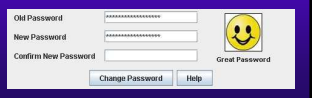
Interface Designs to Help Users Choose Better Passwords (study design)

Richard M. Conlan, Peter Tarasewich
Northeastern University
College of Computer & Information Science

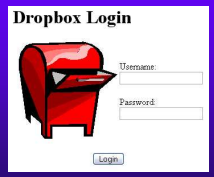
Study Summary

- Implemented four password selection applets
- Each applet offers real-time feedback on password quality based on a continuously updated Password Quality Score (PQS) which it submits to the server along with the new password



Study Summary (cont.)

- Embedded applets into **Dropbox-Online.com** homework submission system



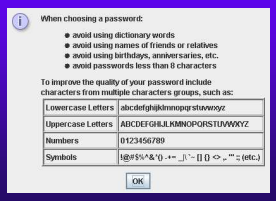
- Homework submission system implemented in PHP with MySQL database
- HTTPS site
- Be careful with SSL certs – browser support doesn't mean it is supported by Java, etc.

Study Summary (cont.)

- Decided to do a between-user study due to concern about confusion / learning effects
- Evenly distributed the password selection applets over the user population
- Forced users to change their passwords at three points in the semester
- Informed users of the study and got consent at the end of the semester

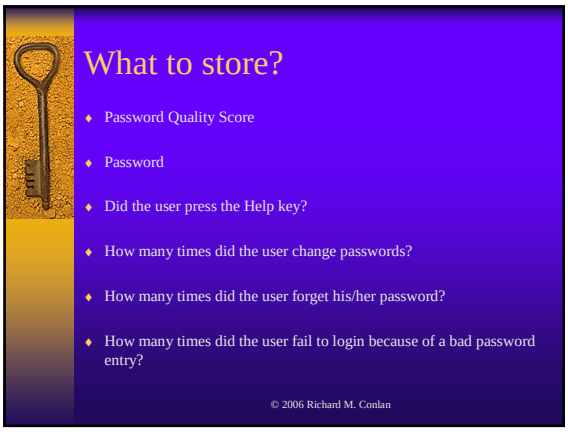
Help

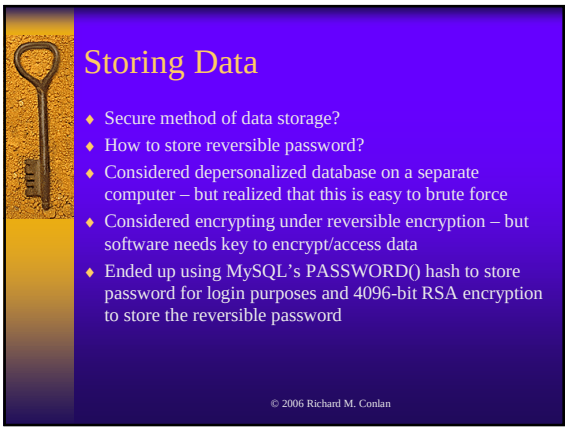
- How should the Help be worded? Should it be specific to the applet? We decided to use the same Help across accounts, and based it on standard Help messages found on various web sites
- Might the user's confusion at the password applet cause a problem that might be remedied by adequate help?

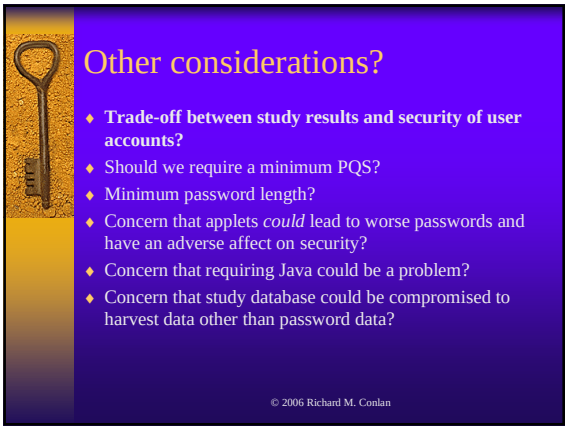


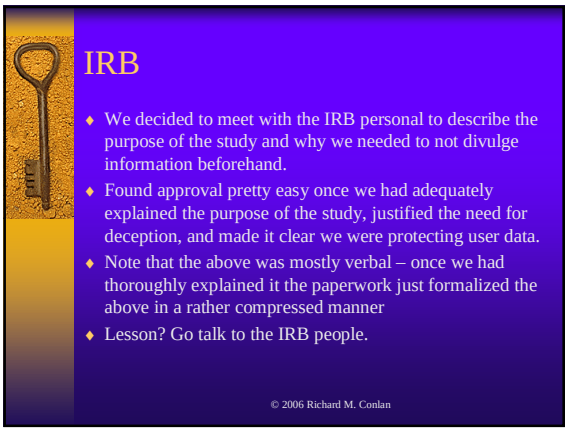
Structural Decisions

- Students were not informed of the study in advance because we felt that informing them that we were focusing on password quality would affect password choice
- We chose a classroom rather than a lab setting because in the lab it is hard to know if people are choosing realistic passwords and to get a genuine sense of whether people will remember the chosen passwords in a real-world usage setting


What to store?
Password Quality Score
Password
Did the user press the Help key?
How many times did the user change passwords?
How many times did the user forget his/her password?
How many times did the user fail to login because of a bad password entry?
© 2006 Richard M. Conlan

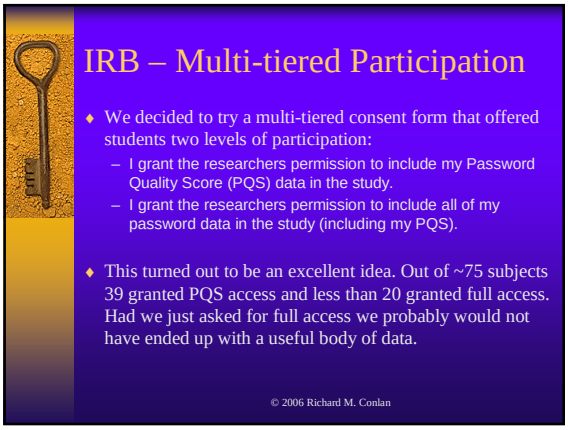

Storing Data
Secure method of data storage?
How to store reversible password?
Considered depersonalized database on a separate computer – but realized that this is easy to brute force
Considered encrypting under reversible encryption – but software needs key to encrypt/access data
Ended up using MySQL's PASSWORD() hash to store password for login purposes and 4096-bit RSA encryption to store the reversible password
© 2006 Richard M. Conlan


Other considerations?
Trade-off between study results and security of user accounts?
Should we require a minimum PQS?
Minimum password length?
Concern that applets could lead to worse passwords and have an adverse affect on security?
Concern that requiring Java could be a problem?
Concern that study database could be compromised to harvest data other than password data?
© 2006 Richard M. Conlan



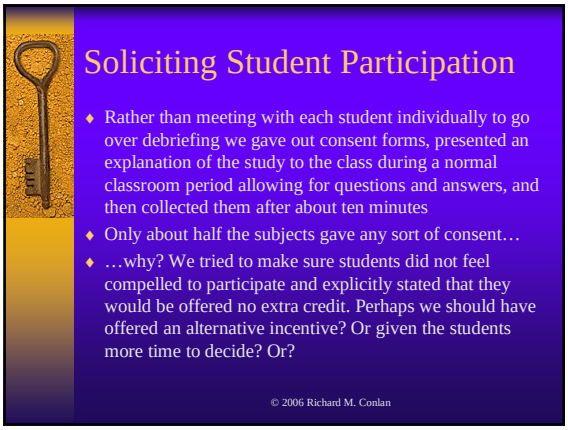
IRB

- We decided to meet with the IRB personal to describe the purpose of the study and why we needed to not divulge information beforehand.
- Found approval pretty easy once we had adequately explained the purpose of the study, justified the need for deception, and made it clear we were protecting user data.
- Note that the above was mostly verbal – once we had thoroughly explained it the paperwork just formalized the above in a rather compressed manner
- Lesson? Go talk to the IRB people.



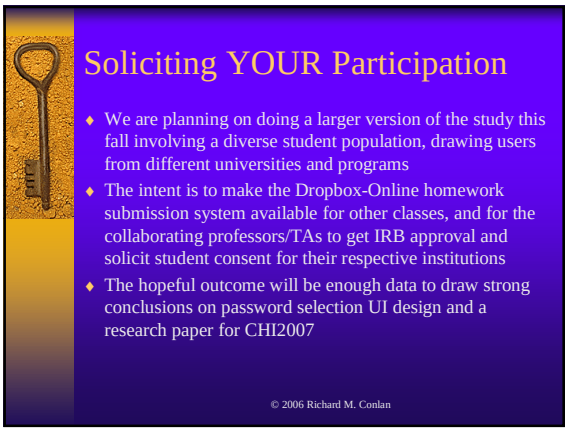
IRB – Multi-tiered Participation

- We decided to try a multi-tiered consent form that offered students two levels of participation:
  - I grant the researchers permission to include my Password Quality Score (PQS) data in the study.
  - I grant the researchers permission to include all of my password data in the study (including my PQS).
- This turned out to be an excellent idea. Out of ~75 subjects 39 granted PQS access and less than 20 granted full access. Had we just asked for full access we probably would not have ended up with a useful body of data.



Soliciting Student Participation

- Rather than meeting with each student individually to go over debriefing we gave out consent forms, presented an explanation of the study to the class during a normal classroom period allowing for questions and answers, and then collected them after about ten minutes
- Only about half the subjects gave any sort of consent…
- …why? We tried to make sure students did not feel compelled to participate and explicitly stated that they would be offered no extra credit. Perhaps we should have offered an alternative incentive? Or given the students more time to decide? Or?


Soliciting YOUR Participation
We are planning on doing a larger version of the study this fall involving a diverse student population, drawing users from different universities and programs
The intent is to make the Dropbox-Online homework submission system available for other classes, and for the collaborating professors/TAs to get IRB approval and solicit student consent for their respective institutions
The hopeful outcome will be enough data to draw strong conclusions on password selection UI design and a research paper for CHI2007
© 2006 Richard M. Conlan


Questions?
© 2006 Richard M. Conlan