建置使用DNSSEC機制對網路釣魚攻擊之研究

張筱涵* 楊富丞+ 鄭進興+ 程毓明*
樹德科技大學資訊管理系研究所* 高雄第一科技大學資訊管理系+
s94631105@mail.student.stu.edu.tw u9424355@ccms.nkfust.edu.tw

摘要

隨著網際網路發展，人們生活對網際網路的依賴性逐漸上升，相對地，網路安全更是重要的一環。網路釣魚攻擊是一種線上身份竊取的行為，像是竊取網路銀行的帳號、密碼以及信用卡卡號等。一旦沒做好防護時，損失的不只是顧客的金錢，企業組織的形象也跟著受損。根據2005年3月由SANS安全組織所發的一個新攻擊警告:「有關於駭客去攻擊DNS伺服器導致對".com"的所有連線請求轉送到另一個假冒網站，有約超過900個IP位址請求與75,000件email訊息受影響」。故提供一個能防範網路使用者遭受網路釣魚攻擊之工具與DNS伺服器不因惡意人士攻擊而無法提供正常服務是現今社會所迫切所需的要求。本研究根據探討問題採用研究方法之質性研究並配合DNSSEC機制，發展一套能針對防範網路使用者遭受網路釣魚攻擊之工具，並分別以DNSSEC機制之簽章技術來防護DNS伺服器的轄區資料不被攻擊與驗證技術來確保網路使用者所請求資料的正確性與完整性，以確保能提供給網路使用者一個完善、安全的網路環境，以間接促進電子商務的發展，避免再次因受到網路釣魚攻擊造成無可彌補的損害。

關鍵詞： 網路釣魚、Pharming、DNSSEC

1、緒論

1.1 研究背景

現今資訊科技與網際網路所提供的各種便利性與重要性已是不可或缺的，然而隨著網際網路的快速發展，網路攻擊事件之數量、規模有越來越嚴重的趨勢，越來越多的系統透過網路連結在一起，惡意人事攻擊系統的危險性也逐漸上升。駭客入侵一直是有網路以來最為頭痛的問題之一，在今日大多數的服務都是可透過網路的線上方式來進行，只需按下滑鼠即可完成金融交易或市場採購。此外，研究發現(CNET，2005)(台灣電腦網路危機處理暨協調中心，2004)，假如DNS伺服器沒有完善的安全防護措施，而導致後果除了資訊洩露、DNS伺服器無法提供服務外，亦可能演變成網路欺騙行為並造成受害者金錢上的損失或無法想像的損害。尤其是在未來IPv6的IP位址，其組成更為複雜。IPv6的IP位址不像IPv4的容易去記憶，一段惡意人士利用人性的弱點去混淆IP位址而有所利用時，嚴重時，亦使整個DNS伺服器服務無法提供服務。根據CERT/CC的統計資料顯示(CERT/CC，2004)，網路入侵事件之數量在近年來已有倍增的趨勢，截至2003年CERT/CC總共接獲了319,992個入侵事件的求助。由此可見，不論攻擊事件或安全弱點都節節上升，弱點發現的速度增快，相對在利用弱點入侵的事件也增加許多。有許多弱點攻擊程式都放在網路上任人下載，故不需到高深技術即可入受他人的系統，因此強化個人、企業或是政府的電腦安全之工作，是有其急迫性與重要性。

1.2 研究動機

駭客入侵他人電腦皆有其目的，其中以圖利個人經濟利益為最嚴重。根據網路釣魚防制工作小組(Anti-phishing Working Group)2006年7月份的Phishing Email Reports指出，在統計網路釣魚事件中，產業分佈中的金融產業事件佔了93.5%驚人數量;而新網路釣魚網站成立的數量為14191，比上個月暴增了4144個。由此可見，網路釣魚之事件雖然已不是新的案例，但仍是層出不窮的出現在生活中。如何避免事件一再發生，除了靠使用者的認知、判斷外，仍需靠些外在的工具或其他方式來避免。就目前市面上所提供的工具，仍未可完全防止網路釣魚事件的發生，

不論安全的防護機制做的如何地滴水不漏，還是免不了會有應用程式弱點、人的知識不足、系統架構等問題存在，這些問題的存在就成了內部及外部惡意的攻擊者或駭客最好的入侵管道，若要以網路釣魚防護工具-toolbar，例如：Netcraft、SoofStick、AntiPhish…等進行偵測。儘管有提供了網路釣魚防護工具，仍擋不住如洪流猛獸的攻擊及入侵。分析其原因有二：一為安全防護設定不良及忽略了相關的系統弱點修補，使用駭客仍有機可趁去攻佔網路服務器；二為使用者未建立對網路釣魚的認知與判斷，包含新技術的產生、使用者的資訊安全知識建立、網路釣魚防護工具的使用等。因此較有效的方式是採用折衷的方式，建立一套能整合上述工具之優點，並配合DNSSEC機制做防護，建立能防止DNS Spoofing技術發生，並透過對使用者所發出的query與DNS做一簽章與驗證的程序，使得使用者能安全的透過網際網路進行交易，避免遭受金錢上的損失。

現今網際網路所提供的各項服務，無一不仰賴DNS伺服器提供最正確的IP位址。假若DNS伺服器沒有完善的安全防護措施，那後果除了資訊洩露、DNS伺服器無法提供服務之外，亦可能演變成網路欺騙行為並且造成受害者金錢上的損失或是無法想像的損害(台灣網路資訊中心，2003)(鄭進興、陳威安、陳嘉玫、林敬皇，2004)。目前由IETF(The Internet Engineering Task Force)的NIST所發展的DNSSEC機制(Olaf. M. Kolkman，2002)，雖可有效的避免DNS系統冒名欺騙

(DNS Spoofing)，但因DNSSEC機制的設計不良而至現今仍無法全面實施。DNSSEC機制要全面實施非配合公開金鑰機制(PKI)不可，但DNSSEC機制在設計之初卻是使用共同金鑰(secret key)，而此一設計並無法配合現今的DNS架構。

1.3 研究目的

綜合上述分析中不難發現，雖然使用了相關的資訊安全措施，但駭客仍藉由網路服務和電腦系統中存在的弱點來進行入侵並建立假網站。因此，本研究預期建立一套網路釣魚及Pharming的防護系統。整個系統將結合上述軟體之部份優點與功能，並搭配DNSSEC安全防護機制來防制DNS Spoofing，建立主動式的DNS層級網域名稱防護機制以及被動式的網域名稱白名單資料庫系統，分別對網路使用者之網路釣魚防護工具、DNS與網路使用者間之簽章與驗證二大方面做開發，以防止網路使用者因網路釣魚攻擊而蒙受金錢損失。

本研究機於這樣的前提，發展及建立相關網路釣魚攻擊偵測與防護之方法，藉由偵測網路釣魚攻擊並提供適當的防護機制，杜絕與防護企業及組織單位的網頁服務器或Email服務器能夠免於駭客的入侵與破壞。並進一步地捍衛網路、使用者個人隱私資訊與系統的安全。

2、文獻探討

談到網路釣魚攻擊行為預防，首先要了解網路釣魚攻擊的由來與現況，以了解各種網路釣魚攻擊行為的產生方式、使用技術以及攻擊手法後，再針對網路釣魚攻擊進行分析才能確實了解此一特定的攻擊行為在整個網路環境中的影響；接著是分析預防此類攻擊行為之現有的機制、技術與產品之模式，從中取得各項優點做為機制與系統建立之基石；最後結合現今各個組織、機構所發展的預防網路欺騙攻擊之優點來建立一套機制與系統以預防網路釣魚攻擊行為，並觀察、分析本研究所建立的機制、系統能否有效降低網路釣魚攻擊行為之發生。

2.1 網路釣魚攻擊

2.1.1 網路釣魚的興起

Phishing的攻擊方式是在騙取網路上的使用者洩露有關於個人隱私資訊的銀行帳號和詳細資料。近來的攻擊方式不斷的進步，最新的攻擊方式是運用客戶尋找和連接組織的名稱主機或服務的方法透過對名稱做lookup的程序做修改，一般被稱為「Pharming」。Pharming最早約莫出現在2004年，它藉由入侵DNS（Domain Name Server）的方式，將使用者導引到偽造的網站上，因此又稱為DNS下毒（DNS Poisoning）(黃志輔，2005)，此種攻擊行為是能躲避過目前現有防護網路釣魚攻擊工具的。因此，此種攻擊最受影響深切。

在2005年3月由SANS安全組織發佈一個新攻擊的警告，是有關於駭客去污濁一些DNS伺服器，導致所有對".com"要求連結的都導引到另一個釣魚者所架設的替代網站。透過簡單的社會工程和好的電話態度，攻擊者通常可以愚弄網域名稱註冊並獲取網域名稱的控制。

2.1.2 網路釣魚的攻擊手法

網路釣魚是當前世上蔓延相當快速的一種詐騙行為，攻擊技術不斷地出新招，讓人總是無法即時地反應去避免受到災害。進行一個網路釣魚行動前，最基本的就是架設假冒網站。攻擊者會先從網路中掃描有漏洞的主機，當有掃描到可入侵的主機時，則進行建立後門的動作，為以後留個後路以方便進出。等到建立好後門後則將事先做好的假冒網站上傳至有漏洞的主機中，開始發送垃圾郵件直到等到受害者上鈎後取得其隱密資訊和金錢。此一動作就依此循環一直循環下去。

然而，網域名稱下毒也就是目前網路釣魚所延伸出最新的技術 - Pharming是現今最擔心的攻擊之一。而網域名稱下毒即是駭客利用他們所控制的一個DNS伺服器向其他DNS伺服器提供不正確的資訊(避開新陷阱，2005)。駭客即利用DNS能將收到網域名稱轉換成IP位求的請求給予回應，來造成使整個網路上的DNS伺服器都會受其遭害。Pharming近年來已越演越烈，攻擊範圍也越來越大，攻擊並破壞DNS伺服器後，再透過這些伺服器來找尋更多的網路用戶連接到駭客的魁儡網站，假的IP位址從出現到消失的度越來越快。

透過上述分析可知，網路釣魚犯罪在實體層面並沒有想像中的複雜，但需要注意的事，複製現有網站已無技術性可言，只需靠滑鼠及少數選項即可完成。現今科技的進步速度可說是日新月異，防治網路釣魚的攻擊行為甚至是任何網路犯罪可說是正面的資訊科技與負面的資訊科技之間的戰爭。

2.2 現在工具、產品之分析

目前市面上較常使用的工具與產品中，分為二大類。一類為網路釣魚，所阻擋的包含Email或是一般假冒網站的連結；另一類為Pharming，所阻擋的是對於DNS查詢時以防止查詢到經網域名稱中毒所回傳的假資料。

屬於網路釣魚：

Netcraft工具(Netcraft，2005)：此工具bar是由

Netcraft社群所提供的網路釣魚站台資料庫中比對，其運作方式是透過比對IP位址與所註冊的網域名稱的區域是否同屬同一國家所有來做為判斷。但若註冊網域名稱與IP位址所屬於不同國家，則易誤判為惡意網站。

SpoofStick工具(台灣網域名稱俱樂部，2005)：此工具bar是由CoreStreet企業所提供的免費瀏覽器助手，其運作方式是透過去尋找是否有註冊網域名稱來做比對。但有個問題點，若連結的是IP位址，則可能被判定為惡意網站。

SpoofGuard工具(Neil Chou，2004)：此工具bar主要是由Host Name、URL、Image、Links以及Password共五個做為其主要的判斷惡意網站的加權指數-門檻值。但使用上可能在相似網站上，當第一次連結時會先被判為惡意網站，需經手動別後，當再次連結才可能判為正常網站。

屬於Pharming：

AntiPharming 工具(PC OFFICE，2005)(AntiPharming，2005)：是由NGSEC公司所提出的，其運行在Windows平台上來鎖定DNS伺服器中的Host檔案不被他人修改，以及在DNS查詢中察覺疑似DNS Pharming的異常時，最少再和3個安全無虞的DNS伺服器做比對，來降底網路使用者被引導至詐騙網站上進行各項網路查詢、交易操作。

此工具有個問題，DNS query(查詢)有二種方式，一種為DNS Cache，另一種為command。若其與3個安全無虞的DNS伺服器做比對的方式是採用經由DNS Cache時，則可能因DNS Cache Poisoning而已造成無論再如何查詢也是查到假冒的網站；而若是以command的方式，則可透過先將DNS Cache清除後，再經由dig或是nslookup的指令來做查詢。雖不能說保證能查到最乾淨的回應，但至少會比經由DNS Cache查到的安全。

2.3 DNS 攻擊

網路釣魚攻擊事件與網路基礎服務的網路名稱伺服器習習相關，因此DNS的安全防護是相當重要的一環。DNS Spoofing攻擊之作法，即是利用竄改DNS名稱查詢服務的回應。目前已有真正能避免DNS伺服器遭受DNS Spoofing攻擊的安全機制(DNSSEC)，但實際應用上卻未能真正全面實施。就BIND 9版本已有加入DNSSEC機制，但預設是關閉的。為了對抗上述的惡意攻擊或是入侵行為，於1997年發表了第一個防護DNS安全的RFC文件，之後相關的技術與文件亦陸續被學者提出(Giuseppe Ateniese & Stefan Mangard，2001)。

2.4DNSSEC安全機制

因應上述DNS Spoofing問題，IEFT發展一個DNSSEC(DNS Security Extensions)機制(D. Eastlake，1999)以解決DNS通訊或傳輸資訊的驗證與保密的方案。如圖1所示，DNSSEC機制可協助DNS伺服架之間及DNS伺服器與一般使用者端之間的通訊安全。

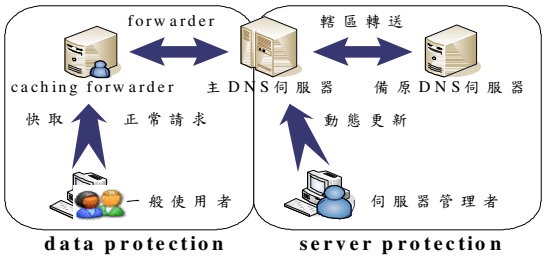

圖1：DNS通訊或傳輸之解決方案
資料來源：(鄭進興、陳威安、陳嘉玫、林敬皇，2004)

DNS安全的主要技術為TSIG與DNSSEC：交易簽章(Transaction Signature, TSIG)指利用密碼學編碼方式為通訊傳輸資訊加密以保護DNS訊息的安全，確保在進行轄區資料傳送時不被竊取與監聽；DNS安全防護功能的擴充(DNS Security Extensions)指利用密碼學的公開金鑰加密機制，以保證每一傳輸的可驗證性與不可否認性，確保資料傳輸遭受Spoofing或竄改等安全問題。(Olaf. M. Kolkman，2002)。此外，TSIG主要應用於DNS之間Zone Transfer的動作，故可確認DNS資訊是否由某特定DNS伺服器所提供，相對的講法，就是可避免發現資料遭篡改或DNS Spoofing攻擊。

3、研究架構與方法

3.1 採用之研究方法與原因

根據探討網路釣魚問題，本研究主要目標是從網路基礎服務著手，建構一個能讓使用者查詢正確網址並防護攻擊發生的系統，以避免網路釣魚攻擊事件之發生，並減少網路使用者及金融機構之有形金錢與無形商譽的損失，故本研究所採用的研究方法為質性研究方法中的實驗法。本計畫以網路服務的安全角度來看，透過防護網路釣魚攻擊與DNSSEC機制，尋找並消彌危害網路安全的相關因子，以鞏固及強化網路使用者、網路伺服器主機及服務的安全性。

3.2 危害網路服務安全的相關因子

維護網路服務的安全，可分從四個層面來看，分別是網路使用者的資訊技能教育、網路服務伺服主機(一般主機)的作業系統、網路服務伺服主機(一般主機)所使用的應用程式以及網域名稱註冊到期日。

現今人們的生活環境已離不開網路，購物、銀行作業都是透過網路來進行。安全弱點存在於我們使用

網路、作業系統上的每個環節，因此為找出防範網路釣魚事件之發生，則必須分別針對網路使用者、DNS、網路服務伺服主機及一般個人電腦進行不同的防護。本計畫基於此一概念下，進行研究與建構系統化、有效率及低成本的網路釣魚防護機制 並發展一自動化防護網路釣魚、DNS查詢的簽章與驗證等功能，提供網路使用者、網路管理者以及企業管理及防護網路釣魚攻擊事件之發生，並更進一步地捍衛網路與系統的安全。

3.3 研究架構

本計畫研究架構如下圖2所示，主要的部份為：建構運用在使用者之網路釣魚防護機制、建構DNS查詢之簽章與驗證之主動式網域防護機制、主動式網域名稱回報、系統實測與數據蒐集分析等四個部份。

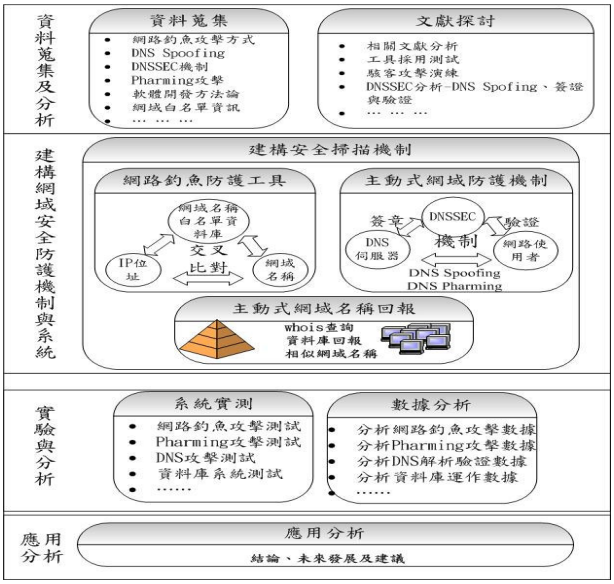

圖2：本研究之研究架構方塊圖

3.3.1 建構網路釣魚防護工具

本研究的上述主要部份之第一功能將分為二個部份：一個是建構網域名稱白名單資料庫系統；另一個是建構具正確性、完整性之交叉比對IP位址與網域名稱之網路釣魚防護之機制。

網路釣魚攻擊，本身就像個作業系統似的，會有不斷的弱點或漏洞被發現。網路釣魚即是隨著新技術的產生即有新的攻擊事件發生。目前沒有一套能完整阻隔網路釣魚攻擊事件之發生。在此，本研究將透過網域名稱與所屬IP位址做交叉性比對，比對條件將包含IP位址與網域名稱所申請的國家區域是否相同、指令式dig或nslookup、host來做查詢對應IP位址、攻擊特徵比對、掃描相似網域名稱之註冊等比對方式。此外，將透過與目前現在產品做比較與分析其優缺點，以調整此研究之網路釣魚防護工具為更完善，其檢測流程如下圖3所示。

- **前置準備階段**

網域名稱白名單資料庫的資料可能一直得追隨著腳步來更新，否則此資料庫的資料若不是最新的話，可能會造成誤判率的發生。

- **內部資料比對階段**

網域名稱白名單資料庫，第一步檢測即是與資料庫中的資料做比對，若此筆資料存在於資料庫中，則此網站為真正的網站，反之，則先判定為疑似為假冒的網路釣魚網站。

- **外部資料比對階段**

比對所屬國家，從IP位址可以判定出是屬於哪個國家所擁有，可藉由這項資料來判斷IP位址與其擁有的網域名稱是否同屬同一個國家擁有。藉此連結到惡意人士的伺服主機以騙取金錢。

透過指令dig、nslookup、host來查詢網域名稱與IP位址之對應，查詢對應方式有二種，一種是透過網頁連結去對DNS Cache做查詢，一種是透過命令列模式對DNS做查詢。此二項的優缺點，透過DNS Cache做查詢的情況，可能因已遭受到DNS Spoofing攻擊而導致DNS Cache到的資料都是錯誤的；而透過命令列模式的，則可先將DNS Cache重新清除後再對DNS重新做查詢，以保障所查詢的資料之正確性。在此研究中，是採用透過命令列模式來做查詢比對。

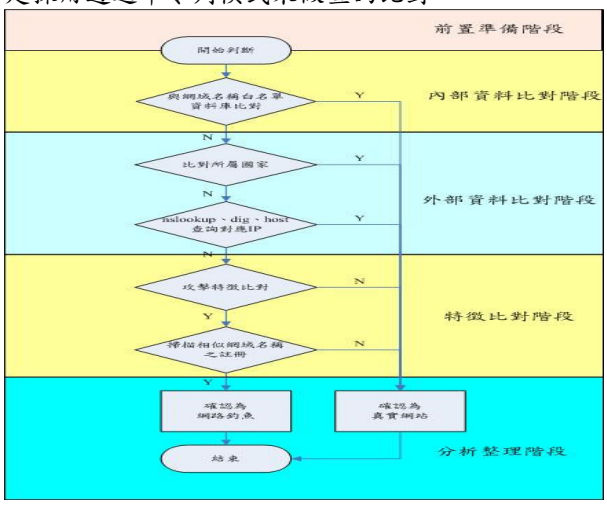

圖3：檢測流程

- **特徵比對階段**

攻擊特徵比對，是透過對網路釣魚攻擊相關文獻之分析而找出可能的攻擊特徵及後端資料庫以做為檢測之依據。在實驗環境中，會架設一台IDS以做為網路釣魚攻擊之研究分析，以配合對特徵比對做詳細的

分析。

- **分析整理階段**

最後的階段是將以上各階段的比對分析統整後加以整理與整合，佐以歷史資料，分析與比對並做出最後的決定，判斷是否為假冒的網路釣魚網站。而針對於最後是否要連結與否，為避免因產生誤判率而造成無法連結至網站，工具僅是提醒使用者連結的安全性，而決定權仍在於使用者。

進行網路釣魚防護所必須要考慮的層面很廣，為能有效地進行防護受到攻擊，對網站的網址進行檢測是必要的。

3.3.2 建構網域安全防護機制與系統

本研究之網域安全防護機制系統是以目前的DNS運作方式為基礎，規劃將以DNSSEC機制來防止發生DNS Spoofing、DNS Pharming發生，並以DNSSEC機制對DNS伺服器之間做簽章動作以及DNS伺服器與網路使用者間的DNS查詢加以驗證的動作，讓惡意人士無法去竊改資料。因此使用DNSSEC機制之後的每筆記錄，皆具有完整性與可驗證性，網路使用者可驗證其查詢的記錄是否為惡意造假的。

本研究的網域防護機制是植基於原本的DNS之上，因此運作方式與目前DNS運作方式相同，而網域防護機制與原本DNS在運作上的不同之處，在於下圖4的DNS運作方式已使用密碼學的加密演算法保護其轄區資料：

(1). 使用者向TW的DNS伺服器發出查詢某個網域之請求；

(2) . TW的DNS伺服器會先尋找其轄區資料有否該筆記錄，如果有該筆記錄便回覆給請求者，若無該筆記錄則向另一個DNS伺服器(例如COM.TW的DNS)進行詢問的動作；

(3). 直到擁有該筆記錄的DNS伺服器回覆該筆記錄給TW的DNS伺服器；

注意：而在從TW的DNS伺服器向其他擁有該筆記錄的DNS伺服器之間的溝通時，利用DNSSEC機制對該筆記錄做簽章的動作，以防止有DNS Spoofing的情況發生。

(5). TW的DNS伺服器回覆使用者其請求的網域之IP位址；

(6). 使用者收到TW的伺服器之訊息。

注意：當使者用收到TW的伺服器之訊息，則利用DNSSEC機制對所收到的訊息做驗證的動作，以確保資料未被竄改。

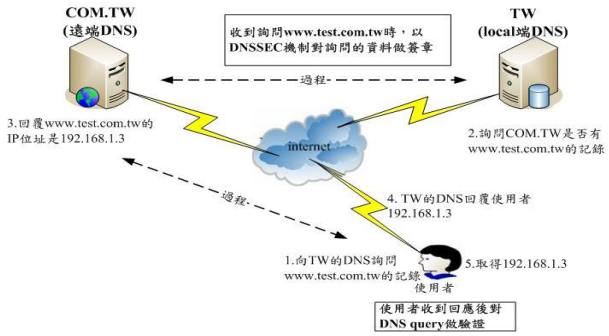

圖4：適用於本研究之DNS運作

本研究的網域防護機制之主體是由三個部份所組合而成，分別為：

(1). 最基本的DNS伺服器；

(2). 用來防護DNS伺服器的DNSSEC機制；

(3). 網路使用者。

網域防護機制所提供的服務是一個具備安全性的DNS服務，最後機制能否成功需仰賴實際環境的配合，因在實驗的模擬環境是可實施的，但若要應用在實際網路環境時，則有全面的DNS伺服器是否支援與使用者端作業系統是否支持等問題。然而，本研究之主要構想是當一般網路使用者看到某一個涉及錢金交易的網域，例如www.citybank.sec時，便能夠信任此一網址為合法的網站，而不必擔心受騙。

3.3.3主動式網域名稱回報

本研究之主動式網域名稱回報，是一個可主動地回報網域名稱給所擁有此網域名稱的組織單位。將計畫設計一個能主動掃描whois資料庫中所提供能查詢資料中的網域名稱註冊資訊，並透過定期的掃描以確保能在網域名稱即將到期前主動的通知所擁有該網域名稱之組織單位，以確保不會被盜用。

3.3.4 系統實測與數據蒐集分析

在系統實測與數據蒐集部分，本研究在實驗環境中加入一個入侵偵測防禦系統，如下圖5所示，利用此一系統蒐集相關資訊，例如惡意人士的企圖入侵、攻擊以及正常網路服務請求，並且同時進行流量分析。

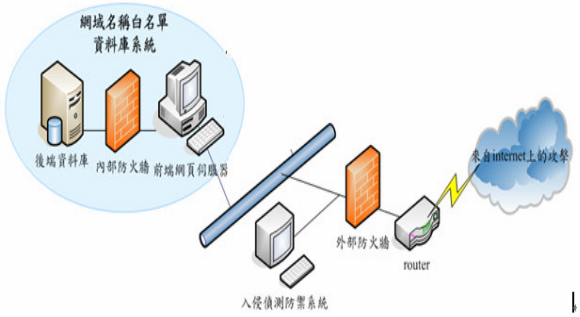

圖5 系統實測與數據蒐集網路環境圖

本研究在進行系統實測的部分，會以正常請求與異常攻擊兩種方式進行，正常請求方式是為了驗證本研究之系統是否能正常運作於真實網路環境之中，而異常攻擊方式是為了驗證本研究於真實網路環境中運作時，能否抵禦惡意人士的入侵與攻擊。

本研究將實驗的測試數據記錄於技術報告之中，並以客觀的角度來分析本研究發展之機制與系統能否抵禦惡意人士的入侵與攻擊，以及有效減少網路釣魚攻擊，最後是分析本研究所發展的機制與系統之可行性。

3.3.5 應用分析

最後的一部份為應用的相關分析，將防護網路釣魚機制、主動式網域防護機制、主動式網域名稱回報等等的機制做更緊密的結合，做為公司或組織單位中防範網路釣魚的強大助力而免受弱點之威脅。使此類網路釣魚防護機制能夠持續發展，以期未來改善可能受遭害的網路伺服主機或一般個人主機、DNS伺服器的安全。

4、結論

網路釣魚攻擊在生活中是越來越常遇到，而該如何去做真正的阻擋，這是需靠大家以及工具的配合。本研究提供網路釣魚防護工具之建置、利用DNSSEC機制來防護DNS伺服器的轄區資料，並利過DNS spoofing/hijacking的攻擊測試來測試是否能達到防護的功能。

網路安全為一整體性之工作，因此本研究將以網路釣魚防護機制、主動式網域名稱防護機制，並透過建立入侵偵測防禦系統來偵測，達成遭受攻擊前的防禦、攻擊時的防護與追查等網路安全之徹底解決方案。預期透過檢測機制來強化各類網路服務安全與幫助公司及組織單位規避因網路釣魚、安全弱點而引起的安全威脅。

ACKNOWLEDGEMENT

This work was supported in part by TWISC@NCKU, National Science Council under the Grants NSC 94-3114-P-006-001-Y.

5、參考文獻

DNS

[1] D. Eastlake(1999). Domain Name System Security Extensions. RFC2535,

[2]Giuseppe Ateniese & Stefan Mangard. (2001). A New Approach to DNS Security(DNSSEC). Computer and Communications Security, 86-95.

[3]Olaf. M. Kolkman(2002). DNSSEC Operational H OWTO. (RIPE NCC No. 43)

[4]鄭進興、陳威安、陳嘉玫、林敬皇(2004)。DNSSEC安全防護機制實作之研究。資通安全。2004台灣網際網路研討會，台東大學。

網路釣魚

[1]Anti-Phishing Working Group ， APWG(2004), http://www.antiphishing.org/.

[2] APWG(2006,July). Phishing Activity Trends Report. Retrieved July 28, 2006, from http://www.antiphishing.org/reports/apwg_report_july_2006.pdf .

[3] Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz(2005), "Anatomy of a Phishing Email".

[4] Ed Felten(2005, March 14). Freedom to Tinker-Pharming. Retrieved October 21, 2005, from http://www.freedom-to-tinker.com/index.php?p=781 .

[5] Knight, William, "Goin' phishing?", Infosecurity Today Volume: 1, Issue: 4, pp. 36-38, July - August, 2004.

[6] Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh and John C. Mitchell(2004). "**Client-side defense against web-based identity theft".** 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, February, 2004.

[7] SANS (SysAdmin, Audit, Network, Security) http://www.sans.org

[8] TWCERT/CC(2005), http://www.cert.org.tw/.

[9] 巫坤品、曾志光(2004，初版二刷)。密碼學與網路安全原理與實務。台北：碁峰。

[10] AntiPharming官方網站(2005)。上網日期，94年12月3日，檢自：http://www.ngsec.com/ngproducts/antipharming/?lang=en .

[11]Netcraft推出防網路釣魚工具(2005)。上網日期：2005年12月5日，檢自：http://pc4.gamebase.com.tw/content.jsp?l=2002&no=37003&cno=370030002& sno=65022919&rc=2&lock=0&top=0&p1=6 .

[12]台灣網域名稱俱樂部(2005)。安全研究:網絡釣魚的原理與防範。上網日期：2005年11月3日，檢自：http://www.domain.club.tw/printthread.php?t=6715 .

[13]黃志輔(205，7月)。新網釣技倆：Pharming。上網日期：94年12月10日，檢自：http://taiwan.cnet.com/enterprise/column/0,2000062893,20101093,00.htm .

[14]避開新陷阱(2005，4月25日)。網路世界周報，第14期，上網日期：94年11月23日，檢自：http://www.cnw.com.cn/store/detail/detail.asp?articleId=29055&ColumnId=3162&pg=&view= .