Fourth Step: Progress Report

The progress report must be organized as below, with an updated bibliography in addition to all the relevant updates from the project proposal. The project description should describe the current project scope together with the current limitations or changes in respect to the initially proposed project description. The project timeline should be updated to include all the recent changes in terms of project steps and milestones (if there are any), and should indicate the time of the progress report

1. Project description relevant at the reporting time (*3 points*)
2. Work accomplished (*2 points*)
3. Work remaining and timeline indicating both the major project steps and the current progress report (*3 points*)
4. Updated bibliography; if no updates, say so (*1 points*)
5. Any project difficulties experienced up to the reporting phase and respective mitigation plan; if none, say so (*1 points*)

Coping Mechanisms in Password Selection

Brian Curnett and Teri Flory

Problem Statement

Stringent password policies include requirements such as not including a dictionary word, or including a capital letter, special character, or number. To analyze how the requirements of these policies effect users, passwords will be collected from individuals within three different password policies over seven required password modifications, and will be reviewed for coping mechanisms such as using a capital letter first, using a number or special character last, repeating the same character or word multiple times within the password, repeating the same root password over multiple changes, or incrementing numbers or special characters over multiple changes. The NIST entropy calculation will be modified for any of these coping mechanisms observed and with the results showing numerically how coping mechanisms decrease the actual entropy of a specific policy.

Work accomplished

The group rewrote the proposal, edited and modified the literature review, and wrote the IRB Application. In addition, we have completed the required consent form and wrote the survey questions. Based upon timing concerns, the group decided to pursue the Mechanical Turk collection process initially, and have submitted the required IRB Application. After receiving feedback from the IRB, the Application has been modified as required and will be resubmitted for review on Friday October 31, 2014.

We have met with Statistical Consulting at Purdue University as well as with Lisa Zilinski to discuss our data management plan. Additionally, we have collected fake passwords from classmates and professors at Purdue and calculated both the actual NIST entropy and a post coping mechanism entropy for each password. This has allowed us to determine the mean of the NIST entropy and post coping mechanism entropy, the standard deviation, and confidence interval. In addition, through the analysis of this fake data the group has narrowed down and determined the specific coping mechanisms to be evaluated, and assigned a value for each one. We have used this information to create the presentation to be given in class on October 31, 2014.

Work remaining

The most time sensitive item remaining is to finish creating the website. If a website designer is not located, the team will work to create a website on our own with the assistance of other individuals in the CERIAS program.

We have calculated the actual NIST entropy and post coping mechanism entropy of the fake passwords by hand, and we need to determine whether we will continue to do this calculation by hand with the actual data, or whether there is a program to assist with this task. Additionally, the team has used SAS software for calculation of the mean entropy, standard deviation, and confidence interval, and this will also be reviewed for determination of whether this is the most appropriate software for use in our analysis. These decisions will be made once the full analysis of the fake data is complete, which we hope to accomplish before November 14, 2014.

We have received initial feedback from the Institutional Review Board (IRB) and modified the Application as requested. Upon receiving final approval from the team will launch the Mechanical Turk HITS and the website. Within two days after the first Mechanical Turk HIT is posted, we will review whether the each participant correctly completed the survey. If yes, then the payments to the Mechanical Turk participants will be approved, and each participant will be invited back to participate in the second iteration of the password creation. If a participant does not complete the task, then we will notify Mechanical Turk of this and that participant will not receive compensation nor an initiation to participate in a subsequent round.

Each instance of the data collection will be downloaded and analyzed as it is received. This will allow the team to present limited data findings by the end of the semester as well keep the workload spread out over the data collection, instead of attempting to calculate the entropy of all passwords at one time. The team will present a final presentation and paper on the data that has been collected to date on December

5, 2014. If the data collection is not completed by that date, Brian Curnett will continue on after that date with the final iterations of password collection.

The team is still interested in collecting data from Purdue students, and will be submitting an IRB Application for that portion of the project. The goal is to have that IRB Application turned in on or before December 1, 2014, to allow sufficient time for review and any modifications that may be needed prior to the spring semester starting on January 12, 2014.

Updates to bibliography

None.

Problems encountered

None.