Semestral Project

PV204 – Security Technologies

Spring 2022

CROCS

Centre for Research on Cryptography and Security

Introduction

- Team of three people
- Selection of a topic
  - JavaCard Secret Storage
  - Secure Channel with Noise Protocol and TPM
  - MPC Trusted Timestamp Server
  - *Special:* Proprietary NFC communication analysis
  - Your Own Topic (JavaCard, TPM, MPC, SGX, Noise, Cryptocurrency wallets …)
- Four phases (~3 weeks each)
- Up to 30 points awarded
  - Bonus points possible for exceptional contribution
- Questions
  - Anytime by email: xdufka1@fi.muni.cz
  - Consultation possible upon request

Project phases

- Phase I – deadline 3rd week
  - Form teams of 3 people
  - Decide on project and study the selected technology stack
  - Setup GitHub repository
- Phase II – deadline 6th week
  - Design project
  - Start implementation
  - Report (3-4 A4)
- Phase III – deadline 9th week
  - Finalize implementation
  - Recording and live presentation of your project (5-7 minutes)
- Phase IV – deadline 13th week
  - Analyze project of another group
  - Final presentation at the last lecture (10 minutes)

JavaCard Secret Storage

- Implement an applet for storing secrets on JavaCard
  - PIN is required to access the storage
  - Store secrets as key-value pairs
  - List available keys
  - Reveal value for a requested key
  - If DURESS_PIN is entered instead of PIN, erase all stored secrets
- Implement application for interacting with the smartcard
- Secure the communication with the card
  - e.g., authenticated ECDH
- Resources
  - https://docs.oracle.com/javacard/3.0.5/api/index.html
  - https://github.com/licel/jcardsim
  - https://github.com/crocs-muni/javacard-gradle-template-edu

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
- 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
- Provide interface for storing short messages on the server
- Resources
  - http://www.noiseprotocol.org/
  - https://github.com/tpm2-software/tpm2-tools

MPC Trusted Timestamp Server

- Implement a trusted timestamping server that secures its signing key via multi-party computation
- The trusted timestamping server will
  - Publish its public key
  - Provide interface through which users can submit a document 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 to create the signatures
- Resources
  - https://github.com/ZenGo-X/multi-party-ecdsa
  - https://github.com/isislovecruft/frost-dalek

Proprietary NFC Communication Analysis

- Capture NFC communication between proprietary smartphone app and a smartcard
  - Analyze the messages a reverse engineer the protocol
- Provide open-source implementation of the application side
  - PC application via NFC reader or Mobile app via phone's NFC stack
- Demonstrate its functionality with the smartcard
- Resources
  - If you are interested, contact us and we can provide necessary hardware

Your Own Topic

- Come up with your own topic using technologies discussed in this course
  - JavaCard, TPM, MPC, SGX, Noise, Cryptocurrency wallets, …
- Opportunity to start an interesting open-source project
- Requirements
  - The project idea must be well specified
  - Submit the project proposal by the end of the 2nd week
  - Explicit approval of the topic is needed

Phase I

- Form teams of 3 people
- Decide on project and study the selected technology stack
  - Prepare development environment for your project
  - Make sure it works for everyone in your team
- Create GitHub repository for your project
  - Agree on a unique name
- Write mail to xdufka1@fi.muni.cz containing:
  - Team member names
  - Selected project
  - Link to GitHub repository
    - Add `dufkan` as reader if you choose private repository
- Deadline Tuesday 1. 3. 2022 12:00

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 3-4 A4 report of project design
  - Brief description of used technologies
  - How do you intend to use the technologies
  - Project design
  - Current progress
  - Encountered obstacles
- Deadline Tuesday 22. 3. 2022 12:00

Phase III

- Finalize implementation
- Prepare and record a presentation of your project (5-7 minutes)
  - Project design
  - Implementation
  - Issues and solutions
  - Short (live) demo
- Discussion of the presentation
  - Design decisions
  - Possible attacks
- Assignment of other team projects for the next phase
- Deadline Tuesday 12. 4. 2022 12:00

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 a presentation 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 Tuesday 10. 5. 2022 12:00