

# SNMPv3網路管理之資訊安全防護機制弱點研究

蔡明隆、曹偉駿

E-mail: 9707251@mail.dyu.edu.tw

## 摘要

目前所有網路設備日益普及的環境，網路管理系統讓遠端維護者能藉由遠端登入，監控設備狀態與查修故障告警訊息，各家廠商為了後續的整合，在西元1988年時企業界共同制定了簡單網路管理協定(Simple Network Management Protocol, SNMP)，正是為了整合網路監控與提供網路管理者重要的功能，例如HP的OPENVIEW可以迅速地找到網路故障的根源，自動發現新設備，並協助網路管理人員設計網路擴充的功能，但早期SNMP的訊息是以明文形式發送的，而這些消息很容易被Microsoft網路監視器或者Sniffer這樣的網路分析程式截取並解碼。因此安全的SNMP環境一直被學者們所探討。此外，在SNMP架構之下，已有文獻指出現行的SNMPv3均無法有效地抵禦分散式阻絕服務攻擊(Distributed Denial of Service, DDoS)，與鮮少有支援網頁式管理系統。是故，本論文設計可預防DDoS的SNMPv3並結合公開金鑰基礎建設與網頁式管理功能，進行資安防護機制弱點的研究，以提供日後網路管理之精進建議與參考。

關鍵詞：網路安全;簡單網路管理協定;分散式阻絕服務攻擊;公開金鑰基礎建設

## 目錄

中文摘要	iii	英文摘要	iii
iv 誌謝辭	v	內容目錄	v
vi 表目錄	viii	圖目錄	viii
ix 第一章 緒論	1	第一節 研究背景與動機	1
1 第二節 研究目的	3	第三節 研究流程	3
3 第四節 論文架構	5	第二章 文獻探討	5
6 第一節 SNMP簡單網路管理協定	6	第二節 SNMP各版之比較	6
8 第三節 SNMPv4 架構	10	第四節 USN(User-Based Security Module) 安全模組	14
15 第五節 VACM(View-Based Access Control Module)存取控制模組	15	第六節 SNMPv3 的資安防護機制弱點	18
21 第七節 SNMPv3 可能遭到的攻擊方式	21	第三章 安全的SNMPv3網頁式管理系統	25
25 第一節 WBEM 網頁式管理子系統	25	第二節 USM 安全子系統	28
29 第三節 抵禦 DDoS 子系統	29	第四章 系統建置與實驗	32
32 第一節 開發工具與環境	32	第二節 系統實作	32
34 第三節 實驗結果	37	第四節 成果討論	37
38 第五章 結論與未來發展	40	第一節 結論	40
40 第二節 未來發展	40	參考文獻	41

## 參考文獻

- 一、中文部份 Cole, E. (2005), SNMP的革命進程 [線上資料], 來源: [http://www.isecutech.com.tw/article/article\\_detail.aspx?aid=530](http://www.isecutech.com.tw/article/article_detail.aspx?aid=530) [2008, January 28]. Mauro, D. R., & Schmidt, K. J. (2007), SNMP網管實務(蔣大偉譯), 台北:美商歐萊禮股份有限公司台灣分公司, 497, (原文於2007年出版)。王芬, 趙梗明(2006), 基於SNMPv3網路管理系統的研究和應用, 計算機應用研究期刊, 16(4), 199-202。台灣電腦網路危機處理暨協調中心(2007), 弱點資料庫SNMP VACM [線上資料], 來源, [https://sas3.cert.org.tw/vuldb\\_detail.php?plugin\\_id=10688](https://sas3.cert.org.tw/vuldb_detail.php?plugin_id=10688) [2008, January 30]。何煒, 陳思(2003), SNMPv3網路管理中的安全機制研究, 江西通信科技期刊, (3), 1-5。林育民(2003), 以逢甲大學為基礎之無線網路監視管理系統, 逢甲大學資訊工程學系專題報告, 1-34。林軒立(2003), SNMP網路管理觀念介紹及實作練習 [線上資料], 來源: <http://www.leetide.net/> [2007, September 15]。張毅, 王小非(2006), SNMPv3協議安全機制的研究, 計算機與數字工程期刊, 34(3), 34-37。陳昶, 高小?, 龍翔(2007), 一種基於PKI/數字證書的SNMPv3安全模式, 航空計算技術期刊, 37(1), 117-121。程妍, 王俊, 周永福(2007), 基於VACM MIB的訪問控制策略及其配置, 計算機與數字工程期刊, 35(9), 99-100。路豔麗, 雷英傑(2004), SNMPv3網絡安全管理研究, 現代電子技術期刊, 27(9), 86-88。劉經緯(2007), 基於多代理人架構之洪水式分散阻絕服務攻擊偵防機制, 資訊科技國際研討會。盧寧, 易雅鑫, 何銳, 肖俊(2007), 基於WBEM的系統管理技術研究, 電腦應用技術期刊, (3), 14-18。蕭

富方(2006), 遠端伺服器監控管理系統設計與實作, 世新大學管理學院資訊管理學系未出版之碩士論文, 1-51。二、英文部份

Blumenthal, U., & Wijnen, B. (1998). User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [Online]. Available: <http://dret.net/rfc-index/reference/RFC2574> [2007, June 22].

Blumenthal, U., & Wijnen, B. (1999). User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [Online]. Available: <http://dret.net/rfc-index/reference/RFC2274> [2007, June 22].

Blumenthal, U., & Wijnen, B. (2002). User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [Online]. Available: <http://dret.net/rfc-index/reference/RFC2274> [2007, June 22].

Chen, S., Yong, T., & Wenliang, D. (2007). Stateful DDoS attacks and targeted filtering. *Journal of Network and Computer Applications*, 30(3), 823-840.

Cisco. (2001). Simple Network Management Protocol [Online]. Available: <http://www.cisco.com/> [2007, June 18].

Douligeris, C., & Mitrokotsa, A., (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44(5), 643-666.

Hia, H. E. (2001). Secure SNMP-Based Network Management in Low Bandwidth Networks [Online]. Available: <http://scholar.lib.vt.edu/> [2007, June 20].

Internet Engineering Steering Group. (1999). SNMP Version 3 (SNMPv3) [Online]. Available: <http://www.ibr.cs.tu-bs.de/> [2007, June 19].

Iran Hackers Security Team. (2000). Misoskian's Packet Builder 0.6b Ping of Death [Online]. Available: <http://www.hackerz.ir/forums/ceocn-ac/449-list-hack-tools.html> [2007, June 16].

Kenney, M. (1997). Ping of Death [Online]. Available: <http://www.insecure.org/splouts/ping-o-death.html> [2007, June 21].

Koblitz, N. (1987). Elliptic curve cryptosystems, *Mathematics of Computation*, 48(17), 203-209.

Miller, V. S. (1986). Use of elliptic curves in cryptography, *Advances in Cryptology: Crypto '85* (pp. 417-426), Springer-Verlag.

Networksorcery. (2005). SNMP, Simple Network Management Protocol [Online]. Available: <http://www.networksorcery.com/enp/protocol/snmp.htm> [2007, June 17].

Stallings, W. (1998). SNMPv3: A security enhancement for SNMP. *IEEE Communications Surveys*, Fourth Quarter, 1(1), 1-17.

Toni, P. (1999). The Security of Network Management [Online]. Available: <http://scholar.ilib.cn/Abstract.aspx> [2007, June 15].