行政院國家科學委員會專題研究計畫成果報告

網際網路攻擊偵防研究之一--SYN Flooding

Study on Network attack – SYN Flooding

計畫編號：NSC 90-2213-E-009-159
執行期限：90 年 8 月 1 日至 91 年 7 月 31 日
主持人：蔡文能　　交通大學 資訊工程系

一、中文摘要

網際網路(Internet)的蓬勃發展帶來了許多便利，不過也引來許多新問題、新風險。自從 1996 年起，網路上出現了一種稱爲阻絕服務(Denial of Services)的網路攻擊方式，像是在 2000 年 2 月時所發生的 Yahoo、Amazon、CNN、eBay 等線上知名網站遭人癱瘓，以致無法提供正常之服務的事件，經過進一步追查與瞭解之後，發現癱瘓的原因並非是駭客直接入侵服務網站所引起的，而是利用所謂的DoS（Denial of Servies）所發動的網路攻擊。其方法是利用程式在瞬間產生大量的網路封包，以癱瘓對方之網路及主機，使得正常的使用者無法獲得主機及時的服務。值的注意的是，這次攻擊是採用分散式的方法 DDos(Distribued DoS)，攻擊者在已經遭受入侵的 Internet 主機上安裝攻擊程式，同時發動一波又一波的攻擊，造成目標主機所提供之服務癱瘓甚至中斷。

目前常見的 DoS 攻擊有三種型態的。第一種是利用 TCP/IP 規格本身的漏洞，例如 SYN Flooding 和 LAND 攻擊、第二種是利用主機系統的 TCP/IC 漏洞例如 Ping of Death 和 Teardrop 攻擊、第三種則是 smurf 攻擊，這三種攻擊的共同特點爲皆是利用 TCP/IP 的漏洞或是網路程式的漏洞，讓被攻擊的主機當機或是讓網路塞滿了垃圾封包，導致網路停擺使得被攻擊的主機無法繼續服務，以達到攻擊的目的。

本計畫主要是針對最常見的 SYN Flooding 攻擊方式研究防制的方法，以便使伺服器在遭受到 SYN Flooding 時仍可以提供服務。

關鍵詞：網路入侵、網路攻擊、電腦駭客、系統缺陷、組絕服務(DoS)

Abstract

The emergence of Internet brings business opportunities to enterprises and convenience to users. However, since the Internet is open to public, we have to face many new questions and risks, e.g. intrusion, attack, virus, and spam mails. Since September 1996, several dozen sites on the Internet have been exposed to a *Denial-of-Service* (DoS) attack, popularly called *SYN Flooding*.

We would conduct further studies on attack and intrusion, so that we could propose methods to detect attack and intrusion. We call the behaviors that want to paralyse the system or the network as "Attack", and call those break-ins or data-stealth as "Intrusion".

Denial of Service (DoS) is a

frequently seen network attack. There are many kinds of DoS attack. They all use the holes of TCP/IP protocols or System flaws to jam the network with garbage packet to make the network or the system mal-function..

This project is to study SYN Flooding and try to find a feasible solution for this kind of DoS attack.

Keywords: Network Intrusion, Hacker, System flaws, Denial of Services(DoS)

二、緣由與目的

既然 Internet 是公眾皆可使用，也就存在許多問題和風險，如非法入侵(Intrusion)、網路攻擊(Attack)，甚致電子郵件遭受網路廣告疲勞轟炸等等。

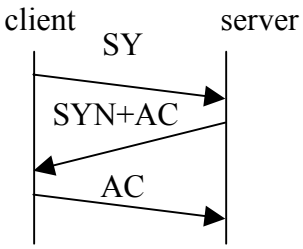
常見的網路攻擊是 Denial of Service (DoS)。許多攻擊必須先以 DoS 阻絕正常主機或網路服務再發動其它弱點探測，如 TCP 序號攻擊（Sequence Number Attack）。

本計畫目的是要針對 SYN Flooding 的網路攻擊設計高效能的網路 DoS 攻擊偵測及防禦系統，結合加密技術與運算能力，期解決目前存在網路環境中的安全性、保密性、穩定性與低效能表現等問題。本計畫著重在安全性方面，期使網路攻擊防禦至少要有以下功能:

1. 防禦 SYN Flooding 攻擊： 防止駭客利用 TCP SYN ACK 的機制，製造假像，而造成系統資源的浪費，進而癱瘓系統。
2. 防禦分散式(DDoS)攻擊：除了傳統的攻擊外，攻擊者有可能利用其他的電腦來造成大量的 SYN 攻擊封包，進而讓系統主機癱瘓。
3. 高效能的服務：在系統遭受到 DoS 攻擊時，通常系統的服務能力會下降，因此必須維持系統效能，以服務正常連線要求。

三、背景知識與方法

在 TCP 的通訊協定中，Client 若要和 Server 建立連線，必先經過三個步驟：Client 送"SYN_X"封包給 Server、Server 回應 Client "ACK_{X+1}+SYN_y"的封包、Client 再回應 Server "ACK_{y+1}"的封包，這也就是所謂的 *TCP 3-way handshaking*。如下圖所示：



SYN Flooding 攻擊原理：

當 Server 送出"ACK_{X+1}+SYN_y"之後，在收到"ACK_{y+1}"之前，由於 Server 必須要記住此時的連線狀態，Server 會將這個``未建立完成之連線''的狀態資訊記錄在記憶體佇列中，而這佇列的大小，即決定了 Server 在這個 port 上，所能接受的"未建立完成之連線"的個數。

SYN Flooding 攻擊，就是藉由不斷地送"SYN"封包給 Server 的某個 port，使 Server 在該 port 上的佇列耗盡，如此一來 Server 若再收到任何來到此 port

的 SYN 封包，便會將之丟棄，也就是說 Server 無法再接受任何此 port 的 TCP 連線服務。

因爲SYN Flooding危害非常普遍，有許多相關的研究用企圖解決SYN Flooding的攻擊，但都不是很有效果。其中包括(a) Firewall Relay：此種方法主要是利用防火牆（Firewall）的方式來防禦，即client須跟firewall先建立TCP連線，然後firewall再跟server建立另一個TCP連線。(b) SYN cookie：此方法是利用加密或是雜湊含數的方式，來對client做認證，且在第一個SYN封包到達伺服器時也不配置計憶體給此TCP連線需求。其認證的方式爲，比對封包內雜湊函數的值是否相同。通過認證的封包，伺服器才會配置計憶體佇列給此連線，因此這個方法，最大的優點在於，能夠保證服務。但因爲要對每個TCP的連線做加密認證，亦較花費CPU。(c) Random Drop：此方法是遭受到攻擊，計憶體佇列已經耗盡時，以隨機的方式刪除一筆佇列中的資料，因此新的TCP連線服務一定可以被接受。而且可以保證計憶體佇列不會有耗盡的現象。(d) Reset Cookie：此方法跟Linux SYN Cookie一樣是以加密或是雜湊函數的方式，來對client做認證，但跟SYN cookie的差別在於：

(1) client端送SYN封包給server時，server會先檢查是client是否在一個特殊的資料結構中，稱之爲Security Association。

(2) 如果不存在則回應``錯誤的SYN+ACK封包''。此時client會重置這個TCP連線，送出RST的封包。

(3) server端會驗證此RST封包，如果此RST的封包的雜湊函數值跟先前server所產生的值一樣的話，則把client端加入Security Association中

我們使用了改良式 SYN cookie 的方法，配合修改 FreeBSD 系統的 Kernel source，用以抵擋惡意 SYN Flooding 的網路攻擊。

四、結果與討論

在 SYN Flooding 攻擊中，攻擊者把大量的 SYN 封包傳送到欲攻擊的伺服器。 然而，這些 SYN 封包中的來源位址皆爲假造的 IP 位址。因此，被攻擊的伺服器其連線佇列中充滿了 SYN+ACK 封包，但是卻不能正常的送出。原因是尚未收到相對應的 ACK 封包。此時受到攻擊的伺服器就不能繼續提供服務，因爲它的連線佇列已滿並且不能接受合法的 SYN 連線要求。

本計畫研究了現有的防禦方法並且比較其優缺點。我們透過修改 SYN Cache 的機制來改進 SYN Cookie 的方法。此外，我們也提出了一個新的解決方案，並且解釋它的設計、並且在 FreeBSD 平台上實作一個雛型系統，然後實測其效能表現。最後，實驗的結果也說明了我們所提出的方法能夠有效地防禦 SYN Flooding 攻擊。

五、成果自評

我們已經在 FreeBSD 平台上實作一個可以防制 SYN flooding 的雛型系統，經過實測已經可以成功地偵測並減低 SYN Flooding 網路攻擊行爲的影響。在研究過程中我們針對網路攻擊問題中的 SYN flooding 導致的 DoS 之防制方法做了充分

的研究，並且將研究心得寫成論文，投稿到 IEEE 國際期刊，預計 2003 年可以獲准發表。

不過我們的系統還有很多改善的空間，這部份我們會在未來研究中繼續努力。

六、參考文獻

[1] Jian-Wei Wang, Hwei-Kai Chang, and Wen-Nung Tsai, “A Study on Router Security with OSPF Routing Protocol,”to appear on International Conference on Advanced Science and Technology Oct, 2001,Chicago

[2] Elliott, J. IT Professional, “Distributed Denial of Service attacks and the zombie ant effect” Volume: 2 Issue: 2 , March-April 2000

[3] Chen, Y.W., “Study on the prevention of SYN flooding by using traffic policing,” Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP.

[4] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni “Analysis of a Denial of Service Attack on TCP,” 1997. Proceedings., 1997 IEEE Symposium on, 1997, pp 208-223

[5] L. S. Laboratories. Livemore Software Labs. Announces Defense against SYN Flooding Attacks, Oct. 1996.

[6] 張惠凱, 蔡文能, "路由器安全性之研究," 國立交通大學資訊工程研究所，碩士論文, June, 2001.

[7] Landwher, C. E, Bull, A. R., and Mc Dermott J. P.,”A Taxonomy of Computer Security Flaws.”, ***ACM Computing Surveys***, Vol 26, No.3, September 1995, pp211-254

[8] 黃韜維, 蔡文能, "A Study on SYN Flooding," 國立交通大學資訊工程研究所，碩士論文

[9] Shih-Kun Huang and Shiao-Rong Tyan, "Intrusion Detection and Vulnerability Analysis for GCA Service, " 1999 Project for Institute of Telecommunication.

[10] David Detlefs, K. Rustan M. Leino, Greg Nelson, and James B. Saxe. “Extended Static Checking,” ***SRC research report #159***, December 1998

[11] Vern Paxson, “Bro:A System for Detecting Network Intruders in Real-Time,”***Proceedings of the 7th USENIX Security Symposium***, San Antonio, TX, January 1998.

[12] Charlie Kaufman, etc., “Network Security: Private Communication in a PUBLIC World,” **PTR Prentice Hall**, New Jersey, 1995.

[13] Bishop,M. “A Taxonomy of Unix System and Network Vulnerabilities”, ***Technical Report CSE-95-10***, Department of Computer Sciences, University of California at Davis, 1995

[14] Biswanath Mukherjee, L. Todd Heberlein, and Karl N. Levitt, “Network Intrusion Detection, “ ***IEEE Network***, May/June 1994.

[15] Some Denial of Service attack tools, http://www.technotic.com/denial.html