行政院國家科學委員會專題研究計畫　成果報告

# 主動網路安全系統服務之功能研究與實作

計畫類別：個別型計畫

計畫編號：NSC93-2213-E-216-031-

執行期間：93年08月01日至94年07月31日

執行單位：中華大學資訊工程學系

計畫主持人：歐陽雯

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 94年10月18日

## 成果報告：

### （一）中、英文摘要及關鍵詞

隨著資訊時代的來臨，電腦與網路的安全問題日益受到重視，但目前的網路無法處理許多的情況。本計畫預計實做出能立即取代傳統網路設備之新一代網路環境，具有高相容性、高擴充性、低成本之優點，能夠有效解決目前網路系統無法解決之阻斷服務攻擊、蠕蟲散播等各種安全性問題。更能夠有效的將自動化程度提至最高以即將管理成本降至最低。就相容性而言，由於本研究採用公開且完整的主動網路環境架構，與其他主動網路研究相較，本研究能夠實做出與傳統網路設備以及其他主動網路環境共存之網路系統，而非無法與其他主動網路系統研究共存、只能在純主動網路環境下才能運作之系統，就擴充性而言，由於各種傳統與主動網路所需要的功能，皆採用彼此獨立的服務來達成，在日後需要新功能或有新規格標準時，只需安裝或替換新的服務，而不必替換硬體設備。本計畫之研究範圍涵蓋了網路安全服務之細部功能與執行方式。計畫重點在於傳統網路服務、安裝服務、偵測服務、過濾服務與傳輸優先權服務等各種服務之細部功能的研究與實作。

The coming of the information age brings out the importance of the computer networks security problems. However, many situations are not well-resolved in the tradition network architectures. This project plans to develop a new network architecture utilizing active network structures to replace the traditional network architecture. This new structure is expected to be highly compatible with the traditional network architecture. It’s also expandable and with low cost since it can coexists with the current traditional networks.

This project covers the research of various services, i.e. traditional network services, installation services, intrusion detection services, filtering services, etc that can be provided in the network security field.

**Keyword:** DoS, worm spreading, active network, response mechanisms, Active Network Security Immune System

### （二）報告內容

#### 前言

Computer networks have brought convenience to many people and change the life styles of human beings greatly. However, the popularity of Internet has seriously intensified the computer security problems at the same time. The denial of service (DoS) attacks have especially received wide attentions due to the reason that it’s hard to predict, prevent, and respond to this type of attacks. All the existing security techniques or solutions such as security authentication, data encryption, antivirus software, firewall, and intrusion detection systems cannot defend the computer systems from DoS attacks and its transformations effectively.

## 研究目的

The purpose of this research is to propose and implement an active network based security system with a new high detection rate technique and new response mechanism. This system is a compatible, scalable and practical network framework. It copes with any type of DoS, including novel worm spreading. Moreover, it has the same characteristics as creature and its immune system. The system not only improves the security of network system substantially, but also reduces the cost of management and maintenance by a wide margin.

## 文獻探討

The DoS, DDoS, and worm DoS have caused a great loss since its first appearance. DoS would make victim or network taken out of commission by sending flurry packets to victim and cause victim to consume their system resources like CPU and memory or network bandwidth. DoS had evolved to Distributed Denial of Service (DDoS) attack. Cracker scans computers over Internet randomly by robot program to see if there are vulnerable computers. The robot program will embed Trojan horse program on these vulnerable computers and make them become intermediary attacker. Those intermediary attackers will start up DoS using above way to attack victim at predefined time or when receiving cracker's command. The DDoS has more destructive power than DoS because the number of DDoS intermediary attackers is much more than one DoS attacker. The newest generation of DoS is worm DoS. Usually, there are only a few worm do DoS itself, but worm spreading that causes server or whole network system paralyzed can be seen as DoS too. Worm spreading sends packets all the time and has amplifying effect. Even the anti-spam email system and firewall cannot detect worm emails or block the all the worm DoS attacks. All existing security defense mechanisms don't work well for these types of attacks.

Passive networks which we use today can only forward packets while active networks are able to do computation and process packets before forwarding them; for example, they can copy the packets, modify the context of packets, then reroute or re-forward the packets. That is, active networks are programmable. Because of this, active networks are capable of solving many problems which passive networks can't such as vulnerability. The main problems of active networks are the throughput and the security. Most security researches based on active network are done through active routers. If there are some passive routers in the network, then the effect will be cut-rate or become inapplicable.

Here are the steps that most network security systems operate nowadays: 1. Computers collect data and logs security event automatically. 2. Computer would make judgments from the collected data and then advises administrators. 3. Administrators re-examine the judgments done by computers and solve the problem thoroughly. It's obvious that almost all important steps are still tackled by administrators for network security systems today. This consumes too much man power and costs too much in terms of management effort.

## 研究方法

In order to establish a full defense mechanism to cope with DoS and its variants, we considered every situation of each type DoS attack. We implemented an active switch and some security services in order to prove the practicality of our system's framework and the detective techniques. The four security services implemented are detection service, filter service, alert service, and mail service. We setup a simulative network environment to experiment the throughput of our active switch and the accuracy of detection service and then compare the results with those from Hogwash system. The experimental results show that our detection services and filters can block all worm packets without any false positives. Our active switch can produce the throughput of active network up to 100Mbs and can coexist with passive network perfectly. Our alert service implements the mechanism of sending warning message to malicious packet sender and the mail service implements the mail sending authentication mechanism. These new mechanisms not only warn user that his computer is infected by worms but also solve the problem of worm spreading through email. The experiments also showed our active switch has superior performance than Hogwash can do

Our system sends the warning message when under attacks not only to the infected computer but also to the network administrators; therefore, users who use the infected computer will know that their computers are sending malicious packets and have been blocked. To inform users is a very important thing. To the cracker, these messages can warn them the security system was found what they did and make them give it up. To the victims, these messages can tell them their system has such problems and can let them to repair their systems.

The procedures of this system, such as blocking attack even when it is novel, attack response, and post processes including restituting, generating signature database, and updating the database are all done automatically just like creature and its immune system do. Therefore, our system is a compatible, scalable, and practical network security framework.

## 結果與討論

In conclusion, the proposed platform has been proved to be with the following advantages:

1. It improves the security of network system substantially since it can cope with any type of DoS, including novel worm spreading. The detection service is with high detection capability and without false positives.
2. It reduces the cost of management and maintenance by a wide margin due to the fact that it has the same characteristics as creatures and their immune systems that automatically generates signature database, and updates the database.
3. It can coexist with passive networks seamlessly so this framework can be combined with any existing network without modifying or upgrading the

existing equipments.

The above proves that our system is a a compatible, scalable, and practical network security framework.

## （三）參考文獻

[1] 賴榮滄, 許明陽, "利用攔截 API 偵測電腦病毒", 逢甲大學

[2] 陳苡萍, "應用 Active Networks 在網路管理及 DoS 監測之研究" 中原大學

[3] 賴守全, 謝木政, “校園網路安全事故自動防治系統之設計與實作”, 國立清華大學

[4] 周文正, “校園區域網路病毒攻擊自動偵測與阻斷系統”, 國立清華大學

[5] D. Scott Alexander, bob Braden, Carl A. Gunter, Alden W. Jackson, Angelos D. Keromytis, Gary J. Minden and David Wetherall. “Active Network Encapsulation Protocol (ANEP)”, RFC Draft. 1997.

[6] S. Bhattacharjee, K.L Calvert, and E.W. Zegura, “Reasoning about Active Network Protocols,” Proc. Int’1 Conf. Network Protocols, 1998, pp.31-41

[7] S. Bhattacharjee, K. Calvert, Y. Chae, S. Merugu, M. Sanders, E. Zegura, "CANEs: an execution environment for composable services" DARPA Active NEtworks Conference and Exposition, 2002. Proceedings , 29-30 May 2002 Page(s): 255 -272

[8] Kenneth L. Calvert, Samrat Bhattacharjee, Ellen Zegura, and James Sterbenz, "Directions in Active Networks", IEEE Communications Magazine October 1998

[9] William La Cholter, Priya Narasimhan, Dan Sterne, Ravindra Balupari, Kelly Djahandari, Arvind Mani, and Sandra Murphy, "IBAN: Intrusion Blocker based on Active Networks", DANCE'02, IEEE

[10] John E. Dickerson and Julie A. Dickerson, “Fuzzy Network Profiling for Intrusion detection”, 2000 IEEE

[11] David Endler, “Intrusion Detection Applying Machine Learning to Solaris Audit Data”, IEEE

[12] J.J. Hartman, P.A Bigot, P. Bridges, B. Montz, R. Piltz, Q. Spatscheck, T.A Proebsting, L.L Peterson, A. Bavier, "Joust: a platform for liquid software", IEEE Computer , Volume: 32 Issue: 4 , April 1999 Page(s): 50 -56

[13] M. Hicks, J.T. Moore, D.S. Alexander, C.A. Gunter, S.M. Nettles, "PLANet: an active internetwork", INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE , Volume: 3 , 21-25 March 1999 Page(s): 1124 -1133 vol.3

[14] Michael Hicks, Pankaj Kakkar, Jonathan T. Moore, Carl A. Gunter, and Scott Nettles, “PLAN: A Packet Language for Active Networks”, 1998 ACM

[15] Michael Hicks, Jonathan T. Moore, David Wetherall, and Scott Nettles,

"Experiences with Capsule-based Active Networking", DANCE'02, IEEE

[16] Jarnes A. Hoagland and Stuart Staniford, “Viewing IDS alerts: Lessons from SnortSnarf”, 2001 IEEE

[17] Nen-Fu Huang and Roger S.W. Chien, "An Extensible Framework for Active Network Intrusion Detection System", National Tsing Hua University

[18] Susan C. Lee and David V. Heinbuch, “ Training a Neural-Network Based Intrusion Detector to Recognize Novel Attacks”, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS-PART A: SYSTEMS AND HUMANS, VOL. 31, NO. 4, JULY 2001

[19] Susan C. Lee and David V. Heinbuch, “Building a true anomaly detector for intrusion detection”, 2000 IEEE

[20] Sixto Ortiz Jr. "Active Networks: The Programmable Pipeline", August 1998, Computer IEEE

[21] Dan Sterne, Kelly Djahandari, Ravindra Balupari, William La Cholter, Bill Babson, Brett Wilson, Priya Narasimhan, and Andrew Prutell, "Active Network Based DDoS Defense", DANCE'02, IEEE

[22] Beverly Schwartz, Alden W. Jackson, W. Timothy Strayer, Wenyi Zhou, r. Dennis Rockwell, and Craig Partridge, “Smart Packets for Active Networks”

[23] Jonathan M. Smith, Kenneth L. Calvert, Sandra L. Murphy, Hilarie K. Orman, and Larry L. Peterson, "Activating Networks: A Progress Report", Computer 1999 IEEE

[24] Sushil da Silva, Yechiam Yemini, and Danilo florissi, “The NetScript Active Network System”

[25] David L. Tennenhouse, Jonathan M. Smith, W. David Sincoskie, David J. Wetherall, and Gary J. Minden, "A Survey of Active Network Research", IEEE Communications Magazine Janury 1997

[26] David J. Wetherall and David L. tennenhouse. “The ACTIVE IP Option”, In proceedings of the 7th ACM SIGOPS European Workshop, Connemara, Ireland, September 1996.

[27] D. Wetherall, J. Guttag, and D.L. Tennenhouse, “ANTS: A toolkit for building an dynamically deploying network protocols”, In IEEE OpenArch '98, San Francisco, CA, April 1998

[28] "Active Network technology: A through overview of its applications and its future", February/March 2001, IEEE POTENTIALS

[29] Douglas r. Mauro & Kevin J. Schmidt, “ Essential SNMP”, O’REILLY

[30] http://www.snort.org/

[31] http://caml.inria.fr/

[32] http://www.inria.fr/

## （四）計畫成果自評

This research has been conducted according to the original plan. It has achieved the goal set that is to study and implement an active network based security system for DoS attacks with a new high detection rate technique and new response mechanism. This system is also a compatible, scalable and practical network framework that can be applied to current network without the need to upgrade any existing network equipment. A paper has been published as a result of this research.

Kunming Yu, Wen Ouyang, Ching-Hsien Hsu, Wen-Ping Lee, “A Honey Pot Security Mechanism Based on Active Networks”, IASTED International Conference on Networks and Communication Systems (NCS 2005), April 2005

## （五）可供推廣之研發成果資料表

N/A

## （六）附錄

N/A