行政院國家科學委員會專題研究計畫成果報告

全球資訊網站安全機制與安全通訊協定之研究

A Study on the WWW Security Monitoring Mechanism and Secure Communications Protocol

計畫編號：NSC87-2416-H-009-010
執行期間：86 年 8 月 1 日至 87 年 7 月 31 日
主持人：羅濟群 交通大學資訊管理研究所副教授

一、摘要

隨著網際網路的發展，全球資訊網 (World Wide Web, WWW) 上的商業應用日漸普遍，儼然已成為一個新興的行銷通路。針對 WWW 的安全需求，相關的安全協定也已被提出，例如由 Netscape 所提出的 Secure Socket Layer (SSL) 與由 CommerceNet Consortium 所提出的 Secure HTTP (S-HTTP)。

保護與攻擊是一體的兩面，要能夠保護系統，必須先瞭解攻擊的方法。所以我們將先以攻擊的觀點來著手，研究針對全球資訊網的攻擊方式，再進而提出一套全球資訊網站的安全監控機制。一般網路監督軟體 (Sniffer)，可以達到即時監督的需求，但卻無法提供系統管理者控制的能力，屬於被動的方式；這裡我們將對於現有的安全機制作一番研究，探討其所可能面臨的安全問題和攻擊方式，並提出一個主動式的網路安全監控機制，讓系統管理者除了監督外，還有能力進行控制。對於此主動式安全監控機制，我們也建構了一個雛形架構來驗證其可行性。

關鍵詞：全球資訊網、主動式、安全監控機制

Abstract

With the advent of the Internet, doing business on the World Wide Web (WWW) is becoming more and more popular. In order to meet the web's security requirements, several secure communications protocols, such as Netscape's Secure Socket Layer (SSL), and CommerceNet Consortium's Secure HyperText Transport Protocol (S-HTTP), have been proposed.

Protection and attack are the same thing. If you really want to protect your system, you have to understand all possible attacks in the first place. First, will investigate all possible attacks on the web. Then, on the basis of these attacks, we will suggest a security monitoring mechanism. This security monitoring mechanism is an active control mechanism, which is different from the traditional passive mechanisms, like Sniffer. This active security monitoring mechanism will allow the system administrator to actively protect his web site. We also construct a prototype to examine its feasibility.

Keywords：WWW, Active, Security Monitoring Mechanism

二、緣由與目的

全球資訊網使用 TCP/IP 通訊協定，因此我們從 TCP/IP 來著手，討論全球資訊網站的安全問題。首先探討網站的安全問題與攻擊方法，並提出一個主動式的安全監控機制；然後再針對現有安全協定的缺點加以改進，以防止主動式的攻擊法。本研究之目的是希望能夠發展出一套有效

的安全防護機制，並運用於全球資訊網上。主要包括下列兩項：

1. 設計出一套適用於網站的主動式安全監控機制
2. 設計出一套適用於網站電子商務應用的新一代安全通訊協定

三、結果與討論

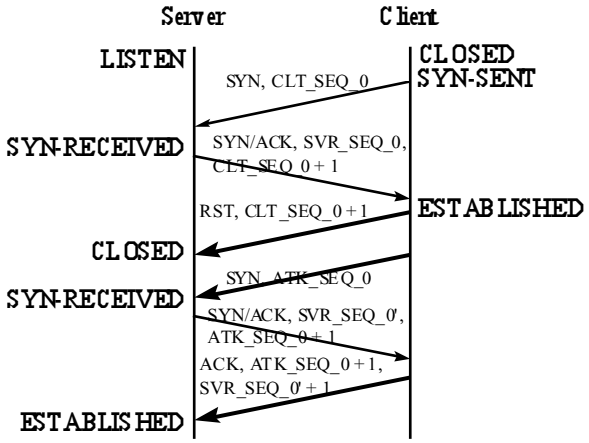
1. 主動式的攻擊方法

在這裡將 TCP 連接分為三個階段：連接建立 (Opening a connection)、訊息交換 (Message exchange) 和連接結束 (Closing a connection) 階段，在此精簡報告中我們只介紹在連接建立階段中如何進行主動式攻擊。

主動式攻擊法主要是要造成連線兩端不同步 (Desynchronization) 的狀態，也就是讓兩邊賴以聯繫的 Sequence number 造成不一致的現象，這些數值包括 Server 端之 Sequence/Acknowledgment number (SVR_SEQ 、SVR_ACK) 和 Client 端之 Sequence/Acknowledgment number (CLT_SEQ 、CLT_ACK)。在連接建立階段的攻擊方式是針對 TCP/IP 之 Three-way Handshake 來作的，造成不一致的方式稱為 Early desynchronization，其過程如圖一所示。

圖一中之粗線箭頭代表攻擊者所傳送的封包。其攻擊流程說明如下：

- 首先，Client 送出初始之 CLT_SEQ_0 與 SYN flag 要求連線，Server 回應其初始之 SVR_SEQ_0、CLT_SEQ_0 + 1 與 SYN/ACK flag，Client 收到後進入 ESTABLISHED 狀態，其所維護的 Seq./Ack. Number 為 [CLT_SEQ_0 + 1, SVR_SEQ_0 + 1]。

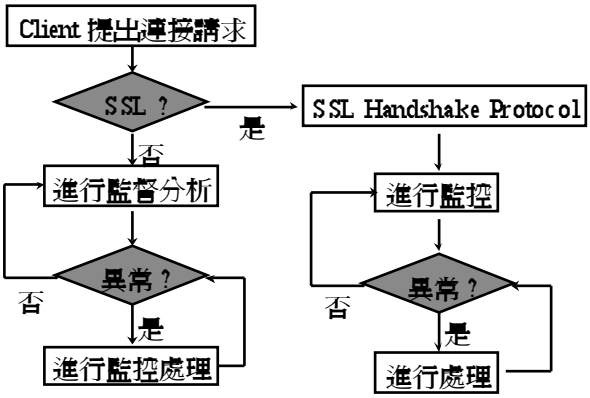


圖一、連接建立階段之主動式攻擊法

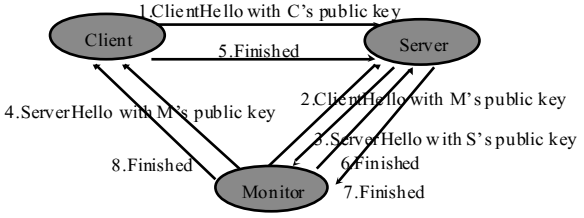
- 此時攻擊者以 Client 之 CLT_SEQ_0 + 1 送出 RST flag 給 Server，於是 Server 結束此連接，但是 Client 不知道。
- 攻擊者馬上緊接著以 Client 之 IP 位址發出另一個連接，送出其初始之 ATK_SEQ_0 與 SYN flag 給 Server，Server 回應另一個初始的 SVR_SEQ_0'、ATK_SEQ_0 + 1 與 SYN/ACK flag，Client 因其 Seq. Number 錯誤而忽略，此時攻擊者則回應 ATK_SEQ_0 + 1、SVR_SEQ_0' + 1 與 ACK flag 給 Server，Server 至此也進入 ESTABLISHED 狀態，但其維護的 Seq./Ack. Number 為 [SVR_SEQ_0' + 1, ATK_SEQ_0 + 1]，而攻擊者所維護的 Seq./Ack. Number 為 [ATK_SEQ_0 + 1, SVR_SEQ_0' + 1]（配合 Server 端）和 [SVR_SEQ_0 + 1, CLT_SEQ_0 + 1]（配合 Client 端）。

至此，攻擊者偽裝成 Client 端與 Server 通訊，而 Client 端卻因 Seq. Number 不對而忽略 Server 所送的訊息，其所送訊息亦因此被 Server 所忽略，只有攻擊者能夠與兩端正確通訊，因此攻擊者必須作為兩者之間的橋樑，幫雙方互傳訊息，而在此時，攻擊者不僅能夠看到兩者之間所傳遞的所有訊息，更能夠依自己的意思隨心所欲地插入、修改和刪除其間的訊息。

2. 主動式安全監控機制



圖二、主動式網站監控流程



圖三、針對使用 SSL 安全機制之主動式安全監控流程

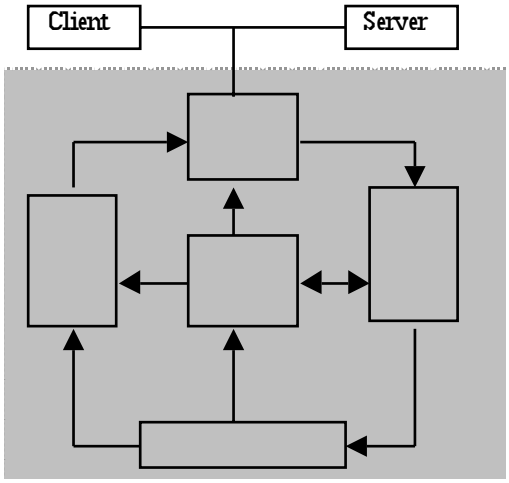
一般網站的安全監控方式有記錄檔分析法和被動式監督法等，除了這些方法，我們應用前面所提出的主動式攻擊法，提出適用於全球資訊網站的主動式安全監控機制。如圖二所示。

針對網站使用 SSL 和沒有使用 SSL 的情況，主動式的監控機制之運作流程如圖二所示。而以前面所提的 SSL 攻擊範例為例，在使用 SSL 安全機制的情況下，主動式安全機制的運作過程如圖三。

使用主動式攻擊法可以獲得比被動式攻擊法 (Sniffer) 更多的主控權，以此方法來實作網路監控程式將可以讓系統管理者擁有更大能力，也更能維護系統的安全。水可載舟，亦可覆舟，端看使用者如何利用這樣的技術。

3. 主動式安全監控機制之可行性模擬

封包收送模組：將封包送出或收入。
封包製作模組：將訊息製成封包。



圖四、主動式安全監控機制架構圖

封包分析模組：將收進來的封包分析，重組還原為原來的訊息。
控制模組：控制封包分析模組、封包製作模組及封包收送模組。

當監控者想要對在網路上傳輸的某個訊息作解析等動作時，監控者透過使用者介面對控制模組下達收封包的命令，控制模組再控制封包收送模組，透過網路卡將想要收的訊息封包收進來。當屬於指定訊息的封包都收進來後，封包收送模組會將這些封包傳給封包分析模組，將封包分析組合，還原為監控者可閱讀的訊息，傳回給監控者。

相反的，當監控者想要送出訊息時，會將想要送的訊息交給封包製作模組。由控制模組告訴封包製作模組該將訊息製成何種格式的封包，最後封包再交由封包收送模組送出去。

當採用主動式監控機制時，監控者要先主動介入連線。監控者透過使用者介面告訴控制模組所要監控的連線，當封包分析模組由封包收送模組收到的封包所分析的訊息中發現所要監聽的連線時，封包分析模組會自動通知控制模組，此時控制模組就會控制送出假訊息，成為一個主動攻擊者，介入連線監聽。當監控者想要介入連線時，再告知控制模組。

測試環境：

Server 端－

機器：SUN Sparc

作業系統：SunOS 4.1.4

WWW Server：Apache 1.2.5 + SSL patch for Apache 1.13

SSL Library：SSLeay 0.8.1b

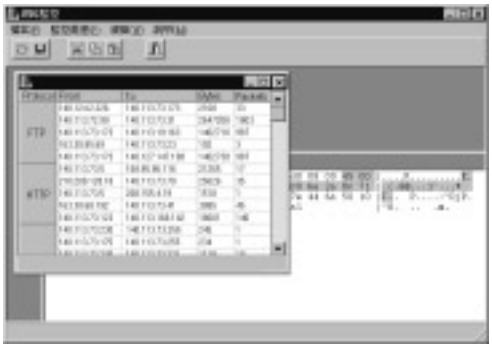
Client 端與監控端－

機器：PC

作業系統：Win95/98

瀏覽器：Netscape Communicator 4.5

以下為此主動式監控程式之部分畫面：



四、成果自評

本計畫原本規劃為三年期的計畫，目前僅為第一年之成果，設計出一套適用於網站的主動式安全監控機制。本年度我們針對全球資訊網站在電子商務上的應用，以及其所面對的安全問題、已知的攻擊方法，和現有的安全機制作一番研究，再針對安全需求，提出一套主動式的安全監控機制，並設計出雛形系統驗證其可行性，能夠完全達到預計之具體成果。在第二年我們將設計出一套主動式安全監控工具，作為系統管理員之安全維護工具。

五、參考文獻

[1] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communications Review 19:2, April 1989, pp.32-48

[2] R. Morris, "A Weakness in the 4.2BSD UNIX TCP/IP Software", Bell Labs Computing Science Technical Report #117, February 1985

[3] L. Joncheray, "A Simple Active Attack Against TCP", Proceedings of the Fifth UNIX Security Symposium, June 1995

[4] M. Neuman, "Monitoring and Controlling Suspicious Activity in Real-time With IP-Watcher, En Garde Systems, 1996

[5] I. Goldberg, D. Wagner, "Randomness and the Netscape Browser", Dr. Dobb's Journal, January 1996

[6] Ray Bird, Amir Herzberg, Phillippe A. Janson, Shay Kutten, Refik Molva, Moti Yung, "Systematic Design of a Family if Attack-Resistant Authentication Protocols", *IEEE Journal on Selected Areas in Communications*. Vol.11, No.5, June 1993

[7] Colin Boyd, Wenbo Mao, "Development of Authentication Protocols: Some Misconceptions and a New Approach", *IEEE Communications*, 1994

[8] Michael Burrows, Martin Abadi, Roger Needham, "A Logic of Authentication", *ACM Transactions on Computer Systems*, vol. 8, no. 1 pp.18-36

[9] Santosh Chokhani, "Toward a National Public Key Infrastructure", *IEEE Communication Magazine*, September 1994

[10] Dorothy E.Denning, Giovanni Maria Sacco, "Timestamps in Key Distribution Protocols", *Communications of the ACM*, Vol.24, No.8, pp.533-536, Dec.1981

[11] W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.644-654, 1976

[12] Warwick Ford, "*Computer Communication Security: Principles, Standard Protocols and Techniques*", Prentice Hall, 1994

[13] Li Gong, Mark A. Lomas, Roger M. Needham, and Jerome H. Saltzer. "Protecting Poorly Chosen Secrets from Guessing Attacks", *IEEE Journal on Selected Areas in Communications*. Vol.11, No.5, June 1993

[14] Li Gong, "Optimal Authentication Protocols Resistant to Password Guessing Attacks", *IEEE Communications*, 1995

[15] "Entity Authentication Using Symmetric Techniques," ISO-IEC Jtc1.27.02.2(20.03.1.2), June 1990

[16] Charle Kaufman, Radia Perlamn, Mike Speciner, "*Network Security: PRIVATE Communication in a PUBLIC World*," Pentice Hall, 1995

[17] S.P. Miller, B.C. Neuman, J.I. Schiller, and J.H.Saltzer, "Kerberos Authentication and Authorization System, "Project Athena Technical Plan, Section E.2.1, MIT Project Athena, Cambridge MA, December 1987.
[18] Needham, R. M. , and Schroeder, M. D. ,"Using encryption for authentication in large networks of computers", *Communications of the ACM*, Vol21, December 1978, pp.993-999.
[19] Donal O'Mahony, Neil Weldon, "X.500 directory service support for Electronic Data Interchange", *Computer Networks and ISDN System* 27 (1995), pp.691-701
[20] Bruce Schneier, "*Applied cryptography: Protocols, algorithms, and source code in C*", Wiley
[21] "資訊工業透析", Nov. 1994