PV204 Security technologies

Labs: Secure authentication and authorizat

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

CS
Centre for Research on Cryptography and Security

Laboratory

1. Uploading SimpleApplet into real smart card
   - Process
   - Authorization of upload request
   - What to do be aware (blocking card etc.)
2. JavaCard implementation of HOTP/TOTP
   - https://github.com/Yubico/ykneo-oath
   - Uploading compiled applet, using desktop application
   - Inspection of application code

What is necessary - prerequisities

- Java SDK installed
  - JAVA_HOME environment variable set
  - JAVA_HOME = c:\Program Files\Java\jdk1.8.0_72\
- Apache Ant installed
  - Path to ant binary set in PATH environment variable
  - PATH += c:\Program Files (x86)\apache-maven-3.3.9\bin\
- Restart cmd console after setting these variables

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

Be aware – real card can be blocked

- Too many unsuccessful authentication requests

```
>gp --list -debug
# Detected readers from SunPCSC
[*] Alcor Micro USB Smart Card Reader 0
SCardConnect("Alcor Micro USB Smart Card Reader 0", T=*) -> T=0, 3BF71800008031F
E45736674652D6E66C4
SCardBeginTransaction("Alcor Micro USB Smart Card Reader 0")
A>> T=0 (4+0000) 00A40400 00
A<< (0018+2) (56ms) 6F108408A0000000030000000A5049F6501FF 9000
A>> T=0 (4+0008) 80500000 08 6265E168FB2639C1
A<< (0028+2) (118ms) 000031269600975431740102001035 95AC1420213D2969EA8B8C41F3 9
00
openkms.gp.GPException: STRICT WARNING: Card cryptogram invalid!
Card: 3D2969EA8B8C41F3
Host: DB1E6E1E71958A15
!!! DO NOT RE-TRY THE SAME COMMAND/KEYS OR YOU MAY BRICK YOUR CARD !!!
        at openkms.gp.GlobalPlatform.printStrictWarning(GlobalPlatform.java:156)

        at openkms.gp.GlobalPlatform.openSecureChannel(GlobalPlatform.java:471)
        at openkms.gp.GPTool.main(GPTool.java:348)
```

Be aware – real card can be blocked

- Don’t write script that executes many authentications at once (cycle, multiple commands)
- If unsuccessful one/two authentication is detected, then as for help, please!!!

YUBIKEY OAUTH

Yubikey OATH applet

- Yubikey OATH applet
  - https://github.com/Yubico/ykneo-oath/
  - Already included in AppletPlayground
- Desktop OAUTH utility
  - https://developers.yubico.com/yubioath-desktop/Releases/
- Change name of reader
  - File → Settings → Card reader name
  - Insert your reader name (use gp to obtain it)
    - E.g.,Gemplus USB Key Smart Card Reader 0

Add new secret File → Add

- Credential name: *anything*
- Secret key: *key shared with verification server*
  - Base32 encoding (a-z0-9=)
  - E.g., *password*=
- Try HOTP option (rfc4226)
- Try TOTP option (rfc6238)
- What difference you can see?
- What is advantage/disadvantage of TOTP to HOTP

Testing OATH applet

- YkneoOathTest project
- No main function, execution via unit tests
- Add JUnit library
  - Libraries → RClick → JUnit 4.10
  - YkneoOathTest should now compile
- Run test you wish
  - Place breakpoint into target test
  - RClick → Debug focused test method for run
- Can you localize functions responsible for TOTP/HOTP computations?

Homework –bonus from last week

- 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: 29.3. 6am (soft deadline for bonus part)