INTEGRATING SECURITY SERVICES INTO ACTIVE NETWORK

SATRIA MANDALA

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

OCTOBER 2005

ACKNOWLEDGEMENTS

Praise to Allah, the most Gracious and Most Merciful, Who has created the mankind with knowledge, wisdom and power. Being the best creation of Allah, one still has to depend on others for many aspects directly and indirectly. This is, however, not an exception that during the course of study the author received so much of help, co-operation and encouragement that need to dully acknowledge.

First of all the author whishes to express profound gratitude to my research supervisor Prof. Dr. Abdul Hanan Abdullah for the noble guidance and valuable advice throughout the period of study. His-ever-dynamic approach, love and dedication for promoting research and development have paved the way to attain a smooth finishing of the present study.

Special dedication to my mother who always has pushed me to achieve to the limits of my ability and have done what she could to ensure that I had the best education possible. For my wife, Ary Nur Azizah and my son, Ahmad Thariq, which they always give their spirit, love, encouragement, and understanding so I can complete this work, thanks honey. This thesis dedicated for them.

Special gratitude is reserved for my best friend, Mr. Dipl.Ing. Amrifan Saladin Mohruni and Dr. Khisbullah Huda, that gives guidance for editing and general writing advice. Then, I would like to thanks to all members of Netsecure group such as Dr.Asri, Cahyo Crysdian, Aishah Nik Mazian, and all of my friends in S46 such as Mr. Hakilo Ahmed Sabit, Rival, Mr. Nourudden Bashir Umar, Mr. Nazori Aghani, Mr. TD. Kusworo, and etc that I cannot mention all of them here.

ABSTRACT

Active network is a new approach to network architecture in which allows node do computation against active packets within the network, for instance, Active Network Transport System (ANTS) from University of UTAH. The ANTS is easily adaptable to new services that are injected into the network. However, the ANTS apply no node policy enforcement to the local node's users and the network packets. As results, the nodes become susceptible from several network attacks such as address spoofing, Distributed Denial of Service – (DDOS), SYN-Flooding, and virus attack. To overcome these problems, a new layer that supports security modules is introduced into the ANTS's node operating system and a minor modification to the operating system is made. The modified ANTS, "Secure JANOS ANTS" (SJANTS), has shown to be more secure than the conventional ANTS while still maintaining the flexibility of the ANTS. The advantages of the SJANTS are as the followings: It can be modified on the fly in the node policy enforcement, it can be conformed to many database vendors, it has independent platform, and it has top-down approach of enforcement to the network packets and the users. In addition, SJANTS security model that based on the Role Base Access Control (RBAC) supports authentication process by using MD5, RIPEMD320, and SHA-512 hash functions, and relies on Java Authentication and Authorization Service (JAAS). Testing was performed to investigate the response time of authentication using these hash functions. The results demonstrated that the authentication based on RIPEMD320 was faster than MD5 and SHA-512., and SHA-512 is more secure than the others.

.

ABSTRAK

“Rangkaian Aktif” adalah satu pendekatan baru terhadap senibina rangkaian di mana ia membenarkan nod di dalam suatu rangkaian saling melakukan pemprosesan terhadap ‘Paket Aktif’. Contoh ‘Rangkaian Aktif’ ialah *Active Network Transport System* (*ANTS*) daripada *University of UTAH*. *ANTS* memberi kemudahan penyesuaian kepada perkhidmatan yang dimasukkan ke dalam rangkaian. Walau bagaimanapun, *ANTS* tidak menyediakan penguatkuasaan polisi keselamatan nod terhadap penceroboh dari pengguna nod setempat dan paket rangkaian. Situasi ini boleh membahayakan keselamatan nod tersebut kerana terdedah kepada ancaman seperti penipuan identiti, *Distributed Denial of Service* (*DDOS*), *SYN-Flooding* dan serangan virus. Sebagai penyelesaiannya, tesis ini telah mengubah-suai sistem pengoperasian nod di dalam *ANTS* dengan memasukkan modul keselamatan di dalamnya dan diberikan nama sebagai Secure JANOS ANTS (SJANTS). Di dalam tesis ini, SJANTS telah menunjukkan ianya lebih selamat daripada *ANTS* disamping mengekalkan kemudahan yang terdapat di dalam *ANTS*. Kelebihan SJANTS ialah ia membenarkan perubahan terhadap penguatkuasaan polisi nod pada bila-bila masa, penyesuaian terhadap vendor pangkalan data, tidak bergantung kepada sebarang platform, dan ia mempunyai pendekatan penguatkuasaan polisi atas-bawah terhadap paket rangakaian dan pengguna. Tambahan pula, model keselamatan SJANTS adalah berasaskan *Role Base Access Control* (*RBAC*) yang menyokong proses pengesahan menggunakan fungsi keselamatan seperti MD5, RIPEMD320, dan SHA-512, dan bersandarkan kepada *Java Authentication and Authorization Service* (*JAAS*). Ujian telah dilakukan untuk mengenal-pasti tempoh respon bagi proses pengesahan untuk ketiga-tiga fungsi keselamatan di atas. Keputusan ujian yang diperolehi menunjukkan bahawa pengesahan menggunakan fungsi keselamatan RIPEMD320 memberikan tempoh respon yang cepat berbanding MD5 dan SHA-512. Sebaliknya, SHA-512 memberikan tahap keselamatan yang tertinggi berbanding fungsi MD5 dan RIPEMD320.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TERMINOLOGY

§ *Active node* refers to a computer which functions as end-system or programmable router or switch.

§ *Algorithm* is a set of instructions, especially ones that can be implemented on a computer, for a procedure that can manipulate data. Cryptographic algorithms are used to encrypt sensitive data files, to encrypt and decrypt messages, and to digitally sign documents

§ *Authentication is* an act of verifying a claimed identity, in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the end-point of a channel (entity authentication).

§ *Authorization* is an act an act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.

§ *Capsule* refers to special packet in traditional network that contains "*program-code*" and may have some embedded data, which is executed within the network. Capsule is similar to *active-packet or smart packet or active application.* The terms capsule, active-packet smart packet and active application are interchangeable, and used in the whole thesis.

§ *Computation* refers to the execution of capsule's forwarding routine at an active node.

§ *Cryptography* defined as 'the science and study of secret writing' concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers, and other methods, so that only certain people can see the real message.

§ *Denial-of-service attack* is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

§ *Domain (Security usage)* is an environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources.

§ *End-to-end security* is continuous protection of data that flows between two points in a network, provided by encrypting data when it leaves its source, leaving it encrypted while it passes through any intermediate computers (such as routers), and decrypting only when the data arrives at the intended destination.

§ *Hop-by-hop security is* security model that requires that each nodes network share a security association. This security model carries information that has to be examined and process by each node on the packet's path, with the source and destination included.

§ *Non-repudiation service is* a security service that provides protection against false denial of involvement in a communication.

§ *Principal* is an entity that has access to resources.

§ *Protocol* refers to primitive program language which defines an agreed-upon format for transmitting data within an active network. This program is composed by capsule or active packet or smart packet for determining some features such as the type of error checking to be used, data compression method, if any; how the sending device will indicate that it has finished sending a message, how the receiving device will indicate that it has received a message.

§ *Repudiation is* a denial by a system entity that was involved in an association (especially an association that transfers information) of having participated in the relationship.

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

The aim of resource-sharing computer network is to usefully interconnect through geographically distributed hardware, software and human resources. Internet successfully becomes a framework that allows resource-sharing and communication between users. Internet-applications oriented have increased rapidly. However, the supporting services on the network have grown very slowly and limited on standardization and manual. To overcome this problem, active network exploits programmable infrastructure to provide rapid and specialized services.

Active network is *a novel approach* to network architecture in which customized programs are executed within the network [1]. Two key benefits of active network are: enable new applications that leverage computation within the network, and accelerate the pace of innovation by decoupling services from underlying infrastructure. The emerging of active network, which is flexible to handle new network services, is expected to solve the remaining problems on today's Internet.

On the active network, nodes are important component which need special protection. Many sensitive information and critical resources for supporting packet processing on nodes can damage if malicious intruder forges them. Potential threats to nodes may come from injected packets into the network, or from the local users of nodes.

Network Security can be expected to secure the nodes from any threats. In fact, cryptography is a major enabling technology for network security, and access control is the heart of the network security. A right implementation of access control for handling active packets and knowing *who* is currently running the application will decrease security risk [50]. For the reason, the user that injects customized program to the network should be identified, and then privileged access should be managed appropriately by the network security. Moreover, un-trusted codes from the network should get special concern too.

This thesis presents a network security concept to secure the active network by providing a pluggable security services. The security services force authentication and management access control (authorization) process to the local users and the network packets.

1.2 Background

Traditional network has several security concerns regarding its resources, i.e.: security of the residing data within host, the data being sent over the network, the applications on host, the Central Processing Unit (CPU), and the bandwidth available on communications links. A hostile party may want to steal these resources or to damage them.

Besides having the same security interest as the internet, the active network also interests on the security of active packets or capsules. In addition, there are two general research categories of the active network security [2]. The first deals with the more traditional notion of security, which includes authentication, access control, policies and enforcement. The second category mostly focuses on protection of nodes against mobile code originating in foreign domains, and protection of capsules or code from malicious hosts.

For active network nodes, security is important. This is due to the fact that the active nodes could be used as a server application and as a router in which the router allows the network to contact with the rest of the world. It is no doubt that the nodes must be safe, reliable and efficient to handle all of their tasks. For the reason, the nodes should have capability to authenticate their users before granting any permission to the node's services or resources. They should also be equipped with ammunitions to protect their self or their assets from any malicious threats. It has been reported by many researches that there are several security threats on active network namely denial of service, address spoofing, and virus (see Chapter 2). In summary, preserving resources are important, and should become main security concern of the nodes because many entities in the real world can attack them directly or by obscure manner.

In general, active network can be divided into two groups, they are discrete active network and integrated active network. Detail description about discrete and integrated active network will be presented on chapter 2. The SwitchWare is an example of the discrete active network. Meanwhile, MIT's ANTS, UTAH's ANTS (this is a successor and mirror of MIT's ANTS, see 2.4), NetScript and PLAN are integrated active networks. In addition, both of Active Network Transport System (ANTS) are tools for developing active network based on capsules. The main characteristics of the ANTSes are flexibility and programmability. Many new services on the network can be developed and deployed easily by using this tool.

The ANTSes are just equipped with simple security. Wetherall [3] describes that the security concept on those ANTSes are like sand-box in Java, where execution of un-trusted codes are separated in a restricted area (referred as Execution Environment - EE) to limit the codes access the shared resources. There are some of weaknesses of the ANTS, i.e.: the nodes do not provide any type of users authentication or traditional security schemes, the nodes lack to identify who is running their services, and the nodes have no capability to authorize arbitrary capsules and users. Additionally, the nodes just protect the capsules integrity by using MD5 fingerprint to ensure that there are no malicious in *byte codes* of the capsules. In conclusion, *the nodes are risky and vulnerable of attacks*. It can be imagined that many security accidents could be emerged by packets without active codes in traditional network, such as trojans and viruses, what did the security disasters strike the nodes if the packets carried active-codes.?

In fact, the ANTS (from this point forward, the “ANTS” without additional information will refer to UTAH’s ANTS) has no safety mechanism to prevent the capsule to be corrupted by other capsule in the node cache. Meanwhile, Van [4] informs that it is difficult to guarantee the uniqueness of a MethodID for individual capsule type, because different user writing different capsule classes can accidentally use the same MethodID. It is clear that additional security mechanisms are necessary to ensure the node safety. Thus, access control management should be introduced to limit the capability of these capsules.

Refer to the weaknesses of the node, development of additional security is necessary, especially to strengthen the node against threats, i.e: from the nodes local users and the capsules. This security mechanism relies on Java 2 security features, such as Java Authentication and Authorization Service (JAAS) and Java Cryptography Architecture (JCA).

1.3 Problem Statements

The open issues described in the previous section lead to some research questions to be solved in this study as follows:

1. How to design secure node architecture.
2. How to design and develop the security extension.
3. How the security extension can be integrated to the node for guarding the node from un-trusted capsule and node local users in the active network.
4. How Java 2 security features encryption technology – JCA, and "authentication and authorization" (JAAS) – can be implemented to the security extension architecture.

From these points, the main research question can be mention as:

"How to develop and introduce security services for guarding the active network node from its local users and capsules"

1.4 Research Objectives

The objectives of this research are:

§ To design secure node architecture, a top-down enforcement policy to active packets and node users.

§ To develop security modules based on the secure node architecture.

§ To modify the Node Operating System (Node OS) abstraction for to support the security modules

§ To integrate the security modules in the modified Node OS. This is known as SJANTS, a prototype of secure active network incorporates authentication and authorization on the active network node. The prototype is based on

UTAH'S ANTS which does not provide security services related these authentication and authorization mechanisms.

- To evaluate the effectiveness of cryptography algorithms applied on the prototype (for supporting authentication process). The variables evaluated are the response time and memory consumption.
- To evaluate the effectiveness of security enforcement applied on the local users and injected simulation capsule.

1.5 Theoretical Framework

In this research, active network security is rooted from field of the active network based on capsule. The high-level architecture of the active network node is shown in Figure 1.1. In this Figure, the architecture has tree layers level; they are active application (AA), Execution Environment (EE) and NodeOS layer. The detail description of this architecture can be found in section 2.2.4.

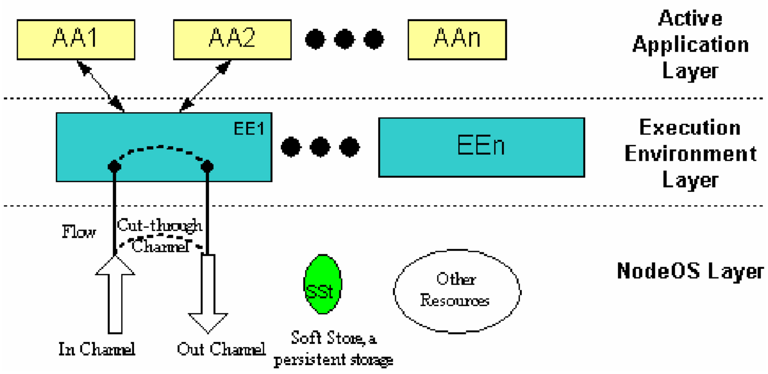

Figure 1.1 Active Network Node Architecture

In the active network, a node operating system (NodeOS) manages the resources such as memory regions, CPU cycles and link bandwidth, and multiplexes packets among multiple execution environments (EEs) running on the node. In order to support the porting EEs to multiple underlying NodeOSes, a NodeOS interface is specified by the NodeOS working group [9].

The objectives of the NodeOS interface are to support fast network packets forwarding and fine-grained quality of service. It defines the following five primary abstractions of system resources:

- Thread Pool
- Memory Pool
- Channel
- File System
- Flow: a flow is a sequence of packets satisfying some predefined attributes of interests.

Section 2.4.2.1 will detail all of these abstractions.

In summary, the current NodeOS research focuses on high performance, extensibility, and resource management. The NodeOS interface doesn't explicitly specify any security API, and there is little research on explicit security support for authentication, authorization, integrity, and dynamic access control on this network.

Fortunately, Java 2 Security evolved an attractive concept to provide fine-grained access control, configurable policy, extension of security checks to all Java programs, including its applications as well as applets. It is believed that the new concept of the Java Security would cover the weakness of sand-box concept in active network - EE. Figure 1.3 describes a new approach security of Java (JAAS).

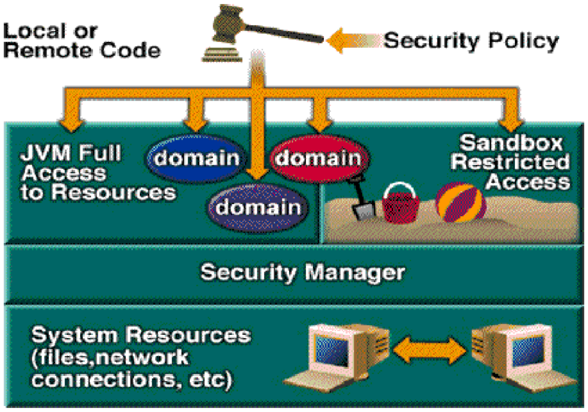
Local or Remote Code
Security Policy
JVM Full Access to Resources
domain
domain
domain
Sandbox Restricted Access
Security Manager
System Resources (files,network connections, etc)

Figure 1.2 Security architecture in Java 2

Refer to Java 1.xx Security concept, *all local code is trusted*; otherwise *anything from network is un-trusted*. Gong [10] stated that this built-in security concept was no longer available in Java 2. In Java 2, the local code is subjected to the same security control as applets. As a result, this enables such code to effectively run as totally trusted. The Java 2 security model also has introduced the concept of a `ProtectionDomain` which permitted a highly flexible security policy to be decoupled from its implementation.

Although cryptography and security are two distinct subjects, the security relies on the cryptography in many ways. In Java, the native cryptography library is both of Java Cryptography Architecture (JCA) and Java Cryptography Extension (JCE). This research has applied the cryptography to encrypt the user password and to maintain the integrity of injected code in the network.

1.6 Scopes

Some limitations are applied to research activity in order to keep the observation on its place. They can be mentioned as follows:

- The prototype runs on Java 1.3.X and focuses in small active network.
- Active packets from this network (SJANTS – our prototype) will be granted as un-trusted entity, i.e. *RemoteUsers*. Thus, all of the packets get same enforcement with limited access to NodeOS resources and services.
- Security only focuses on the node of the active network; no address protection of capsules from malicious host or node.
- The security test has not been performed on the ANTS because the ANTS applies no security.

1.7 Contributions

Contribution of this research can be viewed from few different perspectives as follows:

- From the active network perspective, there is a challenge to explore active network technology; a new concept to improve the active network has been addressed by providing security services on its node. This includes how the node handles it's the local users and the un-trusted capsule. This is due to avoiding of attack which may disturb its operation.
- From access control point of view, a user management access control "role based access control" has been introduced to give administrators a capability for granting or revoking permission to its own user.
- From active network technology, our prototype "The SJANTS" fixed also the problems as deprecated classes and upgraded codes UTAH'S ANTS for running in JDK 1.3.X.

1.8 Thesis Organization

This section presents how this thesis is organized. This thesis has five chapters, i.e.: Introduction, Literatures Review, Research Methodology, Result and Discussion, and Conclusion and Future Works.

Chapter I: Introduction, this chapter introduces topic consisting eleventh sections: Overview, Background, Statements of the Problems, Research Objective, Theoretical Framework, Scope, Research Contribution, and Thesis Organization.

Chapter II: Literature Review, this chapter presents current studies in the area of active network, followed by discussion of security requirements in active network, java security and cryptography related this research.

Chapter III: Research Methodology, this chapter describes the methodology of the research which is conducted on: how the research is setup, which data is analyzed and observed and what experiment will be held.

Chapter IV: Result and Discussion: this chapter details the result achievement of the research. An inclusive discussion for analyzing the result of testing is also addressed in the chapter.

Chapter V: Conclusion and Future Works: this chapter describes conclusion and Future Works of the research.

REFERENCES

1. Wetherall, D.J. ANTS: A Toolkit for Building and Dynamically Deploying Network Protocols. *Proceedings IEEE OpenArch98*. 1998.
2. Liu, Z., Campbell, R.H., Mickunas, M. D. *Securing the Node of An Active Network.* Active Middleware Services. Kluwer Academic Publishers, Boston, MA. September 2000.
3. Wetherall, D.J. *Service Introduction in an Active Network.* PhD. Thesis. Massachusetts Institute of Technology. February 1999.
4. Van, V.C. *A Defense Against Spoofing Using Active Networks.* Master Thesis. Massachusetts Institute Of Technology. May 1997.
5. Campbell, R.H, et al. Seraphim: Dynamic Interoperable Security Architecture for Active Networks. *Third IEEE International Conference on Open Architectures and Network Programming (OPENARCH 2000)*. Tel-Aviv, Israel. March 2000.
6. Liu, Z., Campbell, R.H., Varadarajan, K., Naldurg, P., Yi, S., Mickunas, M.D. Flexible Secure Multicasting in Active Networks. *The International Workshop on Group Computation and Communications (in conjunction with ICDCS 2000)*. Taipei, Taiwan. April 2000.
7. Liu, Z., Campbell, R.H., Varadarajan, K., Naldurg, P., Yi, S., Mickunas, M.D. Pluggable Active Security for active Networks. *In the Twelfth IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS 2000)*. Las Vegas, Nevada. November 2000.
8. Murphy, S., Lewis, E., Puga, R., Watson, R., and Yee, R. Strong Security for Active Networks. *IEEE OPENARCH*. 2001.

9. Peterson, L., Gottlieb,Y., Hibler, M., Tullmann, P., Lepreau, J., Schwab, S., Dandekar, H., Purtell, A., and Hartman, J. *An OS Interface for Active Routers*. IEEE Journal on Selected Areas in Communications. 2001.

10. Gong, L. *Java™SecurityArchitecture (JDK1.2) - Version 1.0*. Sun Microsystems. Inc. 901 San Antonio Road, Palo Alto, California 94303 U.S.A. October 2. 1998.

11. Psounis, K. Active Networks: Applications, Security, Safety and Architectures. *IEEE Communications Surveys*. Vol.2 No.1. First Quarter 1999

12. Tennenhouse, D.L.; Wetherall, D.J. Towards an active network architecture. *DARPA Active NEtworks Conference and Exposition*. 2002. Proceedings 29-30 May 2002 Page(s):2 - 15

13. Huang, I.H. *Active Networks: An Overview*. Unpublished research report. Department of Computer Science and Engineering, Yuan Ze University. 2000

14. Nygren, E.L., J.Garland, S.J, Kaashoek, M.S. PAN: A High-Performance Active Network Node Supporting Mobile Code Systems. *Proceeding IEE OPENARCH'99*. March 1999.

15. Fernando, A., Kummerfeld, B., Fekete, A., Hitchens, M. A new dynamic architecture for an active network. *Openarch 2000 - IEEE Thirds conference on Open Architectures and Network Programming*. 2000. Proceedings Volume 1, pp.121-127.

16. Fernando, A., Kummerfeld, B., Fekete, A. *Pants: Active Node Transfer System*. Technical Report. University of Sydney, Australia. 1998

17. Galis, A., Plattner, B., Smith,J.M, Denazis S., Moeller, E.,Guo, H.,Klein, C.,Serrat, J., Laarhuis, J., Karetsos, G.T and Todd, C. A Flexible IP Active Networks Architecture. *Active Networks, Second International Working Conference*. IWAN 2000. Tokyo, Japan. October 16-18, 2000. Pages (1-15), Pub. Springer

18. Alexander, D.S, Arbaugh, W.A., Hicks, M.W., Kakkar, P., Keromytis, A.D, Moore, J.T., Gunter, C.A., Nettles, S.C., Smith, J.M. *The Switchware Active Network Architecture*. IEEE network, Vol. 12(3). 1998

19. Mosberger, D., Peterson, D., Making paths explicit in the Scout operating system. *Proceedings of the Second Symposium on Operating Systems Design and Implementation*. October 1996.

20. Merugu, S., Bhattacharjee, S., Zegura, E., Calvert, K. *Bowman: A Node OS for Active Networks.* IEEE Infocom 2000.

21. Tullmann, P., Hibler, M., Leprau, J., Janos: A Java-oriented OS for Active Network Nodes. *DARPA Active Networks Conference and Exposition*. 2002

22. Alexander, D.S., Arbaugh, W.A., Keromytis, A.D., and Smith, J.M. *A Secure Active Network Environment Architecture, Realization. in SwitchWare*. IEEE Network Special Issue on Active Networks. May/June 1998

23. Bagnulo, M., Alarcos, B., Calderón, M., Sedano, M. ROSA:Realistic Open Security Architecture for Active Networks. *IWAN 2002.* LNCS 2546, pp. 204-215. Zurich, Switzerland. December. 4-6 2002. ISBN: 3-540-00223-5.

24. Galtier, V., Mills, K., and Carlinet, Y. Modeling CPU Demand in Heterogeneous Active Networks. *Proceedings of the DARPA Active Networks Conference and Exposition, IEEE.* May 2002

25. Tennenhouse, D.L., Smith, J.M., Sincoskie, W.D., Wetherall, D.J., Minden, G.J. *A Survey of Active Network Research.* IEEE Communications Magazine. Vol. 35, No. 1. Jan 1997. pp80-86.

26. Kulkarni, A.B., Minden, G.J. Active Networking Services for Wired/Wireless Networks. *Proceeding of INFOCOM'99*. Mar 1999.

27. Bin, X., Depei, Q., Yueming, L., Lei, W. An Active Network-Based Network Management Framework. *ICCT - World Computer Congress*. Beijing, China. 2000

28. Di Fatta, G., Gaglio, S., Lo Re, G., Ortolani, M. Adaptive Routing in Active Networks. *Proceedings of OpenArch 2000*. *IEEE Third Conference on Open Architecture and Network Programming*. Tel Aviv. March 2000.

29. Witherall, D.J., *Safety Mechanisms for Mobile Code.* Unpublished research report:Area Exam Paper. MIT Laboratory for Computer Science. November 1995.

30. Tullmann, P., Hibler, M., Leprau, J. *Janos Java NodeOS Programming Manual.* Unpublished research report. Flux Research Group, Department of Computer Science. University of Utah. March 2002.

31. Hicks, M., Kakkar, P., Moore, J.T., Gunter, C.A. and Nettles, S. PLAN, A Packet Language for Active Networks *Proceedings of the Third ACM SIGPLAN International Conference on Functional Programming Languages*. September 1998. pp. 86–93, ACM.

32. Merugu, S., Bhattacharjee, S., Chae, Y., Sanders, M., Zegura, E., Calvert, K., Bowman and CANEs: Implementation of an Active Network. *Proceedings of 37th Annual Allerton Conference*. Monticello, IL. September 1999.

33. Calvert, K.L. *Architectural Framework for Active Network*, a DRAFT - Active Network Working Group - University of Kentucky. July 1999

34. Liu, Z., Naldurg, P., Yi, S., Qian, T., Campbell, R.H., Mickunas, M.D. An Agent-based Architecture for Supporting Application Level Security. *The DARPA Information Survivability Conference and Exposition.* Hilton Head Island, SC. January 2000.

35. Campbell, R.H., Liu, Z., Mickunas,M.D., Naldurg, P., Yi,S. An Agent-based Architecture for Supporting Application Aware Security. *The Workshop on Research Directions for the Next Generation Internet.* Vienna, VA. May 1997.

36. The ISI ARP Project. *Active Network Security for the ABone*. Unpublished research report. University of Southern California/Information Sciences Institute (ISI). 18 November 2001

37. La Cholter, W., Narasimhan, P., Sterne, D., Balupari, R., Djahandari, K., Mani, A., Murphy, S. IBAN: Intrusion Blocker based on Active Networks. *DARPA Active Networks Conference and Exposition*. 2002

38. Sterne, D., Djahandari, K., Balupari, R., La Cholter, W., Babson, B., Wilson, B., Narasimhan, P., Purtell. A. Active Network Based DDoS Defense. *DARPA Active Networks Conference and Exposition*. 2002

39. Flux Research Group. *JanosVM User's Manual and Tutorial Version 1.0.* Unpublished research report. School of Computing University of Utah. February 13, 2003

40. Hicks, M., Moore, J.T., Alexander, D.S., Gunter, C.A., and Nettles, S.M. PLANet: A Packet Language for Active internet work. *Proceedings of Eighteenth IEEE Computer and Communication Society INFOCOM Conference*. March 1999. pp. 1124-1133, IEEE.

41. Joshi, J. B.D. *A Generalized Temporal Role Based Access Control Model For Developing Secure Systems*. A PhD Thesis. Purdue University. August 2003

42. Lampson, B.W., Protection, *Princeton Symposium on Information Sciences and Systems*. March 1971. Reprinted in ACM Operating System review, 8(1). 1974

43. Graham, G. and Denning, P., Protection - principles and practice *Proceedings of Spring Joint Computer Conferences*. AFIPS Press. 1972

44. Denning, D. *Cryptography and Data Security*. Addison-Wesley Publishing Company. 1982

45. Sandhu, R.S. and Coyne, E.J. Role-based access control models. *IEEE Computer*. 29(2). February 1996.

46. Ferraiolo, D.F., Sandhu, R.S., Kuhn, D.R., and Chandramolu, R. Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security.* 4(8). August 2001. Pages 224-274

47. Gasser M. *Building a Secure Computer System*. New York, NY, USA: Van Nostrand Reinhold Co. ISBN:0-442-23022-2. 1988

48. Shirey, R. *Internet Security Glossary*. Technical Report RFC 2848, GTE/BBN Technologies. May 2000

49. Mandala, S., Abdullah, A.H., Ngadi, A. Securing Communication on Active Network based RSA. *The 7th International Conference Quality in Research*. 4-5 Agustus 2004. EE-CM-11-3

50. Lai, C., Gong, Li., Koved, L., Nadalin, A., Schemers, R. et al., User Authentication and Authorization in Java Platform *Proceedings of the 15th Annual Computer Security Applications Conference*. Phoenix, AZ. December 1999

51. Housley, R., Ford, W., Polk, W., Solo, D. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile.* Request for Comments 2459 - Internet Engineering Task Force. January 1999.

52. Ryutov, T. and Neuman, B.C., *Access Control Framework for Distributed Applications.* Internet Draft, Internet Engineering Task Force. November 1998.

53. Lampson, B., Abadi, M., Burrows, M., and Wobber, E. Authentication in Distributed Systems: Theory and Practice, *ACM Transactions on Computer Systems.* 10(4):265-310. November 1992

54. Neuman, B.C. and Ts'o T., Kerberos: An Authentication Service for Computer Networks, *IEEE Communications*, 32(9):33-38. September 1994.

55. Dierks, T and Allen, C. *The TLS Protocol* — Version 1.0. IETF RFC 2246. January 1999

56. Lenstra, A. K., Verheul, E.R. *Selecting Cryptographic Key Sizes*. The Journal of Cryptology. Springer-Verlag 14(4): 255-293 – 2001.

57. Metzger, P., Karn, P., and Simpson, W. *The ESP-DES-CBC Transform*. RFC-1829. August 1995.

58. Shin, D. *Role-Based Access Control For Trust Management : Model, Process, and Management*. A PhD Dissertation. The University of North Carolina at Charlotte. 2004

59. AN Node OS Working Group. *NodeOS Interface Specification*. Unpublished research report. January 2001

60. Dobbertin, H., Bosselaers A., and Preneel, B. *RIPEMD-160: A Strengthened Version of RIPEMD*. Fast Software Encryption, LNCS 1039. D. Gollmann, Ed. Springer-Verlag. pp. 71-82. 1996

61. Keromytis, A. *The Use of HMAC-RIPEMD-160-96 within ESP and AH*. Request for Comments: 2857, Network Working Group. June 2000

62. Preneel, B., Bosselaers, A., Dobbertin, H. *The cryptographic hash function RIPEMD-160*. CryptoBytes. Vol. 3, No. 2, pp. 9-14. 1997.

63. Brown, C., Cobb, G., Culberston, R. *Rapid Software Testing*. Prentice Hall PTR. Apr 12. 2002.

64. Panzl, D.J. Authomatic Revision of Formal Test procedures. *International Conference on software Engineering*. 1978.

65. Adrion, W.R., Branstad, M.A., Cherniavsky, J.C. Validation, Verification, and Testing of Computer Software. *ACM Computing Surveys (CSUR*), p 159-192. June 1982

66. Montgomery D.C., Runger, G.C., Hubele, N.F. *Engineering Statistics*. Second Edition. John Wiley & Sons, Inc. 2001.

67. Grafen, A. and Hails, R. *Modern Statistics for the Life Sciences*. Oxford University Press. Great Clarendon Street, Oxford OX2 6DP, New York. 2002

68. Active Networks. http://www.darpa.mil/ato/programs/activenetworks/smartpackets.htm. accessed on May 19, 2005

PUBLICATIONS

1. Mandala, S., Abdullah, A.H, Active Web Caching Management, *Seminar Nasional Informatika 2004*, SNI 2004. Yogyakarta. February 2004

2. Mandala, S., Abdullah, A.H., Ngadi, A. Securing Communication on Active Network based RSA. *The 7th International Conference Quality in Research*. 4-5 Agustus 2004. EE-CM-11-3

3. Mandala, S., Abdullah, A.H. Securing Communication on Active Network. *Konferensi Nasional Sistem informasi 2005*. Bandung. 15 January 2005.

4. Mandala, S., Abdullah, A.H., Ngadi, A. SJANTS (Secure Janos – ANTS), a Prototype to Secure Active Network. *International Conference on Instrumentation, Communication and Information Technology (ICICI) 2005* Proc., Bandung, Indonesia, August 3rd -5th , 2005

5. Abdullah, A.H., Mandala, S., Ngadi, A. A Defense Active Node against Un-trusted Packet on Active Network, *The 8th International Conference On Quality in Research (QIR)*. Jakarta – Indonesia. 9-10 August 2005