Semestral Project

PV204 – Security Technologies

Spring 2024

CRoCS

Centre for Research on
Cryptography and Security

Project introduction

- Teams of three people
- One of three topics
  - JavaCard secret storage
  - Message board secured by TPM
  - Trusted timestamping server with threshold signing key
- Four project phases (each ~3 weeks)
- Up to 30 points awarded
  - Bonus points possible for exceptional contribution
- Questions
  - By email xdufka1@fi.muni.cz
  - Consultation possible after a request
- Phase deadlines are strict (one day extension possible for 20% point penalization)

Teamwork rules

- All team members are expected to contribute equally
- Do not split work sequentially
  - Your work should not depend on someone else doing their work
- Everyone should work with the selected technology
  - It is not acceptable to just implement a website
  - It is not acceptable to just prepare presentations and reports
- All team members should participate in the work on reports/presentations
- After each phase state who worked on which part
  - This should be reflected in git commits

Project topics

JavaCard secret storage

- Implement a JavaCard applet for storing secrets with functionality:
  - Storage of secrets (name-value pairs)
  - Listing of available secret names
  - Revealing the value of a requested secret (only when the correct PIN is provided)
  - PIN change
- Implement an application for interacting with the applet
  - An application that will be able to query all the required functionality
- Establish a secure channel for communication with the smartcard
- Resources
  - https://github.com/crocs-muni/javacard-gradle-template-edu
  - https://docs.oracle.com/javacard/3.0.5/api/index.html
  - https://github.com/licel/jcardsim

Message board secured by TPM

- Implement a simple message board to which clients can post messages
- Clients authenticate to the board with their TPM
  - Register on the first interaction
    - At this point only the server needs to be authenticated (e.g., known certificate)
  - Further communication is fully authenticated
    - Both sides need to be authenticated (the server does not need to use TPM)
    - The client should not be able to connect from a different device after the registration (e.g., remote attestation)
- Resources
  - https://github.com/tpm2-software/tpm2-tools
  - https://github.com/tpm2-software/tpm2-tss

Trusted timestamping server with threshold signing key

- Implement a trusted timestamping server
  - Generate a signing key and output the corresponding public key
  - Provide an interface for submitting documents for timestamping
  - Output timestamped documents signed with its private key
- Use multi-party computation to avoid a single point of failure
  - Distribute the private key shares among multiple servers
  - Use threshold signing scheme (2-of-3) to create the signature
- Implement an application for submitting documents and verifying timestamps
- Resources
  - https://github.com/bnb-chain/tss-lib
  - https://github.com/ZcashFoundation/frost

Project schedule

Project schedule

- Phase I – deadline 3. 3. 2024
  - Teams of 3 people, project topic, GitHub repository
- Phase II – deadline 24. 3. 2024 (5 points)
  - Project design, the first part of the implementation, report
- Phase III – deadline 14. 4. 2024 (10 points)
  - Final implementation, recording of a project presentation
- Phase IV – deadline 12. 5. 2024 (15 points)
  - Report of analysis of another team's project, presentation at the last lecture

Phase I

- Form teams of 3 people
- Decide on a project topic
  - Prepare development environment for the selected technology stack
  - Make sure everyone in your team can use it
- Create a repository on GitHub
  - If you chose private repository, invite `dufkan` as a collaborator with read access
- Write an email to xdufka1@fi.muni.cz containing:
  - Team member names + GitHub usernames
  - The selected project topic
  - A link to your GitHub repository
- Deadline: 3. 3. 2024

Phase II

- Study the selected security technology
- Design your project
  - Describe the architecture and explain your choices (what attacks is it preventing, …)
- Start working on the implementation
  - You should have a prototype ready by the end of this phase
- Prepare 3-4 page report
  - Brief description of the selected security technology
  - Project design (architecture, intended use of the selected technology, design choices, …)
  - Current progress (+ individual contribution of each team member)
- Deadline: 24. 3. 2024
  - Submit the report to IS

Phase III

- Finalize the implementation
- Prepare and record a presentation of your project (10 minutes)
  - Project design
  - Overview of the implementation (+ individual contribution of each team member)
  - Issues that you had during the work on the project and how did you solve them
  - Application demonstration
- Deadline: 14. 4. 2024
  - Submit the presentation slides and the recording to IS
  - Submission from this phase will be made available to reviewing teams

Phase IV

- Perform security analysis of assigned teams’ project
  - Search for issues both in the design and the implementation
  - Discuss what attacks the issues can lead to
  - Try to exploit the discovered vulnerabilities
  - Prepare a report of your analysis (3+ pages)
- Prepare a presentation for the last lecture (~8 minutes)
  - Description of the analyzed project
  - Design and implementation issues (at least 1 of each)
  - Possible attacks due to the issues
  - Realized attacks (try at least 1)
- Deadline: 12. 5. 2024
  - Upload the report and the presentation slides to IS