University Of Washington, CSE 590P – Computer Security - Homework 3

Tadayoshi Kohno, John Manferdelli

Due: 4:30pm February 1, 2007. This homework is worth 33 points.

See the course website (http://www.cs.washington.edu/education/courses/csep590b/07wi/) for instructions on how to submit your homework. For this assignment, you should submit a PDF file named 'YourLastName-YourFirstInitial-HW3.pdf. Please type your name on the first page of your assignment.

1. (15 points total.) The first part of this assignment gives you the opportunity to explore and comment on the new PwdHash password manager. You can download the PwdHash plugin here: http://crypto.stanford.edu/PwdHash/. Or you can use the online PwdHash tool here: https://www.pwdhash.com/. Please tell us which you choose to use (you may choose both).

   Next, please do the following tasks or answer the following questions.

   1.1. Create an account on the class Wiki. Use a regular, non-PwdHash-protected password when you create this account. (You should have already done this.)
   1.2. Now use PwdHash to manage your account's password. This means that you will have to first use PwdHash to change your password, and then you will have to login using the PwdHash-protected password.
   1.3. (4 points total.) Answer the following questions:
      1.3.1. Did you find it easy to change your Wiki password to a PwdHash-protected password? Explain why or why not.
      1.3.2. After you changed your password, did you find it easy to login to the Wiki with your PwdHash-protected password? Explain why or why not.
      1.3.3. Having now had some experience with PwdHash, would you plan to continue to use PwdHash to protect your passwords? Explain why or why not.
      1.3.4. Do you think that your friends and family would find PwdHash usable? Will you encourage your family members to use PwdHash? Explain why or why not?
   1.4. (4 points.) For each Issue that we discussed in class, please comment on how the Issue might or might not apply to PwdHash.
   1.5. (4 points.) For each Response we discussed in class, please comment on how PwdHash might or might not address that Response.
   1.6. (3 points.) How would you improve the usability of PwdHash? Or, more generally, how would you create a more usable authentication scheme? This is a very open-ended question.

2. (18 points total.) Identify what you believe to be three fundamental problems or challenges spanning usability and computer security. We already talked about user authentication in class, so please pick three different problems (or find some twist to authentication that we didn't discuss in class).

   For each of the problems/challenges that you identified, answer the following questions.

   2.1. (3 points for each problem.) How each of the Issues we discussed in class relates to your problem.
   2.2. (3 points for each problem.) How each of the Responses we discussed in class might or might not apply to your problem.
   2.3. (Extra Credit.) Discuss how you would proactively address these challenges (new designs, etc), and what would constitute "success."

Reading:

Chiasson and van Oorschot paper on password managers:
http://www.scs.carleton.ca/~paulv/papers/usenix06.pdf.
Yee's paper on security and usability, page 253-264:
http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec9extra/ch13yee.pdf.