CSC84400: Privacy, Security and Usability

Homework 2

Print your homework out and submit it in person at the start of class on Monday, February 25. Homework will not be accepted late.

Pick a tool from Wikipedia's list [1] of encryption tools (see blue box labelled "Cryptographic software" near the bottom). Download and install (or, if applicable, simply enable) the tool you chose. Adapting similar approaches as the "Why Johnny Can't Encrypt" paper [2] , Perform an expert evaluation of the tool (similarly to the approach introduced in the "Why Johnny Can't Encrypt" paper). You should turn in a summary which covers the following points::

- Your choice of tools and a description of the steps you took in your expert evaluation. Explain your methodology and the reasons for choosing it.
- Did you detect any usability flaws that were originally identified in the above paper [2] in the tools you tested? If so, describe those flaws.
- Are there any additional usability flaws does this tool have (beyond those previously identified in the Johnny paper)? If so, describe those flaws.
- What usability flaws identified in the Johnny paper have been addressed in a satisfactory matter? Describe the challenge and the current solution.

If you believe any of those aspects is not applicable (e.g., the tool has no usability flaws not described in the Johnny paper), instead briefly explain why you believe it is not applicable.

[1] https://en.wikipedia.org/wiki/Encryption_software

[2] A. Whitten and J.D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. USENIX Security 1999