

# 自傳

我是李士暄，畢業於台大資管所。

就學期間，修習資管系/所課程外也選修許多資訊工程系/所的課程，技術上熟悉Linux作業系統、Git版本控制、開發過linux kernel module以及Android App，碩士論文實作一套**虛擬化惡意軟體側錄系統(VMI-based Malware Analysis System)**，同時也樂愛研究開源軟體，並積極參與各項開源軟體大會。

目前在尋找「軟體工程師」的職缺，期望未來成為一位專業的軟體工程師。

## 大學畢業專題

大學畢業專題中，我擔任Programmer的角色，主要負責程式的撰寫與系統架構設計，我們將傳統桌遊-殺手，流程改造至智慧型手機上，並在無須行動網路下，透過Hotspot/WiFi即可連線進行遊戲，本遊戲在Google Play上架(<https://goo.gl/9hbK7e>)累積下載量約為**10000~50000**。



## 研究所的資安訓練

研究所期間，我參與研究室的計畫，並在ubuntu上自行編譯Linux Kernel以做後續開發kernel module之用，同時，我也研究過**Android系統安全**，包含root手機、對App進行逆向工程、交叉編譯Samsung toolchain。我也協助實驗室學長建設惡意軟體分析系統，我們修改UC Berkeley的TEMU系統，使其可以在虛擬機器中側錄惡意軟體的行為特徵，並結合docker與VirusTotal API製作成一套**自動化惡意軟體分析平台**。



在論文研究上，我透過研讀Windows kernel資料結構後，開發「虛擬機器記憶體檢測指令」到QEMU介面中，再研究Windows function call stack後，在KVM code中撰寫x86 Assembly使其能側錄虛擬機器內惡意程式所呼叫Windows APIs call的參數值與回傳值，並將側錄結果以in-memory的方式存成檔案，以供後續分析之用，最後本研究獲得「**科技部資訊安全實務**



## 趨勢科技的暑期練功

碩一暑假，我參與全球資安領域領導品牌**趨勢科技**的實習，藉由加入防毒軟體測試團隊(PC-Cillin QA Team)，我學習到完整的軟體開發流程，並嘗試撰寫test plan進行測試以維持軟體品質，在過程中運用Python撰寫「自動化測試工具」減少測試步驟，同時與RD Team緊密合作解決產品的bug。

在趨勢的實習不僅擴展了我在職場上的視野，同時也了解一個成熟軟體的開發生命週期。

