適用於Android行動?置之有效的未知型僵屍網路惡意軟體偵測機制

高家緯、曹偉駿

E-mail: 344740@mail.dyu.edu.tw

摘 要

目前智慧型手機系統蓬勃發展，其中以Android為目前市場佔有率之冠，Android以 開放式作業系統之姿，提供各方有效的開發應用程式(Application, APP)供使用者裝載。 然而，正如同劍呈雙刃，可防身亦會傷己，故於Android眾多APP中卻可能隱含著惡意軟 體，本研究主要探討的是，濫用Android強大連網功能的Android殭屍網路惡意軟(Botnet)，其所發動之分散式阻絕服務(Distributed Denial of Service, DDoS)攻擊擁有大規模殭屍 網路的特點，再加上Android行動裝置的高移動性，故對攻擊目標之傷害高於傳統DDoS 攻擊，且難以追蹤攻擊來源。該惡意軟體除了造成Android連線緩慢，致使無法正常使用網路服務外。更大的威脅為阻斷伺服器的運作，迫使未受感染的Android智慧型手機也無 法正常使用網路服務。 現今傳統DDoS偵測機制多數設計於伺服器端，此等偵測機制只能暫時減緩DDoS攻 擊以穩固正常服務為優先，但其未能有效解決Android殭屍網路問題，且傳統偵測機制 並非以行動裝置作為設計標的，因此其所設計之機制並不適用於低效能、有限電力、較 少儲存空間的行動裝置。因此為設計有效的未知型殭屍網路惡意軟體偵測機制，本研究 首先研製以HTTP Flood為攻擊類型的Android殭屍網路惡意軟體，因為此類型為目前較 難以偵測且廣為氾濫的DDoS攻擊，並且知名防毒軟體皆無法偵測出此惡意軟體。 隨後則進一步開發能有效偵測未知型Android殭屍網路惡意軟體之機制，其除了可 偵測本研究所研製之殭屍網路惡意軟體之外，對於變形後的新型Android殭屍網路惡意 軟體亦具有相同的偵測能力。透過效能測試與分析，本偵測機制保有高偵測精確率，並 且在效能需求與實際應用面優於相關研究，因此我們堅信本偵測機制具有極高的實際應 用價值。

關鍵詞 : 殭屍網路、分散式阻絕服務攻擊、系統安全

目錄

參考文獻

[1]Pu Wang, Marta C. Gonzalez1, Cesar A. Hidalgo, and Albert-Laszlo Barabasi, " Understanding the spreading patterns of mobile phone viruses, " Science, vol. 324, no. 5930, pp. 1071-1076, 2009.
[2]Andre van Cleeff, " Future consumer mobile phone security: A case study using the data-centric security model, " Information Security Technical Report, vol. 13, no. 3, pp. 112-117, 2008.
[3]Android Developer, http://developer.android.com, 2011.
[4]Margaret Butler " Android: Changing the mobile landscape, " IEEE Pervasive Computing, vol. 10, no. 1, pp. 4-7, 2011.
[5]Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer and Yael Weiss " Andromaly: a behavioral malware detection framework for android devices, " Journal of Intelligent Information Systems, Online Article, 2011.
[6]Arbor Networks " Worldwide infrastructure security report " , vol. vi, 2010.
[7]Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao " Survey of network-based defense mechanisms countering the DoS and DDoS Problems, " ACM Computing Surveys, vol. 39, no. 1, pp. 1-46, 2007.
[8]Dmitry Rovniagin and Avishai Wool " The geometric efficient matching algorithm for firewalls, " IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 147-159, 2011.
[9]Android Market, http://Market.android.com, 2011.
[10]Android Open Source project, http://Source.android.com, 2011.
[11]Brian C. Williams and Errin W. Fulp " A biologically modeled intrusion detection system for mobile networks, " Proceedings of the Broadband Wireless Computing Communication and Applications, no.6, pp. 453-458, 2010.
[12]Kamer Ali Yuksel and Osman Kira " Enhancing security of linux-based Android devices, " Proceedings of the 15th International Linux Kongress, no.5, pp. 26-34, 2008.
[13]A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Gleze " Google Android: A comprehensive security assessment, " IEEE Security & Privacy, vol. 8, no. 2, pp. 35-44, 2010.
[14]Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi and Marcel Winandy " Privilege escalation attacks on Android, " Proceedings of the 13th Information Security Conference pp. 346-360, 2010.
[15]Wook Shin, Shinsaku Kiyomoto, Kazuhide Fukushima and Toshiaki Tanaka " A formal model to analyze the permission authorization and enforcement in the Android framework, " Proceedings of the IEEE Social Computing, pp. 994-1002, 2010.
[16]William Enck, Peter Gilbert, Byung-Gon Chun, Landon Cox, Jaeyeon Jung, Patrick McDaniel and Anmol Sheth " Taintdroid: an information-?ow tracking system for realtime privacy monitoring on smartphones, " Proceedings of the USENIX Symposium on Operating Systems Design and Implementation, pp. 34-43, 2010.
[17]G.Portokalidis, P.Homburg, K.Anagnostakis, and H.Bo " Paranoid Android: versatile protection for smartphones, " Proceedings of the 26th Annual Computer Security Applications Conference, pp. 48-54, 2010.
[18]Avik Chaudhuri " Language-based security on Android. " Proceedings of the 4th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, pp. 1-7, 2009.
[19]D. Barrera, H. G. u. c. Kayacik, P. C. van Oorschot and A. Somayaji " A methodology for empirical analysis of permission-based security models and its application to android, " Proceedings of the 17th ACM conference on Computer and communications security, pp. 73-84, 2010.
[20]W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka " Towards formal analysis of the permission-based security model for Android, " Proceedings of the 5th International Conference on Wireless and Mobile Communications, pp. 87-92, 2009.
[21]Wook Shin, Sanghoon Kwak, Shinsaku Kiyomoto, Kazuhide Fukushima and Toshiaki Tanaka " A small but non-negligible flaw in the Android permission scheme, " Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks, pp. 57-62, 2010.
[22]Mohammad Nauman, Sohail Khan, and Xinwen Zhang " Apex: extending Android permission model and enforcement with user-defined runtime constraints, " Proceedings of the 5th ACM Symposium on Information Computer and Communications Security, pp. 85-94, 2010.
[23]Asaf Shabtai, Uri Kanonov and Yuval Elovici " Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method, " Journal of Systems and Software, vol. 83, no. 8, pp. 1524-1537, 2010.
[24]Cui Xiang, Fang Binxing, Yin Lihua, Liu Xiaoyi, and Zang Tianning " Andbot: towards advanced mobile botnets, " Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats, pp. 41-50, 2011.
[25]Shui Yu, Wanlei Zhou, and Robin Doss " Information theory based detection against network behavior mimicking DDoS attacks, " IEEE Communications Letters, vol. 12, no. 4, pp. 318-321, 2008.
[26]Tom Fawcett " An introduction to ROC analysis, " Pattern Recognition Letters, vol. 27, no. 8, pp. 861-874, 2006.
[27]Wireshark, http://www.wireshark.org, 2011.