網路安全協定模擬器設計與實作

學生：林恆琳　　指導教授：楊 武 博士

國立交通大學資訊科學研究所碩士班

摘要

由於電腦及網路科技的發展，許多資料都可以數位化後儲存，然後在網路上方便地傳送，但是網路上有著許多的網路駭客在竊聽傳送資料，本論文以資料傳送的安全協定為研究對象，利用模擬安全協定的過程中，設計偵測各種安全漏洞的法則，以提升我們要在安全傳送資料的信心度。

本論文中，利用編譯器技術中的 Scanner 及 Parser，將輸入的 Protocol 做分析，以及利用物件導向技術，將 Check Rules 當作輸入，我們使用漏洞法則(pattern)的方法來分析安全協定，並且探討各個漏洞的特性，這幫助我們在偵測安全協定時有沒有發生漏洞。另外，從實驗的結果，我們知道，在安全檢測法則(pattern)的分析之後，我們認定若符合 pattern 的條件之下，很有可能產生 pattern 下所描述的 Flaw，但若不符合 pattern 的條件的話，就一定不可能產生 pattern 下所描述的 Flaw。因此本論文提出的安全協定模擬方法對偵測安全漏洞和增強安全性質都有很好的助力。

Security Protocol Simulator

Student: Lin-Hen Lin Adivsors: Dr. Wuu Yang

Department of Computer and Information Science

National Chiao Tung University

ABSTRACT

Since computer science and network are developed, many data can be digitized and stored in hard discs or compact discs. And it is convenient to transmit in the network. But there are a lot of network hackers who can steal the transmitting information in the network channel. This paper focus on network security protocol simulation. In the process of the simulation, we design all kinds of check rules about detecting security flaw. It can help us promote the confidence of transmitting data.

In our paper, we use the technology of compiler-- Scanner and Parser, and we have the analysis of the input network security protocol. We use the technology of object orient to take some check rules as input. We use the method of check pattern to help the analysis of the network security protocol. On the other hand, from the result of experiment, we can get some message. After the analysis of check pattern, if we confirm that it can match the condition of check pattern, it could have this kind of flaw. But if it doesn't match to check pattern, it will not have this kind of flaw. Therefore, the method of security protocol simulator in our paper is helpful to detect the security problem and enhance the security property.

誌謝

首先，我要感謝我的指導教授　楊武博士的指導，由於老師專業知識的傳授與持續不斷的幫助和指導，並督促我做實驗和寫論文，假如沒有老師的鼓勵和指導，學生很難順利完成這篇論文，在此，向老師致上最深的謝意。

接下來，我要感謝的是程式語言與系統實驗室的所有同學，大家的陪伴讓我在這兩年來的生活中感到許多溫暖。畢業的仁和學長、明彥、承穎學長及雅芬學姐，在我功課繁忙時，常常關心我的生活和課業，並提供意見，這讓我很快地適應研究生的生活，真的很謝謝他們。俊元和宗強是和我要一起畢業的同學，我們同舟共濟，互相鼓勵，我在寫論文的過程中，著實受到他們許多幫助，我非常感謝他們。

最後，感謝我的家人，爸爸、媽媽、老婆和妹妹，我在研究所的這段日子，生活作息非常不規律，對於爸媽的許多關心，我覺得很窩心也覺得很抱歉，在生活上給予我的照顧和支持，使我無後顧之憂，能夠順利完成碩士學位，最後僅以此論文獻給我最親的家人和朋友，由衷地謝謝他們。

目錄

圖表目錄