Semestral Project

PV204 – Security Technologies

Spring 2021

CRoCS

Centre for Research on Cryptography and Security

Introduction

- Team of three people
- Selection of a topic
  - PSBT Parser on JavaCard
  - Secure Channel with Noise Protocol and TPM
  - SGX Device-Locked Password Manager
- Four phases (3 weeks each)
- Up to 30 points awarded
  - Bonus points possible for exceptional contribution
- Questions
  - Anytime by email: xdufka1@fi.muni.cz
  - Online consultation possible upon request

PSBT Parser on JavaCards

- Implement parser of Partially Signed Bitcoin Transactions Format (PSBT) for JavaCard
  - JavaCard library
  - Standalone applet (for demonstration)
  - Optionally command-line interface for sending APDU
- Given a PSBT transaction, the applet should be able to
  - Parse the PSBT and store the result
  - Respond to queries on the parsed PSBT
    - Number of inputs/outputs
    - Value of the transaction inputs/outputs
    - …
  - Clear the context

Resources

- PSBT Specification
  - https://en.bitcoin.it/wiki/BIP_0174
- JavaCard API
  - https://docs.oracle.com/javacard/3.0.5/api/index.html
- JavaCard Simulator
  - https://github.com/licel/jcardsim
- JavaCard Gradle Template
  - https://github.com/crocs-muni/javacard-gradle-template-edu
  - Remote access to physical cards can be provided

Secure Channel with Noise Protocol and TPM

- Establish forward-secure channel between client and server over TCP/IP with Noise protocol
- Initial registration
  - Client registers to server, authentication is not required
    - Preshared value can be set
- Subsequent communication
  - Server and client need to be authenticated
  - Changes to client should be detected (TPM)
    - User should be informed
    - Secure channel should not be established
- Implement some auxiliary functionality
  - E.g., simple message board

Resources

- Noise Protocol Framework
  - http://www.noiseprotocol.org/
- TPM2 Tools
  - https://github.com/tpm2-software/tpm2-tools

SGX Device-Locked Password Manager

- Initialize a password vault within an enclave
  - Optionally protected by a master password
- Securely store the password vault (SGX sealing)
- Implement enclave interface for (at least):
  - Storing credentials (username and password for a service)
  - Receiving credentials for a service
  - Listing all stored services
  - Changing master password
- Provide suitable (command-line) interface
  - Can fully utilize implemented enclave interface

Resources

- SGX 101
  - https://sgx101.gitbook.io/sgx101/
- Intel SGX Documentation
  - https://software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html
- Linux SGX SDK
  - https://github.com/intel/linux-sgx
- OpenSGX (SGX Emulator)
  - https://github.com/sslab-gatech/opensgx

Project phases

- Phase I – deadline 3rd week
  - Form teams of 3 people
  - Decide on project
- Phase II – deadline 6th week
  - Study the selected technology stack
  - Design project
  - Start implementation
  - Report (4 A4), brief overview at seminar group (5 minutes)
- Phase III – deadline 9th week
  - Finalize implementation
  - Presentation for seminar group (5-7 minutes)
- Phase IV – deadline 13th week
  - Analyze project of another group
  - Final presentation for lecture (10 minutes)

Phase I

- Form teams of 3 people
- Create GitHub repository for your project
  - Choose a good name
  - Can be private
- Prepare development environment for your project
  - Try JavaCard/TPM/SGX Hello world
  - Make sure it works for everyone in your team
- Write mail to xdufka1@fi.muni.cz containing:
  - Team member names
  - Link to GitHub repository
    - Add `dufkan` as reader if you choose private repository
- Deadline Thursday 18. 3. 2021

Phase II

- Study the selected technology stack
- Design your project
  - Prepare high-level design of your project
- Start the implementation
  - You should have a prototype ready by the end of this phase
- Prepare 4 A4 report of project design, present at your seminar (5 min)
  - Brief description of used technologies
  - How do you intend to use the technologies
  - Project design
  - Work undergone so far
  - Envisioned issues
- Deadline Thursday 8. 4. 2021

Phase III

- Finalize implementation
- Prepare presentation for seminar (5-7 minutes)
  - Project design
  - Implementation
  - Issues and solutions
  - Short (live) demo
- Discussion of the presentation
  - Design decisions
  - Possible attacks
- Assignment of projects for the next phase
- Deadline Thursday 29. 4. 2021

Phase IV

- Perform security analysis of another team’s project
  - Search for issues in design and implementation
  - Discuss what attacks the issues can lead to
  - Try to exploit discovered vulnerabilities
  - Prepare a report of your analysis
- Prepare presentation (slides) for the last lecture (10 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 Monday 24. 5. 2021 16:00

Phase IV – Ideas to check

- PSBT Parser on JavaCards
  - Can the applet handle large packets?
  - Is memory usage limited by the implementation?
  - Can the applet be tricked to parse incorrect information?
- Secure Channel with Noise Protocol and TPM
  - Is the channel correctly established?
  - Is the selected Noise pattern appropriate for this application?
  - Is TPM utilized during channel establishment, separately, or not at all?
- SGX Device-Locked Password Manager
  - Is the enclave separation used correctly?
  - How is the master password stored?
  - Is SGX sealing used to store password vault persistently?