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--總計畫
研究成果報告(精簡版)

計 畫 類 別 ： 整合型
計 畫 編 號 ： NSC 99-2218-E-009-013-
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 ： 林寶樹
共 同 主 持 人 ： 林盈達、邵家健、陳昌盛
計畫參與人員： 碩士級-專任助理人員：呂俊男
碩士班研究生-兼任助理人員：余尚哲
碩士班研究生-兼任助理人員：江易達
大專生-兼任助理人員：王媛如
博士後研究：洪瑞村

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 11 月 01 日

中文摘要：　資安技術於使用者環境(Beta Site)進行測試以降低「顧客端發現問題(CFD)」的數量，是其產品化上市銷售之前測試流程中重要的一環，現今多樣化的網路環境與複雜化的產品設計使得實驗室測試(Lab Test)愈來愈難模擬出真實世界的網路環境來刺激(Stimulate)出產品的問題，這也讓 Beta Site 的測試更顯得重要。

此整合型計畫的目標在於提供資安技術一個良好的真實流量測試平台(RealFlow Test Platform)以降低顧客端發現問題的數量及評估誤擋漏擋率(False Positive/False Negative)，其中除了要建置實地測試(Field Test)所需要的 Beta Site 環境之外，同時也會發展重播測試(Replay Test)所需要的工具如錄製(capture)、重播(replay)、分類(classification)以及萃取(extraction)，我們將真實流量測試平台分為通用(Generic)以及特定(Specific)兩種範疇的發展方案(solutions)，通用方案(Generic solutions)是要提供基礎共通的環境與工具給所有類型的資安技術使用，其著眼點在於廣度，而特定方案(Specific solutions)是要提供給特定的、目前迫切需要的資安技術更完整深入的環境與工具，其著眼點在於深度，而這些特定迫切需要的資安技術包括了網頁應用程式防火牆(WAF)、反惡意軟體(Anti-Malware)、反殭屍網路(Anti-Botnet)、入侵防禦系統(IPS)、點對點應用控制(P2P Control)。

總計畫目標在於建置一個有別於傳統的 Beta Site，對於資安技術開發者可以更方便地進行測試與除錯，同時對於網路使用者也能兼顧其網路使用品質，為了滿足產品開發者的需求預計要建置多「類型測試區域」、「遠端控制」、「流量分級」、「流量剖析」等環境與機制；為了滿足網路使用者的需求預計要建置「網路故障自動偵測、通報與復原機制」，除此之外對於召募 Beta Site 參加者的方式是以「募兵制」而非強制。預期在一年內可以設計與建置出六種不同的測試區域以提供各類型的資安產品進行實地測試，發表 Beta Site 架構設計相關之專利與論文，同時將執行至少上三件以上的資安產品測試案。

英文摘要：　Testing on the Beta Site is important for security technologies to reduce the Customer Found Defects (CFDs). Now, it is paid much more attention since the security technologies themselves and the network environment are getting more complicated and diversified. Compared with testing on Beta Site, Lab Test can only stimulate and reproduce a small part of the CFDs.

The goal of this integrated project is to provide security technologies with a RealFlow Test Platform to improve the quality, to reduce the number of CFDs and to evaluate False Positive/False Negative rates. This platform consists of environment and tools for Field Test and Replay Test, respectively. The environment for Field Test is actually the Beta Site, and the tools required by Replay Test are capture, replay, classification, and extraction. We develop the

RealFlow Test Platform with two kinds of solutions, one is Generic and the other is Specific. Generic solutions cover the fundamental and common facilities for all kinds of security technologies while Specific solutions take care of the needs of particular security technologies such as WAF, Anti-Malware, Anti-Botnet, IPS, and P2P Control.

The goal of the grand project is to establish a new type of Beta Site. For developers of security technologies, it is easy to do the test and debugging. For the network users, the network quality can remain as usual. We plan to develop several mechanisms on the Beta Site such as ’various test zones’, ’remote control’, ’degrees of traffic volume’, ’traffic profiling’, ’auto detection, notification, and recovery’, and ’voluntarism’. In a year, six different kinds of testing zones, the related patents and papers about Beta Sites, and at least three testing cases should be executed and completed.

一、前言

資安技術於開發的過程中會經歷一系列不同階段的測試[1]，在通過層層關卡的驗證後才有辦法產品化上市銷售。在這一系列的測試裡，除了在實驗室測試(Lab Test)進行以功能性為主的測試之外，也會將產品放在日常運作中的網路上讓一般使用者進行使用，透過一般使用者的使用來挖掘出產品在實際使用上會出現的問題，進而減少產品在銷售後才被顧客發現的問題(Customer Found Defect; CFD)[2]，對於這樣用來測試產品的日常運作網路就是所謂的 Beta Site，而透過 Beta Site 進行測試我們稱之為 Beta Site Test 或是 Field Test，即是「實地測試」。

資安技術只靠 Lab Test 是不夠的，因為 Lab Test 難以模擬出真實世界多樣化及複雜的網路環境來刺激(Stimulate)出產品的問題；以 Application layer 來說，P2P applications、Video Streaming、On-line Gaming 日漸盛行，由於這些應用程式的種類繁多、多數 Server 未公開、多數協定為 proprietary 等原因造成在 Lab Test 時無法使用 PC(數量要很多或者需要安裝 Server)或專門的 Traffic Generator(需要知道協定)來建置出完整的 testbed；以 Network and Transport layer 來說，由於使用者所使用的 OS 差異度增大、IPv6 的使用以及眾多不同的設定等原因造成了 TCP/IP 協定行為更加多樣化；以 Data-Link layer 來說，存在著各式各樣不同廠牌的網路卡以及各式各樣的協定 (ex. Fast/Gigabit/10G Ethernet, 802.11 a/b/g/n WLAN, 3G, WiMAX)，造成了 Data-Link layer 的協定行為十分的多樣化。然而以一個完整的網路封包傳遞過程來看，實際的情況會是上述三種層面的結合，其交互影響的結果必定會加深其複雜性與多樣性，從 test coverage[3, 4]的角度來思考我們必須製造出相當的 test cases (i.e. input or stimulus)讓程式碼中各種的 statements, branches, paths 盡可能地都被執行過才能更完整地找出產品問題點，因此我們必須透過 Field Test 來彌補 Lab Test 所無法製造出來 test cases 的缺口，而這個缺口如上述正日益擴大中。

以真實流量來進行測試的方式除了實地測試以外還可以利用重播測試(Replay Test)的方式。所謂的真實流量重播測試就是先將真實流量錄製(capture)[12, 13, 14]下來成為檔案(一般稱之為 trace files)，後續便可將錄製好的 trace files 以重播(replay)[15, 16, 17, 18, 19, 20]的方式來測試資安技術；重播測試的好處在於可結合 Field Test 與 Lab Test 的優點，一方面可以使用真實網路流量進行測試，另一方面可以快速地重製出問題，同時也可以藉由調整流量播放的速度來測試不同等級的待測物，我們將實地測試與重播測試統稱為「真實流量測試(RealFlow Test)」。對於實地測試來說需要的是一個 Beta Site 環境，而對於重播測試來說所需要的是工具，如: capture, replay, classification 以及 extraction。

二、研究目的

整體計畫(總計畫+三子計畫)目的在於提供資安技術一個良好的真實流量測試平台(RealFlow Test Platform)以降低 CFD(Customer Found Defect)發生的機率及評估誤擋漏擋率(False Positive/False Negative)，其中包括實地測試所需要的環境與重播測試所需要的工具，我們將真實流量測試平台分為通用(Generic)以及特定(Specific)兩種範疇的發展方案(solutions)，分別如表 1、表 2 所列。Generic solutions(表 1)是要提供基礎共通的環境與工具給所有類型的資安技術使用，其著眼點在於廣度；而 Specific solutions (表 2)是要提供給特定的、目前迫切需要的資安技術更完整深入的環境與工具，其著眼點在於深度，而這些特定迫切需要的資安技術如網站應用防火牆(WAF)、入侵防禦系統(IPS)、點對點控制(P2P Control)、反惡意軟體(Anti-Malware)、反僵屍網路(Anti-Botnet)。

Generic solutions

所需之環境或工具	規格需求
Beta Site 環境	Variety of Systems Under Test、Remote Control、Degrees of Traffic Volume、Traffic Profiling、Auto Failure Detection, Notification, and Recovery、Voluntaryism
Capture 工具	高速流量下之錄製、儲存空間之節省、Data anonymization
Replay 工具	高速重播、Stateful replay、Wireless Replay
Classification 工具	by Good or Bad、by Applications (ex. game、P2P、streaming)
Extraction 工具	session association

表 1：通用方案的規格需求

Specific solutions

資安技術 / 環境或工具	WAF	IPS	P2P Management	Anti-Botnet	Anti-Malware
Beta Site 環境	Web applications 要夠多、Web 應用流量要夠大	流量要夠大	P2P 流量要夠大、種類要夠多	Honeynet	軟體與硬體
Capture 工具	Web 應用相關流量		長時間	多點	
Replay 工具	Stateful	Stateful	Stateful	Stateful	Stateful
Classification 工具	Signature	Signature	Behavior	Behavior	Signature
Extraction 工具	HTTP header	Payload Similarity	連線量多、port locality	關聯性低	

表 2：特定方案的規格需求

總計畫的目的在發展 Generic solutions—建置資安技術之基礎共通實地測試環境，建置一個有別於傳統的 Beta Site，對於資安技術開發者可以更方便地進行測試與除錯，同時對於網路使用者也能兼顧其網路使用品質，為了滿足產品開發者的需求預計要建置多「類型測試區域」、「遠

端控制」、「流量分級」、「流量剖析」等環境與機制；為了滿足網路使用者的需求預計要建置「網路故障自動偵測、通報與復原機制」，除此之外對於召募 Beta Site 參加者的方式是以「募兵制」而非強制，表 3 是各計畫分工方式。總計畫主要是建置共通實地測試環境、子計畫一主要是設計開發共通重播測試工具、子計畫二則是針對網站應用防火牆、攻擊防禦與點對點應用控制資安技術的測試、子計畫三則是針對反惡意軟體及反殭屍網路資安技術的測試。

	發展方案範疇	主要工作內容
總計畫	Generic solutions	建置資安技術之基礎共通實地測試環境 (i.e. Beta Site 環境)
子計畫一	Generic solutions	開發資安技術之基礎共通重播測試工具 (i.e. capture, replay, classification, extraction)
子計畫二	Specific solutions	資安技術網站應用防火牆、攻擊防禦與點對點應用控制之實地測試環境與重播測試工具
子計畫三	Specific solutions	資安技術反惡意軟體與反僵屍網路之實地測試環境與重播測試工具

表 3：各計畫分工方式

三、 文獻探討

[1] Dann Gustavson, “Design verification and production test: use them as tools for faster development,” in *Proceedings of Wescon Conference*, November 1997.

[2] Mauricio J. Ordonez and Hisham M. Haddad, “The State of Metrics in Software Industry,” in *Proceedings of Information Technology: New Generation (ITNG)*, pp. 453-458, April 2008.

[3] H. Zhu, P. A. V. Hall, and J. H. R. May, “Software unit test coverage and adequacy,” *ACM Comput. Surv.*, 29(4):366–427, 1997.

[4] YK Malaiya, MN Li, JM Bieman, R Karcich, “Software Reliability Growth With Test Coverage,” *IEEE Transactions On Reliability*, vol. 51, no. 4, December 2002.

[5] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar, “An integrated experimental environment for distributed systems and networks,” in *Proc. Symposium on Operating Systems Design and Implementation*, pp. 255–270, December 2002.

[6] T. Benzel, R. Braden, D. Kim, et al. “Design, deployment, and use of the DETER testbed,” in *Proceedings of the DETER Community Workshop on Cyber-Security and Test*, Aug 2007.

[7] Toshiyuki Miyachi, Ken-ichi Chinen, and Yoichi Shinoda, "Automatic configuration and execution of Internet experiments on an actual node-based testbed," in *Proceedings of Testbeds and Research Infrastructures for the Development of Networks and Communities (Trident)*, pp. 274-282, Feb. 2005.

[8] Junya NAKATA, Satoshi Uda, and Toshiyuki Miyachi, "StarBED2: Large-scale, Realistic and Real-time

Testbed for Ubiquitous Networks," in *Proceedings of Testbeds and Research Infrastructures for the Development of Networks and Communities (Trident)*, pp. 1-7, May 2007.

[9] Andy Bavier , Nick Feamster , Mark Huang , Larry Peterson , Jennifer Rexford, "VINI veritas: realistic and controlled network experimentation," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, September 11-15, 2006, Pisa, Italy.

[10] Kashi Venkatesh Vishwanath , Amin Vahdat, "Realistic and responsive network traffic generation," in *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, September 11-15, 2006, Pisa, Italy.

[11] Spyros Antonatos , Kostas G. Anagnostakis , Evangelos P. Markatos, "Generating realistic workloads for network intrusion detection systems," in *Proceedings of the 4th international workshop on Software and performance*, January 14-16, 2004, Redwood Shores, California.

[12] Tcpdump, http://www.tcpdump.org/.

[13] F. Schneider, J. Wallerich, A Feldmann, "Packet Capture in 10-Gigabit Ethernet Environments Using Contemporary Commodity Hardware," in *Passive and Active Measurement Conference*, April 2007.

[14] S. Kornexl, V. Paxson, H. Dreger, A. Feldmann and R. Sommer, "Building a Time Machine for Efficient Recording and Retrieval of High-Volume Network Traffic," in *Proceedings of ACM Internet Measurement Conference*, October 2005.

[15] A. Turner, Tcpreplay, http://tcpreplay.synfin.net/trac/.

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

[17] Traffic IQ Professional: http://www.karalon.com/.

[18] Nick Weaver Weidong Cui, Vern Paxson and Randy H. Katz. "Protocol-Independent Adaptive Replay of Application Dialog," in *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, Feb 2006.

[19] James Newsome, David Brumley, Jason Franklin, Dawn Song, "Replayer: automatic protocol replay by binary analysis," in *Proceedings of the 13th ACM conference on Computer and communications security*, October 30-November 03, 2006, Alexandria, Virginia, USA.

[20] Y.-C. Cheng, U. Holzle, N. Cardwell, S. Savage, and G. Voelker, "Monkey see, monkey do: A tool for tcp tracing and replaying," in *Proceedings of the 2004 USENIX Annual Technical Conference*, June 2004.

[21] CAIDA: The Cooperative Association for Internet Data Analysis, http://www.caida.org/.

[22] PMA: Passive Measurement and Analysis, http://pma.nlanr.net/

[23] Ying-Dar Lin, I-Wei Chen, Po-Ching Lin, Chang-Sheng Chen, Chun-Hung Hsu, "On Campus Beta Site: Architecture Design, Operational Experience, and Top Product Defects," in *IEEE Communications Magazine*, Vol. 48, Issue 12, December 2010.

[24] Ying-Dar Lin, Shun-Lee Chang, Jui-Hung Yeh, Shau-Yu Cheng, "Indoor Deployment of IEEE 802.11s Mesh Networks: Lessons and Guidelines," in *Ad Hoc Networks*, May 2011.

[25] Chia-Yu Ku, Ying-Dar Lin, Shiao-Li Tsao, Yuan-Cheng Lai, "Utilizing Multiple Channels with Fewer Radios in Wireless Mesh Networks," in *IEEE Transactions on Vehicular Technology*, Vol. 60, No. 4, pp.

594-601, April 2011.

[26] Ying-Dar Lin, Chi-Heng Chou, Yuan-Cheng Lai, Tze-Yau Huang, Simon Chung, Jui-Tsun Hung, Frank C. Lin, “Test Coverage Optimization for Large Code Problems,” in *Journal of Systems and Software*, in Press, Corrected Proof, May 2011.

[27] Ying-Dar, Ren-Hung Hwang, Fred Baker, “Computer Networks: An Open Source Approach,” *McGraw-Hill*, February 2011.

四、研究方法

待測物類型 (Variety of SUT)

圖 1 為 Beta Site 的網路拓撲示意圖，共分成六個測試區，終端使用者即是在 Zone 1；在 Zone 1 可以進行軟體的測試如 Anti-Virus、Malware Detection—將要測試的軟體安裝在使用者的電腦上，使用者端具有各式各樣的應用軟體與作業系統，可以測試出 SUT(System Under Test)運作過程中是否有跟任何應用軟體或作業系統 Compatibility 問題；在 Zone 2 可以進行 Ethernet Switch 及 Access Point 的測試—使用者端使用各種廠牌的 Adapter，可以測試出是否有與 SUT 發生 Interoperability 問題；在 Zone 3 可以進行 Core Router 的 Stability 測試；在 Zone 4 可以進行 transparent mode (one-in-one-out)的網路安全產品測試如 Firewall、UTM、IPS、Bandwidth Management 等，可以測試其功能面(Functionality)、效能面(Performance)及穩定性(Stability)；在 Zone 5 可以進行 sniff mode 的產品測試如網路鑑識產品(Network Forensics)，可以測試 Performance 與 Stability；在 Zone 6 是以流量錄製/重播的方式來測試產品，可以進行 Residential Gateway 的 Stability 測試，我們所使用的流量重播工具包括 tcpreplay、tomahawk、avalanche、Traffic IQ 以及 NBL 自行開發的工具，之所以用不同的 replay 工具測試是要彌補各自不足的部份。總共可以測試十幾種不同類型的網通產品。

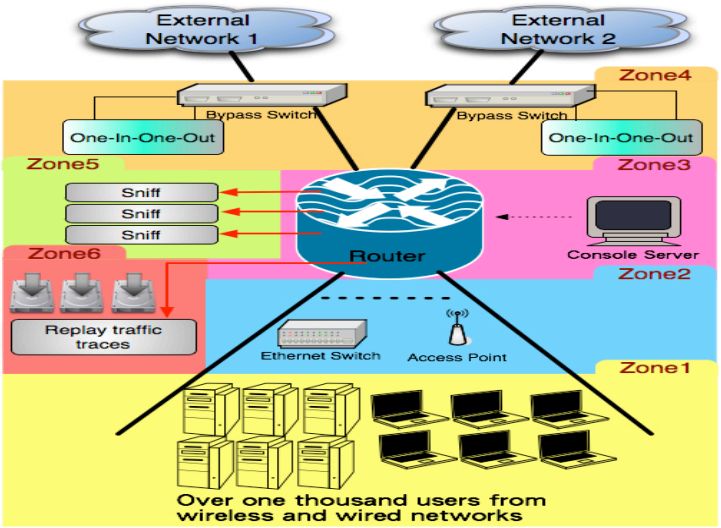

圖 1：Beta Site 架構

遠端控制及遠端電源 (Remote Control and Remote Power)

進行測試的過程中，研發人員可以透過 Internet access 方式，從 network port(ex. Ethernet)連進(ex. Telnet, SSH)待測物觀察；然而一方面透過 network port 所能觀察的除錯訊息有限，另一方面是當 SUT 出狀況時 network port 有可能會失靈導致無法收集訊息；因此 Beta Site 提供 *Remote Console* 機制—讓研發人員在遠端可以從 SUT 的 console port(ex. RS-232)連進 SUT。除此之外，在測試或除錯過程中，如果遇到 SUT 因為當機而一定要重啟電源才能恢復運作時，Beta Site 還提供 *Remote Power* 讓研發人員可以遠端重啟 SUT 的電源。

流量分級 (Degrees of Traffic Volume)

我們在 Zone3 增加一台 router(請參考圖 2)，並且在其下游的 switch 中以 VLAN 的方式選擇性地將部份 downstream ports of switch 的流量導入此新增加的 router 裡，流量被導入 auxiliary router 後會再經由 original router 送往 external networks。在這樣的架構中，auxiliary router 與 original router 之間的那條 link 的流量大小便可以輕易地被調節，該 link 可以擴充成為 Zone 4 的測試範圍；這樣一來，在 Zone 5 裡可以使用流量過濾的方式來調節進入 SUT 的流量大小，而且在 Zone 6 的流量重播測試中，replay 流量的工具可以因此設定播放流量時的速度。

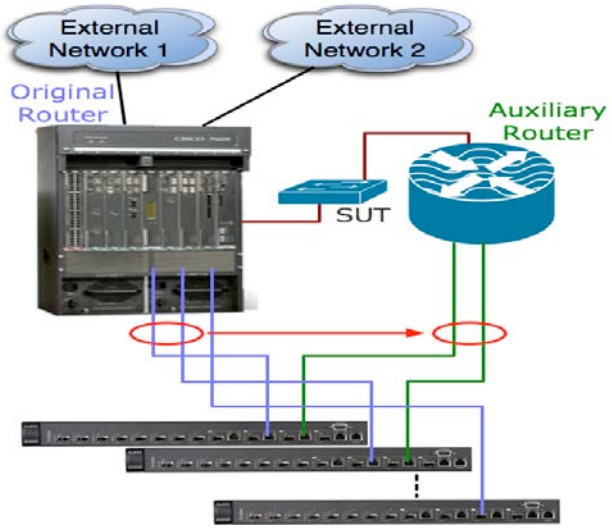

圖 2：SUT 流量分流機制

流量剖析 (Traffic Profiling)

為了獲得流量內容特性的有關訊息，Beta Site 使用各種不同的軟硬體工具，嘗試從各種不同的層面剖析流量內容；*MRTG* 可以提供某一 link 在某一時間點上的進或出的流量大小統計，可以了解網路使用量的高峰與離峰流量各為多少、各是何時；*NTOP* 可以依封包不同欄位資料分析出網路流量中的

種種分佈比例，其中包括 Layer 3& 4 protocols、封包大小、transmission types、TCP/UDP port numbers 等，而有些套件可以根據應用層(application layer)資料進行分析，進而知道各種應用程式(ex. P2P file sharing, gaming, VoIP, video streaming, Web, email, FTP, etc.)在網路流量中所占的比例，這類型的套件包括 *L7-filter*, *IPP2P*, *Ourmon*, *Panabit* 等等。

志願參與者 (Volunteers)

為了讓同學願意加入 Beta Site 參與測試，我們必須要提供鼓勵誘因來吸引，並且要能保障參加者產生的網路流量的隱私性，以及要能自動地將參加者的流量導入 Beta Site 以避免手動接線過程造成參加者正常使用上的不便。其中鼓勵誘因包括更先進或更快速的網路環境—如 Gigabits Ethernet、802.11 n WLAN 以及 Security Protection、更寬鬆的管理政策—如在 P2P 應用的限流政策中給予較大的頻寬及較少的使用限制，以及更完善網路服務團隊協助使用者解決日常電腦網路使用上所遇到的問題。而為了保障參加者網路流量的隱私性，對於所有參加測試的廠商人員都必須簽署 NDA(Non-Disclosure Agreement)；對於將網路流量自動地導入到 Beta Site，我們採取 port-based VLAN 的作法(如圖 3)—在參加者電腦所連接的 L2 switch 上將其所連接的 switch port 設定成對應到往 Beta Site 路徑的 VLAN id，那麼該台電腦所產生的流量在進入 L2 switch 後即會被 tag 上 VLAN id，等流量到 L3 Switch 後，L3 Switch 即可根據 VLAN id 作判斷，自動將流量傳向 Beta Site。

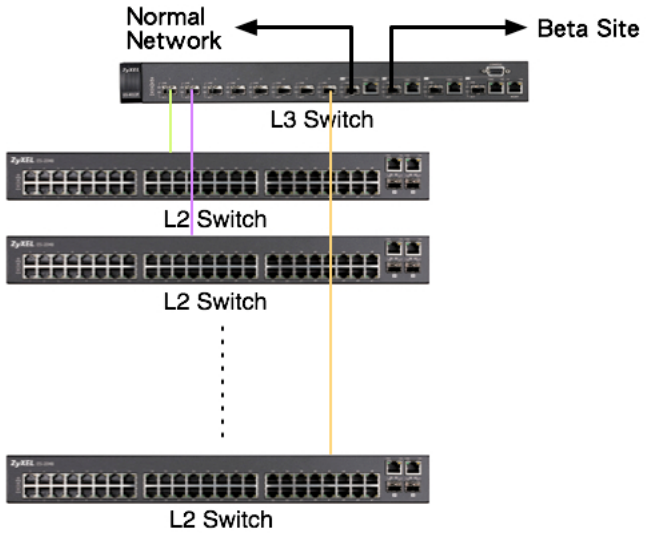

圖 3：用 VLANs 隔開 Beta Site 與一般網路

自動錯誤偵測、回報及恢復 (Auto Failure Detection, Notification, and Recovery)

當產品在測試過程中因為錯誤而造成網路不能正常提供連線時，我們希望可以愈快知道愈好，這樣才能愈快地解決問題進而維持網路正常使用的品質，圖 4 即是圖 1 中的 Zone 4；在 Zone 4 中我們使用 Bypass Switch 來達到此目的—Bypass Switch 的 Network Ports A 跟 B 分別接上 Internal Network

及 External Network，其 Monitor Ports 1 跟 2 分別接上 SUT 的兩端。當 SUT 正常運作時 Bypass Switch 是以 Normal Mode 運作，此時流量由內往外的路徑是 Internal Network -> Port B -> Port 1 -> SUT -> Port 2 -> Port A -> External Network；然而一旦 SUT 出了問題被 Bypass Switch 偵測到時，Bypass Switch 就會自動以 Bypass Mode 運作，流量由內往外的路徑是 Internal Network -> Port B -> Port A -> External Network，此刻即是『bypass』了 SUT，而在『bypass』SUT 的同時，Bypass Switch 會主動發出 email 通知 Beta Site 系統管理者。

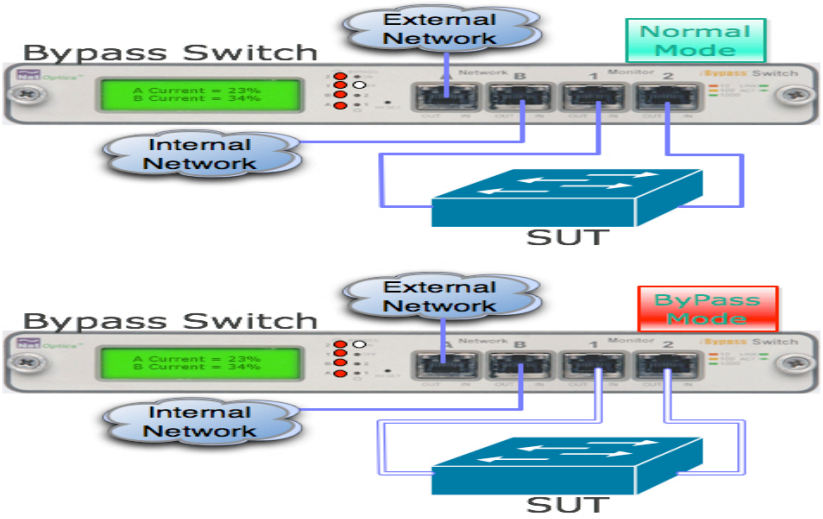

圖 4：Bypass Switch 模式: Normal mode vs. Bypass mode

Bypass Switch 會周期性地(a configurable timer)送出『heartbeat 封包』來檢查 SUT 是否能 forward heartbeat 封包讓它回到 Bypass Switch 上；若該 heartbeat 封包沒有回到 Bypass Switch 上，而且發生這種情況的連續次數已超過一定門檻(a counter is configurable)時，Bypass Switch 就會啟動 bypass 功能。除此之外，在 Zone 1 中我們安置了一些 PC 並且在這些 PC 上面安裝了我們自行撰寫的測試程式，這些測試程式會模擬常見的使用者網路使用行為，例如瀏覽知名網站、透過 P2P 應用程式上傳/下載檔案、觀看網路電視等等，我們將這些 PC 稱作 Beta Clients。Beta Clients 在進行網路使用的同時也會檢查使用時的狀況如是否可以使用該應該與使用時的 delay 情況，定期且主動地以 email 的方式寄出使用情況報告給 Beta Site 系統管理者。

五、 結果與討論

本計劃自執行開始，迄今已得到多項成果：建立一真實流量測試平台–BetaSite、建立六大類型測試區、設計測試分析回報機制、發表四篇國際期刊論文(包含*IEEE Communication Magazine*[23]、*Ad Hoc Networks*[24]、*IEEE Transactions on Vehicular Technology*[25]及*Journal of Systems and Software*[26]等)、學術專書章節[27]、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備廠商(如威播科技、喬鼎資訊)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網通產品測試與除錯。

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網通產品的測試是不夠的，此特性在高階網路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網通產品測試的重要性。

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: 總計畫
	計畫主持人: 林寶樹
	計畫編號: 99-2218-E-009-013- 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：林寶樹	計畫編號：99-2218-E-009-013-
計畫名稱：資安技術真實流量實地評比--總計畫	

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	2	2	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	1	1	100%		
國外	論文著作	期刊論文	5	5	100%	篇	發表四篇國際期刊論文(包含 IEEE Communication Magazine、Ad Hoc Networks、IEEE Transactions on Vehicular Technology 及 Journal of Systems and Software 等)
		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)

共四篇國際期刊論文，各刊登在 IEEE Communications Magazine、JSS、Ad Hoc Networks、IEEE TVT。

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）

此計畫目標在於建置一個有別於傳統的網通設備實地測試(Field Test)環境-BetaSite，提供基礎共通的網通設備測試環境與工具給所有類型的資安技術使用；對於技術或產品開發者可以更方便地進行測試與除錯，同時也能兼顧測試網路之運作品質。為了滿足開發者的需求，建置了「六大類型測試區」、「遠端電源及遠端控制」、「依待測物特性分級測試流量」、「流量內容剖析」等環境與機制；為了滿足網路使用者的需求，建立了「網路故障自動偵測、通報與復原機制」以確保測試網路不致因為待測物故障而中斷運作；為了真實網路流量來源擴大更新，以「募兵制」方式持續召募更多志願者加入 BetaSite 測試網路。

本計劃自執行開始，迄今已得到多項成果：建立一真實流量測試平台－BetaSite、建立六大類型測試區、設計測試分析回報機制、發表四篇國際期刊論文(包含 IEEE Communication Magazine、Ad Hoc Networks、IEEE Transactions on Vehicular Technology 及 Journal of Systems and Software 等)、產出研究報告、培育碩博士學生持續進行相關研究與訓練，並與網通資安設備廠商(如威播科技、喬鼎資訊)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網通產品測試與除錯。

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網通產品的測試是不夠的，此特性在高階網路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網通產品測試的重要性。