Android 上的入侵偵測系統

學生：羅日宏　　指導教授：曾文貴 博士

國立交通大學資訊科學與工程研究所碩士班

摘　　要

當手機的功能變得越來越強大，並且在結合了 WIFI 上網功能之後，我們該如何確保手機的安全性？我們或多或少都會在手機裡面儲存一些重要資訊，舉凡：通訊錄，簡訊內容，用手機拍下的照片，其重要性不亞於電腦中的各種檔案，或者可說是更敏感的個人資料。Android 系統是由 Linux 系統當作基礎，並且加上 JAVA framework 所構成，目前 Android 被廣泛地使用在手機上並且當作一個作業系統，Android 上的安全性還沒有辦法完全被確保，所以我們將 Snort，一個 Linux 平台上相當熱門的入侵偵測系統，移植到 Android 手機中，並利用 Snort 的強大功能封包檢查功能以確保手機在上網時的安全。

Porting Snort on Android

student：Jih-Hong Lo　　Advisors：Dr. Weng-Guey Tzeng

Department of Computer Science and Engineering
National Chiao Tung University

ABSTRACT

When the cell phone becomes more and more sophisticated, and the wireless network has been integrated with the cell phone network, how do we ensure that the cell phone has the security features? In Android, an open source embedded system developed by Google, although by its Linux-based design, there are not that many attacks exist, but sooner or later, the virus, the Trojan horse, or even worms will be developed for the Android platform. Back to the basic point of view, how can we ensure the security when we are surfing on the internet? The most trivial and important way to ensure the security is to scan the packets that flow in our cell phone. We present Snort, a popular intrusion detection system, on Android platform and with its powerful ability, we can detect that if there are malicious contents in the packet flow.

誌　　謝

首先感謝我的指導教授曾文貴老師，在我碩士班兩年間的學習過程中，帶領我深入密碼學的領域。老師積極認真的教學態度，使我受益良多。另外，我要感謝我的口試委員，中研院呂及人教授，交大謝續平教授以及交大蔡錫鈞教授，在論文上給我許多指導與建議，讓我的論文更加地完善，除此之外，我還要感謝實驗室學姊林孝盈的許多幫助，以及實驗室的學弟妹和其他碩士班同學的幫忙。最後，我要感謝我的家人，不論在精神上以及物質上都給我極大的支持，讓我在無後顧之憂的情況下可以順利完成學業。在此，謹以此文獻給所有我想要感謝的人。要謝的人太多了，那就謝天吧。