Mobile Phone Usage by Low Literate Users

Pankaj Doke
Tata Consultancy Services Limited
Yantra Park, Opp. Voltas HRD Centre, Subhash Nagar, Thane 400 601
Telephone +91 022 6778 8068
pankaj.doke@tcs.com

Anirudha Joshi
Industrial Design Centre
Indian Institute of Technology Bombay, Powai, Mumbai 400 076
Telephone +91 022 2572 2545
anirudha@iitb.ac.in

ABSTRACT
We describe a qualitative study conducted using Contextual Inquiry of 60 low-literate users in India. For the purpose of this study, we define low-literate as those users whose education is equal or more than Standard Four and less than or equal to Standard Eight in the Indian State education system. Our users were recruited primarily from the contractual house-keeping staff of a very large Private Organization and an Educational Institute (42 Male, 3 Female), household help (3 Female), drivers (5 Male), guards (1 Male), shopkeepers (1 Male, 1 Female) and homemakers (4 Female). Our objective was to develop an understanding of information security issues in the context of the mobile phone, identification of problems and design ideas for design of interventions. Our methodology included Contextual Inquiry and Analysis with notes pertaining to User Statements, Task Breakdowns, Observations and Design Ideas. The notes across the study were consolidated using Affinity Diagrams.

We found that users have an elementary understanding of asset valuation and response. Literacy impedes adoption of an appropriate response to the threats using the mechanisms provided by the mobile phone since conceptual models are not clearly comprehended. It is also impeded because the users are unable to articulate a structured response to the landscape of threats. Due to the cognitive load induced by the possible factors which may get involved in risk articulation, users tend to adopt mitigation techniques propagated by the micro-networks without complete comprehension of risks or due analysis. Belief systems are more likely to drive a response than a more reasoned, well-aware response. Information or awareness is propagated via social mechanisms – however, these are not necessarily correct most of the times, primarily due to the inappropriate conceptual models formulated. The interface and conceptual model complexity of a modern touch screen smartphone compounds matters. Mobile Learning aids or Gamification of concepts can help users adopt more appropriate response mechanism to perceived threats to privacy and security issues. Interfaces built with single sign-on, local language display and text input would also help in building more safe environments for users to use the mobile phone. While more-literate users are likely to mimic a 'plan-do-check-act' model low-literate are more likely to have a 'do' or a 'do' or a 'do-act' cycle due to non-awareness or non-comprehension of 'plan-check' components.

IndiaHCI'15, December 17 - 19, 2015, Guwahati, India

ACM 978-1-4503-4053-3/15/12…$15.00

DOI: http://dx.doi.org/10.1145/2835966.2835968

CCS Concepts
• Human-centered computing→ Human computer interaction (HCI)→ HCI design and evaluation methods→ User studies.

Keywords
Mobile Security, ICT4D, User Study, Contextual Inquiry, Low-Literate Users, Android, Smartphone, Usable Security, Mobile Phones, Feature Phone, Mobile Applications.

1. INTRODUCTION
The recently concluded census activity has placed the literacy rate at 68.9 % in Rural India and 85% in Urban India. In terms of gender, 78.6% males in rural and 89.7% males in Urban India are literate while the corresponding values for females are 58.8% in rural and 79.9% in urban India[43]. For the purpose of this study, we adhere to the definition of Rural and Urban as defined in [43]. The number of literates in India are 49.30 crore for Rural and 28.54 crore for Urban population. This leaves the absolute value of illiterate population at 34 crore in Rural India and 9.16 Crores in Urban India. To re-articulate this in a perspective, where a crore is ten million, the total illiterate population is 431.6 million, while the population of USA is 320 million.

On another angle, the mean years of schooling of the workforce, as per the 2007-2008 data, is about 5.5 years [50]. The drop-out rates for the educational levels are 19.8% for Standard I-V, 36.3% for Standard I-VIII and 47.4% for Standard I-X [51]. As per the data of the planning commission of India, circa 2007-8, about 59.2% of the population aged more than 15 years, had no literacy (34.5%) or were educated till primary school (24.7%). This number goes up to 75.9% if we also consider middle school (16.7%) [50]. On the other hand, the percentage of children who are in standard V but are unable to read a Standard 2 level text is 47.2% and the percentage of children who cannot read English sentences is 74.3%[46][47][48].

While the figures for literacy are not encouraging, interestingly though, the teledensity (number of phone connections for every hundred individuals within an area) is about 72.94 (2014) with about 39.26 (2012) in Rural India and 169.17(2012) in Urban India [44][45]. - The recent subscription figures from the Telecom Regulatory Authority of India indicates 55.3 crores wireless subscribers in Urban India and 39.8 crores in Rural India[44][45]. The overall wireless teledensity is 76.02, with the values being 46.08 for Rural and 142.96 for Urban. The total number of rural households which have a only mobile phone is 47.9% and the value for Urban households is 64.3% [9].

The Internet and Mobile Association of India, a not-for-profit Industry body and IMRB a market research firm estimated that the Mobile Value Added Services market to be valued around INR 33,280 crore by end of 2013, primarily due to consumers [52]. While, according to [53] [54] the market size would be INR 482 billion by 2015.

In summary, the socio-economic impact of Mobile VAS on the population would be significant. The primary nature of the VAS applications would be mobile applications which run on smartphones and features-phones.

While we recognize the impending intersection of these two aspects – a deluge of mobile VAS across a stream of financial and non-financial domains with the literacy of a massive population, it leads us to wonder and ask ourselves if the population is ready to handle this onslaught from a security perspective? What would be the security issues involved? As the population stands at the initial stages of this wave, how are they reacting to the security aspects of the initial breed of mobile applications? How do they use passwords? What should be the password policies for low-literate users? Which passwords do they use? Does literacy constrain their choices of passwords? Do they share passwords? How do they recall passwords? How do they handle aspects of privacy? What are the behavioural responses to events of devices compromise or content compromise? What are their preferences between PINs, Patterns and Text passwords? How does information propagate? Do interventions work? Do users build appropriate conceptual models?

Our objective of this qualitative study is to try to attempt to understand the user perspectives on the above questions, generate insights and conceptualize design interventions where secure usable mobile applications for low-literate populations are a reality..

2. BACKGROUND

"Security is another word for control, and control may be control of anything…" "Security at its most basic requires the ability to differentiate, to recognize one object is different from another." "Privacy is the term used for what is perceived to be the boundary of mandatory control over information and what is not; the boundary that is perceived to separate personal space from public space." [24].

Security of Information has been important event before the advent of computers. However, with the advent of computers, the quantum of information generated increased increasing the need to protect it. Further, with the advent of the mobile phone, this quantum has significantly increased since the masses were now generating a huge amount of data, which to them, was important. As the quantum of information generated and it's availability via computer network or in case of mobiles, via cellular networks, increased, so did the attraction (and benefit) for those who were interested in circumventing and getting access to the information. This competition between allowed and disallowed access has led to much progress in the field of security. However, at the end of all the technological progress, security is still means within the hands of human and human with their perspective and behavior tend to either increase or circumvent security. If the deployed models and implementations of security are not found usable (or convenient) by the users while achieving their objective (business goals), humans adapt themselves or processes which render the security mechanism less effective. It is not uncommon, in the context of a developing country, to visit a bank and notice that passwords and credentials are stuck to the monitors (screens) of the bank officials or officials sharing the same in a loud voice across the designated areas. Such a behavioural response to a security procedures in a financial institution is probably the proverbial tip of the iceberg of how humans respond to security measure.

While the above statements warrant attention, the users in these cases are fairly literate and professional in their domain. On the other hand, with the rapid adoption of mobile phone and mobile phone based applications, the low-literate masses are now faced with a situation of discerning what is important, what is private, how to respond to needs of information protection.

We believe the problem could be much worse and the users are at significant risk in terms making appropriate choices of measures of security.

Recent body of work in terms of attempts to break into user passwords is impressive to say the least. In the aftermath of compromise of linked.in databases and RockYou databases, releases of newer software like oclHashcat, theoretical work of Philippe resulting in the rainbow tables being built, parallel computations with GPU, is just the beginning, is what we feel. To give an idea, a password like "Ph'nglui mglw'nafh Cthulhu R'lyeh wgah'nagl fhtagn1 "was cracked in a very short time.

3. LITERATURE SURVEY

A study done [59], indicates that users seems to have about 7 passwords which they tend to use across sites. [42] covers a study in Switzerland on how illiterate users use their mobile phone for various purposes and report that contacts and SMS are the primary areas of attention. It also argues for not using text-free UI since uses would not want to be identified and segregated based on their literacy. [42] Argues for complementing the existing interfaces with speech, voice and visuals to aid the users. [62] advocates the use of a cultural tool (Rangoli) for adaptation of the Phonebook for the low-literate users in India. [12] Reports in work done for mobile money transfers for illiterate and low-literate users that text based UIs are less effective and the interfaces should be either voice based or rich media based to be of aid to the users. In an another work [37], the researchers report that the mobile phone is now the "personal computer" of the developing world in the context of mobile based learning for rural children, there is an opportunity.

While we found that a significant amount of work is happening in the area of ICT4D, we were unable to locate much work in the area of Information Security and in Usable Security for low-literate users.

4. OBJECTIVE

As the literature survey indicates, there has been significant amount of work happening in the area of ICT4D in various areas, including financial areas like banking. Also, it is inevitable that application, services and systems would be made available to the low-literate users over mobile phones in the years to come. This 'push' would also be amplified by the 'pull' from users which increasingly, at least the sub-30 years old population, increasingly adopts smartphones. One example of such 'consumer pull' is the adoption of 'WhatsApp' in large numbers across India. However, to the best of our awareness, there has been not qualitative study of how low-literate users use mobile phones from a information security perspectives and their practices, conceptual model et cetera.

The objective of this study is to develop an understanding of the security practices, password properties, privacy concerns and security choices in the context of mobile phone usage of low-literate users.

.

5. METHOD

Our attempts to identify locations where we could study a sizable population of low-literate users on a continuous basis lead us to large private organization and an educational campus where the support staff were likely to have levels of education which were of interest to us as well as where users used mobile phones per significantly adopted as part of daily lives. We took approval from the Administrative Officers of the private organization and collected Demographic information about the house-keeping staff. The total strength of the staff on the campus is a little more than 150 and operate in 3 shifts. For the purpose of our study we interacted with the staff in the morning and afternoon shifts due to logistical constraints. As per the initial information collated, we shortlisted 59 users who were working on the campus with education levels between standard 4 and standard 8 (both inclusive) across two shifts. Of these, 14 were rejected either because they were in the night shift or did not offer consent to the Contextual Inquiry. Overall, we studied 45 users from the campuses. Of these, 3 were Female and 42 Male. Of the 45 users, 44 were involved in house-keeping activities and one was with Facility management. We did not select users working in the late-night shift.

We also recruited another 15 users outside the campus, namely 1 security guard (Male), shopkeepers (1 Male, 1 Female), 3 household helps (Female), 5 drivers (Male) and 4 homemakers (Female). Thus the total sample size for this qualitative study is 60 users.

The Semi-Structured Interviews were conducted in the National Language Hindi or Marathi, the State Language; whichever was comfortable to the user.

The interviews focused on the following:

Password Management: How does the user manage his/her password? How frequently do they change them? How do they store them? What do they do when passwords are shared or compromised? How do they keep easy to recall and difficult to guess passwords? How do they share passwords?

Password Properties: What kind of password do user prefer? What is their choice between PINs, Patterns and Text passwords? What is their preferred language for textual passwords? How do they chose Patterns? How do they chose PINs?

Asset Valuation, Threat Perception and Risk Mitigation: Which aspect / content is important to the user? Will the loss of the phone affect their lives? How significantly? What is the value of a phone? What is the role of the phone in their life? Do they share phones? Will they loan a phone to a stranger? What do they do when a phone is damaged? How do they service their phones?

Knowledge Acquisition: How does the user learn new features? What features of the phone does the user use? Does he try using other features? What does the user do when things go wrong? How does the user comprehend things? Does the user build a conceptual model of working? Can the user demonstrate a feature, example phonebook to the researcher and explain how things work? How does the user learn about new mobile applications, like Whatsapp? How does the user use such applications?

The users were explained the background of the work and their consent was sought to record the interviews. All the interviews were recorded in audio format and then subsequently transcribed. Field notes were made of observations and photographs of the users and their artifacts were taken. In some cases where the user demonstrated usage of a phone feature, video recordings were also done.

After the Contextual Inquiries and Analysis, the findings were consolidated in an inductive (data driven) manner using Affinity Diagrams as a tool. Affinity Diagrams helped us consolidate the findings into clusters of patterns, high-level insights and design interventions.

6. USER PROFILE

While we chose the locations from a perspective of colocation of users, we believe, it offered us good variability of users. Apart from the two locations/campuses, we also interviewed other users. There were 49 Males and 11 Females. The average age was 34 years, with a minimum age of 19 years and a maximum of 53 years.36 users were of age greater than or equal to 30 and 22 were less than or equal to 30, we missed the data for 2 users. Education was between Standard 4 and Standard 8, both inclusive, and as provided by the State Government. Professions of the users were house-keeping, house help, shopkeeper, homemaker, driver and security guards. Users had received their education in Hindi and in Marathi. Users were experienced in using phones running Android OS, Symbian (Java ME) and standard feature phones.

7. FINDINGS, INSIGHTS AND IMPLICATIONS

7.1 Easy to Recall, Difficult to Guess

Users have the traditional challenge [57] between choosing an easy to recall and difficult to guess passwords. They also exhibit attributes as reported in [57], namely, proper names, birthdates, personal characteristics et cetera. While making this decision, they seemed skewed towards a very easy to recall password in their context. This makes their passwords significantly vulnerable to attack and misuse. Compared to this, literate users in developed countries have interesting passwords [58]. In this context, Password Cues can be provided to users to help recall their passwords as well setting passwords. While setting passwords, compromise/strength meters can indicate passwords or PINs which can be easily compromised. This is a small intervention which can be easily set as part of the password policy but, over a period of time, people will set comparatively better passwords. This can be complemented by a system where cues are provided to recall the set password. These cues can be drawn possibly from a taxonomical/ontological tree of the set password. One can conceptualize Single Sign On with Localized Cues for enabling users to remember only on password. The recall ability of this password can be increased by providing the user with local and contextualized cues pertinent to the user. After having the user a password which can be computationally proven to be difficult to guess and at the same time, since it has contextual information, easy to recall, the system can use a Single Sign-On would take away the burden from the user to remember many passwords. From a search space perspective (attack space), the user could be encouraged to choose longer text as passwords. Such longer passwords can make the security higher for the user, while the custom cues ensure that the only the user is able to recall the

passwords. Since most of the attack mechanism still are 'smarter' brute force techniques, longer passwords would keep the user comparatively safer.

7.2 Numerical Passwords

Users seem to have a preference for numerals as compared to text – whether English or local language since the dynamics of alphabet construction in local language or words in English seem more than choosing a digit. Also, due to the advent of mobile numbers and use, users have committed to their memory 10 digit numbers which belong to individuals close to them. This factor could be exploited to construct strings of quartets from mobile numbers, separated by white space, to construct difficult to guess passwords but with significant length. Cues could be given to the user in terms of names of entities to whom these quartets have been mapped. However, this approach needs to be investigated from a cryptographic space perspective whether it offers enough entropy to withstand an attack. One can conduct a longitudinal experiment whether people are able to generate 10 digit unique numbers and recall them without errors. If this Design intervention works, it could also help people who are used to recalling mobile numbers – the duration of reset of the mobile number could be linked to the strength offered by the 10 digit number.

7.3 PINs, Patterns and Text

The users seemed to prefer Patterns over PINs over Text input of passwords. While inherently, they would prefer local text, due to the cognitive load associated with the spellings of words and the extra motor actions required for entry of text, patterns seemed to be preferred. In patterns, too, one can see the bias towards choosing their names or family member's name as a basis for selection of a character for pattern. Since pattern grids on mobile phones are set to a default value of 3x3 or 4x4, users tend to choose English character set as pattern set to draw from. If the grid were to have an extra line, in the default setting, it could be possible that users choose their local language character set as a pattern set. Once could conduct an experiment to ascertain if such a position is recommended. Another option could be calling pattern locks as Rangoli Locks. Culturally, in India, people are familiar with Rangoli and have used that to create beautiful patterns. If the positioning of a pattern lock is converted into a Rangoli, it is quite possible that users could draw interesting patterns, which they remember, but offer computationally strong passwords. It seems the initial conditioning and propagation via social training has oriented towards keeping their names as patterns – an application which acts as a central lock to the system, like a single sign-on but is rooted in the cultural way of a Rangoli could be interesting longitudinal experiment.

The other aspects is that the higher penalties in terms if a phone requiring resetting if the PIN is incorrect can be rectified by requiring longer PINs – just like longer Passwords seem to have a better usability for literate users, longer PINs modelled on the lines of Phone Numbers could be evaluated.

Yet another intervention could be in terms of Remote On-Device Management for assistance

7.4 Privacy and Asset Valuation

Users seem to have upgraded the phone from a communication devices to an information store. The first step in this process is the maximum use of phonebook since that is the application that they are first initiated in 'phoneland'. Users seem to have adapted the phone book into various scenarios such

7.4.1 Storage of ATM PINs .

This theme by far dominates the usage amongst the user. Informal interviews and verification amongst literate/graduates shows this to be a more common phenomenon. A typical entry would entail entering the bank's name and then the PIN in the text-area for the phone. In cases, where the user understand the importance and risk of PIN compromise, they use fictitious names instead of Bank names. Few outlier cases went a step further and embedded the ATM within a 10 digit number. This aspect, to the researcher, was interesting.

This shows that the users are able to associate value with information (PIN) and resort to mechanism to secure it in a manner such the 'key' is always with them (as the carry the phone) and at the same time sufficiently disguised to protect from accidental or intentional snooping. It would also not get others suspect if the user inspects the phone during an ATM transaction, while he is really accessing the PIN.

The seems a strong association that if the content is numeric then the data is most likely to find it's way to the phonebook. One could conduct a survey of phonebook to ascertain the distribution of data across various applications on the mobile. This numeric data set which is known to the user can then be exploited to construct a secure random code for the user. In such cases, the application can use a cue in the form of the name/text entry under which the number is stored while the actual number is utilized as a longer string as a password. This experiment conducted as a variation of Lorrie's work could possibly be interesting in terms of result. A single sign-on application can then be constructed which utilizes this as a data store for generating passphrases.

7.4.2 Asset Valuation

As the device accumulates data, namely in the form of contacts and subsequently in terms of photographs, video clips, its valuation for the user increases. From a valuation perspective, for the users, the most important content seems to that housed in the PhoneBook followed by Personal Photos and Videos. Users are also aware of the presence of memory cards and the differentiation between memory cards and phone memory. They tend to choose the former for their storage. They also tend to migrate their contacts to the SIM card. In terms of information security, this indicates their assessment of the phone as a device which houses 2 stores, namely on the SIM card (SIM memory) and the memory card. While conceptually having split the phone into these three parts – the phone per se, the SIM and the Memory card, they accord highest valuation to the SIM followed by the Memory card and comparatively lower to the Phone. As the stores acquire more content, the valuation for the user increases. However, the valuation seems bounded at this level, compared to a literate person, who is likely to use the phone for purposes such as email, social networking, ecommerce, netbanking et cetera. Thus, literacy impedes the upper bound of valuation of the phone for a less literate person, as he is conceptually not able to use the phone for higher functions.

Our view is that one could have an asset score like a CIBIL score for the smart-phone, which is on the landing-page/home-page/home-screen on the phone. This score which could also use an innovative visual design, could in the simplest case be a band /spectrum which indicates the valuation of the phone in terms of number of contacts or media contents. In case these exceed a threshold, the user could be prompted to a mechanism, such as

upload to a cloud, where the contents are archived. Again, the cloud archive could be protected with a single sign-on as described earlier in the document.

7.4.3 Privacy

Users are aware that there is a potential for misuse if the content they value is compromised. The most area of concern for them is personal and family phots and videos. Current practices of users include setting application or folder level locks so that the content is not available or visible to others with whom they have to share due to cultural obligation or social demands. If possible users do not share phones and there is a noticed trend that phone-sharing is decreasing and personal use is increasing.

This desire for protection of what is of value offers an opportunity for Design intervention in terms of privacy measure as interpreted in the context of the users. While traditional privacy measures have considered a three level gradation – namely, public, limited circulation and not-for-circulation, these could be visited in the socio-cultural contexts of the Indian users. Special interfaces or controls could be added to the camera application and media players which generate contents with inherent higher levels of privacy, that is, not-for-circulation. User could be prompted for these are inadvertently been selected by application for sharing for sending. Such identified, rather, all media could be made to reside only on a secure area of the memory card which could be accessed by a secure mechanism. A mechanism on which the phone owner has control after due authentication.

7.5 Phone Valuation – Information Valuation v/s Commodity valuation Security of Data v/s Security of Phone (hardware)

These user statements indicate, two perspectives – one in which, as earlier highlighted that the phone has been reduced to a commodity. The valuation attached to this phone does not go beyond the price paid for the "bare metal". While the other perspective indicates that the value of the phone increases as it is increasingly used for professional and personal use. In these cases, the value is in proportionate increase to the quantum of data stored by the users in Phonebooks, SMS and Media Gallery. The value attached in media, is more to personal or family content as opposed to media associated with entertainment. This is due to the view held that entertainment related media can be replenished in the even to a loss but, personal media cannot be.

Such a view offers an opportunity to Design and deploy solutions which offer low cost archival services – which could start from a simple memory card to CD transfer (which albeit do exist with photography studios) to more digital and online services. The 'safe' area of the memory card where in the images and videos lie could be uploaded to a more permanent location.

Apart from the "information" users, there are users who view the phone more from a consumption perspective and for them the phone is a commodity from a different perspective. The word "timepass" is a more rooted word in this context. It indicates non-productive usage of time and is generally frowned upon by elders. It offers them leisure or a gateway to a world which is distinct and different from their daily lives; lives where they are not happy with their professions. Most of the users in this segment us the phone for video consumption of Bollywood and Hollywood media. While the initial value of songs, mp3 does exist, there seems to be a new interest in video based content. Typically, users would load the content from freely available internet connections and then share within their social circles via WhatsApp or via Bluetooth.

From a Design Intervention, these users are morely likely to be interested in MicroNetworks – than usual social networks. Such users are more likely to use WhatsApp than Facebook. Such a well designed MicroNetwork would be more popular and can be used for interventions which aid in the growth of the individual – such as game based learning et cetera

7.6 Secure Storage

7.6.1 Archival Strategies

Users seem to adopt the phone as an instant storage or an archival point. The conceptual model seems to regard the phone's Phonebook and memory card as a point where important information can be conveniently stored and immediately retrieved when in need. The paradigm seem that if a user classifies the data as numeric – he is most likely to store it in the Phonebook. The Phonebook has thus evolved into a store which any valuable, as assessed by the user, numeric content makes it ways. Thus apart from phone contacts, users seem to use it for ATM pins, while the textual data mapping to the name is usually a misspelled word. This also is likely since the Phonebook was a cognitive association to the diary which have been traditionally maintained by users. Just like the physical diary is a portable means for record keeping than just recording phone numbers, users seem to be repurposing the PhoneBook for record keeping.

At the very base level, in terms of Design Intervention, the Phone book can be re-conceptualized as a Record Keeper and possibly re-designed with this perspective.

The other interpretation is that any Information of value to the user seems to be recorded in the Phonebook. This suggest that the Phone can provided a SecureStorage facility where by the user could be allowed to record things of importance to him/her Easy to Recall, Difficult to Guess

7.7 Social Training and Conceptual Models

Users acquire a lot of information from their micro-social-networks. This can be leveraged to provide them learning content which could teach them the correct conceptual models. Learning interventions which are self-paced and can be used. One example of this is 'Tantra Mantra'. There is significant opportunity to evaluate social learning using different learning methodologies. However most of these methodologies should make use of Video as a media as compared to text, given the literacy context and the affinity of the users towards Video.

Users also seem to have conceptual models developed based on incorrect information. For example, one of the users had a high-end Sony Ericsson. While he had purchased the device specifically for playing games – he had only one game on it. When queried he said that he wanted more games, but, his friends told him that there is space only for one – hence he has only one game. Due to his inability to ascertain the amount of storage he had, (he had 1 GB of memory card in addition to phone memory), he was unhappy that he was stuck with only one game. Apart from this, is the notion of "software marna", a colloquial word indicating resetting or re-installing the software on the phone. Incase an application breaks down frequently, possibly due to its own bug, users tend to reset the entire phone. Typically, this entails a visit to the local store who charges a few for this service. In such contexts, one could design interventions which allow remote diagnostic to the user. If the user indicates to an application that he perceives something is wrong with his/her

phone, a remote agent, which is either a human agent or a software agent can then provide immediate assistance.

7.8 Behavioural (PDCA – Plan Do Check Act)

Our users seem to be aware of the potential risks and threats to their (information) devices. Also, if an incident seems to affect them, they change their usage behavior. For example, removing memory card before giving device before "software maarna", valuing SIM card more since it has contacts and treating the rest of the phone as a commodity, putting password locks on "personal images" which they receive via WhatsApp, restrict child's access to the phone. In a way, these seem to stem from experiences which possibly caused harm to their interests. In a way, users have a set of

"Do" based on experiences and "Act" in a certain modified way if an incident happens. However, what seems to be missing is a conspicuous "Plan" – which is enlisting what could happen and hwat is important to them, updating "Do" based on "Plan" , then "Check" or monitor events to ascertain if listed events have happened and accordingly "Act" to modify to change Plan and Do actions.

This could be a potential intervention option to have a system like Plan-Do-Check-Act (PDCA) monitoring application. This application which mimics the ISO 27000 series model can be used to assign various compliance levels to the mobile application. Since the user may not be able to identify all the potential risks with the mobile, the guidelines and checklist which are readily available could be adapted to the context of the mobile phone. The entire PDCA process can be automated and the user provided a better level of security monitoring.

8. CONCLUSIONS AND FUTURE WORK

India will have an increased adoption of smart phones and feature phones across the population, where people, despite their apparent shortcomings such as literacy, will find workarounds to adopt new changes and use technology. However, this adoption and use of technology for everyday life, exposes them to a significant amount of security risks and privacy issues. While the users are aware and trying their best to deal with whatever wherewithal they have, it is clearly inadequate. There are many issues pertaining to password composition, password management, protection of privacy, password policies, inadequate conceptual models, lack of trainings/course materials for their contexts, advices from 'technology quacks' , need for privacy, privacy measures and information inaccuracy. Another important aspect is that the Mobile Application area is a networked ecosystem than an isolated device running a standalone program. The mobile is no longer just a communication device but is an "always 'on' networked computer". In this ecosystem, with its network effect, compromise of any component due to poor usability has a cascading/ network effect.

While the users under study may have lower literacy and lower levels of income, but, their needs for privacy and protection are no different from those with higher affordances when it comes to personal media.

This qualitative study establishes that there is a need for Design Interventions such as in terms of password policy designs, guided authentications, single sign-on, training modules and user interface standards/guidelines which will help the users develop a reasonably credible form of response to security and privacy issues on mobile devices. Given these requirements, Usable Security and Privacy needs to be considered from a multi-vector perspective or a framework perspective which touches various aspects of the mobile phone ecosystem in a cohesive manner. The framework or guidelines would then aid the interplay between various components to provide the user with a credible amount of protection. One way could be adaption of the 'Plan-Do-Check-Act' ISO27000 model for the context of the users with appropriate levels of usable automation.

Based on our insights into the usability needs of low-literate users in the area of security and privacy whilst using mobile applications, we are devising a series of experiments which try to ascertain the usability performance of the system when components of it are migrated to instruments familiar to the user. One such experiment is about the recallability of passwords if the passwords are allowed to be set in local languages. Other experiments would be in the area of guided passwords which the user can chose and provided cues for recall.

9. ACKNOWLEDGMENTS

We would like to thank all our users who patiently participated with the study. We would also like to thank the administration of Indian Institute of Technology Bombay and Tata Consultancy Services Limited who allowed us access to facilities to conduct this user study. The first author would also like to thank interns and members of the TCS Innovation Labs who aided in this study.

10. REFERENCES

[1] Joshi, A., Rane, M., Roy, D., Emmadi, N., Srinivasan, P., Kumarasamy, N., Pujari, S., Solomon, D., Rodrigues, R., Saple, D. G., Sen, K., Veldeman, E., and Rutten, R. 2014. Supporting treatment of people living with HIV / AIDS in resource limited settings with IVRs. In Proceedings of the 32nd annual ACM conference on Human factors in computing system. CHI '14. ACM, New York, NY, USA, 1595-1604. DOI= http://doi.acm.org/10.1145/2556288.2557236.

[2] De Angeli, A., Athavankar, U., Joshi, A., Coventry, L., Johnson, G. 2004. Introducing ATMs in India: a contextual inquiry.

[3] Beyer, H., Holtzblatt, K. 1998. Contextual design: defining customer-centered systems. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[4] Introduction - Rapid Contextual Design. Retrieved June 2015 from https://www.safaribooksonline.com/library/view/rapid-contextual-design/9780123540515/.

[5] Harboe, G. and Huang, E. M. 2015. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. CHI '15. ACM, New York, NY, USA, 95-104. DOI= http://doi.acm.org/10.1145/2702123.2702561.

[6] Hackos, J. T. and Redish, J. C. 1998. User and Task Analysis for Interface Design. John Wiley & Sons, Inc., New York, NY, USA.

[7] Panjwani, S. and Cutrell, E. 2010. Usably secure, low-cost authentication for mobile banking. In Proceedings

of the Sixth Symposium on Usable Privacy and Security. SOUPS '10. ACM, New York, NY, USA, Article 4 , 12 pages. DOI= http://doi.acm.org/10.1145/1837110.1837116.

[8] Panjwani, S., Ghosh, M., Kumaraguru, P., and Singh, S. V. 2013. The paper slip should be there!: perceptions of transaction receipts in branchless banking. In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. MobileHCI '13. ACM, New York, NY, USA, 328-331. DOI= http://doi.acm.org/10.1145/2493190.2493236.

[9] Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., Chen, J., and Brewer, E. A. 2011. Computing security in the developing world: a case for multidisciplinary research. In Proceedings of the 5th ACM workshop on Networked systems for developing regions. NSDR '11. ACM, New York, NY, USA, 39-44. DOI= http://doi.acm.org/10.1145/1999927.1999939.

[10] Cutrell, E. 2011. Technology for emerging markets at MSR india. In Proceedings of the ACM 2011 conference on Computer supported cooperative work. CSCW '11. ACM, New York, NY, USA, 9-16. DOI= http://doi.acm.org/10.1145/1958824.1958827.

[11] Medhi, I., Gautama, S. N. N., and Toyama, K. 2009. A comparison of mobile money-transfer UIs for non-literate and semi-literate users. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '09. ACM, New York, NY, USA, 1741-1750. DOI= http://doi.acm.org/10.1145/1518701.1518970.

[12] Sambasivan, N., Cutrell, E.,Toyama, K., and Nardi, B. 2010. Intermediated technology use in developing communities. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '10. ACM, New York, NY, USA, 2583-2592. DOI= http://doi.acm.org/10.1145/1753326.1753718.

[13] Parikh, T. S. and Ghosh, K. 2006. Understanding and Designing for Intermediated Information Tasks in India. IEEE Pervasive Computing. 5, 2 (April 2006), 32-39. DOI http://dx.doi.org/10.1109/MPRV.2006.41.

[14] Joshi, A., Ganu, A., Chand, A., Parmar, V., and Mathur, G. 2004. Keylekh: a keyboard for text entry in indic scripts. In Proceeding of CHI '04 Extended Abstracts on Human Factors in Computing Systems. CHI EA '04. ACM, New York, NY, USA, 928-942. DOI= http://doi.acm.org/10.1145/985921.985950.

[15] Chipchase, J. 2006. How do you manage your contacts if you can't read or write?. interactions - Waits & Measures. 13, 6 (November 2006), 16-17. DOI= http://doi.acm.org/10.1145/1167948.1167966.

[16] Holtzblatt, K. 2005. Introduction. Communications of the ACM - Designing for the mobile device. 48, 7 (July 2005), 32-35. DOI= http://doi.acm.org/10.1145/1070838.1070862.

[17] Blom, J., Chipchase, J., and Lehikoinen, J. 2005. Contextual and cultural challenges for user mobility research. Communications of the ACM - Designing for the mobile device. 48, 7 (July 2005), 37-41. DOI= http://doi.acm.org/10.1145/1070838.1070863.

[18] White, G. 2008. FEATURE: Designing for the last billion. interactions - Toward a model of innovation. 15, 1 (January 2008), 56-58. DOI= http://doi.acm.org/10.1145/1330526.1330544.

[19] Medhi, I., Patnaik, S., Brunskill, E., Gautama, S. N. N., Thies, W., and Toyama, K. 2011. Designing mobile interfaces for novice and low-literacy users. AACM Trans. Comput.-Hum. Interact. 18, 1, (May 2011), 28 pages. DOI= http://doi.acm.org/10.1145/1959022.1959024.

[20] Abraham, R. 2007. Mobile phones and economic development: Evidence from the fishing industry in india. Inf. Technol. Int. Dev. 4, 1 (October 2007), 5-17. DOI= http://dx.doi.org/10.1162/itid.2007.4.1.5.

[21] Heffernan, C. and Nielsen, L. 2007. The livestock guru: The design and testing of a tool for knowledge transfer among the poor. Inf. Technol. Int. Dev. 4, 1 (October 2007), 113-121. DOI= http://dx.doi.org/10.1162/itid.2007.4.1.113.

[22] Esselaar,S., Stork, C., Ndiwalana, A., and Deen-Swarray, M. 2007. Ict usage and its impact on profitability of smes in 13 african countries. Inf. Technol. Int. Dev. 4, 1 (October 2007), 87-100. DOI= http://dx.doi.org/10.1162/itid.2007.4.1.87.

[23] Schaefer, R. 2009. The epistemology of computer security. ACM SIGSOFT Software Engineering Notes. 34, 6 (December 2009), 8-10. DOI= http://doi.acm.org/10.1145/1640162.1655274.

[24] Toyama, K. 2013. Reflections on HCI for development. interactions. 20, 6 (November 2013), 64-67. DOI= http://doi.acm.org/10.1145/2527298.

[25] Baumer, E. P. S. and Silberman, M. S. 2011. When the implication is not to design (technology). In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '11. ACM, New York, NY, USA, 2271-2274. DOI= http://doi.acm.org/10.1145/1978942.1979275.

[26] Renaud, K. and Biljon, J. V. 2008. Predicting technology acceptance and adoption by the elderly: a qualitative study. In Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology. SAICSIT '08. ACM, New York, NY, USA, 210-219. DOI= http://doi.acm.org/10.1145/1456659.1456684.

[27] Steinfield, C., Wyche, S., Cai, T., and Chiwasa, H. 2015. The mobile divide revisited: mobile phone use by smallholder farmers in Malawi. In Proceedings of the Seventh International Conference on Information and Communication Technologies and Development. ICTD '15. ACM, New York, NY, USA, Article 8 , 9 pages. DOI= http://doi.acm.org/10.1145/2737856.2738022.

[28] Wyche, S. P., Densmore, M., and Geyer, B. S. 2015. Real mobiles: Kenyan and Zambian smallholder farmers' current attitudes towards mobile phones. In Proceedings of the Seventh International Conference on Information and Communication Technologies and

Development. ICTD '15. ACM, New York, NY, USA, Article 9 , 10 pages. DOI= http://doi.acm.org/10.1145/2737856.2738013.

[29] Boehner, K., Vertesi, J., Sengers, P., and Dourish, P. 2007. How HCI interprets the probes. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '07. ACM, New York, NY, USA, 1077-1086. DOI= http://doi.acm.org/10.1145/1240624.1240789.

[30] Reid, R. C. and Gilbertm, A. H. 2010. Using the Parkerian Hexad to introduce security in an information literacy class. In Proceedings of InfoSecCD '10 conference on 2010 Information Security Curriculum Development . ACM, New York, NY, USA, 45-47. DOI= http://doi.acm.org/10.1145/1940941.1940953.

[31] Karunanayake, A., Zoysa, K. D., and Muftic, S. 2008. Mobile ATM for developing countries. In Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture. MobiArch '08. ACM, New York, NY, USA, 25-30. DOI= http://doi.acm.org/10.1145/1403007.1403014.

[32] John (Jong Uk) Choi, Soon Ae Chun, and Joo-Won Cho. 2014. Smart SecureGov: mobile government security framework. In Proceedings of the 15th Annual International Conference on Digital Government Research. dg.o '14. ACM, New York, NY, USA, 91-99. DOI= http://doi.acm.org/10.1145/2612733.2612756.

[33] Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., and Möller, S. 2011. On the need for different security methods on mobile phones. In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. MobileHCI '11. ACM, New York, NY, USA, 465-473. DOI= http://doi.acm.org/10.1145/2037373.2037442.

[34] Guo, M., Bhattacharya, P., Yang, M., Qian, K., and Yang, L. 2013. Learning mobile security with android security labware. In Proceeding of the 44th ACM technical symposium on Computer science education. SIGCSE '13. ACM, New York, NY, USA, 675-680. DOI= http://doi.acm.org/10.1145/2445196.2445394.

[35] Geater, J. A. 2013. Security composition in the real world: squaring the circle of mobile security with contemporary device economics. In Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices. SPSM '13. ACM, New York, NY, USA, 1-2. DOI= http://doi.acm.org/10.1145/2516760.2516761.

[36] Kumar, A., Tewari, A., Shroff, G., Chittamuru, D., Kam, M., and Canny, J. 2010. An exploratory study of unsupervised mobile learning in rural India. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '10. ACM, New York, NY, USA, 743-752. DOI= http://doi.acm.org/10.1145/1753326.1753435.

[37] Smyth, T. N., Kumar, S., Medhi, I., and Toyama, K. 2010. Where there's a will there's a way: mobile media sharing in urban india. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '10. ACM, New York, NY, USA, 753-762. DOI= http://doi.acm.org/10.1145/1753326.1753436.

[38] Kumar, D., Martin, D., and O'Neill, J. 2011. The times they are a-changin': mobile payments in india. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '11. ACM, New York, NY, USA, 1413-1422. DOI= http://doi.acm.org/10.1145/1978942.1979150.

[39] Gitau, S., Marsden, G., and Donner, J. 2010. After access: challenges facing mobile-only internet users in the developing world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '10. ACM, New York, NY, USA, 2603-2606. DOI= http://doi.acm.org/10.1145/1753326.1753720.

[40] Rangaswamy, N. and Sambasivan, N. 2011. Cutting Chai, Jugaad, and Here Pheri: towards UbiComp for a global community. Personal Ubiquitous Computing. 15, 6 (August 2011), 553-564. DOI= http://dx.doi.org/10.1007/s00779-010-0349-x.

[41] Knoche, H., Huang, J. Text is not the enemy: How illiterates' use their mobile phones. (May, 2012). Retrieved November 2015 from http://cs.swan.ac.uk/nuisworkshopCHI/papers/TextIsNotTheEnemy-NUI-Workshop.pdf.

[42] Census of India 2011. Retrieved May 2015 from http://censusindia.gov.in/2011-prov-results/paper2/data_files/india/Rural_Urban_2011.pdf.

[43] Teledensity of India. Retrieved May 2015 from https://data.gov.in/catalog/tele-density-india.

[44] Highlights of Telecom Subscription Data. Retrieved May 2015 from http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/PR-TSD-120315.pdf .

[45] State-wise Literacy Rates (1951-2011). Retrieved May 2015 from http://planningcommission.nic.in/data/datatable/data_2312/DatabookDec2014%20224.pdf.

[46] Drop-out Rates in Classes I-V and I-VIII and I-X in India. Retrieved May 2015 from http://planningcommission.nic.in/data/datatable/data_2312/DatabookDec2014%20227.pdf.

[47] Percentage of Children who can Read, Read English & Do Arithmetic. Retrieved May 2015 from http://planningcommission.nic.in/data/datatable/data_2312/DatabookDec2014%20231.pdf.

[48] Households having various assets (Mobiles et cetera). Retrieved May 2015 from http://planningcommission.nic.in/data/datatable/data_2312/DatabookDec2014%20329.pdf.

[49] Education Specific Mean Years of Schooling of Work Force. Retrieved May 2015 from http://planningcommission.nic.in/data/datatable/data_2312/DatabookDec2014%20232.pdf

[50] Total Drop-out Rates in School Education, Table 22. Retrieved May 2015 from http://mhrd.gov.in/sites/upload_files/mhrd/files/statistics/EAG2014.xlsx.

[51] Mobile VAS in India Report. Retrieved May 2015 from http://www.iamai.in/pdf/AnnualReport201314LowRes.pdf.

[52] Telecom Regulatory Authority of India, Recommendations on Application Services. (May 2012). Retrieved May 2015 from http://www.trai.gov.in/writereaddata/recommendation/documents/as140512.pdf.

[53] Telecom Regulatory Authority of India, Consultation paper. Retrieved May 2015 from http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/1-main.pdf.

[54] Bonneau, J. and Shutova, E. 2012. Linguistic properties of multi-word passphrases. In Proceedings of the 16th international conference on Financial Cryptography and Data Security. FC'12, Jim Blyth, Sven Dietrich, and L. Jean Camp (Eds.). Springer-Verlag, Berlin, Heidelberg, 1-12. DOI= http://dx.doi.org/10.1007/978-3-642-34638-5_1.

[55] Kuo, C., Romanosky, S., and Cranor, L. F. 2006. Human selection of mnemonic phrase-based passwords. In Proceedings of the second symposium on Usable privacy and security. SOUPS '06. ACM, New York, NY, USA, 67-78. DOI= http://doi.acm.org/10.1145/1143120.1143129.

[56] Brown, A. S., Bracken, E., Zoccoli, S. and Douglas, K. (2004), Generating and remembering passwords. Appl. Cognit. Psychol., 18: 641–651. doi: 10.1002/acp.1014.

[57] ArsTechnica.com. 2013. How the Bible and YouTube Are Fueling the Next Frontier of Password Cracking. Retrieved November 2015 from http://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking/.

[58] Goodin, D. 2013. “thereisnofatebutwhatwemake”—Turbo-charged cracking comes to long passwords | Ars Technica. (August 2013). Retrieved November 2015 from http://arstechnica.com/security/2013/08/thereisnofatebutwhatwemake-turbo-charged-cracking-comes-to-long-passwords/.

[59] Goodin, D. 2013. Anatomy of a hack: How crackers ransack passwords like “qeadzcwrsfxv1331” | Ars Technica. (May 2013). Retrieved November 2015 from http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/.

[60] Anderson, N. How I became a password cracker | Ars Technica. (March 2013). Retrieved November 2015 from http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/.

[61] Goodin, D. 2012. 25-GPU cluster cracks every standard Windows password in <6 hours | Ars Technica. (December 2012). Retrieved November 2015 from http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/.

[62] Goodin, D. 2012. Why passwords have never been weaker—and crackers have never been stronger | Ars Technica. (August 2012). Retrieved November 2015 from http://arstechnica.com/security/2012/08/passwords-under-assault/.

[63] Florencio, D. and Herley, C. 2007. A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web. WWW '07. ACM, New York, NY, USA, 657-666. DOI= http://doi.acm.org/10.1145/1242572.1242661.

[64] Avoine, G., Junod, P., and Oechslin, P. 2008. Characterization and Improvement of Time-Memory Trade-Off Based on Perfect Tables. ACM Trans. Inf. Syst. Secur. 11, 4, Article 17 (July 2008), 22 pages. DOI= http://doi.acm.org/10.1145/1380564.1380565.

[65] How White Card Fraud Works? Retrieved July 2015 from http://www.sid.in-berlin.de/nedkelly-world/howwhitecardfraudworks.html.

[66] Joshi, A., Welankar, N., Naveen, B.L., Kanitkar, K., and Sheikh, R. 2008. Rangoli: a visual phonebook for low-literate users. In Proceedings of the 10th international conference on Human computer interaction with mobile devices and services. MobileHCI '08. ACM, New York, NY, USA, 217-223. DOI= http://doi.acm.org/10.1145/1409240.1409264.