A Distributed Denial-of-Service Resistant Intrusion Detection Scheme Using Mobile Agents

吳正光、曹偉駿

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

ABSTRACT

Today, computer networks become increasingly, and the attacks have grown in complexity and automation. Successful distributed denial of service attacks can put e-commerce-based organizations out of business. As the capabilities of IDSs advance, attackers may attempt to penetrate more valuable targets before disabling organizations' IDSs. Thus, the preventive defense has been merged to improve the performance of intrusion detection systems (IDSs). In this thesis, we investigate effective methods for detecting and responding to DDoS attacks. We find that the existing hierarchical IDS architectures are prone to have single points of failure that are easily discovered by an attacker. To solve the problem of finding attackers and improving IDS's weakness, we present an integrated scheme that is resistant to distributed denial of service attacks. First, we propose a cooperative intrusion detection System (CIDS) that consists of packet filtering, traceback of DDoS attack and network monitoring schemes. Second, CIDS can frustrate attackers by mobile agents' fault-tolerant ability, and backup hosts that it intruded. Finally, we present formal proofs using the logical reasoning to validated our attack-resistant model. We also analyze the computational complexity of the proposed algorithm, and further implement the mobile agent based program. The results derived in the thesis consolidate the feasibility of our proposed schemes.

Keywords : Intrusion detection system, Mobile agent, Distributed d- enial of service, Single points of failure.

Table of Contents

REFERENCES

[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.