崑山科技大學學報第十期 第61~71頁 (民國104年9月)
Journal of Kun Shan University, No.10, pp.61~71 (September, 2015)

網路威脅分析與防禦評估

王平[*]　劉佳琪[**]

崑山科技大學 資訊科技學院 資訊管理系
副教授[*]　研究生[**]

摘要

許多網路威脅分析(threat analysis)方法已提出，但經常假設威脅之攻擊情境與系統脆弱點為已知。但因變種病毒的流行，許多已知威脅之攻擊屬性改變，例如下載惡意程式名稱可由攻擊者定義、隨網址改變連線之網域名稱伺服器及隨機改變連線的埠號，故防衛者常無法偵測及估算威脅之衝擊，造成資安評估所建議之防禦方案結果無法確認是否合適。因此，本研究結合網路誘捕系統(honeypot) Dionaea 進行蒐集特定病毒與行為分析，透過已知共通弱點報告(CVE)進行交叉比對，確認病毒是否已變種，再運與利用情節頻繁法則(frequent episode)估算出感染惡意程式機率。最後，透過繪製攻擊樹(attack tree) 以模擬威脅分析案例，估算系統脆弱點所造成的威脅與產生的衝擊；由本研究發現所研提方法可有效分析威脅所造成的衝擊，及決定適合的防禦方案。

關鍵詞：資訊安全、威脅分析、惡意程式、變種病毒、攻擊樹

壹、前言

僵屍網路(botnet)是由 Internet Relay Chat(IRC) 網路的功能基礎發展出來的，駭客依據 IRC 通訊功能來執行客製化程式碼(script)，並加以透過受感染之跳板主機將原始碼大肆散佈。僵屍網路之惡意程式入侵主機後會引發多次下載以置入外殼程式(shellcode)間接取得作業系統控制權並隱藏惡意程式，進一步載入網路偵測程式，蒐集受害組織其他主機組態與脆弱點，設法突破資訊網路其他節點之資安弱點，入侵重要伺服器衍生出更嚴重的災害，已使得資訊防護的困難度大為增加。常見的 botnet 感染型態為集中式模式，通常集中式模式存有一控制與命令伺服器(Command and control server)，受感染之主機會自動與主控端(bot master)連線與回報訊息，並接受主控端的控制指令，但集中式模式較容易被發現，故駭客將 P2P 通訊功能導入其 Botnet 架構中，形成一點對點傳輸模式(P2P)，如 Sinit 病毒。Botnet 主要特點為可讓主控端輕鬆地針對所有的 Bots 進行控制與命令(Control and Command, C&C)，進而竊取具有利益的資料，如個人隱私資料，來達成獲利。防衛者須透過威脅分析，定期評估僵屍網路之衝擊, 提昇組織的資訊安全防禦警覺是管理者的一項艱鉅挑戰。

Bruce Schneier(1999)將失效樹分析法(Fault Tree Analysis, FTA)應用於威脅情境分析，命名為攻擊樹(Attack Trees)，其運用樹的結構以探索威脅清單之可能攻擊手法，將攻擊過程轉變為樹狀結構，以根節點以組合攻擊目標[2]。攻擊樹可回答不同威脅的假設問題

分析，並估計各種攻擊組合的成本與衝擊。其仍存在部份缺點是缺乏防禦思考。Edge et al. (2007)以反向思考提出防禦樹(protection trees)分析複雜資訊系統之脆弱點, 改進其資安的防禦措施 [13]；其仍將攻擊與防禦分開成兩個不同程序，分別以攻擊樹與防禦樹分析與評估，改進攻擊樹缺乏防禦的缺點。

本研究參考 Roy(2010)等學者提出攻擊防禦樹(Attack Countermeasure Tree, ACT) [1]，運用 ISOGraph 公司研發之攻擊樹工具 Attack Tree+[8]，考慮攻擊與防禦措施間互動情境，透過邏輯反向原理調適將攻擊路徑的參數轉換為防禦樹分析，正確估算惡意程式威脅之嚴重性與衝擊，提出合適的防禦解決方案。本文共分為四節，各節內容簡述如後；第貳節介紹文獻探討，第參節本研究所提的風險評估步驟與模式，第肆節舉一案例說明攻擊防禦樹應用於之網路威脅與防衛評估，第伍節作出結論及建議未來研究方向。

貳、文獻探討

本節回顧現有之威脅風險分析方法及介紹攻擊樹。

一、威脅風險分析方法

失效樹始於 80 年代後期，應用於系統可靠度分析[16]，後續發展則加入風險分析概念，如 Weiss 的風險邏輯樹和 Amoroso 風險樹；Schneier(1999)將決策樹應用於攻擊分析並提出攻擊樹的攻擊成本評估。Schnerier 利用 PGP 為例說明攻擊樹的應用。Mauw(2006)運用攻擊樹，分析攻擊目標與事件間的關聯性，發現攻擊和故障常會導致系統錯誤，使其攻擊樹應用在複雜案例分析，成效無法達到預期的期望[21]。 Bistarelli 等(2007)學者利用防禦樹(Defense Trees, DT)和遊戲理論，找尋最具成本效益的有效對策[23]。Edge 等(2007)學者根據 Foo 等[24]學者提出入侵圖(Intrusion Graphs, I-GRAPHs)攻擊樹結構，提出了類似正規化防禦樹，其利用 I-GRAPHs 分析動態入侵行為[13]。Fovino 等(2009)學者應用圖形理論，整合故障樹結構攻擊，命名為擴展故障樹(Extended Fault Tree, EFT)[22]。Zonouz 等學者(2009)提出攻擊回報樹(Attack-Response Tree, ART)，其利用可擴展的狀態空間模型，進行尋找一個最佳的防禦策略，建立基於隨機遊戲模型觀察部分的 ART，循序評估動態入侵結果[25]。Roy(2010) 等學者提出攻擊防禦樹(Attack Countermeasure Tree, ACT) [1]，係為一簡單有效的網路安全分析方法，具上述學者所提到模型的優點，可依不同的攻擊案例，使用單一和多目標優化後，擬訂出最佳的防禦策略。

二、攻擊樹

攻擊樹主要是由分為閘(Gate)與事件(Event)所組成，閘代表為攻擊的目標，事件型態分為及(AND)節點與或(OR)節點，事件節點代表為攻擊必要的步驟(如圖 1 之 A、B、C、D 節點)，若閘的型態為 OR 匣，則必須至少一個事件節點條件成立；反之，則必須皆為條件成立，才可成功完成閘攻擊目標，如圖 1。

本研究參考[8, 26~27]並改良攻擊與防禦樹之風險分析，以強化威脅分析(Threat Analysis, TA)，性能評估是透過攻擊回報(Return on Attack，ROA)之評估指標(metrics)計算，包括各子節點之攻擊成本、衝擊與風險，據以擬定網路威脅可行之防禦策略，防禦行動如圖 2 中綠色節點之部分。

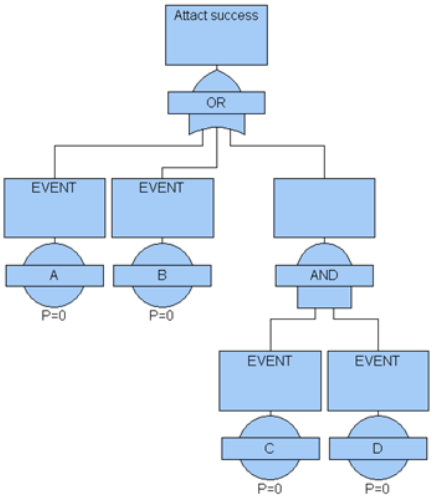

圖 1. 攻擊樹基本架構

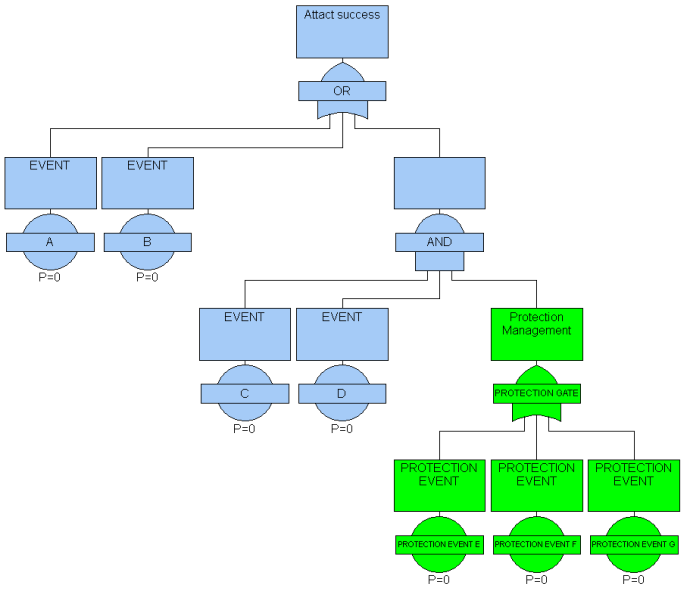

圖 2 攻擊防禦樹基本架構

參、研提的風險評估模式

本研究參考國際標準 ISO/IEC 27005：2008(E)之風險管理程序[7]，將威脅分析納入在「建立全景」、「風險評估」、「風險處理」程序中，詳細說明如下。

一、建立全景

本研究架設一 Dionaea 之低互動式誘捕系統[6]進行惡意程式誘捕，其為 Google Summer of Code 2009 之 Honeynet Project 的始源項目，Dionaea 為 Nepenthes 的研究延伸之成果。其設計目的是誘捕惡意攻擊，以獲取惡意程式攻擊的樣本與識別感染過程，其能模擬某些標準伺服器已知的漏洞，如：FTP、HTTP、Telnet 等，並能模擬完整區域網

路 IP 位址、紀錄攻擊行為及通知管理人員，如：當系統檔案被修改或被植入後門程式時，主機可處存相關系統資訊，Dionaea 運作架構如圖 3。

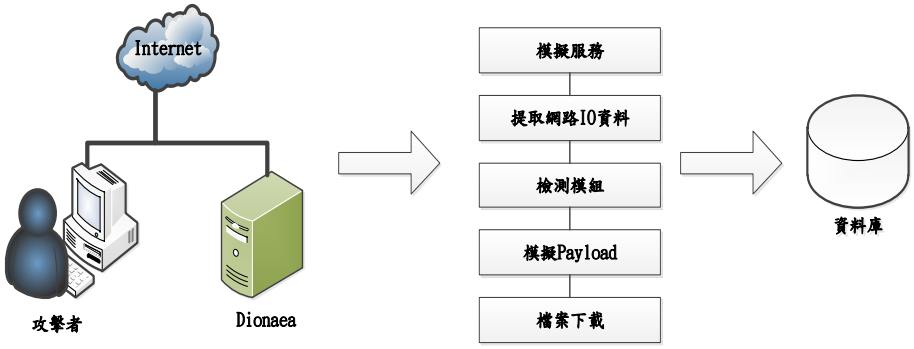

圖 3. Dionaea 運作架構

如圖 3 所示，工程師須先安裝 Dionaea 程式於伺服器之/opt/dionaea 目錄下，用戶端向模擬網路服務之上傳的文件，並存放於伺服器/opt/dionaea/ var/dionaea/wwwroot 中，當發生惡意攻擊時，記錄將會被保存於/opt/dionaea/var/dionaea/bistreams，下載的惡意程式檔案則儲放於/opt/dionaea/ var/dionaea/binaries；另外，Dionaea 會將檢測到的事件訊息，將記錄在 Dionaea 所連接的 SQLite 之事件資料庫(logsql.sqlite)中，預設儲放位置於/opt/dionaea/var/dionaea，完整資料庫之資料表關聯圖如圖 4。

病毒之行為特徵可透過事件關連分析，關連分析方法包括資料探勘(data mining)及順序分析(sequence analysis)法；前者方法缺乏時間計量，只能分析事件的順序對應的信度，而病毒行為分析重點在於其事件(events)發生的順序及對應發生的時間(timing)，故本研究選用順序分析技術之頻繁情節法則(frequent episode rules) [4-5,28]，透過情節(episode)進行比對特定事件序列(特徵)，其結合了時間變數詳細分析事件關連，找出特定的事件序列 (event sequences)。

防護網路系統感染特定病毒的機率則是統計頻繁情節中之特徵事件之序列及數量加以估算。一段情節就是表示一個特定事件的序列，例如開啟通訊埠、修改註冊機碼(registry) 及下載檔案等三個有順序的事件，若透過特定的時序性項目集合比對及統計發生頻率，可以找到感染特定病毒的徵兆，並計算出感染發生的機率(p_i)。透過特定時序性的項目集合中進行比對時間視窗(win) $\omega = (\omega, T_s, T_e)$，事件序列的所有行為事件中，特定情節(α)發生的為支持度 sup 即為感染特定病毒 i 之發生機率(p_i)

$$\sup(\alpha) = p_i(\alpha, s, win) = \frac{|\{\alpha \text{ occurs in } \omega\}|}{|\{W(s,win)\}|} \qquad (1)$$

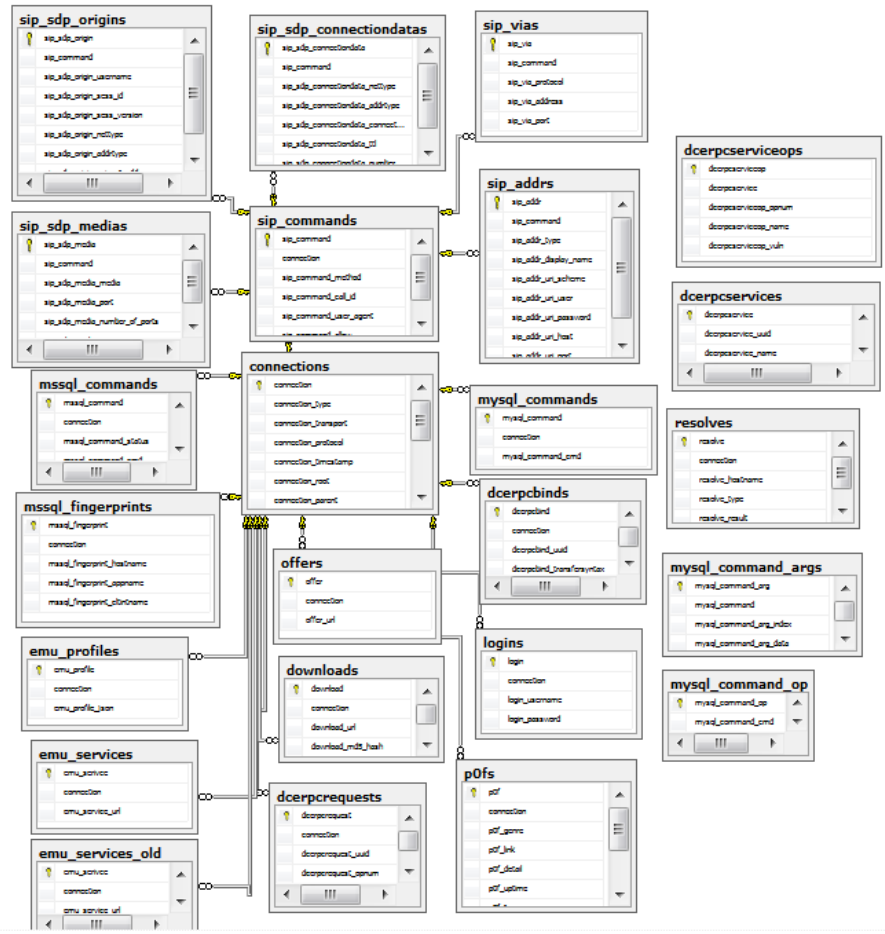

圖 4. Dionaea 之 ERD

二、風險評估

本研究將參考 Edge 等(2007)學者攻擊防禦樹及失效樹分析法[13]，用以補充 Roy(2010)等學者提出攻擊防禦樹[1]之防禦方案成本的估計，評估指標包括攻擊成功機率、攻擊成本、(修正)系統衝擊與防禦方案的成本。威脅 i 之發生機率 (p_i)代表一組威脅 i (i=1,...,m)可能成功攻擊資訊系統的機會，數值為介於 [0,1]之間。攻擊成本 (c_i)為攻擊所需的人力成本以美金計價，而防禦成本 (d_i) 代表防禦所需的人力成本及所需的資安設備。為簡化起見，每 100 人力小時作一個單位成本。威脅 i 所造成系統衝擊以順序尺度 [1~10]來量化其衝擊的嚴重程度(l_i)。

理論上，未修補之脆弱點將增加受攻擊的機會，造成較高的系統衝擊；系統加入防禦措施、定期更新及完整修補之系統脆弱點將增加防禦成本，但降低遭受攻擊的機會；根據 Roy(2010) 等學者提出 ACT，每一子節點於時間 t 之攻擊回報(ROA)可由攻擊的成功機率(p_i)、攻擊成本(c_i)及系統衝擊(l_i)三者估計。攻擊樹之風險評估是從底層樹葉 (leafs) 開始，反向遞迴至攻擊次目標(sub-goals)，每一次遞迴須計算次目標之評估指標如表 1，最後可求得根節點(root node)之攻擊回報如公式(2)。

$$ROA(t) = \frac{p_i(t) \cdot l_i(t)}{c_i(t)} \qquad (2)$$

表 1. 攻擊防禦樹之威脅分析之評估指標

評估指標	及閘運算	或閘運算	*K*-out-of-*N* 運算
威脅成功機率$p_i(t)$	$\prod_{i=1}^{n} p(i)$	$1-\prod_{i=1}^{n}\left(1-p(i)\right)$	$\sum_{j=k}^{n}\binom{n}{j}p^j\,(1-p)^{n-j}$
攻擊成本$c_i(t)$	$\sum_{i=1}^{n} c_i$	$\forall_i \min c_i$	$\sum_{i=1}^{k} c_i$
系統衝擊$l_i(t)$	$\sum_{i=1}^{n} l_i$	$\forall_i \max l_i$	$\sum_{i=1}^{k} l_i$
防禦成本$d_i(t+1)$	$\sum_{i=1}^{n} d_i$	$\forall_i \max d_i$	$\sum_{i=1}^{k} d_i$

三、風險處理

依據 Edge (2007)定義之攻擊防禦樹(protection trees)，其節點型態為攻擊樹的節點互補型態，例如 AND 匣之互補型態為 OR 閘，故防禦成本分析評估後，協助管理者對感染攻擊途徑修復下達決策。當完成初步風險評估後，管理者了解那些脆弱點的存在，針對上述之高風險攻擊路徑，於時間 *t*+1 採取有效的資安措施(safeguards)，將可降低攻擊回報，增加攻擊者的攻擊成本與降低系統衝擊。每一安全措施方案對應之風險降低，攻擊成本的增加與系統衝擊降低效用不同，可用兩參數α及β說明，則攻擊回報估計公式(2)改為

$$ROA(t+1)=\frac{p_i(t)\cdot(\alpha\circ l_i(t))}{\sum_{k=1}^{q}(1+\beta)c_k(t)} \qquad (3)$$

其中α代表能降低系統衝擊的比率，β代表增加攻擊成本的比率。

肆、系統測試與驗證

本節舉一雲端資安風險評估案例，透過 ZeuS 網路攻擊為例說明雲端服務若遭受 Botnet 攻擊之風險評估過程與風險管理改進做法。首先參考 Zeus Tracker 網站 (https://zeustracker.abuse.ch/index.php) 已公布之 Zeus 病毒樣本進行感染行為繪製攻擊樹，識別 Zeus 病毒可能之感染行為。

一、建立全景

防衛者須針對最新網路威脅，確認 APT 攻擊之惡意程式之特徵，以利後續之威脅分析及風險評估。Zeus 在 2007 年被資安人員發現，最初設計用來獲取金融機構網頁認證碼，但是它可以通過改變證券認證碼等內容，其中包括購物和社交網站等。2009 年 3 月因駭客透過網站銷售原始碼，造成大量散佈。ZeuS 網路攻擊是利用社交工程與釣魚(phishing)手法，針對微軟作業系統，以 Facebook、電子郵件連線下載或利用 PDF Launch 及更新程序功能漏洞實施攻擊，在 Adobe 還未來得及更新時，駭客已透過上述方法在 PDF 檔案中夾帶惡意程式，當使用者開啟該 PDF 檔時，就會在使用者電腦中植入 Zeus 殭屍程式，駭客再透過遠端連線竊取線上銀行網站交易帳密、社交工具及使用者應用軟體之帳密[12]。

二、風險評估

攻擊樹工具是選用 ISOGraph 研發之 Attack Tree+[8]，參考 Schneier[2]所提出的風險攻擊成本與 Edge *et al.*[13] 的相對防衛概念，分析 ACT 網路威脅和可能遭受到的攻擊 ROA 與防衛 ROI 的估計。本研究根據 Zeus Tracker 網站公布之 Zeus 感染行為繪製攻擊樹，透過已知共通弱點報告(CVE) [19]與沙網(SandNet)[9-10]兒進行交叉比對，確認病毒是否已變種。假設發生惡意程式感染事件，每一攻擊行為所造成系統衝擊之損失及攻擊成本以一萬美金為單位，所有事件之成功攻擊機率及計算完成評估指標如圖 5 所示，感染駭客工具程式之風險評估指標如表 2。

表 2. 感染駭客工具程式之風險評估

評估指標	符號	數值
攻擊 ROA		0.716
成功機率	$p_i(t)$	0.309
攻擊成本	$c_i(t)$	4.7 萬美金
系統衝擊	$l_i(t)$	7.5

根據圖 5 進行防禦成本分析，分析遭受到的攻擊風險與防禦成本進行擇優(trade-off)評估。針對上述之高風險攻擊路徑，增加安全措施，將可降低風險，增加攻擊者的攻擊成本與降低系統衝擊。但每一安全措施方案對應之風險降低，攻擊成本的增加與系統衝擊降低效用不同，以下運用兩參數α及β說明。其中α代表能降低系統衝擊的比率，β代表能增加攻擊成本的比率。以安全措施 1 為例，其資安防禦能力可表示為 S_1(α=0.85, β=0.55)如表 3。

表 3. 安全措施之防禦能力參數表

Safeguards ID	α	β	ROA
Safe 1	0.55	0.85	0.416
			0.27
Safe 2	0.20	0.70	0.51
			0.34

Safe 3	0.25	0.65	0.56 0.22
Safe 4	0.35	0.80	0.3 0.22

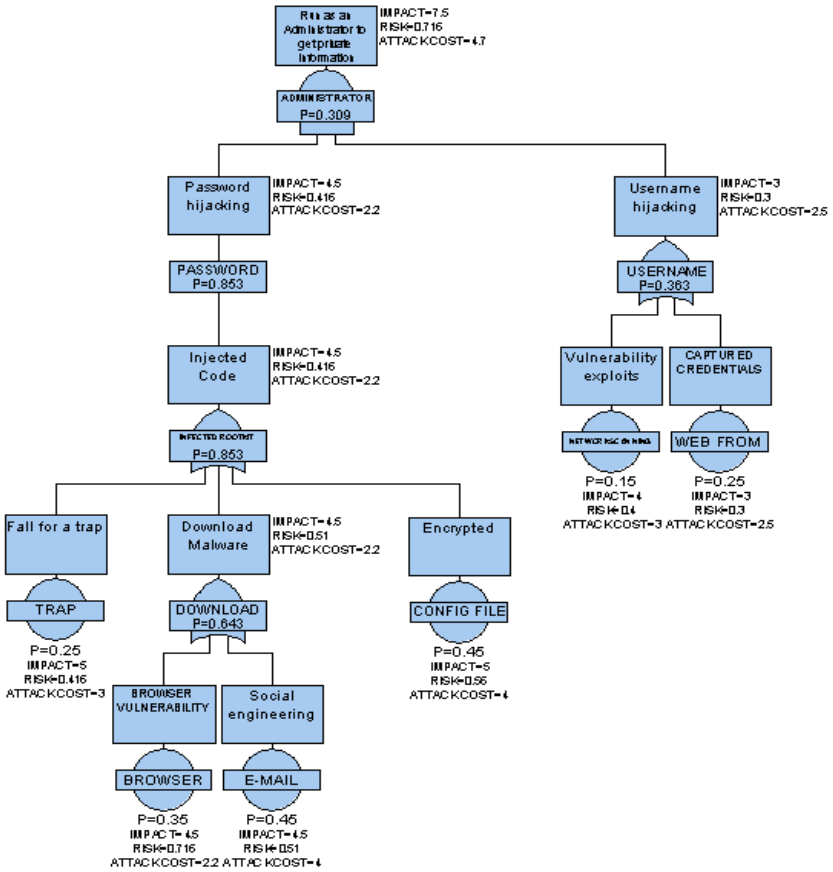

圖 5. 以 Attack Tree+ 繪製 Zeus 病毒並加上評估指標之攻擊圖

三、風險處理

經過評估後，透過瀏覽器的弱點進行下載惡意程式，並將其惡意程式執行進行取得管理者身份,該最佳感染途徑對應於最低攻擊成本路徑,與對系統主機衝擊最大的路徑，故管理者應優先進行系統修補。建議優先系統修補路徑如圖 6。根據圖 6 進行防禦成本分析，防禦者須投入 4.4 萬美金的防禦成本，有效將 ROA 由 0.716 降低至 0.22，系統衝擊由 7.5 降低至 2.45，而攻擊成功機率由 0.309 降低至 0.0546，計算結果如表 4。

表 4. 防禦方案之評估

評估指標	符號	數值
攻擊 ROA		0.716→0.22
攻擊成本	$c_i(t)$	4.7 萬美金

防禦成本	$d_j(t+1)$	4.4 萬美金
系統衝擊	$l_i(t)$	7.5→2.45

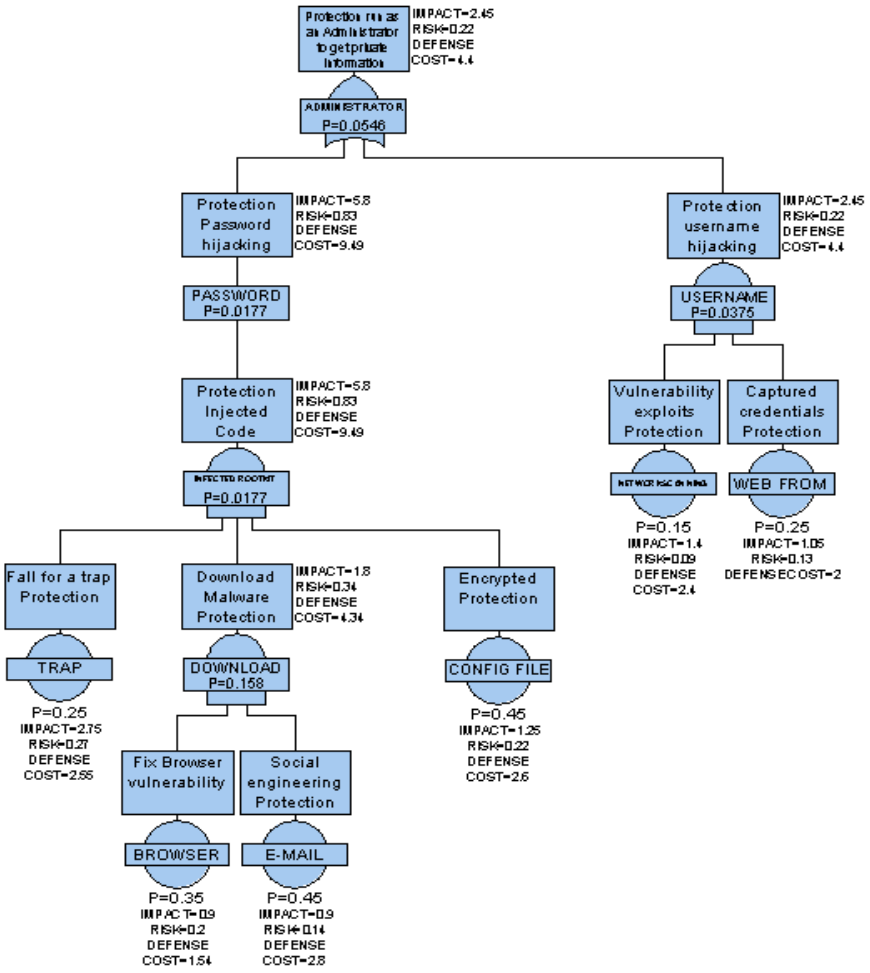

圖 6. 惡意程式攻擊之防禦規劃

伍、結論

本研究整合惡意程式特徵分析及補充 Roy *et al.*(2010) [1]所提出的攻擊防禦樹分析法對防禦成本估算的方法，透過攻擊成本計算，估算威脅的風險等級的，協助資訊服務安全管理之風險評估進行。最後透過 ZeuS 病毒攻擊案例分析，透過指標評估分析，合理進行網路威脅與防衛方案之分析。

參考文獻

[1] A. Roy, D. Kim, and K. S. Trivedi. “Cyber Security Analysis using Attack Countermeasure Trees”. In CSIIRW’10, April 21-23 2010.

[2] B. Schneier, "Attack Trees: Modeling Security Threats." Dr. Dobbs' Journal: Dec 1999.

[3] CSI Computer Crime 2010, source from http://gocsi.com/survey.

[4] H. Mannila, H. Toivonen, and A. I. Verkamo,“Discovery of Frequent Episodes in Event Sequences.”, Data Mining and Knowledge Discovery, Vol.1, No. 3, 1997, pp. 259-289.

[5] H. Mannila, H. Toivonen,and I. A. Verkamo, , “Discovery of FrequentEpisodes in Event Sequences,” DataMining and Knowledge Discovery,1(3):259-289, 1997.

[6] Honeynet Project, Dionaea honeypot, available at ftp://ftp.carnivore.it/projects/dionaea/mercury-dvd

[7] International Organization for Standardization, “Information Technology-- Security techniques-- Information security risk management (ISO/IEC 27005:2008) ” .

[8] ISOGraph, http://www.isograph-software.com/2011/.

[9] J. Clausing, “Building an automated behavioral malware analysis environment using open source software, ” SANS Institute Reading Room2009.

[10]J. Stewart, "Behavioural malware analysis using Sandnets," Computer Fraud & Security, vol. 2006, pp. 4-6, December, 2006.

[11]K. S. Edge, A Framework for Analyzing and Mitigating the Vulnerabilities of Complex Systems via Attack and Protection Trees. PhD thesis, Air Force Institute of Technology, 2007

[12]K. Stevens and D. Jackson, ZeuS Banking Trojan Report, available at http://www.secureworks.com/research/threats/zeus/?threat=zeus

[13]K. S. Edge, G. C. Dalton II, R. A., Raines, R. F., Mills, “Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security” , MILCOM 2007, pp. 1–7.

[14]K. Scarfone T. Grance K. Masone, “Computer Security Incident Handling Guide”, NIST SP 800-61 Rev 1, MAR. 2008.

[15]Mitre Corporation, Common Vulnerabilities and Exposures. available at http://www.cve.mitre.org.

[16]M. Rausand and A. Høyland, System Reliability Theory; Models, Statistical Methods and Applications, Wiley, 2004.

[17]OWASP Foundation, “OWASP Top Ten for 2011: The ten most critical web application risks,” (accessed February 09, 2011), available at http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

[18]S. Gary, G. Alice, and F. Alexis, “Risk Management Guide for Information Technology Systems,” Special Publication 800-30, National Institute of Standards and Technology (NIST), 2002.

[19]US-CERT, National Vulnerability Database, (accessed January 12, 2012), available at http://www.kb.cert.org/vuls/html/search.

[20]V. J. Randwyk, L. L. Chiang, and K. Vanderveen, “Farm: An automated malware analysis environment, ” in Security Technology, 2008. ICCST 2008.42nd Annual IEEE International Carnahan Conference on Prague, 2008.

[21]S. Mauw and M. Oostdijk, “Foundations of Attack Trees” LNCS, 3935:186–198, 2006.

[22]I. N. Fovino, M. Masera, and A. D. Cian. “Integrating Cyber Attacks within Fault Trees”. Reliability Engineering & System Safety, 94(9):1394–1402, 2009.

[23]S. Bistarelli, M. D. Aglio, and P. Peretti. “Strategic Games on Defense Trees”. LNCS, 4691:1–15, 2007.

[24]B. Foo, Y. S. Wu, Y. C. Mao, S. Bagchi, and E. Spafford. “ADEPTS: Adaptive Intrusion Response Using Attack Graphs in an E-Commerce Environment”. In Proc. DSN, pages 508–517, 2005.

[25]S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley. “RRE: A Game-Theoretic Intrusion Response and Recovery Engine”. In Proc. DSN, pages 439–448, 2009.

[26]黃元平與彭勝龍，「一個攻擊樹之延伸研究」，國立東華大學資訊工程研究所碩士論文，2011。

[27]楊欣哲與彭勝寶，「延伸型攻擊樹分析法以評估網站安全風險之研究」，東吳大學資訊管理研究所碩士論文，2011。

[28]曹偉駿、柯文元、林明孝，「模糊關聯與情境法則探勘於入侵偵測」，2005 年全國計算機會議，台南: 中華民國電腦學會，2005。

Network Threat Analysis and Defense Evaluation

Ping Wang * Jia-Chi Liu**
Department of Information Management, Kun Shan University
Associate Professor * Graduate student**

ABSTRACT

Some network threat analysis approaches regularly assume both the attack scenario and the corresponding impact are known. However, some malware got updated with new features along with its variant appearing leads to the alternation of attack sequences, for example, random filename of download malware; retrieve a domain name based on IP address and random port generation. As a result, defender cannot effectively detect and estimate their impact that affect the correctness of safeguards put in place. Accordingly, the present study proposes a new method for analysis of malware signature problem aggregating Dionaea honeypot system for investigating its malevolent behavior. In the proposed approach, signature reports are sent to compare with CVE(Common Vulnerability and Expose) for a specific virus, ensure that whether the variant got updated with information or not. The probability of virus affection is enhanced by means of frequent episode. Finally, a series of case studies for threat analysis are performed to investigate the attack actions required to successfully estimate the threats from system vulnerabilities thru attack trees. Overall, the results confirm that the proposed method provides an effective means of analyzing the impact losses and selecting suitable safeguards for defenders from malware threats.

Keywords: Information security, Threat analysis, Malware, Variant, Attack trees