RepliSEC

Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication

Agenda

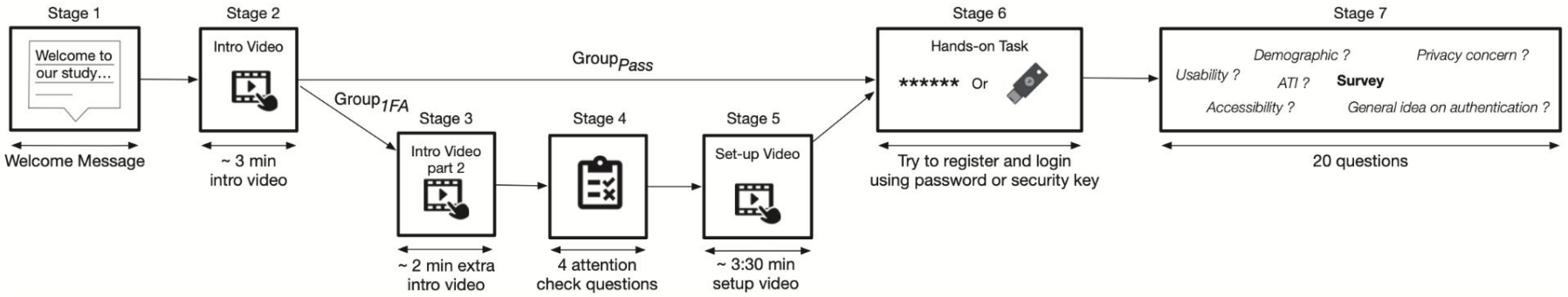
- Topic of research
- Explanation of existing paper
- Study design
- Data analysis
- Pitfalls
- Related research

RepliSEC

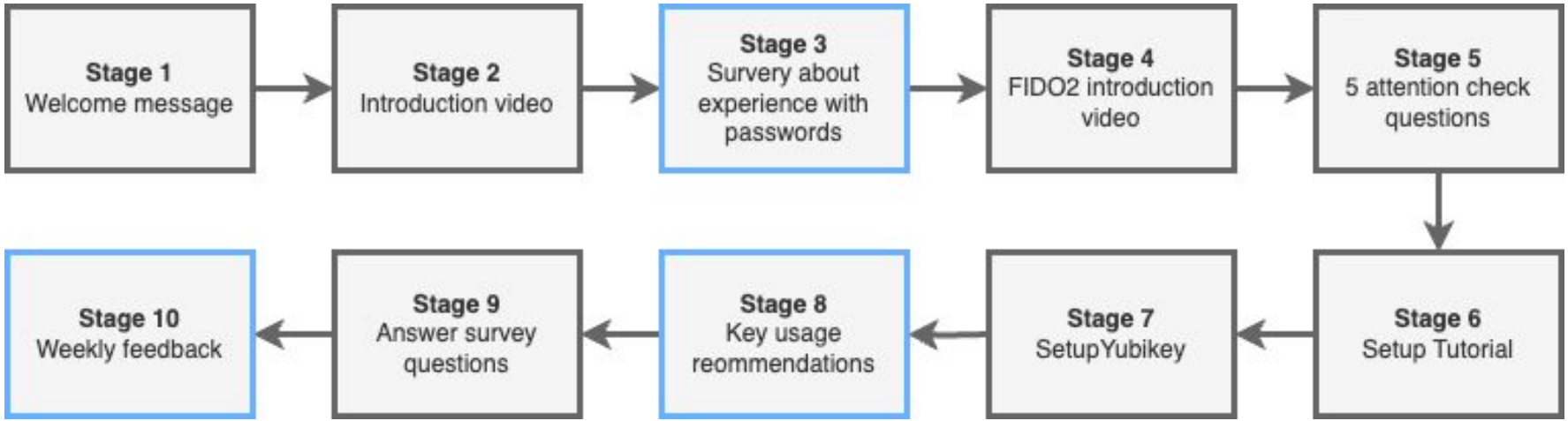
- We want to replicate an existing research
- Research in question
  "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication"
- How usable is FIDO2 as a passwordless authentication option?

Explanation of existing paper

The study design can be summarized in this flow diagram



Our Study Design



Major differences to the study

- Using real websites instead of fake websites
- Services chosen
  - Google
  - Amazon
- Using the current implementation of FIDO2 passwordless authentication which are Passkeys
- Passkeys do not work exactly the same way like the fake websites implemented in the paper

Before the study

- Test subjects
  - Colleagues at work
  - Friends and family
  - Students
- Ask if the person has Google or Amazon account
- Organize individual appointment (30 Minutes)
- Laptops will bring their own laptop
- Sitting in alone in room. Try to find a location with reliable/fast network connection or use Hotspot
- A USB C to USB A adapter will be provided
- Convince them to participate by luring them in with Yubikey

Study: Stage 1

- Greet participants
- Read Welcome Message from paper for conformity
- Contains
  - Description of study
  - General overview of the process
- User signs his life and soul to us

Study: Stage 2

- Watch first video from paper
- Video contains information about password based authentication and the dangers of using passwords
- Link to video on YT
- With german subtitles
- On our laptops not the participants' laptops
- Maybe switched with Stage 3 (to be discussed)

Study: Stage 3 (New)

- Study has control group, we don't…
- Our control group are the participants themselves, or at least their past selves
- Survey about the participants experience with password based authentication on the given platforms
- Survey questions are the same questions as stage 9 or a subset (to be discussed)

Study: Stage 4

- Watch second video from paper
- Video contains information about FIDO2 passwordless authentication and the benefits of using Yubikeys
- Not how to setup keys, just information about passwordless authentication
- Link to video on YT
- With german subtitles
- On our laptops not the participants' laptops

Study: Stage 5

- Fill out short 4-question survey about the previous two videos to check if the participants paid attention
- Paper didn't specify the questions
- Kick out anybody who fails the test

Study: Stage 6

- Participant chooses service (Google/Amazon) to setup the Yubikey on
- Participant is shown a video on how to setup the Yubikey for the chosen platform
- We're not using Videos from Paper, because those do not correspond to passkeys authentication
- We're going to create similar videos
- Videos will have subtitles
- Should the key setup (next stage) be done in parallel to watching the videos?

Study: Stage 7

- Participants setup Yubikey on their laptops
- Participants are allowed to ask questions regarding the setup process
- … ?

Study: Stage 8 (New)

- Explain to participants the importance of keeping the Yubikey safe
- Explain methods of recovery
- Read to participant from a pre-written script

Study: Stage 9

- Survey contains the same set of questions from the Paper
  - Acceptance
  - System Usability Scale
  - Affinity for technology interaction
  - Privacy Concern
  - Technical Problems
  - Open-Ended questions
- Total 26 questions, depending on how u count
- Paper posted multiple open-ended questions and participants had no limit
  We're going to post one question and limit the answer to one sentence.
- Shouldn't open-ended questions be done in the next stage?
- Like all other surveys it will be hosted on the university Limesurvey Service

Study: Stage 10 (New)

- Give participants 3 weeks of real-life usage of the yubikey
- Weekly feedback for the first two weeks
- We're going to send a separate Email to each participant on Sunday morning to remind them
- On week 3 participants are sent a Limesurvey link to fill out
- Survey contains the same questions as the one from Stage 9

Data analysis

- Data will collected over a period of time
- Because sessions will be done separately for each participant, estimated 1 month for data collection on first round.
  MATH
  20 participants / (3 sessions per week per person * 2 people) = 3.3333 Weeks
- This means the data for the first round and follow-up round will be spread over 1 month and 3 weeks
- Somewhat optimistic estimation
- Data from first round can be analysed separately, i.e. before second round begins

Pitfalls

- We're going to get USB C Yubikeys with NFC, this poses the following questions:
  - What if the user's laptop doesn't have a USB C port?
  - Should we consider using the NFC functionality on the Yubikey?
- Dropout? How many participants will do the first part to get the yubikey and then bailout on us on the second part? I can't tell
- Will the participants actually use the Yubikey in those three weeks? Or are they going to login once and never have to login again?

Related research

- Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, & Markus Durmuth (2020). “You still use the password after all” – Exploring FIDO2 Security Keys in a Small Company. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (pp. 19–35). USENIX Association.
- Stephane Ciolino, Simon Parkin, & Paul Dunphy (2019). Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 339–356). USENIX Association.
- Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, & Kent E. Seamons (2018). A Tale of Two Studies: The Best and Worst of YubiKey Usability. 2018 IEEE Symposium on Security and Privacy (SP), 872-888.

Interested in taking part of our survey? ;)