04- Field studies, ecological validity, and ethics

Lorrie Cranor and Blase Ur

January 23, 2014
Today!

• Another Lorrie NSA anecdote
• “Users are not the enemy”
• Homework
• Field studies
  – Ecological validity and ethics
• Mechanical Turk
• IRB process and example
Users are not the enemy!!!
Users are not the enemy

• “These observations cannot be disputed, but the conclusion that this behavior occurs because users are inherently careless — and therefore insecure — needs to be challenged.”

• Study methods:
  – Online survey with 139 responses
  – 30 semi-structured interviews
Discussion points

• Are the participants representative?
  – Would a different group of participants produce different results?

• “Without feedback from security experts, users created their own rules on password design that were often anything but secure… many users do not understand how password cracking works.”
  – What feedback should we give?
Discussion points

• “Users identified certain systems as worthy of secure password practices, while others were perceived as ‘not important enough.’”
  – How do you motivate users?
  – How do you treat users as partners?
• Are shared passwords the solution?
• Are single-sign-on passwords the solution?
Homework
Homework 1

- Privacy tools’ usability
  - Usability problems?
  - Improvements?
  - Comparison to paper
Field studies
An entire university’s passwords

• 25,000 faculty, staff, students at CMU
• What are their password characteristics?
• How guessable are their passwords?
• How do demographic factors correlate with password strength?
• How do these real passwords compare to leaked / collected passwords?
It’s official: Computer scientists pick stronger passwords

Landmark study says people in business school choose weakest passwords.

by Dan Goodin - Nov 8 2013, 12:28pm EST
Ethics questions

• How did we get people’s passwords?
• How did we obtain consent?
• What ethical concerns are there?
  – What seemed to be done well?
  – What could have been done better?
Ecological validity / external validity

• Is this study ecologically valid?
  – How could it have been improved?
  – Are other password studies ecologically valid?

• To what degree can we generalize about our results?
  – Do all b-school students make bad passwords?
Social phishing

- Use social networking sites to get information for targeted phishing
  - “In the study described here we simply harvested freely available acquaintance data by crawling social network Web sites.”

- “We launched an actual (but harmless) phishing attack targeting college students aged 18–24 years old.”
Social phishing

• Control group: message from stranger
• Experimental group: message from a friend
• Used university’s sign-on service to verify passwords phished
Ethics

• How did they obtain consent?
• What ethical concerns are there?
  – What seemed to be done well?
  – What could have been done better?
• Who was potentially affected by the study?
• “The number of complaints made to the campus support center was also small (30 complaints, or 1.7% of the participants).”
Amazon’s Mechanical Turk

Image from http://www.salon.com
M Turk

• Human intelligence tasks (HITs)
• Studies usually start with consent form
• Pay relatively low wages (ethics concerns)
• Quality control necessary
  – Lots of shady folks; lots of good folks
  – Can be done through obvious questions
  – Can be done through open-ended questions
• Don’t need to host study on Mturk
Institutional Review Board (IRB)
IRB process

• Is it research? Are there human subjects?
• Full review vs. expedited vs. exempt
• Fill out and submit protocol
  – Include all study materials (e.g., surveys)
  – Include recruitment text and/or poster
  – Leave plenty of time