行政院國家科學委員會專題研究計畫 成果報告

資安技術真實流量實地評比--子計畫二:資安技術網站應用防火牆、攻擊防禦與點對點應用控制之真實流量評比(資訊安全技術)

研究成果報告(精簡版)

計 畫 類 別 ： 整合型
計 畫 編 號 ： NSC 99-2218-E-009-015-
執 行 期 間 ： 99 年 08 月 01 日至 100 年 07 月 31 日
執 行 單 位 ： 國立交通大學資訊工程學系（所）

計 畫 主 持 人 ： 邵家健

計畫參與人員： 碩士班研究生-兼任助理人員：王馨卉
碩士班研究生-兼任助理人員：鍾佳妤
碩士班研究生-兼任助理人員：蔡禮陽
碩士班研究生-兼任助理人員：陳星閔
大專生-兼任助理人員：段佳宏

公 開 資 訊 ： 本計畫涉及專利或其他智慧財產權，1 年後可公開查詢

中 華 民 國 100 年 10 月 31 日

中文摘要：

根據『Symantec Internet Security Threat Report』2007 年第一季的報告指出，有高達 66%的新型態攻擊都是與 web application 有關的；以往的資安威脅大多是針對網路層或是系統底層，有越來越多的新型態網路攻擊是針對應用層、網路應用服務或是系統本身的漏洞而來；可能是利用程式碼間的漏洞，也有可能是把攻擊夾帶在檔案或是可植入程式碼的圖片中再予以散佈，尤其是以透過 Peer-to-Peer 應用服務影響更大，因為使用者可能不清楚檔案來源主機是否安全；現今的 network firewall 及 IDS/IPS 如果沒有持續地更新系統、病毒碼及特徵碼的話，將只適用約 25%的網路攻擊，因為有高達 75%的網路攻擊將超出其偵測能力範圍。

本計畫將著重於資安偵測防禦系統測試平台之建置與測試評比網路應用程式防火牆(WAF)、入侵預防系統(IPS)及點對點控管(Peer-to-Peer Control)三項資安偵防技術；結合流量錄製、流量萃取、資訊重組、資訊詢問及流量重播技術，重播真實網路流量來找出任何潛在的資安威脅或是已發展的資安偵防技術不足之處。預期在一年內可以發展出 WAF、IPS 及 P2P control 三類 Specific 資安技術之實地與重播測試技術，發表這三類資安技術相關之專利與論文如: malicious webpage scoring、extracting ambiguous sessions with IPS、QoE of P2P streaming、evasion survey，研發多個網路監測點錄製流量的工具以及可萃取這三類資安技術相關流量內容的萃取工具，同時將執行至少上三件以上的資安產品測試案。

英文摘要：

According to Symantec Internet Security Threat Report in the first quarter of 2007, threats for web applications and web applications related are as high as 66% of new types of attacks. Former security threats mostly aimed at network or system level, but nowadays more and more threats aim at application layer, application service and system vulnerabilities. They may use unsafe programs or be attached or implanted in the picture to distribute widespread, especially by peer-to-peer applications that users even have no ideas about which peers they exchange information with. If network firewalls or IDS/IPS don’t continue to upgrade their systems, virus definitions and signatures, they would fail to detect the newest network threats. They may only be applied to 25% of network threats because 75% of attacks are beyond their detection capabilities.

The project will focus on the building of security detection/protection system and the benchmarking of three types of security technologies-Web Application Firewall (WAF), Intrusion Prevention System (IPS) and Peer-to-Peer Control. Combined five benchmarking technologies-traffic recording, traffic extraction, information reorganization, querying, and traffic replaying with real

flows, we can discover and resolve any potential network threats and find out the advantages/disadvantages of the security technologies. This project aims to develop security techlogies about WAF, IPS, P2P Control capturing, extracting and replaying and to propose related patents and papers, including malicious webpage scoring, extracting ambiguous sessions with IPS, QoE of P2P streaming, evasion survey. Besides, at least three testing cases are also executed.

一、 前言

根據資策會 MIC 分析報告指出，2008 年台灣資訊安全市場規模約為新台幣 140 億元，如果每年穩定成長 14.6%，預估 2012 年市場規模將挑戰新台幣 242 億元。若再依產業類型進一步分析，其中的安全威脅管理及應用安全管理的複合成長率高達 17.7%，是資訊安全產業中成長潛力最高的。

點對點應用(Peer-to-Peer, P2P)

點對點技術(Peer-to-Peer)[1, 2]是依賴參與者可以提供的計算能力與頻寬，沒有客戶端與伺服器端等不同角色；所有的客戶端在擷取網路資源的同時，本身也在提供某部分的網路資源供他人使用。參與者間的連接可以是任意的，也可以是依照某特定規則而形成的；點對點技術有很多種應用，包含檔案下載(BitTorrent、eMule、Gnutella 等)、視訊串流(PPLive、PPStream 等)或語音通話(skype)等，透過在多個網路端點上複製、傳送資料來加速或是降低系統出錯的機率。雖然起意是好的，但是目前已知可以透過 P2P 發起的攻擊已經有病毒、垃圾郵件、間諜軟體，及拒絕服務等攻擊。在 2007 年 CA 公司更發表資安警訊明確指出，在 Foxy、BitComet、eDonkey 等 14 種 P2P 軟體存在安全威脅，包含可能會覆寫檔案、重新命名檔案、刪除檔案或是被第三方植入惡意程式等。

入侵預防系統(Intrusion Prevention System, IPS)[9, 10, 11]

入侵預防系統是一個能夠監管網路應用程式傳輸行為的網路安全設備，能夠即時的調整、阻擋或中斷某些不正常或是具有傷害性的網路傳輸行為。入侵預防系統也像入侵偵測系統(IDS)一樣，會檢查封包，查找系統內已定義的威脅代碼特徵值，並加以記錄以利後續分析。但是，入侵偵測系統在發現異常情況時僅能及時向網管人員或是防火牆發出警報，並不能有進一步防護措施。入侵預防系統則不同，在發現有異常情況或是發現入侵時，可以迅速做出反應，並自動採取相對應的措施，如過濾、阻擋、丟棄或是中斷連線等，以期降低受害機率及影響範圍。

網路應用程式防火牆(Web Application Firewall, WAF)[12, 13, 14]

OWASP 在 2010 年提出『The Ten Most Critical Web Application Security Risks』，分別是『注入(Injection)』、『跨站腳本攻擊(Cross-Site Scripting, XSS)』、『失效的驗證與連線管理(Broken Authentication and Session Management)』、『不安全的物件參考(Insecure Direct Object Reference)』、『跨站請求偽造(Cross-Site Request Forgery, CSRF)』、『不正確的安全設定(Security Misconfiguration)』、『不安全的加密資料儲存(Insecure Cryptographic Storage)』、『限制網址存取失效(Failure to Restrict URL Access)』、『傳輸層保護的不足(Insufficient Transport Layer Protection)』及『未驗證的重新導向與轉發(Unvalidated Redirects and Forwards)』等十種，其中『跨站腳本攻擊』與『SQL 注入弱點』更是已經

連續幾年列為全球嚴重資安弱點。

在新一代應用層服務架構中，不論是通訊協定本身、Web 應用伺服器、Web 應用程式、資料庫存取服務、資料庫系統等，都各自存在不同程度的資安漏洞，而這些漏洞更可被駭客串成許多不同的攻擊方式，衍生成不同的資安威脅[15, 16, 17]，所以發展了網路應用防火牆技術(Web Application Firewall, WAF)來保護 Web 應用服務本身的安全威脅、防止企業用戶受惡意網站之程式污染，及找出隱藏在 Web 應用服務中新型態之攻擊手法，以確保整個 Web 應用服務的完整及可靠性。

流量來源(Traffic Source)

此整體計畫預計使用由交大網路測試中心(NBL)結合交大資訊技術服務中心(ITSC)，在總計畫與子計畫一中共同以交通大學宿舍網路所建置之 Beta Site 做為真實網路流量來源。目前 Beta Site 在交通大學學生宿舍共擺放 48 台 48 port switch 銜接學生個人電腦，有來自 1200~1500 位同學長期使用各種網路應用程式所產生的網路流量。這個環境提供本計畫一個絕佳的平台，除了提供真實流量以發展及評估網路鑑識各個元件的技術，更可用以部署所發展的鑑識系統，協助產品問題重製(Bug Reproduction)及校園流量分析(Traffic Profiling)與問題鑑識(Forensics)。

二、 研究目的

本計畫將著重於資安偵測防禦系統測試平台之建置與測試評比網路應用程式防火牆(WAF)、入侵預防系統(IPS)及點對點應用控管(Peer-to-Peer Control)三項資安偵防技術所需要的工具或機制，結合流量錄製、流量辨識萃取、資訊重組、資訊詢問及流量重播技術，重播真實網路流量[18, 19, 20]來找出任何潛在的資安威脅或是已發展的資安偵防技術不足之處。

針對上述類型的資安技術產品，預計使用交大 Beta Site 與測試儀器的交互使用進行測試，測試的項目有：(1) 串連模式(in-line)系統之功能性、穩定性與效能性，以及(2)主動偵測系統之功能性與相容性。

真實情境之自動化驗測與除錯

1)串連模式系統之功能性、穩定性與效能性

對於串連模式系統的『穩定性測試』，我們可以直接利用 Beta Site 進行測試，驗測系統在面臨一千多位使用者時的穩定程度，是否有出現如當機、重開機、程式當掉、變慢、容易斷線…等等不穩定的情形；若系統出了問題，也有良好的除錯機制，其中包括遠端電源(remote power)、遠端控制(remote control)等方便研發人員從遠端進行觀察，還有 bypass switch 的設備可以在待測物發生問題時，讓網路流量繞道不要經過待測物，如此便不會影響一般使用者的網路使用，可兼顧測試及正常使用。整體

架構如圖 1 所示。

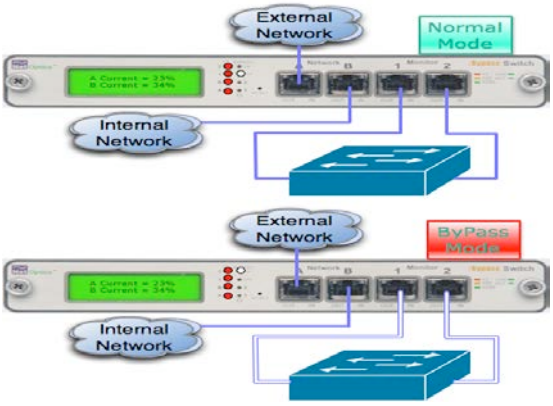
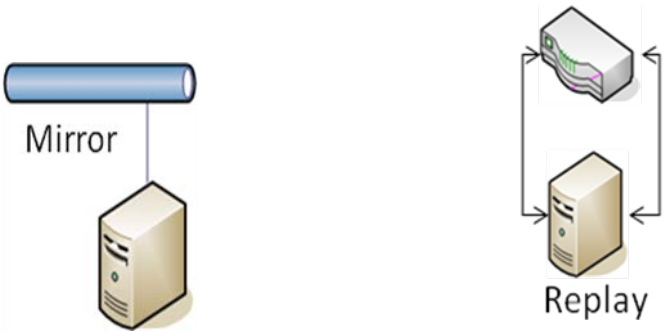


圖1：串連模式系統示意圖

對於『功能性測試』與『效能性測試』，我們可以利用流量重播(traffic replay)的技術來與測試設備交互使用，讓整個測試環境更逼近真實面，如圖 2 所示。先以 mirror 方式將真實網路錄製下來，再利用 replay 方式，根據待測物的系統規格、特性，將網路流量重播至待測物上，監控待測物在整個測試過程中所發生的反應。



先錄製網路流量　　再加以重播進行測試

圖2：流量錄製與重播測試示意圖

2)主動偵測模式系統之功能性與相容性

對於主動偵測模式系統的相容性測試，我們可將該系統放上 Beta Site 各種不同網域的環境，對各式各樣不同環境進行主動式的偵測與掃瞄來進行測試，藉以驗測該系統是否可以正確判斷出不同類型網域、不同主機上所出現的弱點或漏洞，如圖 3 所示—Beta Site 透過終端使用者(Endpoint)收集各種網路應用程式流量以供測試，再根據待測物不同特性及設定情境進行測試。在進行此測試同時，我們必須建立一通順的測試結果回報系統，讓各終端使用者可以針對偵測與掃瞄的結果給予相對的建議。

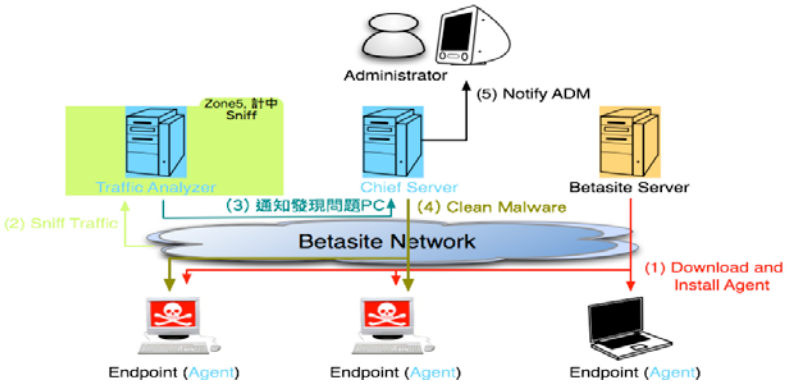


圖 3：主動偵測模式系統

除此之外我們還可以測試在這樣擁有大量終端使用者的環境中，驗證系統於各區域內是否能偵測與掃瞄的使用者電腦、Server、Security 及 Internet Host 數量。

三、 文獻探討

[1] T. Karagiannis, A. Broido, N. Brownlee, K. Claffy, and M. Faloutsos, “Is P2P dying or just hiding?”, in *IEEE GLOBECOM* 2004.

[2] T. Karagiannis, A. Broido, M. Faloutsos, and K. Claffy, “Transport Layer Identification of P2P Traffic,” in *Proceedings of the 4th ACM SIGCOMM conference on internet measurement* 2004.

[3] A. W. Moore and K. Papagiannaki. “Toward the Accurate Identification of Network Applications”, in *Proceedings of the 6th Passive and Active Measurement Workshop* (*PAM*), Oct. 2005.

[4] M. Roesch. “SNORT: Lightweight Intrusion Detection for Networks”, in *LISA ’99: Proceedings of the 13th USENIX Conference on Systems Administration*, Nov. 1999.

[5] Saifulla, M.A., Murthy, H.A., Gonsalves, T.A. “Identifying Patterns in Internet Traffic,” in *Proceedings of the 15th international conference on Computer Communication*, 2002.

[6] M. Crotti, F. Gringoli, P. Pelosato, L. Salgarelli, “A Statistical approach to IP-level classification of network traffic,” in *Proceedings of the 41th IEEE International Conference on Communications*, June 2006.

[7] M. Crotti, M. Dusi, F. Gringoli, L. Salgarelli, “Traffic Classification through Simple Statistical Fingerprinting,” in *ACM SIGCOMM Computer Communication Review on Volume 37, Number 1*, January 2007.

[8] L. Bernaille, R. Teixeira, I. Akodjenou, A. Soule, K. Salamatian, “Traffic Classification on The Fly”, *ACM SIGCOMM Computer Communication Review*, 2006.

[9] Neil Desai, “Intrusion Prevention Systems: the Next Step in the Evolution of IDS,” on SecurityFocus.com, 2003.

[10] Nick Ierace, Cesar Urrutia, and Richard Bassett, “Intrusion prevention systems”, *Ubiquity*, Volume 6, Issue 19, 2005

[11] MB Rash, A Orebaugh, G Clark, and B Pinkard, “Intrusion Prevention and Active Response: Deploying network and host IPS,” BOOK, 2006.

[12] P Byrne, “Application firewalls in a defence-in-depth design,” *Network Security* 2006.

[13] JP Pereira, “Comparison of Firewall, Intrusion Prevention and Antivirus Technologies”, Juniper Networks, Inc. 2004.

[14] D.W. Park, “A study about dynamic intelligent network security systems to decrease by malicious traffic”, in *IJCSNS* 2006.

[15] S.J. Stolfo, “Worm and attack early warning”, in *IEEE Security & Privacy*, 2004.

[16] V.A. Siris, F Papagalou, “Application of anomaly detection algorithms for detecting SYN flooding

attacks", in *Computer Communications* 2006

[17] A Shulman, "Web Application Worms", on packetstorm.austin2600.net.

[18] Tcpreplay, http://tcpreplay.synfin.net/trac/

[19] Tomahawk, http://www.tomahawktesttool.org/, 2005

[20] Y.C. Cheng, U. Holzle, N. Cardwell, S. Savage, and G.M. Voelker, "Monkey see, Monkey do: A tool for TCP tracing and replaying,"in *USENIX 2004*.

[21] Po-Ching Lin, Ying-Dar Lin, Yuan-Cheng Lai, Tsern-Huei Lee, "A Hybrid Algorithm of Backward Hashing and Automation Tracking for Virus Scanning," in *IEEE Transactions on Computers*, Vol. 60, No. 4, pp. 594-601, April 2011.

四、 研究方法

串連模式系統之功能性、穩定性與效能性

測試項目：

本測試項目如表 1~表 3 所列，可分為：Security Effectiveness、Performance，以及 Stability & Reliability 三類。Security Effectiveness 主要是測試待測物在不同情境設定下是否能夠正確執行防禦機制；Performance 主要是測試待測物在不同情境設定下之效能表現；Stability & Reability 主要是測試待測物在不同情境設定下是否能夠持續穩定地進行操作。

Security Effectiveness:

Item	Description
OWASP Top 10 attacks	確定DUT是否能夠偵測出以及並抵擋掉OWASP Top 10 attacks的攻擊。
Capable of detecting and blocking EVASION attacks	驗證DUT是否能夠偵測以及抵擋搭配evasion逃脫工具產生的攻擊行為。
Effectiveness of the fragment reassembly mechanism	進行IP layer的packet size進行切割，藉此考驗DUT的IP fragment reassembly機制的運作。
Effectiveness of the stream reassembly mechanism	該項目針對的對象是TCP封包的packet size進行切割，以考慮DUT對於TCP stream的reassembly機制進行考驗。
URL obfuscation & normalization	試圖向攻擊目標(web server)，發出經由工具產生的惡意URL，以讓DUT無法分辨出request URL是否為惡意連結。

表 1：Security Effectiveness Test

Performance:

Item	Description

Maximum Capacity	驗證DUT在sensor mode及host/agent mode下，在不同的connections/sec、transactions/sec、packet size以及concurrent connection的條件下，DUT的detection engine會有什麼樣的表現及影響。
Attack detection / blocking – normal load & maximum exceeded load	驗證在DUT(sensor mode and host/agent mode)在不同負荷下(e.g.：75%、100%、150%)，detection engine是否能夠完整地阻擋測試過程中產生的exploits。此項測試的基準值是取上一項測試中得到的數據為代表。
Real World application traffic	這項測試除了包含了真實環境中的web server至測試環境中，另外也加入了現實網路中常見的各種application、media及一些知名的web-based application及包含一些惡意攻擊來當背景流量。

表 2：Performance Test

Stability & Reliability (結果的表示為Pass或Fail其一)

Item	Description
Blocking under extended attack for 8 hours	產生持續性的內容為exploit的流量與正常合法的連線穿越DUT(如果是host/agent mode的話，則是與DUT連線)以100Mbps(或是50000pps，平均封包大小在120-360 bytes)的速度，持續8小時的測試。觀察對象為非法的exploits是否有漏擋的情況。
Passing legitimate traffic under extended attack	與上一項測試一樣(8小時)，差異在於觀察的對象不一樣，該項測試觀察正常合法的連線流量是否全數通過，沒有被誤擋下來。
Protocol fuzzing / mutation	將DUT曝露於各類fuzzing/mutation tools所產生的流量下，並觀察整個過測試過程裡是否有漏擋任何exploits。
Detect exploits over both IPV6 and IPV4	驗證是否能在同時在ipv4及ipv6的網路上，正確無誤的辯識出exploits。
Failover test	如果DUT有支援ha的功能的話，會進行active-active(A-A）以及active-passive(A-P)的負載平衡以及備援機制的驗證。
RealFlow Field Test (Beta Site Test)Need in-line mode	運用交大beta-site內參與測試的學生平日對於網路上的使用習慣以及內容，運用在待上市的產品，進行上市前的穩定性考慮及產品潛在問題的尋找。

表 3： Stability and Reliability Test

測試架構圖:

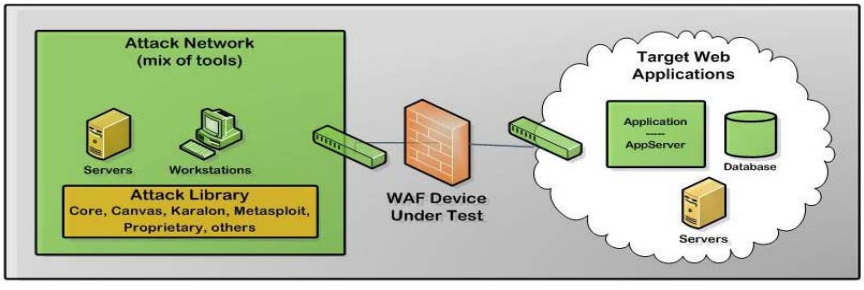


圖 4：應用層資安威脅偵測及防禦平台測試架構圖

如圖 4 所示，整個測試環境可分成三部份，左半部為攻擊發起端(attacker)，組成元件可能會有：nessusd/webscarab/paros…等。右半部則是攻擊受害端(victim)，包含了各類的 service 以及可能的潛在弱點(包含 webgoat)。中間則是放置 DUT 或是其它 inline mode 測試對象(IPS)。進行測試所需硬體及軟體設備如表 4 所示：

Traffic generator	Test tool	Test Equipment
Spirent SmartBits (L2~L4 traffic)、Spirent Avalanche (L7 traffic)	SmartFlow、Attack library、WebGoat/webscrab、Karalon traffic IQ、Whisker(HTTP exploits)、Acunetix Web Vulnerability Scanner、ISIC suites utilities、fragroute、nikto	High level Cisco switch、High level Hub

表 4：軟硬體設備

測試方法:

Security Effectiveness：

1) Capable of detecting and blocking OWASP Top ten attacks：
   在左半部的環境裡會安排attacker以及準備各類evasion工具(fragroute/nikto)，在右半部則是準備一victim(至少會準備webgoat)，再依上一年在OWASP列出來的top ten attack進行驗證，以確定DUT能夠正確無誤的辯識及阻擋OWASP top ten的攻擊。
2) Capable of detecting and blocking EVASION attack：
   從attack library中挑出幾樣較常見的attack，確定一般情況下DUT能夠正確辨識並阻擋該攻擊，再配合evasion tool(fragroute)，以進行原本的攻擊，並觀察是否能正確無誤的將attack阻擋下來。
3) Effectiveness of the fragment reassembly mechanism：
   用fragroute進行IP fragment、duplicate及改變封包發出順序，藉此驗證DUT的IP封包的重組能力。
4) Effectiveness of the stream reassembly mechanism：
   用fragroute進行TCP的segment、duplicate封包及改變封包發出順序，藉此驗證DUT的TCP封包的重組能力。
5) URL obfuscation & normalization：
   用nikto進行web scan的evasion測試，該工具使用libwhisker library來產生9種URL的變形，藉此發出變形的http request以嘗試躲過偵測。

Performance:

1. Maximum Capacity：
   驗證不同模式設定下，對於不同條件的TCP/HTTP connections/sec、transactions/sec、packet size、concurrent connection，DUT的detection engine表現上會有什麼樣的表現及影響。
2. Attack detection/blocking – normal load & maximum exceeded load：
   該項測試欲驗證在DUT未達max load及超過max load情況下，是否能夠正常辨識及阻擋各類exploits。
3. HTTP capacity with no transaction delays – real world traffic & with background traffic loads：
   主要目的希望給予DUT的http detect engine相當程度的負荷（藉由把reflector的transaction處理方式

為no delay，試圖給予DUT在處理上的壓力及負荷），再以不同的packet size、connection rate，找出DUT在不同的條件下，detect engine在表現上有什麼樣的差異。

4. HTTP capacity with transaction delays – real world traffic & with background traffic loads：
   與上一項測試類似，主要差異在於reflector端在每次的transaction的處理回應上，會給予10秒的延遲時間，這樣的情境會導致在測試過程中產生大量的open connections，再搭配不同的packet size、connection rate，最後再來觀察DUT在各種的條件辨識及阻擋exploits的表現。
5. Real World application traffic–Threat Vectors Testing, HTTP traffic, Jpeg images, genuine QuickTime movie content and MP3 files with background traffic loads：
   使用avalanche以application mode模擬一般使用者進行http的transaction行為，包含了google/yahoo及一些real world存在的web-based application，另外再搭配smartflow在背景產生固定%的流量及attack library或是exploits來營造出更真實的網路使用情景。最後觀察的指標是avalanche產生各類application的 response time(可能的項目有：TCP Average Time to Open、TCP Average Time to Response Packet、TCP Average Time to Close、Application Average Response Time: HTTP、Application Average Response Time: SMTP、Application Average Response Time: DNS等…)。

Stability & Reliability:

1. Blocking under extended attack for 8 hours：
   想驗證DUT在長時間（8小時）處理大量的流量的過程中，是否會因為loading過重，而導致detect engine誤擋正常的連線或流量。
2. Passing legitimate traffic under extended attack：
   想驗證DUT在長時間（8小時）處理大量的流量的過程中，是否會因為loading過重，而導致detect engine漏擋惡意的連線或流量。
3. Protocol fuzzing/ mutation：
   以各類protocol fuzzing/mutation工具產生多種動態隨機/無法預期的輸出，以考驗DUT的protocol及detect engine的強健及穩定性，並觀察DUT是否會因為接收到無法處理或處理不來的流量，而導致crash、功能失效等問題或是尚未發現的問題。
4. Detect exploits over both IPv6 and IPv4：
   分別在ipv4及ipv6的網路環境，進行各類exploits，以了解原先在ipv4有效的exploit，換到ipv6後，是否還能正常發生效用。
5. Failover test：
   設定好DUT的ha的運作方式後，再藉由產生流量經過DUT的方式，觀察的DUT的ha功能是否正常起動，以了解DUT在A-A情況下，有高loading時，是否能正常將loading分流，或是A-P情況下，適時的達到備援的用途及目的。
6. RealFlow Field Test (Beta Site Test)：
   送至交大Beta Site進行field Test，參與該實驗平台的學生平均有1200 ~ 1500人，對外雙向總流量最高約3 ~ 4Gbps、平均約1~2G，藉由這樣的環境及平台以了解及實驗DUT如果放置到真實環境下可能會遇到的問題。

主動偵測式系統之功能性與相容性

測試項目:

本測試項目中(如表 5、表 6 所示)可分為:功能性測試(Functionality)及相容性測試(Compatibility)兩類。功能性測試主要是測試待測物在不同情境設定下是否可以正確地操作；相容性測試則是測試待測物在不同情境設定下是否能跟 CVS Controller 及 CVS Agent 正確地合作操作。

Functionality：

Item	description
Information Gathering Test	確定CVS Agent是否能正確收集目標主機及服務等相關資料
Known Vulnerabilities Detection	確定CVS Agent是否能正確偵測出已知弱點
Penetration Test	確定 CVS 是否能透過模擬攻擊, 測試已知/未知弱點及相關設定
Analysis Report	確定 CVS 是否能正確回報找到的威脅及風險, 並給予正確的建議及處理方式, 供各被偵測項目參考
Maximum CVS Agent Capacity Under RealFlow Traffic	於真實流量下, 驗證CVS Agent於各區域內能Scan的使用者電腦, Server, Security及Internet Host數量

表 5： Functionality Test

Compatibility：

Item	description
System Stability Under RealFlow Attack	於真實流量下, 驗證CVS Controller及Agent於各區域內接受真實項流量及攻擊時, 系統的穩定性
Detect Exploits Under Realflow Traffic	於真實流量下, 驗證CVS Controller及Agent於各區域內進行各項掃描的準確度

表 6：Compatibility Test

本計畫預計使用 in-line 測試，將各項待測設備佈置於各宿舍網段，用 DUT 對 Beta Site 內使用者的電腦、Beta Site 伺服器及各項不同的網路設備(ex: Firewall)進行掃描，可以了解對各個不同的作業系統、網路應用程式及網路應用服務；同時交大 Beta Site 的使用者會產生真實且大量的背景流量，可供 DUT 進行在具背景流量下之弱點掃描的正確性,透過網路管理人員以及使用者實際的 feedback，了解掃描的準確度。

測試方法

1. DUT Controller

目標：定義評估系統策略以及控制策略，同時也收集來自 DUT Agent 的評估結果與報告；可以對 DUT Agent 利用安全連線進行遠端控制。

Beta Site 區域：適合放置於 Zone 3 中，Zone 3 位置是 Beta Site 核心位置，網路拓樸結構不會有經常性的變更，置於此區域有助於與其它區域 DUT Agent 方便進行溝通及控制。

2. DUT Agent

接收來自 DUT Controller 的評估系統策略，並實際執行針對各區域的評估工作，依進行測試的區域以及對象不同，可以分為三部份：

(1) LAN Security Assessment

目標：針對區域內的所有使用者電腦進行掃描。

Beta Site 區域：適合放置於 Zone 2 中，Zone 2 的位置是宿舍機房，可以將 DUT Agent 連接在宿舍機房端 L2/L3 Switch 上，進行對各個使用者的電腦掃描，放置於此區域可以確保 DUT Agent 端能直接掃描，而不會受到其它安全機制干擾。

(2) Critical Asset Security Assessment

目標：針對區域內提供開放服務伺服器進行掃描。

Beta Site 區域：適合放置於 Zone 3 中，Zone 3 位置在 Beta Site 機房，因具有網路拓樸常態性，原本就適合放置各項伺服器提供 Beta Site 使用者使用，因此將 DUT Agent 放置於本區域，可以直接對各項伺服器進行掃描，而不會受到其它安全機制阻礙。

(3) Perimeter Security Assessment

目標：針對區域週邊(i.e. 防火牆外圍)進行掃描。

Beta Site 區域：適合放置於 Zone 4 中，Zone 4 的位置在 Beta Site 機房，作為 Beta Site 進出口的骨幹線路，主要提供 IPS/IDP 或 Firewall 等 Security Appliance 設備進行測試，放置於此區域可以針對 IDS/IPS、Firewall 等設備及 Internet 上 host 進行掃描。

五、 結果與討論

本計劃自執行開始，迄今已獲得多項成果：建置一適用WAF、IPS及P2P Control的實地與重播測試環境與機制、設計開發蒐集網站攻擊相關流量的誘捕機制、實際蒐集各種真實網站攻擊相關流量、萃取重組出真正相關的各session真實網站攻擊相關流量、發表一篇國際期刊論文(*IEEE Transactions on Computers*[21])、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備(如合勤科技、威播科技、利基網路等)進行合作執行資安產品測試案；在追求相關測試技術研究發展外，也協助國內相關廠商進行各種資安產品測試與除錯。

網路持續發展，各種擁有複雜網路行為的網路應用程式層出不窮、使用者使用網通產品的情境與各種網站攻擊流量行為途徑也日趨複雜及難以預料，光靠實驗室測試及人造流量來進行測試是不夠的，此特性在高階資安產品的測試上尤為顯著。期望透過此項計畫的執行成果，能對國內相關產業界提供另一產品測試機制，並正視真實流量在未來高階資安產品測試的重要性。

國科會補助計畫衍生研發成果推廣資料表

日期:2011/10/31

國科會補助計畫	計畫名稱: 子計畫二:資安技術網站應用防火牆、攻擊防禦與點對點應用控制之真實流量評比(資訊安全技術)
	計畫主持人: 邵家健
	計畫編號: 99-2218-E-009-015- 學門領域: 資訊

無研發成果推廣資料

99 年度專題研究計畫研究成果彙整表

計畫主持人：邵家健	計畫編號：99-2218-E-009-015-
計畫名稱：資安技術真實流量實地評比--子計畫二:資安技術網站應用防火牆、攻擊防禦與點對點應用控制之真實流量評比(資訊安全技術)	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	4	4	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	1	1	100%	篇	發表一篇國際期刊論文（IEEE Transactions on Computers）
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	無

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

共一篇國際期刊論文，發表在 IEEE Transactions on Computers。

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

本計劃目的在於建置一資安技術偵測防禦系統之測試平台與測試評比「網路應用程式防火牆(WAF)」、「入侵防禦系統(IPS)」及「點對點應用控制(Peer-to-Peer Control)」三項資安偵防技術所需要的工具與機制；透過結合流量錄製、流量萃取、資訊重組、資訊詢問及流量重播等技術，重播真實網路流量來找出任何潛在的資安威脅或是已發展的資安偵防技術之不足之處。

本計劃自執行開始，迄今已獲得多項成果：建置一適用 WAF、IPS 及 P2P Control 的實地與重播測試環境與機制、設計開發蒐集網站攻擊相關流量的誘捕機制、實際蒐集各種真實網站攻擊相關流量、萃取重組出真正相關的各 session 真實網站攻擊相關流量、發表一篇國際期刊論文(IEEE Transactions on Computers)、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備(如合勤科技、威播科技、利基網路等)進行合作執行資安產品測試案；在追求相關測試技術研究發展外，也協助國內相關廠商進行各種資安產品測試與除錯。

網路持續發展，各種擁有複雜網路行為的網路應用程式層出不窮、使用者使用網通產品的情境與各種網站攻擊流量行為途徑也日趨複雜及難以預料，光靠實驗室測試及人造流量來進行測試是不夠的，此特性在高階資安產品的測試上尤為顯著。期望透過此項計畫的執行成果，能對國內相關產業界提供另一產品測試機制，並正視真實流量在未來高階資安產品測試的重要性。