Security and privacy design considerations for low-literate users in developing regions

Shrirang Mare, Aditya Vashistha and Richard Anderson
University of Washington

ABSTRACT

With the increasing adoption of mobile phone, the previously hard-to-reach low-literate low-income users in developing regions can now be reached through their mobile phones. Government and other agencies are providing mobile services such as banking and healthcare to this marginalized population to improve their quality of life. In this paper we highlight the security and privacy challenges in developing solutions for this user group.

1. INTRODUCTION

Mobile phone adoption throughout the world has rapidly increased in recent years. In fact, mobile phone growth is higher in the developing regions compared to developed regions [9, 22]. Internet is also becoming accessible to everyone: today, about 95% world population has 2G access, and 73% population has 3G/4G access [12]. With a mobile phone in nearly every household, and the widespread Internet access, we can now reach the previously hard-to-reach low-literate low-income users in developing regions and provide them with (limited) services such as banking and healthcare to improve their quality of life.

Designing technological solutions for developing regions is challenging due to the various constraints of the developing regions such lack of infrastructure, poor (or lack of) network connectivity, low literacy, and so forth [6]. Even translating existing solutions from the developed regions is challenging. Illiteracy is a significant barrier to understanding user requirements (through traditional means, e.g., recruiting and testing) and to develop systems that the illiterate or low-literate users can understand.

A significant population in developing regions has low language literacy (low-literate in the traditional sense, i.e., with respect to English or the local language) or low technology literacy (cannot use technology, e.g., cannot operate a mobile phone). Language literacy and technology literacy are not always correlated. People who are language literate can be technology low-literate, whereas language low-literates can learn enough to operate devices and become technology literates. As we introduce new mobile technology and services to this marginalized population, it is important to have reasonable security and privacy measures in place to build users' confidence in the technology they use, so they continue to adopt and use the technology.

Most of the previous work on low-literate low-income users has been focused on understanding how these users use technology and developing suitable solutions [2, 15, 19]. The security and privacy issues of this user group are largely unexplored. Past user studies suggest that low-income users desire privacy with regards to their data on their devices they share with others, and some technology literate users go so far as to use ad hoc measures to protect their data [7, 14]. We believe there is a need to examine their mental models surrounding security and privacy issues.

In this paper we highlight the challenges and design considerations, based on past literature and our experiences in the field, in understanding low-literate low-income users' security and privacy perceptions, and in building secure solutions for them.

2. CHALLENGES AND DESIGN CONSIDERATIONS

There are various factors that make developing technological solutions for low-literate low-income users in developing regions challenging. We highlight four factors that touch different aspects of this challenge: differences in security and privacy attitudes (cultural differences); lack of user awareness of basic technology (knowledge gap); technology use and how it puts users at risk (unintended use); and finally, the poor incentives for designers to develop secure and usable solutions for this marginalized population (low-profit user group).

2.1 Cultural differences

Cultural values are known to affect individuals' attitudes about privacy [4]. According to the Hofstede, who developed a model on cultural differences across nations, developed and Western countries are *individualists* societies with emphasis on the right to privacy, whereas developing and Eastern countries are *collectivists* with an emphasis on trust and belongingness [11]. Depending on the cultural and regional influences, people's preferences and expectation of privacy may vary, but there does seem to exist a universal desire and expectation of privacy, even among the poor [14]. For example, in the slums of Mumbai where the limited physical space is shared with several people (in the family and the community), there is an expectation of privacy behind a closed door and a curtain.

People's preferences for security and privacy reflect in their use of technology. In a recent smartphone usage survey across eight different countries, Harbach et al. found differences in people's attitudes and practices towards securing their data on the smartphone [10]. In a mobile phone usage study of low-literate users, Doke and Joshi found that their participants understood the privacy implications of sharing their mobile phone with others, and they avoided sharing if they could, but

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12–14, 2017, Santa Clara, California.

when they did have to share (e.g., due to cultural obligations or social demands), they took measures such as application level locks to hide their private content [7].

Cultural differences in privacy attitudes are even more evident in low-literate and low-income users in rural regions, which are arguably closer to Hofstede's *collectivist* society notion compared to the metropolitan cities in the developing regions. For instance, in some rural villages in India it is a common practice to display the salaries of community workers on the community public board. Such a practice would be considered an invasion of privacy in other parts of the world, or even in cities in India, but in those villages it is actually desired by the people, for transparency and income security.

Given the differences in attitudes towards security and privacy, a key question is how to design technological solutions for this marginalized population, while accounting for their (different) security and privacy preferences? Studying individual groups is not a scalable approach, especially since security and privacy preferences evolve over time and with exposure to technology. Another approach could be to design solutions with customizable preferences, but the low-literate users may not know enough about the underlying technology to choose the preferences that are right for themselves.

2.2 Knowledge gap

The rapid adoption of mobile phones in developing regions could be (deceptively) seen as an indicator that people in developing countries are becoming technologically literate, but many people learn only a limited set of functions on the phone, e.g., they can only make and receive phone calls [15]. However, even with such limited phone use, the widespread adoption of mobile phones enables agencies to reach this previously unserved population, using simple mobile interfaces such as voice call, SMS [17], USSD [18], and IVR [21], and provide services such as banking and healthcare.

Much of the focus with regards to low-literate and low-income users has been on the challenges of designing interfaces that they can understand and use, which is an important first step. Security and privacy issues for low-literate low-income users remain largely unexplored. Inexperienced users exhibit risky online behavior [20] exposing themselves to higher risk, and adverse user experiences may cause users to develop misconceptions about technology and further delay technology adoption. For instance, a novice low-literate mobile banking user with a fear of getting defrauded by a SMS scam may avoid using mobile banking services. We saw a similar misconception and fear with regards to (ink) signatures in low-literate local-income users during one of our field visits in India. During a field interview one participant refused to sign a user-study consent form. The participant gave verbal consent to the study, but was reluctant to sign the form. We learned from a local guide that some people associate signing a form or giving a thumb print on a form to property transactions, and hence the strong objection to signing a consent form.

Lack of user awareness – knowledge gap – about how the underlying technology works is not unique to low-literate users; it is a challenge for any new technology [8]. Low-literate users, however, have limited access to technology, which puts them far behind on the technology adoption curve, and as a result, they often lack the technology knowledge that many take for granted today. For example, gestures such as taps and swipes, recognizing soft buttons and icons on a display, navigating menus and screens on a phone, locating symbols when entering input [15]. These users also lack the understanding of security and privacy risks associated with how they use technology (e.g., phone [1]). Their knowledge gap is far wider than that of a technologically low-literate user in a developed region. Given the knowledge (or lack of) of low-literate low-income users, a key question is how to make such users aware of the security and privacy risks of the technology they use? And how to design solutions that meet such users' security and privacy expectations?

2.3 Unintended use

In the context of developing regions, people often use technology in ways unintended (by technology designers) to suit their own needs. The most common example is sharing of resources (e.g., mobile phones, PCs, media, PIN). Mobile phones are designed as single-user devices to be used as personal devices, but they are often shared within a family and with friends, especially in low-income users [7, 19]. To hide content from others, people use ad hoc measures such as renaming files (security by obscurity), using folder-level locks, or using app-level locks [7], but none of these methods offer a secure and usable solution for this sharing use case.

Another unintended use case is about the vibrant repair ecosystem in developing regions [2, 19]. People leave their devices (e.g., PCs and mobile phones) with third-party repair workers, giving the repair workers full access to the data in the devices, without fully realizing the security and privacy implications. Some people are completely unaware of the security and privacy risks; some people realize the risks of sharing their data, but are not aware that the repair worker can access their data; and some people are aware of the risks during the repair process, but they do not know how to avoid it [1]. Full-disk encryption on mobile phones may help in such circumstances, but if the repair worker asks for the phone password, customers have little choice but to comply if they want to get their phone repaired.

Low-income users also engage in the use of mobile phones for media dissemination and consumption [13, 16]. Mobile shops serves as a source of dissemination of the content: people bring their mobile phones to mobile shops to get new content, and hand over their phone to the worker in the shop to load the content of their choice. The worker gets access to the data in the phone and could also easily steal sensitive information form the phone or install a malware on the customer's phone. In fact, anecdotal evidence suggests that mobile shop workers copy the media in the customers phone, without the customer's permission, to expand their own media repository. Downloading content is expensive due to the limited and expensive Internet access, so mobile shop owners use alternate ways to build their content repository. They copy content from customers and co-share their repository with other mobile shop owners; their repositories can get as big as 300GB. Because the mobile shop owners co-share data, a customer's data, copied in one shop, can traverse long geographical distances.

Low-income users also engage in piracy, obtaining pirated media and software (mostly for PCs). Pirated media and softwares may not be a security risk in and of themselves, but it may be challenging to verify the integrity of the media and the software or to get software updates, which may put the user at risk [5]. Without any effective means to combat piracy, content generators (e.g., local folk musicians) trade-off the security of their content (DRM) with popularity, even when it comes at the expense of lost earning [13].

2.4 Low-profit user group

Low-income users, due to their low paying capacity, is a less attractive customer base for for-profit companies. Low-income users will choose the free option or the least expensive option, even if it is illegal (e.g., piracy). Developers and designers have to work with very small profit margins, if at all any, when developing technology solutions for low-income users. In such resource constrained development environment, developers are likely to choose functionality over security or privacy features [3]. A key question here is how can we incentivize developers to add reasonable security and privacy measures in their apps and services, and make it economical to do so, when they are working in a resource constrained environment?

3. CONCLUSION

Low-income low-literate users in developing regions are rapidly adopting technology (primarily through mobile phones), but without appropriate security and privacy measures, they remain vulnerable to attacks. This marginalized user group presents unique challenges for developing security and privacy solutions. In this paper, we discussed four challenges that put these marginalized users at risk, but the security and privacy issues of this user group are largely unexplored, waiting to be discovered and addressed.

4. REFERENCES

[1] S. I. Ahmed, S. Guha, M. R. Rifat, F. H. Shezan, and N. Dell. Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in Bangladesh. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*, June 2016. DOI 10.1145/2909609.2909661.

[2] S. I. Ahmed, S. J. Jackson, and M. R. Rifat. Learning to fix: Knowledge, collaboration and mobile phone repair in Dhaka, Bangladesh. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*, pages 1–10. ACM Press, 2015. DOI 10.1145/2737856.2738018.

[3] R. Anderson. Why information security is hard - an economic perspective. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 358–365. IEEE Comput. Soc, Dec. 2001. DOI 10.1109/ACSAC.2001.991552.

[4] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5):313–324, Nov. 2004. DOI 10.1080/01972240490507956.

[5] Y. Ben-David, S. Hasan, J. Pal, M. Vallentin, S. Panjwani, P. Gutheim, J. Chen, and E. A. Brewer. Computing security in the developing world: A case for multidisciplinary research. In *Proceedings of the ACM Workshop on Networked Systems for Developing Regions (NSDR)*, pages 39–44. ACM, June 2011. DOI 10.1145/1999927.1999939.

[6] E. A. Brewer, M. J. Demmer, M. Ho, R. J. Honicky, J. Pal, M. Plauché, and S. Surana. The Challenges of Technology Research for Developing Regions. *IEEE Pervasive Computing*, 5(2):15–23, 2006. DOI 10.1109/MPRV.2006.40.

[7] P. Doke and A. Joshi. Mobile Phone Usage by Low Literate Users. In *Proceedings of the International Conference on HCI, IndiaHCI*, pages 10–18. ACM Press, 2015. DOI 10.1145/2835966.2835968.

[8] W. K. Edwards and R. E. Grinter. At Home with Ubiquitous Computing: Seven Challenges. In *Trust, Privacy and Security in Digital Business*, pages 256–272. Springer Berlin Heidelberg, Oct. 2001. DOI 10.1007/3-540-45427-6_22.

[9] The mobile economy 2017. GMSA Report, 2017. Online at https://www.gsmaintelligence.com/research/?file=9e927fd6896724e7b26f33f61db5b9d5.

[10] M. Harbach, A. De Luca, N. Malkin, and S. Egelman. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 4823–4827. ACM, May 2016. DOI 10.1145/2858036.2858273.

[11] G. Hofstede. Dimensionalizing cultures: The hofstede model in context. *Online readings in psychology and culture*, 2011. DOI 10.9707/2307-0919.1014.

[12] State of connectivity 2015. a report on global internet access, 2015. Online at https://fbnewsroomus.files.wordpress.com/2016/02/state-of-connectivity-2015-2016-02-21-final.pdf.

[13] N. Kumar, G. Chouhan, and T. Parikh. Folk music goes digital in India. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, May 2011. DOI 10.1145/1978942.1979151.

[14] P. Kumaraguru and L. F. Cranor. Privacy in India: Attitudes and Awareness. In G. Danezis and D. Martin, editors, *Proceedings of the International Workshop on Privacy Enhancing Technologies (PET)*, pages 243–258. Springer, May 2005. DOI 10.1007/11767831_16.

[15] I. Medhi, S. Patnaik, E. Brunskill, S. N. N. Gautama, W. Thies, and K. Toyama. Designing mobile interfaces for novice and low-literacy users. *ACM Transactions on Computer-Human Interaction*, 18(1):1–28, Apr. 2011. DOI 10.1145/1959022.1959024.

[16] J. O'Neill, K. Toyama, J. Chen, B. Tate, and A. Siddique. The increasing sophistication of mobile media sharing in lower-middle-class Bangalore. In *Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD)*, June 2016. DOI 10.1145/2909609.2909656.

[17] T. Perrier, N. Dell, B. DeRenzi, R. Anderson, J. Kinuthia, J. Unger, and G. John-Stewart. Engaging Pregnant Women in Kenya with a Hybrid Computer-Human SMS Communication System. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 1429–1438. ACM Press, 2015. DOI 10.1145/2702123.2702124.

[18] T. Perrier, B. DeRenzi, and R. Anderson. USSD: The

Third Universal App. In *Proceedings of the ACM Symposium on Computing for Development (DEV)*, pages 13–21. ACM Press, 2015. DOI 10.1145/2830629.2830645.

[19] N. Rangaswamy and N. Sambasivan. Cutting chai, jugaad, and here pheri: Towards UbiComp for a global community. *Personal and Ubiquitous Computing*, 15(6):553–564, Apr. 2011. DOI 10.1007/s00779-010-0349-x.

[20] M. B. Schmidt, A. C. Johnston, K. P. Arnett, J. Q. Chen, and S. Li. A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness. *Journal of Global Information Management*, 16(2):91–103, Jan. 1. DOI 10.4018/jgim.2008040106.

[21] A. Vashistha, E. Cutrell, G. Borriello, and W. Thies. Sangeet Swara: A Community-Moderated Voice Forum in Rural India. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 417–426. ACM, Apr. 2015. DOI 10.1145/2702123.2702191.

[22] G. Zhang. Smarthpones now account for half the world's mobile connections. GMSA Intelligence Report, 2017. Online at https://www.gsmaintelligence.com/research/?file=66baa3fc91a95337ff99e4e9214e2185.