10- Quantitative data collection, lab and field studies, simulating attacks

Lorrie Cranor

February 20, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today's class

- HW5 – literature review
- Proposals due Wednesday!
- Reading discussion?
- Research questions and hypothesis testing
- Quantitative data collection
- Laboratory studies and field studies
- Simulating attack scenarios

Research questions

- Describe the questions your research is trying to answer
- May be exploratory
  - *How do people come up with passwords?*
- May test specific hypotheses
  - *If we prime people by displaying a photograph on a password creation page, will they include elements from the photograph in their password?*
- Need to scope research questions to the time and available resources
  - If to broad, you won't be able to answer it in the time you have
  - Focus on a narrower question that you may be able to answer

Hypothesis testing

- A hypothesis is a conjecture, or guess, that might be true
  - Longer passwords are more secure than shorter passwords
- A hypothesis must be falsifiable
- A good hypothesis for a research study is one that is feasible to test within the scope of the study

Discuss with your project team

- What is the main research question (or questions) that your project team will be investigating this semester?
- Identify one or more hypotheses that you are interested in testing that are relevant to this research question

Quantitative data collection

- Surveys
  - Opinions, preferences, self-reported behavior or experiences, demographics
- Measure something
  - Speed (e.g. to complete a task)
  - Accuracy
  - Number of occurrences
  - Heart rate, eye movements, brain activity
  - Temperature, humidity, size, weight
- Analyze existing data (ethical considerations!)
  - From previous study
  - Collected for another purpose
  - “Found”

How can we measure these things?

How might they be used in a UPS study?

Lab studies vs field studies

Advantages of lab studies

- More controlled
- You can simulate software and products that don't exist yet
- You can trigger events that might normally be infrequent or hard to observe in the wild
- You can observe normally risky activities in a safe environment
- You can more easily instrument devices and the environment for data collection

Advantages of field studies

- More realistic
- Less chance of bias from experimenter
- Participants more likely to behave and respond to risk naturally
- Participants perform task in the context of their normal activities
- More conducive to long term data collection

What can you do in a lab study?

- Interviews, focus groups, surveys
- Observe participant reactions to various designs, prompts, stimuli
- Observe participants performing tasks
  - Perhaps while thinking aloud
- Observe participant interaction
  - With devices, software, messages from “computer” (wizard of oz)
  - With researcher
  - With other participants
  - With actor posting as someone in the lab for a particular reason (participant, maintenance worker, etc.)

What can you do in a field study?

- Observe users doing their normal activities
  - Experimenters watching, visible or hidden cameras, sensors, instrumented software
  - Contextual inquiry: watching, interviewing users in their own environment
  - Challenges: getting permission, not causing behavior changes when people feel they are being watched, instrumentation
- Observe user interaction with devices or software provided by experimenter
  - Usually instrumented for automatic data collection
  - Diary studies, follow-up interviews or surveys

Experience sampling

- Participants fill out questionnaires in response to periodic alerts, responses are based on what is happening now
- Often used to understand mood, time use, and social interactions
- Need to find way to alert participants and have them respond to short survey (< 2 minutes)
  - Beepers, email, SMS, diaries, etc.

S. Consolvo and M. Walker. Using the Experience Sampling Method to Evaluate Ubicomp Applications.Pervasinve Computing, April-June 2003.

M. Mazurek, P. Klemperer, R. Shay, H. Takabi, L. Bauer, L. Cranor
Exploring reactive access control. In CHI 2011: Conference on Human Factors in Computing Systems, May 2011.

Paratyping

- Measuring real-life experiences instead of testing the technology
- Paratypes
  - a simulation, or model, of interaction ("-type") with a technology which is evaluated alongside ("para-") real-world experience
  - "proxies" act as substitutes for researcher
  - As they go about their daily life they survey the people they interact with

Iachello, G., Truong, K. N., Abowd, G. D., Hayes, G. R., and Stevens, M. 2006. Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. CHI2006. DOI= http://doi.acm.org/10.1145/1124772.1124923

Date: 11 / 08 / 04

1) What were you doing / talking about?

Work - some interviews of car dealers

2) Sensitive information involved

No Financial Health (Other) Proprietary

3) Physical location

at work near one another

4) Number of people around at microphone reach

1 + me

5) Notes (include your relationship with the person)

Co-worker

0216

The Personal Audio Loop

The Personal Audio Loop (PAL) continuously records sound and voices from the user's environment. The device allows the user to replay, at any specific moment in time, any sound that was heard in the recent past, up to a defined maximum time span (for example, up to 1 hour in the past). Sound older than that is automatically erased and cannot be replayed. Currently, PAL is integrated in a cell phone (see figure), but the device only records sound from the environment, and not phone conversations. The user can replay the recording and rewind and fast forward through it. The stored audio can be heard either through the loudspeaker on the phone, or through the external speaker/mike.

People who used this device, employed it as a memory aid, as a reminder tool, as a short-term voice notepad and to relay information from one person to another. Although PAL could be useful to many people, we are also aware that other people might have concerns about the privacy of their conversations.

Suppose that the person who gave you this survey is using PAL. We would like to know your opinion about PAL. Please complete the survey on both sides of the card, as soon as possible.

1) How important would it be that she had told you **before** starting the conversation that PAL is running?	Does not matter	1	2	3	(4)	Matters very much 5
2) How important would it be that she had asked for your permission to use PAL?	Not important	1	2	(3)	4	Very important 5
3) For how long after the end of your conversation do you think should PAL store the conversation?	☐ as long as he needs ☒ at most one week ☐ at most one day ☐ at most one hour ☐ at most 10 minutes ☐ I do not know					
4) How likely would it be that you ask her to erase the recording of the conversation you just had?	Not likely	1	(2)	3	4	Very likely 5
5) How important is it that she asks for your permission to copy the conversation to a tape?	Not important	1	2	3	4	(5) Very important
6) How important is it that she asks for your permission to play the recorded conversation to someone else?	Not important	1	2	3	4	(5) Very important
7) Do you consider the conversation you were conducting with her confidential?	Not confidential	(1)	2	3	4	Very confidential 5

8) Your Age Range: ☐ 18-29 ☐ 30's ☐ 40's ☒ 50's ☐ 60 or over

9) Your Sex: ☐ M ☒ F

10) Your Occupation: media producer

11) Today's date: 11 / 8 / 04

↳ turn card

0216

Simulating attack scenarios

- Secure systems need to be usable, even when under attack
  - Prevent attackers from tricking user
  - Prevent attackers from exploiting mechanisms designed to increase usability
- Would like to observe system + users while under attack
  - But it would be unethical to increase actual risk
- Use hypothetical scenarios and role play
  - If participants are invested enough in scenario they may behave naturally, even though they know everything including risk is fake
- We may be able to ethically deceive participants
  - Need to demonstrate we are not actually increasing their risk and deception is necessary
  - Need to debrief participants afterwards

Example of attack scenarios in studies

- Tell users purpose of the study is unrelated to actual purpose, then expose them to simulated attacks
  - Study about video games, browser warnings popped up
  - Study about online shopping, fake email from ecommerce site triggered phishing warning
- Send users fake phishing emails
- Role play that includes other participants or actors playing the role of attackers
  - Campaign worker simulation included (unsigned) email from opponent's campaign impersonating someone from participant's campaign