A Study on Vulnerabilities of Information Security Protection Mechanism on SNMPv3 Network Management

蔡明隆、曹偉駿

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

ABSTRACT

With increasing popularity of network equipments, managers can log in the network management system remotely, monitor the states of equipments, and process alarm signal. For integration, many manufacturers jointly develop SNMP(Simple Network Management Protocol) to provide important network management functions, such as network monitoring. For example, HP OPENVIEW can find the cause of network failure rapidly, search new equipments, and help network managers design expanded functions for the network. However, previous SNMP messages are sent by the form of plaintext. These messages will be captured and decoded easily by programs such as Micorsoft Internet Monitor or Sniffer. In addition, under the architecture of SNMP, there are some literatures to point that SNMPv3 can not resist DDoS (Dirtributed Denial of Service) attacks, and support web-based management seldomly. So, this article designs a system for preventing SNMPv3 from DDoS attacks, and combines the public key infrastructure and web-based management function, in order to solve the weaknesses of mechanisms of information security. In such a way, it provides useful suggestions for network managers.

Keywords : network security ; network management protocol ; access control module ; security module

Table of Contents

REFERENCES

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 [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網絡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 [2008, January 30]。 何煒，陳思(2003)，SNMPv3網絡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.leet ide.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-inde x/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-inde x/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/fo rums/ceocn-ac/449-list-hack-tools.html [2007, June 16]. Kenney, M. (1997). Ping of Death [Online]. Available: http://www.insecure.org/sploits/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].