

Assignment 2

INSE 6150: Security Evaluation Methodologies

Due: **March 16**. Hand in during class.

Updates:

Correction 1 (Mar 8): Updated due date and added that assignments should be typed out (rather than handwritten)

Other potential mistakes? Please email j.clark@concordia.ca

*Assignments are to be completed individually. Any reference to external material should be cited. Each student has available one slip day for use on one, and only one, assignment of his/her choosing. Using the slip day allows the assignment to be submitted at noon on the **Friday** that follows the due date without penalty (in this case, assignments must be placed in my mailbox in EV 7.640). Late assignments will not otherwise be accepted (exceptions made for medical certificates).*

Usability Study (10 marks)

In this assignment, you will perform a usability study using the cognitive walkthrough method, as done in class.

As a first step, choose a security or privacy tool (software works best but it can be hardware or physical if you want) that requires the users to interact with it in order to get the security benefit of using it. Like in Assignment 1, the topic is wide open and can be anything. Give a lot of consideration to choosing a good topic.

Once you have a topic, come up with a comprehensive list of criteria or heuristics for each step of the walkthrough. You should use the list from class as a starting point, and adapt it to fit your chosen tool more specifically as needed. Next list the core tasks that the user should perform to benefit from the tool. You can list more tasks than you will evaluate, since the assignment is limited in scope. Choose one or two core tasks (or you can look at the same core task in different tools) to use for your evaluation and briefly justify the reason for the task(s) you choose.

Perform the evaluation and write up an explanation listing how well the security tool matches the heuristics. The report should be a maximum of 5 pages (and you can include one extra page of screenshots or pictures if you want as an appendix). Please type up the report rather than handwriting it.

Some further resources:

More on the cognitive walkthrough method: <http://hcibib.org/tcuid/chap-4.html#4-1>

Applied to PGP: <http://www.gaudior.net/alma/johnny.pdf>

Applied to Tor: http://users.encs.concordia.ca/~clark/papers/2007_soups.pdf

Applied to Bitcoin: http://users.encs.concordia.ca/~clark/papers/2015_usec.pdf

Topics that intersect with anonymizing technologies (e.g., proxies, vpns, etc.) are not eligible for this assignment.