계층적 보안 정책에서의 Cross 연동 메커니즘

이지인*o, 엄남경*, 이상호*
충북대학교 전자계산학과 *
{jilee, family8, shlee}@cnlab.chungbuk.ac.kr *

Design of A Cross Working Mechanism for Hierarchical Security Policy

Lee Ji-In *° , Um Nam-Kyoung *, Sang-Ho Lee *
Dept. of Computer Science, Chungbuk National Univ *

요 약

인터넷은 전세계를 대상으로 구축된 네트워크로서 개방형 구조의 프로토콜을 사용하므로 대부분의 호스트 컴퓨터 시스템들은 정보보안에 취약한 상태이다. 이와 같은 보안 취약성으로 인해 상용화 서비스에 대한 교환 정보의 수정, 검색, 파괴 등의 역기능이 발생하고 있다. 이 논문에서는 기존의 보안 방식 정책으로는 인터넷 보안의 역기능에 대한 완벽한 대책이 될 수 없으므로 이에 따른 보안정책 크로스 연동 메커니즘을 설계하여, 기존의 방식과 비교 분석해서 앞으로의 차세대 인터넷에 적합한 연동메커니즘을 제안하고자 한다

1. 서론

인터넷 확산으로 인하여 컴퓨터 사용자들에게 편리성을 제공해 주는 반면 개방형 구조인 TCP/IP 프로토콜의 보안 취약성 때문에 역기능이 발생하고 있다. 따라서 이에 대한 보안 대책이 요구되는데 통신망 규모가 확대되면서 이러한 보안정책을 적용할 수 있는 정책 시행 점들이 많아지고 이로 인하여 그 시행 점들 간의 보안정책에 관한 연구가 절실히 요구된다. 따라서 이 논문에서는 계층적 구조를 갖는 보안정책 모델에 따른 보안정책 연동 방식을 설계한후 이에 따른 크로스 연동 메커니즘을 설계하여 비교 분석하겠다.

이 논문의 구성은 다음과 같다. 2장에서는 보안정책 관리와 정책관리 시스템에 대해 기술하고 3장,4장에서는 기존의 보안정책 연동 메커니즘 방법에 대해 분석하고 제안하고자 하는 Cross 연동방식에 대해 기술한 후, 두 가지 방식을 비교 분석한다. 결론 및 향후 연구 방향은 5장에서 제시된다.

2. 보안정책

2.1 보안정책 관리와 정책관리 시스템

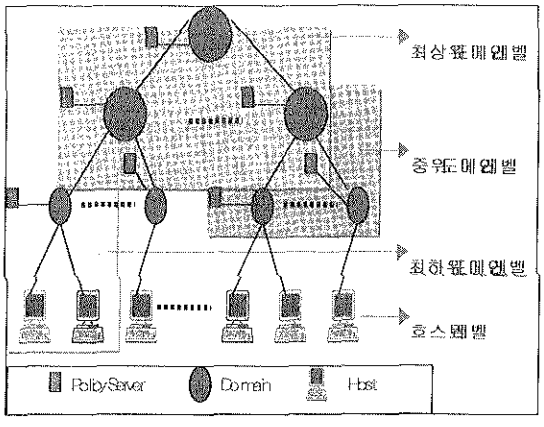
보안정책(Security Policy)은 조직의 기술과 정보 자산에 접근하기 위해 지켜야 하는 규칙의 형식문으로 시스템 자원에 접근하고자 하는 요구에 대한 허가 및 거부를 정의한다.

보안 정책 시스템의 구성요소는 크게 네 부분으로 나눌 수 있으며, 정책 관리 도구, 정책 저장소, 정책 소비자, 정책 대상으로 나누어진다[1]. 정책 관리 도구는 정책을 명세 할 수 있도록 사용자 인터페이스를 제공하는 부분이며 정책 저장소는 명세된 정책을 저장하는 부분이다. 디렉토리 서비 및 데이터베이스를 이용할 수 있으며 저장소 접근 프로토콜로는 LDAP V.3 를 이용한다. 정책 소비자는 정책 저장소나 정책 관리 도구로부터 정책을 획득하고 이를 해석하는 기능을 수행한다. 정책 소비자는 주로 정책 대상에 위치하게 되는데 정책 대상은 정책

소비자로부터 해석된 정책 정보를 가지고 정책을 시행하는 곳이다.

2.2 계층적 보안 정책 모델

보안 정책 모델에 접근하는 방식으로는 flat structure 방식과 hierarchical structure 방식이 있다. flat structure 접근 방식은 전체 보안정책 공간의 효율적인 사용이 가능하고 인터넷 환경에서 보안정책 복제로 능률을 유지할 수는 있다. 그러나 분산된 보안정책 변화에 따른 갱신의 어려움이 존재한다. Hierarchical structure는 중앙 집중 방식이 아닌 분산방식으로 보안정책 변화에 따른 갱신이 쉽다. 또는 같은 도메인 내 정책 협상이 불필요하다는 장점이 있다.



[그림 1]계층적 보안 정책 모델

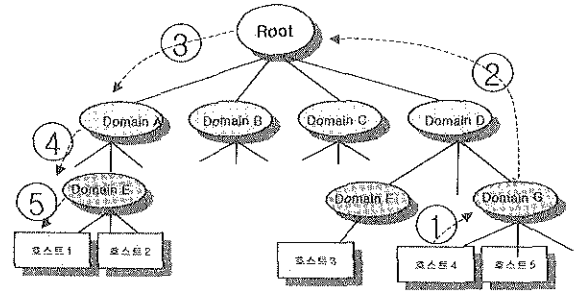
[그림1]과 같이 계층적 보안 정책 모델은 최상위 - 중위 - 최하위 도메인 레벨과 호스트 레벨로 추상화시킬 수 있다[2]. 이 때, 루트로부터의 객체지향형의 상속 개념을 적용시킬 수 있으며, 오버라이드를 정책 수정에 허용하여 설계한다.

3. 연동 메커니즘

3장에서는 기존의 제안되어 있는 연동 방식을 기술하고, 이에 대해 SA(Security Association)를 효과적으로 할 수 있는 크로스 연동 방식을 제안한다. 또한 기존의 제안된 연동 방식과 크로스 연동 방식을 비교 분석하여 효율성을 입증하고자 한다.

3.1 기존의 연동 메커니즘

도메인간의 보안 정책 설정은 실질적인 통신이 시작되기 전에 보안 정책 협상의 단계가 요구된다. 루트보안정책 서버로부터 도메인 A~D는 보안 정책을 상속받으며 도메인 D는 도메인 F와 G에게 보안정책을 상속한다. 상속된 보안정책과 각 도메인마다의 보안정책을 합하여 각 도메인에 요구되는 보안정책을 설정하게 된다.

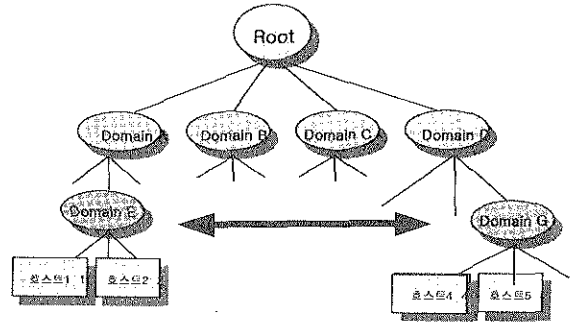


[그림 2] 기존의 연동 방식

호스트 4로부터 도메인 G에게 호스트 1과 정책 정보를 전달하고 도메인 G는 자신에게 속한 호스트가 아님을 확인하고 루트에게 전달한다. 루트는 호스트1이 속한 최상위 도메인인 도메인 A에게 전달하고 도메인 A는 호스트 1이 속한 상위도메인인 도메인 E에게 전달한다. 이어 도메인 E는 호스트 1에게 호스트 4가 전달한 정보를 전달하여 두 호스트는 정책정보를 협상하게 된다.

3.2 크로스 연동 메커니즘

3.2.1 연동 메커니즘 동작



[그림 3] 크로스 연동 방식

호스트4와 호스트1의 정책협상이 자주 이루어진다고

가정했을 때, 도메인 G나 최상위 서버를 일일이 거치는 과정은 매우 번거로운 일이다. 최상위로부터 도메인E와 도메인G 사이에 정책 협상이 이루어졌다면 최상위를 거치지 않고 호스트4와 호스트1 사이의 보안 정책 협상이 이루어질 수 있는데 이를 크로스 정책 협상(Cross SA)이라 한다.

3.2.2 보안정책 SA 제약에 관한 확장 필드

Cross SA를 할 경우, 여러 연동 메커니즘 방법이 존재할수 있는데 이에 대한 정책이 필요하며 정책에 따라 여러 가지 제약이 따를 수 있다. 제약에 관한 자세한 사항은 표1과 같다.

[표1] 보안정책 SA 제약에 관한 확장 필드

필드이름	의 미
basicConstraints	도메인사이의 SA경로 길이를 제한하는 내용이 포함
nameContraints	정책 경로상의 이름 제한
policyConstraints	포함 또는 금지하는 정책

SA 설정시 프로토콜과 함께 전달되는 PDU(Packet Data Unit)는 기존의 방법에서 제시하고 있는 확장된 메시지 포맷을 이용한다[2].

4. 제안 방식에 대한 비교 분석

4.1 기존의 방식과의 비교분석

기존의 연동 방식과 앞에서 설계한 크로스 연동 방식에 대해 검색 체인과 협상 시간, 관리의 용이성 등을 들어, 비교 분석하였다. 여기서는 [2]에서 설계한 방식2에 대한 예를 들어 기술하였다.

[표 2] 연동방식의 비교

비교항목	기존방식(Case1)	크로스방식
검색체인	7	1
협상시간	길다	짧다
관리의 용이성	효과적이다	덜 효과적이다
취약점	망의 크기가 커지면, 망에 부하가 생길 수 있다.	망의 크기가 커지더라도 망의 부하를 감소시킬 수 있다.

네트웍의 크기가 커지면 커질수록 크로스 연동 방식이 이상적인 검색체인을 가지고 있으므로 보안 정책을 위한 계층적 연동 방식으로 크로스 연동방식이 더 효과적임을 알 수 있다.

5. 결론 및 향후 과제

이 논문에서는 계층적 정책보안모델에서 적용 가능한 연동 방식들을 설계하고 이에 필요한 PDU의 구조를 정의하였으며 설계한 연동 방식의 효율성을 비교하였다. 네트웍의 크기가 커지고 각각의 도메인마다 상이한 정책을 적용하여야 하는 차세대 네트웍에서 계층적인 모델 설계는 반드시 필요하며 이에 따른 연동 방식은 필수적이다. 크로스 연동메커니즘 설계시 최상위나 상위 도메인을 불필요하게 거치지 않고 바로 정책협상이 이루어질수 있으나 보안정책 수정시 상속에 대한 여러 가지 정책이 필요하고 정책에 따른 제약 사항 등 개선해야 할 연구과제로 남아있다.

향후에는 크로스 연동방식의 정책 및 정책에 대한 제약 방법, 양방향 제어를 위한 상호 연동 방식 설계에 대하여 연구하여 계층적 보안 정책의 적용 분야에 이용하는 방식을 연구하여야 한다. 또한 이를 위해 보안정책 제어를 위한 기반 규칙 설계와 계층적 보안 구조의 특성 및 보안 취약성 분석, 대책 마련이 필요하다.

[참고문헌]

[1] IETF RFC 2026, "The Internet Standards Process", October, 1999.

[2] 이용주,엄남경,이지인,이상호,김건우 "보안정책에서의 계층적 연동 방식 설계", 정보과학회 충청지부 학술발표대회, Nov, 2000.

[3] 엄남경, 김건우, 이종태, 손승원, 이상호, "안전한 통신을 위한 계층적 구조의 보안정책 적용 방안", 한국통신정보보호학회 충청지부, Nov, 2000.

[4] 신종태, 강창구, 이대기, "정보 보호 센터의 구성에 관한 연구", 정보보호와 암호에 관한 학술대회논문집, 10, 1994.

[5] 송주석, "통신 정보 보호 정책 방향에 관한 연구", 한국통신학회 정보통신의 날 기념학술발표회논문집, 1997.

[6] 최창호, 정태일, 김성조, "계층적 서버 모델을 기반으로 한 이동 호스트 프로토콜 설계", 한국정보과학회 학술발표논문집 (봄) 1997. 설계", 정보과학회 충청지부 학술발표대회, Nov, 2000.