MTAT.07.017
Applied Cryptography

Course Projects

Juri Hudolejev
University of Tartu
Spring 2011

Course Project

Not required – but strongly recommended

20% of final grade

- Home tasks give at most 80%

Solution Presentation: 2011-05-27 (last week)

- Also during exam session, if needed

Project Requirements

Team: 1 to 4 people (depending on project)

Working solution should be presented

- Concepts are awesome but will not get a grade

Programming language and platform – your choice

Some open-source license strongly recommended

Topics

BouncyCastle library related work

Trusted timestamping

Estonian (maybe some other) ID-cards

Other topics

Project Proposals: EstEID

Implement DigiDoc client (in Java)

- Should be able to read ID-card data
- Should be able to sign documents
- Should be able to verify EstEID signatures
- Should run on Linux / OS X / Windows

Optionally, use some other national ID-cards

Project Proposals: EstEID

Implement signing plugin for Firefox or Chrome

- Currently, old applet is used in several banks
- Option 1: native plugin NPAPI, maybe XPCOM
- Option 2: plugin in Java
- Option 3: Java WebStart application

Optionally, use some other national ID-cards

Project Proposals: Timestamping

Implement timestamping protocol that would use `TimestampedData` container instead of regular RFC 3161 timestamps

- TSA (standalone app or webserver component)
- Client API (methods to handle requests and responses)
- Command-line client
- Should do full timestamp validation
- You should demonstrate client-server communication

Project Proposals: Timestamping

Produce a mortal-oriented description of hash-linked timestamp verification process

- Spreadsheet or **simple** Python/BASIC script to verify hash chains and hash trees

Requested by GuardTime

Project Proposals: Timestamping

Embed a timestamp into another data format

- Timestamp integrations with PDF and PNG exist
- Research a possibility to embed a timestamp into JPEG images
- Provide a proof-of-concept implementation

Requested by GuardTime

Project Proposals: BouncyCastle

Implement **`DigestedData`** container handling classes for **`provider`** and **`cms`** libraries

- Should be similar to other ASN.1 structures in **`provider`** library
- Should use standard generators and validators from **`cms`** library

Project Proposals: BouncyCastle

Improve documentation

- Choose some class or package that lacks documentation – well, almost any qualifies (:
- Research the related RFCs
- Produce valid and sensible Javadoc and usage examples with explanations
- Publish that (public repository is fine)

Note on BouncyCastle tasks (Java)

Your solution should use latest BouncyCastle Java API – version 1.46 as for today

API version 2 is in active development

It is recommended that your project is compatible with the API version 2 too

Bonus

Every critical or major issue of BouncyCastle library (either Java or C#) that is

- discovered by you,
- properly reported in issue tracker, and
- accepted by library authors

can already be considered a completed project.

Issue tracker: http://www.bouncycastle.org/jira/

Project Proposals: Other

Questions?

•

Registering the topic, questions:

Contact me personally or via juri@ut.ee

Deadline to register project topic:

2011-04-30

Next lab session:

Friday 2011-04-29 **08:30** EEST @ Liivi 2 - 205