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

第一章 緒論 1.1 研究背景 1 1.2 研究動機與目的 3 1.3 研究流程 4 1.4 論文架構 6
第二章 相關文獻探討 2.1 多代理人 7 2.2 阻絕服務攻擊 8 2.2.1 分散式阻絕服務攻擊 9 2.2.2 攻擊步驟 10 2.2.3 現今分散式阻絕服務攻擊方式 12 2.2.4 洪水式分散阻絕服務攻擊防禦手法 14 2.3 橢圓曲線密碼系統 18 2.4 小結 19
第三章 多代理人架構之洪水式分散阻絕服務攻擊偵防機制 3.1 多代理人架構 21 3.2 多代理人架構之洪水式分散阻絕服務攻擊偵防機制 23 3.3 防禦洪水式分散阻絕服務攻擊機制設計 25 3.3.1 植基於橢圓曲線公開金鑰密碼系統防禦機制 27 3.3.2 轉移服務埠防禦機制 31 3.3.3 備援機制 34
第四章 系統實作與模擬測試 4.1 模擬測試工具 41 4.2 軟硬體規格 42 4.3 系統操作流程 43 4.4 安全性分析 54
第五章 結論與未來方向

REFERENCES


