Users' Perceptions of Mobile Phone Security: A Survey Study in the Kingdom of Saudi Arabia

Thamer Alhussain, Rayed AlGhamdi, Salem Alkhalaf, and Osama Alfarraj

***Abstract*—With the rapid growth of mobile phone devices, there is a growing need for user authentication for the protection of data and services, and to promote public trust. This paper explores the perceptions of mobile phone users in the Kingdom of Saudi Arabia (KSA) regarding the security of mobile phone devices. It presents a survey study aiming to determine the preferred authentication technique among mobile phone users. The questionnaire results indicate that mobile phone users require an advanced level of privacy protection for information stored on their mobile device. The results show that applying biometric authentication can meet the users' requirements for protecting sensitive information on their mobile device.**

***Index Terms*—Mobile phone, users' perceptions, security, Saudi Arabia.**

I. Introduction

Mobile devices have become the most common means of communication around the whole world. According to the latest statistics produced by the Central Intelligence Agency (CIA), there were 6 billion mobile subscriptions worldwide in 2011 out of a world population of about 7 billion people [1].

With the rapid growth of communication network use, breaches in system security and incidents of transaction fraud are increasing. For this reason, developing a highly secure authentication system is imperative. The increased use of mobile devices to store large amounts of data carries the risk of loss or theft, which can compromise the security of information. This compromise of security is especially dangerous when sensitive personal information is involved. The current authentication method for the security of mobile devices depends on the use of a Personal Identification Number (PIN) to verify the user; however, simply using the correct PIN does not guarantee a person's identity. Thus, a higher level of security is needed especially with the developments of mobile phone devices.

II. Security Considerations

A. Authentication Strategies

There are three general categories of authentication as follows:

- Something the user knows (e.g. PIN or password).
- Something the user has (e.g. cards or tokens).
- Something the user is (e.g. biometrics).

The Personal Identification Number (PIN) is a secret-knowledge authentication method and consequently relies upon knowledge that only the authorized user has. Although the PIN and password are the most commonly used methods for authentication in information systems [2], such secret-knowledge approaches unfortunately have long-established problems, with weaknesses often being introduced by the authorized users themselves. These are most clearly documented in relation to passwords, with bad practices including the selection of weak and easily guessable strings, sharing passwords with other people, writing them down where others can find them, and never changing them [3]-[4]. Consequently, these approaches are the easiest target of hackers [5].

A security token is a physical entity or item that an individual possesses to establish personal identification, such as a passport, ID card, and credit card [6]. This token based approach is approximately similar to the secret knowledge approach, as it basically relies upon the user remembering to bring along something to ensure security whereby the token needs to be physically present [7]. Therefore, secret knowledge and token based authentication approaches are unsatisfactory methods of achieving the security requirements of information systems, as they are unable to differentiate between an authorized and an unauthorized person who fraudulently acquires the knowledge or token of the authorized person [6]. On the other hand, biometric authentication relies upon the unique physiological and behavioural characteristics of an individual; hence, it cannot be forgotten, lost or stolen.

B. Security for Mobile Devices

Security in mobile devices must be able to protect the interests of users, including their privacy, as well as those of the device manufacturers, network operators, and service providers [8]. However, mobile devices may contain sensitive and confidential user data; consequently, theft and loss of mobile devices are becoming a serious issue and the need for advanced user authentication in mobile devices is becoming vital. Furthermore, as mobile devices become smarter and support more data functions, mobile manufacturers are facing many of the same threats as

Manuscript received January 10, 2013; revised March 8, 2013.

T. Alhussain is with the Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Al-Ahsaa, Saudi Arabia (e-mail: talhussain@ kfu.edu.sa).

R. AlGhamdi is with the Faculty of Computing & IT, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: raalghamdi8@kau.edu.sa)

S. Alkhalaf is with the School of Science and Arts, Gassim University, Al-Rass, Saudi Arabia (e-mail: s.alkhalaf@live.com).

O. Alfarraj is with the Department of Computing, Teachers' College, King Saud University, Riyadh, Saudi Arabia (e-mail: osalfarraj@hotmail.com).

DOI: 10.7763/IJCTE.2013.V5.798

personal computers, namely, malicious software attacks [8]. The current security method for mobile devices is based on the use of a PIN which has several weaknesses. Security from unauthorized use can more effectively be achieved by more advanced user authentication systems [4]-[9].

C. User Authentication in Mobile Networks

With regard user authentication, mobile network providers are mainly concerned with the fraudulent use of their network; therefore, the authentication mechanisms are designed to ensure that only legitimate devices connect to the network. For example, GSM networks validate the credentials in the SIM card. Moreover, there are no provisions in 2G cellular networks to authenticate the network to the user system. This allows man-in-the-middle attacks where an attacker can control low-powered equipment which simulates a wireless network and can acquire the credentials of the user. However, with the security enhancement of UMTS, most mobile devices for both GSM and UMTS allow for devices to be configured so that the user must enter a PIN before using the device. Yet, the user can easily disable this system [10]. Therefore, the security for both GSM and UMTS mobile devices relies on a PIN approach which is under-utilized and can, consequently, be considered to provide inadequate protection in several cases.

III. ICT in Saudi Arabia

The Kingdom of Saudi Arabia is located in the south-eastern part of the Asian continent. It occupies 2,240,000 sq km (about 865,000 sq mi). The total population reached 26,534,504 in 2012; however, 5,576,076 of the population is non-Saudis [1].

The use of mobile devices is rapidly increasing among the people in the KSA. According to a recent report in 2012 by Communications and Information Technology Commission (CITC) in Saudi Arabia, the latest statistics in 2012 indicated that there are 4.63 million telephones - main lines in use while the total number of mobile subscriptions is 54.3 million. This reports also stated that mobile penetration in Saudi Arabia stood at 188.5% which is higher than the world average of 67%, the developing countries average of 57% and the developed countries average of 114%. However, the CITC report indicates that the Internet users estimated by 14.2 million of Internet users with a penetration rate of 49.1% [11]. Therefore, as mobile phone users are higher than Internet users, the Saudi government is concentrating on delivering its services through mobile devices.

IV. Methodology

The review of the current literature on the security and authentication of mobile devices guided our research and the literature on methods available for an exploratory study. Given the exploratory nature of the study the research question was aimed at providing descriptive information on the perceptions of mobile phone users regarding the information protection in their devices.

Since the questionnaire is an effective method to explore people's attitudes and opinions regarding particular issues [12], it was used to gather the required data related to mobile communication users' perceptions of the security in their mobile devices. In particular, the questionnaire was a printed document seeking responses to a selection of choices, with the participants having the opportunity to add their comments after each question. The literature on the security and authentication was used to help design the questionnaire. The method of sampling was purposive as it is a strategy in which "particular settings, persons, or activities are selected deliberately in order to provide information that can't be gotten as well from other choices" [13] (p.88).

Consequently, mobile phone users were approached in a range of public settings in the KSA. Users from both genders were sought from a range of relevant age groups and occupations to ensure that a representative sample of the user population was surveyed. A total of 420 questionnaires were distributed and 330 were returned; however, nineteen were excluded, because they were deemed incomplete. Thus, a total of 311 questionnaires were included in the data analysis.

V. Data Analysis and Discussion

The Statistical Package for Social Sciences (SPSS) software was used to accomplish the statistical analysis of the 311 questionnaires. However, missing values were eliminated from the analysis. In this section, only those survey questions will be presented which are relevant to detecting problems in this context and seeking solutions for mobile phone security by understanding the perceptions of mobile communication users.

Table I shows several concerns for mobile phone users regarding their mobile device security. It shows that a majority of participants agreed about the importance of the information that they have in their mobile devices. The level 'Moderate importance' was chosen most frequently (46.6%) as an important level of the information stored in the participants' mobile devices. Next was 'High importance' at 29.9% and the lowest was 'Low importance' at 20.9%, while only 2.6% of the participants think that it is not important. Furthermore, with regard to the use of PIN and password in participants' mobile devices, a high percentage (72.3%) of the participants answered "Yes", they use a PIN or password to log onto their mobile devices. However, table I shows that (51.1%) of the participants have lent the PIN or password of their mobile devices to somebody else which relates to the literature finding by [14] who found that 26% had shared their PIN with someone else. This result indicates that the PIN and password face important challenges in terms of correct usage.

The table also illustrates the level of protection of privacy that the users require for their information in their mobile devices. 'High protection' was an important level at 47.1%. The second most important protection level was 'Moderate protection' at 37.7%. 'Low protection' ranked second last at 11.7%, while only 3.6% of the participants indicated no need for protection. This has been supported by several studies such as [15], [16], and [4] who found that users have great concerns about the security and privacy of mobile devices. More specifically, a report by McAfee in 2008 indicated that 86% of mobile phone users are worried about security risks to their mobile devices and 34% question the general safety of mobile devices and services.

TABLE I: USERS PERCEPTIONS ABOUT MOBILE PHONE SECURITY

Questions and responses	Total No.	 %
How would you rate the level of importance of the information stored in your mobile device?		
High importance	93	29.9
Moderate importance	145	46.6
Low importance	65	20.9
No importance	8	2.6
Do you have a PIN or password to log onto your mobile device?		
Yes	225	72.3
No	86	27.7
Have you ever shared the PIN or password of your mobile device with somebody else?		
Yes	114	51.1
No	109	48.9
What level of protection of privacy do you require for the information in your mobile device?		
High protection	145	47.1
Moderate protection	116	37.7
Low protection	36	11.7
No protection	11	3.6
Based on information about authentication that was provided, which authentication method would you like to have to protect the important information in your mobile device?		
PIN or password	123	40.5
Biometric	175	57.6
Other	6	2.0
Based on the information on biometric authentication that was provided, to what extent do you think that applying biometrics in your mobile device will protect your sensitive information?		
Meets your need	262	87.3
Does not meet your need	28	9.3
Other	10	3.3
If you should use biometrics, which kind of biometrics do you prefer?		
Fingerprint scan	206	66.24
Iris recognition	86	27.65
Voice recognition	20	6.43
Signature analysis	17	5.47
Other	3	0.96
If you would have biometric scanning features in your mobile device, would you store more private information in your device?		
Yes	240	78.9
No	64	21.1
Are you willing to pay more money to have a biometric authentication in your mobile device?		
Yes	263	84.8
No	47	15.2

Another question in the survey investigated the most preferred authentication method by mobile phone users for the information security of their mobile device. The biometric method (57.6%) was the preferred authentication method, followed by the PIN or password (40.5%). However, a majority (87.3%) of the participants agreed that biometric authentication will meet their need to protect sensitive information on their mobile device. While a large majority of the respondents agreed that biometric authentication will meet their need to protect sensitive information on their mobile device, however, there is a difference of opinion whether biometrics would protect sensitive information on a mobile device, based on differing levels of importance attached to information stored on a mobile device. About 89.1% of participants thought that their information was of high importance and that biometrics would meet their need for security, while 9.8% thought that it would not meet their need. 88.7% of the participants thought that their information was of moderate importance and that biometrics would meet their need for security, while those who thought it would not meet their need was 7.1%. The percentage of participants who thought their information was of low importance and that biometrics would meet their need for security was 83.9%, while those who thought it would not meet their need was 14.5%. The percentage of the participants who thought their information was of no importance and thought that biometrics would meet their need for security was 60%, while no participants thought that it would not meet their need.

Moreover, table I shows that ‘Fingerprint scan’ was the most preferred kind of biometrics authentication by mobile phone users to be in their mobile device (66.24% of the participants). ‘Iris recognition’ was preferred by 27.65% of the total participants. ‘Voice recognition’ was preferred by 6.43%, while only 5.47% of the participants preferred ‘Signature analysis’ and 0.96% preferred other kinds of biometrics. This may agree with [17] study where most employees pointed to fingerprint technology as their preferred biometric. Moreover, this result may affect the adoption and convenience of such technology.

Moreover, table I shows the results for the question, “If you would have biometric scanning features in your mobile device, would you store more private information in your device?” The highest percentage (78.9%) of the participants answered ‘Yes’. The final question investigated whether the users would be willing to pay more money to have a biometric authentication in their mobile device. The above table shows that a high percentage (84.8%) of the mobile phone users who took part in the survey was willing to pay more money to have a biometric authentication in their mobile devices which might further be expressed in their demand for information protection.

VI. COMPARING BIOMETRICS FOR MOBILE DEVICES

While it is not easy to determine which biometric technology is the best, some biometrics would be better suited than others for specific applications. In mobile devices, the iris scan and fingerprint can be the most suited biometrics. They can provide a high level of security, accuracy, reliability, and stability compared with other biometrics [18]. Fransson and Jeansson [19] indicated that the system with an iris scan is almost impossible to deceive, as the camera can easily install a sensor that checks for pupil dilation. Moreover, the iris is very difficult to damage, as it is very well protected behind the eyelid and cornea. However, the iris scan is still expensive and can be affected by a person wearing sunglasses [20]. The camera also has to have specific technical features such as a Charge-Coupled Device (CCD) [19]. On the other hand, the fingerprint biometric is much cheaper and is rapidly being integrated into more applications [21]; however, it is easily damaged and gets dirty, which makes it hard to be processed and accepted [22]. While the retina scan can also provide a high level of security, accuracy, and reliability, it is less suited for mobile devices, because it is too expensive and needs a difficult process [20].

However, the security and reliability of face recognition, hand geometry, a person's signature, speaking voice, and keystroke have lower security than the fingerprint and iris scan [18]. In our study, we found that fingerprint is the most preferred type of biometrics by mobile phone users in the Kingdom of Saudi Arabia.

VII. Conclusion

A study was undertaken to investigate mobile phone users' perceptions and concerns about the security and authentication of their mobile devices. The results of this study supported a number of findings reported in the literature regarding the security and authentication of mobile devices. It can be concluded that mobile phone users require an advanced level of privacy protection for information stored on their mobile device; and biometric authentication can meet the need for protection for a majority of users. It appears that this growing need would significantly relate to the adoption of mobile applications. The negative security perception is a serious issue that mobile users may have regarding the use of mobile services and this may affect their acceptance and adoption of the technology for critical applications.

References

[1] World Fact Book 2012. Central Intelligence Agency. [Online]. Available: https://www.cia.gov/index.html.

[2] M. Scott, T. Acton, and M. Hughes, "An assessment of biometric identities as a standard for e-government services," *Services and Standards*, vol. 1, no. 3, pp. 271-286, 2005.

[3] R. Morris and K. Thompson, "Password security: a case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594-597, 1979.

[4] N. Clarke and S. Furnell, "Authentication of users on mobile telephones – A survey of attitudes and practices," *Computers and Security*, vol. 24, no. 7, pp. 519-527, 2005.

[5] F. Zahidi and W. E. Hajj, "Two Factor Authentication Using Mobile Phones," in *Proc. The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-2009)*, Rabat, Morocco, 2009.

[6] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 43, no. 2, pp. 90-98, 2000.

[7] N. Clarke and S. Furnell, "Advanced User Authentication for Mobile Devices," *Computers and Security*, vol. 26, no. 2, pp. 109-119, 2007.

[8] Trusted Computing Group (TCG) 2005. *Mobile Device Security and Trusted Computing*. Viewed on 14th of January 2009. [Online]. Available: http://www.trustedcomputinggroup.org/groups/mobile/MPWG_Primer.pdfH.

[9] S. Kadhiwal and A. Zulfiquar, "Analysis of mobile payment security measures and different standards," *Computer Fraud and Security*, vol. 2007, issue 6, June 2007, pp. 12-16, 2007.

[10] Rysavy Research 2007. Security Requirements for Wireless Networking. Wireless Technology: Assessment and Integration. [Online]. Available: http://www.rysavy.com/

[11] Communications and Information Technology Commission (CITC) 2012. Kingdom of Saudi Arabia. [Online]. Available: http://www.citc.gov.sa/

[12] J. Fraenkel and N. Wallen, *How to Design and Evaluate Research* in education, McGraw-Hill, New York, 2000.

[13] J. Maxwell, *Qualitative Research Design: An Interactive Approach*, 2nd Ed, Thousand Oaks, Sage Publication, 2005.

[14] N. Clarke, S. Furnell, P. Rodwell, and P. Reynolds, "Acceptance of subscriber authentication methods for mobile telephony devices," *Computers and Security*, vol. 21, no. 3, pp. 220-228, 2002.

[15] J. Carroll, "What's in it for me: Taking M-government to the people," in *Proc. 19th Bled eConference eValues*, Bled, Slovenia, June 5-7-2006.

[16] McAfee Mobile Security Report. (2008). McAfee. [Online]. Available: http://www.mcafee.com/us/research/mobile_security_report_2008.html.

[17] I. Giesing, *User Perceptions Related to Identification through Biometrics within Electronic Business*, University of Pretoria, 2003.

[18] B. McLindin, *Improving the Performance of Two Dimensional Facial Recognition Systems*, University of South Australia, 2005.

[19] L. Fransson and T. Jeansson, "Biometric methods and mobile access control," Master Thesis, Computer Science, Blekinge Institute of Technology, Sweden, 2004.

[20] S. Giarimi and H. Magnusson, "Investigation of User Acceptance for Biometric Verification/Identification Methods in Mobile Units," Department of Computer and Systems Sciences, Stockholm University, Sweden, 2002.

[21] Authen Tec. (2009). Fingerprint Biometrics. [Online]. Available: http:www.authentec.com, viewed on 30 March 2009.

[22] R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior, *Guide to Biometrics*, Springer, New York, 2004.

Thamer Alhussain is an assistant professor in the Department of Computer Science, College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia. Thamer's doctoral dissertation investigated the factors influencing the adoption of biometrics in m-government applications; and his PhD degree from the School of Information and Communication Technology at Griffith University in Australia. He has a Master degree in Information and Communication Technology from Griffith University as well. Thamer also obtained a Graduate Certificate in Information Systems from Griffith University. His research interests include mobile services, e-government, and adoption of biometric technology.

Rayed AlGhamdi is a Ph.D. candidate in the School of Information and Communication Technology at Griffith University, Australia. He got his Bachelor degree in Computer Education from Jeddah Teachers' College, Saudi Arabia. He also has a Master degree in Information and Communication Technology from Griffith University in Australia. His PhD dissertation focuses on the diffusion of online retailing in Arab countries. His other research interests include e-services applications, social media networks in Education, and research skills for school students.

Salem Alkhalaf is a Ph.D. candidate in the School of Information and Communication Technology at Griffith University, Australia. Salem obtained his Bachelor of Education in Computer Since with Honors degree in 2003 from the Department of Computer, Teachers' College, Riyadh, Saudi Arabia. He also has a Master degree in Information and Communication Technology from Griffith University, Brisbane, Australia in 2008. His PhD dissertation focuses on the evaluation of e-learning in Saudi Arabia. His research interests include collaborative e-learning and e-learning environments for higher education.

Osama Alfarraj is a lecturer in the Department of Computing, Teachers' College, King Saud University, Riyadh, Saudi Arabia. Osama doctoral dissertation investigates the reasons for the delay of the implementation of e-government applications in Saudi Arabia; and his PhD degree from the School of Information and Communication Technology at Griffith University in Australia. He has a Master degree in Information and Communication Technology from Griffith University as well. His research interests include e-government applications, e-learning, and mobile services.