5. Conclusion and future work

Although the majority of user actions are considered as risky processes, users of the device can perform almost all tasks at the beginning of a session, using a PIN or password, without having to periodically re-authenticate or re-validate their identity after the point-of-entry authentication. The purpose of this paper is to draw the attention of studying the risk for each process within the application. Based on our findings and result, this paper has suggested a novel risk assessment model for mobile applications data, called *MORI,* in order to determine the risk level for each process on a single application. In particular, the *MORI* model depends upon the value of user action and the worst consequences if user data are disclosed to unauthorised users or modified without permission. Finally, this model has introduced a risk matrix which might help to move the access control system from the application level to the intra- process application level, based on the risk for the user action being performed on these processes.

This risk matrix could, in the future, assist research activities to investigate the risks within the application. Future research will focus upon suggesting and applying a usable approach for accessing mobile phones by considering the risk level for each sensitive process and introducing the level of authentication beyond the PoE approach. Furthermore, the future work should focus on the usability and how the user interacts with the proposed risk matrix to ensure that it fits the best of the individual's favourite settings.

6. References

[1] Statista, (2016). "Forecast: smartphone users in the United Kingdom (UK) 2011-2018", available at:http://www.statista.com/statistics/270821/smartphone-user-in-the-united-kingdom-uk/[Accessed 4th September 2015]

[2] Statista, (2016b). "Worldwide mobile app revenues in 2015, 2015 and 2020 (in billion U.S. dollars)", available at: http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ [Accessed 21th November 2015]

[3] Rodwell, P. M., Furnell, S. & Reynolds, P.L., (2007). "A non-intrusive biometric authentication mechanism utilising physiological characteristics of human head" *Computer & Security*, vol.26, no.7, pp.468-478

[4] McAfee, (2015). Threats Predictions [online], available at:http://www.mcafee.com/es/resources/misc/infographicthreats- predictions-2015.pdf [Accessed 24 September 2015].

[5] Kurkovsky, S., & Syta, E., (2010). "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security". *IEEE International Symposium on Technology and Society. IEEE, 441–449.*

[6] Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. & Smith, J.M., (2010). "Smudge Attacks on Smartphone Touch Screens" *Proceeding in WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies.*

[7] Furnell, S., & Clarke, N., (2014). "Biometrics: making the mainstream." *Biometric Technology Today*, pp.5-9.

[8] Elftmann, P., (2006). "Secure Alternatives to Password-based Authentication Mechanisms, Lab. for Dependable Distributed Systems," *RWTH Aachen Univ.*

[9] Clarke, N., Karatzouni, S. and Furnell, S., (2009). "Flexible and transparent user authentication for mobile devices". *In IFIP International Information Security Conference (pp. 1-12). Springer Berlin Heidelberg.*

[10] Ledermüller, T. and Clarke, N.L., (2011), August. "Risk assessment for mobile devices". *In International Conference on Trust, Privacy and Security in Digital Business (pp. 210-221). Springer Berlin Heidelberg*.

[11] Alotaibi, S., Furnell, S. and Clarke, N., (2015). "Transparent authentication systems for mobile device security: A review". *In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 406-413). IEEE.*

[12] Davey, J., (1991). "Risk Analysis and Management. Data Protection and Confidentiality in Health Informatics", *IOS Press, pp.350-359.*

[13] Tam, K., Khan, S.J., Fattori, A. and Cavallaro, L., (2015). "CopperDroid: Automatic Reconstruction of Android Malware Behaviors", *In NDSS.*

[14] Theoharidou, M., Mylonas, A. and Gritzalis, D., (2012). "A risk assessment method for smartphones". *In Information security and privacy research (pp. 443-456). Springer Berlin Heidelberg.*

[15] Mylonas, A., Theoharidou, M., & Gritzalis, D., (2013). "Assessing privacy risks in android: A user-centric approach". *In Risk Assessment and Risk-Driven Testing (pp. 21-37). Springer International Publishing.*

[16] Alotaibi, S., Furnell S., and Clarke N., (2016). "A Novel Taxonomy for Mobile Applications Data". *In the International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 5, No. 3, pp115-121.*

