Modeling Less-Literate User's Choices of Smartphone Authentication Modes

Pankaj Doke, Sylvan Lobo, V. S. Shyama, Ulemba Hirom, Mridul Basumotari

Modeling Less-literate User's Choices of Smartphone Authentication Modes

Pankaj Doke, Sylvan Lobo, Shyama V. S, Ulemba Hirom, Mridul Basumotari

Tata Consultancy Services Ltd.

{pankaj.doke, sylvan.lobo, shyamav.s, ulemba.h, mridul.basumotari}@tcs.com

Abstract. Smartphones are increasingly becoming a device of choice or are imperative in the discourse of Digitization of services such as banking within a developing country like India. At the same time, a large population within India is less-literate [1, 4, 5] who are also the primary beneficiaries of our research. We believe that Emergent Users [2] are the next set of users who are likely to adopt smartphones and technology in a larger context. Amongst these emergent users we expect that a large class of users are less-literate, more comfortable with native languages and have never directly consumed any digital technology based information system. For this fieldtrip study, we would be considering only users who fall under such criteria. Specifically those within an age limit of 40 years, prior exposure to a smartphone for a duration of at least 6 months, education not more than class 10, and no prior (non-mediated) use of desktop computer information systems.

Within the ecosystem of the smartphone, namely, the phone itself comprising of an operating system and mobile applications on the phone, as well as those on the Internet cloud, a mandatory creation of a Digital Identity in the form of a Google Account is required.

Currently, the notion of digital identity Authorization in most smartphone-based applications is implemented using a variety of choices, such as, password, PIN, patterns, biometrics such as fingerprint, voice. In the context of our users, namely emergent users [2], each of these authentication modes has a Usability aspect to it, which has a strong influence on the user and their adoption. For example, issues such as literacy levels are expected to play a role in the composition of passwords or use of local languages in usability of passwords.

In this Field Study, we wish to explore the Migration Model of the users amongst all these authentication modes. For example, how do users trade off PIN to Passwords to Biometrics; what triggers in their context of use, bring about these migrations when potentially the user may have chosen an alternative authentication mode.

Keywords: Less-literate users • Usable Security • Smartphone • Demonetization • Digitization • Migration model • User modeling

1 Introduction

Smart phone adoption in India is increasing across the society and there is a significant push towards Digitization at various levels within the country. At the same time, a large population within India is less-literate [1, 4, 5] and have technology adoption challenges. We also observe rapid adoption of smartphones in the country by less-literate users [2] with no prior familiarity with computers and Internet ecosystem. Digitization, for example of services like Banking, DigiDhan [6], could leave the user vulnerable to a variety of cyber-security attacks. The theoretical security measures available against such attacks are lowered by user behavior, which stems from poor Usability [3]. The available digital identity authorization modes in smartphones are subject to adoption by emergent users [2] based on various aspects of usability. In this study, we are trying to understand the influence of "Context of Use" on the adoption of authentication mechanisms. We are trying to model how context dictates adoption of security modes, rather than security or strength as a decider or a user preference in isolation from the context.

In this study, we are modeling the intersection of smartphone, security and specifically authentication modes, by exploring what forces are at play and how they affect each other. This investigation may help in design interventions based on the model for making security contextually usable.

2 Plan

2.1 User group and recruitment criteria

The field trip would be for one day and comprise of either 9 or 15 participants. Each team would have 3 participants of which one would be a local language or national language speaking person. Each team would interact with either 3 or 5 users, totaling 9 or 15 users. Effectively each participant would get an opportunity to interact with 1 user. Users would be chosen through stratified convenient sampling. 6-8 female users and 6-8 male users would be chosen from the mess and housekeeping staff at Indian Institute of Technology Bombay as well as the residential areas around the Campus with the help of NGOs like Vidya.

An alternative location could be APMC (Agricultural Produce Market Committee) in Navi Mumbai – which is Asia's largest market. Here we could interact with the users who are loader-unloaders of gunny bags – called Mathadi. For female users, we could interact with those who work in the shops/establishments at APMC.

We may identify users with the following criteria: An age limit of 40; Prior exposure to a smartphone for duration of at least 6 months; Education not more than class10; No prior (non-mediated) use of desktop computer information systems.

One pilot test would be conducted and all the users would be recruited prior to the field trip.

2.2 Method and Agenda

The team briefing would start at around 1000 hours and be limited to 1100 hours. We would followed two methods 1) retrospective data elicitation and 2) speculative data elicitation.

Retrospective data elicitation. Expecting the migration of authentication have happened in the past, one can only recall the account through retrospection and the data elicitation could be via Contextual Inquiry. At some point the Trigger could take longer time frame for instance, a recently married mother may have a pattern password, but after having the child she may have migrated to PIN or Password, this could be due to propensity of the child to play with phone and draw patterns on it. We could also investigate the lack of child-profile which could be tailored for the child. Similarly, for the case of an auto-driver, they may have chosen a password due to the demands of their profession. In these contexts, we cannot trigger a natural occurrence of a scenario and context and hence have no recourse but to rely and use data from retrospective accounts. Since the Field trip is limited to 1 day and we desire to interact with either 9 or 15 users within a span of half a day, retrospective accounts seems the only recourse at the moment for data acquisition.

Speculative data elicitation. Users are requested to visit to the lab and speculate with a given scenarios which trigger their past/retrospective accounts of password change, e.g rainy season, taking a child to hospital or shop. By stitching the field interaction and lab conversations, we would be able to gather a data point on how adoption and migration of authentication modes happen on the smartphone. We believe that not in all circumstances would it be possible to recreate natural scenarios for example, Mother–child case. Hence we would have imaginary scenarios which possibly act as triggers for decision making with users in a lab environment. And believe that their reasoning and thoughts would reflect in action or course of action in future they are likely to reason and follow in the future, if faced with such a situation.

The data could be possibly triangulated by cross positioning the question .eg an unmarried person would be asked what he /she would do after marriage and child or observed a married person on what they do with authentication or asking an non-auto drivers on what if they were auto driver. Later the data could be collated and validate through data triangulation with the users in the context and in lab environment.

In the lab environment, the user would be shown a paper prototype of an android phone and briefed that she could assume this to be their personal phone and have valuable data such as their Aadhaar card photo, PAN card photo, PayTM, WhatsApp and personal family photographs. The user would then have to participate in three scenarios as described below. The 3 scenarios would be conducted using paper prototypes of various authentication modes.

- **Scenario 1.** The user is provided with paper prototypes of multiple authentication modes and has to choose one out of them for safeguarding their phone.

- **Scenario 2.** In this scenario, user would be provided with the same choices of authentication modes, but in addition the user would also receive another set of cards which depict the scenarios from his context of use. User then has to make associations between the authentication modes provided and the context scenarios mentioned in the cards. Examples of context could be: Parent trying to make a mobile based payment in a dispensary while accompanied by a child who needs treatment; Paying school fees for child while parent stands in a queue in the rainy season; Paying the local vegetable vendor on the way back from school; etc. – i.e. scenarios where the users could be at risk while using their phone (data or monetary loss, privacy).
- **Scenario 3.** In this scenario, user has already chosen a preferred authentication mode based on the context provided in Scenario 2. For that particular authentication mode within the context, user is provided with a preset of password options. The password options are based on researcher assessed usable complexity. For example an L or Rangoli pattern for a pattern lock. The user is then asked to choose a password they prefer from the choices provided.

At the end of the tasks, we will also do a qualitative open-ended interview with the users to capture summative information or any formative data points we may have missed. After coming back from field trip around 5pm, all the participants would submit the field finding in the form of field note capture in excel file including the photos and videos in shared folder. Then everyone attempt to do the migration model with the team whosever come first.

3 Participants

We would have 9 or15 participants which comprises of:

- **Facilitator and Research Team:** Researchers would help in recruitment of the users, training and project management.
- **Mediators and Design Team:** Local Language speakers, who would help in translation. Designers for making deriving design insights.
- **Senior Researchers:** At least one researcher (desirable not mandatory) who has similar experience in a developed country and at least one researcher who has a mobile security awareness.

The participants in this field trip will get first hand user study exposure on practices and adoptions of security practices by emergent users in a developing country. They would do the actual user study and scenario triggering with the user. At the end for user, as a take-away, they would be informed on how to set better password using textual passwords and gain knowledge on what comprise a good password.

4 Requirements

We would be considering the location on the basis of lesser commute timing (not more than 30 minutes) either at IIT Bombay and surrounding areas or APMC. We need some assistance in recruitment process and also travel expenses (in case the location is APMC, our suggestion would be IITB bus rented for a half-day trip). We also need some budget on gifts which would be given as a gesture of appreciation to users, refreshments (lunch), internet connection, stationery and room space in conference venue.

5 Expected Outcomes

We expect to have a report on the observations and insights of the usability issues of the various authentication schemes in a context when used by an emergent user. We also hope to model the user-technology-migration as indicated by the data.

References

1. Chandramouli C Rural Urban Distribution of Population (Provisional Population Totals). http://censusindia.gov.in/2011-prov-results/paper2/data_files/india/Rural_Urban_2011.pdf. Accessed 31 Jan 2017
2. Devanuj, Joshi A (2013) Technology adoption by "emergent" users: the user-usage model. ACM, pp 28–38
3. Dourish P, Redmiles D (2002) An approach to usable security based on event monitoring and visualization. ACM, pp 75–81
4. (2013) State-wise Literacy Rates. In: Open Gov. Data OGD Platf. India. https://data.gov.in/catalog/state-wise-literacy-rates. Accessed 31 Jan 2017
5. Performance of States of India (Rural) - ACER 2009. http://planningcommission.nic.in/data/datatable/data_2312/DatabookDec2014%20231.pdf. Accessed 31 Jan 2017
6. DigiDhan Mela. https://digidhan.mygov.in/. Accessed 31 Jan 2017