successfully corrupts a mobile OS system partition or system module, the mobile device is rendered unusable and a denial of mobile payment service does happen for that particular user of the mobile device. This model does protect a mobile device from becoming completely unusable, as a corrupted OS can be reinstalled easily and SE is reusable after that. On the other hand a 'bricked' mobile device's SE is totally unrecoverable.

5. Conclusion

The current design and implementation of SE access control is flawed, and is vulnerable to different kinds of attacks that threaten to compromise the whole system. We propose a theoretically sound and portable trusted computing model and design. However, the concepts and logical model presented in this paper must be implemented and tested for full assurance in real world applications. It must also be noted that our design ensures the integrity of a device OS to enforce SE related security only at boot time, but not at run time.

6. References

[1] GlobalPlatform, *http://www.globalplatform.org*, (Access Date: 15/9/ 2012).

[2] N Elenkov, "Exploring Google Wallet using the secure element interfaces," *http://nelenkov.blogspot.ca/2012/08/exploring-google-wallet-using-secure.html*, (Access Date: 30/8/ 2012).

[3] XDA Developers Forum, "[02/02/12] Google Wallet v1.1-R48V4 - ICS v4.0.3+," *http://forum.xda-developers.com/showthread.php?t=1311072*, (Access Date: 22/10/ 2012).

[4] R. Johnson, Z. Wang, C. Gagnon, A. Stavrou, "Analysis of Android applications' permissions," Software Security and Reliability Companion (SERE-C), 2012 IEEE sixth international conference on, vol., no., pp.45-46, 20-22, June 2012, *http://doi: 10.1109/SERE-C.2012.44*.

[5] A. Gargenta, "Deep dive into Android security", Presented at the Android Developer Confernce, San Franscisco CA, USA. 2012, *http://marakana.com/static/tutorials/AnDevCon2-DeepDiveIntoAndroidSecurity.pdf*, (Access Date: 10/11/ 2012).

[6] N. Elenkov, "Accessing the embedded secure element in Android 4.x," Aug 22, 2012, *http://nelenkov.blogspot.ca/2012/08/accessing-embedded-secure-element-in.html*, (Access Date: 10/11/ 2012).

[7] L. Francis, G. Hancke, K. Mayes and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," In 6th international conference on Radio Frequency Identification: Security and Privacy Issues (RFIDSec'10), Siddika Berna Ors Yalcin (Ed.). Springer-Verlag, Berlin, Heidelberg, 35-49, 2010.

[8] Trusted Computing Group, *http://www.trustedcomputinggroup.org/*, (Access Date: 08/11/ 2012).

[9] H. Uppal, "Enabling trusted distributed control with remote attestation," August, 2012, *http://people.cs.umass.edu/~hardeep/Thesis.pdf*, (Access Date: 13/11/ 2012).

[10] K. Dietrich and J. Winter. 2008. "Secure Boot Revisited," In Proceedings of the 2008 The 9th International Conference for Young Computer Scientists (ICYCS '08). IEEE Computer Society, Washington, DC, USA, 2360-2365, DOI=10.1109/ICYCS.2008.535, *http://dx.doi.org/10.1109/ICYCS.2008.53*.

[11] A. Vasudevan, E. Owusu, Z. Zhou, J. Newsome and J. M. McCune, 2012. "Trustworthy execution on mobile devices: what security properties can my mobile platform give me?" In Proceedings of the 5th international conference on Trust and Trustworthy Computing (TRUST'12), S. Katzenbeisser, E. Weippl, L. J. Camp, M. Volkamer and M. Reiter, (Eds.). Springer-Verlag, Berlin, Heidelberg, 159-178. DOI=10.1007/978-3-642-30921-2_10, *http://dx.doi.org/10.1007/978-3-642-30921-2_10*.

[12] J. Ekberg and S. Bugiel, 2009, "Trust in a small package: minimized MRTM software implementation for mobile secure environments," In Proceedings of the 2009 ACM workshop on Scalable Trusted Computing (STC '09). ACM, New York, NY, USA, 9-18, DOI=10.1145/1655108.1655111, *http://doi.acm.org/10.1145/1655108.1655111*.

[13] J. Grossschadl, T. Vejda, D. Page "Reassessing the TCG specifications for trusted computing in mobile and embedded systems," Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, vol., no., pp.84-90, 9-9 June 2008, doi: 10.1109/HST.2008.4559060.

[14] M. Landsmann, "Evaluating an MTM based security concept for Linux-kernel grounded mobile systems," Bachelor Thesis, Dept. of Comp. Science, Hamburg Univ. of Applied Sci., Hamburg, 2011, *http://opus.haw-hamburg.de/volltexte/2012/1447/*.

[15] M. Lemay, C.A. Gunter, "Cumulative Attestation Kernels for Embedded Systems," Smart Grid, IEEE Transactions on , vol.3, no.2, pp.744-760, June 2012, doi: 10.1109/TSG.2011.2174811.

[16] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC), strengths and weaknesses" Philips Semiconductors, June 2010.

[17] Google Inc. Android SDK, 2013, *http://developer.android.com/sdk/index.html*, (Access Date: 19/01/ 2013).

[18] P. England and T. Tariq, "Towards a programmable TPM," In proceedings of the 2nd international conference on Trusted Computing (Trust '09), L. Chen, M. J. Chris and A. Martin, (Eds.). Springer-Verlag, Berlin, Heidelberg, 1-13, 2009, DOI=10.1007/978-3-642-00587-9_1, *http://dx.doi.org/10.1007/978-3-642-00587-9_1*.

[19] K. Dietrich and J. Winter, "Implementation aspects of mobile and embedded Trusted Computing," In proceedings of the 2nd international conference on Trusted Computing (Trust '09), L. Chen, M. J. Chris and A. Martin (Eds.). Springer-Verlag, Berlin, Heidelberg, 29-44, 2009, DOI=10.1007/978-3-642-00587-9_3, *http://dx.doi.org/10.1007/978-3-642-00587-9_3*.

[20] G. Alpár, L. Batina and R. Verdult, "Using NFC phones for proving credentials," In proceedings of the 16th international GI/ITG conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance (MMB'12/DFT'12), Jens B. Schmitt (Ed.). Springer-Verlag, Berlin, Heidelberg, 317-330, 2012, DOI=10.1007/978-3-642-28540-0_26, http://dx.doi.org/10.1007/978-3-642-28540-0_26.

