以網路流量偵測 SSH 字典攻擊之研究

薛昱仁
國立高雄大學亞太工商管理學系
m0957113@mail.nuk.edu.tw

蕭漢威
國立高雄大學資訊管理學系
hanwei@nuk.edu.tw

摘要

隨著各式網際網路應用程式的快速發展，在網路上進行身份認證是無可避免的流程，密碼認證的方法是目前仍無法取代的認證方式。而字典攻擊手法為利用字典中經常出現的字詞猜測使用者可能的密碼，所以這類字典攻擊的技術仍被入侵者拿來做為主要的入侵手段之一。近年來觀察台灣學術網路，經常有許多入侵者以字典攻擊的方法試圖入侵學校的主機，這類的攻擊方法因為網路程式的技術日益發達，有許多利用字典攻擊自動入侵的機制被發展出來，所以這類的攻擊事件有越來越嚴重的趨勢，造成了各級網管人員的困擾。

本研究利用了網路 NetFlow 的流量資料，蒐集了針對 SSH 進行字典攻擊的流量記錄，以資料探勘中分類分析的技術建立了一個有效的偵測模組。在本研究中實證了這個偵測模組有很好的效果，在預測準確率上可達 90% 以上的正確率。相信這個研究的結果未來可以有效的提供網路管理人員從網路流量的記錄中自動找出那些潛在進行的 SSH 字典攻擊行為，對於提高網路安全防護具有很大的幫助。

關鍵詞：字典攻擊、網路流量、資料探勘、網路攻擊

Abstract

With the rapid growth of technology, there are a lot of applications system needs to authenticate on the Internet environment. Password is an intrinsic way for authentication in our daily life. Adversaries attempt to login accounts by trying all possible password is called dictionary attack. When we inspected the server authentication logs in the TANET environment, there are a lot of login failed records. It implies that dictionary attack is a serious intrusive event. and is needed to defend .

In this paper, we proposed an SSH dictionary attack detection module. We used two well-known data mining classification algorithms, Naïve Bayes and C4.5 to build our detection module. We collected real world SSH normal and dictionary attack NetFlow data in a month as training samples. As a research result, This detection module has over and above 90% accuracy detection rate. In the future, we hope this research result that could be helpful for network managers to detect implicit dictionary attack behaviors using network traffic data and improve the network security.

Keywords: Dictionary Attack, NetFlow, Data Mining, Network Attack

1. 前言

網際網路的快速發展，使得各式各樣的網路服務興起，如網路拍賣、網路銀行、電子信箱與線上遊戲等。這些網路服務普遍上是使用密碼認證機制，來提供有關於個人化的服務，例如可以檢視該帳號的相關資料紀錄，如電子郵件、網路銀行存款餘額等。起先註冊時，使用者需在網路服務系統設定一組系統帳號密碼，之後使用者登入時，只需登入先前設定的帳號密碼即可登入系統，使用該系統所提供的服務。密碼認證是檢驗使用者是否有權限存取這些網路服務最簡便也最普及的方法。雖然有其他的認證方式如公鑰加密認證(Public-Key Cryptography)[3]、智慧卡認證(Smart Card Authentication)[5]與生物辨識(Biometrics)[9]等，但這些方法因為建置成本過高，在一般網路服務認證使用上並不普及。

密碼認證雖然簡便，但也有其缺點。例如密碼的命名與使用者的習慣有關，缺乏安全管理概念的使用者會挑選簡便與容易記憶的密碼，如簡單英文單字與數字組合、生日、身份證字號、電話號碼等。並且使用者最常使用的密碼最多只有四到五組[1]，在現今大量需要密碼認證的網路服務下，密碼的重複使用率很高[4]。再者，使用者貪圖方便或職務管理不得已狀況之下，會有多人共用一組帳號密碼情形發生，例如管理者帳號只有一組，但是卻有兩個管理員，這兩個管理員就會共用同一組簡單容易記憶的管理者帳號密碼。因此，由使用者不良的密碼使用習慣，入侵者便發展出字典攻擊(Dictionary Attack)來攻擊這些容易記憶的密碼帳號。如 2002 年國外知名網路拍賣網站 eBay 發生入侵者利用字典攻擊工具破解這些使用簡便密碼的賣家帳號，利用這些賣家帳號，進行非法的網路詐欺行為，而這些被盜帳號的擁有者，就成為入侵者進行網路詐欺行為的代罪羔羊[10]。由 eBay 字典攻擊事件可得知使用簡便密碼會帶來網路安全的問題，但因為使用者使用密碼不良習慣，目前尚未出現其他方案能替代密碼做為系統認證方式，字典

攻擊儼然形成一個網路安全上的隱憂。

觀察台灣學術網路環境中的伺服器日誌紀錄檔(Server Log)時，經常可以發現許多針對SSH(Secure Shell Handler)服務的字典攻擊事件發生。伺服器開啟 SSH 服務能讓管理者透過網路，以加密連線方式，遠端登入與管理伺服器日常業務。但攻擊者以字典攻擊方式，攻擊開啟 SSH 服務的伺服器，試圖取得伺服器的登入權限。台灣學術網路各單位因為研究或教學等需求，自行架設伺服器狀況十分普遍，然而因維護人員缺乏密碼管理概念或者疏忽管理的緣故，某些伺服器的管理者帳號的密碼，也常常挑選簡便與容易記憶的密碼，這些採用簡便密碼的管理者帳號，便成為學術網路內字典攻擊的主要瞄準目標。

台灣學術網路的環境使得網路管理者不易取得各單位伺服器的日誌檔。網路管理者欲維持管轄範圍內的網路安全，有其必要發展從其他網路管理資訊著手的偵測方法。因此，本篇研究欲利用 SSH 協定與 SSH 字典攻擊的特性，以網路 NetFlow 流量資料偵測針對 SSH 協定所發動的字典攻擊，試圖以資料探勘分類分析方法，提出 SSH 字典攻擊偵測模組，並實際利用高雄大學的網路環境驗證其偵測效能。

2. 文獻探討

本研究接下來欲探討與 SSH 字典攻擊相關文獻，包括字典攻擊的定義、字典攻擊細項分類與說明與字典攻擊的攻擊特徵。並且說明相關防禦 SSH 字典攻擊的方法與其缺點與限制。

2.1 字典攻擊

對於字典攻擊意指字典攻擊為在一組小範圍的字典檔中，攻擊者從中嘗試使用各種可能的密碼，利用這些可能的帳號密碼登入伺服器，直到找到正確的密碼為止。過去的相關研究中，在 Pinkas and Sander[7]曾對字典攻擊有較明確的定義：

> “A small password domain enables adversaries to attempt to login to accounts by trying all possible passwords, until they find the correct one. ”

當攻擊者欲嘗試的密碼皆驗證完畢無法順利登入時，字典攻擊也會停止。字典攻擊還可細分為線上(Online)與離線(Offline)兩種攻擊方式[7]，線上字典攻擊定義是攻擊者在網路上直接對伺服器做帳號密碼登入驗證，以便檢查猜測的密碼是否可正確登入，線上字典攻擊會在伺服器日誌紀錄檔中留下大量的試誤紀錄，如先前所提到的 eBay 字典攻擊事件所採用的攻擊方式。而離線字典攻擊不需與伺服器做互動帳號密碼驗證，攻擊者透過伺服器中其他程式漏洞盜取伺服器的密碼檔。取得密碼檔後，可讓攻擊者不需透過登入伺服器，可離線使用如 John the Ripper[6]的離線字典攻擊工具，在攻擊者的電腦驗證所猜測伺服器使用者的密碼是否正確。SSH 字典攻擊需要對伺服器做即時帳號密碼登入驗證，可歸屬為線上字典攻擊，因此本研究是針對線上字典攻擊行為進行偵測。

本研究從網路流量觀察到 SSH 字典攻擊特徵。當 SSH 字典攻擊發動時，攻擊者會先大規模刺探一段網域內有哪些伺服器開啟 SSH 服務，針對網域中每個 IP 針對預設 SSH 通訊埠 22 發送 TCP SYN 封包 ，若有網域中有伺服器於通訊埠 22 回應 ACK 封包，字典攻擊程式就認定該伺服器有開啟 SSH 服務，之後就針對有回應的伺服器進行一連串的 SSH 字典攻擊。

2.2 目前防禦 SSH 字典攻擊的方法

目前防禦 SSH 字典攻擊的方法主要還是以伺服器管理為主，如稽核伺服器日誌檔、公私鑰非對稱加密認證、修改伺服器 SSH 服務通訊埠。以下部份將深入探討這些防禦 SSH 字典攻擊的方法以及其缺點。

第一種防禦 SSH 字典攻擊方法為稽核伺服器日誌檔(e.g. auth.log)中，若有出現 SSH 字典攻擊的相關行為的 IP，例如同一個 IP 進行 SSH 連線認證，使用不存在的帳號登入失敗次數達數次以上，便使用防火牆或進行 IP 封鎖或者加入拒絕連線的列表中(e.g. hosts.deny)。在伺服器日誌檔中出現 SSH 字典攻擊的相關行為如表 1。

表1. auth.log 中出現字典攻擊行為的相關紀錄

- Jul 8 03:14:14 host1 sshd[13676]: Invalid user divine from 192.168.0.1
- Jul 8 03:14:19 host1 sshd[13680]: Invalid user popa3d from 192.168.0.1
- Jul 8 03:14:26 host1 sshd[13684]: Invalid user aptproxy from 192.168.0.1
- Jul 8 03:14:32 host1 sshd[13688]: Invalid user desktop from 192.168.0.1
- Jul 8 03:14:38 host1 sshd[13692]: Invalid user workshop from 192.168.0.1

在表 1 中，divince、popa3d、aptproxy 等帳號都是伺服器中不存在的帳號，192.168.0.1 這個 IP 試圖使用這些不存在的帳號進行 SSH 認證登入，並且登入失敗次數超過數次以上，透過稽核日誌檔的方式，將 192.168.0.1 加入防火牆封鎖 IP 或拒絕連線列表中，以防該 IP 下次惡意攻擊行為影響到伺服器系統安全。相關偵測軟體如 Denyhosts[2]，安裝軟體後透過稽核日誌檔，封鎖這些被偵測出來

的具有字典攻擊行為的 IP，還可以進一步同步到 Denyhosts 的共享黑名單中，讓所有安裝 Denyhosts 的伺服器共同使用與封鎖。

稽核日誌檔的防禦方法缺點為若管理者無法拿到伺服器日誌檔的時候，就無法針對日誌檔中進行字典攻擊的 IP 進行封鎖，例如在網路管理業務上，不易取得與管理底下授權給其他單位的伺服器日誌檔。在無法稽核日誌檔的狀況下，便無法利用日誌檔得知伺服器曾經遭受過哪些網路 IP 的字典攻擊。此外，共享黑名單的機制屬於封鎖黑名單表列上的 IP，若字典攻擊者的 IP 不在黑名單上，就無法事先進行阻擋。因此，對於不在黑名單上的字典攻擊者的 IP，共享黑名單也無法全面阻擋其字典攻擊。

第二種防禦 SSH 字典攻擊的方法，則是利用非對稱金鑰加密認證方式。使用者可以在 SSH 客戶端選擇產生一對 RSA 或 DSA 演算法的公鑰與私鑰，將客戶端產生出來的公鑰置入欲登入的 SSH 伺服器中的帳號相關設定資料夾中。如此一來，SSH 客戶端欲登入 SSH 伺服器時便可使用私鑰進行認證，不需要輸入帳號密碼，即可完成登入程序。這種以公私鑰加密的認證方式能有效防禦 SSH 字典攻擊，因為使用者登入時不需要輸入帳號密碼，直接使用約定的公私鑰認證即可登入。字典攻擊者因為無法產生與認證公鑰對應的私鑰，就無法順利登入伺服器。

使用非對稱金鑰認證的防禦方法缺點為非對稱金鑰認證機制並不普及。原因有兩點，一為管理者大量派發私鑰不易，管理者得先利用其他的安全連線傳輸將私鑰派送給所有使用者。若使用者眾多時，管理者就不容易兼顧派送私鑰的安全性與便利性。二為使用者接受程度不高，對於使用者而言，帳號密碼登入方式也比非對稱金鑰認證方式熟悉並且簡單許多。

第三種防禦方法為修改 SSH 服務通訊埠，針對 SSH 字典攻擊的行為，伺服器管理者的修改 SSH 服務通訊埠從 Port 22 修改為其他的通訊埠號碼。因為普遍的 SSH 字典攻擊都是針對 SSH 預設的通訊埠進行攻擊，字典攻擊者對 SSH 預設通訊埠進行連線時，若發現連線失敗就會停止攻擊。所以修改 SSH 服務的通訊埠，便能有效的防禦 SSH 字典攻擊。

修改 SSH 服務通訊埠的防禦方法缺點為管理者雖然修改 SSH 通訊埠，但攻擊者只要進行通訊埠掃描(Port Scan)，攻擊者就能得知管理者修改過的 SSH 通訊埠號碼。攻擊者將字典攻擊程式目標 SSH 通訊埠修改為掃描到的通訊埠後，伺服器仍然會遭受到字典攻擊。

綜合上述的各防禦方式的缺點，若我們能由流經網路骨幹路由器的流量特性，蒐集 SSH 字典攻擊的流量資料建立出一個有效的分類偵測模式，則可找出網路上發生的 SSH 字典攻擊事件，並且提高網路的防禦能力。因此，本研究利用網路 NetFlow 流量資料，利用資料探勘的分類分析演算法提出一個偵測 SSH 字典攻擊的模組。

3. 網路流量偵測字典攻擊模組

文獻中提到防禦 SSH 字典攻擊大多從伺服器管理下手，網路管理者若無權限管理伺服器時，便無法防禦 SSH 字典攻擊。對於網路管理者而言，網路流量資料相對取得容易，本研究便試圖使用網路流量資料進行偵測與防禦。而 SSH 協定使用加密連線，無法以監聽網路封包內容的方式偵測字典攻擊。本研究使用 NetFlow 資料，分析正常 SSH 連線與 SSH 字典攻擊在 NetFlow 資料中的異同之處。並且根據兩者差異之處，進一步發展偵測 SSH 字典攻擊的方法。

3.1 SSH 連線網路流量資料

本研究利用 NetFlow 資料觀察正常 SSH 連線資料，如表 2。

表2. 正常客戶端 SSH 連線 NetFlow 資料

SIP	DIP	SPort	DPort	Octs	Pkts
sip1	sip2	22	57103	6480	49
sip2	sip1	57103	22	6816	66

表 2 中第一個欄位 SIP 是連線來源 IP(Source IP)。第二個欄位 DIP 是連線目標 IP(Destination IP)。第三個欄位是 Sport 是連線來源通訊埠(Source Port)。第四個欄位是連線目標通訊埠(Destination Port)。第五個欄位為 Octs 是傳輸的 bytes 數(Octets)。第六個欄位為 Pkts，是傳輸的封包數(Packets)。從表 2 中可以發現正常 SSH 連線在 NetFlow 資料裡面總共彙整成為兩筆流量資訊。第一筆為伺服器(sip1)流向客戶端(sip2)的流量，第二筆為客戶端流向伺服器的流量。

SSH 字典攻擊的網路流量資料如表 3。資料來源為高雄大學內部收集到一整天實際進行 SSH 字典攻擊 NetFlow 資料。表 3 的欄位名稱意思與表 2 相同。

表3. SSH 字典攻擊 NetFlow 資訊

SIP	DIP	SPort	DPort	Octs	Pkts
ip1	ip2	46310	22	60	1
ip1	ip3	44763	22	60	1
ip1	ip4	56004	22	60	1
ip1	ip5	54297	22	60	1

ip1	ip6	35660	22	60	1
…	…	…	…	…	…
ip7	ip1	22	41701	2316	14
ip8	ip1	22	47847	2464	15
ip1	ip9	47847	22	1268	14
ip10	ip1	22	47359	2268	12
ip11	ip1	22	59326	2351	14
…	…	…	…	…	…

表 3 中流量資料前五行是攻擊者(ip1)發出 TCP SYN 封包刺探目標網域中的 IP 是否有開啟 Port 22 服務。TCP SYN 一個封包大小為 60 bytes，攻擊者使用 TCP SYN 封包欲對網域中的 IP 進行 TCP 連接。後五行是攻擊者針對先前有回應 TCP ACK 的 IP，進行 SSH 字典攻擊。

3.2 SSH 字典攻擊偵測模組

本研究將分辨正常 SSH 客戶端的網路流量與 SSH 字典攻擊的網路流量視為資料探勘中的分類問題。使用兩種知名的資料探勘的分類演算法，貝式機率(Naïve Bayes)演算法與 C4.5 決策樹(Decision Tree)[8]演算法，訓練建立 SSH 字典攻擊分類模組。利用已知的正常 SSH 連線的流量資料與 SSH 字典攻擊資料訓練建立 SSH 字典攻擊分類模組，利用分類模組偵測網路流量中是否有未知的 SSH 字典攻擊存在。本研究提出 SSH 字典攻擊偵測模組如圖 1。

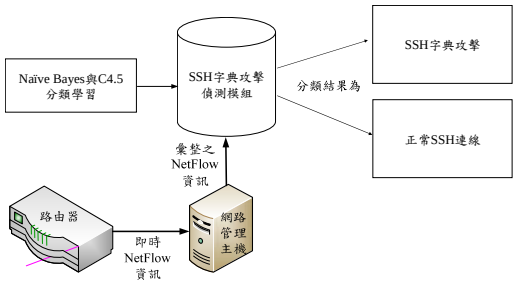

圖1. SSH 字典攻擊偵測系統架構

為建立圖 1 的 SSH 字典攻擊偵測模組，本研究以五分鐘為單位，彙整高雄大學管理學院路由器一個月內的 NetFlow 資料，SSH 字典攻擊 NetFlow 資料與正常 SSH 連線 NetFlow 資料各 500 筆。利用伺服器日誌檔驗證收集真實網路中的 SSH 字典攻擊 NetFlow 資料與正常 SSH 流量資料。本研究分析比較正常 SSH 連線時的 NetFlow 資訊(e.g. 表 2)與發動 SSH 字典攻擊時的 NetFlow 資訊(e.g. 表 3)，提出四個可能有效的流量變數，

1. SSH 客戶端開啟的總通訊埠數(Port Counts)：計算五分鐘內，計算 NetFlow 資料中單一 SSH 客戶端開啟向所有 SSH 伺服器連線的通訊埠的總和，挑選此變數的原因為 SSH 字典攻擊發動時，會開啟比正常 SSH 連線還要多的通訊埠(e.g. 表 3 ip1)。

2. SSH 客戶端傳輸總 bytes 數(Octets Sum)：為單一 SSH 客戶端向所有 SSH 伺服器傳輸的 bytes 數總和，挑選此變數原因為比較表 2 與表 3，單一客戶端正常 SSH 連線，在五分鐘之內傳輸的總 byte 數會比頻繁的 SSH 字典攻擊傳輸的總 byte 數總和較小。

3. SSH 客戶端傳輸的總封包數(Packets Sum)：SSH 客戶端傳輸的總封包數為計算五分鐘內，計算 NetFlow 資料中單一 SSH 客戶端向所有 SSH 伺服器傳輸的封包數，挑選此變數原因為比較表 2 與表 3，單一客戶端正常 SSH 連線，在五分鐘之內傳輸的總封包數會比頻繁的 SSH 字典攻擊傳輸的總封包數也要來得小。

4. SSH 客戶端傳輸的平均封包量(Average Packet Sizes)：為 SSH 客戶端傳輸的總封包數除以 SSH 客戶端傳輸的總封包數，挑選此變數原因為比較表 2 與表 3，SSH 字典攻擊只會傳輸欲驗證的帳號密碼封包，比起正常的 SSH 連線會輸入多樣化的系統管理指令，單一封包大小與格式較固定。

3.3 實證評估

本研究收集實際 SSH 字典攻擊與正常 SSH 連線網路流量，整理為本研究提出四個流量變數後，使用貝式機率演算法與 C4.5 決策樹演算法進行分類，並且使用十折交叉驗證(10-Fold Cross Validation)。而實證結果貝式機率演算法對於 SSH 字典攻擊的分類正確率為 91.9%，C4.5 演算法正確率則是 91.6%。其他分類效能評估結果如表 4。

表4. 貝式機率與 C4.5 演算法的分類效能結果

	準確率	召回率	正確率	F-measure
貝式機率	99.3%	84.4%	91.9%	91.2%
C4.5 決策樹	98.8%	84.2%	91.6%	90.9%

由表 4 得知，貝式機率演算法的準確率(Precision Rate)為 99.3%，意指辨識結果為 SSH 字典攻擊中，每次的偵測判斷能準確辨識出 SSH 字典攻擊的資料正確性為 99.3%。而 C4.5 決策樹演算法的準確率為 98.8%。貝式機率演算法的召回率(Recall Rate)為 84.4%，意指透過貝式機率演算法在實驗樣本中對於所有 SSH 字典攻擊紀錄，有 84.4%的 SSH 字典攻擊資料都能被正確地發現出來。而 C4.5 決策樹演算法的召回率為 84.2%。貝式機率演算法的正確率(Accuracy Rate)為 91.9%，意指辨識結果中，能正確分辨 91.9%的正常 SSH 連線資料與 SSH 字典攻擊資料。而 C4.5 決策樹演

算法的正確率為 90.9%。在資料探勘分類分析結果中，準確率與召回率有此消彼長的情形。為了客觀評估本研究訓練出來的 SSH 字典攻擊偵測模組，本研究另外計算 F-measure 數值。而 F-measure 公式為 2(Precision Rate＊Recall Rate) / (Precision Rate+ Recall Rate)，貝式機率演算法的 F-measure 為 91.2%，而 C4.5 決策樹演算法的 F-measure 為 90.9%。

實證評估發現貝式機率演算法對於 SSH 字典攻擊的分類效果比 C4.5 決策樹演算法來的優異。而兩種分類演算法對於分辨 SSH 字典攻擊均有九成以上的正確率，分類效果相當良好。因此，對於 SSH 字典攻擊偵測，使用貝式機率演算法與 C4.5 決策樹演算法均有不錯的效果。

本研究另外使用資訊獲利(Information Gain)計算四個本研究所提出偵測流量變數的重要程度排序，並且同樣以十折交叉驗證，計算結果重要排序如表 5。

表5. 分類流量變數重要程度排序

排名	分類屬性
1	SSH 客戶端開啟的總通訊埠數
2	SSH 客戶端傳輸的平均封包量
3	SSH 客戶端傳輸總位元數
4	SSH 客戶端傳輸的總封包數

表 5 中，排名數字越小代表越重要。最重要的分類流量變數為 SSH 客戶端傳輸的總封包數，意指 SSH 客戶端開啟的總通訊埠數與其他三個流量變數在分類效果上比較容易分辨流量資料中是否有存在未知的 SSH 字典攻擊資料。可能的原因為當 SSH 字典攻擊發動時，從一開始大量發送 TCP SYN 封包與之後一連串的字典攻擊的行為均會開啟許多的通訊埠。而跟正常 SSH 連線所開啟的總通訊埠數比較，SSH 字典攻擊客戶端開啟的總通訊埠數明顯較多。因此，使用 SSH 客戶端開啟的總通訊埠數流量變數能明顯比較出 SSH 字典攻擊與正常 SSH 連線行為的差異。

而次重要為 SSH 客戶端傳輸的平均封包量，意指 SSH 客戶端傳輸的平均封包量流量變數分類效果比其餘兩個流量變數較佳。可能的原因為，SSH 字典攻擊發動時，一開始大量發送固定 TCP SYN 封包，大小皆為固定大小，之後一連串的字典攻擊的封包內容皆為欲驗證的帳號密碼，所以平均封包量大小也相當固定。而正常的 SSH 連線流量產生因為是管理者遠端登入管理伺服器，所以平均封包量取決於管理者登入後所進行的管理行為(e.g. 輸入的指令、閱讀檔案、程式輸出畫面等)，傳輸平均封包量大小根據管理者的行為較不固定。因此，使用 SSH 客戶端傳輸的平均封包量流量變數能明顯比較出 SSH 字典攻擊與正常 SSH 連線行為的差異。

4. 結論

本研究收集實際 SSH 字典攻擊與正常 SSH 連線的網路流量，利用資料探勘中的兩種分類演算法，貝式機率演算法與 C4.5 決策樹演算法，進行 SSH 字典攻擊的分類分析。利用兩種分類演算法，建立 SSH 字典攻擊的偵測模組。並且本研究提出四個有效的偵測分類屬性，對於 SSH 字典攻擊有不錯的偵測效果。研究結果貝式機率演算法與 C4.5 決策樹演算法均有九成以上的準確率，而貝式機率演算法分類表現比 C4.5 決策樹演算法來的優異。

建議未來相關的偵測 SSH 字典攻擊研究中，若有使用分類分析技術，可以考慮貝式機率演算法。另外在分類屬性方面，就本研究所評估的四種不同的流量變數，對於 SSH 字典攻擊發動時，客戶端大量開啟的總通訊埠數量，該流量變數在偵測 SSH 字典攻擊時，在判斷攻擊事件的偵測效力是要優於其他三種的流量變數。希望未來研究能朝向偵測多種網路協定上的字典攻擊發展，如 http、telnet、pop3、https 等。偵測網路範圍也能朝向更大的網路範圍，而偵測的字典攻擊型態也能更多元。

參考文獻

[1] A. Adams and M. A. Sasse, “Users Are Not the Enemy, ” Commun. ACM., Vol. 42, No. 3, pp. 40–46, December 1999.

[2] Denyhosts Project, http://denyhosts.sourceforge.net, July 2008.

[3] S. Halevi and H. Krawczyk, “Public-key Cryptography and Password Protocols,” ACM Trans. Inf. Syst. Securi., Vol. 2, No. 3, pp. 230–268, August 1999.

[4] B. Ives, K. R. Walsh, and H. Schneider, “The Domino Effect of Password Reuse, ” Commun. ACM., Vol. 47, No. 4, pp. 75–78, April 2004.

[5] H. S. Kim, S. W. Lee, and K. Y. Yoo, “Id-based Password Authentication Scheme Using Smart Cards and Fingerprints, ” ACM SIGOPS Oper. Syst. Rev., Vol. 37, No. 4, pp. 32–41, October 2003.

[6] Openwall Project, “John the Ripper Password Cracker, ”http://www.openwall.com/john/, July 2008.

[7] B. Pinkas and T. Sander, “Securing Passwords against Dictionary Attacks, ”In Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, November 18-22, 2002, pp. 161–170.

[8] J. R. Quinlan, C4.5: Programs for Machine Learning, San Mateo, CA: Morgan Kaufmann, 1993.

[9] N. K. Ratha, J. H. Connell, and R. M. Bolle, " Enhancing Security and Privacy in Biometrics-based Authentication Systems, " IBM Syst. Journal., Vol. 40, No.3, pp. 614–634, April 2001.

[10] T. Wolverton, "Hackers Find New Way to Bilk eBay Users," http://www.news.com/2100-1017-868278.html, March 2002.