# 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--子計畫一:資安技術真實流量重播評比
## 研究成果報告(精簡版)

計 畫 類 別 ： 整合型
計 畫 編 號 ： NSC 99-2218-E-009-014-
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
計畫參與人員： 碩士班研究生-兼任助理人員：鄭融懋
碩士班研究生-兼任助理人員：彭炳衡
碩士班研究生-兼任助理人員：紀琇儀
大專生-兼任助理人員：陳玠竹
大專生-兼任助理人員：游本永
大專生-兼任助理人員：吳宗瑋

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：　重播測試是將真實網路流量錄製成為檔案(traces)後再加以重播出來對待測物進行測試，它的好處在於綜合(combine)實地測試與實驗室測試的優點，一方面有實地測試的真實性另一方面又有實驗室測試的可控制性，可讓真實流量下所發生的問題更快速地重製便利開發者解決問題。

本計畫的目的在於提供資安技術一組通用(Generic)的重播測試工具，其中包括了流量錄製、流量重播、流量分類以及流量萃取，透過這些工具來進行重播測試除了可以快速地重製出真實環境下的問題之外，同時亦可找出造成待測物出問題的流量提供給開發者進一步地分析與除錯，這些工具除了可以獨立使用之外，我們打算整合這些工具發展出一套應用系統「PCAP Library」，其最主要的功用在於測試資安技術誤判跟漏判的問題並提供可能造成誤判及漏判的 traces 給開發者分析，進而提高資安技術的辨識準確度。

PCAP Library 系統架構中包括了五大元件，這五大元件分別是流量錄製、流量分類與萃取、資訊重組、詢問以及流量重播，流量錄製時要避免封包遺失(packet loss)及存儲空間效率低落，流量分類與萃取時要將錯誤的機率壓低，資訊重組時要注意資訊尋找與更新，詢問時要兼顧效能及正確性，流量重播時必須讓流量的狀態(stateful)盡可能的重現。預期在一年內可以發展出與重播測試相關三種類型的 Generic 技術其中包括重播、萃取及分類，發表流量重播相關專利與論文如: low-storage capture and loss-recovery selective replay、proxy replay、replay ineffectiveness factors analysis、techniques for PCAP library、classification state machines、PCAP Lib 1.0: overview and case studies，研發 socket replay 與 proxy replay 兩套重播工具及 PCAP Library 應用系統，同時將執行至少上三件以上的資安產品測試案。

英文摘要：　’ Replay Test’ first captures network traffic into a file, called ’trace’, and then replays the trace to stimulate defects of System Under Test (SUT). It combines the advantages of reality and controllability in the Field Test and Lab Test, respectively. Defects found by ’Replay Test’ can be reproduced more easily than those found by ’Field Test’ since what we need to do to reproduce them is just replaying the trace again.

The objective of this project is to provide security technologies with a generic tool set for Replay Test. This tool set contains Capture, Replay, Classification, and Extraction. They can be used to reproduce real-world defects more efficiently than Field Test. Besides, the traffic which causes defects can also be searched out and offered to developers for further analysis and debugging. Each of these tools can be solo exercised, but what we want to do is to integrate all of them to become a very useful system, named ’PCAP

Library'. The main function of PCAP Library is to stimulate false-positive and false-negative problems in the security technologies. The traffic which causes false-positive and false-negative problems can be supplied for developers to analyze and increase the accuracy of security technologies.

There are five components in the PCAP Library, which are traffic capturing, traffic classification and extraction, information reorganization, querying, and traffic replaying. Some issues exist and need to be paid attention. For examples, traffic capturing should avoid packet loss and inefficient utilization of storage, traffic classification and extraction require high accuracy, information reorganization concerns lookup and update, querying needs to consider both performance and accuracy, traffic replaying has to be careful about the state of flows. This project aims to develop three kinds of security technologies and to propose related patents and papers, including low-storage capture and loss-recovery selective replay, proxy replay, replay ineffectiveness factors analysis, techniques for PCAP library, classification state machines, PCAP Lib 1.0 and to execute at least three testing cases.

# 一、 前言

重播測試(Replay Test)的技術核心是希望結合 Lab Test 與 Field Test 的兩項優點，更快速地重製真實環境下所遇到的問題，同時創造更好的測試範圍與更精確的尋找發生事件的原因；而實地測試(Field Test)是將待測物放到 Beta Site 上進行測試，如果產品發生問題無法繼續服務時，則可以利用自動通報機制通知網路管理員，以通知產品開發者儘速觀察待測物；而 Lab Test 則是在實驗室的環境下產生流量，看網路產品是否有按照規格上的設定執行，或進行壓力測試觀察待測物的極限值，如果在測試過程中發現有異狀，可以使用同樣的設定再重播一遍流量就可以重製發生的問題，以方便產品的開發者釐清問題。

但 Lab Test 中測試範圍則無法像 Field Test 中以大量真實使用者、多元網路程式、複雜的網路行為來測試產品，也無法產生比 Field Test 更接近使用者的行為；Field Test 則是無法像 Lab Test 可以很快速的從已知的設定中重置網路流量以便更仔細觀察待測物的狀態與反應；Replay Test 的作法則是用 Field Test 中所經過的流量經由 Switch Mirror 一份錄製下來後(如圖 1)，再用 Lab Test 的環境再造真實網路流量(如圖 2)，讓測試的網路流量不但可以包羅萬象、更接近使用者的行為、也可以加速釐清問題的產生讓網路產品能更快的提升品質。

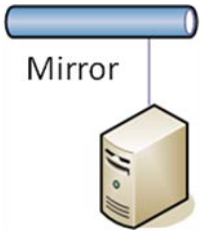



圖 1：Traffic Mirror Mode

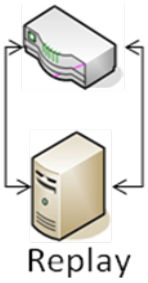



圖 2：Traffic Replay

Replay Test 的第一步是要將網路流量分邊，這是為了模擬真實流量中一進一出網路介面的網路行為，但最重要的是第二步，重播出來的流量要讓待測物看起來就像在 Field Test 環境所產生一樣真實，若只是將錄製的流量原封不動的播出去有可能會不符合網路規約以致於待測物不會建立 session table 去處理該流量，導致失去測試的意義。因此在流量重播的過程中，除了將流量推出網路之外，也必須去聽取另外一端經過待測物後的流量，觀察此流量有沒有經過什麼改變，以便重播下一個符合網路規約的封包。

「流量重播測試」的技術分為兩大項來評估，第一個是「順序的正確性」，另一個是「資料的準確性」。「順序」代表著流量必須等到另外一端收到後才將下一個封包推出，而不是單純的依照當初錄製的時間為準，這是因為每個待測物處理封包的時間可能都不同。而「正確性」則是強調若封包經過待測物修改或重播時因為特別需求使得我們修改要重播的流量時，是否仍然符合網路規約，讓待測物看起來這不是造假的流量而像是真的使用者在使用待測物的服務流量。而「資料的準確性」關鍵在於

傳輸層(ex: TCP、UDP)與應用層(ex: FTP、HTTP)是否仍能符合網路規約的規定。以傳輸層的 TCP 為例，當遇到 NAT 修改了 IP、Proxy 改變了 sequence number、IPS(Intrusion Prevention System)可能阻擋了部分封包時，必須在重播機制上有相對應的處理才能確保接下來的重播對待測物來說是有效的。以應用層的 FTP 為例，Control connection 會在 payload 中會告訴另外一端使用者下一條 data connection 要建立 TCP 連線必須連到哪一個 IP address 和 port，因此在重播時若我們使用的 IP address 跟錄製時不同，就必須修改 control connection 的 IP address，以讓 data connection 重播時能符合 FTP 規約的規定。

表 1 列出幾種常見既有的流量重播工具之比較，涵蓋有需不需要完整流量檔資訊(Completed PCAP)、有狀態性(Stateful)，以及是否提供選擇性播放(Selected Replay)等特性。

| Name | Feature | Completed PCAP | Stateful | Selected Replay | Configure Option |
|---|---|---|---|---|---|
| TCPreplay | Support many link types | No | No | No | Speed |
| Tomahawk | Background traffic | No | Yes | No | Concurrent users |
| Monkey | Test web server | Yes | Yes | No | Congestion |
| Avalanche | Traffic generator | No | Yes | No | Concurrent users |
| Traffic IQ | Management | No | Yes | No | Gateway |

表 1：各種既有流量重播工具之比較

在現有研究技術和工具中，重播真實錄製的準確性仍有些實際的問題沒被完整的解決，第一個問題是錄製流量時連線在錄製時間點就開始建立，因此無法錄置完整的連線，或在真實環境下的流量太大導致錄製不完全，第二則是前段所說明的問題，第三個是重播後如何在龐大流量中尋找產生事件(如待測物 crash 或待測物產生的 error、bug)的流量。而我們打算開發新的重播工具則提供同時解決這三項問題，使產品開發者不但可以測試到真實流量的網路行為，也可以節省分析流量的時間與加速重置事件的過程，讓產品開發者能更能有效的除錯，最後讓產品更穩定。

## 二、 研究目的

此計畫目的在於提供資安技術一組通用(Generic)的重播測試工具，透過這些工具來進行流量重播測試以便可以快速地重製出待測物在真實環境下的問題，這些工具包括了流量錄製(Capture)、流量重播(Replay)、Classification 以及 Extraction，這些工具除了可以單獨使用進行測試之外，還可以整合發展出一套應用系統「PCAP Library」，其最直接的用途在於可以用來測試資安技術有沒有誤判跟漏判的問題存在，更可以進一步地分析誤判與漏判的原因並提供 traces 給開發者參考分析。

PCAP 是一種儲存網路流量的通用檔案格式，我們將 Beta Site 上的各種網路流量儲存成 PCAP 格式的檔案，並分門別類地存入資料庫，當使用者想使用真實流量來進行測試時，可以指定查詢條件來搜尋想要的網路流量。PCAP Library 的使用情境(scenario)如表 2 所示，可分成三種：第一種，漏判與誤判之分析；第二種，根據應用程式不同作流量分類；最後一種，根據流量本身是否含有惡意軟體作分類(如果有含惡意軟體，則稱為 bad；反之，則稱為 good)。

| 使用情境 | 目的 | 效益 |
|---|---|---|
| 漏判與誤判之分析 | 測試待測物漏判與誤判的情況，並提供造成漏判與誤判的流量給研發人員進一步分析 | 提升資安產品的偵測準確性 |
| 流量分類 by applications | 提供各式各樣已分類好的應用流量，可加速問題的釐清過程 | 提高資安產品品質改善的效率 |
| 流量分類 by good or bad | 提供已分類好的 good 及 bad 流量，提高漏判與誤判分析的準確度 | 提升資安產品的偵測準確性 |

表 2：PCAP Library 的三種使用情境

## 三、 文獻探討


[1] L. Deri, “Improving Passive Packet Capture: Beyond Device Polling”, in *Proceedings of SANE* 2004.

[2] L. Deri, “nCap: Wire-speed Packet Capture and Transmission,” in *E2EMON*, May 2005.

[3] S-H. Han, M-S Kim, H-T Ju, and J.W-K. Hong, “The architecture of ng-mon: A passive network monitoring system for high-speed ip networks,” in *IFIP/IEEE 13th International Workshop on Distributed Systems: Operations and Management (DSOM 2002)*, 2002.

[4] L. Deri, “High-Speed Dynamic Packet Filtering,” in *Journal of Network and Systems Management*, 2007

[5] F Schneider, J Wallerich, A Feldmann, “Packet Capture in 10-Gigabit Ethernet Environments Using Contemporary Commodity Hardware,” in *Lecture Notes in Computer Science*, 2007.

[6] Tcpreplay, http://tcpreplay.synfin.net/

[7] Feng, Wu-chang, Goel, A., Bezzaz, A., Feng, Wu-chi, Walpole, J. “TCPivo: a highperformance packet replay engine,” in *MoMeTools ’03: Proceedings of the ACM SIGCOMM workshop on Models, methods and tools for reproducible network research*, 2003.

[8] Ramaswamy Ramaswamy, Tilman Wolf, “High-speed prefixpreserving IP address anonymization for passive measurement systems,” in *IEEE/ACM Transactions on Networking (TON)*, 2007.

[9] Hong, S.-S., Wu, S.F., “On Interactive Internet Traffic Replay,” in *International Symposium on Recent Advances in Intrusion Detection (RAID 2005)*, Seattle, Washington, USA, 2005, pp. 247-264.

[10] Wang Yang, Jian Gong, Wei Ding, Xiong Wu, “Network Traffic Emulation for IDS Evaluation,” in 2007 IFIP International Conference on Network and Parallel Computing – Workshops.

[11] J. E. van der Merwe et al., “mmdump - A Tool for Monitoring Internet Multimedia Traffic,” in AT&T

Labs-Research Technical Report 00.2.1, Feb. 2000.

[12] C Indexing, N Indexing, “A multi-gigabit rate deep packet inspection algorithm using TCAM,” in *GLOBECOM* '05.

[13] Manuel Crotti; Murizio Dusi; Francesco Gringoli; Luca Salgarelli; “Traffic Classification through Simple Statistical Fingerprinting”, in *ACM SIGCOMM Computer Communication Review (CCR)* on Volume 37, Number 1, January 2007.

[14] Ying-Dar Lin, Chun-Nan Lu, Yuan-Cheng Lai, Wei-Hao Peng, Po-Ching Lin, “Application Classification Using Packet Size Distribution and Port Association,” in *Journal of Network and Computer Applications*, Vol. 32, Issue 5, pp. 1023-1030, September 2009.

[15] I-Wei Chen, Po-Ching Lin, Tsung-Huan Cheng, Chi-Chung Luo, Yin-Dar Lin, Yuan-Cheng Lai, Frank C. Lin, “Extracting Attack Sessions from Real Traffic with Intrusion Prevention Systems,” in *ICC*, Dresden, Germany, June 2009.

[16] Peng Ning , Yun Cui , Douglas S. Reeves, “Constructing attack scenarios through correlation of intrusion alerts,” in *Proceedings of the 9th ACM conference on Computer and communications security*, Washington, DC, USA, November 2002.

[17] S. Mathew, R. Giomundo, S. Upadhyaya, M. Sudit, A. Stotz, “Understanding multistage attacks by attack-track based visualization of heterogeneous event streams,” in *Proceedings of the 3rd international workshop on Visualization for computer security*, 2006.

[18] Ying-Dar Lin, Chien-Chao Tseng, Cheng-Yuan Ho, Yu-Hsien Wu, “How NAT-Compatible are VoIP Applications?,” in *IEEE Communication Magazine*, Vol. 48, Issue 12, pp. 58-65, December 2010.

[19] Cheng-Yuan Ho, Chien-Chao Tseng, Fu-Yu Wang, Jui-Tang Wang, Ying-Dar Lin, “To call or to be called behind NATs Is Sensitive in Solving the Direct Connection Problem,” in *IEEE Communications Letters*, Vol. 15, Issue 1, pp. 94-96, January 2011.

[20] Cheng-Yuan Ho, Fu-Yu Wang, Chien-Chao Tseng, Ying-Dar Lin, “NAT-Compatibility Testbed: An Environment to Automatically Verify Direct Connection Rate,” in *IEEE Communication Letters*, Vol. 15, Issue 1, pp. 4-6, January 2011.

## 四、 研究方法

### ***流量錄製與流量重播(Traffic Capture/Traffic Replay)***

錄製與重播在流量重播測試中扮演著非常重要的角色，它決定了整個系統的輸入輸出值，也間接決定了重播測試的價值。表 3 所列的是現今適用於高速網路上封包錄製的技術，可大致分為軟體及硬體兩部分。軟體部分可再細分三項：修改核心、分散式分流，及邊錄製邊處理三項；硬體部分則是流量分流與測試錄製速度。

| 類型 | 方法 | 論文或方法 |
|---|---|---|
| 軟體 | 修改核心以改進錄製速度 | ● Improve Passive packet capture [1]<br>● nCap [2] |

| | | |
|---|---|---|
| | 分散式分流給不同的系統 | ● NG-MON [3]<br>● Our Method |
| | Capture 時加速 packet filter 並節省 storage | ● High-Speed Dynamic Packet Filtering [4]<br>● Our Method |
| 硬體 | 分流與測試 capture 速度 | ● Packet Capture in 10-Gigabit [5] |

表 3：高速環境下 Capture 的相關技術

為了降低單位時間要儲存的資料量，讓錄製流量的工作可以順利進行。我們先在底層以 IP address 過濾流量、只錄某些 subnet 的 traffic。同時為了可以顧及到完整性，我們以 Regeneration TAP 複製出多份流量，對於每份流量又各以不同的 IP address 作過濾，這樣便可錄製到所有的流量。

流量重播除了能用現成的工具 tcpreplay[6]根據 timestamp 重播網路流量外，尚有其他新的研究議題和研究成果如表 4 所示，可分為三類：高速環境下重播、保護隱私，以及模擬 TCP stack 重播等。

| 議題 | 方法 | 論文 |
|---|---|---|
| 高速環境下 replay | 修改核心以加速 replay | ● TCPivo [7] |
| 保護隱私 | Anonymization algorithm | ● IP anonymization [8] |
| 模擬 TCP stack replay | Stateful replay | ● Interactive Internet Traffic Replay [9]<br>● Network Traffic Emulation for IDS Evaluation [10] |

表 4：Replay 的研究技術

為了能夠達到前述幾項流量重播測試工具的特性—可以正確重播網路流量、即使僅有封包部分資訊(至少包含標頭資訊)亦可進行重播、有狀態地重播，及可選擇性地重播某部分錄製下的流量以重製某特定事件，我們開發了 SocketReplay；在進行重播測試過程中，SocketReplay 會根據預先給定的 subnet IP address 範圍來改寫流量檔內的 IP address 資訊，以確保封包可以被正確送出；而且，隨著重播的進行，SocketReplay 會記錄(log) transaction 中已經過的封包狀態，確保重播過程中會一直維持有狀態性；此外，為了可以快速地移到觸發產生問題的關鍵連線或是封包，提供了 selected replay 特性，透過使用者給定的特定事件或是時間定義，在流量檔內進行搜尋，一旦找到後，會根據封包/連線的 five-tuple 值找出包含在此定義內/前後的所有相關連線資訊並進行重播。

***流量辨識(Traffic Classification)***

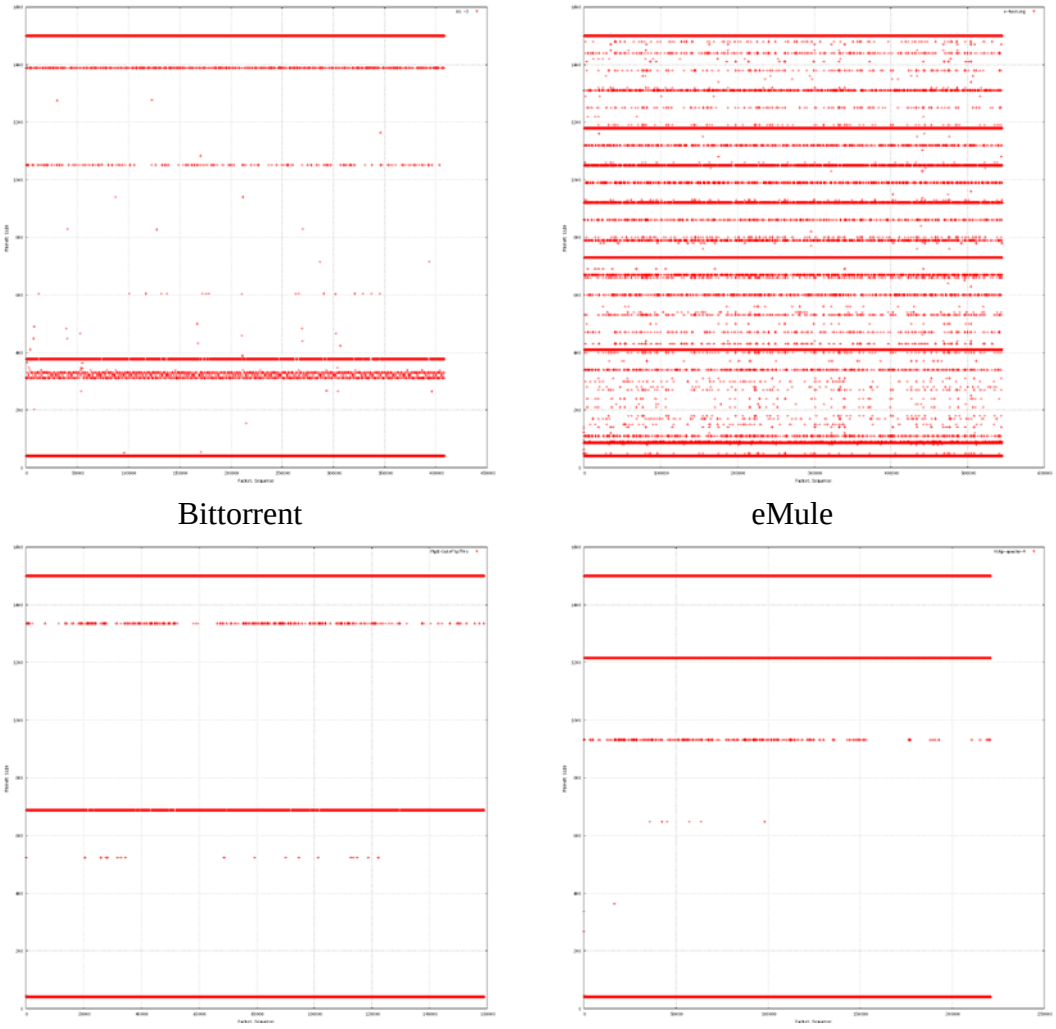
表 5 所列的目前透過辨識來分類流量的技術，可大致上分為以 signature 為主及以行為(behavior)為主的分類技術。Signature-based 分類技術則可再細分成兩項：以 stateful 辨識流量及利用硬體加速

的內容比對兩種技術；Behavior-based 技術則可分為以統計方式(statistical)獲取特徵及根據過程中使用的 port number/payload size 為主的分類技術。

| Approach | 技術 | 論文 |
|---|---|---|
| Signature-based | Statefully classify multimedia traffic | mmdump [11] |
| | 硬體加速的 content matching | A multi-gigabit rate deep packet inspection algorithm [12] |
| Behavior-based | Statistical Fingerprint | Traffic Classification [13] |
| | Port 與 Packet Size Distribution | Our Method [14] |

表 5：流量分類的研究技術

我們提出了一種辨識網路流量的方法，是由根據 Packet Size Distribution (PSD，如圖 3，不同的應用程式所使用的 PSD 有明顯的不同)和使用的埠關連性，我們嘗試用來辨識各種複雜甚至加密的網路應用程式行為。



Bittorrent　　eMule

zFTP server(Ftp)　　Apache (Http)

圖 3：不同 application 的 PSD，橫軸是 packet sequence、縱軸是 packet size。

我們提出了如圖 4 的處理機制，這種方法可以適用於未來辨識未知的網路應用程式。首先我們必須建造該應用程式的各種行為樣本流量，將它輸入 Phase I : Center Training，產生各種向量(vector)後算出中心點；再透過這個中心點輸入到 Phase II: Classification Algorithm，以讓真實流量的各種 connection 都能被分類到各種不同的 application。在真實流量中的每條連線皆會經由特徵值運算後變成多維空間中的一個向量，並且藉由計算先前分析出的各應用程式在空間中的代表點之差異即可辨識出該連線屬於何種應用程式；若再加上利用埠關聯性，對於網路應用程式連線的辨識正確率平均可高達 96%以上，且擁有平均 4%的誤判率及 5%的漏判率，圖 5 是使用此辨識機制的結果，透過後續的驗證發現，這樣的誤判主要發生於即時通訊軟體中因為使用了相近的封包長度導致出現判斷錯誤。

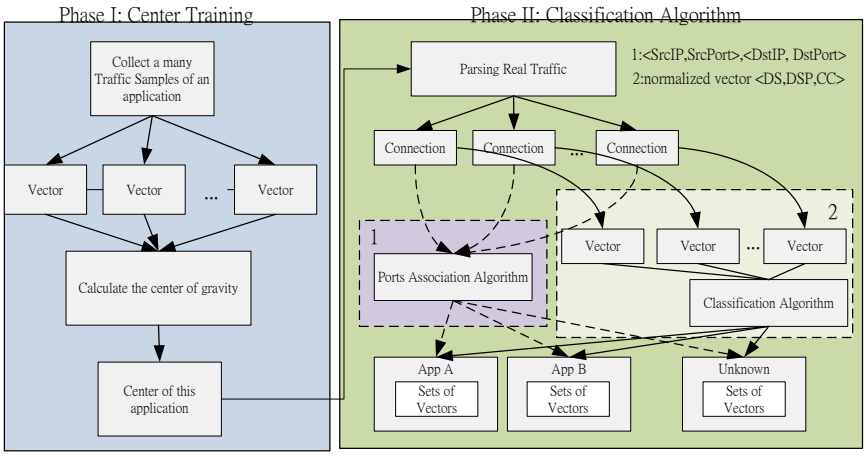



圖 4：利用封包長度及埠關連性之網路流量辨識機制

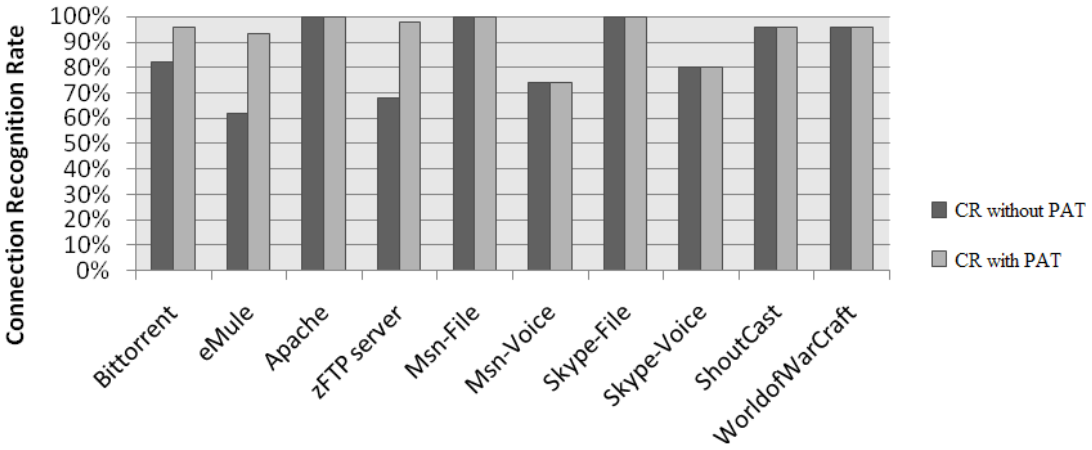



圖 5：連線辨識結果

## ***流量萃取(Traffic Extraction)***

在辨識流量、獲得攻擊資訊後，我們該如何透過得到的資訊轉換成我們所想要萃取的流量，以便更進一步分析像是惡意程式的攻擊行為或重製惡意程式的攻擊呢？我們提出一個萃取特定流量的方法，主要是與現有的 malicious traffic detection 技術和產品合作，例如: Anti-Virus/IPS/UTM/Network

Forensics/Application Firewall。概念如下:

Step 1. 將一 PCAP file 打入(可利用 tcpreplay、flowreplay、avalanche、tomahawk 等流量重播技術)各類資安偵防技術的產品。

Step 2. 搜集這些產品所產生的 Log。

Step 3. 根據 Log 的資訊，如流量的 5-tupule 連線資訊，再搭配時間作為參數來萃取出該有害物質(ex. Attack、malware download/transfer)s 的完整流量，並存成另一個 PCAP file。

根據上面的想法，我們提出了 Attack Session Extraction[15]，這個萃取被偵測到的惡意流量的方法有兩個 stage：從封包(packet)到連線(connection)、從連線到整個會談(session)，如圖 6、圖 7 所示。

a. From packets to connection：利用 IDS alert 中的 5-tuple 跟 timestamp 從流量中萃取 connection；

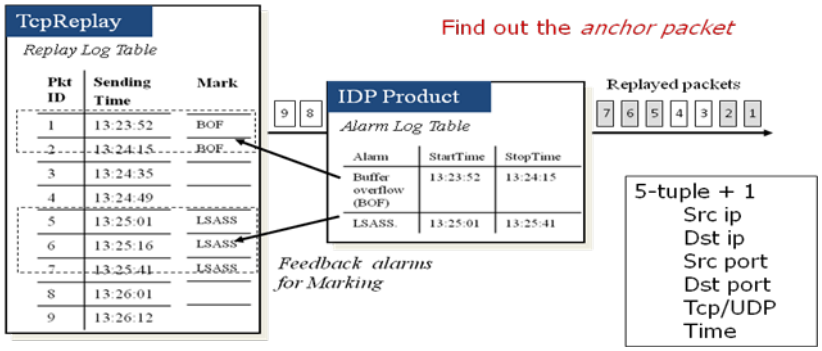



圖 6：從 IDS alert 萃取 connection 示意圖

b. From connection to session：利用相似度將不同的 connection 合成一個 session；

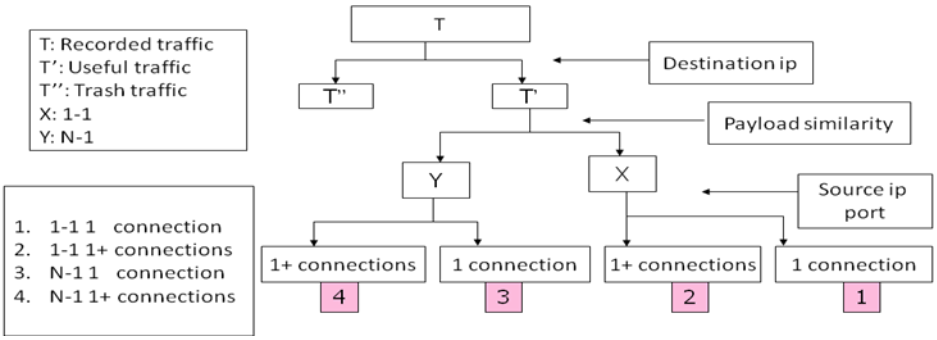



圖 7：從相似度萃取 session 示意圖

***PCAP 資料庫 (PCAP Library)***

整套 PCAP Library 系統可以分為三大部份（圖 8），首先，透過流量錄製設備將網路流量轉存為 PCAP 檔並從 Capture Site 傳回 Replay Site，為了瞭解這個 PCAP 檔裡面包含了哪些流量，我們將這個 PCAP 檔重播到不同的網路安全產品去檢視，在網路流量經過這些網路安全產品的同時，網路安全產品會檢測出其中是否含有有害網路流量；如果有，則會將有害流量的資訊以 syslog 的方式傳回播放設備上，播放設備再根據這些偵測結果將該 PCAP 檔切割成多個較小的 PCAP 檔，使得每個較小 PCAP

中只包含原先流量中的一條 connection，最後再將這些小 PCAP 檔連同網路安全產品的偵測結果一併上傳至資料庫中儲存。

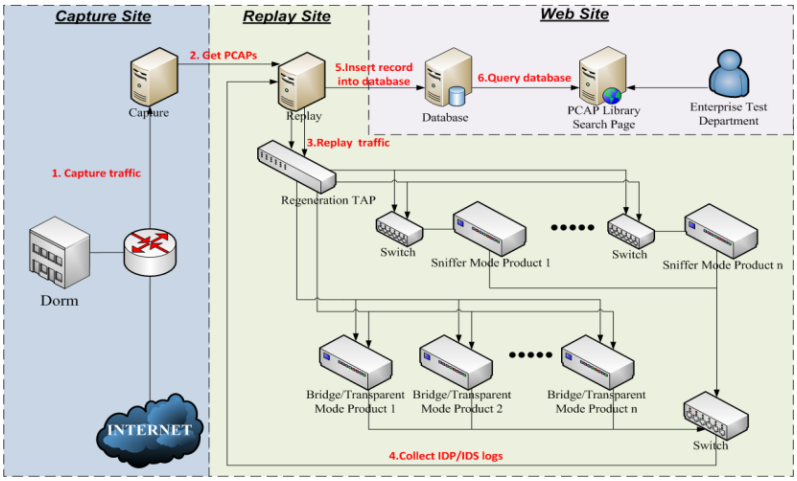
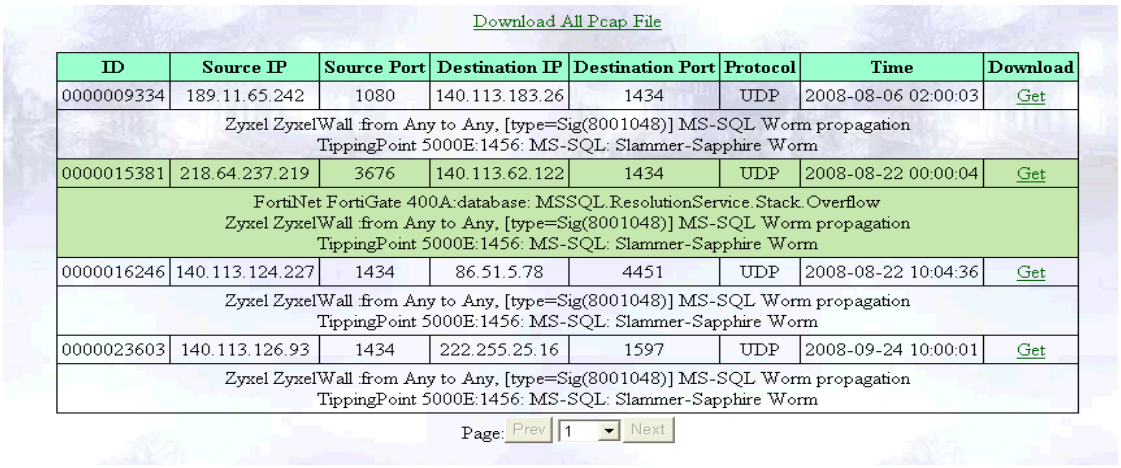



圖 8：PCAP Library 架構

PCAP Library (如圖 9)中允許使用者透過編號、連線資訊、時間、偵測裝置四大類索引來進行搜尋；每一個被上傳到資料庫中的 PCAP 都會被賦予一個獨一無二的 PCAP ID，當使用者知道上次使用的 PCAP ID 為何時，也可以直接的輸入 PCAP ID 進行搜尋、快速地尋找上次所使用的 PCAP；若使用者為第一次使用 PCAP Library，可以透過指定 IP 或 Port 的方式來搜尋特定的主機或服務被攻擊的流量，也能指定攻擊時間來搜尋 PCAP，或者選定特定的網路安全產品來瞭解這些產品偵測到哪些攻擊流量。


圖 9：PCAP Library 搜尋頁面

搜尋結果（圖 10）中會顯示出符合搜尋條件的 PCAP 連線資訊、時間、攻擊名稱，並可以透過『Get』這個連結來下載 PCAP，或使用『Download All Pcap File』來下載所有符合條件的 PCAP。



Download All Pcap File

| ID | Source IP | Source Port | Destination IP | Destination Port | Protocol | Time | Download |
|---|---|---|---|---|---|---|---|
| 0000009334 | 189.11.65.242 | 1080 | 140.113.183.26 | 1434 | UDP | 2008-08-06 02:00:03 | Get |
| Zyxel ZyxelWall :from Any to Any, [type=Sig(8001048)] MS-SQL Worm propagation<br>TippingPoint 5000E:1456: MS-SQL: Slammer-Sapphire Worm | | | | | | | |
| 0000015381 | 218.64.237.219 | 3676 | 140.113.62.122 | 1434 | UDP | 2008-08-22 00:00:04 | Get |
| FortiNet FortiGate 400A:database: MSSQL.ResolutionService.Stack.Overflow<br>Zyxel ZyxelWall :from Any to Any, [type=Sig(8001048)] MS-SQL Worm propagation<br>TippingPoint 5000E:1456: MS-SQL: Slammer-Sapphire Worm | | | | | | | |
| 0000016246 | 140.113.124.227 | 1434 | 86.51.5.78 | 4451 | UDP | 2008-08-22 10:04:36 | Get |
| Zyxel ZyxelWall :from Any to Any, [type=Sig(8001048)] MS-SQL Worm propagation<br>TippingPoint 5000E:1456: MS-SQL: Slammer-Sapphire Worm | | | | | | | |
| 0000023603 | 140.113.126.93 | 1434 | 222.255.25.16 | 1597 | UDP | 2008-09-24 10:00:01 | Get |
| Zyxel ZyxelWall :from Any to Any, [type=Sig(8001048)] MS-SQL Worm propagation<br>TippingPoint 5000E:1456: MS-SQL: Slammer-Sapphire Worm | | | | | | | |

Page: Prev 1 Next

圖 10：PCAP Library 搜尋結果

除了基本的搜尋功能外，PCAP Library 也可以應用在測試網路安全產品誤判與漏判問題；同一份 PCAP 若 A,B,C 三台產品有偵測到，而 D 產品沒有偵測到，這份 PCAP 是 D 產品漏判的機會就相當高；反之，若 A,B,C 三台產品沒有偵測到而 D 產品偵測到，則很有可能是 D 產品的誤判。

## 五、 結果與討論

本計劃設計開發了一組通用的資安技術流量重播測試工具—Socketreplay，整合了包含流量錄製、流量重播、流量分類以及流量萃取等技術，除了可以快速地重製出真實環境下的問題之外，同時亦可以找出觸發待測物發生問題的關鍵流量，以提供給產品開發者進行分析與除錯。除此之外，我們也發展出一套應用系統「PCAP Library」，其最主要的功用在於測試資安技術誤判與漏判的問題並提供可能造成誤判及漏判的流量給開發者分析，進而提高資安技術的辨識準確度。

本計劃自執行開始，迄今已獲得多項成果：調查比較各種既有重播工具、設計開發適合總計畫所建置之測試環境的測試機制、開發完成一套流量重播測試工具–socket replay(支援有狀態地重播網路流量、萃取特定流量、在有少許封包遺失的前提下仍可重播網路流量)、PCAP Library應用系統(整合流量錄製、流量萃取、流量重播、流量資訊重組，以及流量資訊查詢等功能)、發表三篇國際期刊論文(包括*IEEE Communications Magazine*[18]及*IEEE Communications Letters*[19、20])、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(如鴻璟科技)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，因為產品本身功能設計與測試網路規模考量，流量重播測試具有極重要的地位；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: 子計畫一:資安技術真實流量重播評比 |
| | 計畫主持人: 林寶樹 |
| | 計畫編號: 99-2218-E-009-014- 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-009-014- |
|---|---|
| 計畫名稱：資安技術真實流量實地評比--子計畫一:資安技術真實流量重播評比 | |

| 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 | 3 | 3 | 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 | 3 | 3 | 100% | 篇 | 發表三篇國際期刊論文(包括 IEEE Communications Magazine 及 IEEE Communications Letters) |
| | | 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<br>(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)

共三篇國際期刊論文，一篇發表在 IEEE Communications Magazine、兩篇在 IEEE Communications Letters)

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）

本計劃目的在於提供資安技術一組通用的流量重播測試工具，其中包括了流量錄製、流量重播、流量分類以及流量萃取等，透過這些工具來進行重播測試除了可以快速地重製出真實環境下的問題之外，同時亦可以找出觸發待測物發生問題的關鍵流量，以提供給開發者進一步分析與除錯。除此之外，我們也發展出一套應用系統「PCAP Library」，其最主要的功用在於測試資安技術誤判與漏判的問題並提供可能造成誤判及漏判的流量給開發者分析，進而提高資安技術的辨識準確度。

PCAP Library 系統架構中整合了五大元件，分別是流量錄製、流量分類與萃取、資訊重組、查詢以及流量重播。流量錄製時要避免封包遺失以及存儲空間使用效率低落，流量分類與萃取時要將錯誤的機率壓低，資訊重組時要注意資訊尋找與更新，查詢時要兼顧效能與正確性，流量重播時必須是有狀態性(stateful)重播等。

本計劃自執行開始，迄今已獲得多項成果：調查比較各種既有重播工具、設計開發適合總計畫所建置之測試環境的測試機制、開發完成一套流量重播測試工具－socket replay(支援有狀態地重播網路流量、萃取特定流量、在有少許封包遺失的前提下仍可重播網路流量)、PCAP Library 應用系統(整合流量錄製、流量萃取、流量重播、流量資訊重組，以及流量資訊查詢等功能)、發表三篇國際期刊論文(包括 IEEE Communications Magazine 及 IEEE Communications Letters)、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(如鴻璟科技)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，因為產品本身功能設計與測試網路規模考量，流量重播測試具有極重要的地位；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。