Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

DAFTAR PUSTAKA

[1] Agus Priyo Utomo dan Isbat Uzzin Nadhori. (2011). "Pelaporan Intrusi Pada Web *Server* Berbasis Sms Gateway". Surabaya: Institut Teknologi Sepuluh Nopember.

[2] Andrew S. T. dan Maarten V.S. 2007. *Distributed Systems: Prinsciples and Paradigms*.New Jersey: Pearson International Edition.

[3] Anthony Lopyrev. 2010. "How to Implement Push Notifications for Android". http://tokudu.com/2010/how-to-implement-push-notifications-for-android/ (diakses 21 Desember 2011).

[4] Antonio Fidalgo. 2009. *PUSHED NEWS: When the news comes to the cellphone*. Covilhã: Universidade Beira do Interior.

[5] BASE. Tanpa Tahun."Basic Analysis and Security Engine (BASE)". http://base.secureideas.net (diakses 10 November 2011).

[6] Canalys. 2011. "Android takes almost 50% share of worldwide smart phone market". http://www.canalys.com (diakses 1 Desember 2011).

[7] Dale Lane.2011."Push notifications for mobile apps". http://dalelane.co.uk/blog/?p=938 (diakses 21 Desember 2011).

[8] Fengmin Gong. 2003. "Intrusion Prevention: Myths, Challenges, and Requirements". http://www.atlantatechservices.com/downloads/My%20Documents/my_white_papers/download.pdf (diakses 10 Desember 2011).

[9] Google. 2011. "Activities". http://developer.android.com/guide/topics/fundamentals/services.html (diakses 10 Januari 2012).

[10] Google. 2011. "Frequently Asked Question". http://source.android.com (diakses 20 Desember 2011).

[11] Google. 2011. "What is Android ?". http://developer.android.com/guide/basics/what-is-android.html (diakses 23 Maret 2012).

[12] Hargyo Tri Nugroho, Yu-Kuen Lai, dan Wen-Yaw Chung. 2010. *Performance Improvement of Intrusion Detection System Using Locality Aware Buffer*. Chungli: Chung Yuan Christian University.

[13] Hyosu Kim, Minsub Lee, Wookhyun Han, Kilho Lee, Insik Shin. 2011. *Aciom: Application characteristics-aware disk and network I/O management on Android platform*. Daejeon: KAIST.

[14] IBM. 2007. “Using the IBM Lotus Expeditor micro broker MQTT client to publish messages”. http://www.ibm.com/developerworks/lotus/library/expeditor-mqtt/#N10080 (diakses 11 Januari 2012).

[15] J. F. Di Marzio. 2008. *Android A Programmers Guide*. Columbus: McGraw-Hill Prof Med/Tech.

[16] Jay Beale, Andrew R. Baker, dkk. 2004. *SNORT 2.1 Intrusion Detection*. Burlington: Syngress Publishing Inc.

[17] Jay Beale, Andrew R. Baker, dkk. 2007. *SNORT: IDS and IPS toolkit*. Burlington: Syngress Publishing Inc.

[18] Jones, S.2010. “Push To Learn”. http://www.simon-jones.com/PUSH%20TO%20LEARN%20Draft%20A.pdf (diakses 8 Januari 2012).

[19] Logix Softech Pvt Ltd.”Corporate SMS Applications”. http://www.logixmobile.com/downloads/docs/whitepapers/Corporate_SMS_Applications.pdf (diakses 10 Januari 2012).

[20] Marcel Bonar Kristanda. (2011). “Optimasi Publikasi Informasi Akademik Bagi Mahasiswa Dengan Aplikasi Blackberry Berbasis Push Technology (Studi Kasus: Universitas Multimedia Nusantara)”. Jakarta: Universitas Multimedia Nusantara.

[21] Michael Franklin, Stan Zdonik. 1998.“Data In Your Face: Push Technology in Perspective”. http://www.iicm.tugraz.at/thesis/cguetl_diss/literatur/Kapitel05/References/Franklin_et_al._1998/p516-franklin.pdf (diakses 8 Januari 2012).

[22] Microsoft. 1999. “Chapter 2 – What is Network QoS?”. http://technet.microsoft.com/en-us/library/bb742481.aspx (diakses 01 Juli 2012).

[23] MQTT. Tanpa Tahun. “FAQ: Frequently Asked Question”. http://mqtt.org/faq (diakses 12 Februari 2012).

[24] Nicolas Gramlich.”Android Programming”. http://andbook.anddev.org/files/andbook.pdf (diakses 20 Desember 2012).

[25] Rafeeq Ur, Rehman. 2003. *Intrusion detection systems with SNORT: advanced IDS techniques using SNORT, Apache, MySQL, PHP, and ACID*. New Jersey: Prentice Hall Professional.

[26] Sang Shin, Michèle Garoche. Tanpa Tahun. “Android Activity”. http://www.javapassion.com/android/android_activity.pdf (diakses 12 Januari 2012).

[27] SNORT. Tanpa Tahun. “About SNORT”. http://www.snort.org (diakses 08 September 2011).

[28] Umbach, K. W. 1997. “What is Push Technology”. http://www.library.ca.gov/crb/97/notes/V4n6.pdf (diakses 08 Januari 2012).

[29] Zone-H. 2011. “Yearly & Monthly & Daily Attacks”. http://www.zone-h.org (diakses 10 Januari 2012).

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA