Part I

SURVEY

Password managers have long been controversial in the field of information security, because they solve one problem by creating a different one. However, a less studied topic is the usability of a password manager, rather than the security of one. Using a survey study, one can attempt to answer the question: “are password managers a viable means for quickly and easily storing and retrieving sensitive information (e.g. passwords)?” Is the general public even aware of password managers? Are they too mentally complex such that a person would prefer to write on paper? For this study, it would be important to ask about demographic information (e.g. age), as well as their experience with technology. Additionally, we would ask how people currently store or remember their passwords — do they store their passwords in their head? Do they write their passwords down on paper? If they write their passwords down on paper, would they be open to an analogous system on a computer? A survey study is a good choice for such a question because it’s broad and attempting to gage a whole population of attitudes so that we can design effectively with this background knowledge.

DIARY

Because the survey study provides a breadth of information about general attitudes, we will use a dairy study to determine: are people are able to maintain using a password manager in the long term? For this study, we would assemble three groups of people: (1) people who have never used any kind of system to manage their passwords (e.g. they remember all of their passwords), (2) people who write down their passwords either on a piece of paper or on an unencrypted document on their computer (or similar), and (3) people who currently use a password manager. This study would give everyone the same password manager, and request that the participants use it for storing their day-to-day passwords. With the diary entries, we would be able to see if people were able to keep up with using a manager; more specifically: do the people who use paper adapt to the password manager better than people who remember all their passwords? How do people who use paper (an analog password manager) compare to people who already use a manager? This diary study design is the best choice to analyze long term behavior because it allows us to observe long term habits to see if people can actually use a password manager, and what kind of people (i.e. what group of participants) need what kind of nudging (e.g. if the people who have

never used a manager tend to not be able to pick up the concept, maybe we should only target people who write their passwords on paper).

INTERVIEW

Where the survey brought us general breadth, the diary brought us long-term habits, an interview study which provides qualitative depth would allow us to answer: is there a need for a password manager? This study would have experimenters ask about people's current password behavior. This would include asking how often people type in passwords (e.g. does the browser remember every time?) and how much they care about their passwords. We would ask if people have difficulty remembering their passwords, and if they use the same couple of passwords for everything; as a followup: would people use better passwords if they didn't have to remember them? Is it concerning to have all of the information in one place, even if everything is securely encrypted? The interview format is a good choice because it allows us to dive more deeply into attitudes than the survey study to get a good feeling for how people qualitatively perceive passwords and understand people's needs regarding them.

USABILITY

With a usability test, we can evaluate: is the setup of current password mangers an effective one? Does the conceptual model make sense to people? Is it strange that you have to remember a password for the rest of your passwords? What if the system used some form of touchID or 2 factor authentication to unlock passwords — is this viewed as more secure or does it at least make more sense? For this study, experimenters would observe as participants (who had never used a password manager) set up a password manager and save their commonly used passwords (email, bank, social media, etc.). After the passwords had been saved, the participants would be sent home and brought back a few days later. This would allow experimenters to evaluate if password managers, as they stand today, are usable to the general public. The fact that the study design is a usability test is useful because it would allow us to evaluate if we need to rethink the structure or flow of password managers and pinpoint where people have difficulty.

OBSERVATIONAL/EXPERIMENTAL

Because passwords are such a private thing, collecting observational data clandestinely in the field comes with many ethical concerns as the participants are not choosing to participate in the study directly. Ethical concerns mostly aside, one question we could hypothetically try to answer would be: in a non-experimental context, do people have difficulty with passwords? The experiment would involve accomplices going to public places where people use computers (e.g. universities, libraries, coffeeshops) and asking people to borrow their computer "to send a quick email." The accomplice would then proceed to enter his/her password incorrectly many times — while this is happening, a second accomplice will be nearby taking note of the subject's reaction. The researcher would express frustration about passwords, and the subject's visual reaction and if they had anything to say would be noted. Although the study design is slightly contrived due to the nature of the subject being studied, it would allow for a more genuine conversation about passwords and perhaps people's genuine frustrations about them.

Part II

A. CONCERNS

- In general, when recording subjects it's best to get their permission (after the fact if need be)
- Setting up recording equipment to capture a transaction that is supposed to be private (e.g. banking) is a questionable practice because while photographing people in public is usually okay, the rule stipulates that if people have an expectation of privacy they cannot be recorded.
- The experiment wants to upload photos taken without consent of the subject and upload these pictures on the internet for people to judge, which should require the subject's approval
- The study says that the first thing that happens after coming in the lab is that participants are given a demographic survey, when really they should be given a consent form
- Retaining a fingerprint is a sensitive activity — storing a fingerprint without someone's permission is certainly questionable at the least, regardless of how secure the storage is. Even with their permission, I would be nervous of such sensitive information leaking out.

B. MODIFICATIONS TO PART I

This study design is not completely poor — if the design were changed in a few key ways, the study would be far more ethical. If the researchers wanted to take video of subjects, the subjects should be given consent forms either before (if it wont skew the results) or after. If they don't give consent after, the video gets deleted. If they choose not to use a video recording, the study would be simplified if researchers just took traditional notes which require no consent.

B. MODIFICATIONS TO PART II

Instead of giving the participants a demographic survey when they first walk in, participants should first be given a consent form explaining the extent of the study, including risks and benefits. Additionally, the "reward" an undergraduate class might get from examining fingerprints might outweigh the risk of storing these fingerprints. If the researchers are adamant about studying the partial prints to find the print tolerance, the researchers themselves (or other IRB approved colleagues) should do this work.