Reverse Engineering Java SIM card

ILLUSTRATION OF THE IMPACT AND POTENTIAL OF JAVA CARD VULNERABILITIES

DESCRIPTION

This document provides sample know-how acquired as part of the reverse engineering process of Java based smartcards [1].

Security Explorations conducted reverse engineering of selected Gemalto [2] SIM cards by exploiting a weakness in their Java Card implementation. As a result, significant information about cards' implementation, environment and security could be obtained.

The next paragraphs provide mostly output generated by the commands of our custom Gemalto Java SIM card reverse engineering tool that was developed during reverse engineering process of the following cards:

- *GemXplore 3G V3.0-256K*
  ATR 3b9f95801fc78031e073fe211b63e208a8830f900089
- *3G USIMERA Prime*
  ATR 3b9e96801fc78031e073fe211b66d0017a7b0e000e

GemXplore 3G V3.0-256K

Application list

```
*******************************************************
*                      APPLETS                        *
*******************************************************
[0]
- addr    b828
- type    STK_APPLET [tar: b0:00:01 msl: No Ciphering, Cryptographic Checksum]
- aid     a0:00:00:00:18:03:15:00:00:00:00:00:b0:00:01
- privs   0
- id      29
- sec dom 3388
- def_pkg 350 com/gemplus/javacard/sim/system/ota/installer/usim
- inst    b878 class cc00
[1]
- addr    b7b8
- type    STK_APPLET [tar: b0:00:00 msl: No Ciphering, Cryptographic Checksum]
- aid     a0:00:00:00:18:03:09:00:00:00:00:00:b0:00:00
- privs   0
- id      22
- sec dom 3388
```

```
- def_pkg 330 com/gemplus/javacard/sim/system/ota/installer
- inst    b808 class ca01
[2]
- addr    b750
- type    STK_APPLET [tar: b0:00:10 msl: No Ciphering, Cryptographic Checksum]
- aid     a0:00:00:00:18:03:09:00:00:00:00:00:b0:00:10
- privs   0
- id      21
- sec dom 3388
- def_pkg 330 com/gemplus/javacard/sim/system/ota/installer
- inst    8760 class ca00
[3]
- addr    8720
- type    APPLET
- aid     a0:00:00:00:87:10:02:ff:33:ff:ff:89:01:01:01:00
- privs   0
- id      19
- sec dom 3388
- def_pkg 310 com/gemplus/javacard/sim/applet/installer/usim
- inst    8758 class c800
[4]
- addr    190
- type    APPLET
- aid     a0:00:00:00:09:00:01:ff:33:ff:ff:89:c0:00:00:00
- privs   0
- id      12
- sec dom 3388
- def_pkg 2f0 com/gemplus/javacard/sim/applet/installer
- inst    1e0 class c600
[5]
- addr    590
- type    APPLET
- aid     a0:00:00:00:87:10:01:ff:33:ff:ff:89:01:01:01:00
- privs   4 [Default selected]
- id      11
- sec dom 3388
- def_pkg 2f0 com/gemplus/javacard/sim/applet/installer
- inst    5c8 class c601
[6]
- addr    5d0
- type    APPLET
- aid     a0:00:00:00:62:03:01:0c:01:01
- privs   0
- id      9
- sec dom 3388
- def_pkg 2170 (null)
- inst    21d0 class d001
...
```

Packages list

```
shell> pkglist
*******************************************************
*                      PACKAGES                       *
*******************************************************
[com/gemplus/javacard/sim/system/bipsecuritydomain]
- addr    570
- aid     a0:00:00:00:18:10:01:88
- id      ee
- def     59ff
- tr      5a7f
- deps    0
- statics 0
[com/gemplus/javacard/sim/system/proxyinstaller]
- addr    550
- aid     a0:00:00:00:18:10:a3
```

```
- id      ec
- def     58a7
- tr      59e7
- deps    0
- statics 0
[com/gemplus/javacard/sim/system/bip20]
- addr    530
- aid     a0:00:00:00:18:10:a1
- id      ea
- def     d4f
- tr      56f7
- deps    0
- statics 288
[com/gemplus/javacard/bip20]
- addr    510
- aid     a0:00:00:00:18:10:a2
- id      e8
- def     7
- tr      ce7
- deps    0
- statics 278
[com/gemplus/javacard/sim/system/ota/installer/usim]
- addr    350
- aid     a0:00:00:00:18:03:15
- id      cc
- def     e27b
- tr      e31b
- deps    0
- statics 0
[com/gemplus/javacard/sim/system/ota/installer]
- addr    330
- aid     a0:00:00:00:18:03:09
- id      ca
- def     e1bb
- tr      e263
- deps    0
- statics 0
[com/gemplus/javacard/sim/applet/installer/usim]
- addr    310
- aid     a0:00:00:00:18:03:14
- id      c8
- def     e123
- tr      e1ab
- deps    0
- statics 0
[com/gemplus/javacard/sim/applet/installer]
- addr    2f0
- aid     a0:00:00:00:18:03:18
- id      c6
- def     e04b
- tr      e10b
- deps    0
- statics 0
[com/gemplus/javacard/gop]
- addr    8559
- aid     a0:00:00:00:18:03:05
- id      c4
- def     ce3b
- tr      dfab
- deps    0
- statics 178
[com/gemplus/javacard/sim/applet]
- addr    8539
- aid     a0:00:00:00:18:03:08
- id      c2
- def     c21b
- tr      cdcb
```

```
- deps    0
- statics 170
[com/gemplus/javacard/sim/toolkit]
- addr    8519
- aid     a0:00:00:00:18:03:04
- id      c0
- def     bdf3
- tr      c1cb
- deps    0
- statics 0
...
```

Extracted packages (files)

```
1189    0003_java.rmi.dis
81081   0007_com.gemplus.javacard.bip20.dis
982     0053_java.io.dis
62067   009b_javacard.framework.dis
76493   07b8_(null).dis
60614   0893_javacard.framework.service.dis
473571  0d4f_com.gemplus.javacard.sim.system.bip20.dis
11698   122b_visa.openplatform.dis
26619   13e3_uicc.toolkit.dis
81978   1783_sim.toolkit.dis
5496    2258_(null).dis
3299    2383_sim.access.dis
24390   240b_com.gemplus.javacard.sim.filesystem.dis
368     2713_com.gemplus.javacard.sim.toolkit.interfaces.dis
606     274b_com.gemplus.javacard.sim.access.interfaces.dis
3682    278b_com.gemplus.javacard.sim.access.exceptions.dis
794     2823_com.gemplus.javacard.sim.ota.interfaces.dis
334     286b_com.gemplus.javacard.sim.applet.constants.dis
174850  28a3_com.gemplus.javacard.sim.system.ota.layer.dis
2822    3901_com.gemplus.javacard.stub.dis
11032   3981_java.lang.dis
32285   3ac1_javacard.security.dis
3152    3e71_javacardx.crypto.dis
138739  3ec9_com.gemplus.javacardx.crypto.dis
122560  413b_com.gemplus.javacard.sim.system.filesystem.dis
248511  51c1_com.gemplus.javacard.system.dis
3699    543b_com.gemplus.javacard.sim.access.dis
6858    54db_com.gemplus.javacard.uicc.access.dis
78832   55fb_com.gemplus.javacard.sim.ota.dis
6295    58a7_com.gemplus.javacard.sim.system.proxyinstaller.dis
2872    59ff_com.gemplus.javacard.sim.system.bipsecuritydomain.dis
34147   62a3_com.gemplus.javacard.sim.system.ota.dis
561468  67fb_com.gemplus.javacard.sim.system.toolkit.dis
13047   7419_com.gemplus.javacard.util.dis
7293    7581_uicc.access.dis
7294    7681_uicc.system.dis
923     7799_uicc.usim.access.dis
2851    77c9_uicc.usim.toolkit.dis
25652   bdf3_com.gemplus.javacard.sim.toolkit.dis
77367   c21b_com.gemplus.javacard.sim.applet.dis
113811  ce3b_com.gemplus.javacard.gop.dis
4412    e04b_com.gemplus.javacard.sim.applet.installer.dis
2967    e123_com.gemplus.javacard.sim.applet.installer.usim.dis
3638    e1bb_com.gemplus.javacard.sim.system.ota.installer.dis
3109    e27b_com.gemplus.javacard.sim.system.ota.installer.usim.dis
```

Sample of a package extraction

```
PACKAGE: com/gemplus/javacard/sim/system/ota/installer/usim
 * addr                    e27b
 * tl_addr                 e31b
 * static_data_addr        0000
```

```
 [CLASS cc00]
 - addr                    e295
 - flags                   40
 - token                   0000
 - superclass              bc08
 - instanceSize            01
 - FirstReferenceToken     00
 - ReferenceCount          00
 - publicMethodTableBase   0b
 - publicMethodTableCount  00
 - packageMethodTableBase  00
 - packageMethodTableCount 00
 - interfaces
    * 8804
    * a201
      - ID 0 method 08
    * bc00
      - ID 0 method 09
[METHOD cc01]
 - addr                    e2aa
 - flags                   00
 - token                   0001
 - maxstack                02
 - nargs                   02
 - maxlocals               00
 - codelen                 0006
0000:  18 1d 8c bc 24 7a  ....$z
      e2aa:0000 aload_0
      e2ab:0001 sload_1
      e2ac:0002 invokespecial bc24   ; com/gemplus/javacard/sim/system/ota
      e2af:0005 return
[METHOD cc02]
 - addr                    e2b2
 - flags                   00
 - token                   0002
 - maxstack                05
 - nargs                   03
 - maxlocals               04
 - codelen                 004f
0000:  1d 18 1d 25 41 06 41 32 18 1f 04 8d 94 d0 28 04  ...%A.A2......(.
0010:  15 04 66 0a 15 04 95 00 be 10 61 08 11 69 85 8d  ..f.......a..i..
0020:  88 2f 15 04 94 00 be 10 8b 01 29 29 05 16 05 61  ./........))...a
0030:  08 11 69 85 8d 88 2f 8f cc 00 3d 16 05 8c cc 01  ..i.../...=.....
0040:  28 06 15 06 18 1d 04 41 18 1d 25 8b 04 02 7a  (......A..%...z
      e2b2:0000 sload_1
      e2b3:0001 aload_0
      e2b4:0002 sload_1
      e2b5:0003 baload
      e2b6:0004 sadd
      e2b7:0005 sconst_3
      e2b8:0006 sadd
      e2b9:0007 sstore_3
      e2ba:0008 aload_0
      e2bb:0009 sload_3
      e2bc:000a sconst_1
      e2bd:000b invokestatic 94d0    ; com/gemplus/javacard/system
      e2c0:000e astore 0004
      e2c2:0010 aload 0004
      e2c4:0012 ifnull 001c
      e2c6:0014 aload 0004
      e2c8:0016 instanceof  be10
      e2cc:001a ifne 0022
      e2ce:001c sspush 6985
      e2d1:001f invokestatic 882f    ;  "throwIt(S)V"
      e2d4:0022 aload 0004
      e2d6:0024 checkcast  be10
      e2da:0028 invokevirtual 0129
```

```
      e2dd:002b sstore 0005
      e2df:002d sload 0005
      e2e1:002f ifne 0037
      e2e3:0031 sspush 6985
      e2e6:0034 invokestatic 882f    ;  "throwIt(S)V"
      e2e9:0037 new cc00             ; com/gemplus/javacard/sim/system/ota/installer/usim
      e2ec:003a dup
      e2ed:003b sload 0005
      e2ef:003d invokespecial cc01   ; com/gemplus/javacard/sim/system/ota/installer/usim
      e2f2:0040 astore 0006
      e2f4:0042 aload 0006
      e2f6:0044 aload_0
      e2f7:0045 sload_1
      e2f8:0046 sconst_1
      e2f9:0047 sadd
      e2fa:0048 aload_0
      e2fb:0049 sload_1
      e2fc:004a baload
      e2fd:004b invokevirtual 0402
      e300:004e return
[APPLETS]
- aid     a000000018031500000000055534d
  install method   cc02
```

Sample ROM disassembly (Samsung CalmRISC16) with RE annotations

```
#####################################################
# PROC 012462
#####################################################
      0x012462   PUSH      A14[, A14]
      0x012464   PUSH      R1[, R0]
      0x012466   SUB       A15, #02
      0x012468   LD        R0, R2            ;=1
      0x01246a   LD        R1, R3            ;=1
      0x01246c   LD        R2, #ffff
      0x012470   LDW       @[A9+0292], R2    ;ffff
      0x012474   LDW       @[A9+0294], R2    ;ffff
      0x012478   LDW       A10, @[A9+000a]   ;Java SP
      0x01247c   LDW       R2, @[A10 + 0000] ;=0x0b
      0x01247e   LDW       @[A9+006c], R2    ;=0x0b
      0x012482   CMP       EQ, R0, R9
      0x012484   BRF       012492            ;-> jump in our case
      0x012486   LDW       @[A9+0078], R9
      0x01248a   LD        R2, #01
      0x01248c   LDW       @[A9+0076], R2
      0x012490   BRA       0124a8
      0x012492   LDW       A10, @[A9+000a]   ;Java SP
      0x012496   SUB       A10, #04
      0x012498   LDW       R2, @[A10 + 0000] ;=00
      0x01249a   LDW       @[A9+0078], R2    ;=00
      0x01249e   LD        R2, #03
      0x0124a0   JSR       00ee9a            ;load local arg from Java SP (R2 idx)
      0x0124a4   LDW       @[A9+0076], R2    ;SMS-PP data len
      0x0124a8   LDW       A10, @[A9+000a]   ;Java SP
      0x0124ac   SUB       A10, #02
      0x0124ae   LDW       R2, @[A10 + 0000] ;TR addr 074c size 00fc (SMS-PP data buf)
      0x0124b0   LDW       R3, @[A9+0078]    ;=00 (offset)
      0x0124b4   LDW       R10, @[A9+0076]   ;=SMS-PP data len
      0x0124b8   LDW       @[SP + 0002], R10 ;=SMS-PP data len
      0x0124ba   JSR       019d54            ;resolve ptr
      0x0124be   CMP       EQ, R2, R9
      0x0124c0   BRF       0124c6            ;-> error
      0x0124c2   CMP       EQ, R1, R9
      0x0124c4   BRF       0124ca            ;-> always jump
      0x0124c6   LD        R2, #00
      0x0124c8   BRA       0124f4            ;-> jump to the end
```

```
0x0124ca   LDW       R2, @[A9+0076]    ;SMS-PP data len
0x0124ce   CMP       EQ, R2, R9
0x0124d0   BRF       0124d6            ;-> jump if data len > 0
0x0124d2   LD        R2, #00
0x0124d4   BRA       0124f4
0x0124d6   CMP       EQ, R0, R9
0x0124d8   BRF       0124e4            ;-> jump in our case
0x0124da   LDW       R2, @[A9+00f6]
0x0124de   LDW       @[A9+0074], R2
0x0124e2   BRA       0124f2
0x0124e4   LDW       R3, @[A9+0078]    ;=00 (offset)
0x0124e8   LDW       R2, @[A9+0076]    ;=SMS-PP data len
0x0124ec   ADD       R3, R2
0x0124ee   LDW       @[A9+0074], R3    ;=SMS-PP data len
0x0124f2   LD        R2, #01
0x0124f4   ADD       A15, #02
0x0124f6   POP       R0[, R1]
0x0124f8   POP       A14[, A14]
0x0124fa   JMP       A14
```

Native Java methods

```
*****************************************************
*                    NATIVE PROCS                   *
*****************************************************
00019804 native id 0000
00019816 native id 0001
000119e6 native id 0002
00011a0a native id 0003
00011382 native id 0004
000113ce native id 0005
000113a8 native id 0006
000113f2 native id 0007
00011388 native id 0008
0001148e native id 0009
00011848 native id 000a
0001186c native id 000b
000114a0 native id 000c
000115a8 native id 000d
000117b4 native id 000e
000116ec native id 000f
000119c8 native id 0010
000119ae native id 0011
00011a2e native id 0012
00011a34 native id 0013
00019828 native id 0014
00019e88 native id 0015
0000951a native id 0016
0000da36 native id 0017
0000da7a native id 0018
0000da50 native id 0019
0000db0c native id 001a
0000dab8 native id 001b
0000daea native id 001c
000199c8 native id 001d
000093ae native id 001e
0000acf6 native id 001f
00009456 native id 0020
0001984c native id 0021
0001315c native id 0022
00013266 native id 0023
000095c8 native id 0024
0001983a native id 0025
00011152 native id 0026
0001985e native id 0027
00019870 native id 0028
```

```
00019882 native id 0029
00013340 native id 002a
000132e6 native id 002b
00013304 native id 002c
00013360 native id 002d
00011a3c native id 002e
00011a46 native id 002f
00011a7e native id 0030
00011a8c native id 0031
000095c8 native id 0032
0001d06a native id 0033
...
```

Java Card bytecode instructions dispatch

```
*****************************************************
*                      BYTECODES                    *
*****************************************************
0000de44 opcode 00 nop
0000def2 opcode 01 aconst_null
0000ded8 opcode 02 sconst_m1
0000def2 opcode 03 sconst_0
0000def2 opcode 04 sconst_1
0000def2 opcode 05 sconst_2
0000def2 opcode 06 sconst_3
0000def2 opcode 07 sconst_4
0000def2 opcode 08 sconst_5
0000de36 opcode 09 iconst_m1
0000de36 opcode 0a iconst_0
0000de36 opcode 0b iconst_1
0000de36 opcode 0c iconst_2
0000de36 opcode 0d iconst_3
0000de36 opcode 0e iconst_4
0000de36 opcode 0f iconst_5
0000df0e opcode 10 bspush
0000deba opcode 11 sspush
0000de36 opcode 12 bipush
0000de36 opcode 13 sipush
0000de36 opcode 14 iipush
0000de6a opcode 15 aload
0000de6a opcode 16 sload
0000de36 opcode 17 iload
0000de46 opcode 18 aload_0
0000de46 opcode 19 aload_1
0000de46 opcode 1a aload_2
0000de46 opcode 1b aload_3
0000de46 opcode 1c sload_0
0000de46 opcode 1d sload_1
0000de46 opcode 1e sload_2
0000de46 opcode 1f sload_3
0000de36 opcode 20 iload_0
0000de36 opcode 21 iload_1
0000de36 opcode 22 iload_2
0000de36 opcode 23 iload_3
0000ecee opcode 24 aaload
0000ecee opcode 25 baload
0000ecee opcode 26 saload
0000de36 opcode 27 iaload
0000dea6 opcode 28 astore
0000dea6 opcode 29 sstore
0000de36 opcode 2a istore
0000de7e opcode 2b astore_0
0000de7e opcode 2c astore_1
0000de7e opcode 2d astore_2
0000de7e opcode 2e astore_3
0000de7e opcode 2f sstore_0
```

```
0000de7e opcode 30 sstore_1
0000de7e opcode 31 sstore_2
0000de7e opcode 32 sstore_3
0000de36 opcode 33 istore_0
0000de36 opcode 34 istore_1
0000de36 opcode 35 istore_2
0000de36 opcode 36 istore_3
0000ed58 opcode 37 aastore
0000ed58 opcode 38 bastore
0000ed58 opcode 39 sastore
0000de36 opcode 3a iastore
0000de20 opcode 3b pop
0000df22 opcode 3c pop2
...
```

3G USIMERA Prime

Application list and APDU handlers

```
*******************************************************
*                      APPLETS                        *
*******************************************************
[0]
- addr    fb4b06
- aid     a0000000030000
- state   0f
- flags   e0
- type:   native [CARD MANAGER]
- code    f99bf4
- sd      fb4b25
- APDU tables
  [id 0] 2G cmds
    * cla a0 ins f2 code 00fb1851 flags 02:02 [no auth] STATUS
    * cla a0 ins a4 code 00f9adf8 flags 03:03 [no auth] SELECT FILE
    * cla f0 ins fb code 00f9dfbf flags 03:02 [no auth]
    * cla a0 ins c2 code 00f9375d flags 02:03 [no auth] ENVELOPE
    * cla a0 ins 12 code 00fa7c3d flags 02:02 [no auth] FETCH
    * cla a0 ins 14 code 00f94837 flags 02:01 [no auth] TERMINAL RESPONSE
    * cla a0 ins b0 code 00fb1b22 flags 03:02 [no auth] READ BINARY
    * cla a0 ins b2 code 00fb1b15 flags 03:02 [no auth] READ RECORD
    * cla a0 ins d6 code 00fb1b0f flags 03:01 [no auth] UPDATE BINARY
    * cla a0 ins dc code 00f92f9d flags 03:01 [no auth] UPDATE RECORD
    * cla a0 ins 88 code 00f9e7c9 flags 02:03 [no auth] AUTHENTICATE
    * cla a0 ins 20 code 00fa962e flags 03:01 [no auth] VERIFY
    * cla a0 ins 10 code 00fb0b45 flags 02:01 [no auth] TERMINAL PROFILE
    * cla a0 ins a2 code 00fb1a78 flags 03:01 [no auth] SEARCH RECORD
    * cla a0 ins 04 code 00fb1a49 flags 03:01 [no auth] DEACTIVATE FILE
    * cla a0 ins 44 code 00fb1a49 flags 03:01 [no auth] ACTIVATE FILE
    * cla a0 ins 32 code 00fb1af4 flags 03:01 [no auth] INCREASE
    * cla a0 ins 24 code 00fa962e flags 03:91 [no auth] CHANGE PIN
    * cla a0 ins 26 code 00fb1ac1 flags 03:01 [no auth] DISABLE PIN
    * cla a0 ins 28 code 00fb1ac1 flags 03:01 [no auth] ENABLE PIN
    * cla a0 ins 2c code 00fa962e flags 03:01 [no auth] UNBLOCK PIN
    * cla a0 ins c4 code 00faeb8b flags 01:01
    * cla a0 ins fa code 00fb1a36 flags 02:01 [no auth]
  [id 3] 3G cmds
    * cla 80 ins f2 code 00f9af79 flags 02:02 [no auth] STATUS
    * cla 00 ins a4 code 00f94e5e flags 03:03 [no auth] SELECT FILE
    * cla 80 ins c2 code 00f9375d flags 02:01 [no auth] ENVELOPE
    * cla 80 ins 12 code 00fa7c3d flags 02:02 [no auth] FETCH
    * cla 80 ins 14 code 00f94837 flags 02:01 [no auth] TERMINAL RESPONSE
    * cla 00 ins b0 code 00fb134e flags 03:02 [no auth] READ BINARY
    * cla 00 ins b2 code 00fb1467 flags 03:02 [no auth] READ RECORD
    * cla 00 ins a2 code 00f9efef flags 03:03 [no auth] SEARCH RECORD
    * cla 00 ins dc code 00fb140a flags 03:01 [no auth] UPDATE RECORD
    * cla 00 ins d6 code 00fb1330 flags 03:01 [no auth] UPDATE BINARY
```

```
    * cla 80 ins 10 code 00fb0b45 flags 02:01 [no auth] TERMINAL PROFILE
    * cla 00 ins 20 code 00f9e93e flags 03:01 [no auth] VERIFY
    * cla 00 ins e0 code 00fb2175 flags 03:01 [no auth]
    * cla 00 ins e4 code 00f95e37 flags 03:01 [no auth] DELETE
    * cla 80 ins d4 code 00fb2171 flags 03:01 [no auth]
    * cla 80 ins 32 code 00fb13c8 flags 03:03 [no auth] INCREASE
    * cla 00 ins 44 code 00f9476e flags 03:01 [no auth] ACTIVATE FILE
    * cla 00 ins 04 code 00f9476e flags 03:01 [no auth] DEACTIVATE FILE
    * cla 00 ins 24 code 00f9e93e flags 03:01 [no auth] CHANGE PIN
    * cla 00 ins 2c code 00f9e93e flags 03:01 [no auth] UNBLOCK PIN
    * cla 00 ins 26 code 00fa9593 flags 03:01 [no auth] DISABLE PIN
    * cla 00 ins 28 code 00fa9593 flags 03:01 [no auth] ENABLE PIN
  [id 2] AUTH cmds
    * cla f0 ins a8 code 00fb18f2 flags 05:02
    * cla f0 ins 2a code 00fa962e flags 02:81 [no auth] VERIFY KEY
    * cla f0 ins e0 code 00f9db84 flags 03:01 [no auth]
    * cla f0 ins e4 code 00f95d22 flags 03:01 [no auth] DELETE
    * cla f0 ins d4 code 00f95f7e flags 03:01 [no auth]
    * cla 80 ins d4 code 00fb2171 flags 03:01 [no auth]
    * cla f0 ins 22 code 00fa9749 flags 81:01
    * cla 00 ins 84 code 00fac266 flags 02:82 [no auth] GET CHALLENGE
    * cla 00 ins 82 code 00f98d2d flags 02:83 [no auth] EXTERNAL_AUTHENTICATE
    * cla f0 ins 0c code 00fad315 flags 01:01
    * cla f0 ins c4 code 00faeb8b flags 01:01
    * cla 80 ins 0c code 00faff83 flags 02:02 [no auth]
    * cla 80 ins ee code 00fb18b5 flags 10:02 [cm_state<secure]
  [id 1] ADMIN cmds
    * cla f0 ins 06 code 00fb17dc flags 10:01 [cm_state<secure]
    * cla f0 ins 08 code 00fb17dc flags 10:03 [cm_state<secure]
    * cla 80 ins e8 code 00fa7f21 flags 41:a1 LOAD
    * cla 80 ins f2 code 00f9874a flags 05:83 STATUS
    * cla 80 ins ca code 00f97f70 flags 03:83 [no auth] GET DATA
    * cla 00 ins ca code 00f97f70 flags 03:83 [no auth] GET DATA
    * cla 80 ins e6 code 00f8b878 flags 41:a1 INSTALL
    * cla 80 ins e4 code 00f9cd8a flags 41:a1 DELETE
    * cla 80 ins f0 code 00f997d8 flags 41:81 SET STATUS
    * cla f0 ins f2 code 00f9ede1 flags 05:82 STATUS
    * cla 80 ins d8 code 00fad63e flags 81:81 PUT KEY
    * cla f0 ins d8 code 00f99f68 flags 10:81 [cm_state<secure] PUT KEY
    * cla f0 ins 22 code 00fa9749 flags 81:01
    * cla f0 ins f0 code 00fadffd flags 10:81 [cm_state<secure] SET STATUS
    * cla f0 ins 4e code 00faff73 flags 10:01 [cm_state<secure]
    * cla f0 ins 12 code 00fb17f0 flags 10:02 [cm_state<secure] FETCH
...
```

Packages list

```
******************************************************
*                     PACKAGES                       *
******************************************************
[]
- addr    fb4dad
- aid     a0000000620001
- pkgid   04
- def     f827cf
- tr      f89061
- statics f82c0c
- CAP     f82ade
[]
- addr    fb4ddc
- aid     a0000000620002
- pkgid   08
- def     f82a87
- tr      f89093
- statics 0
- CAP     f82c0c
```

```
[]
- addr    fb4e0b
- aid     a0000000620003
- pkgid   0c
- def     f829d9
- tr      f89097
- statics 0
- CAP     f82c42
[]
- addr    fb4e3a
- aid     a0000000620101
- pkgid   10
- def     f82469
- tr      f8909d
- statics f832c4
- CAP     f82c8f
 []
- addr    fb4e69
- aid     a000000062010101
- pkgid   14
- def     f82982
- tr      f8919f
- statics f837db
- CAP     f832c4
[]
- addr    fb4e98
- aid     a0000000620102
- pkgid   18
- def     f826ca
- tr      f891fd
- statics f84675
- CAP     f837db
[]
- addr    fb4ec7
- aid     a0000000620201
- pkgid   1c
- def     f8292b
- tr      f89379
- statics f84aef
- CAP     f84675
[]
- addr    fb509d
- aid     a00000003006011000200010000
- pkgid   20
- def     f82673
- tr      f893bf
- statics 0
- CAP     f84aef
...
```

Extracted packages (files)

```
10600   fb4dad_a0000000620001.dis
997     fb4ddc_a0000000620002.dis
668     fb4e0b_a0000000620003.dis
57742   fb4e3a_a0000000620101.dis
31130   fb4e69_a000000062010101.dis
114293  fb4e98_a0000000620102.dis
30747   fb4ec7_a0000000620201.dis
9719    fb4ef6_a0000000090003ffffffff8910710001.dis
126924  fb4f25_a0000000090003ffffffff8910710002.dis
12355   fb4f54_a0000000090005ffffffff8911000000.dis
9384    fb4f83_a0000000090005ffffffff8911010000.dis
4208    fb4fb2_a0000000090005ffffffff8913000000.dis
68524   fb4fe1_a0000000090005ffffffff8912000000.dis
1990    fb5010_a0000000871005ffffffff8913200000.dis
```

```
518     fb503f_a0000000871005ffffffff8913100000.dis
333     fb506e_a0000000871005ffffffff8914100000.dis
3922    fb509d_a000000030060110002000010000.dis
21849   fb50cc_a000000030060120002014100000.dis
4941    fb50fb_a00000003000011000200189.dis
12378   fb512a_a000000030060120002016100010100.dis
196669  fb5159_a000000030000210002006890000200.dis
5375    fb6e2e_a00000006203010c02.dis
74296   fb6fa8_a00000006203010c01.dis
```

Sample of a package extraction

```
PACKAGE: a00000003000011000200189
 * addr                    fb50fb
 * tl_addr                 f8971f
 * static_data_addr        f86f29
[CLASS 4c00]
 - addr                    f86e88
 - flags                   00
 - token                   0000
 - superclass              0400
 - instanceSize            04
 - FirstReferenceToken     00
 - ReferenceCount          01
 - publicMethodTableBase   01
 - publicMethodTableCount  07
 - packageMethodTableBase  00
 - packageMethodTableCount 00
 - publicMethods
    * [01] 4c05
    * [02] 4c06
    * [03] 4c07
    * [04] 4c08
    * [05] 4c09
    * [06] 4c0a
    * [07] 4c0b
[METHOD 4c01]
 - addr                    6ea6
 - flags                   00
 - token                   0001
 - maxstack                03
 - nargs                   01
 - maxlocals               00
 - codelen                 0008
0000:  18 8c 04 0c ec 87 00 7a  .......z
      6ea6:0000 aload_0
      6ea7:0001 invokespecial 040c   ; null
      6eaa:0004 unk_ec
      6eab:0005 putfield_a 0000
      6ead:0007 return
[METHOD 4c02]
 - addr                    6eb0
 - flags                   00
 - token                   0002
 - maxstack                05
 - nargs                   03
 - maxlocals               00
 - codelen                 000a
0000:  18 8c 04 0c ec 87 00 ed 3b 7a  ........;z
      6eb0:0000 aload_0
      6eb1:0001 invokespecial 040c   ; null
      6eb4:0004 unk_ec
      6eb5:0005 putfield_a 0000
      6eb7:0007 unk_ed
      6eb8:0008 pop
      6eb9:0009 return
```

```
[METHOD 4c03]
 - addr                    6ebc
 - flags                   20  NATIVE [id 02ab ]
 - token                   0003
 - maxstack                00
 - nargs                   09
 - maxlocals               00
 - codelen                 0000
[METHOD 4c04]
 - addr                    6ec0
 - flags                   20  NATIVE [id 01ac ]
 - token                   0004
 - maxstack                00
 - nargs                   05
 - maxlocals               00
 - codelen                 0000
...
```

Native Java methods

```
*******************************************************
*                    NATIVE PROCS                     *
*******************************************************
00fb179e native id 0000
00facfab native id 0001
00facfab native id 0002
00fb170b native id 0003
00facfab native id 0004
00fb1b39 native id 0005
00fadfbe native id 0006
00fb1725 native id 0007
00fa789c native id 0008
00fb177f native id 0009
00fb175d native id 000a
00fb1731 native id 000b
00fb176d native id 000c
00fa4dde native id 000d
00fb1627 native id 000e
00fb1665 native id 000f
00fb1661 native id 0010
00fb165d native id 0011
00fb1669 native id 0012
00facdfa native id 0013
00facdee native id 0014
00fa56e0 native id 0015
00facde2 native id 0016
00fb1772 native id 0017
00fae1a7 native id 0018
00facebe native id 0019
00f9d63b native id 001a
00f9b02c native id 001b
00f9b68b native id 001c

00fb1706 native id 001d
00fb21a0 native id 001e
00fb2226 native id 001f
00f98e94 native id 0020
00fa2b8b native id 0021
00fb1676 native id 0022
00fb166e native id 0023
00facd42 native id 0024
00fb1695 native id 0025
00fb17ac native id 0026
00faca8d native id 0027
00fb1671 native id 0028
00face17 native id 0029
```

```
00fa1ed5 native id 002a
00fa4f8f native id 002b
00fa7502 native id 002c
00fb1710 native id 002d
00fa5005 native id 002e
00fb1671 native id 002f
...
```

Java Card bytecode instructions dispatch

```
******************************************************
*                      BYTECODES                     *
******************************************************
00f8fffc opcode 00 nop
00fa1a5d opcode 01 aconst_null
00fac916 opcode 02 sconst_m1
00fac916 opcode 03 sconst_0
00fac916 opcode 04 sconst_1
00fac916 opcode 05 sconst_2
00fac916 opcode 06 sconst_3
00fac916 opcode 07 sconst_4
00fac916 opcode 08 sconst_5
00fac8d9 opcode 09 iconst_m1
00fac8d9 opcode 0a iconst_0
00fac8d9 opcode 0b iconst_1
00fac8d9 opcode 0c iconst_2
00fac8d9 opcode 0d iconst_3
00fac8d9 opcode 0e iconst_4
00fac8d9 opcode 0f iconst_5
00fac8a4 opcode 10 bspush
00fac77f opcode 11 sspush
00fac8bc opcode 12 bipush
00fac895 opcode 13 sipush
00fac791 opcode 14 iipush
00fac861 opcode 15 aload
00fac861 opcode 16 sload
00fac8ec opcode 17 iload
00fac82b opcode 18 aload_0
00fac82b opcode 19 aload_1
00fac82b opcode 1a aload_2
00fac82b opcode 1b aload_3
00fac84f opcode 1c sload_0
00fac84f opcode 1d sload_1
00fac84f opcode 1e sload_2
00fac84f opcode 1f sload_3
00fac94d opcode 20 iload_0
00fac94d opcode 21 iload_1
00fac94d opcode 22 iload_2
00fac94d opcode 23 iload_3
00fa0f27 opcode 24 aaload
00fa0e9e opcode 25 baload
00fa0f67 opcode 26 saload
00fa0fb1 opcode 27 iaload
00fb2467 opcode 28 astore
00fb2467 opcode 29 sstore
00fb2430 opcode 2a istore
00fb247d opcode 2b astore_0
00fb247d opcode 2c astore_1
00fb247d opcode 2d astore_2
00fb247d opcode 2e astore_3
00fb2490 opcode 2f sstore_0
00fb2490 opcode 30 sstore_1
00fb2490 opcode 31 sstore_2
00fb2490 opcode 32 sstore_3
00fb24b4 opcode 33 istore_0
00fb24b4 opcode 34 istore_1
```

```
00fb24b4 opcode 35 istore_2
00fb24b4 opcode 36 istore_3
00fa09cd opcode 37 aastore
00fa0ee4 opcode 38 bastore
00fa0f84 opcode 39 sastore
00fa0ff1 opcode 3a iastore
00fafe35 opcode 3b pop
00facfbc opcode 3c pop2
00fa4047 opcode 3d dup
00facbbc opcode 3e dup2
00faf12c opcode 3f dup_x
00faf1a4 opcode 40 swap_x
00fa4f7f opcode 41 sadd
00fb2378 opcode 42 iadd
...
```

Security domain information

```
[KSET 16]
- usage     00 []
- msl       00 [No Ciphering, No RC, CC or DS, No counter available]
- APDU mask 00
- id        00
     type      4e [Ki_KEY]
     value     00 11 22 33 44 55 66 77 88 99 aa bb cc dd
- id        08
     type      42 [Op/Opc_KEY]
     value     01 02 03 04 05 06 07 08 09 10 11 12 13 14
- id        0a
     type      4e [Ki_KEY]
     value     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- id        0b
     type      4e [Ki_KEY]
     value     40 00 20 40 60 00
[KSET 1]
- usage     c0 [AUTHENTICATE cmd,VERIFY_KEY cmd]
- msl       02 [No Ciphering, Cryptographic Checksum, No counter available]
- APDU mask ee
- id        00
     type      01 [VERIFY_KEY]
     trycnt    10
     deftrycnt 10
     value     11 11 11 11 11 11 11 11
- id        01
     type      80 [STK KEY]
     trycnt    10
     deftrycnt 10
     value     XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
- id        02
     type      80 [STK KEY]
     trycnt    10
     deftrycnt 10
     value     XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
- id        03
     type      80 [STK KEY]
     trycnt    10
     deftrycnt 10
     value     XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
[KSET 2]
- usage     e0 [AUTHENTICATE cmd,VERIFY_KEY cmd,ENVELOPE cmd]
- msl       02 [No Ciphering, Cryptographic Checksum, No counter available]
- APDU mask ee
- id        01
```

```
    type      80 [STK KEY]
    trycnt    10
    deftrycnt 10
    value     XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
- id        02
    type      80 [STK KEY]
    trycnt    10
    deftrycnt 10
    value     XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
- id        03
    type      80 [STK KEY]
    trycnt    10
    deftrycnt 10
    value     XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
- id        00
    type      01 [VERIFY_KEY]
    trycnt    10
    deftrycnt 10
    value     22 22 22 22 22 22 22 22
...
```

REFERENCES

[1] JAVA CARD TECHNOLOGY
https://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html

[2] Gemalto
https://www.gemalto.com/

About Security Explorations

Security Explorations (http://www.security-explorations.com) is a security company from Poland, providing various services in the area of security and vulnerability research. The company came to life as a result of a true passion of its founder for breaking security of things and analyzing software for security defects. Adam Gowdiak is the company's founder and its CEO. Adam is an experienced Java Virtual Machine hacker, with over 100 security issues uncovered in the Java technology over the recent years. He is also the Argus Hacking Contest co-winner and the man who has put Microsoft Windows to its knees (the original discoverer of MS03-026 / MS Blaster worm bug). He was also the first expert to present a successful and widespread attack against mobile Java platform in 2004.