Detection and Prevention of Flooding Distributed Denial-of-Services Based on a Multi-agent Structure

劉經緯、曹偉駿

E-mail: 9510830@mail.dyu.edu.tw

ABSTRACT

With the rapid growth of Internet, malicious attacks are getting more numerous and menacing. Distributed denial-of-service (DDoS) attacks are different from most other attacks, because they are not targeted at gaining access to information systems. These attacks focus on making a service unavailable for normal use, which is typically accomplished by exhausting some resource limitation on the network or within an operating system or application. This attack interferes with trading online and causes the damages to the business. Therefore, establishing efficient detecting and preventing schemes will become the main concern for the business. General flood DDoS detecting schemes can't prevent attacks by legal users, and it can't backup immediately crashed servers, either. Therefore, this thesis proposes a multi-agent structure to integrate three protection schemes. The first is based on elliptic curve public key cryptosystems to authenticate users. The second is the protection scheme of the service port transformation, which servers still can operate normally even if being attacked by numerous abnormal packets. The third is the backup scheme. When the agent finds out flood DDoS attacks crash the servers, the backup scheme will start on to notice the near hosts to backup the crashed host. In summary, this study is based on three schemes to develop a practical system, which still can provide services normally and also have the ability to backup hosts immediately even if they are attacked by flood DDoS.

Keywords : Network security ; Distributed denial of service ; Intrusion detection systems ; Elliptic curve public key cryptosystems ; Backup scheme

Table of Contents

REFERENCES

林楷勛(2004)。適用於保護應用伺服器以防止分散式阻斷服務攻擊之入侵保護系統。國立清華大學資訊系統與應用研究所碩士論文，新竹市。 曹偉駿、吳正光(2003)，用行動代理人以抵抗分散式阻絕服務之入侵偵測機制,第十三屆全國資訊安全會議，頁349-360。 CERT Statistical Weaknesses in TCP/IP Initial Sequence Numbers, from http://www.cert.org/stats/index.html CERT/CC Statistics (1988-2006). Retrieved May 19, 2006, from http://www.cert.org/stats/cert_stats.html Barros, C., A proposal for ICMP trace back messages, Internet Draft. from http://www.research.att.com/lists/ietfitrace/2000/09/msg00044. html, Sept 18, 2000. Burch H., & Cheswick H. (2000). Tracing anonymous packets to their approximate source. in Proc. USENIX Conference, (pp. 319-327) Caelli, W., Dawson, E., & Rea, S., (1999). PKI, elliptic curve cryptography and digital signatures. Computer & Security, 18(1), 47-66. Chen, L., Longstaff, T., & Carley, K. (2004). Characterization of defense mechanisms against distributed denial of service attacks, Computers & Security, 23(8), 665-678. Chen, S., Tang, Y., & Du,W. (2006). Stateful DDoS attacks and targeted filtering. Journal of Network and Computer Applications, (Accepted). Chen, S., & Song, Q. (2005). Perimeter-Based Defense against High Bandwidth DDoS Attacks. IEEE Transactions on Parallel and Distributed Systems, 16(7), 784-799. Cubaleska B., & Schneider M. (2002). Detecting DoS attacks in mobile agent systems and using trust policies for their prevention. The 6th World Multiconference on Systemics Cybernetics and Informatics, (pp. 421-434). Douligeris, C., & Mitrokotsa, A., (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 44(5), 643-666. ElGamal T., (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469-472. Ferguson, P., & Senie, D., (2000). Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing agreements performance monitoring, RFC 2827. Habib, M., Hefeeda, & Bhargava, B., (2003). Detecting service violations and DoS attacks. in Proc. Network and Distributed System Security

Symposium (NDSS '03), San Diego. Jansen, W. (2002). Intrusion detection with mobile agents. Computer Communications, 25(15), 1392-1401. Jurisic, & Menezes, A.J., (1997). Elliptic curves and cryptography. Dr. Dobb ' s Journal, (pp. 26-35). Kenney, Malachi, Ping of Death, January 1997, Available from http://www.insecure.org/sploits/ping-o-death.html Kargl, F. Maier, J. Schlott, & Weber, S., (2001). Michael Protecting Web Servers from Distributed Denial of Service Attacks. In Proceedings International WWW Conference(10), (pp. 150-162). Koblitz, N., (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(17), 203-209. Kemmerer R., & Vigna G., (2002). Intrusion Detection: A Brief History and Overview. IEEE Computer Special Issue on Security and Privacy, (pp. 27-30). Mirkovic J., Martin J., & Reiher P., (2001). A Taxonomy of DDoS Attacks and DDoS Defense Mechanism. UCLA CSD Technical Report CSD-TR-020018. Mell, P., Marks, D., & McLarnon, M., (2000). A denial-of-service resistant intrusion detection architecture. Computer Networks, 34(7), 641-658. Mirkovic J., Prier G., & Reiher P., Attacking DDoS at the source. Proceedings of ICNP 2002, (pp. 312-321). Miu, K. N., Chiang, H. D., & McNulty, R. J., (2000). Multi-Tier Service Restoration Through Network Reconfiguration and Capacitor Control for Large-Scale Radial Distribution Networks. IEEE Trans. on Power Systems, 15(3), 1001-1007. McCanne S., Floyd S., NS-2 Network Simulator from http://www.isi.edu/nsnam/ns.hml. Miller., V.S. (1986). Use of elliptic curves in cryptography. Advances in Cryptology:Crypto ' 85, Springer-Verlag, (pp. 417-426). National Bureau of Standards, (1977). Data encryption standard. Federal Information Processing Standards Publication FIPS PUB 46 U.S. Department of Commerce. Park K., & Lee H., A proactive approach to distributed DoS attack prevention using route-based packet filtering. in Proc. ACM SIGCOMM, (pp. 124-136). Snoeren, C., Patridge, L ., Sanchez, C., Jones, F., & Tchakountio, B., Schwartz, et al., (2002). Single-packet IP trace back. IEEE Transaction on Networking, (pp. 721-755). Schulba I., Krsu, & Kuhn M.., (1997). Analysis of a Denial of Service Attack on TCP. Proceedings of the 1997 IEEE Symposium on Security and Privacy, (451-468). Spafford, C., (2000). Intrusion detection using autonomous agents. Computer Networks, 34(4), 547 – 570. Savage, S., Wetherall, D., Karlin, A., & Anderson, T., (2001). Network support for IP trace back. IEEE/ACM Transaction on Networking, 9(3), 226 – 237. Steels, L., (1995). When are robots intelligent autonomous agents?. Journal of Robotics and Autonomous Systems, 15(1-2), 3-9. Shakshuki, E., Luo, Z., & Gong, J., (2005). An agent-based approach to security service. Journal of Network and Computer Applications, 28(2), 183-208. Schnorr C.P., (1990). Efficient identification and signatures for smart cards, Advances in Cryptology: Crypto ' 89, Springer-Verlag, (pp. 339-351). Tsaur, W. J., (2005). Several Security Schemes Constructed Using ECC-Based Self-Certified Key Cryptosystems. Applied Mathematics and Computation, 168(1), 447-464. Vanstone, S., (1977). Elliptic Curve Cryptosystem-The Answer to Strong, Fast Public-key Cryptography for Securing Constrained Environments. Elsevier Information Securtiy Technical Report, 2(2), 78-87. Wang, Y., Behera, S., Wong, J., G., Helmer, V., Honavar, L., Miller, Lutz, R., & Slagell, M., (2006). Towards the automatic generation of mobile agents for distributed intrusion detection system. Journal of Systems and Software, 79(1), 1-14.