

## Final essay

**Goal:** For this essay, I'd like you to delve more deeply into a topic related to one or two areas - cryptography and issues in its use from a computer science perspective, or programming languages and security. Either is a great topic, so I'm going to let you choose the one you are most interested in.

**Assignment:** Choose one of the following options:

- Read the article “Lessons learned in implementing and deploying crypto software”, from the 2002 Usenix. Beyond reading this paper, find some more recent examples of issues connected to cryptography. Do you think the issues described by the author remain a problem in the computer industry? If it is still an issue, what steps need to be taken in order to reduce such issues? If it is not, what steps has the industry taken to solve these issues, and what new ones have arisen?
- Consider your favorite programming language from a security perspective. Are there attacks written in or well known security issues with the language? (Suggestion: google “top programming languages vulnerabilities” before you answer this - I've actually read up on this, so don't just claim that there are none, since almost every language has some!) What security implications exist, either due to language design choices or due to poor programming practice in the language? Do you consider any such issues to be a serious problem, and (whether serious or minor) what would you like to alter in order to address any issues?

Note: If you choose this topic, note that you may not write on either C or C++ for this essay. We have considered them plenty in class, so I'd like you to focus on other languages. Also, you can consider me as your target audience, so I'm quite familiar with basic programming issues and programming language design, but not necessarily with any given programming language. You'll need to include enough code discussion or snippets in order to illustrate some of the security issues, although I'm not really looking for pages of code - higher level descriptions of the issues are fine.

**Details:** For this assignment, please aim for concise yet informative - 1-2 pages should be more than enough to accomplish this. I will expect at least reputable 3 sources, with proper citations for relevant facts from those references. Of course, you are welcome to use web or book resources of any type; just be sure to use at least 3 **reputable** sources and include them in your bibliography.

Please note that since both of these topics have at least some component that is opinion-based, I expect a clear thesis statement which summarizes your opinion or finding, which must then be supported by relevant facts and reasonable arguments in the body of your essay.