適用於入侵偵測之模糊關聯法則機制研究

施衣喬、曹偉駿

E-mail: 9222463@mail.dyu.edu.tw

摘 要
目前大多數入侵偵測系統的架構可分為主機式或網路式的方式來判別及防制電腦駭客，無論是哪種架構，都是以行為樣式比對的方法來判定是否為駭客入侵。而每種架構的偵測系統，其偵測是否為駭客入侵的技術也可大致區分為兩類，建立正常行為樣式的異常偵測技術；及建立不正常行為樣式的誤用偵測技術。但是若以單一種偵測技術判定是否有入侵行為時，通常都會發生誤報率或誤判率過高的情形，如何降低錯誤率是偵測技術需要探討的主題。此外，隨著網路使用量越來越高，在系統記錄檔中所記錄的資料也越來越多，如何能正確及有效率的從大量資料中，找出有用的使用者行為樣式也是入侵偵測研究的一個方向。在駭客入侵系統手法不斷翻新的情況下，要能防禦未知型的攻擊手法是入侵偵測系統的一項重點。

針對上述情況，本論文提出一適用於主機式入侵偵測之模糊關聯法則機制，利用系統記錄檔為資料來源，先以模糊群集技術將資料分群，再由此結果導出較精確的關聯法則，並將這些法則建構於異常及正常的法則資料庫中，而日後若有新資料產生，則再以模糊漸進式關聯法則對新資料進行運算，以降低產生法則所需運算的時間，並獲得最新的關聯法則。此機制的設計不但能有效率地從大量資料中，精確地建立出使用者行為樣式，在綜合異常及誤用偵測技術後，能提供入侵偵測引擎更精確地判定是否為駭客入侵行為，進而降低錯誤率，並抵擋未知型的入侵手法。而在論文最後，也將開發一套系統驗證本論文提出之機制的成效。

關鍵詞  入侵偵測系統、資料探勘、模糊理論、群集技術、關聯法則、漸進式資料探勘

目錄
第一章 緒 論 ..............................................1

1.1 研究背景與動機 ......................................1

1.2 研究目的 ..............................................3

1.3 研究範圍及限制 ......................................4

1.4 論文架構 ..............................................5

第二章 文獻探討 ......................................6

2.1 入侵偵測系統 ......................................6

2.2 模糊理論 ..............................................10

2.3 資料探勘 ..............................................13

第三章 適用於入侵偵測之模糊關聯法則機制 ......................25

3.1 研究流程 ..............................................25

3.2 模糊關聯法則機制 ......................................27

3.3 研究方法 ..............................................30

第四章 系統分析與實作 ......................................49

4.1 網頁記錄檔分析 ......................................49

4.2 資料轉換 ..............................................50

4.3 開發工具與環境 ......................................51

4.4 實證結果 ..............................................52

第五章 結論 ..............................................63

5.1 結論 ..............................................63

5.2 研究貢獻 ..............................................63

5.3 後續發展建議 ......................................64

參考文獻 ..............................................65

参考文獻


