中原大學

暨

定興實業有限公司

無線網路側錄鑑識系統效能測試及報告

委託研究契約書

中華民國 95 年 7 月 1 日

委託學術界研究契約書

立約人中原大學(以下稱「甲方」)及定興實業有限公司(以下稱「乙方」)。緣甲乙雙方為進行無線網路側錄鑑識系統效能測試及報告研究事宜，特立本契約，並同意條件如下：

第一條：雙方合意

乙方同意委託甲方執行無線網路側錄鑑識系統效能測試及報告(以下稱「本研究」)，甲方同意承包，從事本研究。

第二條：研究內容

本研究之內容如附件：無線網路側錄鑑識系統效能測試及報告研究計畫書(以下稱「計畫書」)。

第三條：研究進度

本研究執行期間自民國 95 年 7 月 1 日起至民國 96 年 6 月 30 日止。

第四條：研究進度

一、甲方應依計畫書之約定，進行本研究。

二、乙方得視需要要求甲方就本研究之進度提出口頭報告及相關資料，或派人員至甲方了解甲方執行本研究之情形。甲方對該人員應提供一切必要之協助。

第五條：成果交付及驗收

一、甲方應於每次測試完成後繳交測試報告予乙方。

二、甲方應依計畫書之規定期間繳交期末研究成果。

三、研究成果之內容及形式應依一般規定辦理。另凡屬特定技術或演算法的程式實作應交付該成果原始碼。

第六條：研究費用

本研究之費用總計新台幣(下同)NT$241,500 元整，其細目如計畫書。

第七條：付款辦法

本計畫付款方式共分 12 期：

1. 本契約生效後支付 21,500 元
2. 本契約生效後每隔一個月支付 20,000 元，共 11 期。

第八條：保密義務

甲方為執行本契約所取得或持有的資訊，非經乙方事先書面同意，不得洩漏或交付予任何第三人或運用於本契約無關之工作。甲方應要求其參與本研究之人員遵守本契約之約定。甲方或其參與本研究之人員違反本條契約約定者，甲方應負責賠償乙方因此所受之損害。

第九條：契約份數

本契約壹式陸份，正本貳份，副本肆份，由乙方執正本一份，副本一份，甲方執正本一份，副本三份。

立合約書人：

甲方：中原大學
代表人姓名：熊慎幹
職稱：校長
地址：中壢市中北路 200 號中原大學

統一編號：45002502
計畫主持人：鍾斌賢
職稱：資訊工程系副教授

乙方：定興實業有限公司
代表人姓名：張侃
職稱：總經理
地址：台北市民生東路五段 36 巷 4 弄 31 號 4F
統一編號：22367327

中華民國 95 年 7 月 1 日

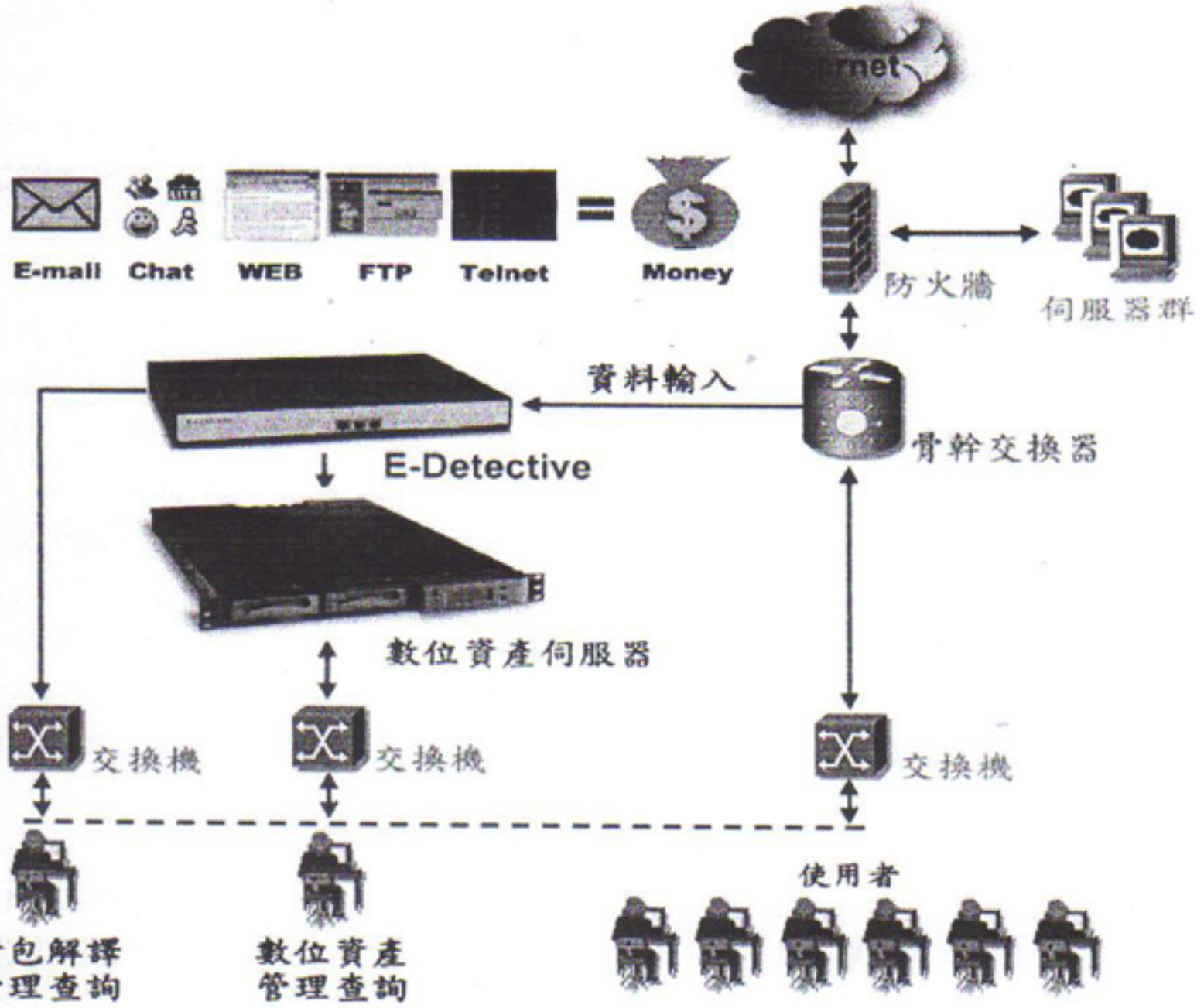
定興實業有限公司專題研究計畫申請書

申請機構/系所（單位）	中原大學資訊工程學系
本計畫主持人姓名	鍾斌賢
職　稱	副教授
本計畫名稱	無線網路側錄鑑識系統效能測試及報告
全程執行期限	自民國 95 年 7 月 1 日起 至民國 96 年 6 月 30 日
計畫連絡人	姓名：鍾斌賢　電話：(公) (03)2654716
通訊地址	中原大學資訊工程系
傳真號碼	(03)2654751
E-MAIL	bsjong@ice.cycu.edu.tw

一、前言

定興實業有限公司開發完成之數位資產管理系統(E-DETECTIVE)可以自動側錄電子郵件、即時訊息、網頁瀏覽、檔案上傳及下載、Telnet 等網路資訊交流活動內容。E-DETECTIVE 採優質化的 Linux 為設計核心，並搭配 Java 超強的外掛功能，提供一個完整的操作介面，讓使用者可以快速安裝使用；E-DETECTIVE 的快速封包監聽技術，可以在不影響原來的網路環境架構下，進行特定目標或範圍之側錄工作。

數位資產管理系統建置圖



E-DETECTIVE 系統包含網際網路封包與訊息之偵測、截取、側錄、解讀、內容管理、資料儲存與查尋功能。E-DETECTIVE 能完整的「記錄」並「保存」所有企業網路上流通的資訊，並且能夠提供給管理階層調閱、查詢及稽核所需之訊息。E-Detective 將資料儲存在資料庫及知識庫中，可以依需求製作出各類網路活動管理報表。管理者可透過報表資料的分析，了解每位員工上網的活動，包括電子郵件（包含 e-mail, web mail, hotmail）、即時訊息（Instant Message）、瀏覽網頁（Web Pages Browser）、傳送及接收檔案（FTP）及遠端登入(Telnet)。

本計畫之團隊於上年度之「數位資產管理系統網路效能測試及報告」計畫完成測試 E-DETECTIVE 在各種網路環境下之執行效能，並提供完整測試報告。我們從 E-DETECTIVE 硬體平台、網路交換器、及網路流量三方面來測試效能，並已經提供完整之報告及建議事項，對貴 公司之產品效能提供許多的助益。

本年度之計畫將針對 E-Detective 無線網路側錄鑑識系統進行測試，並提供完整之報告及建議事項。

二、E-DETECTIVE 無線網路側錄鑑識系統

無線網路監聽及定位是利用無綫網路卡收集收發信息双方溢出在空中傳遞之無線電波，予以解碼分析，且可與己完成之有線側錄監聽設備及 GPRS 等電信服務進行系統串聯，完成資訊傳遞交換，並整合資料庫成為一體，達成全方位之無線監聽和定位，及信息內容側錄監視等功能。

E-Detective 無線網路封包擷取與還原解析設備主要包含前端偵測擷取單元及後端還原解析單元。前端偵測擷取單元用於偵測無線區網的基地台(Access Point，簡寫為 AP)及與該基地台通訊的通訊戶(Station，簡稱為 STA)，並進行傳輸封包之側錄；後端還原解析單元則是將擷取到的網路封包電磁紀錄依特性加以分類，還原先後次序及儲存，同時並將分類後的封包依所知的規則(Protocol)，予以解譯成明碼儲存在資料庫中，隨時供使用者查核。

E-Detective 無線網路封包擷取與還原解析設備之前端偵測擷取單元共計有二個產品。第一個產品為無線網路偵測器(Wireless LAN Detector)，該產品具有 802.11b/g 網路通訊第二層(Layer2)之偵測功能；第二個產品為探嗅器(Sniffer)，用於側錄無線網路封包。

1. 802.11b/g 無線網路封包偵測器(Wireless LAN Detector)

主要功能是偵測本偵測器可觸及範圍內所有 802.11 無線網路之通訊，並在偵測到的無線網路區域內，偵測出有那一些無線區網的基地台(AP)及與此基地台通訊的通訊戶(STA)。

偵測到的無線區網的相關資訊包含如下:

- AP 的 BBSID(MAC 位址)。
- 所使用的頻道。
- 有多少個 STAs。
- 有多少個加密封包。
- 有多少個資料封包。

- AP 的一些額外資訊(依 AP 品牌,必須 AP IC 元件製造商已經過國際註冊認證者)。
- 雜訊強度(noise level)及訊號強度。
- SSID or BBSID。
- 無線網路的形態：Probe， Ad-hoc， Infra。
- WEP 狀態。
- 無線區網內封包傳輸總數量。
- 其他。

至於所偵測到 STA 的相關資訊如下:

- 有多少個加密的封包進出這個 STA。
- 總共有多少個封包進出這個 STA。
- 這個 STA 的 IP 位址(IP Addess)。
- 這個 STA 的 MAC 位址。
- 這個 STA 的製造商(已經過國際註冊認證者)。
- 這個 STA 的最大傳輸速率。
- 這個 STA 的雜訊和訊號強度。
- 這個 STA 的種類(Established， To-DS， From-DS)。
- 其他。

2. 802.11b/g 無線網路探嗅器(Sniffer)

主要的功能是側錄某個指定無線區網內所有無線封包。為達成側錄之完整性，探嗅器可以建立以下各種組態(Configuration)及功能。

- 可以架設多個探嗅器分散式地側錄，並可透過網路聯線將各個探嗅器側錄到的資料集中處理分析。
- 每個探嗅器可以裝上多張無線網卡同時側錄。
- 每張無線網卡可以跳頻道地或鎖定某頻道的方式去側錄。
- 在知道 WEP KEY 的情形下，可以即時邊側錄邊解開加密封包。
- 可在側錄到足夠量的 WEP 加密封包之後，嘗試求得加密的 WEP KEY，進而用以解出過去側錄得到的資料。
- 側錄下來的 802.11 資料封包可以進一步用 E-Detective 作應用層（Application Layer）的處理，並儲存到資料庫作日後的分析運用。

三、預期完成工作

本計畫預期完成工作計有：

1. E-DETECTIVE 功能測試

協助定興實業有限公司進行 E-DETECTIVE 功能測試，提供測試報告載明系

統錯誤（Bugs）的地方，並提供使用者操作界面建議供參考。於本計畫執行期間，若有新版本完成，則提供該版本之完整功能測試。

2. E-DETECTIVE 網路效能測試

測試 E-DETECTIVE 硬體平台所能負載之頻寬（Bandwidth），並提供完整之負載環境報告。本計畫將進行抗壓測試，且提供定興實業有限公司所生產之各類機型之測試報告。於本計畫執行期間，若有新機型生產，則提供該機型之完整功能測試。測試所需軟硬體及網路器材將由定興實業有限公司提供，並於計畫完成後歸還。

3. 協助進行其他網路環境效能測試

於本計畫執行期間，若定興實業有限公司需進行大型網路服務提供者（Internet Service Provider）之環境測試，則提供必要之測試協助，並完成測試報告予定興實業有限公司。

4. 技術諮詢

於本計畫執行期間，提供產品開發、網路及網路環境效能測試等之技術諮詢服務。

四、預期人力

級別或姓名	人數	月數	總計
計畫主持人	5,000 元/月	12 月	60,000 元
研究生(2 人)	5,000 元/月/人	12 月	120,000 元

五、經費

項目	金額
人事費	180,000 元
雜費(無線網路卡、差旅費、文具、影印、紙、碳粉匣、光碟、、、等)	30,000 元
管理費(15%)	31,500 元
總計	241,500 元