PV204 Security technologies

Labs: JavaCard platform

Petr Švenda svenda@fi.muni.cz
Faculty of Informatics, Masaryk University

CROCS
Centre for Research on
Cryptography and Security

Laboratory

- Programming basic JavaCard 2.x applet (JavaCard)
  - NetBeans environment, JavaCard convertor
  - jcardsim.org simulator
- Pre-prepared simple communication application
  - Java javax.smartcardio.*;
  - Used already during the lab last week
- Upload and communication with real JavaCard
  - AppletPlayground for quick compile and convert into cap file
  - GlobalPlatformPro tool for upload of cap file to card
  - SimpleAPDU project to communicate with card

Setup updated SimpleAPDU (NetBeans)

- Applets/SimpleApplet.java
- Libraries→Add JAR → lib\jcardsim-2.2.2-all.jar
- Project should now compile
- Run in debug mode
  - Should breakpoint also inside applet code

Extend SimpleAPDU and SimpleApplet

1. Try to send create and send command (any)
2. Try to generate random data (INS_RANDOM)
   – Parse and print response, generate different amount of data (inspect SimpleApplet for what to set)
3. Try to encrypt supplied data
   – Prepare input data and parse output
4. Try to decrypt data received in step 3.
   – Compare with original input data

Troubleshooting – jcardsim simulator

- Don’t forget jcardsim-2.2.2-all.jar in classpath
  - -cp jcardsim-2.2.2-all.jar
- Use debugger – insert breakpoint directly into applet’s method
- Local vs. remote simulator jcardsim
  - Only single card can be simulated as local one (CAD.getCardInterface())
  - We will use and debug only one card (so local is fine)
  - Multiple cards can be used as remote simulators (sockets)

Working with real card - compilation

- AppletPlayground (https://github.com/martinpaljak/AppletPlayground)
  - – Copy your source code into SimpleApplet folder
- Run `‘ant simpleapplet’` to compile and convert
  - – simpleapplet.cap is produced (binary for real card)

Working with real card - upload

- GlobalPlatformPro (http://github.com/martinpaljak/GlobalPlatformPro)
- Remove previous installation of applet
  - If exists (use gp --list to obtain list of cards)
  - gp -delete 010203040506 -deletedeps -verbose -all
- Upload applet to real card
  - gp -install simpleapplet.cap --param 00 -verbose

Homework – Secure HOTP card

- Create secure Hash-based One-Time Password (HOTP) applet and corresponding PC application
  - Applet will accept new secret key *K* later used to produce OTP (infrequent)
  - Applet receives input challenge *C* from PC and produce corresponding OTP code using C, K and suitable has-based construction (frequent)
  - OTP code is provided only after PIN verification (OwnerPIN)
    - User can set own PIN (decide what to do with previous key K)
- Produce short (1xA4) text description of solution
  - Describe your design, no need to conform to RFC4226 (standardized HOTP)
- Measure the speed of OTP code generation
  - On simulator (required), On real card [+1 bonus point]
- Submit **before 16.3. 23:59** into IS HW vault
  - Soft deadline: -1.5 points for every started 24 hours

Homework – bonus

- Bonus (up to +5 points):
  - implement bulk encryption with AES and on-card key
  - Key is generated randomly (separate command)
  - Data send in/out (APDU)
  - Encrypted/decrypted by AES in CBC mode (enc/dec mode specified in P1 parameter)
  - Measure speed you can achieve (compare with https://www.fi.muni.cz/~xsvenda/jcalgtest/)
  - Which optimization had biggest speed impact?
- Submit before: 23.3. 23:59 (soft deadline for bonus part)