Semestral Project

PV204 – Security Technologies

Spring 2025

CRoCS

Centre for Research on
Cryptography and Security

Project introduction

- Teams of three people
- Topics chosen by teams, but related to Nostr
- Five project phases
- Up to 30 points awarded
  - Bonus points possible for exceptional contribution
- Questions
  - By email gavenda@mail.muni.cz
  - Consultation possible after a request
- Phase deadlines are strict (one day extension possible for 20% point penalization)
- More detailed description available here

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

Note on LLM chatbots (ChatGPT, etc.)

- You are **allowed** to use them
- Document its usage (prompts you used, e.g., in the form of shared chatbot conversations)
- Verify the responses obtained
- Cut down the clutter of the produced text and code.

Project topics

- The topic for this year is **Nostr**, so each project must incorporate Nostr in some way.
- Suggested technologies:
  - **Threshold cryptography** (e.g. signing Nostr Events using threshold signatures)
  - **Java Card** (e.g., signing Nostr Events with hierarchical key derivation by tapping NFC card to mobile phone)
  - **TPM** (e.g., Nostr Events interaction based on TPM measured boot PCR values)
  - **Noise protocol** (e.g., extensions of Noise secure channel establishment based on web of trust extracted from Nostr)

Project schedule

Project schedule

- Phase I – deadline 2. 3. 2025
  - Teams of 3 people, **project topic**, GitHub repository
- Phase II – deadline 21. 3. 2025 (5 points)
  - **Project design**, the first part of the implementation, report
- Phase III – deadline 13. 4. 2025 (10 points)
  - **Final implementation**, recording of a project presentation
- Phase IV – deadline 11. 5. 2024 (10 points)
  - Report of **analysis of another team's project**, presentation at the last lecture
- Phase V (5 points)
  - Discussion about **mitigations of the discovered problems**

Phase I

- Form teams of 3 people
- Decide on a project topic
  - Have the topic ready for the second seminar on 27. 2. 2025
  - Prepare development environment for the selected technology stack
- Create a repository on GitHub
  - If you chose private repository, invite `jirigav` as a collaborator with read access
- Write an email to gavenda@mail.muni.cz containing:
  - Team member names + GitHub usernames
  - The description of the selected project topic
  - A link to your GitHub repository
- Deadline: 2. 3. 2025

Phase II

- Study the selected security technology
- Design your project
  - Describe the architecture and explain your choices
- 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: 21. 3. 2025
  - 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: 13. 4. 2025
  - Submit the presentation slides and the recording to IS
  - Submission from this phase will be made available to reviewing teams
  - During the 9th week, the team must be available to answer questions of the break-it team, fix minor issues (e.g. in make files) and help them to run the project.

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: 11. 5. 2025
  - Upload the report and the presentation slides to IS

Phase V

- Choose one vulnerability or design problem discovered by the reviewer team
- During the exam you will have to:
  - Describe this vulnerability or problem
  - Propose a solution and describe how the solution can mitigate the vulnerability/problem