Semestral Project

PV204 – Security Technologies

Spring 2023

CRoCS

Centre for Research on
Cryptography and Security

Project introduction

- Teams of three people
- One of four topics
  - JavaCard secret storage
  - Message board secured by Noise protocol and TPM
  - SGX device-locked password manager
  - 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
  - Available for consultations on Thu 12:00-13:00 in A403

JavaCard secret storage

- Implement a JavaCard applet for storing secrets with functionality:
  - Storage of secrets (name-value pairs)
  - Listing of available secret names
  - Reveal 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 required functionality
- Establish secure channel between smartcard and host for communication
- 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 Noise and TPM

- Implement a simple message board to which clients can post messages
- Secure the connection to server via Noise protocol
- Client authentication using TPM
  - Register on the first interaction
    - At this point only the server needs to be authenticated (e.g., known certificate)
  - Further communication is authenticated using TPM
    - Both sides need to be authenticated
    - Changes to the client device should be detectable
- Resources
  - https://www.noiseprotocol.org/
  - https://github.com/tpm2-software/tpm2-tools

SGX device-locked password manager

- Implement a simple password manager that relies on SGX with functionality:
  - Storing credentials (website name, username, password)
  - Reading credentials for a selected website
  - Listing all stored webservice names
  - Changing master password
- Provide a user interface that demonstrates all the functionality
- The password vault should not be decryptable on another device
  - Master password is only optional for additional security
  - See SGX sealing
- Resources
  - https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html
  - https://github.com/intel/linux-sgx

Trusted timestamping server with threshold signing key

- Implement a trusted timestamping server that secures its key via MPC
  - 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 single point of failure
  - Distribute the private key shares among multiple servers
  - Use threshold signing scheme (2-of-3) to create the signature
- Provide an interface for interacting with the server
- Resources
  - https://github.com/ZenGo-X/multi-party-ecdsa
  - https://github.com/isislovecruft/frost-dalek

Project phase outputs

- Phase I – deadline 3rd week
  - Teams of 3 people, project topic, GitHub repository
- Phase II – deadline 7th week (5 points)
  - Project design, the first part of the implementation, report
- Phase III – deadline 10th week (10 points)
  - Final implementation, recording of a project presentation
- Phase IV – deadline 14th week (15 points)
  - Report of analysis of another team's project, presentation at the last lecture

Phase I

- Form teams of 3 people
- Decide on project topic
  - Prepare development environment for the selected technology stack
  - Make sure everyone in your team can use it
- Create a **private** repository on GitHub
  - Invite `dufkan` as a reader
- Write an email to xdufka1@fi.muni.cz containing:
  - Team member names + GitHub usernames
  - Selected project topic
  - Link to the GitHub repository
- Deadline: 26. 2. 2023

Phase II

- Study the selected technology stack
- Design your project
  - Describe the architecture of your project
- 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 selected technologies
  - How you intend to use the technologies in your project
  - Overall project design
  - Current progress
- Deadline: 26. 3. 2023
  - Submit the report to IS

Phase III

- Finalize the implementation
- Prepare and record a presentation of your project (10 minutes)
  - Project design
  - Implementation
  - Issues and solutions
  - Application demonstration
- Deadline: 16. 4. 2023
  - Submit 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 discovered vulnerabilities
  - Prepare a report of your analysis
- Prepare a presentation for the last lecture (~8 minutes)
  - Analyzed project description
  - Design and implementation issues (at least 1 of each)
  - Possible attacks due to the issues
  - Realized attacks (try at least 1)
- Deadline: 14. 5. 2023
  - Upload report and presentation slides to IS