안전한 망 관리를 위한 보안정책 협상모델 설계

박 진 호† · 정 진 욱††

요 약

본 논문에서는 IPSec(IP Security) 환경에서 이동 에이전트 시스템을 이용한 안전한 망 관리를 위한 보안정책 협상모델을 설계하고자 한다. 기존의 안전한 망 관리를 위한 IP 보안 시스템들은 약간의 문제점들이 있다. 각 보안영역과 구현 환경에 따라 각기 다른 보안정책을 내부적으로 정의하여 사용하고 있다. 이로 인하여 패킷 전송시 보안 영역간 정책 요구사항이 서로 달라 패킷이 목적지까지 전달되지 않을 수도 있고, 패킷이 양방향으로 같은 경로를 따라 전송되고 같은 정책으로 보호되는지 보장할 수 없는 문제점을 내포하고 있다. 본 논문에서는 이러한 문제들을 이동 에이전트를 이용하여 해결할 수 있는 모델을 설계하였다. 각각의 보안 영역별로 보안정책의 협상이 필요하다면, 이동 에이전트는 보안정책 협상결과를 패스포트 형태로 관리하고, 이 패스포트를 이용하여 서로간의 인증 및 신뢰성을 보증해 준다.

Security Policy Negotiation Model Design for Secure Network Management

Jin-Ho Park† · Jin-Wook Chung††

ABSTRACT

This paper presents the design of a certain highly efficient security policy negotiation of SPS(Security Policy System) for secure network management using mobile agent system. The conventional IP security systems for secure network management have some problems. A drawback to these systems is that the required policy between each security area is different. Another problem is not possible to guarantee whether a packet is transmitted through the same path by both directions and is protected by the same policy due to the topology of the network. Unlike conventional systems, the model developed herein can be resolved by using a mobile agent technology. If each domain needs a negotiation of security policy, a mobile agent manages the result of the negotiation in the form of a passport and guarantees the authentication and reliability each other by using the passport.

키워드 : 망 관리(Network Management), 정책협상(Policy Negotiation), IP 보안(IP Security), 이동 에이전트(Mobile Agent)

1. Introduction

Use of the present Internet is catching seat by the most general business and living environment. Is used as various and new service offered through the Internet gets born in society all fields such as government agency, enterprise, bank, school and home. Request that wish to use these services more safely from various security threats is also increasing rapidly.

To support various security service required by Internet application efficiently, security protocol that secure transferring certification about data integrity and confidentiality is required, and various products of IPSec, TLS(Transport Layer Security) and VPN(Virtual Private Network) etc. are developed.

According as security products of various form are used, security policy applied by security area becomes various. Therefore, need effective policy negotiation and policy management about various security policies for data transmission between nodes.

Existent IP security system applies own area policy according to each security area without generalization of center concentrative management or policy information about policy in case communicate communicating with communication companion of different security area or flows different security area. Therefore, when use existing IP security service and exchanges IP packet between nodes, because of different policy requirement between security area or complex topology of net, problem happens that transfer following route that packet is same to two-way and that can not secure whether is protected by same policy [1].

These problems in Internet user wanted work through security policy negotiation for each group which security area differs taking advantage of a mobile agent technology that achieve automatic by asynchronous method solve can [2].

† 정 회 원 : 대덕대학 컴퓨터인터넷정보계열 조교수
†† 종신회원 : 성균관대학교 전기전자 및 정보통신공학부 교수
논문접수 : 2003년 9월 22일, 심사완료 : 2004년 2월 5일

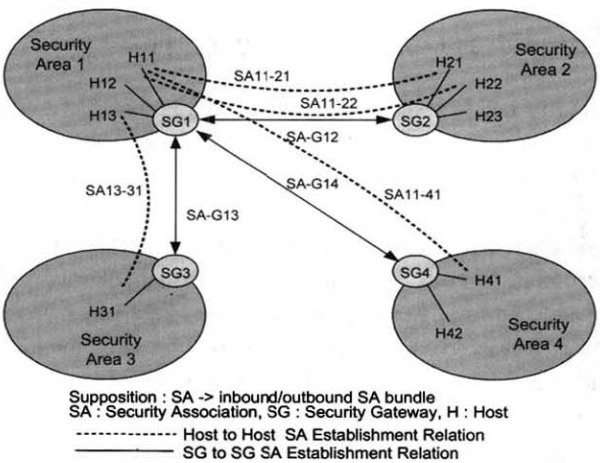
2. Necessity of Research

Existing IPSec system defines and is using different security policy according to each security field and implementation environment interiorly. Policy requirement between security area differs at packet transmission thereby and packet may not be passed to the destination. Also, is connoting problem that can not guarantee whether packet are transmitted along same respect for the old for bothway and are fenced by same policy.

Defined SPS that permit center intensive supervision and negotiation about defined policy informations as is different according to security area in IPSec Work Group to supplement these problem.

SPS defines policy according to each security area interiorly and stores sequentially to Master File. Stored Guideline area being defined policy information separatively, policy relation can exist between these policy.

Existent security policy negotiation process executes communication in each other security area that host and host are trusted through 1 to 1 negotiation after apply various security policy between each domain in IPSec SPS environment with (Figure 1). Because such negotiation process increases burdensomeness and traffic of network that should be enforced in each security sacred ground every time whenever communicate, there is serious problem that communication load is happened between each agent or SPS.



(Figure 1) IPSec SPS SA distribution

Policy information that is stored in master file runs policy negotiation using policy information that is transmitted, and is stored to SPS DB by SPS DB at first drive of SPS. But, can bring policy negotiation result that do not mean by mistake classification applied policy at policy negotiation about data transmission if relation between policy that is stored to SPS DB exists.

In the meantime, mobile agent is self-regulating software object that must move to some place for solution of problem that is given instead of user in different kind distributed environment, and can decide naturally what work must do [3]. That is, mobile agent visits some host sequentially, can assume as applet that can achieve some work over each platform. Mobile agent has advantage that can filter information acting for user in case user does not connect to network because do so that may achieve duty separatively without user's intervention or achieve task [3, 4].

If mobile agent does not encrypt and is executive code, analysis is available anytime. And can modify code without limit if host gets mind. Therefore, need hardware support or digital signature techniques to keep away authentication and agent code transformation mutually between client and server.

Result that mobile agent collects must protect necessarily from host that is enemy of evil. If do not protect mobile agent's result, host that is enemy of evil in result that go with mobile agent loads can cause next two harms.

① When host looks furtively mobile agent's result : Host is similar in result of move host because can look furtively result that mobile agent collects, but can present result that some difference becomes.
② When host manufactures mobile agent's result : Can delete result that collect in other host, and can modify the result by other value.

It is very important that protect result that mobile agent collects about host that visit therefore. Data that mobile agent collects as protectiveness, can trust data that mobile agent collects more, and can use mobile agent more applicatively.

This paper wishes to solve various problem that can happen by relation of dynamic security element during policy negotiation procedure between various security area translation in IPSec's SPS utilizing mobile agent.

3. Characteristic of Proposal Mechanism

Mechanism that propose designed press-button security policy negotiation of mobile agent and group policy division protocol can improve multi group security negotiation problem that was inefficient in existent SPS. Also, presented mechanism to secure integrity and confidentiality of information that mobile agent is used in negotiation and verification mechanism of identity certification information and specially, thing which can apply mechanism that is proposed in this paper that see without a change of existent

SPS system is advantage.

Group security policy negotiation that use mobile agent that propose is based on SPS that is IPSec policy aided system that permit supervision and negotiation about defined policy informations as is different according to security area to secure quality of security service.

SPS offers computerized mechanism that can find main security gateway and secondary security gateway connected with communication between religious order. Also, SPS does can verify security gateway identity in path of communication between religious order, and can verify whether specification security gateway has competence for specification host on prerequisite.

When IPSec uses open key password algorithm to establish SA safety because is basing on SA information that have safe key negotiation between two communication substances, IKE can create key administration session fewer than 60 per 1 second, but division way to use group key can provide service of level that VOD(Video on Demand) application requires using key administration session of number that is less [5].

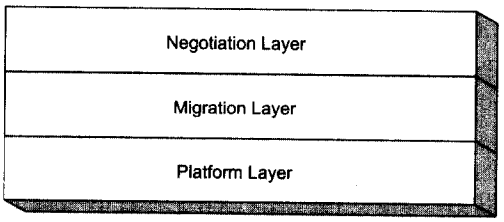
Because group security policy negotiation model who propose uses mobile agent, security policy negotiation between 1 and N group is available, and also, reduce number of times of negotiation so that can be safer and manage security policy negotiation system efficiently.

Negotiation protocol that propose takes way that mobile agent negotiates mobile agent system of each area and group security policy of short once and heighten safety while must run negotiation all in each host of each security area with (Figure 1). Because host to host base protocol applies rule of multiplication by number of case at security policy negotiation, as multiplication of number of host(N) of other security area with number of host(M) of execution opening security area indeed, proposed protocol has (N-1) reconsideration execution number of times using mobile agent while flow execution number of times of (M×N). Therefore, can improve performance of security policy negotiation system because protocol that propose more than existent host to host base security policy negotiation protocol reduces negotiation execution number of times.

4. Design of Secure Mobile Agent System

To guarantee secure mobile agent system operation, mechanisms to sense and defends several attacks need Confidentiality Mechanism to protect data and mobile agent code safely, Authentication Mechanism to confirm mutual identification and Authorization Mechanism to access control about host's resource.

Divide and designed as 3-layer according to each function for mobile agent system design that perform these requirement (Figure 2).



(Figure 2) 3-layer Mobile Agent System

4.1 Platform Layer

Platform layer is lowest layer for operation of mobile agent system, basic system hardware itself and operating system for virtual machine operation is come here, and all of the network architecture for code mobility and platform connected with function are included.

Security in platform layer includes all Securities for safe computing environment such as safe operating system, virtual machine and network, system resources from physical security. Need access control and data confidentiality guarantee as system security framework to protect mobile agent system, and Secure OS for operating system protection, VPN for transmission data security in network, SSL or TLS, and Digital Signed Code for program code certification need.

4.2 Migration Layer

Migration layer is layer for work achievement going network by layer for mobility guarantee that is most important advantage of mobile agent. When mobile agent that is made to base mobile code moves, executive code, data, running state etc. should be moved together.

Authentication is essential mutually between agent's source host and destination host by thing which security in Migration layer achieves agent move safely based on safe platform. Also, agent need method for this because original work achievement should be possible continually after agent's executive code, data, running state are moved. Usually, can achieve agent removal to use together encryption and digital signature about agent code, data and running state.

4.3 Negotiation Layer

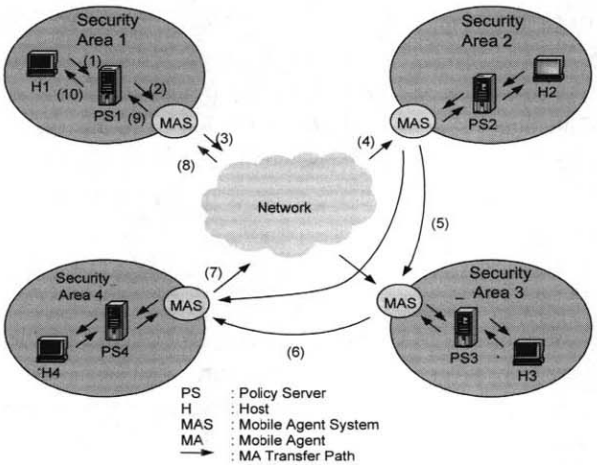
Negotiation layer is layer that user achieves indicating work as agent acts in destination host who move by layer that agent's actuality security policy negotiation achieves. Negotiation layer is layer that user achieves indicating work because it is layer that agent's actuality security po-

licy negotiation achieves, and agent acts in destination host. When agent discharges, life cycle about each agent, transaction processing, data management and synchronization service etc. should be offered.

It is thing to by thing which security in Negotiation layer protects agent from malicious host agent operation being blocked or forge avoid and keeps away unlawful correction of data. Therefore, authentication, confidentiality and integrity need compulsorily for safe agent operation. It need in actuality system that Code Obfuscation [6] that achieve mixing agent code to protect practice from host, security method to protect result after agent practice [7] and Cryptographic Trace [8] to chase host's unlawful access detection.

5. SPS Model using Mobile Agent System

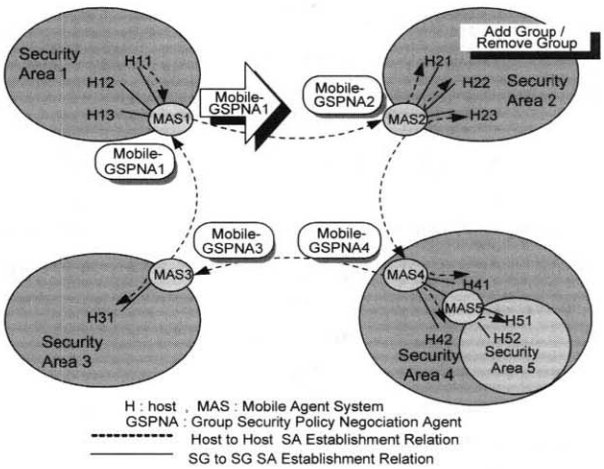
Security policy negotiation model's structure which is based on mobile agent is same with (Figure 3).



(Figure 3) Mobile agent negotiation structure between different security area

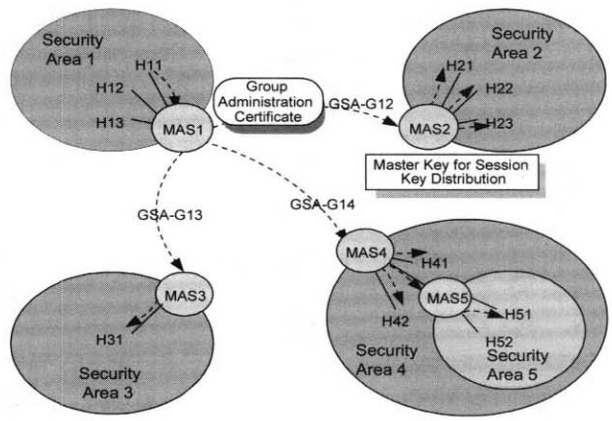
As MAS achieves role of security gateway in this paper that see, it is mobile agent system that execute or transmit MA. MAS delivers negotiated security psolicy to policy server PS using MA and host H communicates safe and reliable thing through security gateway using negotiated policy information. MAS that belong in each security area creates each agent MA to negotiate security policy and is transmitted by other security area in (Figure 3) through network. Transmuted MA is executed and policy negotiation at necessity in MAS in other security area.

Mobile-GSPNA1 has host information and position security area information that host that want connection in MAS1 wishes to connect via several MASs of security area and comes back to original position in (Figure 4).



(Figure 4) Group SA negotiation using mobile agent

Host H11 requests policy negotiation in MAS1 in group base policy negotiation model, and MAS1 transmits by MAS2 including group administration certificate to MA in (Figure 5). MAS2 verifies MA1's certificate and negotiate GSA that is security association information between MAS1 and MAS2 security area. GSA encrypts by the other's public key and divides safety policy information and master key for session key distribution. In MAS2, using policy information and key information that is negotiated, host H21, H22 and H23 about each new session key distribute in own security area2. MAS1, MAS2, MAS3, MAS4 and MAS5 have negotiated GSA information every moment by this method, and safe channel between hosts is formed because using policy information and key information in GSA. Safe channel can divide by transport mode and tunnel mode according to IPSec's mode. Basically, encryption and authentication being performed, MAS security gateway that do decrypt session key information encoded by master key process about GSA achieve.



(Figure 5) Group SA distribution using mobile agent

In the case of MAS5, MAS5's policy can be decided within GSA extent that is negotiated in MAS4 and MAS4 and MAS5 can run each policy negotiation with MAS1 in equal situation. That is, two case of MAS1-MAS4-AS5 and MAS1-MAS5 is possible. this case is decided according to security policy between these case domain. In case of MAS1-MAS5's direction negotiation, MAS5's security policy negotiation is achieved by MAS4's proxy function.

Group security policy negotiation structure that propose in this paper is created by method to divide hierarchical structure of tree style by group intention structure of graph style and it is efficient structure in group security policy negotiation.

6. Comparative Analysis with Existing Study

Decide to compare with E-Lock Technologies' e-Lock VPN 2.1 [12] and Cerberus system [13] that is IPSec embodiment product developing in NIST from some items such as IP security policy's requirement side.

Gateway's discovery function is that decide necessary security gateway gathering so that message may be delivered through single path between two security areas. Is transmitted along path that packet by complex topology of network is same to two-way and can not guarantee whether is fenced using same policy. Therefore, there is necessity to find safe security gateway of various path.

Should do so that mobile agent can authenticate identity of communicating security gateway or mobile agent system. Also, should prove whether security gateway that represent some specific host was delegated authority from the mobile agent system actually. Gateway that represent specific host must be able to certify that have authority that represent the host.

Relation with key management system describes relativity availability with key management protocol. Must be able to utilize with other key exchange protocol in addition to IKE, key exchange protocol for IP security system, because IP security policy is designed separatively with key management system.

Security policy access method, relation with IP security system, security policy API are describing in IP security system and different angle about relation with SPS, security policy's access method described that IP security system can approach how and use security policy. Relation with IP security system describes whether SPS was embodied to IP security system and some topology and security policy API SPS whether interface in outside system is some describe.

Expression of policy should be soft and independent to manufacturer. Vertical node must be able to know policy that is applied to own packet because pass network that packet is over plural administration area in communication between vertical. Though technology of this policy is neutral to manufacturer, opponent IP security nodes can understand and execute (terminal mode or transmission mode) policy at which one end for SA.

Expression of policy was not dependent in product development by accommodating policy description laguage of connection standardization group even if there is on IP security policy's expression, and made policy technology of administrators between digenomic species system can be understood.

〈Table 1〉 Comparative analysis with existing study

Item	e-LockVPN	Cerberus system	Proposing Negotiation Model
Gateway Discovery	Do not support	Do not support	Support
MA or MAS Authentication	Do not support	Do not support	Support
Relation of Key Management System	Dependent	Dependent	Independent
Access Method of Security Policy	Not Open	Not Open	distributed
Relation of IP Security System	Dependent	Dependent	Independent
Security Policy API	Not Open	Not Open	Open
Policy Description	Itself	Itself	IETF의 IPSP WG
Standardization	Itself	Itself	IETF의 IPSP WG
Negotiation Method of Security Policy	Not	Not	1 : Group
Number of Security Policy Negotiation	Not	Not	N - 1

7. Conclusions

This paper proposed group security policy negotiation model who use mobile agent for efficient group security policy in IPSec's SPS environment. To improve problem defined in introduction in this paper, when security policy negotiation between each domain need using mobile agent, enforce once, and negotiated result mobile agent in negotiation group's passport form storage manage, and secure quotation and authentication between each other because using this passport when need. Group security policy negotiation model's advantage which model proposed in paper that can protect and sees mobile agent from host that is spiteful is as following.

① In case do 1 to 1 communication with existing IPSec base SPS server, number of times of security policy negotiation M×N process of degree flow. But, by security policy negotiation of 1 to N-1 by group negotiation that use mobile agent negotiation number of times (N-1) by reducing reduced various security threat ureas, and improved usability of network.

② Solved IKE overload problem through efficient bundle negotiation of group key and group policy, designed so that is suitable in multicast communication environment reducing IKE's work to mobile agent's policy and key exchange negotiation mechanism.

③ Separation between session key and security policy that have different life cycle is impossible, and existent IPSec SPS structure offers mechanism that can redistribute session key efficiently.

④ In different or equal area, multistage group key application that confidentiality/integrity level differs is possible.

Realized with commercialization of the proposed model in this thesis, users among diverse security areas in the electronic commerce, that will be increased far more rapidly in the near future, will be benefited from the improved system performance and reliability through the authentication of more effective security negotiation. That is anticipated to help stimulating the electronic commerce industries as a whole. By ensuring the SPS for the user-demand-oriented security quality support, it can be utilized for the negotiating component of the security policy of the IPSec system. Used together in other security areas of the next generation internet base, it is also expected to meet diverse users' inquiries between security systems.

Future research topic needs to work on ways to increase reliability among security areas via N vs. N security policy negotiation expanded from the proposed method in this research and optimization techniques complied with the granularity of security areas.

References

[1] L. A. Sanchez and M. N. Condell, "Security Policy System," Internet Draft, draft-ietf-ipsec-sps-00.txt, 1998.

[2] C. G. Harrison, D.M. Chess and A. Kershenbaum, "Mobile Agents : Are they a good idea?," IBM Research Division, March, 1995.

[3] M. Wooldridge and N. R. Jennings, "Intelligent Agent : Theory and practice," The Knowledge Engineering Review, 10(2), pp.115-152, 1995.

[4] David Chess and Benjamin Grosof, "Itinerant Agents for Mobile Computing," Available from authors, May, 1995.

[5] Mark Baugher, Ran Canetti, Lakshminath, "Group Key Management Architecture," Internet Draft, draft-ietf-msec-gkmarch-00.txt, 2001.

[6] C. Collberg, C. Thomborson and D. Low, "A Taxonomy of Obfuscation Transformations," Technical Report 148, Department of Computer Science, University of Auckland, 1997.

[7] G. Karjoth, N. Asokan and C. Gulcu, "Protecting the Computation Results of Free-Roaming Agents," Proceedings of the Second International Workshop, MA '98, pp.195-207, 1998.

[8] G. Vigna, "Cryptographic Trace for Mobile Agents," Mobile Agents and Security, Spring-Verlag, Lecture Notes in Computer Science 1419, pp.137-153, 1998.

[9] L. A. Sanchez and M. N. Condell, "Security Policy Protocol," Internet Draft, draft-ietf-ipsec-spp-00, 1999.

[10] M. S. Greenberg, J. C. Byington, T. Holding, and D. G. Harper., "Mobile Agents and Security," IEEE Communications Magazine, 36(7), pp.76-85, July, 1998.

[11] H. Reiser G. Vogt, "Security Requirements for Management Systems using Mobile Agents," Proceedings of the Fifth IEEE Symposiumon Computers and Communications : ISCC 2000, Antibes, France, pp.3-6, July, 2000.

[12] e-Lock VPN 2.1 Policy Management, http://www.e-lock.com/Products/VPN/POLICYMANAGE.HTM.

[13] NIST Cerberus, An IPSec Reference Implementation for Linux, http://snad.ncsl.nist.gov/cerberus/.

박 진 호

e-mail : parkjinho@ddc.ac.kr

1995년 대전대학교 전자계산학과(공학사)

1997년 대전대학교 컴퓨터공학과(공학석사)

1997년~현재 성균관대학교 전기전자 및 컴퓨터공학부(박사수료)

2000년~2002년 송호대학 정보산업계열 전임강사

2002년~현재 대덕대학 컴퓨터인터넷정보계열 조교수

관심분야 : 네트워크 관리, 보안

정 진 욱

e-mail : jwchung@songgang.skku.ac.kr

1974년 성균관대학교 전기공학과(공학사)

1979년 성균관대학교 전자공학과(공학석사)

1991년 서울대학교 전자계산학과(이학박사)

1973년~1985년 한국과학기술연구소(KIST) 실장

1996년~현재 한국정보처리학회 회장

1996년~현재 정보보호 추진분과위원회 자문위원

1985년~현재 성균관대학교 전기 전자 및 컴퓨터공학부 교수

관심분야 : 네트워크 관리, 망 보안, 컴퓨터교육