以攻擊樹為基礎之SIP網路電話弱點檢測系統
SIP phone vulnerability exam system based on Attack Tree

古東明[1] Tung-Ming Koo, 劉作仁[1] Zuo-Ren Liou, 沈志昌[2] Chih-Chang Shen, 游婷敬[1] Ting-Ching Yu
[1]國立雲林科技大學資訊管理系, [2]嶺東科技大學資訊科技系
[1]koo@yuntech.edu.tw, g9523718@yuntech.edu.tw, g9623744@yuntech.edu.tw, [2]huntsam@teamail.ltu.edu.tw

摘要

隨著資訊科技的進步，現代人擁有更多的通訊媒介可供選擇，例如：電子郵件、即時訊息以及網路電話等，而其中的網路電話有逐漸取代傳統PSTN（Pablic Switded Telepwoue Network）的趨勢。網路電話所採用的SIP（Sessiou Initial Protocol）協定雖具有簡單、快速、靈活且便利等特性，但是該協定是基於網際網路所設計，因此SIP也自然繼承了網際網路本身的弱點。有鑑於此，本研究使用滲透測試搭配攻擊樹的指引，針對使用SIP協定的網路電話系統進行安全檢測。本系統可以讓系統管理員明確地找出組織內部潛在的漏洞，以便及早修復。

關鍵字：網路電話、攻擊樹、SIP、滲透測試。

Abstract

Along with the development of information technology, more communication tools, such as email, instant message, and internet telephony, become available. The progress on internet telephony is in its pivoting point to gradually replace the traditional public switched telephone network (PSTN) service. The Session Initiation Protocol (SIP) for the internet telephony has its advantage of simple, speedy, flexible, and convenient. However, SIP is based on internet infrastructure; it inherits all vulnerability natures associated with internet communication. We propose in this paper the vulnerability evaluations of the SIP phones using penetration test under the Attack Tree’s guidance. Our proposed system will help administrators to precisely allocate potential internal weaknesses and to patch issues effectively.

Keywords: Internet telephony, Attack Tree, SIP, Penetration test.

1 前言

近年來隨著資訊科技的進步，現代人生活中使用資訊科技的比例也日益增加，再加上資訊科技所帶來的便利性，其相關產品及服務逐漸成為生活中不可或缺的一部份。同時，由於網際網路的蓬勃發展，除了原有電話、手機、傳真等通訊方式之外，其他基於網際網路所開發的通訊工具，如：電子郵件、即時訊息（Instant Message）以及網路電話（Voice over IP, VoIP）等，也提供現代人挑選通訊媒介的更多選擇[1]。

不過，任何新興的網路殺手級應用，如：WWW、電子郵件、網路電話等，雖然都為一般大眾帶來了許多便利之處，但是，這些應用猶如雙面刃，背後隱藏了許多不為人知的危機。網路電話所採用的SIP協定是基於網際網路所設計的協定，所以SIP也自然繼承了網際網路其本身的弱點，網際網路中曾經發生過的攻擊也可能會發生在網路電話上。除此之外，網路電話是基於現有的網際網路環境所建置的，仍有許多攻擊型態是很難避免的[2]。綜合以上所述，網路電話並沒有想像中的如此強韌，若日後網路電話想要取代現有的PSTN架構，成為新一代電信網路的主要通訊工具，其安全性的議題仍需妥善地處理。

雖然許多系統檢測軟體如雨後春筍般不斷出現，但系統檢測軟體大多還是以弱點掃描的形式為主，其結果報告僅能告知系統管理者目前有哪些弱點可能遭到利用，並無法找出這些弱點之間的相關性。因此，本研究利用滲透測試進行網路電話系統安全性檢測機制，搭配使用攻擊樹模擬駭客攻擊之手法，再以不同的測試個案對網路電話系統進行檢測，並提供相對應的解決方法，以期能夠幫助缺乏經驗的網路電話使用者，找出系統中所存在的漏洞，並提供該漏洞的修補方法。

2 文獻探討

本研究是在使用SIP協定的網路電話環境中進行系統安全性檢測。文獻探討以SIP、SIP攻擊手法以及攻擊樹（Attack Tree）這三個部份來進行相關技術及原理探討，尋求整合上述技術至本研究之檢測系統，以期在SIP協定的網路電話環境中發展出一個完整且準確的系統安全性檢測工具。

2.1 SIP

SIP是由IETF（Internet Eagiueering Task Force）所制定的通訊協定標準，目前大多使用於網路電話。SIP是以ASCII為基礎的通訊協定，在OSI架構中是屬於應用層的協定，用以建立、修改以及終止點對點或多對多的訊號連線，並允許多方的使用者建立一個多媒體串流的會談，而這個多媒體串流可包含聲音、影像或任何以網路為溝通基礎的媒介[3]。

2.1.1 SIP Call Flow

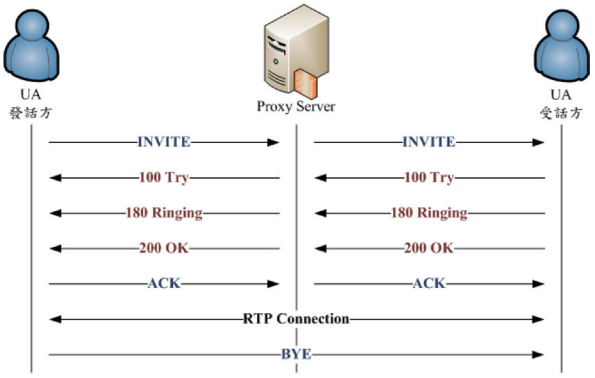
User Agent（UA）雙方透過代理伺服器進行連線，發話方只需知道受話方所使用的號碼即可通話，不需要知道對方的IP位址。其通話流程中所有的訊息都是透過代理伺服器進行轉送，其步驟如圖一所示：

(1)首先發話方傳送INVITE訊息給Proxy Server，當Proxy Server收到此訊息時，便會根據INVITE訊息內的資訊，將此訊息轉送到受話方。

(2)當受話方接受到此訊息之後，若願意與發話方進行通話，便會回傳一個200 OK的訊息給Proxy Server，Proxy Server會再將此訊息轉送給發話方。

(3)當發話方收到受話方所回傳200 OK的訊息時，發話方與受話方之間便會建立一條使用RTP協定的點對點傳輸連線，使雙方能夠進行即時的雙向通話。

(4)若有任何一方想要結束通話時，不需透過Proxy Server，只要直接發送一個BYE訊息給對方即可，便可以中斷此次通話以及RTP的傳輸連線。



圖一 透過Proxy Server的UA-to-UA通話流程
（資料來源：林佳輝，2004[4]）

2.1.2 SIP Message

根據RFC 3261中的描述，SIP協定所使用的訊息種類、格式以及表頭與HTTP協定大致相同，可將訊息種類分成Request和Response兩類。在RFC 3261中定義了八種基本的Request種類，其中較常使用的有REGISTER、INVITE、CANCEL、BYE、ACK這五種Request[5]。Request是直接使用明文來表示其意義，但是Response則是沿用並延伸HTTP／1.1的狀態碼（Status Code）來表示回應的訊息。Response代碼分為六種類型，可從狀態碼的第一個數字可以得知該狀態碼是屬於哪一種類型的。

2.2 SIP攻擊手法

由於網路電話所採用的SIP協定是基於網際網路所設計的協定，想當然爾SIP也繼承了網際網路其本身的弱點，所以網際網路中曾經發生過的攻擊也可能會發生在網路電話系統中，例如竊聽與語音垃圾廣告[4][6]。本研究將目前在SIP協定上較常見的攻擊方式分成三類[7]，接下來將針對各類型的攻擊手法進行詳細的說明。

2.2.1 Flooding Attack

Flooding Attack通常又稱作阻斷服務式攻擊（Denial of Service Attack, DoS Attack），同時也是目前在Internet上經常發生的攻擊類型之一。攻擊者透過本機電腦發送大量的封包至Server端，讓Server端疲於處理攻擊者所發出的封包，造成整個系統處於幾乎停擺的狀況下，便無法提供正常的服務給其他合法的使用者。

2.2.2 SIP Parser Attack

在通話雙方要實際進行通話之前，必須先利用SIP協定去建立通話連線。SIP是透過三方交握（Three-way hand shake）的步驟，使得Server端和Client端可以在封包交換的過程中交換雙方通話時所使用的Port、協定、IP位址以及語音封包編碼類型…等資訊，藉由這些資訊來建立點對點的語音通道。然而，這些資料都是以明文的方式進行傳輸，若程式設計師在開發軟體的同時，並未針對封包內的資料進行驗證，攻擊者便可以很輕易地將錯誤的資料，甚至是惡意的程式碼放至表頭中。舉例來說：攻擊者可以利用現成的工具，自行訂定封包中每個表頭的資料。攻擊者可以根據使用者所使用的軟體電話（Soft-phone）或是硬體電話（Hard-phone）的弱點，針對這些弱點發送一個可以讓使用者的電話無法處理的封包，造成使用者的電話當機，無法正常工作。

2.2.3 SIP-Application Level Attack

造成此類型的攻擊原因在於儘管RFC 3261中完整地規範了SIP整體的運作流程，但是有些枝微末節的部份是在其中並沒有加以詳細規定的。而這些在一般人眼裡看似平淡無奇的東西，在功力高深的攻擊者眼中卻是大有用途。若程式設計師在開發網路電話時並沒有注意到這些細節，很容易就變成攻擊者可利用的漏洞，進一步對於網路電話環境造成傷害。舉例來說：通話雙方要結束當前通話的時候，某一方會直接發出一個帶有BYE方法的Request給通話的另一方，告知對方想要中斷目前的通話連線；當另外一方收到這個Request時，便會將目前的通話連線給切斷。看似簡單的步驟，但這中間卻有個相當嚴重的漏洞。由於這個帶有BYE方法的Request不會經過Proxy Server，而是直接傳送給使用者，因此並沒有辦法存取Registrar Server中的資料，對於發送這個Request的使用者進行身份驗證。因此，攻擊者只要想辦法取得雙方在進行通話時所使用的Call-ID、From Tag、To Tag，偽造成其中一人向對方發出Request即可強制中斷雙方的通話。

2.3 攻擊樹

攻擊樹（Attack Tree）是將系統可能遭受到之攻擊，以樹狀結構的形式來表示。攻擊樹和一般的樹狀結構具有相同的特性，各節點與其上下節點具有父子的關係。以攻擊樹中節點的角度來看，其父節點就是「該節點要完成之目標」；其子節點就是「完成該節點之方法」。整棵攻擊樹最上方之節點稱為根節點，根節點在攻擊樹中所表示之意義為「最終要達成之目標」。

透過攻擊樹之表示法，可將目前已知的攻擊進行分類，便可清楚瞭解當攻擊者進行攻擊時，所採用的步驟為何。除此之外，由於攻擊樹其樹狀結構之特性，因此在修改時具有相當大的彈性，往後若有新型態的攻擊方法，仍可快速地加入到攻擊樹中[8]。

2.3.1 網路電話之攻擊樹

本研究將網路電話中所可能發生之攻擊分成三大類：Flooding Attack、SIP Parser Attack、SIP-Application Level Attack，並根據攻擊樹之定義，建立網路電話專屬之攻擊樹，如圖二所示：

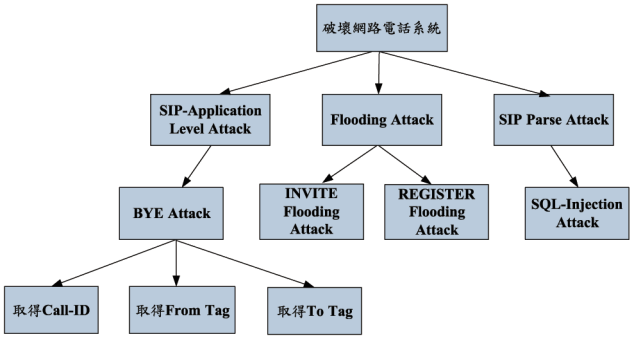


圖 二　網路電話之攻擊樹

由上圖攻擊樹的範例可得知，攻擊者如果對網路電話系統進行破壞時，可以藉由Flooding Attack、SIP Parse Attack、SIP-Application Level Attack這三種途徑達成。若攻擊者採用Flooding Attack的話，可以使用INVITE Flooding Attack或者是REGISTER Flooding Attack來針對網路電話系統進行攻擊；若採用SIP-Application Level Attack方法，則可以使用BYE Attack。那使用BYE Attack此項攻擊時，攻擊者則必須取得通話雙方所採用的Call-ID、From Tag以及To Tag方可成功發起此攻擊[9]。

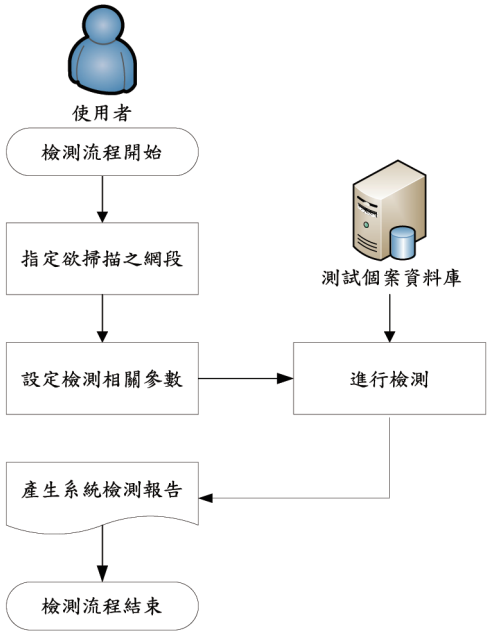
因此，攻擊者若針對網路電話系統發起攻擊時，便可透過攻擊樹清楚地了解攻擊者是採用何種手法、該手法下的哪種攻擊方式，以及進行該攻擊所必需之要素為何[10]。

3 系統設計

本研究提出一個網路電話系統安全性檢測之機制，提供檢測平台讓使用者針對網路電話系統進行檢測。待檢測結束之後，可針對檢測之結果提供使用者相對應的弱點修補方案以供參考，避免該弱點日後遭到不法人士利用。

3.1 本研究之網路電話系統安全性檢測機制流程

本研究採用滲透測試的方式，對使用SIP協定的網路電話系統設計檢測機制，以降低組織內網路電話伺服器與軟／硬體電話等相關裝置遭到攻擊，導致網路電話系統無法正常運作的風險。圖三說明本研究如何進行網路電話系統安全性檢測，並明確描述完整的檢測流程[11]。



圖三　本研究之網路電話系統檢測流程圖

(1)首先，使用者需先指定本次欲掃描之網段。

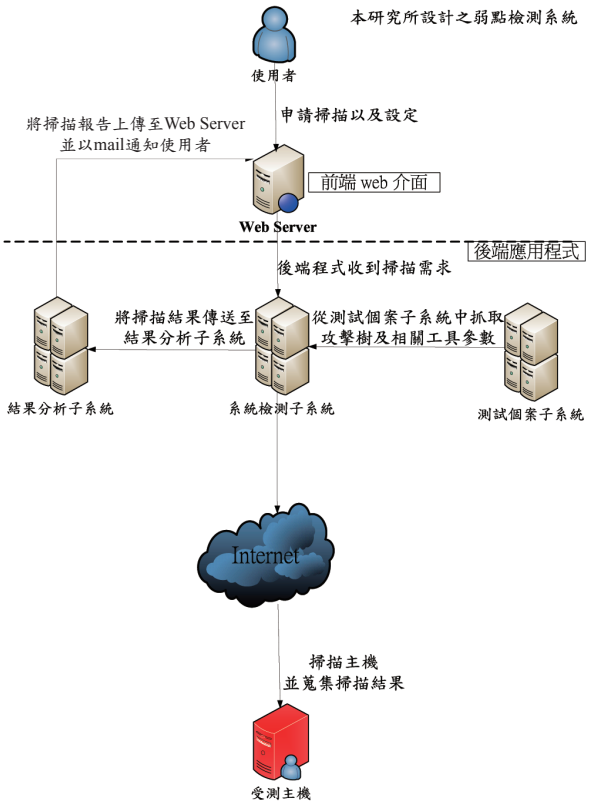
(2)在測試個案資料庫中，每種測試個案都有流行度（Popularity）、簡易度（Simplicity）以及影響度（Impact）三種指標。因此，使用者在指定欲掃描的網段後，需針對本次掃描進行權重值的分配，以利於最後檢測報告的分析。

(3)在掃描設定完成之後，前端網頁便會將本次掃描之需求傳送到後端的程式，後端的程式便會開始進行網路電話系統安全性之檢測。首先針對使用者所設定之網段進行測試，找出有提供網路電話服務的主機並進行檢測，以減少掃描所花費的時間。之後，再搭配採用攻擊樹（Attack Tree）之概念，由測試個案建立其攻擊樹，模擬駭客會如何進行攻擊，並依此步驟對指定目標進行測試。

(4)系統會將所檢測之結果，連同測試個案資料庫中的修補技術資料一同彙整成檢測報告。使用者便可根據此報告將組織內部有弱點的設備進行弱點修補或是汰換的處置，避免駭客日後透過這些弱點破壞網路電話系統。

3.2 整體系統架構分析

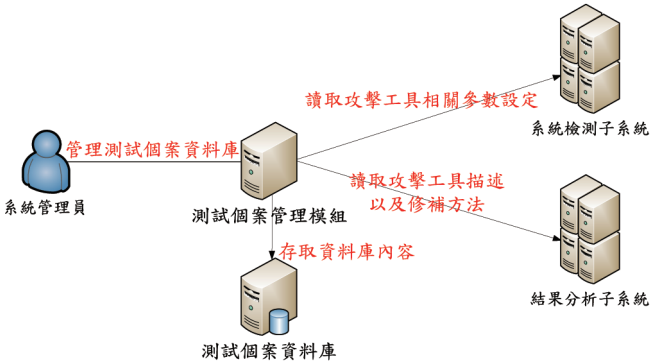
本研究所提出之SIP協定上的網路電話安全性檢測系統，主要由測試個案子系統、系統檢測子系統以及結果分析子系統，這三個子系統所組成，其整體架構以及子系統的說明如圖四：



圖四　本研究之整體系統架構圖

3.2.1 測試個案子系統

由於我們提出使用資料庫的方式儲存測試個案，使得本系統可採用新型態之攻擊手法對網路電話系統進行測試。因此，此子系統之主要功能在於提供其他子系統一個可供存取測試個案資料庫的介面以及管理者用以維護資料庫中所擁有之測試個案。如圖五，當系統掃描子系統要開始針對主機進行掃描時，會透過此介面去讀取目前所要執行的攻擊工具。除此之外，當掃描完成之後，結果分析子系統也會透過此介面存取測試個案資料庫，並提供該針對何種弱點進行修補之建議。



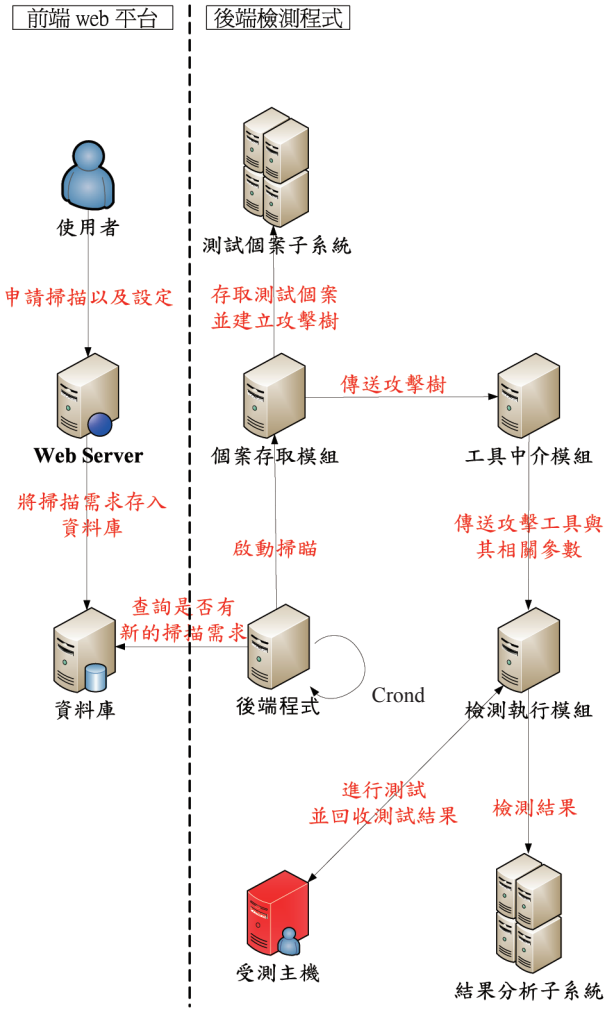
圖五　測試個案子系統運作流程

為了實現上述功能，本研究利用MySQL資料庫儲存測試個案。管理者會將攻擊工具所存放之路徑、分類、風險指數、工具敘述以及修補方法等相關資訊存入資料庫。

3.2.2 系統掃描子系統

系統掃描子系統為整個檢測系統之核心，此子系統分成前端的Web介面以及後端的程式兩部份。當使用者透過前端網頁完成掃描的申請及設定後，會將使用者所申請之資料存入資料庫中。之後，後端的程式會在排程的時間點自動去資料庫中查詢是否有新增的掃描需求。

如圖六，當有新的掃描需求時，後端應用程式便會呼叫個案存取模組去測試個案子系統中取用測試個案資料，用以建立進行測試時會使用到的攻擊樹。由於每個測試工具所需要用到的參數不一，因此本研究使用工具中介模組的方式，在此蒐集每個工具所需之參數，如：Call-ID、From Tag、To Tag、SIP Address、使用者帳號等。待工具中介模組將所有資訊都蒐集完成後，便會將攻擊樹及測試工具所使用到之相關參數交由檢測執行模組，由該模組對檢測對象主機進行測試，並回收測試後的結果。當測試完成之後，檢測執行模組會將檢測之後的結果交由結果分析子系統產生本次檢測的結果，並提供其相對應之說明與解決方案。

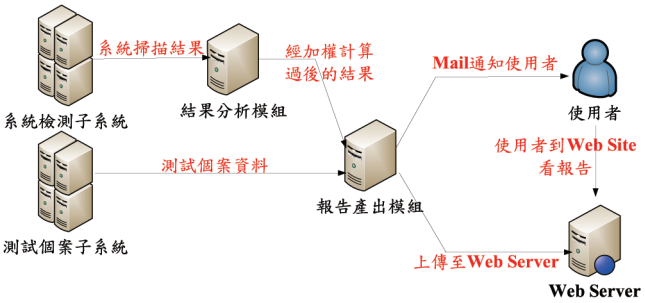


圖六　系統掃描子系統運作流程圖

為了實現上述之功能。本研究使用動態網頁技術JSP搭配MySQL資料庫完成前端Web介面之功能，而後端應用程式則使用Java進行撰寫，並使用Linux系統中的Cron服務來完成排程的工作[12]。

3.2.3 結果分析子系統

待系統掃描完成後，子系統內的結果分析模組會收到系統掃描子系統的掃描結果。如圖七，結果分析模組會根據當初使用者所設定之三種權重值（流行度、簡易度以及影響度）進行計算，找出對於該名使用者而言是比較需要注意的攻擊手法。除此之外，也會透過測試個案子系統所提供之介面，將這些攻擊手法所必須注意的事項以及該如何修補之相關建議一併匯入報告產出模組中，由報告產出模組負責編排並寫入資料庫中。同時，報告產出模組會自動發出Mail告知當初申請之使用者掃描已完成，可自行至網站中查看掃描報告。



圖七　結果分析子系統運作流程圖

為了實現上述之功能，我們撰寫程式從資料庫中去查詢使用者的mail以及掃描相關之資訊，並搭配使用JavaMail套件將掃描已完成之訊息透過mail的方式告知使用者。

4 實驗結果

本研究在此針對功能性以及差異性進行實際測試，驗證我們所提出之網路電話系統安全性檢測機制，以及是否比現有的網路電話系統檢測軟體能偵測出更多網路電話系統的漏洞。

(1)功能性測試：測試本研究使用滲透測試之方法搭配攻擊樹設計之檢測機制，是否能夠偵測網路電話系統中存在的漏洞。

(2)差異性測試：測試本研究所設計之檢測機制和其他功能類似之檢測軟體進行比較，檢視本研究所提供之檢測報告是否有比其他軟體所提供之報告，能給予使用者更多的幫助。

本研究以臺灣某縣市教育網路作為測試對象，但為了不影響該縣市教育網路之整體運作，本研究僅針對其中一個網段進行測試，檢測是否任何主機有遭到入侵之風險。

4.1 功能性測試

本研究所提出使用滲透測試進行系統檢測時，證明本系統可偵測到受測主機中所存在的漏洞[13]。除此之外，為了提供對新型漏洞的檢測能力，本研究採用攻擊樹之架構，可以不斷新增測試個案於攻擊樹中。由此說明攻擊樹可以有效提高本研究偵測新型漏洞的能力。因此，對於功能性測試，我們分為檢測機制以及攻擊樹偵測新型漏洞的能力這兩項驗證。由圖八的檢測報告可得知x.x.x.94主機並沒有提供網路電話服務。

圖八　x.x.x.94主機之檢測報告

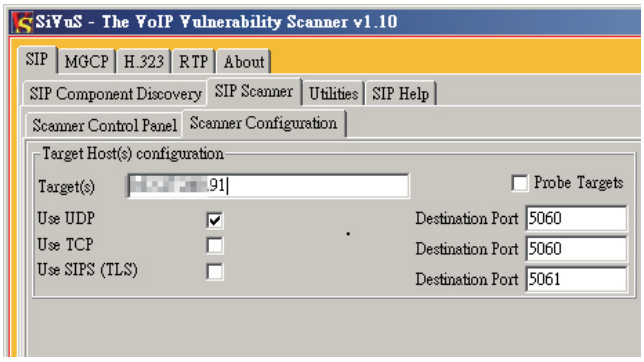
本次所掃描的網路區段中，僅x.x.x.91主機有提供網路電話服務，經過本系統之檢測後，其檢測結果如圖九所示：

圖九　x.x.x.91主機之檢測報告

從圖九可得知，該主機是使用IPTEL公司開發的網路電話套件Sip Express Router，所使用的版本為0.9.6並架設於Linux主機上。根據本研究所設定之權重值，檢測結果報告將所有漏洞分為高、中、低三種危險程度。使用者便可很清楚地知道哪些漏洞是需要儘快修補的。

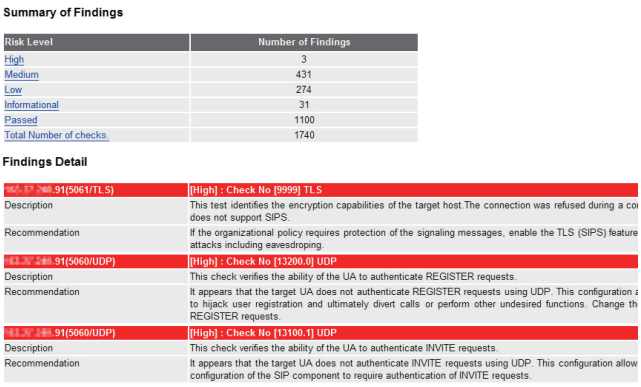
4.2 差異性測試

為了說明本研究所設定之檢測機制可有效地找出其他網路電話相關檢測軟體所無法找出之漏洞。因此，本研究使用目前在網路電話系統檢測中的知名弱點掃描軟體SiVuS，同樣也對該縣市教育網路x.x.x.90～x.x.x.99網段進行檢測，並比較本研究所提供的結果報告與SiVus的結果報告。由於該軟體同時只能針對一個IP進行檢測，在此僅就有提供網路電話服務之x.x.x.91主機進行檢測。如圖十。



圖十　使用SiVuS檢測x.x.x.91

SiVus所掃描的結果如圖十一所示，由圖中可得知SiVus掃描出三個高危險之弱點，這三點弱點分別是：沒有使用TLS、使用REGISTER方法時沒有進行認證、使用INVITE方法時沒有進行認證。



Summary of Findings

Risk Level	Number of Findings
High	3
Medium	431
Low	274
Informational	31
Passed	1100
Total Number of checks	1740

Findings Detail

91(5061/TLS)	[High] : Check No [9999] TLS
Description	This test identifies the encryption capabilities of the target host.The connection was refused during a co does not support SIPS.
Recommendation	If the organizational policy requires protection of the signaling messages, enable the TLS (SIPS) feature attacks including eavesdroping.
91(5060/UDP)	[High] : Check No [13200.0] UDP
Description	This check verifies the ability of the UA to authenticate REGISTER requests.
Recommendation	It appears that the target UA does not authenticate REGISTER requests using UDP. This configuration a to hijack user registration and ultimately divert calls or perform other undesired functions. Change th REGISTER requests.
91(5060/UDP)	[High] : Check No [13100.1] UDP
Description	This check verifies the ability of the UA to authenticate INVITE requests.
Recommendation	It appears that the target UA does not authenticate INVITE requests using UDP. This configuration allow configuration of the SIP component to require authentication of INVITE requests.

圖十一　SiVuS掃描結果報告

將SiVus的報告與本研究的結果報告圖九比較，本研究將該主機的漏洞以實際的駭客手法表示出可能遭到何種攻擊。而本系統也發現該主機在發出BYE訊息時並沒有執行認證之動作，意即該主機無法抵擋TEARDOWN的攻擊；而 SiVus軟體所提供之報告僅能告知使用者該主機對REGISTER以及INVITE訊息沒有進行認證，並沒有偵測到BYE訊息沒有認證動作的潛在風險[14]。

5 結論

在未來幾年內，網路電話可望成為繼電子郵件之後，另一個生活中不可或缺的資訊應用科技。然而，任何新興網路殺手級應用的發展，例如WWW、電子郵件、網路電話等，都像是雙面刃，背後隱藏了許多未知的風險。

現今的系統檢測方式大多是使用弱點掃描的方式，而弱點掃描的報告對於經驗不足的系統管理者而言，只能告知目前系統有哪些漏洞可能遭到利用，並沒有辦法找出這些漏洞之間彼此的相關性。因此，本研究採用滲透測試之概念，設計一套整合性的網路電話系統安全性檢測機制，搭配使用攻擊樹模擬駭客攻擊之手法以及不同的攻擊測試個案對網路電話系統進行檢測。期望能夠幫助經驗不足的系統管理者，找出組織內部所使用的網路電話系統中所存在的弱點，並提供該弱點的修補方案給管理者參考。

致謝

本研究計畫部份經費來自國家科學委員會專題研究計畫NSC 96-2221-E-224-026以及TWISC@NCKU補助編號NSC 97-2219-E-006-009

參考文獻

[1] 張勁為，*網路弱點評估*，2006，http://www.nii.org.tw/tanet/event_060501/default.asp

[2] Dustin Trammel, "*VoIP Attacks!*," 2006, http://www.dustintrammell.com/presentations/VoIP-Attacks.pdf

[3] 賈文康，*SIP會談啟始協議操典*，台灣：文魁資訊，2005。

[4] 林佳輝，*基於安全監聽環境下針對SIP／ENUM通訊架構進行網路電話與即時訊息監聽*，台灣：國立雲林科技大學，2004。

[5] RFC 3261, *"SIP: Session Initial Protocol*," 2002.

[6] Tung-Ming Koo, et al., "*A SPIT Prevention System by Black/White List for P2P SIP*," Journal of Beijing Jiaotong University, Vol. 32, No. 5, Oct. 2008. pp.1-7.

[7] David Endler, Mark Collier, "*Hacking Exposed VoIP*," NewYork: McGraw Hill, 2006.

[8] Bruce Schneier, "*Attack Tree*," 1999, http://www.schneier.com/paper-attacktrees-ddj-ft.html

[9] Shawn McGann, Douglas C. Sicker, "*An Analysis of Security Threats and Tools in SIP-Based VoIP Systems*," 2nd Annual VoIP Security Workshop Washington DC, 2005.

[10] 古東明、劉作仁、沈志昌，*基於SIP協定實現網路電話系統安全性檢測機制*，第十八屆資訊安全會議，花蓮：東華大學，2008。

[11] 劉作仁、沈志昌，*SIP網路電話安全攻擊分析與探討*，*RUN!PC*，167期，頁176-182，12月2日。台灣：旗標資訊，2007。

[12] D. Geneitakis, et al., "*SIP Message Tampering : The SQL code Injection Attack*," 13th International Conference on Software, Telecommunications and Computer Networks, Split: Croatia, 2005.
[13] 蔡威廷、高勝助，*Honeypot based VoIP防禦系統*，全國計算機會議，台中：亞洲大學，2007。
[14] SecurityFocus, "*Two attacks against VoIP*," 2006, http://www.securityfocus.com/infocus/1862

作者簡歷

古東明（Tung-Ming Koo），國立雲林科技大學資管系副教授。主要研究領域為資訊安全、P2P網路、網路電話等。

劉作仁（Zuo-Ren Liou），民國97年畢業於國立雲林科技大學資管所碩士班，目前工作於行政院國家資通安全會報技術服務中心。主要研究領域為網際網路、資訊安全、網路電話等。

沈志昌（Ching-Chang Shen），於民國97年在國立雲林科大學取得博士學位，目前是嶺東科技大學資訊科學系助理教授。主要研究領域為網路安全、網路管理以及網路電話相關議題。

游婷敬（Ting-Ching Yu）目前就讀於國立雲林科技大學資管所。主要研究領域為資訊安全、金鑰管理。

設計U化博物館學習服務架構以縮短數位學習落差
Designing a U-Museum Service Framework to Bridge Digital Learning Divide

翁瑞鋒 Jui-Feng Weng[1], 曾憲雄 Shian-Shyong Tseng[1,2], 廖岳祥 Anthony Y. H. Liao[2], 蘇俊銘 Jun-Ming Su[1]
[1]交通大學資訊工程學系
[2]亞洲大學資訊科學與應用學系
roy@cis.nctu.edu.tw, sstseng@asia.edu.tw, sstseng@cis.nctu.edu.tw, liao@mail.isa.asia.edu.tw, jmsu@csie.nctu.edu.tw

摘要

由於偏遠中小學學童對於資訊工具接觸的機會較少，導致在資訊教育的學習程度，與一般都市化程度較高的學童有所落差，我們稱此為「數位學習落差」。在我們的觀察中發現，雖然偏鄉地區學校或家庭的資訊學習設備不足，但以整個區域的公共數位學習資源來說，例如，博物館，其實是能提供相關的數位學習資源的。若是能協助這些偏鄉學生利用博物館的學習資源，將有效縮短數位學習落差。在博物館的學習環境中，與學校教育不同之處，是強調自我導向式學習與學習場域。近年，由於無線射頻識別（Radio Frequency Indentification, RFID）等通訊技術的普遍，RFID具有辨識學習者身分、所在的位置與及移動的功能，並可藉此資訊搭配學習者個人資訊，提供U化學習服務。因此，本論文參考Instructional Management Systems Global Learning Consortium（IMS/GLC）所提出的 Learner Information Package（LIP）標準，提出了學習者資源管理系統架構（Learner Information Management Framework, LIMF），其中學習者資料模型：有學習者識別資料（Profile）、學習模式資料（Preference）、學習活動資料（Learning Activity），以及學習成就資料（Learning Portfolio），來做為U-Learning環境中學習者資訊之標準欄位。資料處理模型：提供學習者識別服務、學習者活動感知服務與學習資源服務，並提出Web Service技術，以提供系統架構在存取性、標準化與延伸性上，有更好的支援。

關鍵字：數位學習落差、無所不在的學習、博物館學習、學習者資訊、IMS LIP標準。

Abstract

Due to lack of opportunities in utilizing digital learning auxiliary tools, it causes the existence of so called “Digital Learning Divide” between the students of rural or remote areas and those of urban areas. In this research, it is found that the public learning facilities in the community, for example, the museums, can provide related digital learning resources in spite of the shortage of digital learning facilities at the schools and families in rural or remote areas. If the students in the rural or remote areas are assisted to utilize the learning resources, it can bridge the digital learning divide effectively. However, it is different from the education in the school; the education in the museum is informal education which is emphasized on the learner-centered self-learning. In recent years, due to the advance and availability of RFID technology, and the functions of RFID in recognizing the learners’ identities, locations, and movement, it can provide U-Learning services to learners with their personal information. Therefore, in this research, IMS Learner Information Package (LIP) standard is referred to construct a Learner Information Management Framework (LIMF), in which the Learner Model is composed of learner's Profile, Preference, Learning Activity, and Learning Portfolio as the standard fields of learner's information. The Processing Model in LIMF contains the functions of learner identification service, learner activity aware service, and learning resource provision service, and furthermore the web service technology is employed to provide better U-Learning support in accessibility, standardization, and extensibility.

Keywords: Digital Learning Divide, Ubiquitous Learning, Museum, Learning Information, IMS LIP Standard.

1 緒論

近年來，資訊科技及網際網路技術日新月異地快速發展，有如速食一般地容易取得。因此，具備基本的資訊工具使用知識，更是不可或缺。然而，在這樣發展快速的競爭環境當中，不免會有資源分配不平衡及浪費的現象產生。對於偏遠中小學及低收入戶資訊網路的使用及利用資訊工具學習的便利性，相較於一般地區的學童，有非常顯著地落差，儼然形成嚴重的城鄉差距。偏遠中小學學童由於對於資訊工具接觸的機會少，導致在資訊教育上的學習程度，與一般都市化程度高的學童便會有所落差，我們稱此為「數位學習落差」。在我們的觀察中發現，雖然地區學校內或家庭內資訊學習設備不足，但以整個區域的數位學習資源來說，一些博物館其實是能提供相關的數位學習資源的，例如台灣中部地區的自然科學博物館、兒藝館等，就有豐富的數位內容館藏或展覽，若是能輔助這些偏鄉學童利用博物館的資源，將是一個解決數位學習落差的途徑。因此，如何透過資訊技術的輔助，有效導引學生使用鄰近區域內的博物館資源，及改善