rted).
3. (Optional) Set CARD_NAME to sensible string. If APDU_CLEANUP is set, this apdu is send to card after every measurement command (for 'cleaning').
4. Compile and run JCProfiler_client. Measurement apdu commands are send to card and resulting measurements are inserted as comment directly behind the correspoding per
formance trap.
5. Inspect console results and modified files which are copied into directory 'demo/target/profiler_applet//perf/unique_experiment_id'.
```

4. Files from profiler_applet were copied and following code was copied to applet file in process function:-

```
case INS_PERF_SETSTOP:
  PM.m_perfStop = Util.makeShort(buffer[ISO7816.OFFSET_CDATA], buffer[(short) (ISO7816.OFFSET_CDATA + 1)]);
  break;
```

5. The applet was converted using JC2.2.2 convertor kit and was uploaded in Gemplus Javacard

6. Following changes were done in PerfTests.java



7. JCProfiler_client.java was run for to measure Verify User PIN function
The output of the console is as under :-

```
JCProfiler v1.0 by OpenCryptoProject, 2017
Connecting to card...
0 : PC/SC terminal Gemplus USB SmartCard Reader 0
card: PC/SC card in Gemplus USB SmartCard Reader 0, protocol T=1, state OK
3b f8 13 00 00 81 31 fe 45 4a 43 4f 50 76 32 34 31 b7
Selecting applet...
```

--> 00A404000C73696D706C656170706C6574
<-- 9000 [24 ms]
Done.
--> A0F50000020000
<-- 9000 [19 ms]

---------- Performance profiling start ----------

insert nice name
--> A0F50000027771
<-- 9000 [24 ms]
--> A02000000830303030FFFFFFFF
<-- 9000 [36 ms]
--> A0F50000027772
<-- 9000 [18 ms]
--> A02000000830303030FFFFFFFF
<-- 9000 [34 ms]
--> A0F50000027773
<-- 9000 [18 ms]
--> A02000000830303030FFFFFFFF
<-- 7773 [13 ms]
--> A0F50000027774
<-- 9000 [19 ms]
--> A02000000830303030FFFFFFFF
<-- 7774 [35 ms]
--> A0F50000027775
<-- 9000 [19 ms]
--> A02000000830303030FFFFFFFF
<-- 9000 [34 ms]
--> A0F50000027776
<-- 9000 [18 ms]
--> A02000000830303030FFFFFFFF
<-- 9000 [34 ms]
--> A0F50000027770
<-- 9000 [19 ms]
--> A02000000830303030FFFFFFFF
<-- 9000 [34 ms]
[PERF_START-TRAP_methodName_1], failed to reach after 36 ms (0x9000)
[TRAP_methodName_1-TRAP_methodName_2], failed to reach after 34 ms (0x9000)
[TRAP_methodName_2-TRAP_methodName_3], -21 ms
[TRAP_methodName_3-TRAP_methodName_4], 22 ms
[TRAP_methodName_4-TRAP_methodName_5], failed to reach after 34 ms (0x9000)
[TRAP_methodName_5-TRAP_methodName_6], failed to reach after 34 ms (0x9000)
[TRAP_methodName_6-TRAP_methodName_COMPLETE], 0 ms

---------- Performance profiling finished ----------

Disconnecting from card... Done.
##########################
!!! SOME PERFORMANCE TRAPS NOT REACHED !!!
##########################
TRAP_methodName_1
TRAP_methodName_2
TRAP_methodName_5
TRAP_methodName_6
INFO: going to insert profiled info into files in '..\Profiler_applet\' directory
BUILD SUCCESSFUL (total time: 3 seconds)

8. JCProfiler_client.java was run for to measure Verify Operator PIN function
The output of the console is as under :-

JCProfiler v1.0 by OpenCryptoProject, 2017
Connecting to card...
0 : PC/SC terminal Gemplus USB SmartCard Reader 0
card: PC/SC card in Gemplus USB SmartCard Reader 0, protocol T=1, state OK
3b f8 13 00 00 81 31 fe 45 4a 43 4f 50 76 32 34 31 b7
Selecting applet...
--> 00A404000C73696D706C656170706C6574
<-- 9000 [24 ms]
Done.
--> A0F50000020000
<-- 9000 [18 ms]

---------- Performance profiling start ----------

insert nice name
--> A0F50000027771
<-- 9000 [17 ms]
--> A020000108303030303030303030
<-- 7771 [12 ms]
--> A0F50000027772
<-- 9000 [18 ms]
--> A020000108303030303030303030
<-- 7772 [35 ms]
--> A0F50000027773
<-- 9000 [18 ms]
--> A020000108303030303030303030
<-- 9000 [35 ms]
--> A0F50000027774
<-- 9000 [19 ms]
--> A020000108303030303030303030
<-- 9000 [35 ms]
--> A0F50000027775

<-- 9000 [18 ms]
--> A020000108303030303030303030
<-- 9000 [36 ms]
--> A0F50000027776
<-- 9000 [19 ms]
--> A020000108303030303030303030
<-- 9000 [36 ms]
--> A0F50000027770
<-- 9000 [19 ms]
--> A020000108303030303030303030
<-- 9000 [36 ms]
[PERF_START-TRAP_methodName_1], 12 ms
[TRAP_methodName_1-TRAP_methodName_2], 23 ms
[TRAP_methodName_2-TRAP_methodName_3], failed to reach after 35 ms (0x9000)
[TRAP_methodName_3-TRAP_methodName_4], failed to reach after 35 ms (0x9000)
[TRAP_methodName_4-TRAP_methodName_5], failed to reach after 36 ms (0x9000)
[TRAP_methodName_5-TRAP_methodName_6], failed to reach after 36 ms (0x9000)
[TRAP_methodName_6-TRAP_methodName_COMPLETE], 0 ms

---------- Performance profiling finished ----------

Disconnecting from card... Done.
##########################
!!! SOME PERFORMANCE TRAPS NOT REACHED !!!
##########################
TRAP_methodName_3
TRAP_methodName_4
TRAP_methodName_5
TRAP_methodName_6
INFO: going to insert profiled info into files in '..\Profiler_applet\' directory
BUILD SUCCESSFUL (total time: 2 seconds)

9. JCProfiler_client.java was run for to measure Change Operator PIN function
The output of the console is as under :-

JCProfiler v1.0 by OpenCryptoProject, 2017
Connecting to card...
0 : PC/SC terminal Gemplus USB SmartCard Reader 0
card: PC/SC card in Gemplus USB SmartCard Reader 0, protocol T=1, state OK
3b f8 13 00 00 81 31 fe 45 4a 43 4f 50 76 32 34 31 b7
Selecting applet...
--> 00A404000C73696D706C656170706C6574
<-- 9000 [24 ms]
Done.
--> A0F50000020000
<-- 9000 [18 ms]

---------- Performance profiling start ----------

insert nice name
--> A0F50000027771
<-- 9000 [17 ms]
--> A024000110303030303030300103010001010009
<-- 9000 [53 ms]
--> A0F50000027772
<-- 9000 [19 ms]
--> A024000110303030303030300103010001010009
<-- 6309 [28 ms]
--> A0F50000027773
<-- 9000 [20 ms]
--> A024000110303030303030300103010001010009
<-- 6308 [29 ms]
--> A0F50000027774
<-- 9000 [18 ms]
--> A024000110303030303030300103010001010009
<-- 6307 [28 ms]
--> A0F50000027775
<-- 9000 [19 ms]
--> A024000110303030303030300103010001010009
<-- 7775 [14 ms]
--> A0F50000027776
<-- 9000 [19 ms]
--> A024000110303030303030300103010001010009
<-- 6306 [28 ms]
--> A0F50000027770
<-- 9000 [19 ms]
--> A024000110303030303030300103010001010009
<-- 6305 [28 ms]
[PERF_START-TRAP_methodName_1], failed to reach after 53 ms (0x9000)
[TRAP_methodName_1-TRAP_methodName_2], failed to reach after 28 ms (0x6309)
[TRAP_methodName_2-TRAP_methodName_3], failed to reach after 29 ms (0x6308)
[TRAP_methodName_3-TRAP_methodName_4], failed to reach after 28 ms (0x6307)
[TRAP_methodName_4-TRAP_methodName_5], -14 ms
[TRAP_methodName_5-TRAP_methodName_6], failed to reach after 28 ms (0x6306)
[TRAP_methodName_6-TRAP_methodName_COMPLETE], 0 ms

---------- Performance profiling finished ----------

Disconnecting from card... Done.
##########################
!!! SOME PERFORMANCE TRAPS NOT REACHED !!!
##########################
TRAP_methodName_1

TRAP_methodName_2
TRAP_methodName_3
TRAP_methodName_4
TRAP_methodName_6
INFO: going to insert profiled info into files in '..\Profiler_applet\' directory
BUILD SUCCESSFUL (total time: 2 seconds)

10. For the first run (Verify User PIN), following was found to be the measurements:-

```
case INS_VERIFY:   // retrieve the PIN data for validation.

    apdu.setIncomingAndReceive();
    if (P2 == (byte)0x01)
    {   PM.check(PMC.TRAP_methodName_1);
        verify(OperatorPin,buffer);
        if(OperatorPin.isValidated()) UserPin.resetAndUnblock();
        PM.check(PMC.TRAP_methodName_2);
    }
    else
    {
        PM.check(PMC.TRAP_methodName_3); // -21 ms (noCardNameGiven,1525194762453)
        verify(UserPin,buffer);
        PM.check(PMC.TRAP_methodName_4); // 22 ms (noCardNameGiven,1525194762453)
    }
    break;

case INS_CHANGE_PIN:   // retrieve the PIN data for validation.
    PM.check(PMC.TRAP_methodName_5);
    len= apdu.setIncomingAndReceive() ;
    if (len != (short)16)
    ISOException.throwIt(ISO7816.SW_WRONG_LENGTH);
    buffer[4]=(byte)8;
```

11. For the next run (Verify Operator PIN), following was found to be the measurements:-

```
case INS_VERIFY:   // retrieve the PIN data for validation.

    apdu.setIncomingAndReceive();
    if (P2 == (byte)0x01)
    {   PM.check(PMC.TRAP_methodName_1); // 12 ms (noCardNameGiven,1525195009710)
        verify(OperatorPin,buffer);
        if(OperatorPin.isValidated()) UserPin.resetAndUnblock();
        PM.check(PMC.TRAP_methodName_2); // 23 ms (noCardNameGiven,1525195009710)
    }
    else
    {
        PM.check(PMC.TRAP_methodName_3);
        verify(UserPin,buffer);
        PM.check(PMC.TRAP_methodName_4);
    }
    break;

case INS_CHANGE_PIN:   // retrieve the PIN data for validation.
    PM.check(PMC.TRAP_methodName_5);
    len= apdu.setIncomingAndReceive() ;
```

12. For the next run (Change Operator PIN), following was found to be the measurements:-

```
    }
    else
    {
        PM.check(PMC.TRAP_methodName_3);
        verify(UserPin,buffer);
        PM.check(PMC.TRAP_methodName_4);
    }
    break;

case INS_CHANGE_PIN:   // retrieve the PIN data for validation.
    PM.check(PMC.TRAP_methodName_5); // -14 ms (noCardNameGiven,1525196369603)
    len= apdu.setIncomingAndReceive() ;
    if (len != (short)16)
    ISOException.throwIt(ISO7816.SW_WRONG_LENGTH);
    buffer[4]=(byte)8;

    if (P2 == (byte)0x01)
    {   verify(OperatorPin,buffer);
        OperatorPin.update(buffer,(short)13,(byte)8);
    }
    else
    {   verify(UserPin,buffer);
        UserPin.update(buffer,(short)13,(byte)8);
    }
    PM.check(PMC.TRAP_methodName_6);
    break;
```

13. **Conclusion**:
Following are the measurements of three functions:-

Function	Time
Verify User PIN	22ms
Verify Operator PIN	23ms
Change Operator PIN	*

*Change PIN function verifies the old PIN and if found correct then updates the new PIN. JCProfiler could not give measurements for Change PIN function, as this function was called repeatedly using the same APDU Trigger and very first instance PIN was changed and from next repetitions Change PIN function failed to change the PIN as old PIN was not found to be correct

14. **Timings measurements using APDU Logs**: Following is the output of APDU Logs :-

```
Connecting to card...Looking for physical cards... Success.
Cards found: [PC/SC terminal Gemplus USB SmartCard Reader 0]
Connecting... Done.
Establishing channel... Done.
Smartcard: Selecting applet...
--> 00A404000C73696D706C656170706C6574
<-- 9000 [24 ms]
 Done.
User PIN verify
--> A020000008303030 30FFFFFFFF
<-- 9000 [34 ms]
ResponseAPDU: 2 bytes, SW=9000
User PIN verify - DONE
Operator PIN verify
--> A02000010830303030303030 30
<-- 9000 [35 ms]
ResponseAPDU: 2 bytes, SW=9000
Operator PIN verify - DONE
User PIN Change
--> A02400001030303030FFFFFFFF0103010001010009
<-- 9000 [52 ms]
ResponseAPDU: 2 bytes, SW=9000
User PIN Change - DONE
Operator PIN Change
--> A024000110303030303030303001010009010301 00
<-- 9000 [52 ms]
ResponseAPDU: 2 bytes, SW=9000
BUILD SUCCESSFUL (total time: 2 seconds)
```

Function	Time
Verify User PIN	34ms
Verify Operator PIN	35ms
Change Operator PIN	52ms
Change User PIN	52ms