이동 에이전트 시스템을 이용한 SPS 모델 설계

박 진 호* · 정 진 욱**

요 약

본 연구는 IPSec 환경에서 이동 에이전트를 이용한 효율적 그룹 보안정책 협상을 위한 모델 개발을 위한 것이다. 기존의 IP 보안 시스템들은 약간의 문제점들이 있다. 우선 각각의 보안 영역별로 요구되는 보안정책이 서로 다른 단점들이 있으며, 또한 네트워크 토폴로지에 따라 패킷들이 전송되는 경로가 일정하다는 것과 동일한 보안 정책으로 보호받을 수 있다는 것을 보장할 수 없다. 본 논문에서는 이러한 문제들을 이동 에이전트를 이용하여 해결할 수 있는 모델을 개발하였다. 각각의 보안 영역별로 보안정책의 협상이 필요하다면, 이동 에이전트는 보안정책 협상결과를 패스포트 형태로 관리하고, 이 패스포트를 이용하여 서로간의 인증 및 신뢰성을 보증해 준다.

Design of SPS Model using Mobile Agent System

Jin-Ho Park* · Jin-Wook Chung**

ABSTRACT

This research presents the development of a certain highly efficient model for group security policy negotiation using mobile agents in the IPSec environment. The conventional IP security systems has 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.

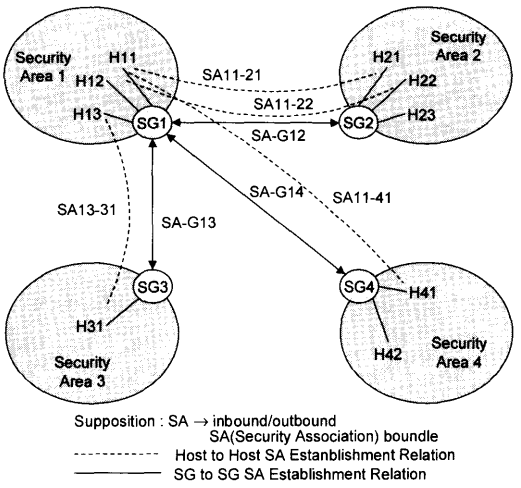
* 대덕대학 컴퓨터인터넷정보계열
** 성균관대학교 정보통신공학부

1. 서 론

기존 IPSec 시스템은 각 보안 영역과 구현 환경에 따라 각기 다른 보안 정책을 내부적으로 정의하여 사용하고 있다. 이로 인하여 패킷 전송시 보안 영역간 정책 요구사항이 서로 달라 패킷이 목적지까지 전달되지 않을 수도 있다. 또한, 패킷이 양방향으로 같은 경로를 따라 전송되고 같은 정책으로 보호되는지 보장할 수 없는 문제점을 내포하고 있다.

이러한 문제점을 보완하기 위해 IPSec WG에서는 보안 영역에 따라 다르게 정의된 정책 정보들에 대한 중앙 집중적인 관리와 협상을 가능하게 하는 Security Policy System(SPS)을 정의하였다.

보안정책 시스템에서는 각 보안 영역에 따라 정책을 내부적으로 정의하여 Master File에 순차적으로 저장한다. 저장된 정책은 영역별 독립적으로 정의된 정책 정보이며, 이들 정책간에는 정책 연관성이 존재할 수 있다.



(그림 1) IPSec 보안정책 시스템의 SA 분배

기존의 보안정책 협상 과정은 (그림 1)과 같이 IPSec SPS 환경에서 각 도메인간의 다양한 보안정책을 적용한 후 서로 host와 host 1 대 1 협상을 통하여 신뢰된 보안영역간에서 통신을 실시한다. 이와 같은 협상과정은 통신을 할 때마다 매번 각 보안영역간에서 실시되어야하는 번거로움과 네트워크의 트래픽을 증가시켜, 각 에이전트나 보안정책시스템 간에 통신 부하가 발생되는 심각한 문제점이 있다.

마스터 파일에 저장된 정책 정보는 보안정책 시스템의 최초 구동시 SPS DB(Database)로 전송되며, SPS DB에 저장된 정책 정보를 이용하여 정책 협상을 수행한다. 그러나 SPS DB에 저장된 정책 사이에 연관성이 존재한다면 데이터 전송에 대한 정책 협상시 잘못 분류 적용된 정책으로 인하여 뜻하지 않은 정책 협상결과를 가져올 수 있다.

한편, 이동 에이전트는 이종 분산 환경에서 사용자를 대신하여 주어진 문제의 해결을 위해 어떤 장소로 이동해야 하며, 어떤 일을 해야 하는지를 스스로 결정할 수 있는 자율적인 소프트웨어 객체이다[1]. 즉 이동 에이전트는 어떤 호스트를 순차적으로 방문하여, 각 플랫폼 위에서 어떤 작업을 수행할 수 있는 애플릿(applet)으로 볼 수 있다. 이동 에이전트는 사용자의 개입 없이 독립적으로 임무를 수행하도록 하여 사용자가 네트워크에 접속하지 않은 경우에도 사용자를 대행하여 정보를 여과하거나 태스크를 수행할 수 있는 장점을 가지고 있다[1, 2].

이동 에이전트는 실행 가능한 코드이므로 암호화를 하지 않는다면 언제든지 분석이 가능하다. 그리고 호스트가 마음만 먹으면 얼마든지 코드를 수정할 수 있다. 그러므로 클라이언트 서버의 상호 인증과 에이전트 코드변형을 막기 위한 하드웨어 지원이나 전자서명 기법이 필요하다.

이동 에이전트가 수집한 결과 값은 악의적인 호스트로부터 반드시 보호하여야 한다. 이동 에이전트의 결과를 보호하지 못하면, 이동 에이전트가 적재하여 가지고 다니는 결과에 악의적인

호스트는 다음의 두 가지 해를 끼칠 수 있다.

- 호스트가 이동 에이전트의 결과를 엿보는 경우 : 호스트는 이동 에이전트가 수집한 결과를 엿볼 수 있으므로, 이전 호스트의 결과에 비슷하지만 약간의 차이가 나는 결과를 제시할 수 있다.
- 호스트가 이동 에이전트의 결과를 조작하는 경우 : 다른 호스트에서 수집한 결과 값을 삭제할 수 있고, 그 결과를 다른 결과 값으로 조작할 수 있다.

따라서 방문하게 될 호스트에 대해 이동 에이전트가 수집한 결과를 보호하는 것은 아주 중요하다. 이동 에이전트가 수집한 데이터를 보호함으로써, 이동 에이전트가 수집한 데이터를 보다 신뢰할 수 있으며, 이동 에이전트를 보다 실용적으로 이용할 수 있다.

본 논문에서는 IPSec의 SPS에서 다양한 보안영역간의 정책협상 절차중에 동적인 보안요소의 연관성으로 인하여 발생할 수 있는 다양한 문제점을 이동 에이전트를 이용해서 해결하고자 한다.

2. 제안한 메커니즘의 특성

제안한 메커니즘은 기존의 SPS에서 비효율적이었던 그룹 다자간 보안협상 문제를 개선할 수 있으며, 이동 에이전트의 자동화된 보안정책 협상 및 그룹정책 분배 프로토콜을 설계하였다. 또한 이동 에이전트가 협상에 사용되는 정보의 무결성과 비밀성을 보장하기 위한 메커니즘과 신원 인증 정보의 검증 메커니즘을 제시하였고 특히, 기존의 SPS 시스템의 변경 없이 본 논문에서 제안된 메커니즘을 적용할 수 있는 것이 장점이다.

제안한 이동 에이전트를 이용한 그룹 보안정책 협상은 보안 서비스 품질을 보장하기 위해 보안영역에 따라 다르게 정의된 정책 정보들에 대한 관리와 협상을 가능하게 하는 IPSec 정책지원시스템인 SPS를 기반으로 한다.

SPS는 종단간의 통신에 관련된 주 보안게이트웨이와 부 보안게이트웨이를 발견할 수 있는 자동화된 메커니즘을 제공한다. 또한, SPS는 종단간 통신의 경로 상에 있는 보안게이트웨이 신원을 검증할 수 있고, 특정 보안게이트웨이가 특정 호스트에 대한 권한을 갖는지를 검증할 수 있다는 점을 전제조건으로 한다.

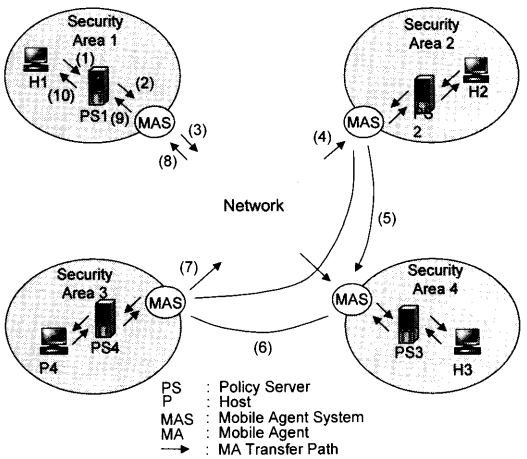
IPSec은 두 통신 실체간의 안전한 키 협상을 갖는 SA 정보에 기초를 두고 있기 때문에, SA를 안전하게 확립하기 위해 공개키 암호 알고리즘을 사용하는 경우, IKE는 초당 60개 이하의 키 관리 세션만을 생성할 수 있지만 그룹키를 사용한 분배방식에서는 적은 수의 키관리 세션을 이용하여 VOD(Video on Demand) 응용이 요구하는 수준의 서비스를 제공할 수 있다[3].

제안하는 그룹 보안정책 협상 모델은 기존의 종단간 1 대 1 보안정책 협상을 이동 에이전트를 이용하여 1 대 N의 그룹간 보안정책 협상을 통하여 시스템의 부하가 많은 협상의 횟수를 줄임으로써 보다 안전하고 효율적으로 보안정책 협상 시스템을 관리할 수 있도록 하였다.

(그림 1)에서와 같이 각 보안영역의 각 호스트마다 모두 협상을 수행하여야 하는데 비해 제안하는 협상 프로토콜은 이동 에이전트가 각 영역의 이동 에이전트 시스템과 단 한번의 그룹 보안정책 협상을 하여 안전성을 높이는 방식을 취한다. "host to host" 기반의 프로토콜은 보안정책 협상 수행시 경우의 수에 의한 곱의 법칙을 적용하면 실행 개시 보안영역의 host 수(M)와 다른 보안영역의 host 수(N)의 곱으로서 즉, (M×N)의 수행 횟수를 거치는데 비해 제안된 프로토콜은 이동 에이전트를 이용하여 (N-1)번의 수행 횟수만을 가진다. 그러므로 기존의 "host to host" 기반의 보안정책 협상 프로토콜 보다 제안하는 프로토콜이 수행 횟수를 줄이므로 보안정책 협상 시스템의 성능을 향상시킬 수 있다.

3. 이동 에이전트 시스템을 이용한 SPS 모델 설계

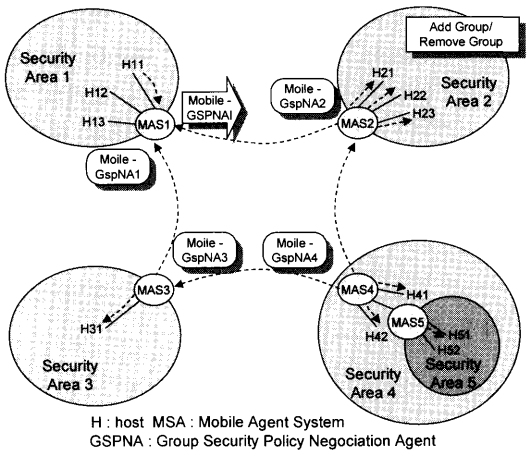
이동 에이전트를 기반으로 하는 보안정책 협상 모델의 구조는 (그림 2)와 같다.



(그림 2) 서로 다른 보안영역간의 이동 에이전트 협상 구조

MAS는 본 논문에서 보안게이트웨이의 역할을 수행하면서 MA를 실행하거나 전송시키는 이동 에이전트 시스템이다. MAS는 MA를 이용하여 협상된 보안정책을 정책서버 PS에 전달하고 통신하고자하는 호스트 H는 협상된 정책정보를 이용하여 보안게이트웨이를 통해 안전하고 신뢰성 있는 통신을 수행하게 된다. 각 보안영역에 속해있는 MAS는 보안정책을 협상할 에이전트 MA를 각각 생성시키고 네트워크를 통해 (그림 2)과 같이 다른 보안영역으로 전송된다. 전송된 MA는 다른 보안영역에 있는 MAS에서 실행되고 필요시 다른 보안영역의 MAS와 정책협상을 수행한다.

(그림 3)에서 Mobile-GSPNA1는 MAS1에서 접속하고자하는 호스트가 속한 보안영역의 여러 MAS를 거쳐 접속하고자 하는 호스트 정보와 소속 보안영역 정보를 갖고 본래의 위치까지 되돌아온다.



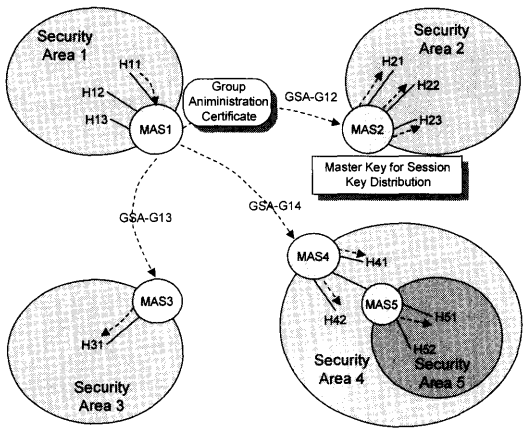
(그림 3) 이동 에이전트를 활용한 그룹 SA 협상

그룹기반의 정책협상 모델에서는 (그림 4)에서와 같이 호스트 H_{11}이 MAS_1에서 정책협상을 요청하고, MAS_1은 MA에 그룹관리 인증서를 포함시켜 MAS_2로 전송한다. MAS_2는 MA_1의 인증서를 검증하고 MAS_1과 MAS_2 보안영역간의 보안연계(Security Association) 정보인 GSA를 협상하게된다. GSA에는 정책정보와 함께 세션키 분배용 마스터키를 상대방의 공개키로 암호화하여 안전하게 분배한다. MAS_2에서는 협상된 정책정보와 키 정보를 이용하여 자신의 보안영역$_2$에 있는 호스트 H_{21}, H_{22}, H_{23} 각각에 대하여 새로운 세션키를 분배하게 된다. 이러한 방법으로 MAS_1, MAS_2, MAS_3, MAS_4, MAS_5에서는 각각 협상된 GSA 정보를 갖게 되고, GSA에 있는 정책정보와 키 정보를 이용하여 호스트들간의 안전한 채널이 형성된다. 안전한 채널 구간은 IPSec의 모드에 따라 트랜스포트 모드인 경우와 터널모드의 경우로 나누어 볼 수 있다. 기본적으로 암호화와 인증이 수행되면서, 마스터키로 암호화된 세션키 정보를 복호화 하는 MAS 보안게이트웨이에서 GSA에 대한 처리를 수행한다.

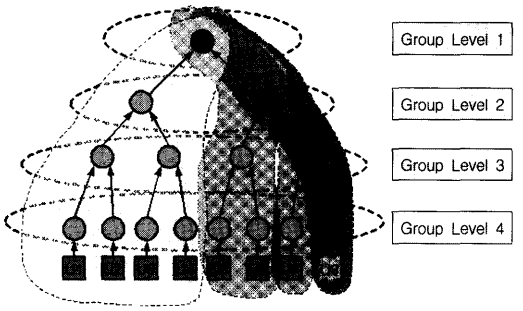
MAS_5의 경우, MAS_4에서 협상된 GSA 범위

내에서 MAS_5의 정책이 결정될 수도 있고 MAS_4와 MAS_5가 동등한 입장에서 MAS_1과의 정책협상을 각각 수행할 수 있다. 즉, MAS_1 - MAS_4 - MAS_5와 MAS_1 - MAS_5의 두 가지의 경우가 가능하다. 이러한 경우 도메인간의 보안정책에 따라 결정된다.

MAS_1 - MAS_5의 직접협상의 경우, MAS_4의 대리(proxy) 기능에 의해 MAS_5의 보안정책 협상이 수행된다.



(그림 4) 에이전트를 활용한 그룹 SA 분배



(그림 5) 그룹의 부서별(세로)/등급별(가로) 접근수준

본 논문에서 제안하는 그룹 보안정책 협상 구조는 트리형의 계층 구조를 (그림 5)와 같은 그래프형의 그룹 지향 구조로 분할하는 방법으로 생성되며, 그룹 보안정책 협상에 효율적인 구조이다.

4. 결 론

본 논문에서는 IPSec의 SPS 환경에서 효율적인 그룹 보안정책을 위하여 이동 에이전트를 이용한 보안정책 협상모델을 제안하였다.

본 논문에서는 서론에서 정의된 문제점을 개선하기 위하여 이동 에이전트를 활용하여 각 도메인간의 보안정책 협상이 필요한 경우 한번 실시하여 협상된 결과를 이동 에이전트가 협상 그룹의 패스포트 형태로 보관 관리하여 필요한 경우 이 패스포트를 이용해서 서로간의 인증 및 신뢰성을 확보한다.

제안한 모델은 악의가 있는 호스트로부터 이동 에이전트를 보호할 수 있으며 본 논문에서 제안한 보안정책 협상모델의 장점은 다음과 같다.

- 기존 IPSec 기반 SPS 서버와의 1 대 1 통신을 할 경우 보안정책 협상의 횟수를 M×N 만큼의 과정을 거쳐야 하나, 이동 에이전트를 이용한 그룹 협상에 의해 1 대 N-1의 보안정책 협상으로 협상 횟수를 N-1로 줄여서 각종 보안위협 요소를 줄였고, 네트워크의 가용성을 향상시켰다.
- 그룹키와 그룹정책의 효율적인 일괄협상을 통하여 IKE 과부하 문제를 해결하였으며, 이동 에이전트의 정책 및 키교환 협상 메커니즘으로 IKE의 작업을 경감시켜 멀티캐스트 통신 환경에 적합하도록 설계하였다.
- 수명 주기가 다른 세션키와 보안정책간의 분리 불가능성을 제공하며, 기존의 IPSec SPS 구조상에서 세션키를 효율적으로 재분배할 수 있는 메커니즘을 제공한다.
- 상이한 영역간 또는 동일한 영역 내에서의 비

밀성/무결성 보안등급이 서로 다른 다단계 그룹키 적용이 가능하다.

본 논문에서 제안한 모델이 상용화로 구현된다면, 앞으로 더욱 급속히 증가할 전자상거래에서 다양한 보안영역간의 이용자들은 보다 효과적인 보안협상의 인증을 통하여 시스템 성능과 신뢰성이 향상되어 산업 전반에 걸쳐 도움이 될 것이다. 또한, 사용자 요구기반 보안품질 지원을 위한 보안정책 시스템을 확보함으로써 IPSec 시스템의 보안정책을 협상하는 요소로 사용될 수 있으며, 차세대 인터넷 기반의 다른 보안영역에서 함께 사용되어 보안 시스템간 다양한 사용자 요구사항을 지원할 것으로 기대된다.

향후 연구 과제로는 논문에서 제안한 방식에서 더 확장된 N대 N의 보안정책 협상을 통하여 각 보안영역간에 신뢰성을 향상시키는 기법에 대한 연구와 보안영역의 크기(granularity)에 따른 최적화 기법연구가 필요하다.

참 고 문 헌

[1] M. Wooldridge and N. R Jennings, "Intelligent Agent : Theory and practice", The Knowledge Engineering Review, Vol.10, No. 2, pp.115-152, 1995.

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

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

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

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

[6] M. S. Greenberg, J. C. Byington, T. Holding, and D. G. Harper., "Mobile Agents and Security", IEEE Communications Magazine, Vol.36, No.7, pp.76-85, July 1998.

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

박 진 호

1995년 대전대학교 전자계산학과 (공학사)

1997년 대전대학교 컴퓨터공학과 (공학석사)

1997년~현재 성균관대학교 전기전자 및 컴퓨터 공학부(박사수료)

2000년~2002년 송호대학 정보산업계열 전임강사

2002년~현재 대덕대학 인터넷정보기술계열 전임강사

관심분야 : 네트워크 관리, 보안

정 진 욱

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 전기전자 및 컴퓨터 공학부 교수

관심분야 : 네트워크 관리, 망 보안, 컴퓨터교육