中文摘要

網際網路在現今扮演著非常重要的角色，相對的，網路安全是一個不可忽視的問題。隨著網路的快速發展，WWW 被廣泛地應用，已成為傳遞各種資訊的使用者介面以及軟體工具，帶給使用者包羅萬象的內容。另一方面，網路安全議題的範圍也不斷地擴大延伸，由通訊協定層級升到應用層級，僅僅靠著防火牆或單純的安全存取控制已不足以抵抗網路上泛濫的攻擊。保護個人電腦或是內部網路，應提升至應用層級，也就是檢視文件封包內容。利用傳統的防毒軟體以及經驗可以由病毒特徵、傳播方式、社交工程技巧來找出這些惡意程式，然而，原本是以善意保護封包內容的加密技術，避免遭非法竊聽或惡意竄改，卻反而成為網路安全設備偵測過程中的漏網之魚，成為攻擊者躲避檢測的另一管道，直接或間接地影響到內部伺服器或者是網路整體的安全。

要作到深層檢測，確保整個網路安全，防火牆應該具備檢視加密封包的能力。因此，我們在這篇論文中，提出 SSL 代理伺服器的設計與實作，主要的工作為檢視 HTTPS 加密封包的內容。在此架構下，可以將文件封包還原成未加密的狀態，提供給應用層級防火牆做深層封包檢查，在通過檢查後，再轉送到原本提供資料的伺服器。另外，在 SSL 代理伺服器的運作過程之中，由於已獲得原始的封包內容，可以結合許多應用層服務，我們也搭配實作快取功能。而本篇的討論重點將在於 SSL 代理伺服器還原封包內容的過程。我們將討論設計與實作過程遭遇到的問題及解決方式，並循序說明如何利用 SSL Handshake 的特性，加速建立連線，以及使用 SSL 彈性的加解密演算法，減少傳輸資料過程中的計算負擔。在此技術下，既可達成我們檢視封包，達成深層內容檢測，同時，又可以分擔原網頁伺服器的負載。

Abstract

As usage of the Internet for typical applications increases and new e-commerce and extranets proliferate, World Wide Web (WWW) has become a popular, powerful and convenient tool and application for billions of users. It offers global access to nearly any type of information. However, another disturbing trend has been with regard to the types of attacks malicious parties have been launching. Network security continues to increase in importance. It has comes a security underside fraught with increasing communications and productivities associated with access information, email, streaming media, instant message, etc. While several years ago most attacks exploited network-level vulnerabilities such as flaws in the TCP/IP protocol, today's hackers primarily exploit application-level bugs and come into next generation network attacks. Blended attacks that target new vulnerabilities found in applications. The Intrusion Detection System (IDS) engine ensures that protocols are indeed valid, the application headers are compliant according to the application's legal syntax and semantics, the header values are validated and overflows are prevented as well as analyzes the application payloads and searches for both known and unknown malicious contents. However, the higher-level attacks used by well-disciplined intruders are often transmitted via encrypted SSL connections to web servers and appeared to be legitimate business activity to network-level security device, these attacks can easily penetrate traditional firewalls and the IDSes.

This thesis presents an approach to a practical framework of the SSL Proxy Server which performs cryptographic functions, decrypts packets, restores the origin contents of HTTPS traffic, also provides layer-7 application firewall to inspect the contents and identity the signatures. After performing in-depth intrusion detection

analysis, the SSL proxy server, then forwards secure traffic to the origin web server. Besides, the proxy server also provides several application-layer services such as caching technique due to cipher-text traffic has been decrypted already. In our points of view in this thesis will focus on the detail procedures of restoring content from encrypted packet. Furthermore, exploring the potentials of innovation and improving the performance, the framework has the ability to take advantage of a characteristic of SSL known as resume handshake. It reduces the burden of establishing connection between SSL proxy server and origin web server. In addition, the flexibility and comprehensive SSL cipher suites help transferring data in diverse context. As a result, the refinement not only mitigates the traffic between SSL proxy server and web server but also off-loads SSL processing from web server. We implement our proposal to demonstrate the efficiency functionalities and also give experimental results for all the proposed techniques.