楊欣哲、彭勝寶(2013),『延伸型攻擊樹分析法以評估網站安全風險之研究』,
資訊管理學報,第二十卷,第一期,頁 1-38。

延伸型攻擊樹分析法以評估網站安全風險之研究

楊欣哲*
東吳大學資訊管理學系

彭勝寶
東吳大學資訊管理學系

摘要

隨著網路技術的快速發展與 Web 應用系統的普及化,網站系統面臨各種入侵攻擊的威脅,例如:木馬病毒的威脅、DDoS 攻擊、系統和應用程式的弱點攻擊等,皆以破壞網站或竊取敏感性資料為目的。針對當前的各種風險評估方法不能有效地找出系統弱點及攻擊手法,造成評估的結果無法完整表現出真正的威脅途徑。因此,本研究以攻擊樹(Attack Tree)為基礎,延伸應用在風險分析上,利用攻擊樹的特性來描繪攻擊情境,並且設計一個改良式威脅計算演算法,亦即考慮攻擊困難度與偵測防禦度以計算威脅的各種攻擊組合,稱之為延伸型攻擊樹分析法。延伸型攻擊樹分析法可針對各種威脅之影響加以評估,此法有別於一般風險評估,是以「威脅」為單位而不是以「資產」為單位來進行風險評估,可改善一般風險分析法之威脅與描述不足的地方。

本研究以網站系統為例,進行安全威脅分析,獲得網站安全的風險評估等級,證明延伸型攻擊樹分析法可有效地評估網站系統的風險值,以作為系統管理者對資訊安全風險評估之依據。最後,將延伸型攻擊樹分析法與傳統風險分析法作一比較,說明此風險評估方法可以改善傳統風險分析法不足的地方,增加風險評估的可用性及客觀性。

關鍵詞:攻擊樹、延伸型攻擊樹分析法、風險分析、資訊安全、網站安全

* 本文通訊作者。電子郵件信箱:sjyang@csim.scu.edu.tw
2011/05/30 投稿;2012/02/16 修訂;2012/03/26 接受

Yang, S.J. and Peng, S.P. (2013), 'Extended Attack Tree Analysis Method to Assess the Security Risks on the Website', *Journal of Information Management*, Vol. 20, No. 1, pp. 1-38.

Extended Attack Tree Analysis Method to Assess the Security Risks on the Website

Shin-Jer Yang*
Department of Computer Science and Information Management, Soochow University

Sheng-Pao Peng
Department of Computer Science and Information Management, Soochow University

Abstract

According to the fast development of network technology and the popularization of extensive Web applications, Web information system faces various kinds of attacks, such as Trojan virus threats, DDoS attacks, system and application's vulnerability attacks, etc. The target of these attacks is for destroying Websites or stealing sensitive data. A variety of risk assessments for current systems cannot effectively identify possible paths of attacks and system vulnerabilities. Thus, the assessment results do not demonstrate a real threat path. This paper utilizes the concept of attack trees and extends and applies it to security risk analysis. Hence, we employ the features of attack tree to illustrate the situations of attacks to propose an extended attack tree analysis approach. We design an enhanced threats computing algorithm for extended attack tree analysis to calculate threats measure with consideration of attack difficulties and detective protections for assessing their influence levels. In essence, this method is different from the general risk assessment. We use 'threat' as the security unit instead of 'assets' in the risk assessment. It improves the general risk analysis approach about the poor descriptions of threats.

In this paper, we use a Website system as a practical example for the Web system's security threat analysis. We can get a risk grade in Website security risk assessment for system administrator's evaluation basis. It proves that an effective risk value can be obtained from extended attack tree analysis approach for assessing a Website system. We do a comparison for our extended attack tree analysis and the traditional risk analysis approaches. Consequently, the final results indicate that our proposed method can improve the insufficient points of the traditional risk analysis and increase the availability and objectivity in risk assessment.

Keywords: Attack Tree, Extended Attack Tree Analysis, Risk Analysis, Information Security, Web Security

* Corresponding author. Email: sjyang@csim.scu.edu.tw
2011/05/30 received; 2012/02/16 revised; 2012/03/26 accepted

壹、緒論

隨著科技發展的演進，網站的數目與日俱增，各種應用服務的網站漏洞一直以來都是駭客攻擊的首要目標。根據 SANS Top 20（2010）網站所公佈的網頁應用程式（Web Applications）弱點描述，每週都會有數千個弱點被發佈出來，而且企圖攻擊大型網站的數量，每天約有幾十萬甚至到幾百萬次之多。另外根據知名網站 Zone-H（2010）在 2010 年的統計約有 150 萬個網頁被置換攻擊，其中攻擊的手法千變萬化，統計的資料顯示有很多是作業系統或 Web 程式本身的弱點造成，由此可看出目前在網站的安全上存在了許多被入侵的風險。因此，網站系統在面臨各種不同的攻擊威脅環境下，我們必須要思考如何加強網站的安全性，而其中的網站安全的風險管理更是基礎工作。

翁浩正（2010）的研究報告指出一個網站的安全取決於很多因素，如作業系統的版本、網站應用程式的撰寫、架構的設計、使用者的設定等。只要任何一個環節出問題，皆會導致整個網站暴露於風險之中。技術層面來看，管理者必須要時時跟隨系統應用程式的腳步，注意最新的消息、技術和攻擊手法，因應進行修補及防護，才能確保系統處於安全的狀態。在政府網際服務網通報（2010）中公告，目前網頁伺服器仍為駭客主要攻擊目標，駭客攻擊手法主要透過網頁弱點掃描工具、自動化蠕蟲工具或以 SQL-Injection 方式，蓄意穿透各企業內部伺服器群安全防線，竊取資訊或植入後門程式遙控主機。

從OWASP（2010）於2010年發表的網頁應用程式弱點統計中，以跨網站腳本攻擊（Cross-Site Scripting）與資料庫查詢注入攻擊（SQL Injection）分佔前兩名。這二種都是高風險的弱點攻擊，其主要的原因皆為網站開發人員未檢核使用者所輸入的內容，使得輸入的資料內容直接交由程式進行處理，導致網頁程式於運作時，產生改變資料庫內容與植入惡意程式等非預期之結果。另外，在網站攻擊當中，癱瘓網站造成網站服務的停止也是常見的攻擊目的，主要使用分散式阻斷式服務（Distributed Denial-Of-Service; DDoS）的攻擊方式來癱瘓網站，而攻擊手法大都以TCP Syn flood、UDP flood或Smurf attack等方式攻擊。

根據歐士源與黃世昆（2000）的網路攻擊模式簡介中說明攻擊存在兩主體：(1)攻擊威脅源；(2)系統缺陷。若無缺陷就無法構成攻擊，當在構築網路防線時，是在彌補「系統缺陷」的漏洞；而攻擊的另一道防線就是在過濾「攻擊威脅源」之攻擊來源。不過這兩種防禦工事並無法完全抵擋攻擊，最後一道防線是「存活」，存活是被動的防禦。隨著攻擊事件所造成的破壞，進行對應的回復，使破壞的效果降低。

對系統安全性影響最大的是人為的攻擊破壞，其中包括外部和內部的攻擊威

脅。外部的攻擊威脅如駭客攻擊、病毒威脅等；內部的攻擊威脅則有人為的非授權存取與破壞、系統存在的漏洞利用等。但要如何評估網站應用系統的風險呢？目前企業在實作風險評估時，不管是軟、硬體資產，皆是用同一套方法評估，大多以特定項目所訂的風險評估表來評估。但針對軟體資產的風險評估方法，尤其是應用系統的風險評估，每項弱點及威脅事件皆採用條例式，不容易看出資訊系統的弱點或攻擊威脅之間的關聯性，在攻擊威脅的描述上明顯不足。此外，由於駭客攻擊的手法多樣化，但目前風險評估的內容主要是集中在系統的操作面及管理面的風險性評估，如機房安全、管理不當、人為疏失、訓練不足等缺失或弱點來評估可能的風險，並沒有特別針對攻擊威脅的層面去探討和評估。對於這樣多變的網路攻擊手法和途徑也無從評估起，故在這方面相對較為不足。

而且有些攻擊手法是有一連串的步驟，例如只有初期的系統資訊探索步驟，實際上是不構成威脅。但是如果攻擊者已取得弱點資訊並且可能利用此弱點展開攻擊，那麼這將是一個嚴重的威脅。很多類型的威脅或弱點是有系統性的，也就是說由好幾個小漏洞組合起來，才造成駭客可能入侵的機會，因而構成了威脅。故僅靠著系統的某一項弱點，就斷定它會造成資訊系統的威脅，會將威脅風險過度放大的缺點，造成風險評估在有效性上不足，因此評估出的結果並不是很客觀。另外，資訊系統之風險評估，如表 1 所示之範例為例，若以「資產」為單位對風險等級做排序時，常常會發現在不同的資訊系統上有相同的威脅和弱點。但因為兩個資產的價值不同，故評估出來的風險值和風險等級也會不同，變成資產 A 和資產 B 雖有相同的威脅和弱點。但資產 A 為高風險（High Risk）等級，所以威脅和弱點是要立即被改善的，資產 B, D 為低風險（Low Risk）等級，而資產 C 則為中風險（Medium Risk）等級。總之，資產 B 雖然與資產 A 有相同的威脅和弱點，卻可不用急著去改善，在實務上是一個比較不合理的地方。

表 1：以資產為單位之風險評估範例

資產列表	資產價值 (1~3)	衝擊（影響） (1~3)	威脅發生的可能(1~3)	風險值（Risk）	風險等級（Ranking）
資產 A	3	3	2	18	高風險（H）
資產 B	1	3	2	6	低風險（L）
資產 C	2	2	3	12	中風險（M）
資產 D	1	2	3	6	低風險（L）

因此，本論文研究主要目的有以下幾點：(1)改善一般資訊系統風險評估之描述性不足的地方，並且嘗試以不同的評估方式來評估應用系統，不同之處在於我

們是以「威脅」為單位而不是以「資產」為單位來進行風險評估；(2)提出一個風險分析的方法參考，將攻擊樹分析法加以延伸應用在風險分析上。結合風險管理的理論基礎和攻擊樹的特性來描繪攻擊情境，並且設計一個簡單的威脅演算法，以計算威脅的各種組合，此風險分析方法稱之為延伸型攻擊樹分析法；(3)本研究將設計一套風險評估流程與架構，並以網站系統為例。實際運用延伸攻擊樹分析法，從攻擊威脅的層面加以分析網站系統所潛在的弱點和攻擊威脅，並評估網站安全之風險，以提供管理者能夠清楚知道威脅來源，從而找出防範之道。透過系統安全風險評估，我們可以很清楚地了解企業內部的安全需求，可以有效地投資在必要的安全防護上，避免盲目投資的浪費。

本研究將於第貳節針對攻擊樹與攻擊樹分析法進行相關文獻探討；第參節將說明我們設計之風險評估流程與架構，詳細說明延伸型攻擊樹分析法及風險評估之運作流程；第肆節將我們所設計之風險評估流程，實際應用在網站安全威脅的風險評估上。同時分析其評估結果，並與其他風險評估方法做一比較，以說明風險評估之有效性不足的地方；第伍節說明本研究的結論及未來研究的方向。

貳、文獻探討與相關研究

一、風險管理相當介紹

國際標準 ISO/IEC 27005：2008(E) 之風險管理程序中有六個步驟，如圖 1 所示，分別為(1)建立全景、(2)風險評鑑、(3)風險處理、(4)風險接受、(5)風險溝通、(6)風險監控與審查（傅雅萍等 2008）。其中風險評鑑包含了風險分析和風險評估兩部份，而風險分析又包含風險識別及風險估計兩部份。從圖 1 中我們可以清楚地看出風險分析時，必須先識別可能危害系統的潛在風險來源有那些，首先從分析資訊系統本身有所存在的弱點有那些，進而分析這些弱點被利用時可能產生的各種攻擊威脅，才能估計各攻擊威脅發生時對系統造成的影響，然後再評估可能的風險。

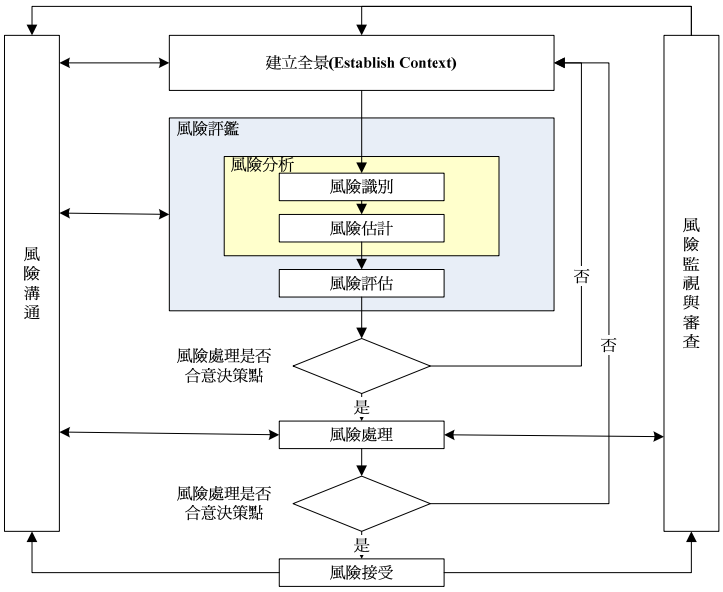

圖 1：ISO/IEC 27005:2008(E) 風險管理程序圖

風險評估是資訊安全管理系統建置流程的關鍵步驟，風險評估的過程是一種：「透過資訊安全政策及資訊安全裝置之選擇，以保護資訊資產免於遭受經由人、設施、硬/軟體、通訊網路、作業系統等之脆弱性而產生安全威脅的傷害。」之方法，其風險評鑑與風險管理關連如圖 2 所示（林勤經等 2002）。

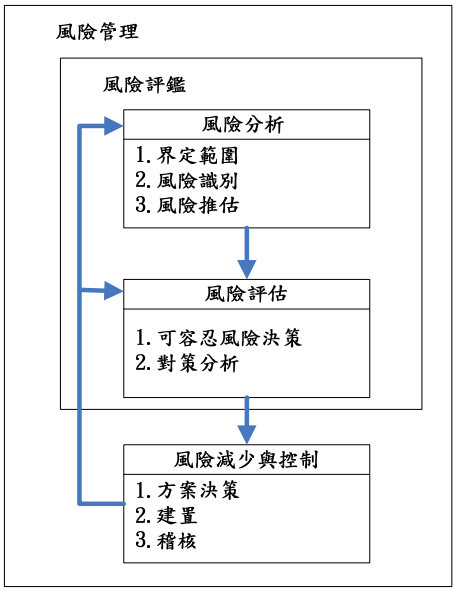

圖 2：風險分析、風險評鑑與風險管理關連示意說明

同時，根據行政院研考會（2009）發行的「風險管理及危機處理作業手冊」，有關資產、威脅和弱點三者的風險管理概念關聯圖，如圖 3 所示。風險的產生是因為資產弱點受到威脅的攻擊造成對資產價值的降低。若增加適當的控制措施則可降低風險的發生，資產、威脅和弱點三者的關係為一動態模式，隨著威脅來源的增加，系統必須適時增加防護措施，才可以維護資產的價值。由此看出面臨當前多變的攻擊方式，如果無法正確識別出威脅來源及弱點，則威脅對資產的影響，將造成評估結果的失真。

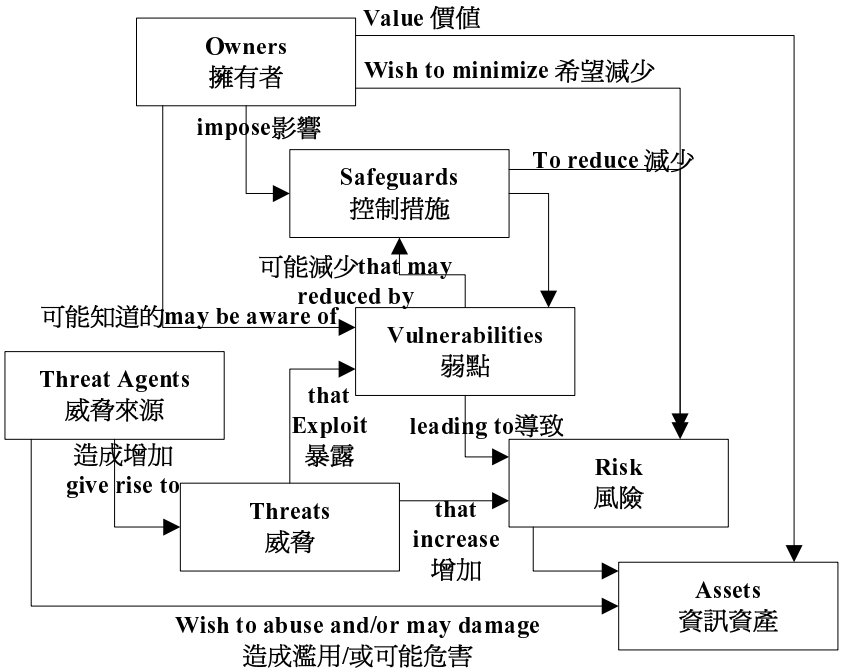

圖 3：風險管理概念關連圖

在資訊系統安全管理中對於系統威脅與對策主要有四個步驟，如圖 4 所示。首先，必須確認可能攻擊的威脅，然後定義威脅所造成的風險，接著針對威脅等級順序建立資訊安全政策，最後再執行降低風險的各種控制手段。由這四個步驟可以看出，資訊系統的安全管理就是要找出系統的威脅所在，並且透過風險管理的程序來降低威脅所造成的風險，這與本研究的理論基礎是相同的。

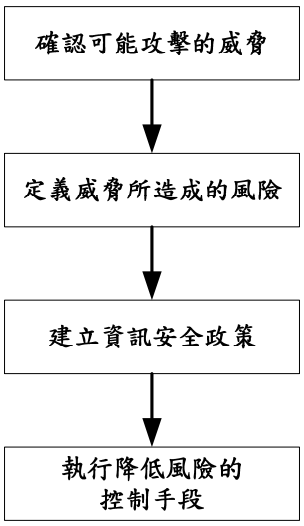

圖 4：資訊系統安全管理的四個步驟

根據 Microsoft TechNet（2006）網站所提供的資產威脅理論模式，可用來說明針對特定資產遭受到的不同威脅所利用之動機與目標、方法及漏洞。圖 5 中說明三種威脅分類的類型，包括無惡意的潛在威脅、惡意的潛在威脅及災難性事件等三種類別，以及這些威脅在危害資產時的可能途徑，並顯示威脅可能會使用的特定工具、技術及方法，利用資產安全性中的某些弱點。圖中的箭頭說明攻擊者企圖危害資產時所採取的路徑，以及可能利用的弱點。其中惡意的潛在威脅是一個可怕的攻擊情境，具有企圖的動機和達成的目標。攻擊者的攻擊動機通常是具有某方面的利益或目的，同時會鎖定特定的攻擊目標，運用各種不同的工具、技巧或方法。透過系統本身存在的漏洞或者不足的安全性控制與原則設定，對資產造成危害，甚至繞過安全性控制與原則設定，直接攻擊資產，那麼對資產的機密性、完整性或可用性造成嚴重衝擊。因此，要是能夠觀察到特定攻擊所利用的弱點，就可以更改現行或實作新的安全性原則及控制，將弱點減到最少。

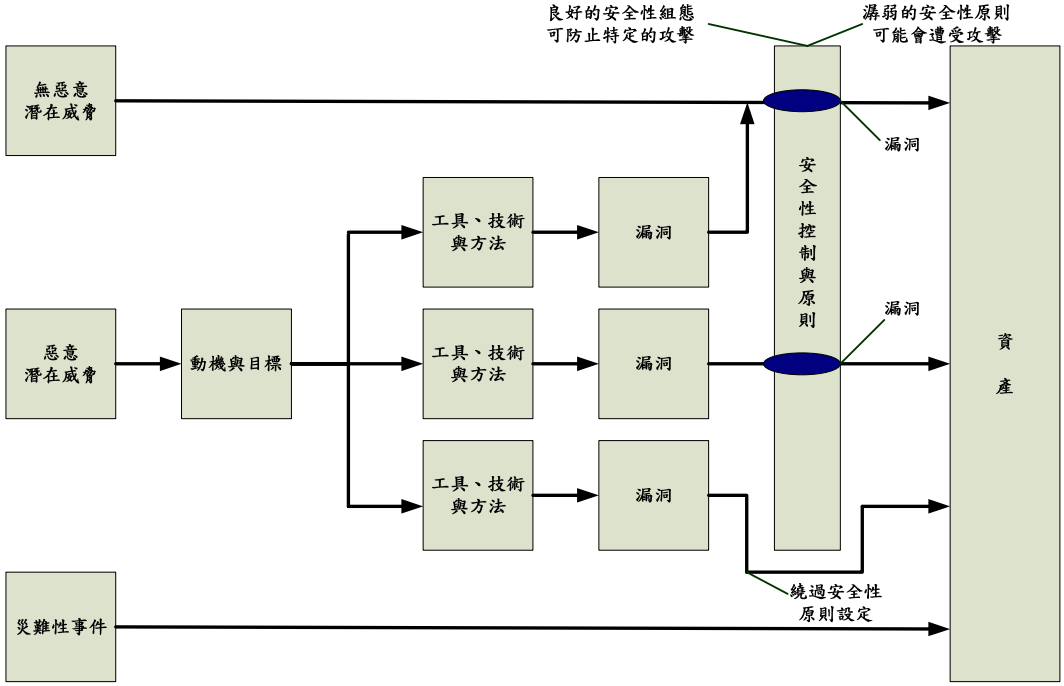

圖 5：資產威脅理論模式（Microsoft TechNet）

另外，樊國楨、林樹國與朱潮昌（2008）在資訊安全風險評鑑的研究中，更詳細說明駭客使用各種攻擊工具、技術、方法等手段。經由資訊系統暴露之脆弱性，造成資訊資產之機密性、完整性、可用性之損失。當資訊系統暴露的弱點被攻擊者利用構成了威脅，而威脅等級的不同，其影響到威脅發生的後果衝擊也不相同。因此在防護策略上，針對資訊系統所暴露的脆弱性，應該有防範的具體措施，在日常的維運當中，應定期更新修補系統漏洞；並且在威脅的衝擊之下，也應有良好的防護對策，定期檢視威脅的變異，做好風險管理的控制。因此，對重要的關鍵系統作出弱點及威脅分析，進而以系統化的風險分析方法，從威脅的角度審視系統上存在的安全問題，做好資訊安全的風險管理，以使風險評估的結果更具客觀性及可行性。

二、攻擊樹介紹

目前資訊安全在實作風險分析的方法有很多種，而本研究將以樹狀結構（Tree Structure）來做為風險分析的呈現方法，並評估資訊系統的弱點及威脅，故以攻擊樹作為風險分析的基礎結構，以下就此法加以說明。攻擊樹（Attack Tree）模型是由 Schneier（1999）提出的一種描述系統安全的方法，它是利用樹狀結構來描述系

統受到的安全攻擊，根節點是攻擊目標，達到目標的不同方法則用葉節點表示，非葉節點表示攻擊的各子目標，包括“與”（AND）、“或”（OR）兩種類型，分別表示要達到攻擊目標所需要滿足的子目標之間的邏輯關係，例如，攻擊者能夠實現「AND」類型的節點所表示的目標的條件是其相關的子節點對應的子目標全都要滿足，「OR」類型的節點則是滿足任意一個子目標即可。參考有關攻擊樹的AND/OR 節點表示，如圖 6 所示。

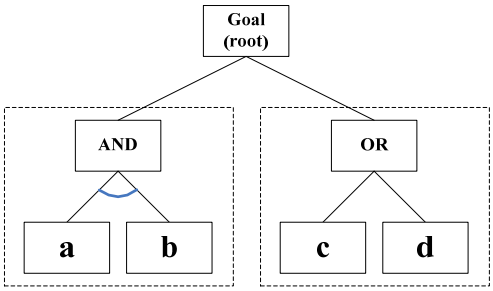

圖 6：攻擊樹 AND/OR 節點表示

攻擊樹分析法（Attack Tree Analysis; ATA）也有人稱之為威脅樹分析法（Threat Tree Analysis; TTA），它的特點是可描繪出系統遭受攻擊所面臨的安全威脅，並描述可導致系統安全事件的集合。Schneier（1999）更說明了攻擊樹分析法提供一個有效的方法論，可應用在系統和子系統的安全性分析上，它提供了一個安全性思考的方法，在安全上可以獲取和重覆使用專門的知識和技術，而且也可以反應出威脅的改變。安全它不是一個產品而是一種程序（process），而攻擊樹的形式是瞭解安全程序的基礎。

圖 7 為一個簡單的系統攻擊樹範例說明，其中最上層的根節點代表攻擊的目標，主要是要獲取系統的存取權限；而底層的葉節點代表要獲取系統存取權限之攻擊目標所使用的方法，例如：「猜帳號」及「猜密碼」兩個攻擊手法必須同時成立才能獲得登入系統的帳號密碼，否則無法登入系統。因此，單一項成立並不構成威脅，但如果同時取得帳號及密碼時，自然可以入侵系統取得存取權限，故對系統構成威脅。而中間的非葉節點表示攻擊的子目標，依其 AND 或 OR 的邏輯關係而定，例如：要成功完成「竊取帳號密碼」之子目標，該非葉節點為 OR 的邏輯關係，故只要子節點其中一個攻擊手法成功就可以達成，如使用「中間人攻擊」（Man in the Middle Attack）手法取得系統權限之帳號密碼。

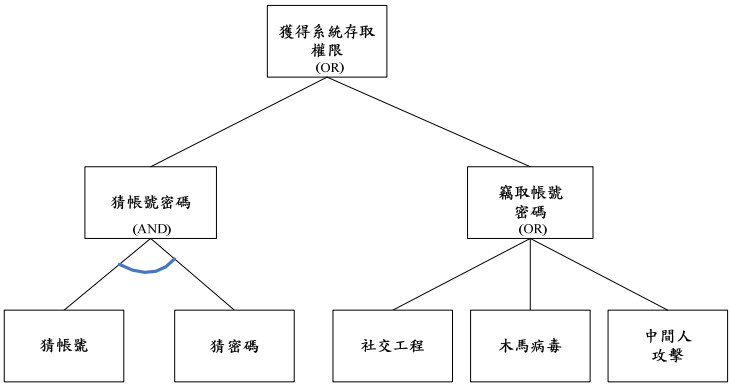

圖 7：一個簡單的系統攻擊樹範例

三、攻擊樹相關應用研究

目前以攻擊樹分析法應用在資訊安全的風險評估尚不普遍，大都是應用在入侵偵測之威脅分析或系統弱點評估上，主要是因為在分析較複雜的攻擊行為，必須依賴資安專家或有經驗的系統安全人員，才能建構出一個完整的攻擊樹表示。參考相關研究文憲，在威脅評估方面的研究中，有研究學者提出一套威脅分析模型，主要在評估網路系統的威脅和脆弱性（Stango et al. 2009）；其風險評量是利用攻擊樹以 CVSS 來評級區分其影響等級，並且優先處理威脅和脆弱性來提升個人網路的安全，其提出的威脅分析模型，如圖 8 所示。

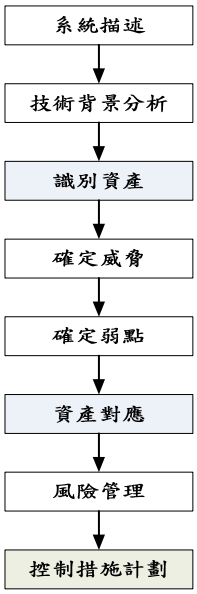

圖 8：Antonietta Stango 等人之威脅分析模型

首先，必須要了解系統相關資訊及環境並加以描述，然後分析可能的技術背景及識別資產類別，並分析潛在的威脅來源和系統本身存在的脆弱性。接下來的資產對應主要在於評估資產的價值，透過分析出的威脅、弱點和資產價值等資訊加以風險評估。最後，再依據風險評估結果之風險水準，做出改善的控制措施。

此外，Li 與 He（2008）、Li 等（2009）將威脅樹模型延伸應用在軟體設計階段，利用所設計攻擊路徑演算法找出攻擊路徑，設計威脅評估演算法來分析和評估威脅，以減少應用程式在開發完成後可能面臨的威脅；此外利用威脅模型來設計攻擊路徑評估演算法，加入損害及發生可能性的相關權重，來估算每個威脅發生的機率，發生的機率愈高代表愈須要加強防護。另外，楊尚青與王憶魯（2009）的研究以蒐集偵測及預防遭受攻擊之相關資料，針對具有高度的複雜性與不確定性的內部威脅行為，進行分析與偵測，以定期完成威脅評估報告為主。

在弱點評估方面的應用，賴義鵬與周世益（2009）之研究以弱點評估方式來提升資訊系統安全需求，其結合通用弱點評估系統（CVSS）的資訊，用於主機上弱點的評估、分析與推測，協助安全人員分析主機的安全性。此外 Wang、Liu 與 Jajodia（2006）利用 Nessus、Nmap 等類的弱點掃描軟體，針對入侵偵測系統所管理的電腦進行掃描的動作，找出各電腦系統存在的弱點。針對這些弱點事先建立網路攻擊圖（Attack Graph），並將此網路攻擊圖轉成佇列圖（Queue Graph），再利用此佇列圖來關聯入侵偵測系統所產生的警訊。另外 Moberg（2000）提出一個利用攻擊樹法應用於資訊系統的安全性分析方法，此方法的工作流程如圖 9 所示。首先定義出威脅來源及途徑，然後將定義的威脅建構成攻擊樹，再以樹狀結構來分析各個攻擊節點。攻擊樹可以清楚描繪出攻擊路徑，並且讓我們可以徹底地了解威脅的途徑，能夠集中心力在目標系統上，處理攻擊可能利用的弱點。

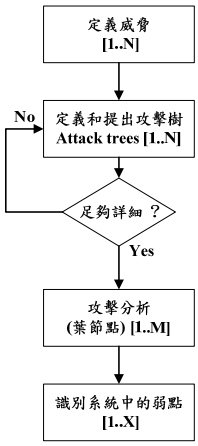

圖 9：Fredrik Moberg 之系統安全性分析步驟

目前攻擊樹的研究與應用愈來愈廣泛，如 Edge 等（2007）的研究使用攻擊樹（Attack Trees）和防禦樹（Protection Trees）評估網路銀行系統的安全，主要方法是從攻擊樹中得到系統的脆弱性，另外再以防禦樹來保護這些系統的脆弱性，其中攻擊樹和防禦樹的表示方法剛好是相反，攻擊樹的 AND 邏輯節點關係剛好是防禦樹的 OR 節點能夠滿足。反之，攻擊樹的 OR 邏輯節點關係剛好是防禦樹的 AND 節點能夠滿足，並以攻擊及防護成本分析提供防護策略以降低風險。另外，Dimitriadis（2007）利用攻擊樹分析網路銀行的認證機制之安全性，以了解認證機制存在的那些弱點並建議採取有效的控制措施。Gan 等（2007）學者將攻擊樹加以改良應用，除了基本的 AND/OR 邏輯關係以外，再改進增加一個 CAND(Conditional AND）的邏輯關係，並以攻擊鏈（Attack chains）表示為一系列的攻擊行為，此法稱之為擴展攻擊樹（Extended Attack Tree）。此外，Jin、Wang 與 Tan（2010）學者也提出相關的攻擊樹擴展應用，主要是以攻擊樹之基本的 AND/OR 邏輯表示之外，並付與每一個節點不同的屬性值。然後，透過每個節點的邏輯性和屬性加以匹配標記出攻擊節點，並且應用在偵測特洛伊木馬程式上。

實際上，我們不太可能識別出所有可能的威脅，我們有可能會忽略某些威脅，其主要原因是它們發生的幾率可能很小或者是事件的發生所造成的損害微乎其微。因此，本研究之威脅和弱點分析主要是協助我們了解資訊系統面臨的攻擊型態，方便我們建立攻擊樹模型，進而可以有效評估每一個攻擊節點。面對越來多的各種不同攻擊威脅，需要一套有效的防護機制及安全，特別是企業中關鍵的資訊系統，更應該做好資訊系統安全的風險管理以及威脅分析。該如何做好這方面的分析評估制度及制定有效的防護策略，這是目前的當務之急。

參、風險評估流程與延伸型攻擊樹分析法之設計

一、風險評估流程與架構說明

由於駭客攻擊的手法多樣化，嚴重威脅到網站系統的安全，因此，本研究依據圖 1 ISO 國際標準之風險管理架構，主要分為風險識別、風險分析及風險評估三個部份，加上風險評鑑結果後的風險處理這部份，設計網站安全風險評估流程，其架構如圖 10 所示。

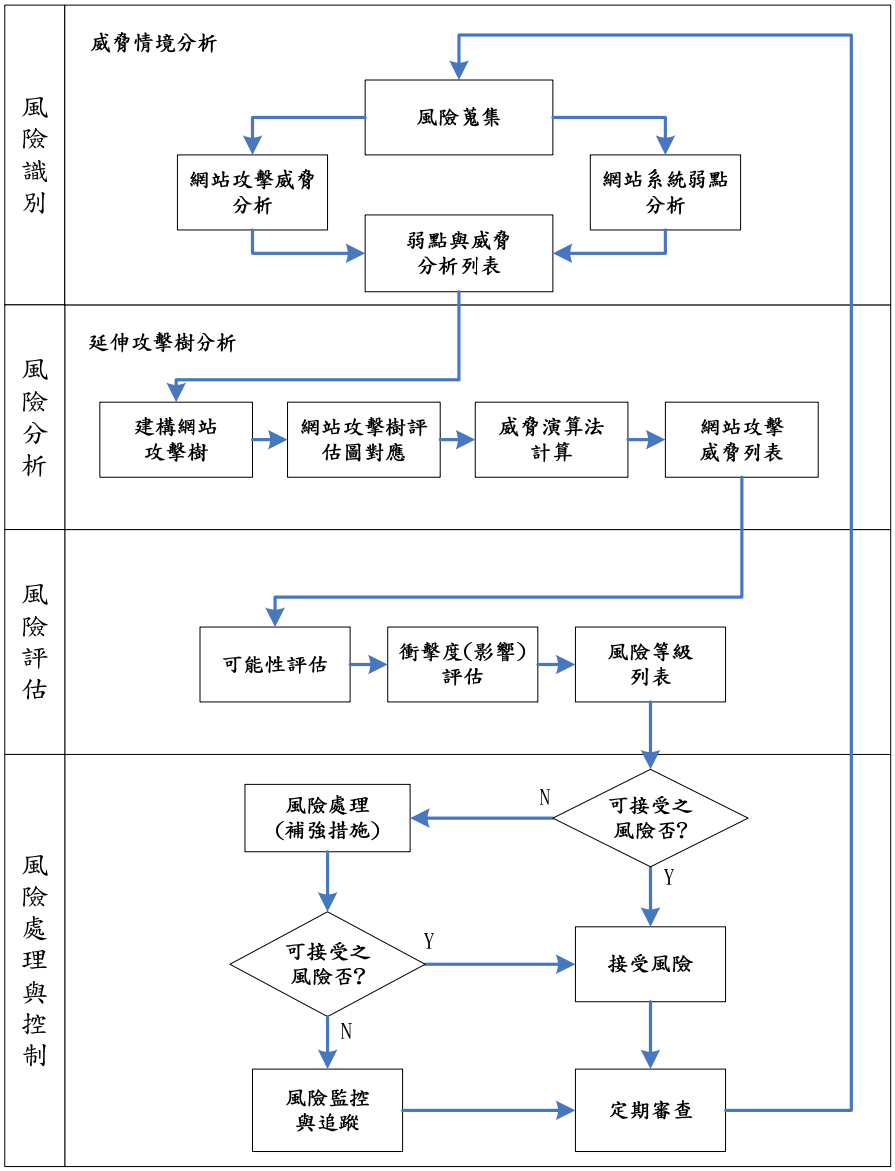

圖 10：網站安全風險評估流程與架構（本研究）

此風險管理流程主要集中在風險分析及風險評估兩步驟上，嘗試以不同的方式來評估網站應用系統所面臨的威脅，提供給企業在實作風險評估的參考。其中風險分析法是利用本研究所提出的延伸型攻擊樹分析法。因此，本研究所設計的網站安全風險評估流程主要可分為四個階段：

第一階段為風險識別：在風險識別這個階段，我們首先要蒐集網站的可能風險有那些，應該徹底瞭解所有相關的風險包括威脅的種類與利用的弱點，在這我們將此部份稱為攻擊情境（Attack Scenarios）分析，從現有攻擊手法和系統存在之

弱點來分析，然後評估每一個威脅事件可能造成的損害程度，如果不構成損害的威脅事件可以剔除，以減少後續的評估的複雜性。然後會整理出一個弱點與威脅列表提供下一階段建構攻擊樹。

第二階段為風險分析：在風險分析這個階段，我們將運用所提出的延伸型攻擊樹分析法加以分析，透過前一階段所找出的風險因子列表建構一個完整網站攻擊樹，此攻擊樹我們再轉換成風險評估圖。依據攻擊目標、子目標、系統的弱點及攻擊手法加以分類表示，再將此攻擊樹評估圖利用威脅演算法計算，找出所有可能的威脅組合及列表，以利下一階段評估各個可能威脅的風險。本階段所建構的網站入侵攻擊樹，可以幫助我們了解所有的威脅型態是如何，對於改善安全防範會有很大的幫助。

第三階段為風險評估：在風險評估階段，我們必須利用前一階段所找出的可能威脅列表，針對每一個可能威脅加以評估。評估的項目主要分為兩個部份，第一個部份是可能性的評估，其主要在評估威脅發生的可能性機率，另外一個部份是影響性（衝擊）評估，其主要在評估威脅發生後其系統對企業造成的衝擊或發生後果的影響，我們依據此兩個評估結果對應出每一個可能威脅的風險值及風險等級。

第四階段為風險處理與控制：在評定出每個威脅的風險等級後，我們必須評估每一個可能的威脅是否為可接受的風險，如果未達可接受的風險等級時，則必須另外提出風險處理及控制對策以降低風險，最後再定期監控與追蹤風險。

二、延伸型攻擊樹分析法之步驟及演算法

本研究所提出之延伸型攻擊樹分析法，是將攻擊樹加以延伸應用在風險分析上，結合風險管理的理論基礎和攻擊樹的特性來描繪攻擊情境，結合各種不同面向的攻擊樹，在將此完整的攻擊樹對應到評估圖中，並且設計一個簡單的攻擊樹威脅演算法，以計算出可能的各種威脅組合，然後列出來做為風險評估之標的，其架構如圖 11 所示。

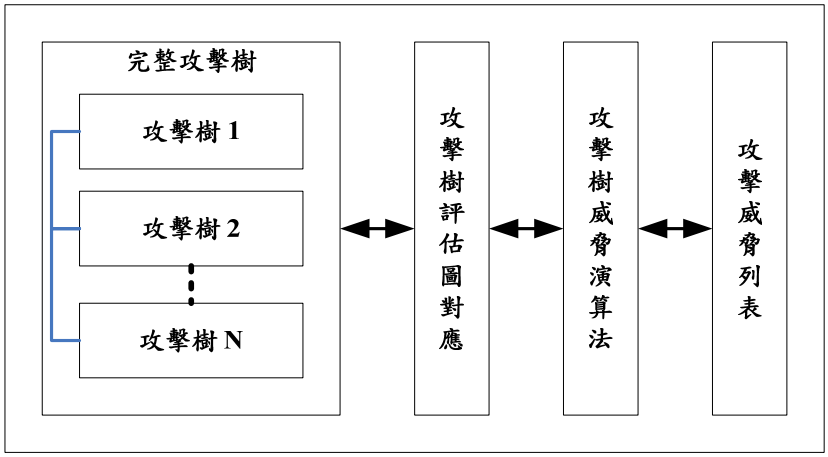

圖 11：延伸型攻擊樹分析法架構

延伸型攻擊樹分析法依據系統弱點及威脅分析的結果，建立各種不同面向的攻擊樹。此攻擊樹利用樹狀結構來描述系統遭受到的可能攻擊，其中最上層的根節點是攻擊目標，而要達到攻擊目標的攻擊手法則用葉節點來表示，而中間的非葉節點表示攻擊的子目標或是威脅利用的弱點。因此，由建構出的各個攻擊樹整合成一個完整的攻擊樹，再將完整攻擊樹對應到風險評估圖。為免攻擊樹分枝過於複雜造成評估上的困難。我們會依據目標、子目標、弱點、攻擊（威脅）等四個階層來區分攻擊樹的結構，以方便計算威脅的數量及後續的風險評估，圖 12 為攻擊樹風險評估 Layout 圖範例。

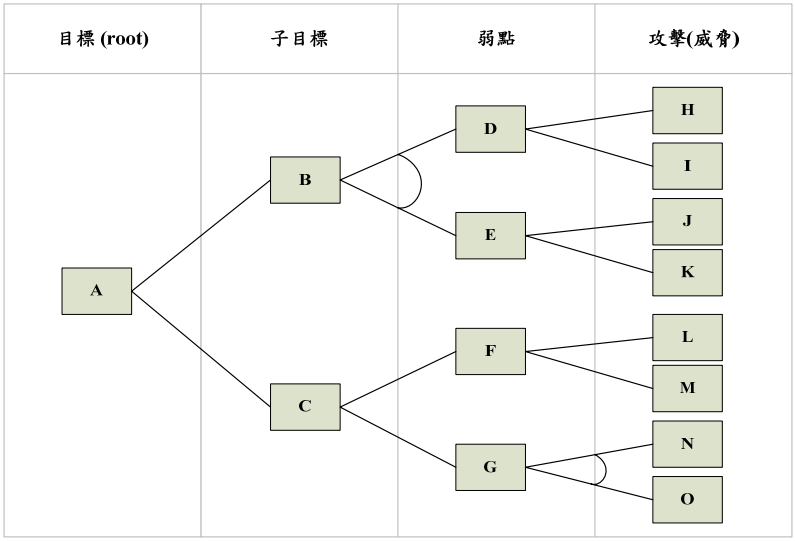

圖 12：攻擊樹風險評估 Layout 圖範例

接下來，將說明攻擊樹威脅演算法，如圖 13 所示為本研究的演算法設計，演算法由下而上推導計算至最上層的根節點為止，而所推導出的根節點值，其所代表的意義即是為達成攻擊目標的所有可能攻擊手法。

```
     Algorithm Compute_Attack_Paths(Tr)
     Input: An Attack Tree T with r being the root
     Output: path(r)
1.   if r is the only node of the tree T then
2.        return path(r)=1
3.   else
4.        let v1,..., vk be the k children of r
5.        for i = 1 to k do
6.             Compute_Attack_Paths(Tvi)
7.        endfor i
8.        do case
9.             case 1: r is an OR node
10.                  return path(r)=∑ path(vi)
11.            case 2: r is an AND node
12.                  return path(r)=Π path(vi)
13.       endcase
14.  endif
```

圖 13：攻擊樹威脅演算法（本研究）

以圖 14 範例說明攻擊樹威脅演算法的計算原理。在此，我們以「＊」號代表「AND」的關係，以「＋」代表「OR」的關係。依據攻擊樹威脅演算法的設計來量化威脅的組合，我們必須在每個葉節點{a、b、c、d、e、f、g、h}給定一個初始值 Path=1，此初始值等於 1 的意義為每一個葉節點代表一種攻擊手法，而一種或多種攻擊手法的結合構成了可能的威脅。當我們遇到上層節點的關係為「AND」邏輯關係時，代表所有的子節點皆必須成立（為真），上層的父節點才能成立（為真），因此，在此邏輯關係下的組合有多少種呢？由圖中的 g 節點和 h 節點可看出，當兩者皆成立時則視為一個威脅組合，故我們的演算法設計為各子節點的權值相乘。如果我們遇到上層節點的關係為「OR」邏輯關係，代表只要其中一個子節點成立（為真），上層的父節點就成立（為真），因此，在此邏輯關係下的組合有多少種呢？由圖中的 a 節點和 b 節點可以看出，當兩者皆成立時則有二個威脅組合，故我們的演算法設計為各子節點的權值相加。最後，由下而上推導計算得出可能的攻擊威脅共有 6 種組合（Path(r)=6），表示如果要達成攻擊網站的頂端目標，總共有 6 種攻擊組合。以本例為例共有 6 種威脅組合（攻擊手法），其攻擊組合分別是{a,c,d,e}、{b,c,d,e}、{a,c,d,f]、{b,c,d,f}、{a,c,d,g,h}、{b,c,d,g,h}，

故每一種組合即代表一種威脅。

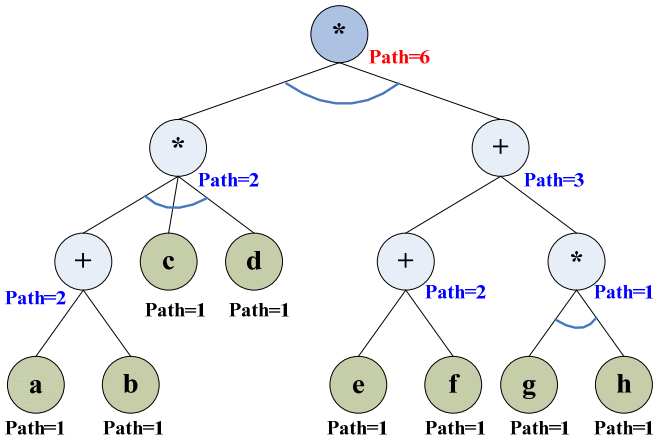

圖 14：攻擊樹威脅組合的計算推導

三、量化風險等級評估說明

本研究將以攻擊事件的角度來評估每一個威脅所帶來的風險（Risk），而風險值的計算是依據風險管理的標準定義，每一個威脅的風險值等於可能性機率乘上事件發生的影響性也就是衝擊度（Risk = Likelihood＊Impact），但實務上要評估每一個威脅攻擊的可能性機率和衝擊度時，有一定的困難度和複雜性。因此我們參照 OWASP（2010）的風險等級方法論，將可能性機率與衝擊度依據評估的機率範圍值對應得出一個等級；而其中可能性（Likelihood）表示威脅發生的可能性機率有多高，從攻擊與防禦的角度思考，考慮現有安全防禦等級，從可被偵測及防護的程度，以及在攻擊面的困難度，例如攻擊的手法、花費的成本……等等來評估，從攻防兩個構面來評估發生威脅的可能性機率，我們將可能性等級的評估分數分為 1~5 個等級，如表 2 所示。其中有關可能性（Likelihood）之風險分數計算，請參照公式(1)之定義。

$$\text{Likelihood} = f(attack, protection) \tag{1}$$

其中 *attack*：表示攻擊困難度（很容易、容易、中等、困難、很困難）。

protection：表示偵測防禦度（很容易、容易、中等、困難、很困難）。

表 2：可能性等級評估表

可能性等級		攻擊困難度									
		很難 (1)		困難 (2)		中等 (3)		容易 (4)		很容易 (5)	
		分數	等級	分數	等級	分數	等級	分數	等級	分數	等級
偵測防禦度	很容易 (1)	1	1	2	1	3	1	4	1	5	1
	容易 (2)	2	1	4	1	6	2	8	2	10	2
	中等 (3)	3	1	6	2	9	2	12	3	15	3
	困難 (4)	4	1	8	2	12	3	16	4	20	4
	很難 (5)	5	1	10	2	15	3	20	4	25	5

另外，衝擊度（Impact）表示這個威脅的發生會對系統影響的程度，由於機密性、完整性和可用性任何一項的損壞都有可能造成企業營運的衝擊或損失。我們可從機密性、完整性和可用性三個層面來評估影響性等級，在機密性上的影響可能導致資料的外洩及不當的授權等，在完整性上的影響可能導致內容被篡改或植入惡意程式，在可用性上的影響可能導致服務中斷或系統當機，所以駭客如果攻擊成功，會對網站系統造成某種程度的傷害，例如系統遭受外在的 DDoS 攻擊時有可能造成系統的可用性喪失，或者 SQL Injection 攻擊可能造成系統的機密性或完整性的喪失，但影響程度不一。因此，我們將增加權重（Weight）項目，其權值範圍為（0~1），若權值為 0 代表此項不影響，然後再將影響系統之機密性、完整性及可用性三項加總起來，最後，再依加總分數對應出相對應之影響性等級，其中有關衝擊度（Impact）之影響性風險分數計算，請參照公式(2)之定義，在此影響性等級共分為 1~5 個等級，如表 3 所示。

$$\textbf{Impact} = E_c * W_c + E_i * W_i + E_a * W_a \tag{2}$$

其中 E_c：表示影響系統機密性（Confidentiality）之分數。
E_i：表示影響系統完整性（Integrity）之分數。
E_a：表示影響系統可用性（Availability）之分數。
W_c：表示影響系統機密性（Confidentiality）之權重。
W_i：表示影響系統完整性（Integrity）之權重。
W_a：表示影響系統可用性（Availability）之權重。

表 3：影響性等級評估表

影響性	機密性（C）	完整性（I）	可用性（A）	C+I+A	影響性等級
極低影響	$1 * W_c$	$1 * W_i$	$1 * W_a$	0 ~3	1
低影響	$2 * W_c$	$2 * W_i$	$2 * W_a$	4 ~ 6	2
中影響	$3 * W_c$	$3 * W_i$	$3 * W_a$	7 ~ 9	3
高影響	$4 * W_c$	$4 * W_i$	$4 * W_a$	10 ~ 12	4
極高影響	$5 * W_c$	$5 * W_i$	$5 * W_a$	13 ~ 15	5

最後，評估各種攻擊威脅發生的可能性及威脅發生對系統的影響（衝擊），並按照風險值（Risk＝Likelihood＊Impact）計算的結果來判定風險等級，從圖 15 中的風險矩陣即可看出風險值及風險等級的對應關係。按照每個威脅的風險值大小來排定威脅排行，以做為優先改善的順序，從「風險管理矩陣」中評估威脅發生的可能性及其對系統的影響，風險的等級會隨著威脅發生的可能性及影響性增加而變高。

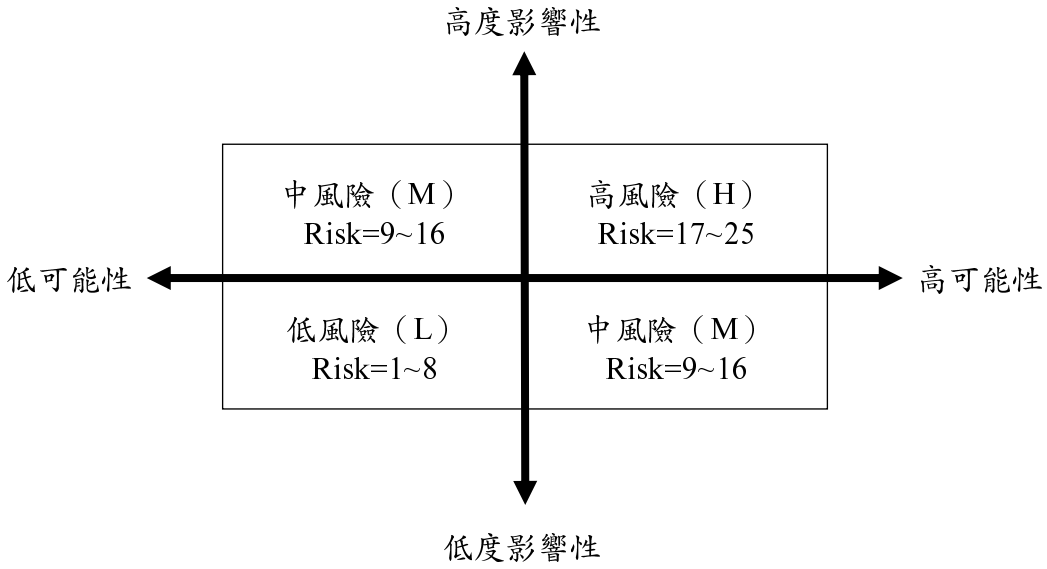

圖 15：風險矩陣

由於在企業中每個應用系統的重要性不同，故其對企業的影響程度也不同，因此透過風險評估小組的評估，如表 4 所示，評量出每一個威脅的風險值及威脅排行。從威脅排行的優先處理順序可以得知威脅 C 其風險值最高，其是透過 a, c, d, f 四種攻擊手法組合而成因。我們針對威脅 C 必須優先處理並加以防範，其次才是

威脅 E 和威脅 A...等以此類推。此外，從整體的網站系統之風險值去評估是否為可接受的等級，如果為不可接受之風險等級則必須加以改善。

表 4：網站系統威脅之風險評估結果範例

威脅組合		可能性等級（1~5）	影響性等級（1~5）	風險評量	風險等級	威脅排行
威脅 A	{a,c,d,e}	3	3	9	M	3
威脅 B	{b,c,d,e}	3	1	3	L	4
威脅 C	{a,c,d,f]	5	4	20	H	1
威脅 D	{b,c,d,f}	1	2	2	L	5
威脅 E	{a,c,d,g,h}	3	4	12	M	2
威脅 F	{b,c,d,g,h}	4	3	12	M	2

肆、網站系統風險評估實證與結果分析

一、網站安全威脅情境分析

根據 SANS 組織的統計在網站系統的弱點利用，以網頁應用程式的弱點利用為主要的攻擊目標，評估網站系統的安全性，應著重在網路上的安全威脅為主。然而各種弱點產生的威脅嚴重程度不同，大部份都是參考 OWASP 將弱點分類並標示嚴重等級，例如 XSS 及 SQL Injection 是歸類為高風險的弱點。將弱點等級分類的好處在於，幫助企業將資源投入在真正需要的地方，例如低風險的弱點，未必會造成威脅，就可以排出處理的優先順序。

通常網站架構多採 3 層式（3-tier）或 N-tier 架構。前端為 Web Client 執行 Browser，中間端為 Web 伺服器，利用網頁應用程式開發使用者介面，並與後端資料庫連接。我們參考 OWASP Top 10（2010）及 SANS Top 20（2010）之網站所公佈的 Web 應用系統弱點攻擊，整理出常見的攻擊型態，目前一般網站伺服器（Web Server）的主要潛在威脅包括：資料外洩、拒絕服務、網頁竄改、未授權存取、任意執行程式碼、權限提升、木馬病毒及蠕等。本研究所分析之 Web Server 架構及常見的弱點與攻擊手法，如圖 16 所示。

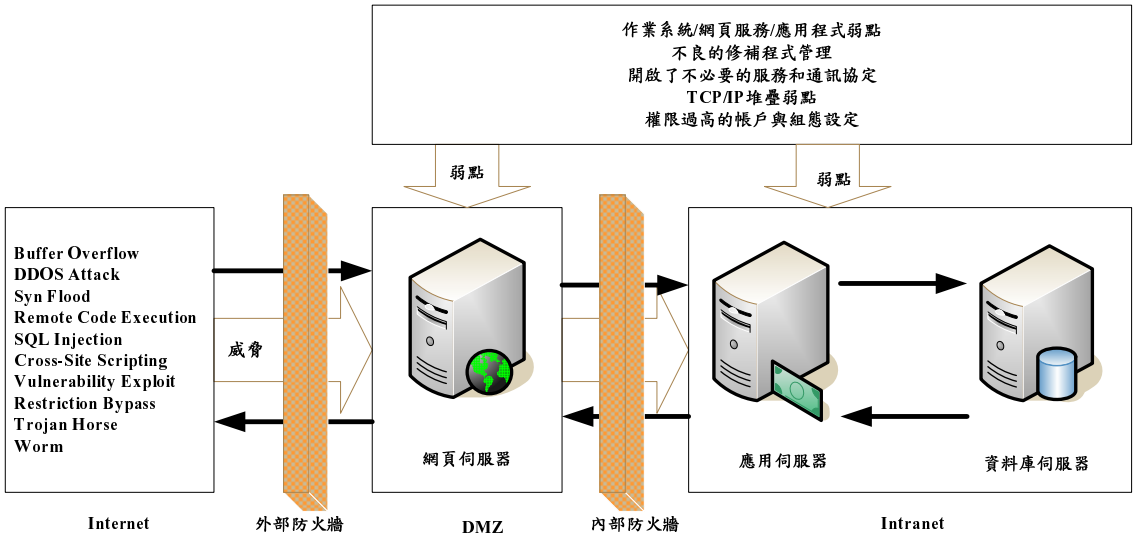

圖 16：Web 伺服器架構及常見弱點與潛在威脅攻擊

一個網站的安全與否取決於很多因素，多數的網站攻擊威脅都是利用應用程式和系統漏洞散播，只要任何一個環節出問題，都會導致整個網站暴露於風險之中。如果網路不安全，網站系統及應用程式的安全性肯定不高。反之，無論網路的安全性再高，管理得再好，只要應用程式不安全，駭客還是有辦法攻擊的。因此要讓各個構面的安全防護能夠面面俱到，並不是一件容易的事。本研究將網站系統的安全區分為主機系統安全、網路安全及網頁應用程式安全三個部份來評估，針對三個構面之安全弱點威脅製作攻擊情境分析，以利後續建立攻擊樹及安全風險評估，分析如下：

（一）主機系統安全

主機系統主要包含了作業系統（Operation System）及網站服務（Web Service）兩者，而目前的網站服務程式主要是 Apache 與 IIS（Internet Information Server），但 IIS 和 Apache 的漏洞也經常被當作是駭客攻擊對象以取得存取權限。而一般弱點掃瞄服務會採用通用弱點和漏洞（Common Vulnerabilities and Exposures; CVE）編號表示，通用弱點和漏洞（CVE）為國際公認之弱點漏洞編號標準，其特點為將每個已知的漏洞，訂定一個唯一的名稱，並且為每個已知的漏洞，提供一個標準的描述，主要在於統一名稱，其編號格式為 CVE-xxxx-xxxx（xxxx 為四位數字）。CVE 格式中第一組數字表示年度，第二組數字表示該年度第幾個被發現的安全弱點，這個作法的好處是使安全評估報告更容易被理解與解讀，同時各廠商所提供的漏洞資料庫，能有較佳的相容性。然而，作業系統存在的漏洞和伺服器管理配置不當，是導致網站被入侵的兩大風險因素，因此攻擊者要攻擊成功，主機系統

的弱點修補是重要關鍵。

攻擊者可利用外部掃描工具，對 Web 伺服器進行掃描，看看是否有存在可以被利用的服務或漏洞。例如：在伺服器安裝的時候，作業系統預設會安裝並啟動一些不需要的服務；或者在伺服器配置的時候，需要啟動一些服務，但是事後卻沒有及時的關閉，使得提供不法攻擊者可利用的機會。最常見的如 SNMP 服務，這個服務在系統安裝完畢後，系統預設是開啟的。但是，這個服務可以為攻擊者提供伺服器系統的詳細資訊，如 Web 伺服器是採用了什麼作業系統，在伺服器上開啟了什麼服務與對應的埠等等寶貴的資訊。攻擊者只有瞭解這些最基本的資訊之後，就能夠開展攻擊。

由於系統的配置不當導致不必要的通訊協定及服務被開啟，造成了可被利用的管道，通常很多的攻擊透過遠端命令執行，以取得網站系統主機權限，使得惡意攻擊者可執行受害者主機的任何程式。甚至最基本的帳戶密碼設定原則，如果沒有嚴謹的密碼設定要求及定期變更密碼的規範，則很有可能用戶使用的是弱密碼登入（例如："123456"、"password"或是 changeme"或者任何字典之單字等等），那麼駭客便能快速地破解使用者的密碼，並可以很簡單的就能盜用這些用戶的帳號入侵系統，那麼這些配置不當的設定，都是導致被威脅利用的弱點。

此外，由於系統本身弱點未修補更新，透過病毒的感染而被植入的惡意程式，讓病毒及惡意程式可以伺機破壞系統，使得大量的機敏資訊遭到竊取。甚至是蠕蟲、木馬、病毒及駭客工具所組合成的混合式攻擊，利用病毒程式來感染。特洛依木馬程式的隱匿入侵，加上蠕蟲的迅速散播和間諜程式高超的偽裝技巧，都有可能使網站系統出現重大的安全威脅。因此，主機系統安裝防毒防駭軟體已經是不可欠缺的基本要求，透過以上的弱點及常見威脅分析，本研究整理出常見對主機系統安全的幾個重要威脅（攻擊手法），如表 5 所示。

表 5：主機系統安全威脅分析

編號	弱點	威脅	威脅描述
A1	權限管理不當	未授權的存取（Unauthorized Access）	非合法的使用者取得受限制的權限，使得可以未經授權而存取系統，或者執行一些不當的作業程序，造成資料外洩或損害系統。
A2	權限管理不當	權限提升攻擊（Elevation of Privileges Attack）	權限提升攻擊是由於設定過大權限的服務帳號（Service accounts）或程序帳號（Process accounts），當攻擊者要執行一些不當的作業程序時，會使用這些被提升權限帳號，造成資料外洩或損害系統。

編號	弱點	威脅	威脅描述
A3	弱密碼管理	暴力密碼攻擊（Brute-force Attack）	以不斷的輸入密碼重複嘗試，直到破解為止，此攻擊亦能取得可用帳號，用來修改重要系統檔案與服務，破壞系統的完整性。
A4	弱密碼管理	字典攻擊法（Dictionary Attack）	字典攻擊法，使用於密碼破解程序，也就是駭客會準備一些常用的單字集，先猜這些密碼，而大幅縮短破解密碼的時間，因此讓駭客取得登入密碼，將造成系統的破壞。
A5	系統存在的安全漏洞	目標主機弱點掃瞄（Vulnerabilities Scan）	駭客利用網站弱點掃描器與檢測工具，來找出這些伺服器存在的漏洞，或者藉由分析伺服器的回應結果，來辨識出許多 Web 伺服器的系統資訊，造成系統資訊及弱點的洩露。
A6	系統存在的安全漏洞	目標主機弱點利用攻擊（Vulnerabilities Exploits Attack）	駭客透過弱點掃描後所得的系統資訊及漏洞，展開有系統的漏洞利用攻擊，藉由入侵系統以取得存取的權限，造成資料外洩或損害系統。（例如：Web Server CGI Exploits）
A7	未更新病毒碼及修補安全漏洞	病毒、蠕蟲（Virues,Worms）	藉由網路傳播感染電腦系統，執行惡意程式，成為僵屍電腦，並會耗用系統資源使系統變慢，甚至造成目標主機所提供之服務癱瘓或資料外洩。（例如：病毒透過 MS08-067 漏洞攻擊）
A8	未更新病毒碼及修補安全漏洞	木馬程式（Trojan horses）	木馬程式是目前洩漏機敏資料的首因，駭客利用植入木馬程式，擷取系統重要資料如使用者帳號、密碼及竊取重要資料。

（二）網路安全

我們前面有提到如果網路不安全，網站系統及應用程式的安全性肯定會不安全。因此，必須要建構一個安全的網路環境，並且必須強化偵測防禦機制以抵擋網路入侵的行為，對於常見的網路攻擊也都必須要有適當的防護，其中防火牆、入侵偵測及防禦系統等都是主要的安全防禦設備。除此之外，有些網路設備，本身也會存在一些瑕疵，而內部人員對網路資源的濫用，或是人為的洩密等，都可能會形成網路安全上的漏洞。一旦網路上出現安全漏洞，便給了入侵者可乘之機。

一般透過網路攻擊的方法有很多，例如：針對特定的網站使用 DDoS 攻擊，利用分散於不同地方的多部電腦主機，發送大量偽造來源地址的封包，癱瘓受害者所在的網路電腦主機伺服器，導致無法服務正常的使用者。攻擊者也可藉由假冒合法的主機來進行非法活動，例如 IP 位址假冒（IP address spoofing）、實體位址

假冒（ARP spoofing）、TCP 連線假冒（Connection spoofing）等。攻擊者為了隱藏自己身分，或欲對受害主機進行 DDoS 攻擊，將攻擊封包來源偽裝，最常使用的方式就是 IP spoofing。透過上述的弱點及威脅分析，本研究整理出常見的網路安全威脅，如表 6 所示之。

表 6：網路安全威脅分析

編號	弱點	威脅	威脅描述
B1	網路安全缺陷	分散式阻斷服務攻擊（Distributed Denial of Service, DDoS）	藉大量對網站主機提出服務請求，影響網站伺服器服務提供或阻斷無辜瀏覽的用戶端程式。（例如：TCP 同步訊號洪水型攻擊）
B2	網路安全缺陷	網路監聽（Network Sniffers）又稱嗅探攻擊	駭客監聽在網路上傳輸的封包，透過網路封包監聽工具取得傳輸的資料，將所有送到該服務器的封包補捉下來，分析傳送的資訊以取得使用者的帳號與密碼資料，再利用此帳戶登入修改檔案，駭客亦能變更封包中的重要資訊。
B3	網路安全缺陷	偽冒攻擊（Spoofing）	攻擊者藉由假冒合法的主機來進行非法活動，攻擊的方式有很多，其中 IP 位址假冒（IP address spoofing）是最常見，使用 IP 位址假冒的話，可以通過防火牆等防禦設備的過濾，而達到入侵攻擊。
B4	網路防護不足	埠掃描攻擊（Port Scan Attack）	埠掃描（Port Scanning）是一種常用的探測技術，攻擊者可將它用於尋找他們能夠成功攻擊的服務埠，進行系統漏洞偵測、服務偵測等行為，之後再利用得到的資訊來判斷可對目標主機進行何種的攻擊動作。
B5	網路防護不足	特定服務埠弱點攻擊（Service Port Attack）	當攻擊者獲得目標主機開啟了哪些特定服務埠，就可以針對該特定服務埠存在的弱點進行攻擊侵，例如發現目標主機提供是一個可以匿名登入的 FTP 服務，則攻擊者不需任何密碼就可進入目標主機執行某些檔案的存取動作。
B6	系統管理員資訊安全意識不足	社交工程（Social Engineering）	以人性弱點瓦解組織安全，利用非技術性手段如惡意郵件、網路釣魚或偽裝成修補程式，獲得存取系統資訊或取得機敏資料的機會。

（三）網頁應用程式安全

最近幾年的網路安全研究報告指出，資訊安全攻擊有 75%都是發生在 Web 應用層而非網路層。Web 應用程式已成為駭客熱門攻擊目標，駭客利用 Web 應用程式的漏洞入侵，可能導致主機被取得控制權、網頁被置換、資料庫資料外洩等嚴重安全威脅。攻擊者非常喜歡利用 CGI 程式的漏洞或者 PHP 腳本進行攻擊，向 WEB 伺服器傳遞了一些不可靠的參數，以取得存取的權限；因此，這些應該程式之漏洞也為 WEB 伺服器的安全帶來嚴重威脅。

本研究參考知名的 Web 安全組織 OWASP Top 10（2010）所公佈的報告，Web 應用程式弱點攻擊中最嚴重的兩種攻擊方式是跨網站腳本（Cross Site Scripting; XSS）攻擊和 SQL 注入（SQL Injection）攻擊。其中 XSS 攻擊是利用會動態產生 HTML 網頁且不驗證回應到網頁之輸入的 Web 應用程式，從而獲得管理員許可權限，控制整個網站。而 SQL 注入攻擊是另一種眾所皆知的攻擊方式，它透過 Web 應用程式未檢核使用者的輸入資訊，來建立資料庫命令碼，以獲得資料讀取和修改的許可權限。所以，如果應用程式利用使用者在某表單欄位內輸入的內容，來建立一個 SQL 命令碼字串，惡意使用者只要存取該網頁，輸入不正當的參數，就可修改查詢的本質。透過網頁的弱點掃瞄或是源碼檢測找出網頁應用程式存在了那些弱點，加以修正或防護以降低威脅攻擊。

由於 Web 應用程式弱點攻擊的主要目的為後端的資料庫，而資料庫本身也是系統運作的一種應用軟體，和作業系統一樣也會被發現有弱點漏洞存在，可能會遭受未經授權存取、遠端程式執行、資料外洩、阻斷服務等攻擊等，因此資料庫也必須要有足夠安全的環境才能正常的運作。然而攻擊者可透過資料庫的弱點掃瞄，找出資料庫存在的弱點，或藉由偵測密碼、存取權限和組態設定的弱點，造成資料庫資料外洩，這些是非常嚴重的安全威脅。通常資料庫的弱點發佈到修補程式出來，往往需要 3~6 個月以上的時間，在這一段期間可能遭受到的資料庫弱點攻擊威脅機率將變高。綜合以上的分析整理出常見對網頁應用程式安全的威脅，如表 7 所示。

表 7：網頁應用程式安全威脅分析

編號	弱點	攻擊 / 威脅	威脅描述
C1	網頁程式弱點（輸入未檢核）	跨網站腳本攻擊（Cross-Site Scripting）	利用網站傳送字元檢查的漏洞，執行跨網站式攻擊執行惡意 Script，並可欺騙 Web Server 取得敏感資料。
C2	網頁程式弱點（輸入未檢核）	資料庫注入攻擊（SQL Injection）	利用字元檢查漏洞進行攻擊，忽略檢查後入侵使用資料庫語法，惡意修改或刪除後端資料庫的資料，影響網站的正常營運。

編號	弱點	攻擊 / 威脅	威脅描述
C3	網頁程式弱點（輸入未檢核）	緩衝區溢位攻擊（Buffer Overflow）	緩衝區溢位攻擊為程式設計者的疏忽，使得攻擊者的輸入大於設計者的預期，造成緩衝區容量不足，導致系統會執行攻擊者欲執行的攻擊程式。
C4	資料庫存在的弱點	資料庫弱點掃瞄（Database Vulnerability Scan）	駭客透過資料庫弱點掃瞄，找出資料庫的弱點，或藉由偵測密碼、存取權限和組態設定的弱點，造成資料庫資料外洩之嚴重安全威脅。
C5	資料庫存在的弱點	資料庫弱點攻擊（Database Vulnerability Attack）	藉由找出資料庫易受攻擊的弱點加以入侵，如果入侵成功可能導致大量的機敏資料遭到竊取及竄改。

二、網站安全之風險分析與評估結果

我們識別與分析常見的攻擊型態後，瞭解網站伺服器的潛在威脅，下一步驟將依圖 10 之風險分析及風險評估兩步驟實作網站安全風險評估，其中風險分析階段將運用所設計之延伸型攻擊樹分析法加以分析。經由網站安全威脅情境分析，我們可以建構出主機系統攻擊樹、網路攻擊樹與應用程式攻擊樹等三種安全威脅的網站攻擊樹。透過這些攻擊樹的樹狀結構表示，使得我們可以很清楚地了解每一個攻擊威脅所利用的弱點，以及每一個攻擊威脅之間的關聯。

由圖 17 中我們可看出主機系統的主要弱點有權限管理不當、弱密碼管理、系統自身存在的弱點及更新管理不當等。其中有一個很特別的現象，如果只是主機系統弱點的探測掃瞄，這本身並不會對目標系統造成危害，自然不會對系統構成威脅。但是如果攻擊者接下來利用探測到的弱點資訊，做進一步的弱點利用攻擊，那麼對系統就有可能造成危害。反之，攻擊者如果沒有弱點資訊，那麼就不會使用弱點攻擊，因此唯有兩者成立才有可能發動攻擊，故兩者的關係具有邏輯 AND 關聯時，就會對系統造成威脅。

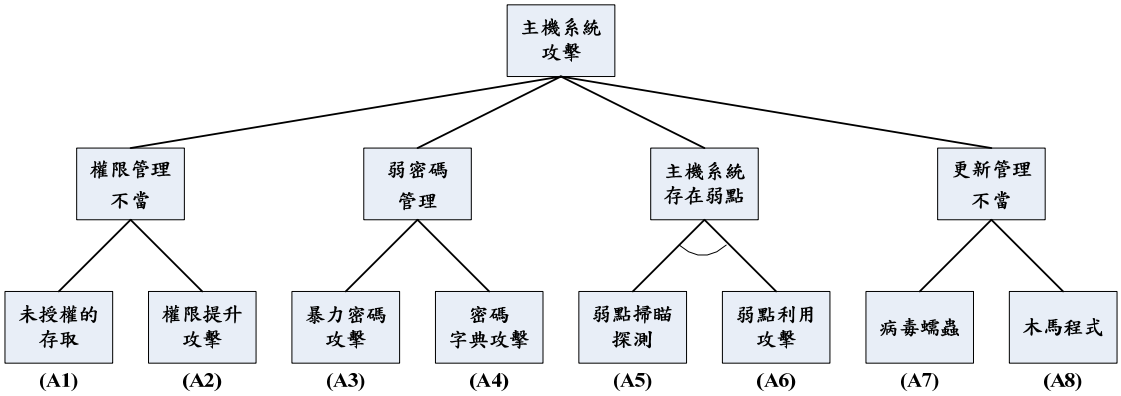

圖 17：主機系統攻擊樹

由圖 18 中可看出網路環境的主要弱點有網路安全缺陷、網路安全防護不足和資訊安全意識不足。其中網路安全缺陷的弱點，主要在於 Internet 是一個開放的網路，可能面對各式各樣的攻擊，再加上通訊協定本身的一些缺陷，使得置身於網路之中的電腦都是不安全的。其中，像 DDoS 攻擊、Sniffers 攻擊和 Spoofing 攻擊等等都是常見的攻擊型態。一般網路攻擊前必須透過 Port Scan 的方式，取得主機的一些服務埠的弱點，但通常埠掃描僅利用對埠所進行的掃描不會造成直接的損失。然而，如果讓攻擊者找到可用於發動各種攻擊的埠，對系統可能就是一個非常嚴重威脅。

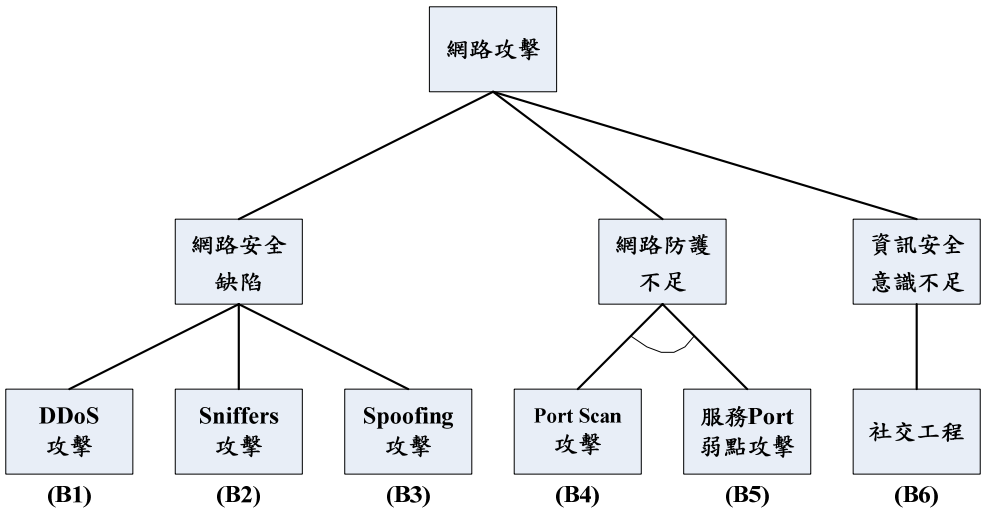

圖 18：網路攻擊樹

由圖 19 中我們可看出應用程式的主要弱點有網頁應用程式的弱點及資料庫的

弱點。本研究依據 OWASP Top 10（2010）所公佈的報告，以常見的幾個 Web 應用程式弱點攻擊做為評估標的，其中最嚴重的幾個攻擊方式是 XSS 攻擊、SQL Injection 攻擊和 Buffer Overflow 攻擊。另外，從資料庫的弱點利用，通常網站後端的資料庫相對於 Web Server 是較安全的。但是駭客的終極目標皆為資料庫，因此針對資料庫的攻擊也有愈來愈多的趨勢。故本研究將資料庫弱點攻擊納入本研究的風險分析，主要是提醒我們資料庫安全的重要。同樣地，如果只是針對 DB Server 做弱點掃瞄，這本身並不會對構成威脅，但是如果攻擊者利用探測到的 DB 弱點資訊，做進一步的弱點利用攻擊，那麼對系統就有可能造成危害，故兩者的關係也具有邏輯 AND 關係。

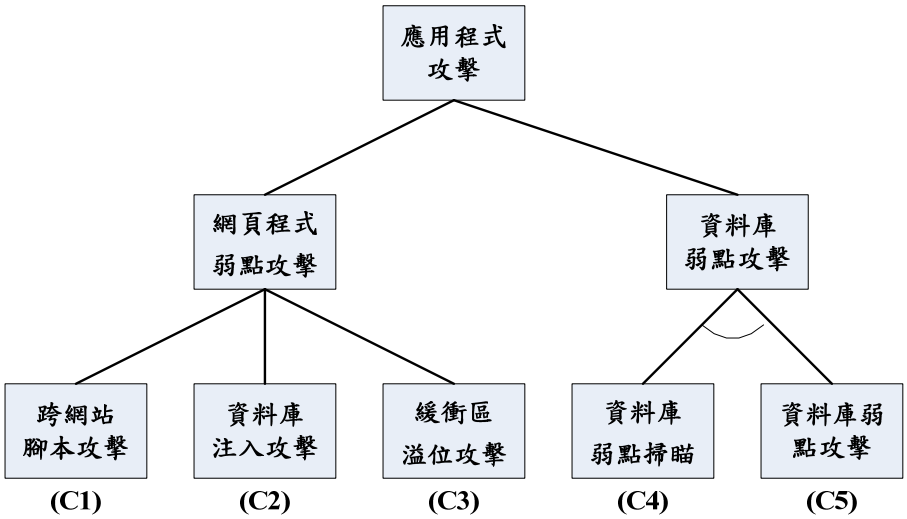

圖 19：應用程式攻擊樹

整合三種不同安全類別的攻擊樹，變成一個完整的網站攻擊樹架構，再依據目標、子目標、弱點、攻擊（威脅）等四個層面分類，轉換成風險評估對應圖，就可以很清楚的看到網站系統的各種安全威脅，以及各種攻擊手法所利用的弱點和攻擊目標（對象）如圖 20 所示。

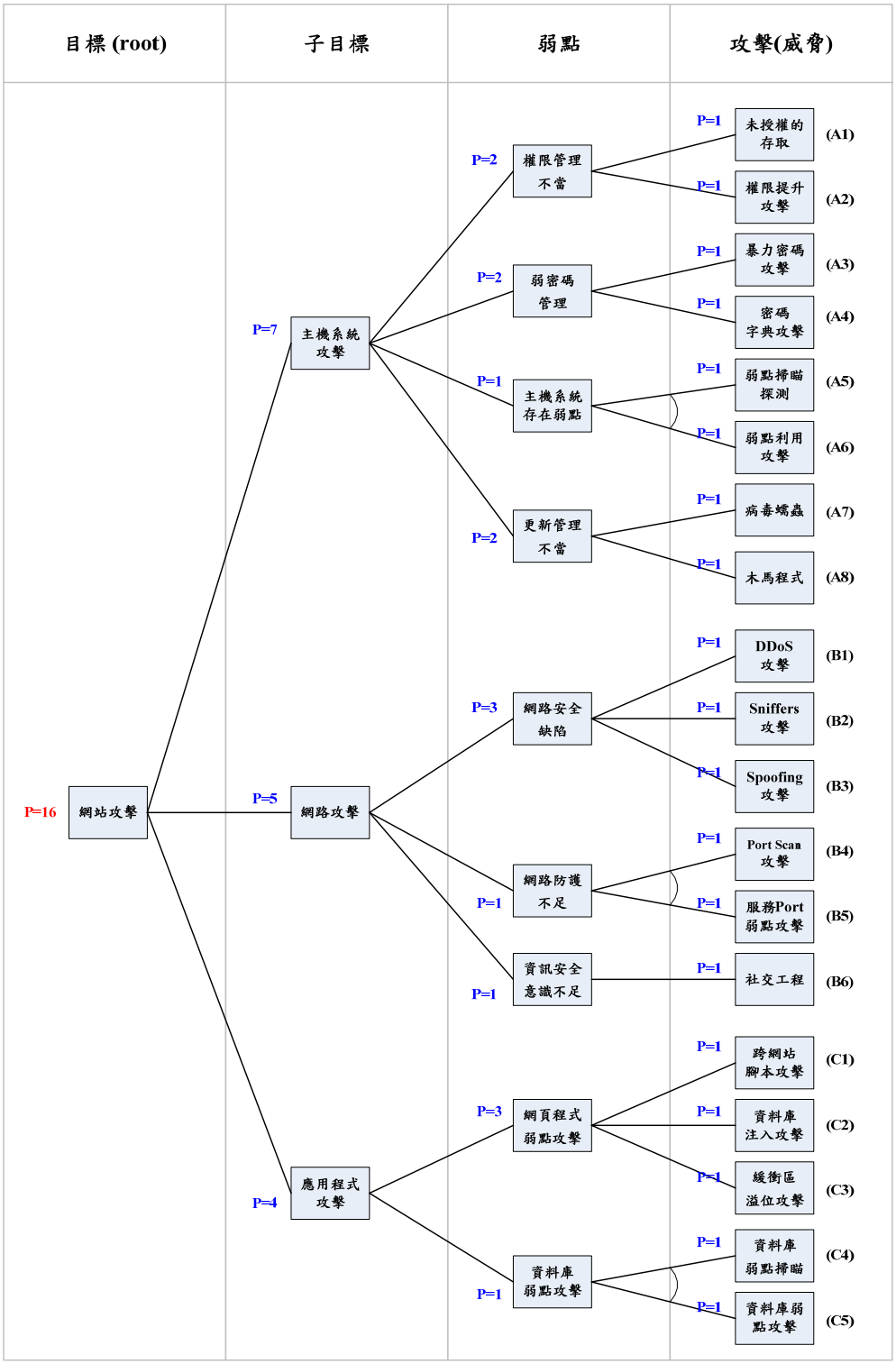

圖 20：完整網站攻擊樹架構及威脅演算法計算推導

接著，我們透過所建構的完整網站攻擊樹，依據攻擊樹威脅演算法計算出威脅的組合，從攻擊樹攻擊威脅演算法由下而上推導得出可能的攻擊威脅共有 16 種組合，其威脅列表所示之攻擊路徑分別為{A1}、{A2}、{A3]、{A4}、{A5,A6}、{A7}、{A8}、{B1}、{B2}、{B3}、{B4,B5}、{B6}、{C1}、{C2}、{C3}、{C4,C5}，如表 8 所示。

針對我們找出的各種威脅組合，執行風險評估程序，找出威脅網站系統的高風險威脅，作為優先改善及強化的目標。我們評估的標準是針對每個威脅組合的攻擊節點去評估，檢視每個攻擊節點現有的防護措施，在面對攻擊節點的威脅是否已有安全的防護對策及控管措施，或是系統漏洞是否有定時修補，網頁程式開發是否有原始碼檢測（Code Review）或驗證測試等，如果有良好的管理措施自然可以避免或減少潛在的威脅攻擊，其發生的可能性機率就會比較低，反之，發生的可能性就會比較高。

表 8：完整網站攻擊威脅列表

威脅組合		威脅說明	威脅組合		威脅說明
威脅 1	{A1}	未授權的存取	威脅 9	{B2}	網路監聽又稱嗅探攻擊
威脅 2	{A2}	權限提升攻擊	威脅 10	{B3}	偽冒攻擊
威脅 3	{A3}	暴力密碼攻擊	威脅 11	{B4,B5}	特定服務埠掃描及弱點攻擊
威脅 4	{A4}	字典攻擊法	威脅 12	{B6}	社交工程
威脅 5	{A5,A6}	目標主機弱點掃瞄與利用攻擊	威脅 13	{C1}	跨網站腳本攻擊
威脅 6	{A7}	病毒、蠕蟲	威脅 14	{C2}	資料庫注入攻擊
威脅 7	{A8}	木馬程式	威脅 15	{C3}	緩衝區溢位攻擊
威脅 8	{B1}	分散式阻斷服務攻擊	威脅 16	{C4,C5}	資料庫弱點掃瞄及弱點攻擊

經透過與企業之資訊安全人員的協助參與討論與評估後，按照可能性等級與影響性等級加以評估對應出相對的級距分數，再計算每一個攻擊威脅的風險值，最後再依風險矩陣表對應出其風險等級及威脅排行，其評估的結果如表 9 所示。經風險評估後發現存在一個高風險的威脅，並且是列為最優先處理的項目，威脅 5 是主機系統的弱點探測與攻擊，很顯然在弱點更新修補方面做的不確實。針對主機系統的弱點掃瞄及 Patch 更新是列為重點工作，因為唯有儘速修復系統漏洞，才可降低弱點攻擊威脅，如果減少了系統的漏洞，自然漏洞攻擊就會減少，對系統

就不會構成威脅。其次在網路安全方面要注意的問題在於防禦 DDOS 及 Spoofing 的攻擊，必須要選擇較好的網路防護設備，例如選擇可偵測及防禦 DDOS 及 Spoofing 攻擊的 IDS/IPS 設備。同時對於網頁應用程式安全的部分，應提防 XSS 及 SQL Injection 的攻擊，在程式開發階段即應注意安全性的程式碼檢測，對於已開發的網站系統也應定期執行網頁應用程式弱點掃瞄及更新，治標的作法可採用網頁應用程式防火牆（Web Application Firewall; WAF）來過濾網頁應用程式弱點的攻擊。至於其他的次要威脅也應好好再重新檢視，提出適當的改善計劃，當然這只是一個評估的例子，主要還是透過攻擊樹的分析，讓我們可以收集到更多的攻擊資訊，然後去做好防護的工作。

表 9：網站系統威脅之風險評估結果

威脅組合		Likelihood（1~5）	Impact（1~5）	風險評量（Measure of Risk）	風險等級（Level of Risk）	威脅排行（Threat Ranking）
威脅 1	{A1}	1	2	2	L	8
威脅 2	{A2}	2	2	4	L	6
威脅 3	{A3}	2	3	6	L	5
威脅 4	{A4}	1	3	3	L	7
威脅 5	{A5,A6}	4	5	20	H	1
威脅 6	{A7}	2	2	4	L	6
威脅 7	{A8}	3	2	6	L	5
威脅 8	{B1}	3	4	12	M	2
威脅 9	{B2}	2	2	4	L	6
威脅 10	{B3}	3	3	9	M	3
威脅 11	{B4,B5}	2	3	6	L	5
威脅 12	{B6}	1	4	4	L	6
威脅 13	{C1}	3	3	9	M	3
威脅 14	{C2}	3	3	9	M	3
威脅 15	{C3}	1	2	2	L	8
威脅 16	{C4,C5}	2	4	8	L	4

最後，由於每一個企業的網路環境與安全防護都不相同，因此在威脅與弱點分析的資料來源也會有不同，例如：防火牆（Firewall）記錄、IDS/IPS 或 WAF 分析報告、弱點掃瞄分析、病毒記錄等，故評估的結果也會有不同；因此，有以下

幾點建議說明：

1. 如果企業實際無法取得威脅分析資料，可藉由資安產業統計或相關安全報告加以分析而得之。本研究即是參考資安廠商、OWASP 及 SANS 組織之網站所公佈的相關分析報告為主。
2. 在風險分析上，有時在可能性與衝擊度有時並不是那麼容易判別，此時必須依賴企業內部有經驗的專業人員或外部專家提供意見判斷。
3. 在評估的結果中若有高風險的攻擊威脅時，必須提供改善措施及防護策略，以降低威脅事件發生的可能性；同時在某些攻擊節點存在的弱點缺陷，有時必需即時處理，才能避免攻擊事件之發生。
4. 在評估結果中即使已經達到可接受之安全水準，仍然可以針對攻擊節點風險值較高的部份加以防護或監控，以降低風險發生的可能。
5. 在新種威脅、弱點被發現時，應重新檢討並修正攻擊樹，再重新評估其系統是否達到可接受之安全性等級，同時也應定期重新檢視及審查系統防護措施是否有新增或變更。至於可接受之安全性等級標準，則依企業內部風險管理所訂定之標準值，以符合企業之風險管控要求。
6. 企業也必須考慮到投入的資安成本問題，如果剩餘風險值不大時，從投資學上來說依 80/20 法則。如果投入 80%的成本只為了改善剩餘 20%的風險，企業可能要好好評估是否值得去做，一般是以內部訂定的可接受風險等級為標準。
7. 攻擊樹可以表示更複雜的威脅圖，建構攻擊樹時可依不同安全屬性建立各個子樹，例如從操作安全、內容安全、管理安全、應用安全等不同安全層面加以分類評估。

三、與一般風險分析法之比較說明

一般針對資訊系統的風險評估方法，如表 10 所示，皆採用制式的風險評估表來評估資訊系統的風險。其風險評估的方法是由影響系統服務之資產價值水準，及威脅事件、脆弱事件與現行管制措施之評估分數所組成，分成脆弱度、威脅度、價值度、難檢度四個評估的指標。當發生的頻率愈大及會造成資產損害愈大時，則分數愈高，評分的方式係採定性型五分制（0～4 分）的評估方式。因每項弱點及威脅事件皆採用條例式，而其中的各個脆弱事件及威脅事件無法展現彼此的關聯性，也無法看出攻擊的路徑及威脅組合，因此評估出的結果並不是很客觀。由於攻擊樹法利用樹狀結構來描述系統受到的安全攻擊事件的集合，因此，將此法應用在風險分析上，可以改善威脅或攻擊途徑描述的不足。而延伸型攻擊樹分析法結合了攻擊樹與一般定性風險分析法的優點，因為採用定性分析法的優點是沒

有太多的計算負擔，同時利用攻擊樹分析法可描繪出系統遭受攻擊的所有安全事件，以及各個安全事件的關聯，再利用所設計的攻擊樹威脅演算法，可以找出各種攻擊組合，使得延伸攻擊樹分析法在面對較複雜的攻擊行為上，可以得到較完整的表示能力。因而也更有利於主觀判斷的準確性，使得可以對傳統風險分析法之有效性不足的地方得以改善，並增加風險評估的客觀性。

表 10：一般風險評估表

資產類別	資產名稱	脆弱事件		脆弱度	威脅事件	威脅度	影響（損失程度）	價值度	現行管制措施	難檢度	個別風險值	平均風險值	風險鑑別 CIA
軟體資產	網站系統	1.	應用軟體感染病毒	1.5	系統無法正常運作	1.5	電腦遭病毒破壞導致無法運作	2.5	電腦已加裝防毒軟體	2	7.5	7.0	C.I.A
		2.	程式瑕疵	2	系統無法正常運作	2	1. 中斷客戶服務 2. 資料維護錯誤	1	加強程式單元及整體測試	2	7.0		I.A
		3.	換版不當	1.5	系統無法正常運作	2	1. 程式執行錯誤 2. 資料維護錯誤	2	換版流程控管	1.5	7.0		I.A
		4.	操作程序設計不當	1.5	系統無法正常運作	2	程式執行錯誤	2	提供正確操作流程文件	1.5	7.0		A
		5.	修改 DB 內容錯誤	2	系統無法正常運作	1.5	資料內容錯誤	1	依 DB 修改流程比對前後資料內容	2	6.5		C.I

表 11 為延伸型攻擊樹分析法與一般風險分析法的改進比較，它改進的最大優點是可以有圖形化的展示及各種威脅彼此之間的關聯性，並且在複雜的攻擊樹可簡易計算出威脅的組合，因此本方法特別適用在攻擊威脅的情境上，尤其是當攻擊手法是有程序步驟的威脅攻擊。

表 11：延伸型攻擊樹分析法、攻擊樹分析法與一般風險分析法三者之比較

評估指標	延伸型攻擊樹分析法	攻擊樹分析法	一般風險分析法
圖形化	具圖形化表示，可描繪出系統遭受攻擊的所有安全事件，易於了解。	具圖形化表示，可描繪出系統遭受攻擊的所有安全事件，易於了解。	制式化評估表，描述性不足，不易了解。
相關性	有些攻擊行動是有階段性、步驟性，可看出各個攻擊威脅之間的關聯性，以利評估完整的威脅組合。	有些攻擊行動是有階段性、步驟性，可看出各個攻擊威脅之間的關聯性，以利評估完整的威脅組合。	不易辨別出各個威脅之間的關聯性，只能各別評估威脅。
評估圖對應	依據目標、子目標、弱點、攻擊（威脅）等四個階層加以分類對應。	無。	無。
威脅組合計算	有攻擊路徑演算法可計算出多少種威脅組合。	無。	無。
風險評估對象	以「威脅」為單位。	部份之風險評估研究仍以「資產」為單位。	以「資產」為單位。
適用情境	網路攻擊、威脅及安全事件之分析。	網路攻擊、威脅及安全事件之分析。	一般資訊安全風險評估。

伍、結論

在現今企業環境建置的資訊系統中，大多是以開放式 Web 平台為開發應用系統的架構，相對的網路入侵攻擊也變得容易且更為頻繁。而根據 SANS 組織的統計在網站系統的弱點利用，以網頁應用程式的弱點利用為主要的攻擊目標。由於當前攻擊威脅的與日俱增及多變的特性，必須要有適當之網站系統風險評估的方法，以找出系統最脆弱的一個環節，給予適當的改正或修補，以降低可能的威脅攻擊。因此網站系統之風險評估，應著重在網路攻擊的威脅為主，以找出系統的脆弱點。

本研究依據風險管理架構，主要在改善風險分析及風險評估兩步驟上，其中風險分析是以攻擊樹（Attack Tree）為基礎，利用攻擊樹來描繪攻擊情境，並且對應到風險評估圖中，設計一個改良式威脅計算演算法，亦即考慮攻擊困難度與偵測防禦度的各種攻擊組合，再評估各種威脅之風險，稱之為延伸型攻擊樹分析法。可以改善一般風險分析法之威脅描述不足的地方，並且嘗試以不同的方式來評估網站系統所面臨的威脅，不同之處在於我們是以「威脅」為單位而不是以「資產」

為單位來進行風險評估。最後，本研究以網站系統為例，套用所提出之延伸型攻擊樹分析法及風險評估流程，證明可以有效地評估網站系統的風險值及威脅等級，以作為系統管 者對資訊安全風險評估之依據。並將延伸型攻擊樹分析法與傳統風險分析法作一比較，說明此風險評估方法可以改善傳統風險分析法不足的地方，增加風險評估的可用性及客觀性。

未來的網站攻擊趨勢上，將朝向虛擬化 / 雲端運算環境（Virtualization/Cloud Computing）。本研究仍有許多未盡完善之處，故在未來的研究上有兩個主要的方向：(1) 將針對雲端安全的威脅進行分析，建構雲端系統攻擊樹以評估可能威脅的風險，並提出防禦對策，有效降低雲端攻擊的危險，讓評估結果更為完整。(2) 真實反應企業環境所面臨的風險，必須先蒐集企業內部完整的攻擊威脅事件及脆弱性資料分析，故未 將朝向自建威脅資料庫，並整合威脅分析模型的研究設計。

參考文獻

行政院研究發展考核委員會（2009），『風險管理及危機處理作業手冊』，http://sec.nuk.edu.tw/updown/news/931916152171.pdf（存取日期 2010/07/12）。

林勤經、樊國楨、方仁威、黃景彰（2002），『資訊安全管理系統建置工作之研究』，*資訊管理研究*，第四卷，第二期，頁 43-65。

政府網際服務網通報（2010），『網路安全服務』，http://gsn.nat.gov.tw/new/05-03.html（存取日期 2010/06/18）。

翁浩正（2010），『資訊安全：Web Security 網站安全基礎篇（一）』，http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1909（存取日期 2010/05/04）。

傅雅萍、樊國楨、楊中皇（2008），『ISO/IEC 27005 風險管理標準整合 CORAS 之可行性研究：以電力公司為例』，資通安全專論 T97022，http://security.nknu.edu.tw/psnl/publications/2009/05_FU,YA-PING/ISOIEC27005.pdf（存取日期 2010/05/04）。

楊尚青、王憶魯（2009），『基於系統動態方法內部威脅之分析與建模』，資訊管理實務研討會，中壢市，臺灣，5 月 8 號，頁 21-40。

樊國楨、林樹國、朱潮昌（2008），『工業控制系統資訊安全風險評鑑實作初探』，http://fsms.bsmi.gov.tw/cat/epaper/工業控制.doc（存取日期 2010/09/26）。

歐士源、黃世昆（2000），『網路安全：網路攻擊模式簡介』，http://www.ascc.sinica.edu.tw/nl/89/1603/2.txt（存取日期 2010/05/04）。

賴義鵬、周世益（2009），『以弱點評估方式來提升資訊系統安全需求之研究』，資訊管理實務研討會，中壢市，臺灣，5 月 8 號，頁 1-20。

Dimitriadis, C.K. (2007), 'Analyzing the security of internet banking authentication mechanisms', *Information Systems Control Journal*, Vol. 3, pp. 1-59.

Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R. and Reuter, C. (2007), 'The use of attack and protection trees to analyze security for an online banking system', Proceeding of 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Hawaii, USA, January 29, pp. 144b.

Gan, Z., Tang, J.F., Wu, P. and Varadharajan, V. (2007), 'A novel security risk evaluation for information systems', Proceeding of 2007 Japan-China Joint Workshop on Frontier of Computer Science and Technology (FCST 2007), Wuhan, China, November 1-3, pp. 67-73.

Jin, C., Wang, X.Y. and Tan, H.Y. (2010), 'Dynamic attack tree and its applications on trojan horse detection', Proceedings of the 2010 Second International Conference on MultiMedia and Information Technology (MMIT '10), Washington, DC, USA, April 24-25, Vol. 1, pp. 56-59.

Li, X. and He, K. (2008), 'A unified threat model for assessing threat in Web applications', *International Journal of Security and its Applications*, Vol. 2, No. 3, pp. 25-30.

Li, X., Liu, R., Feng, Z.Y. and He, K. (2009), 'Threat modeling-oriented attack path evaluating algorithm', *Transactions of Tianjin University*, No. 15, pp. 162-167.

Microsoft TechNet (2006), 'Guidance', available at http://technet.microsoft.com/zh-tw/library/dd548203.aspx (accessed 21 September 2010).

Moberg, F. (2000), 'Security analysis of an information system using an attack tree-based methodology', Unpublished Master's Thesis Automation Engineering Program, CHALMERS University of Technology, Gothenburg, Sweden.

OWASP Top 10 (2010), 'The ten most critical web application security risks', available at http://owasptop10.googlecode.com/files/OWASP%20Top%2010 %20-%202010.pdf (accessed 21 July 2010).

OWASP (2010), 'OWASP risk rating methodology', available at http://www. owasp.org/index.php/owasp_risk_rating_methodology (accessed 21 July 2010).

SANS Top 20 (2010), 'The Top Cyber Security Risks', available at http://www.sans.org/top-cyber -security-risks/ (accessed 24 July 2010).

Schneier, B. (1990), 'Modeling security threats', *Dr. Dobb's Journal*, Vol. 12, No. 24, pp. 21-29.

Stango, A., Prasad, N.R. and Kyriazanos, D.M. (2009), 'A threat analysis methodology for security evaluation and enhancement planning', Proceedings of 2009 Third

International Conference on Emerging Security Information, Systems and Technologies, Athens/Glyfada, Greece, June 18-23, pp. 262-267.

Wang, L.Y., Liu, A. and Jajodia, S. (2006), 'Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts', *Journal of Computer Communications*, Vol. 29, No. 15, pp. 2917-2933.

Zone-H (2010),'Defacements Statistics 2010: Almost 1.5 million Websites defaced, what's happening?', available at http://www.zone-h.org/news/id/4737 (accessed 15 January 2011).