A Study on the Intrustion Tolerance System Applied To the Security System

Seung-jung Shin, Jung-tae Kim, Dae-hyun Ryu and **Jong-Whoa Na,** *Member, KIMICS*

Abstract—The cyber attacks on the computer system in nowadays are focused on works that do not operate specific application. The main key point that we protect information security system has an access control to keep an application. Most of system has a main function to protect an infrastructure such as hardware, network and operating system. In this paper, we have presented an intrusion tolerance system that can service an application in spite of cyber attacks. The proposed system is based on the middle ware integrating security mechanism and separate function of application and intrusion tolerance. The main factor we use security system in nowadays is service to keep a persistency. The proposed intrusion tolerance system is applicable to such as medical, national defense and banking system.

Index Terms—Intrusion Tolerance, Oriented Security, Security

1. INTRODUCTION

The security system has both a vulnerability in availability in service and obstacle of service by traffic of -network.[1] Our society depends on the sensor network system and is faced with vulnerability such as medical system, banking system and national defense. The stop of service by vulnerability makes a disorder. We have to solve the critical problem.[2] The application using security mechanism has a vulnerability in cyber attack. In contrary to this application, application with adaptive mechanism can survive a system for a short time. Therefore the application with intrusion tolerance function realizes using security mechanism and adaptive mechanism.

In this paper, we have implemented intrusion tolerance system by separating application function using a variety of security mechanism and adaptive mechanism in middle ware. The proposed paper is as follows. We proposed intrusion tolerance security model by analyzing security mode and distributed object model of COBA in the second chapter. The third chapter described the theory of intrusion tolerance mechanism and strategy of implementation and extract the intrusion tolerance technology and implementation method. We have designed system analyses by adapting intrusion tolerance security model and element technology. We have confirmed the realization of application of intrusion tolerance using oriented security type with developed intrusion tolerance module.

Manuscript received March 30, 2005.

Seung-jung Shin is with Hansei University, IT Engineering (phone: 031-450-5274; fax: 031-450-5172; e-mail: expersin@ hansei.ac.kr).

Dae-hyun Ryu is with Hansei University IT Engineering (phone: 031-450-0132; fax: 031-450-5172; e-mail: dhryu@hansei. ac.kr).

Jong-Whoa Na is with Hansei University IT Engineering (phone: 031-450-5158; fax: 031-450-5172; e-mail : jwna@hansei.ac.kr)

2. SECURITY MODEL

2.1. Information Model

The software with information system is composed of object that is connected with distributed in network. And object of client calls operation of object operating in remote to realized the function of application. [7] Information model of COBA is described in figure 1. The client object calls method of remote object such as local object.

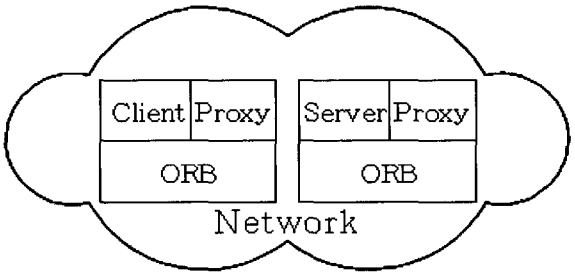

Fig. 1 Information Network Model

Object of proxy transfers remote method call to local ORB after marsharing. ORB transfers message call using IIOP message to remote ORB with servant object. Remote ORB transfers method call to skeleton operating unmarsharing and skeleton transfers message call to implemented object. The final results of operating method transfer the values by reverse. The distributed object model hides the complexity such as variety, compatibility and heterogeneousness and shows the functional interface of component.

2.2. Distributed Object Security Model

COBA distributed object system guarantees confidentiality of object, integrity and availability by using security mechanism based on policy in oriented security. Security policy totally establishes group mechanism by using domain, privilege and usage authority. Security administrator involves object in domain and equally establishes

security policy about group of objects. And security administrator executes usages the security policy on usage group by grouping with same privilege attributes. The method of object groups the methods by contributing same usage privilege and applies security policy on group. The distributed object security model is depicted in figure2

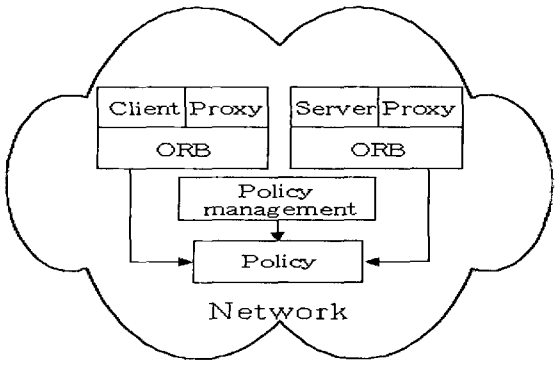

Fig. 2 Information Network oriented security model

2.2. Intrusion tolerance security model

Application such military, medical and banking system needs the requirements for security, reliability and real time performance. The distributed oriented security does not support the requirements because it hides the detailed contents to control the service quality and does not support the system development function that can be applicable to change of service quality. Therefore the deleveloper of application for serving important service must program the function of intrusion tolerance based on oriented security. In this paper, we have proposed extended type of distributed object model such as figure 3 using intrusion tolerance security model.

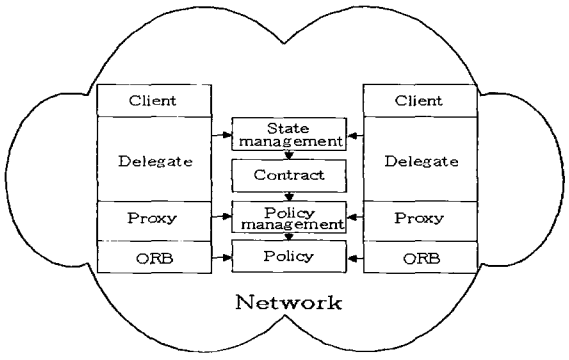

Fig. 3 intrusion tolerance security model

The intrusion tolerance model adds the function of bridge between application and the necessary detailed matters to control and describe and measure the service quality service request and service category maintains in data structure called contract. Delegate investigates the state of system and carry out the proper adaptive object by comparing service level in contract. The object of state management conducts the function of measuring the state of mechanism. The proposed system is aim to supply the framework and control service quality. Therefore mechanism does not integrate the duplication management system, bandwidth management system and intrusion detection system for control the service quality such as reliability, bandwidth and security. We need to consider the necessary mechanism to integrate proposed system by request of service quality.

3. INTRUSION TOLERNACE

3.1. Intrusion tolerance

The intrusion tolerance mechanism is new technology for information security to prepare for unauthorized intrusion or attack based on applicability, duplicability, observation and a variety of principle. The intrusion tolerance technology supports a variety of mechanism to prepare the strategy against attack with high technology employing intrusion resistance system and intrusion detection system.

The application with supporting intrusion tolerance function must adapt the change of state of system generated intentionally such as intrusion or virus attack.

This mechanism can use independently but it can be enhanced its performance of intrusion tolerance function by using complementary cooperation.

3.2. Gateway protocol and Intrusion model

The configuration of gateway protocol is shown in figure 4. Gateway component intercepts IIOP message and transmits to authentication server and realizes proper authentication based on authentication data with returned data when client calls the method of sever implemented object.

3.3. Intrusion Tolerance by Protection

The access control is final barrier to protect distributed information system based on network. Generally, the oriented security is implemented using access control with policy oriented defined in COBA. The intrusion tolerance security mechanism is realized the security on service quality with confidential object containing ID and privilege content as shown in figure 5.

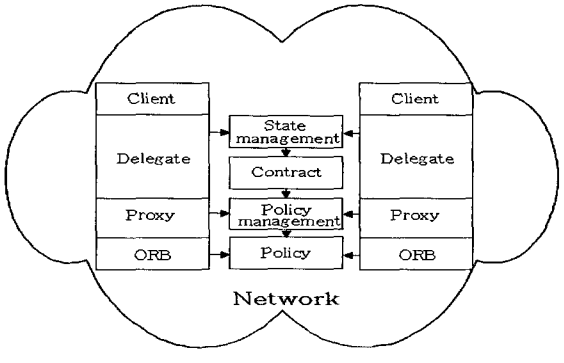

Fig. 4 Intrusion tolerance gateway

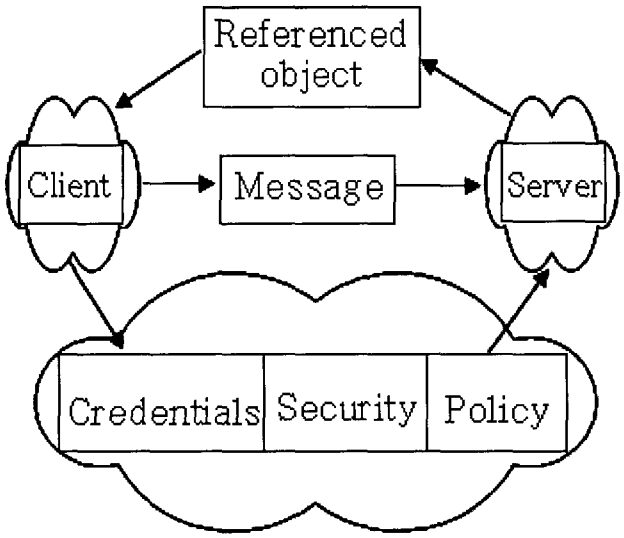

Fig. 5 Intrusion tolerance security mechanism

3.4. Intrusion Tolerance by adaptation

The application has to adapt the system instead of fault of system in the state of degradation of service quality. We have to separate the function of application by implementing oriented security with intrusion tolerance function that can be applicable to system. It should be define the quality of service of application, observe and control the service of application. To develop the distributed information system, we can carry out their work by dividing their role, developer of application for implementing client and implementing object, developer of oriented security like ORB and developer of service quality. We can consider some kind of adaptation strategy to maintain service in spite of cyber attack.

First, we do not anything. Second, we construct system that the cyber attack is impossible. Third, we develop application that cyber attack is expected and can be coped with some mechanism. Fourth, we develop the application using mechanism with applicable to cyber attack. First strategy can cause system fault in case of occurrence of cyber attack. Second and third strategy is not reasonable because the possibility of cyber attack is not expected. Fourth strategy is most reasonable. As shown figure 6, the implemented intrusion tolerance system is realized using adaptive mechanism using duplication management system.

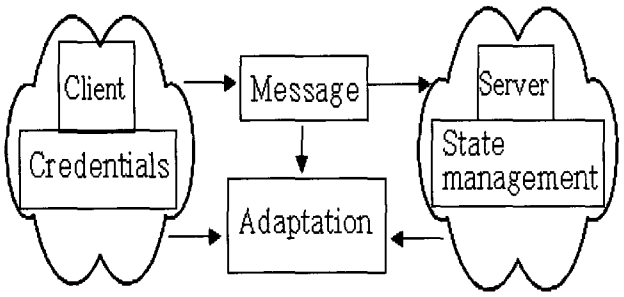

Fig. 6 Intrusion tolerance adaptive mechanism

4. MODELING OF MANAGEMENT INTRUSION SYSTEM

The function of system employing important function is represented with service workflow. We also extract the function of intrusion tolerance by description of intrusion workflow with function of applicable to external circumstance. We have to implement intrusion tolerance system based on external intrusion description and analyses. Also, we define and design an essential service for durable support despites of external cyber attack. The process is divided necessary service, analyses of intrusion detection, design and implementation step. The workflows have a necessary service implementation flow with a series of system architecture components. The work flow represented essential service composes work, information and decision.[9], [11] Execution flow shows the workflow as architecture component and data as information. Figure 8 describes defense, detection and recovery mechanism in intrusion scenario.

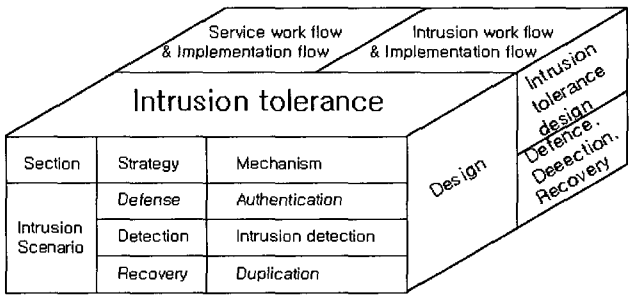

Fig. 7 Modeling of intrusion tolerance strategy

5. IMPLEMENTATION OF INTRUSION TOLERANCE SYSTEM

5.1. Applied intrusion tolerance system

The main purpose of implementing for intrusion tolerance system is presented the practical methods for adaptive mechanism and integration method for a variety of security mechanism in oriented security layer. To realize this mechanism, the stock management system with intrusion tolerance function is implemented. The functions of client have log in process, function of request process and log out function. Server is implemented to provide stock goods DB and stock management service.

Commercial application and operating system is generally used in case of construction for distribution system employing consistency of service. Because the use of commercial products is less cost and effort than develop of application server. But commercial application server has a lot of vulnerability for security. To solve this kind of vulnerability, we use interface as software layer with security function between application server and client. The security interface is realized by intercept a message between client and server in interface layer. Therefore client receive a service of server using lapper

and can change and inspect all messages with transmitting and receiving. The commercial product can have a security attribute by constructing lapper with security function.

Figure 8 shows the changeable configuration with intrusion tolerance function The security mechanism uses intrusion detection system and access control. The object of state management with intrusion detection system and interface role of access control system is implemented using LAPPER object. The function defined agreement object with time delay, access violation and intrusion detection mode to estimate service quality level. Application mechanism uses server with authentication and server without authentication server in repetition. Object of agent is designed to transfer requested message to both in the normal mode of service quality level and without authentication function server. In the case of access violation and detection mode, the object is designed to transfer requested message which carrying out authentication function.

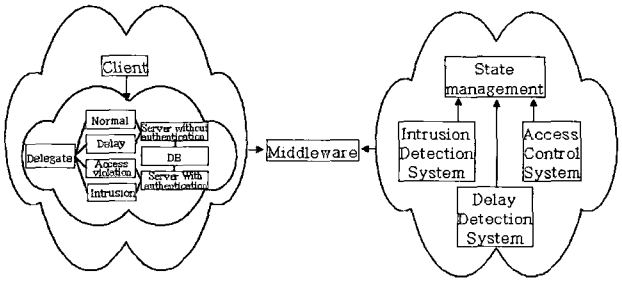

Fig. 8 Intrusion tolerance system

5.3. Comparison of implementation between application layer and middle ware layer

The problem of implementation in application layer with intrusion tolerance function does not divide business logic and intrusion tolerance function. It is not easy to change the program, extend function and is difficult to keep maintenance. Figure 9. shows the configuration of implementing intrusion tolerance in application layer.

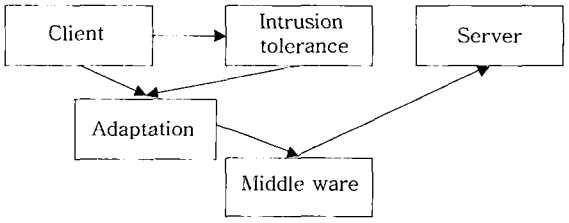

Fig. 9 Intrusion tolerance implementation in application layer

Figure 10 shows configuration for implementing intrusion tolerance function in oriented security. The advantage of this system can implement intrusion tolerance function by dividing business logic. We can establish the application with superior security level by operating their work in separately with developer of application and developer of intrusion tolerance implementation. Also we support the toolkit for developer of intrusion tolerance implementation and enhance the productivity of software. We can use the intrusion tolerance function in oriented security type and can implement easily intrusion tolerance function by plug in. They provide many advantages to integrate the system with different intrusion tolerance system by standardizing intrusion tolerance function.

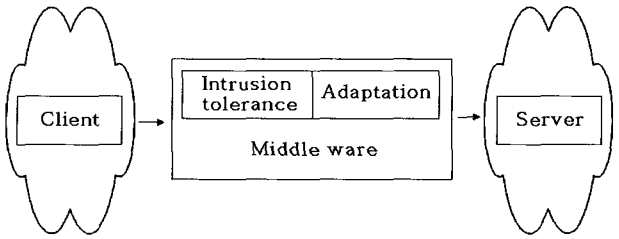

Fig. 10 Intrusion tolerance implementation in oriented security layer

6. CONCLUSION

Security mechanism such access control and cryptography can strengthen intrusion tolerance function by protecting accidental or intentional attack. Adaptive mechanism using bandwidth management or redundancy management can support intrusion tolerance function by adapting a change of system state.

The intrusion accidents reported recently have an attack for application of system with not providing normal service.

Previous information security approaches are aim to resist infrastructure such as hardware, operating system and network to protect attack of application. In this paper, we have presented an intrusion tolerance system that can service application in spite of cyber attacks. The proposed system is based on the oriented security by integrating security mechanism and separate function of application and intrusion tolerance. The proposed intrusion tolerance system in this paper can enhance the reliability and safety to survive a system in violation accident.

REFERENCES

[1] Scambray, J., S. McClure, G. Kurtz, Hacking Exposed: Network Security

[2] Secrets & Solutions (Second Edition), McGraw-Hill, 2001 Schneider, B. Secrets and Lies: Digital Security in a Networked World. New York NY: John Wiley & Sons, August 2000.

[3] Hartman, J. and Evans, W., Fault tolerant application enhanced network-Project A project under the DARPA Fault Tolerant Networks Program. Homepage Internet URL http://www.cs.arizona. edu/ftn, 2000.

[4] Loyall, J. P., Pal, P. P., Schantz, R. E., and Webber. F., Building adaptive and agile applications using

intrusion detection and response. In Proceedings of the ISOC Network and Distributed Systems Security Conference, Februrary 2000.

[5] Cardei, M., Cardei, I., Jha, R., and Pavan. A., Hierarchical feedback adaptation for real time sensor-based distributed applications. In Proceedings of Middleware 2000 (LNCS 1795), pages 415-435. Springer-Verlag, 2000.

[6] Loyall, J. P., Pal, P. P., Schantz, R. E. and Webber. F., Building adaptive and agile applications using intrusion detection and response. Im Proceedings of the ISOC Network and distributed Systems Security Conference, Februrary 2000.

[7] Li, B. and Lahrstedt. K., Qualprobes:middleware qos profiling services for configuring adaptive applications. In Proceedings of Middleware 2000 (LNCS 1795), Pages 256-272. Springer-Verlag, 2000.

[8] Pal, P., Loyall, J., Zinky, J., Shapiro, R. and Megquier, J., Using qdl to specify qos aware distributed(quo) application configuration. In Proceedings of The 3rd IEEE International Symposium on Object-oriented Real-time distributed Computing (ISORC 00), March 2000.

[9] Hevner, A. Linger, R., Sobel, A., and Walton, G. Specifying Large-Scale, Adaptive Systems with Flow-Service-Quality(FSQ) Objects, Proceedings of 10th OOPSLA Workshop on Behavioral Semantics, Tampa, October 2001.

[10] Linger, R., Pleszkoch, M., Walton, G., and Hevner, A Flow-Service-Quality Engineering: Foundations for Network System Analysis and Developement, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2002-TN-019, July, 2002.

[11] Hayes, J., et al. "Workflow Interoperability Standards for the Internet." IEEE Internet Computing 4, 37-45. 3(May/June 2000).

[12] Badger, L., Generic software wrappers. Internet URL http://www.pgp.com/research/nailabs/secure-execution/wrappers-overview.asp. 2000

Seung-Jung Shin

Prof. Seung-Jung Shin received his B.S. degree in Management from Hansung University in 1984 and M.S. degrees in Marketing from the Sejung University in 1988 and M.S. degrees in Electronic Engineering from the Kunkuk University in 1994 and Ph.D. degrees in Management Information Security from the Kukmin University in 1999 , respectively. From 1990 to 1994, he joined at Teasung MIS, where he worked as Technical Director. From 1995 to 2003, he joined the department of Electronic and Information security Management, Joongbu University, Korea, In 2003, he joined the department of Information Technology, Hansei University, Korea, where he is presently a professor. His research interest is in the area of Network communication technology that includes Information Message security system design, Mobile system and Wireless Communication.

Jung-Tae Kim

Prof. Jung-Tae Kim received his B.S. degree in Electronic Engineering from Yeungnam University in 1989 and M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 1991 and 1996, respectively. From 1991 to 1996, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 2002, he joined the department of Electronic and Information security Engineering, Mokwon University, Korea, where he is presently a professor. His research interest is in the area of Information security technology that includes Information security system design, Network security and crypto-processor design.

Dae-Hyun Ryu

Prof. Dae-Hyun Ryu received his B.S. degree, M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Busan National University in 1983, 1985 and 1997, respectively. From 1987 to 1998, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 1998, he joined the department of IT, Hansei University, Korea. His research interest is in the area of Digital image processing, Digital watermark and Information security system design.

Jong-Whoa Na

Prof. Jong-Whoa Na received his B.S. degree in Electronic Engineering from Sogang University in 1985, M.S. degree in Computer Engineering from the Wayne State University, Detroit, MI., U.S.A. in 1988, and Ph.D. degree in Computer Engineering from the University of Arizona, AZ., U.S.A. in 1994. Currently, he is an assistant professor in computer engineering department. His research interests include optical computing, ubiquitous computing, and context-aware computing systems.