# REFERENCES

[1] I-Lung Kao, Global Strategist, IBM Security Services, "Securing mobile devices in the business environment,"[Online]. Available: www-935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_business_environment.pdf  [Accessed: 19-Feb-2012]

[2] ITU, "The World in 2009,"[Online]. Available: www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf  [Accessed: 19-Feb-2012]

[3] P Silva, "Secure iPhone Access to Corporate Web Applications,"[Online]. Available: http://www.f5.com/pdf/white-papers/secure-iphone-access-tb.pdf [Accessed: 19-Feb-2012]

[4] "Symantec Consumer Guide to Wireless Device Security."[Online]. Available: http://spotlight.getnetwise.org/wireless/wirelessguide.pdf [Accessed: 19-Feb-2012]

[5] M. Baldauf, S. Dustdar, and F. Rosenberg, "A survey on context-aware systems," International Journal of Ad Hoc and Ubiquitous Computing, vol. 2, no. 4, pp. 263–277, Jan. 2007.

[6] Google, "Platform Versions."[Online]. Available: http://developer.android.com/resources/dashboard/platform-versions.html. [Accessed: 19-Feb-2012]

[7] "Juniper Networks Inc. Malicious mobile threats report 2010/2011." Technical report, Juniper Networks, Inc., 2011.

[8]    J. Hong, E. Suh, and S. Kim, Context-aware systems: A literature review and classification. 2009.

[9] K. W. Y. Au, Y. F. Zhou, Z. Huang, P. Gill, and D. Lie, "Short paper: a look at smartphone permission models," New York, NY, USA, 2011, pp. 63–68.

[10] N. Husted, H. Saïdi, and A. Gehani, "Smartphone security limitations: conflicting traditions," New York, NY, USA, 2011, pp. 5–12.

[11] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a Better Understanding of Context and Context-Awareness," in Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, London, UK, 1999, pp. 304–307.

[12] E. Snekkenes, "Concepts for personal location privacy policies," New York, NY, USA, 2001, pp. 48–57.

[13] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Supporting location-based conditions in access control policies," New York, NY, USA, 2006, pp. 212–222.

[14] M. J. Covington, P. Fogla, Z. Zhan, and M. Ahamad, "A context-aware security architecture for emerging applications," in Computer Security Applications Conference, 2002. Proceedings. 18th Annual, 2002, pp. 249–258.

[15] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments," in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, New York, NY, USA, 2010, pp. 43–48.

[16] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, "Cerberus: a context-aware security scheme for smart spaces," in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003), 2003, pp. 489–496.

[17] D. Barrera and P. Van Oorschot, "Secure Software Installation on Smartphones," IEEE Security & Privacy, vol. 9, no. 3, pp. 42–48, Jun. 2011.

[18] "Google Inc. Android market." .[Online]. Available: https://market.android.com/. [Accessed: 02-Feb-2012]

[19] M. Lange, S. Liebergeld, A. Lackorzynski, A. Warg, and M. Peter, "L4Android: a generic operating system framework for secure smartphones," New York, NY, USA, 2011, pp. 39–50.

[20] K. Gudeth, M. Pirretti, K. Hoeper, and R. Buskey, "Delivering secure applications on commercial mobile devices: the case for bare metal hypervisors," New York, NY, USA, 2011, pp. 33–38.

[21] G. Bai, L. Gu, T. Feng, Y. Guo, and X. Chen, "Context-Aware Usage Control for Android," in Security and Privacy in Communication Networks, vol. 50, S. Jajodia and J. Zhou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 326–343.

[22] W. Enck, M. Ongtang, and P. McDaniel, "Understanding Android Security," IEEE Security & Privacy, vol. 7, no. 1, pp. 50–57, Feb. 2009.

[23] Timothy Vidas, Nicolas Christin, and Lorrie Cranor, "Curbing Android Permission Creep," In Proceedings of the 2011 Web 2.0 Security and Privacy Workshop (W2SP 2011). Oakland, CA. May 2011.

[24] Timothy Vidas, Daniel Votipka, and Nicolas Christin, "All Your Droid Are Belong to Us: A Survey of Current Android Attacks.," In Proceedings of the 5th USENIX Workshop on Offensive Technologies (WOOT '11). San Francisco, CA. August 2011.

[25] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones," in Proceedings of the 9th USENIX conference on Operating systems design and implementation, Berkeley, CA, USA, 2010, pp. 1–6.

[26] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," New York, NY, USA, 2011, pp. 3–14.

[27] US-CERT, "Cyber threats to mobile Phones." .[Online]. Available: http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf. [Accessed: 12-Feb-2012]

[28] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "'Andromaly': a behavioral malware detection framework for android devices," Journal of Intelligent Information Systems, Jan. 2011.

[29] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for Android," New York, NY, USA, 2011, pp. 15–26.

[30] "Gingerbread most popular Android flavor at 56 percent market share," CNET. [Online]. Available: http://news.cnet.com/8301-1035_3-57524230-94/gingerbread-most-popular-android-flavor-at-56-percent-market-share/. [Accessed: 2-Nov-2012].

[31] "Strace for Android," Android - strace runtime, 05-Apr-2012. [Online]. Available: http://benno.id.au/blog/2007/11/18/android-runtime-strace. [Accessed: 05-Apr-2012].

[32] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Communications Surveys Tutorials, vol. 15, no. 1, pp. 446–471, First 2013.

[33] Ramu, S. "Mobile Malware Evolution, Detection and Defence", April 2012.