



# Assignment 1

**Submission Sunday, April 15th, 12:59pm CEST via email to [sarah.prange@hm.edu](mailto:sarah.prange@hm.edu)**

## Exercise 1-1 Reading task

Please read the following paper: [Why Johnny Can't Encrypt: A Usability Study of PGP](https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten.pdf)  
(available at [https://www.usenix.org/legacy/events/sec99/full\\_papers/whitten/whitten.pdf](https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten.pdf))

## Exercise 1-2 Review of Authentication Apps

In this exercise, you are asked to:

- a) Review Google's Play store and/or Apple's App store for authentication apps.
- b) Choose one of the offered authentication apps and install it on your phone.
- c) Use it over several days.
- d) Perform an expert evaluation of the app, similar to the assessment of PGP encryption in the paper you read as part of Exercise 1-1. In particular you should:
  - Identify the "pain points" of installing and using it.
  - Take the role of an attacker and try to exploit vulnerabilities in the app. These vulnerabilities could be, for example, uninstalling the app, working around the authentication by exploiting a certain bug, etc.
- e) Assess the security of the approach against one of the threat models we discussed in the lecture (smudge attacks, guessing attacks, shoulder surfing, thermal attacks, etc.) in a small user study. In particular, you should:
  - Think about a suitable study design. Which data do you need and how are you going to collect it?
  - Think about a suitable procedure. What are the tasks participants need to perform? In which settings will you run the study?
  - Conduct the study with at least 5 participants.
  - Analyse and interpret your results. What do you learn from them?
- f) Assess the security of the approach against other threat models.
- g) Discuss how could the app/concept be improved to account for the (problematic) threat models?
- h) Summarize your findings in approximately two A4 pages
- i) *Optional:* write a review for your tested app in the app store.

### Submissions:

Submit your solution as a PDF, named "assignment1\_<your\_last\_name>.pdf through email to [sarah.prange@hm.edu](mailto:sarah.prange@hm.edu) with subject "Assignment 1". The submission deadline is Sunday, April 15th, 12:59pm CEST.