Usable Security: User Studies of Low-Literate Smartphone Users

1st Author Name
Affiliation
City, Country
e-mail address

2nd Author Name
Affiliation
City, Country
e-mail address

ABSTRACT

This paper describes the insights gained from user studies conducted with low-literate smartphone users in the context of Usable Information Security. For the purpose of this study, we present the analysis and findings from 70 users. Amongst the users we studied, 54 are male and 16 are female, with the average age for the male user being about 35 years and that for female, 42.87 years. 37 users were selected from a metropolitan city and 33 from a town. The average education of a user is about 8.64 years. Our insights show the users treating the phone as an asset from two perspective – information and as a commodity. In the domain of information security, we report findings on PINs and Pattern passwords, Usage of Ecommerce, Phone as an Information Device and as a Commodity, Asset Valuation, Risk Identification, Risk Assessment, Risk Mitigation, Password Management, Privacy, amongst others.

Author Keywords

Usable Security; Mobility; Smartphone; Low-Literacy; ICT4D; Passwords; Local Language Text Entry.

ACM Classification Keywords

H.5.2. User Interfaces; User-centered design.

INTRODUCTION

India, while being a developing country has seen significant adoption of mobile phones [21,25]. Specifically, the last few years has also seen a spurt in the adoption of android based smartphones and mobile applications. India also offers an interesting demographic, in the sense that, while it seeks to position itself as the world's preferred IT back-office, it also has significant numbers of citizens who are low-literate [20,22,23,24,38]. This opens up interesting research questions as users with low-literacy increasingly adopt and use smartphones in their daily lives [16,17,18,19,21,29,30,31,36,37]. In this paper we try to unravel this phenomenon and attempt to develop a better understanding on a very specific aspect, namely Information Security. We are curious to understand Information Security related aspects on the axes of low-literacy and smartphone based devices and applications [39,41]. We believe a better understanding of mobile phone security would help in building more secure environment when one of the most populous country adopts mobility [18]. We hope that our findings shed more light on how currently designed mobile phone security interventions are performing in the field.

BACKGROUND AND LITERATURE SURVEY

The field of study about protecting entities deemed valuable (assets) is significantly old. Of the various approaches engaged, information based security is one of the oldest. Users are also aware and comprehend the models of access to valuable assets based of knowledge of secret information, for example, even children stories about 'Open Sesame' from 'Ali Baba and the Forty Thieves' have exposed users to such concepts from an early age. However, computing has changed quite a few things in this arena. The ability to guess secretive information via either brute force or intelligent guesses has made information based security systems vulnerable. As a reactive response to the ever increasing threat of attacks from a computing system, complex mechanism have been articulated to defeat or delay the compromise of secretive information. One of the fallout of such designs has been that humans, for whom the systems have been designed, find it increasingly difficult to manage their security needs. Between this push and pull betwixt smarter attacking computers and humans, humans have been at the receiving end. As a consequence of this, humans have been termed as the weakest link in security when compromises have occurred due to human abilities. While this may be a view some hold, another view which is gaining ground is that security has be designed with human as the focus. If security systems were designed to be usable by humans then the compromises would be much lesser [2,4,5,34,35].

Under this overall umbrella, when technology adoption reaches the shores of a developing country with its backdrop of lower-literacy, the challenge of usable security is significantly amplified [7,11]. To the best of our awareness, we are unaware of qualitative studies done to understand usability issues in manifestations of information security on smartphones when used by low-literate users [14,15].

The objective of this study was to glean insights into the adoption and use of information security – practices, cognitive models, processes adopted by low-literate users when using (android based) smartphones.

METHOD

Also, for a working definition of low-literacy, we have chosen standard 10 as the maximum level of education. The users were recruited from two locations. One is a metropolitan city and is considered progressive on various socio-techno parameters. The other location is a town about 250 km away from this metropolitan city. While it is at a significant distance, it has good sociological connects with the city and is also a favourite location for popular cinema shooting; implying the role of sociological processes for transfer of information and technology. In the city users were selected via random sampling while in the town, the users were selected via an intermediary. Some users were also selected from a village adjoin the town. Overall 70 users were chosen for the study, of which 37 were from the city and 33 from the town. The average age of the user was 36.83 years while the average education was 8.64 years. There were 16 females and 54 males.

The interviews were focused on the phone as a tangible device and hence trying to ascertain the asset valuation, risk perception, risk mitigation when treated as a commodity. The other component of the interview focused on the phone as an intangible device, there by positioning it as an information device. When positioned as such, the goal was to assess the modalities of how the user does asset valuation, perceive and measure various risk and designs responses to mitigate various risks.

After the users were explained the nature of work and their consent sought, the Contextual Inquiry proper was conducted [1,3,6,9]. Field notes consisted of images of artifacts, users, observations and notes.

After the Contextual Inquiries and Analysis the findings were consolidated using Affinity Diagrams as a tool [8,10]. These yielded level one notes. These notes were then again analysed and classified in to level two groupings. In the sections below, we present our analysis as these level two notes and the level one notes within them.

FINDINGS AND INSIGHTS

COMMODITISATION

The smartphone is viewed by the users from two dimensions, namely, as tangible device of certain economic valuation or/and an information store whose valuation is associated with the quality and quantum of data on the device. For users who do treat the device as an asset on the tangible dimension, the valuation is the direct mapping to their economic ability and the price which they paid for the purchase of the device. Such users tend to also treat the device as a status symbol and accordingly associate risks, namely arising due to stealing or misplacement of it. In India, in villages and towns, owning a 'motorcycle (bike)' could be associated with the 'coming of age' on the economic dimension of the person. Today, the smartphone - with its associated base-device price seems to be equivalent or possibly replaced the motorcycle (bike). On the other hand, those users, who have perceived and used the device actively as an information store and device associated value to the information content on it. For most of the users, these are in the form of the Contacts in the Phonebook, SMS and media content which is either user-generated or shared via social-media application like WhatsApp or sharing applications like ShareIt. In the following sections, we will discuss how the perception and interpretation of commoditization happens at the tangible (physicality) and at the information level (identity management).

“Un-PIN me, I don’t care”

In the android ecosystem on the mobile, the Gmail-id of the user serves as an Identity Manager. One of the key actions it allows is giving the user access to the Google Playstore where all the applications reside. While it is easy to comprehend the role which Google had designed for the email-id, that is primarily, as a unique identifier, that is not how the users are using the system. In the event that they are unable to recall the password for the account they create another account. While this is a workaround, it probably takes them away from the user identity based protection which Google offers. They also seem to not use password recall mechanisms. So, from this perspective, the users really do not care for Identity Management on the phone – *I don’t care.* Such user behavior is likely to have impacts on the design of the mobile ecosystem. Apart from this, most of the triggers are when the users forget to recall their PINs or their patterns. In these situations, users try to disable PIN or Patterns Password features on their phone, hence the *unpin me*. From these aspects, one can draw inferences about users temperaments towards *unable to recall* situations. Instead of taking recourse to recovery mechanism, users tend to choose strong-handed choices of either not using the feature or circumventing the process.

PASSWORD MANAGEMENT

For those users who identify with the smartphone as an information device, the protection is based on information based security. Accordingly, users either opt for PIN based passwords or Pattern Locks. In the following sub-sections, we cover two types of views *'Ring Out the Old - Ring in the New*' and *'Easy to recall, Easy to guess'*. In the former where users have to share their phones due to cultural obligation seem to be aware of the risks associated with their patterns being known and hence they continuously change their passwords after every session, while the latter users depict the choices which people make in deciding their passwords. Due to the cognitive load associated with having to recall passwords or the implications, in terms of work impact or economic, when the password is forgotten, such users tend to opt for patterns or PINs which are extremely easy to recall or guess. In this context, the recallability of the passwords has an overwhelming effect on the choice of passwords that very weak passwords are chosen. Unfortunately, users seem to believe that their passwords are strong or are completely oblivious to the fact that passwords need to be difficult to guess to others. While users do seem to chose passwords from their context, example initials of names, they could not be categorized as the best choices [12,14,32].

"Easy to Recall, Easy to Guess"

When users are faced with a choice – which they cannot circumvent – they tend to choose passwords which are easy to recall. Given that the interface is in English language and the most familiar words in English language to them are their own names or those of their family members, these seem to be chosen. Users also tend to map glyphs of the Devanagari character to Glyphs in English / Roman and chose Patterns accordingly. However, in spite of choosing easy to recall passwords, there are instances of users not being able to recall. In such situations instead of using recovery mechanism, they create new accounts.

"Ring Out the Old, Ring in the New"

Some users who have more sensitivity towards Privacy, primarily to the nature of content on their devices which may not be amenable to the context, tend to rapidly change their passwords if they ever had to share the phone. Faced with such a situation, users tend to use generative mechanisms to create easy to recall.

PRIVACY

Users also seem to be aware about Privacy and exercise a certain amount of caution and precautionary steps when it comes to content they deem either objectionable (adult in nature) or that which their family members may have concerns about [27]. Such privacy concerns however do not seem to be present however, when the users are in their peer circles [28]. Social and cultural factors play a significant role as a deciding parameter to classify the content and behavioural response to the content handling. Accordingly, in the subsequent sections, we cover three categories, namely 'Forbidden Fruit' where users lock only certain sections of the mobile applications and data, 'Keep your plate clean' where users go to great lengths to ensure that their tracks are cleared and 'Touch me not' where they chose PIN and Patterns to lock the phone. Most of these have their origins in the aspect of sharing of the phone in Indian homes. Thought one does observe that there is a tendency to have 'personal phones' which are 'out-of-bounds'. However, with in the family, we expect the trend to continue, where phones of younger family members are used without permission or phones of elders are used by their children for gaming or 'rationed' usage of the internet - since 'internet' use is a privilege than a utility like electricity.

"Forbidden Fruits"

Users tend to have some applications and certain content/storage areas which are 'off-limits' to everyone. These areas / applications are protected by PINs or Pattern locks. It is observed that when users are initiated into content sharing or social networking mobile applications, the initiator also coaches them about Privacy and locking mechanisms. Such users have a good social networking presence and actively consume media via applications like Whatsapp.

"Keep your plate clean"

Users tend to access content which may not be acceptable culturally. In such cases, they go to great lengths to erase their digital tracks.

RISK MITIGATION

Risk Mitigators not only treat the phone as an information device of value, but, also go to great lengths to protect the information of value. They, hence exhibit a behaviour of asset valuation. Primarily, it has been observed that a contact in the phonebook and media is treated as an asset and valuation is proportional to the quantum of information. Users also exhibit risk enumeration from various events such as loss or theft of device, damage to device et cetera. Mitigation Techniques range from archiving the phonebook in their diaries or copy the contents onto another storage device.

Risk to the users can be discussed on 2 dimensions: (a) where the phone is a commodity, (b) where the phone is an information device. In the case of (a), the users treat the entity (phone) as any high value (compared to the income of the user) object. This is validated when the user's behaviour is modified when dealing with the phone. We observe such cases when the user deposits the phone in the safe of the drawer or in the cupboard/show-case, or keeps in personal close areas. It is also associated when the device is treated as a social/status symbol. In such cases the user resorts to physical security measures to secure the devices. In a reverse phenomenon we observe distress in the users when the phone is hid by known people. In the case of (b), users attached valuation in proportion to the volume of information on the device. In these cases, the measures to mitigate the risk are to backup to memory cards, computer, and physical diaries.

Users are particularly wary of their physical world reputation getting damaged due to security incidents. This is corroborated by actions of the users such as consciously clearing browser history, deleting images, messages and chat history, and using apps to clean the phone.

"Save my Assets"

Users who assess the smartphone as an information device also have simple models of valuation. Contents such as Phonebook, SMS and Media are valued in proportion to their volume. A tendency to backup indicates either a temperament of risk mitigation or a feedback based learner due to undesirable events. Some users tend to archive their contents, namely, contacts to diaries while some go to the higher levels of maintaining redundant or dedicated phones for phonebook or memory cards. The familiarity and convenience of a memory card also serves as a portable archive.

"Tangible transactions"

Our working definition of trust in the virtual world is when the user is able to transfer his relationship from the physical world to the virtual world without any loss of transaction semantics. One example of this is when the user, after having met his acquaintance in the real world, updates his phonebook and transacts with him in the virtual world. On the other hand, if the user has never met the individual in the real world, the interaction is limited to purely simple communications than transactional. [40]

By transactions we mean communications which have value to the sender. The transactions could be of various gradations but the user decides this based on the trust levels which have been assigned by the user in the real world

User's conduct towards online transactions as well as their technology fear indicates absence of trust in things digital [26]. On the other hand, they have a fair amount of faith in what the authors would like to call 'Tangible Transactions'. Tangible Transactions are those where the users can see the goods in physical world or engage in a physical cash transaction. This is peculiar in the Indian context and is also called as the CashOnDelivery model. This model was one of the big enablers of Web based/Desktop Brower ecommerce. It also reflected the users' discomfort with sharing credit card information over the web—another factor which supports the inherent distrust about things digital. On the other hand, WhatsApp represents a context were the trust levels are high. This is because WhatsApp has been using the contacts in the users' phone book to socially/business network. The contacts added in the phone book by the users are representative of the validation mechanism adopted by the user—as in only those contacts are added whom the users knows [33]. Hence the phone book represents a trusted network. WhatsApp leverages this to connect the user to the world/his network. Hence the WhatsApp network is representative of the trust network of the users. Other applications/models which lack these/this aspects of treating the phone book as a trusted data source fail to elicit the user into trust transactions. In such cases the users either resorts to physical world transactions or does not engage in them. This is also validated when the users use a printed advertisement or a call centre to place orders online. The tangibility of the human voice and connection resonates trust within the user resulting in the users doing commerce or trust transactions.

This is also facilitated by the validation model offered by the phone in tandem by WhatsApp since the phone number of the transactee is on the phone —a simple phone call by the users validates the recipient of the transaction. Also, in cases of doubt the user can send the recipient an SMS in addition to a phone call. This phone call validation with the social network aspects of WhatsApp offers a trust validation framework to the user. An interesting future area of work could be correlation between the users' phone call logs and their WhatsApp messages on a temporal/timeline basis indicating whether the call/SMS was preceding or following the WhatsApp messages.

CONCLUSION AND FUTURE WORK

Based on our findings we feel information security needs to be revisited in context of low-literacy. The various modes of engagement which users adopt as well as the conceptual models they have, may not be the most appropriate mechanism to deal with the threat posed by modern systems and attack mechanisms. The over simplifications of responses mechanisms or lower assessments of risks perceived, if at all, makes users vulnerable. While the modern computational attack systems are less forgiving, users seem to be desirous of a benevolent world. Further work could be carried out to delve in to how users model risks or can be taught security paradigms or concepts.

ACKNOWLEDGMENTS

We thank all the users, volunteers, and all publications support and staff, who wrote and provided helpful comments on previous versions of this document.

REFERENCES

1. Antonella De Angeli, Uday Athavankar, Anirudha Joshi, Lynne Coventry, and Graham I. Johnson. 2004. Introducing ATMs in India: a contextual inquiry. *Interacting with Computers* 16, 1: 29–44. http://doi.org/10.1016/j.intcom.2003.11.003
2. Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Möller. 2011. On the Need for Different Security Methods on Mobile Phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, ACM, 465–473. http://doi.org/10.1145/2037373.2037442
3. Hugh Beyer and Karen Holtzblatt. 1999. Contextual Design. *interactions* 6, 1: 32–42. http://doi.org/10.1145/291224.291229
4. Alan S. Brown, Elisabeth Bracken, Sandy Zoccoli, and King Douglas. 2004. Generating and remembering passwords. *Applied Cognitive Psychology* 18, 6: 641–651. http://doi.org/10.1002/acp.1014
5. Jan Chipchase. 2006. How Do You Manage Your Contacts if You Can'T Read or Write? *interactions* 13, 6: 16–17. http://doi.org/10.1145/1167948.1167966
6. Paul Dourish. 2004. What We Talk About when We Talk About Context. *Personal Ubiquitous Comput*. 8, 1: 19–30. http://doi.org/10.1007/s00779-003-0253-8
7. Minzhe Guo, Prabir Bhattacharya, Ming Yang, Kai Qian, and Li Yang. 2013. Learning Mobile Security with Android Security Labware. *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, ACM, 675–680. http://doi.org/10.1145/2445196.2445394

8. Gunnar Harboe and Elaine M. Huang. 2015. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ACM, 95–104. http://doi.org/10.1145/2702123.2702561

9. Karen Holtzblatt, Jessamyn Burns Wendell, and Shelley Wood. 2005. Rapid Contextual Design: A How-To Guide to Key Techniques for User-Centered Design. *Ubiquity* 2005, March: 3–3. http://doi.org/10.1145/1066322.1066325

10. Anirudha Joshi, Mandar Rane, Debjani Roy, et al. 2014. Supporting Treatment of People Living with HIV / AIDS in Resource Limited Settings with IVRs. *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, ACM, 1595–1604. http://doi.org/10.1145/2556288.255723

11. Deepti Kumar, David Martin, and Jacki O'Neill. 2011. The Times They Are A-changin': Mobile Payments in India. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 1413–1422. http://doi.org/10.1145/1978942.1979150

12. Cynthia Kuo, Sasha Romanosky, and Lorrie Faith Cranor. 2006. Human Selection of Mnemonic Phrase-based Passwords. *Proceedings of the Second Symposium on Usable Privacy and Security*, ACM, 67–78. http://doi.org/10.1145/1143120.1143129

13. Indrani Medhi, Somani Patnaik, Emma Brunskill, S.N. Nagasena Gautama, William Thies, and Kentaro Toyama. 2011. Designing Mobile Interfaces for Novice and Low-literacy Users. *ACM Trans. Comput.-Hum. Interact.* 18, 1: 2:1–2:28. http://doi.org/10.1145/1959022.1959024

14. Saurabh Panjwani and Edward Cutrell. 2010. Usably Secure, Low-cost Authentication for Mobile Banking. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM, 4:1–4:12. http://doi.org/10.1145/1837110.1837116

15. Robert Schaefer. 2009. The Epistemology of Computer Security. *SIGSOFT Softw. Eng. Notes 34*,6: 8–10. http://doi.org/10.1145/1640162.1655274

16. Thomas N. Smyth, Satish Kumar, Indrani Medhi, and Kentaro Toyama. 2010. Where There's a Will There's a Way: Mobile Media Sharing in Urban India. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 753–762. http://doi.org/10.1145/1753326.1753436

17. Kentaro Toyama. 2013. Reflections on HCI for Development. *interactions* 20, 6: 64–67. http://doi.org/10.1145/2527298

18. Gabriel White. 2008. FEATURE: Designing for the Last Billion. *interactions* 15, 1: 56–58. http://doi.org/10.1145/1330526.1330544

19. Text is Not The enemy. Retrieved May, 2015 from cs.swan.ac.uk/nuisworkshopCHI/papers/ TextIsNotTheEnemy-NUI-Workshop.pdf

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

21. Teledensity of India. Retrieved May, 2015 from https://data.gov.in/catalog/tele-density-india

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

23. 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

24. 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

25. Mobile VAS in India Report. Retrieved May, 2015 from http://www.iamai.in/pdf/AnnualReport201314LowRes.pdf

26. Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the 1st ACM Conference on Electronic Commerce*, ACM, 1–8. http://doi.org/10.1145/336992.336995

27. R. Balebako and L. Cranor. 2014. Improving App Privacy: Nudging App Developers to Protect User Privacy. I*EEE Security Privacy* 12, 4: 55–58. http://doi.org/10.1109/MSP.2014.70

28. Nicola J. Bidwell, Simon Robinson, Elina Vartiainen, et al. 2014. Designing Social Media for Community Information Sharing in Rural South Africa. *Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology*, ACM, 104:104–104:114. http://doi.org/10.1145/2664591.2664615

29. B. Chaudry, K. Connelly, K.A. Siek, and J.L. Welch. 2011. The design of a mobile portion size estimation interface for a low literacy population. *2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth)*, 160–167.

30. Beenish M. Chaudry, Kay H. Connelly, Katie A. Siek, and Janet L. Welch. 2012. Mobile Interface Design for

Low-literacy Populations. *Proceedings of the 2Nd ACM SIGHIT International Health Informatics Symposium*, ACM, 91–100. http://doi.org/10.1145/2110363.2110377

31. A. Dhir, P. Kaur, N. Jere, and I.A. Albidewi. 2012. Understanding mobile phone battery - Human interaction for developing world A perspective of feature phone users in Africa. *2012 2nd Baltic Congress on Future Internet Communications (BCFIC)*, 127–134. http://doi.org/10.1109/BCFIC.2012.6217992

32. T. Dorflinger, A. Voth, J. Kramer, and R. Fromm. 2010. #x201C;My smartphone is a safe! #x201D; The user's point of view regarding novel authentication methods and gradual security levels on smartphones. *Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT)*, 1–10.

33. K. Gupta, R. Kumar, and S. Loothra. 2014. Smartphone Security and Contact Synchronization. *2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT)*, 621–625. http://doi.org/10.1109/CSNT.2014.130

34. M. Al-Hadadi and A. Al Shidhani. 2013. Smartphone security awareness: Time to act. *2013 International Conference on Current Trends in Information Technology (CTIT)*, 166–171. http://doi.org/10.1109/CTIT.2013.6749496

35. S. Khan, M. Nauman, A.T. Othman, and S. Musa. 2012. How secure is your smartphone: An analysis of smartphone security mechanisms. *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 76–81. http://doi.org/10.1109/CyberSec.2012.6246082

36. Gary Marsden. 2006. Designing Technology for the Developing World. *interactions* 13, 2: 39–ff. http://doi.org/10.1145/1116715.1116743

37. P.M.L. Matyila, A. Botha, R. Alberts, and G. Sibiya. 2013. The design of accessible and usable mobile services for low literate users. *2013 International Conference on Adaptive Science and Technology (ICAST)*, 1–6. http://doi.org/10.1109/ICASTech.2013.6707504

38. Cosmin Munteanu, Heather Molyneaux, Julie Maitland, et al. 2012. Tale of Two Studies: Challenges in Field Research with Low-literacy Adult Learners in a Developed Country. *CHI '12 Extended Abstracts on Human Factors in Computing Systems*, ACM, 489–504. http://doi.org/10.1145/2212776.2212825

39. H. Pieterse and M.S. Olivier. 2013. Security steps for smartphone users. *Information Security for South Africa*, 2013, 1–6. http://doi.org/10.1109/ISSA.2013.6641036

40. A. Susanto, Younghoon Chang, Hangjung Zo, and Myeong Cheol Park. 2012. The role of trust and security in Smartphone banking continuance. *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2133–2138. http://doi.org/10.1109/ICSMC.2012.6378055

41. Yong Wang, K. Streff, and S. Raman. 2012. Smartphone Security Challenges. Computer 45, 12: 52–58. http://doi.org/10.1109/MC.2012.288