Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Information sheet for participants of the

Android Trusted Introductions online usability study

Person of contact for questions: Christelle Gloor, D-INFK, christelle.gloor@inf.ethz.ch

Principal Investigator: Adrian Perrig, D-INFK, aperrig@inf.ethz.ch

Data security official ETH: Tomislav Mitar, tomislav.mitar@sl.ethz.ch

Please read the following text carefully and ask clarifying questions if something is unclear. You may use the feedback form with a throwaway email if you want to remain anonymous.

Information on the study

What is the goal of the study?

The study serves to investigate the usability and perceptions of the new prototype of the Trusted Introductions mechanism for the Android Signal private messaging client, from a sample of expert users.

What will be studied and how?

We are focusing on the usage patterns and perceptions of usefulness and usability of the new Trusted Introduction mechanism in the prototype. This is going to be studied in a field-experiment. We will collect anonymized data w.r.t, this mechanism for the duration of the study. Users will transfer their Signal data to the modified prototype and use the application as they normally would in addition to having the possibility to test the new mechanism.

Who can participate?

Participants must be at least 18 years old. We are looking to recruit people that use Signal and its entity verification mechanism regularly and are security conscious. This population is more likely to naturally use the new mechanism than the average population.

How am I going to be compensated for the study?

The participation in the study will not directly be compensated. You are helping us advance research which will result in an improved resilience against active- and impersonation attacks in private messengers using the Signal protocol.

What is the effort needed to participate in the study?

You will need to transfer your Signal data from the original application to the modified APK and go through the registration process again. This process is described in detail on the project landing page.

Which benefits and risks can I expect?

There is a risk of dataloss (in case the backup process is not carefully followed) or temporarily locking yourself out of your messaging client if your PIN is enabled and you do not have a copy of it when you uninstall the application. The instructions emphasize where appropriate what you need to do such that this does not happen.

The benefits of participating in this study, additionally to advancing research in privacy enhances messaging technologies, is that you may be able to expand the number of contacts that you have verified in a more usable way during the study period. When you revert back to the normal Signal application after the study, any verified contacts, even if it was done with the new mechanism, will be mapped as verified in the old application.

What are my rights during participation?

You may at any time abort your participation in the study and can, if you wish, prompt us for the deletion of the data associated with your account. This can be done by submitting your pseudonym (found inside the modified application on the help page) through the provided anonymous data deletion form.

What data is being collected?

During the installation users will be registered under a pseudonym that the researchers cannot be reassociated to a specific person without additional information provided by the users. Telemetric data related to the new mechanism in the form of counters and optional free-text feedback prompted through the application and in the form of a final survey will be recorded.

For each anonymous participant, we will record the usage patterns relating to the new mechanism and the security nr. verification mechanism. E.g., how many verifications were done, how many trusted introductions were initiated, were received, accepted, rejected, turned stale, raised a conflict, were deleted and when introducer information was erased. This data will only be collected as per-user counters. **No identifying information whatsoever will be telemetrically recorded, either for you or your contacts. We also explicitly do not record your device specs, or the exact time at which actions happened.** You can find the source code for the telemetry server here should you want to check these claims yourself. You may also optionally build the prototype application which includes the telemetry (TODO: add link to relevant source code for the prototype when it is completed) from source yourself to receive a guarantee on the code you are executing on your device.

Additionally, you will be prompted through the application to give us a bit more information about the context in which you used the new mechanism. Providing these answers is entirely optional.

At the end of the study period, we will ask you to fill out a general questionnaire where you can give us your opinions and further freeform feedback.

How will the data be handled?

The data is completely anonymized and only tied to your pseudonym and does not include any identifying information. Only the researchers will have access to the data and by design cannot

deanonymize the pseudonyms without more information from the user associated with the pseudonym.

Data provided via. the forms on the website will only reach the project lead. Provided emails will only be used if an answer is necessary and deleted after used. If a user requests the deletion of the data but chooses to provide a reason for aborting the study, any telemetric data will be deleted but the reasons will be kept associated with the pseudonym for which the data was purged. This helps us reason about missing data and assess added bias. If no reason for aborting is named, the pseudonym will be kept as to indicate that there is missing data there, but everything else will be purged.

What are my rights w.r.t the data?

You may at any time request the deletion of your data or request a copy of the collected information provided you supply us with your pseudonym and a way to send you the data (e.g., through a cloud link or a way to contact you directly).

Who is financing the study?

The study is conducted and financed in the context of the «Centre for Cyber Trust». This is a research collaboration between security research groups of the university of Bonn and ETH Zürich. The project is generously financed by the Werner Siemens Stiftung.

Who reviewed this study?

This study was approved by the Ethics committee of ETH Zürich under the application number 23XX-N-XX (TODO once approved).