運用行動代理人抵抗分散式阻絕服務之入侵偵測機制

吳正光、曹偉駿

E-mail: 9222442@mail.dyu.edu.tw

摘 要

現今網路交易日益頻繁，網路攻擊漸漸朝向自動化，入侵手法亦趨向複雜化。成功的分散式阻絕服務攻擊，足以癱瘓線上交易市場，讓企業損失慘重，而隨著組織的入侵偵測系統提昇能力的同時，攻擊者會滲透更多的可用目標，來達到癱瘓組織入侵偵測系統的目的，所以建立有效率的預防性防禦機制是目前企業首要考量目標。 本研究於尋找有效的防禦阻絕服務的入侵偵測機制時，發現階層分散式架構容易被攻擊者發現單一失敗點，為了解決難以發現攻擊來源及目前的入侵偵測系統的缺點，於是研擬出一整合式的抵抗攻擊機制。首先，提出整合封包過濾、追蹤攻擊來源及監控網路流量的技術，以各網域「互助方式」來建構一道分散式入侵偵測系統防線（Cooperative Intrusion Detection System）。其次，這防線可以利用行動代理人容錯的優點來恢復重要主機功能，經由這防線架構來抵抗分散式阻絕服務攻擊。最後，以邏輯推理的方式加以證明本模組足以抵抗攻擊，並且分析演算法的時間複雜度。另外，亦從實作行動代理人的程式測試來驗證本研究提出方法的可行性。

關鍵詞：入侵偵測系統、行動代理人、分散式阻絕服務攻擊、單一失敗點

目錄

參考文獻

[1] 李勁頤,陳奕明, "分散式入侵偵測系統研究現況介紹", 資訊安全通訊, communications of the CCISA, Vol. 8, Issue 2, pp. 38-61, March 2002。

[2] 陳正昌譯（2002）, 網路入侵偵測教戰手冊, 台北, 培生教育出版, pp.305-309。譯自Stephen northcutt, Judy novak, ISBN 957-2054-57-0。

[3] C. Barros, "A proposal for ICMP traceback messages," Internet Draft. http://www.research.att.com/lists/ietfitrace/2000/09/msg000 44. html, Sept 18, 2000.

[4] J. Bradshaw, An introduction to software agents, In Jeffrey M. Bradshaw, editor, Software Agents, Chapter 1, AAAI Press / The MIT Press, 1997.

[5] H. Burch and H. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. USENIX Conference, pp. 319-327, Dec.2000.

[6] CERT Coordination Center, "CERT Advisory CA-2001-19 'Code Red' Worm Exploiting Buffer Overflow In IIS Indexing Service DLL," http://www.cert.org/advisories/CA-2001-19.html.

[7] T. Cormen, C. Leiserson, R. Rivest, and C. Stein, Introduction to Algorithms, ADDISION-WESLEY, pp. 389-390, Nov 2001.

[8] B. Cubaleska and M. Schneider, "Detecting DoS attacks in mobi- le agent systems and using trust policies for their prevention ," T- he 6th World Multiconference on Systemics, Cybernetics and In- formatics SCI 2002.

[9] N. Duffield, F. Presti, V. Paxson, and D. Towsley, "Inferring link loss using striped unicast probes," in Proc. IEEE INFOCOM, Ala- ska, April 2001.

[10] P. Ferguson and D. Senie, Network ingress filtering: Defeating d- enial of service attacks which employ IP source address spoofing agreements performance monitoring, RFC 2827, May 2000.

[11] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," IEEE/ACM Transactions on Networking, Vol.1, No.4, pp. 397-413, Aug 1993.

[12] A. Habib, M. Hefeeda, and B. Bhargava, "Detecting service viol- ations and DoS attacks," in Proc. Network and Distributed Syste- m Security Symposium (NDSS '03), San Diego, Feb 2003.

[13] D. Lange and M. Oshima, Programming and Deploying Java mo- bile Agents with Aglets, ADDISION -WESLEY, pp. 3-89, Nov 1998, ISBN 0201325829.

[14] P. Mell , D. Marks, and M. McLarnon, "A denial-of-service resis- tant intrusion detection architecture," Computer Networks ,Vol. 3 4, pp. 641-658, 2000.

[15] J. Mirkovic, G. Prier and P. Reiher, "Attacking DDoS at the sour- rce," Proceedings of ICNP 2002, pp. 312-321, Paris, France, No- v 2002.

[16] D. Moore, "Inferring internet denial-of-service activity," Procee- dings of the 2001USENIX Security Symposium, 2001.

[17] K. Park and H. Lee, "A proactive approach to distributed DoS at- tack prevention using route-based packet filtering," in Proc. ACM SIGCOMM, Aug 2001.

[18] R. Power, "Computer security issues & trends," 2002 CSI/FBI Computer Crime and Security Survey, Vol. viii, No. 1, pp. 1-12, spring 2002.

[19] S.Savage, D. Wetherall, A. Karlin, and T. Anderson, " Network s- upport for IP traceback," IEEE/ACM Transaction on Networking, Vol. 9, No. 3, pp. 226-237, June 2001.

[20] A.Snoeren, C. Partridge, L. Sanchez, W. Strayer, C. Jones, and F. Tchakountio, "Hashed-based IP traceback," ACM SIGCOMM, A- ug. 2001.

[21] W. Jansen, Intrusion Detection with Mobile Agents, NIST Speci- al Publication, http://csrc.nist.gov/mobilesecurity/publications.h- tml#MA.

[22] D. Zamboni, "Using internal sensors for computer intrusion dete- ction," CERIAS TR 2001-42 Center for Education and Research in Information Assurance and Security, Purdue University, Aug 2001.