한국시뮬레이션학회 논문지
Vol. 18, No. 2, pp. 1-8 (2009. 6)

분산 환경에서 이종의 보안시스템 관리를 위한 정책 충돌 모델링

이동영[1] · 서희석[2†] · 김태경[3]

Modeling on Policy Conflict for Managing Heterogeneous Security Systems in Distributed Network Environment

Lee Dong Young · Hee-Suk Seo · Tae-Kyung Kim

ABSTRACT

Enterprise security management system proposed to properly manage heterogeneous security products is the security management infrastructure designed to avoid needless duplications of management tasks and inter-operate those security products effectively. In this paper, we defined the security policies using Z-Notation and the detection algorithm of policy conflict for managing heterogeneous firewall systems. It is designed to help security management build invulnerable security policies that can unify various existing management infrastructures of security policies. Its goal is not only to improve security strength and increase the management efficiency and convenience but also to make it possible to include different security management infrastructures while building security policies. With the process of the detection and resolution for policy conflict, it is possible to integrate heterogeneous security policies and guarantee the integrity of them by avoiding conflicts or duplications among security policies. And further, it provides convenience to manage many security products existing in large networks.

Key words : Integrated Security Management, Policy Conflict, Security Model

요 약

이종의 분산환경에서 다양한 보안시스템에 대한 효율적인 보안 관리를 위해서 관리자는 보안 시스템들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야하며, 개방형 네트워크 환경의 경우 새로운 보안시스템이 추가되면 새로운 보안 정책과 기술을 적용해야 한다. 이는 전산망 운영 기관의 보안 관리 비용을 가중시키며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오히려 보안 문제를 야기시키는 역기능을 초래할 수 있다. 그리고, 보안 제품의 개발과 공급이 다수의 공급자에 의해서 공급되므로 서로 상이한 특성을 갖는 보안 시스템들로 구성된 보안 관리 구조의 효율적인 운용과 유지에 상당한 어려움이 있다. 이에 본 논문에서는 이종의 보안시스템을 관리하는 통합보안시스템의 보안정책을 Z-Notation을 통해서 정의하고 통합관리에서 발생되는 정책 충돌 문제를 대표적인 보안시스템인 침입차단시스템(Firewall : 방화벽)을 대상으로 모델링하고 이를 해결하는 알고리즘을 제시하고자 한다.

주요어 : 통합보안관리, 정책 충돌, 보안모델

2008년 12월 2일 접수, 2009년 5월 7일 채택
[1] 명지전문대 정보통신과
[2] 한국기술교육대학교 인터넷미디어공학부
[3] 서울신학대학교 교양학부
주 저 자 : 이동영
교신저자 : 서희석
E-mail; histone@kut.ac.kr

1. 서 론

최근 네트워크나 시스템에 대한 크래킹(cracking)이나 잘못된 조작 등에 의한 피해 사례는 대표적인 정보 보호 시스템인 침입차단시스템(일명: 방화벽)이 설치된 네트워크 도메인에서도 많이 발생하고 있다. 이는 지금까지 침입차단시스템만으로 자신의 네트워크를 안전하게 관리할 수 있다고 믿고 있는 일부 보안 관리자들을 당혹스럽게 만드는 일임에는 틀림없다. 따라서, 보안 관리자는 자신이 관리하고자 하는 네트워크의 환경과 자료의 중요도에 따라 보안정책을 수립하고 이에 맞는 다양한 보안제품을 설치, 운영하여야 한다.

이종의 분산환경에서 다양한 보안시스템에 대한 효율적인 보안 관리를 위해서 관리자는 보안 시스템들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야하며, 개방형 네트워크 환경의 경우 새로운 보안시스템이 추가되면 새로운 보안 정책과 기술을 적용해야 한다. 이는 전산망 운영 기관의 보안 관리 비용을 가중시키며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오히려 보안 문제를 야기시키는 역기능을 초래할 수 있다. 그리고, 보안 제품의 개발과 공급이 다수의 공급자에 의해서 공급되므로 서로 상이한 특성을 갖는 보안 시스템들로 구성된 보안 관리 구조의 효율적인 운용과 유지에 상당한 어려움이 있다[1-3]. 이에 복잡하고 다양한 방식의 보안관리 및 통신망 관리체계의 집중화, 자동화된 관리체계로의 전환, 그리고 이종간의 보안 시스템들에 대한 통합적인 관리를 위한 정책 관리가 요구되고 있다.

그러나, 이러한 통합보안관리시스템은 다양한 보안 제품군들이 갖고 있는 기능적 공통점을 일반화하여 보안정책에 반영하기 보다는 단순히 UI(User Interface)의 통합만을 제공하여 관리 작업을 한 곳에 집중시켜 오히려 관리자의 부담을 가중시키고 있다. 그리고, 보안 제품군들이 갖고 있는 특정 파라미터를 통한 보안정책 설정이나, 통합관리를 위한 보안 제품간의 연동성에 보다 중점을 둠으로써 보안관리를 보다 복잡하게 만드는 경향이 있다. 이와 같은 통합보안관리시스템이 보다 광범위한 네트워크에 적용될 경우, 보안관리의 복잡도를 증가시킴으로써 관리의 어려움은 더욱 심각해 질 것이다.

특히, 대규모 네트워크에서 이종의 보안 제품들을 관리하는 환경에서는 해당 관리대상시스템들에 대한 정책 간의 충돌 및 중복설정은 네트워크 전반에 대한 보안성에 심각한 영향을 미칠 수 있다. 이에 본 논문에서는 이종의 보안시스템을 관리하는 통합보안시스템의 보안정책을 Z-Notation을 통해서 정의하고 통합관리에서 발생되는 정책 충돌 문제를 대표적인 보안시스템인 침입차단시스템(Firewall : 방화벽)을 대상으로 모델링하고 이를 해결하는 알고리즘을 제시하고자 한다.

본 논문의 구성은 2장에서는 정책 적용을 위한 정책모델과 Moffett의 정책 충돌의 분류에 대해서 살펴보고, 3장에서는 정책기반의 통합보안시스템에 대한 정책 정의와 정책 충돌의 검출과 해결 알고리즘에 대해서 언급하고 마지막으로 4장에서는 결론 및 향후 계획에 대해서 기술하였다.

2. 관련 연구

2.1 정책모델

현재 네트워크 보안관리구조는 침입탐지시스템, 침입차단시스템, 가상사설망 등과 같은 공격의 근원지를 찾아내고 차단하는 기능을 가진 하부조직에 속하는 보안 시스템들을 중앙 집중적으로 통합 관리하는 방향으로 지속적인 연구가 진행되고 있다[7-9].

최근 연구활동으로는 통합 보안정책의 동적관리를 위한 MSME(Multidimensional Security Policy Management for Dynamic Coalitions)가 있다. MSME 시스템은 SAL(Security Abstraction Layer)에 기반하고 있으며, MSME SAL은 ISO 보안구조(ISO 7498-2)의 일부분과 ISO 7498-2에서 정의되지 않은 서비스와 메커니즘을 추가적으로 포함하고 있다. 추가적으로 포함된 것으로는 coalition members와 steganography mechanism 사이의 통신서비스를 들 수 있다.

SAL에서 정책 관리자들은 특정한 보안을 독립적으로 이행함으로써, 상위레벨 보안서비스에 관하여 판단과 계획을 세울 수 있다.

그림 1은 MSME에 대한 추상적인 개념을 도시한 것이

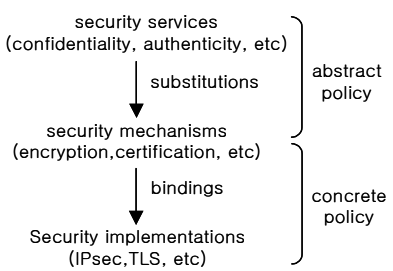

그림 1. Abstraction Levels

다. MSME 시스템은 어떠한 보안 메커니즘으로 보안 서비스를 제공할 것인지를 결정하고, 결정된 보안 메커니즘의 구현 기술을 결정하여 동적으로 연결 구성함으로써 보안정책을 동적으로 구성 관리할 수 있다. 예를 들어, 그림 1에서 MSME 시스템이 특정 네트워크에 기밀성 서비스를 제공하기위해 암호화 메커니즘을 사용할 것을 결정하였다면, IPsec의 DES 또는 Triple-DES 암호화 알고리즘, TLS의 Triple-DES 또는 RSA 등과 같은 구현 기술을 통하여 기밀성 서비스를 제공할 수 있다. 그러나, MSME에서 제안된 이론이 실용화 되기 위해서는 보안 서비스를 제공하기 위해 설정된 보안 정책들이 보안 메커니즘을 정확히 받아들이는지에 대한 모니터링 기능과 정책 적용의 자동화 기능이 필요하다[5].

2.2 정책충돌의 분류

또한 이러한 정책 모델을 기반으로 추상화된 보안정책을 에이전트가 관리대상 보안시스템에 적용시키는 Low Level단위의 정책으로 변경하는 과정에서 정책충돌에 대한 검증과정이 요구된다. Moffett가 분류한 정책 충돌은 크게 형식의 충돌과 목표의 충돌로 구분할 수 있으며 세부 내용은 그림 2와 같다[6].

- **형식의 상반된 정책의 충돌**

의무정책 또는 권한정책과 같은 정책의 허용과 금지가 동일한 주체, 행위, 그리고 대상에 대해서 동시에 적용될 경우에 발생하는 정책 충돌이다. 그림 3은 형식에 대한 상반된 정책의 충돌을 나타낸 것이다.

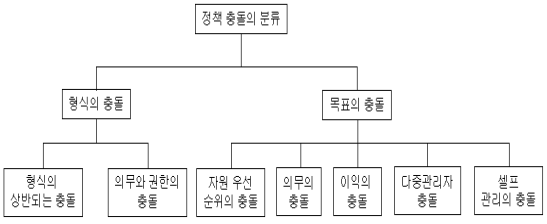

그림 2. Moffett의 정책 충돌의 분류

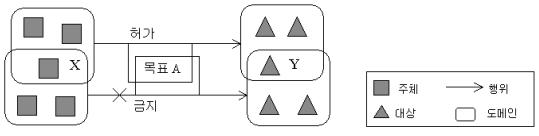

그림 3. 형식에 대한 상반된 정책의 충돌

- **정책의 위임과 권한의 충돌**

정책의 위임과 권한의 충돌은 허용 위임 정책과 금지 권한 정책이 동일한 주체, 행위 그리고 대상에 적용됨으로써 겹침이 발생한 경우에 생성되는 정책 충돌이다. 그림 4는 정책의 위임과 권한의 충돌을 나타낸 것이다.

- **자원에 대한 우선순위 충돌**

자원을 제공하는 대상의 능력보다 많은 양의 자원을 주체가 요구하는 경우에 발생하는 정책충돌이다. 예를 들면, 사용 가능한 예산액에 비해서 많은 금액을 요하거나, 사용자의 등급이나 능력에 따라 설정된 컴퓨터의 자원을 초과해서 자원의 사용을 요구하는 경우가 이에 해당한다. 이는 행위와 정책의 대상의 범위가 겹침이 발생한다.

- **의무의 충돌**

두 개의 허용 인증 정책이 주체-주체 혹은 대상-대상간에 겹침 관계에 있을 때 발생하는 정책 충돌을 말한다. 행위의 겹침 관계가 발생하지 않는다. 이를 의무의 충돌이라고 한다. 예를 들면, 동일한 주체 X가 대상Y에 대해서 인증을 요구(Req_Auth)하고 이를 인증하는 경우를 주체 X와 대상 Y에 대한 의무의 정책 충돌이 발생한다.

- **이익의 충돌**

주체 X의 권한이 겹침 관계에 있고, 대상 A와 B에 대해서 상호 이익이 상반되는 권한의 정책을 설정하였을 때 발생하는 정책 충돌을 말한다. 예를 들면, 은행(주체 X)에서 서로 다른 고객들(대상 A와 B)에게 회사의 인수와 투자를 각 각 조언하는 경우 대상 A와 대상 B간에는 상호 반하는 이익의 충돌이 발생할 수 있다.

- **다중 관리자에 의한 정책 충돌**

다중의 관리 주체들이 동일한 대상 Y에 대해서 두 정책이 겹침의 관계에 있을 때 발생하는 정책 충돌을 말한다. 예를 들면, 동일한 대상 Y에 대해서 서로 다른 관리자가 동시에 서비스의 요구와 관계유지의 정책을 요구하였을 때 이 두 정책은 겹침의 관계가 되면 정책의 충돌이 발

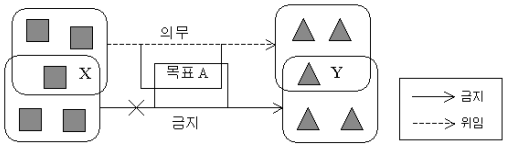

그림 4. 정책의 위임과 권한의 충돌

생한다. 그림 5은 다중 관리자에 의한 정책 충돌을 나타낸 것이다.

- **셀프 관리에 의한 정책 충돌**

셀프 관리에 의한 정책 충돌은 주체와 대상이 같은 경우에 발생하는 정책 충돌을 말한다. 예를 들면, A라는 관리자가 자금을 담당하는 관리자이면서 자금의 집행에 대해서 감사를 하는 경우가 이에 해당 될 수 있다.

3. 통합보안시스템 보안정책 모델링

3.1 통합보안시스템의 구조

정책기반의 통합보안관리시스템(PB-ISMS : PB-ISMS : Policy Based-Integrated Security Management System)은 이종의 분산환경에서 다양한 보안 관련 시스템을 중앙관리 즉, 정책을 설정하고 모니터링하는 기능을 수행하며, 보안 관리자에게 네트워크 보안 상태의 전체적인 뷰(View)를 제공한다.

또한, 보안 정책에 대해서 전문적인 지식이 부족한 사용자의 추상적인 정책 설정 요구에 대해서 보안관리서버에서 이를 수행하며, 추가로 보안시스템에 대해서 통합관리를 하고자 할 경우에는 기존의 보안 시스템들의 재구현이나 수정이 필요 없이 그에 해당하는 에이전트[12]를 추가함으로써 이들을 수용할 수 있는 확장성을 갖고 있다. 그림 6은 정책기반의 통합보안관리시스템의 개념적인 구조를 나타낸 것이다[5-6].

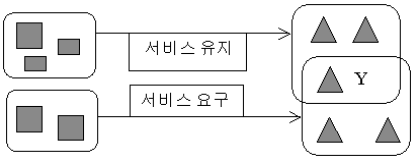

그림 5. 다중 관리자에 의한 정책 충돌

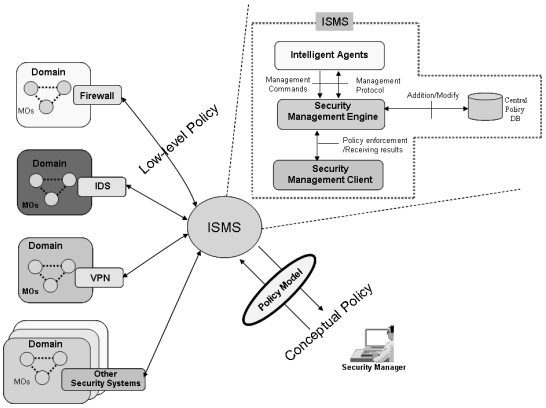

그림 6. 정책기반의 통합보안시스템의 구조

3.2 정책의 라이프사이클

정책의 라이프사이클은 다양한 상태의 변화로 전이된다. PB-ISMS의 정책의 라이프사이클의 동작을 살펴보면, 그럼 7에서 p1은 개념적이고 추상적인 정책을 정의하고, 이들에 대한 정제를 거쳐서 정책을 적용할 수 있는 활동상태인 p2로 전이된다. 그리고 활동 상태의 정책에 따라서 정책의 적용 상태 p3와 정책의 모니터링 p4 상태로 전이된다. 이후 정책의 모니터링 p4 상태에서 정책의 변경사항이 발생할 경우 이를 정책의 적용 p3상태로 이동하고 그와 반대로 정책의 적용 p3상태에서 새로운 정책의 모니터링 p4상태의 요구 사항을 변경될 수 있다. 이를 설정된 정책의 기간이 만료되면 정책 폐기 p5상태가 된다. 그림 7은 PB-ISMS의 정책의 라이프사이클을 표현한 것이다[4].

3.3 Z를 이용한 정책의 표현

추상적이고 개념적인 정책에 대한 정책을 분류·정의하고 이를 템플릿으로 표현한 후 이를 형식화 언어인 Z-Notation을 통해서 정책을 표현하였다. Z-Notation의 특징을 살펴보면, Z-Notation은 자연어를 사용한다. 일반적으로 제기된 문제에 대해서 해결책을 발견하고, 정의에 맞는 설계가 되었는지를 증명하기 위해서 집합이론과 수학적 논리를 사용한다. 그리고 Z-Notation은 정제의 특징을 갖고 있다. 설계모델의 구성과 요구된 행위를 정의하기 위해서 간단한 수학적 데이터 타입을 사용해서 시스템을 설계한다. 그리고 이들에 대한 정제과정을 통해서 설계의 적절성을 파악하고, 시스템 구현을 용이하게 할 수 있으며, 다른 형식화 언어에 비해서 실행코드에 가깝게

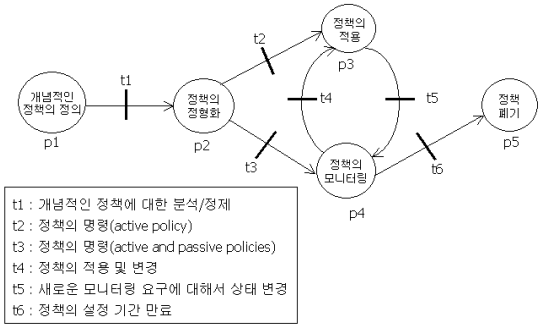

그림 7. PB-ISMS의 정책 라이프사이클

표현할 수 있다[10-14]. 그림 8은 Z의 기본 스키마 구조를 나타낸 것이다.

그림 8에서 보는 바와 같이 Z-Notation은 표현하고자 하는 대상과 이들의 특징을 선언부-술어부의 관계로 표현할 수 있다. si : Ti(i = 1 . . n)는 선언부를 나타내고, 제안된 술어 스키마 fi(i = 1 . . m)의 논리곱을 나타낸 것이다. si(i = 1 . . n)의 집합을 변수라고 하며, Ti(i = 1 . . n)은 타입을 의미한다. 그리고 각 각의 fi는 선언부의 순서에 해당하는 계산식을 나타낸 것이다.

(1) 도메인 정의

관리 도메인은 관리의 목적으로 정확히 함께 그룹화된 관리 대상의 집합체이다. 즉, 도메인은 그것의 멤버 관리 대상들에 대한 참조 포인터들의 리스트를 유지하는 관리 영역이다. (그림 4.12)와 같이 Dom_A가 관리 객체들에 대한 참조를 가진다면 그 객체들은 Dom_A의 직접적인 멤버라고 말하며, Dom_A는 관리 객체들 즉, M1, SP1, SP2, Dom_B, 그리고 Dom_C 들의 부모라고 말한다. Dom_A의 관리 객체가 되는 Dom_B와 Dom_C를 Dom_A의 서브도메인이라고 한다. 서브도메인의 멤버들은 부모 도메인의 간접적 멤버들이다. 이를 적용한 예를 살펴보면, 그림 9는 Dom_PB-ISMS_Objects의 스키마 구조를 나타낸 것이다.

(2) 접근제어 정책

PB-ISMS의 관리자는 접근제어 정책을 통해서 하위의 관리자나 정책 적용 대상 시스템에 대한 자원이나 서비스 제공 여부에 대한 접근을 제어할 수 있다. 접근제어 정책 기능은 PB-ISMS의 주요한 정책 중의 하나다. 접근제어 정책은 앞서 정의된 도메인에서 정책을 관리하는 관리자 객체와 해당 정책의 대상이 되는 목표 객체, 그리고 정책의 적용 대상에게 적용할 정책의 행위객체로 구성할 수 있다. 그림 10은 접근제어 정책 AccRule_Objects스키마를 나타낸 것이다.

(3) 역할 정책

PB-ISMS는 보안관리자의 역할에 대한 정책은 우선 보안관리자들의 등급을 분류하고, 이들 등급에 따른 역할을 구별한다. 역할 정책의 경우, 목표 객체들에 대한 인증의 권한을 갖게되는 것을 의미하다. 따라서 보안관리자는 한 기구에서 하나 이상의 역할 혹은 권한을 갖는 경우도 있다. 그림 11은 Role_PB-ISMS_Objects의 스키마를 나타낸 것이다.

(4) 정책위임

보안관리자의 역할에 대한 정책은 우선 보안관리자들의 등급을 분류하고, 이들 등급에 따른 역할을 구별한다. 역할 정책의 경우, 목표 객체들에게 대한 인증의 권한을 갖게되는 것을 의미하다. 따라서 상위의 관리자의 역할을 하위 관리자에게 권한을 부여/위임 할 수도 있다. 그림 12는 최상위 보안관리자인 M1이 일반보안관리자 M2에게 네트워크관리자인 M3에 대한 인증 권한 Auth_Y를 위임/부여하는 것을 나타낸 것이다.

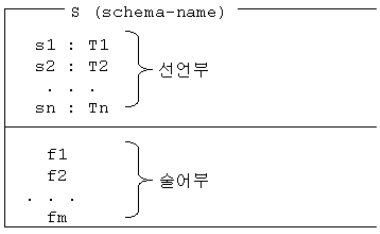

그림 8. Z의 기본 스키마 구조

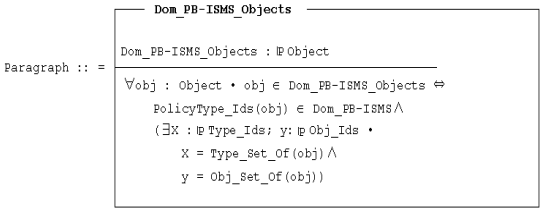

그림 9. Dom_PB-ISMS_Objects 스키마

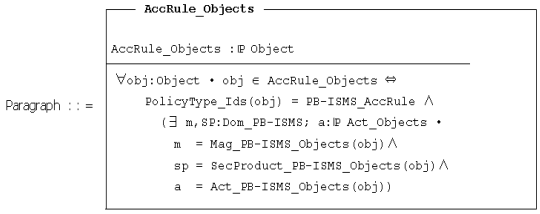

그림 10. AccRule_Objects 스키마

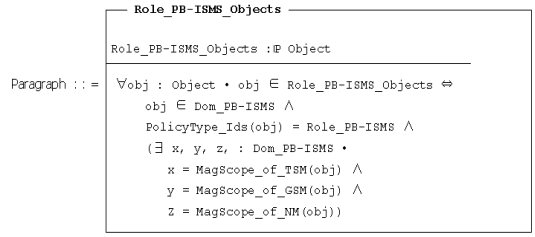

그림 11. Role_PB-ISMS_Objects 스키마

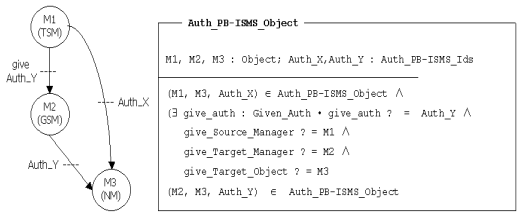

그림 12. Auth_PB-ISMS_Object의 정책 적용 예

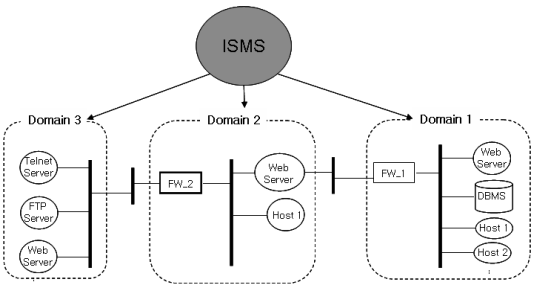

그림 13. 모델링 환경

3.4 정책충돌의 모델링과 해결 알고리즘

본 논문에서는 다중의 보안시스템을 관리하는 통합보안시스템에서 가장 대표적인 네트워크 보안시스템인 침입차단시스템(방화벽 : Firewall)에 정책 충돌을 정의하고 이를 해결하는 알고리즘을 제시하고자 한다. 또한, 본 논문에서 언급하고 사용하는 방화벽은 패킷필터링 방화벽을 사용하며 구성된 환경은 그림 13과 같다.

(1) 중복정책 및 상반되는 정책의 충돌

PB-ISMS의 관리자가 FW1(Firewall 1)에 대해서 Domain 2에 존재하는 Telnet Server에 대해서 이미 설정되어 있는 정책의 중복과 동일한 정책을 설정하거나 상반된 정책(기존 정책 P(old) = > Permit을 새로운 정책 P(new) => Deny로 설정)의 경우 정책의 충돌이 발생한다. P(old) = {Src_e, Dst_e, Rule_e}와 P(new) = {Src_n, Dst_n, Rule_n}에 대해서 Src_e == Src_n, Dst_e == Dst_n, Rule_e ≠ Rule_n인 경우 관리자(Owner_e와 Owner_n)의 등급과 역할(Role)에 의해서 정책 수정여부를 결정한다. 그림 14는 동일정책의 중복과 상반된 정책 충돌 검출 및 해결 알고리즘을 나타낸 것이다.

(2) 포함관계 및 논리적 위배에 의한 정책 충돌

기존의 정책에 관여된 객체와 새로이 추가 요구된 정책에 관여된 객체가 서로 포함관계를 갖는 경우, 이를 포함 관계의 정책에 의한 정책 충돌이라고 정의한다. 이 경우 한 정책의 영향 범위가 다른 정책을 포함하여 포함되는 정책의 효력을 상실하게 되므로 포함되는 쪽의 정책은 그 존재 의미가 없어지므로 불필요한 정책으로 남게 된다.

또한, ISMS에서는 관리대상 내부 도메인(Domain 1, Domain 2, Domain 3)에 있는 시스템들에 대해서 Telnet 서비스를 확인하는 경우 FW_1과 FW_2의 논리적인 불일치로 인한 정책의 충돌이 발생할 수 있다. 표 1은 ISMS

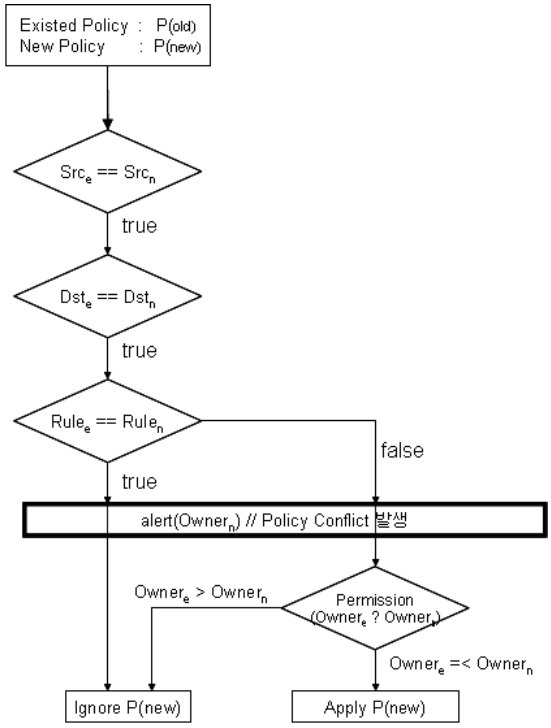

그림 14. 중복 및 상반된 정책 검출알고리즘

표 1. ISMS 정책 테이블

No	FW	Direction	Src	Dst	Rule	Policy Conflict
1	FW_1	Outbound	Domain1 Host 1	Domain2	Deny	-
2	FW_1	Outbound	Domain1 Host 1	Domain2 Host 1	Permit	Collision
3	FW_1	Inbound	Domain2 Host 1	Domain1 Web서버	Permit	-
4	FW_1	Inbound	Domain2	Domain1	Deny	Collision
5	FW_1	Inbound	Domain1 Host 1	Domain1	Permit	-
6	FW_2	Outbound	Domain1 Host 2	Domain3 Telnet	Permit	Collision

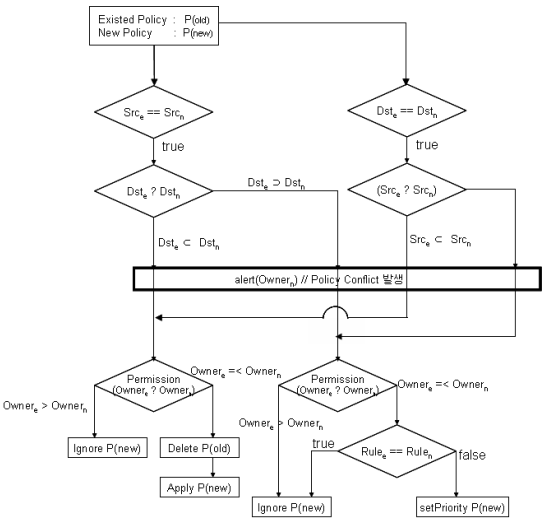

그림 15. 포함관계 및 논리적 정책 충돌 검출알고리즘

의 정책 테이블을 나타낸 것이다.

이러한 포함관계 및 논리적 정책 충돌에 대한 검출 및 해결 알고리즘은 그림 15와 같다.

4. 결론 및 향후 연구계획

본 논문에서는 다중의 통합보안시스템을 관리하기 위한 정책 기반의 통합보안시스템에 대한 정책을 Z-Notation을 통해서 정의하였다. Z-Notation은 우선 자연어를 사용하며, 일반적으로 제기된 문제에 대해서 해결책을 발견하고, 규정에 맞는 설계가 되었는지를 증명하기 위해서 수학적 방법을 사용한다. 현실 세계에서는 객체들에 대한 수학적 요소를 연결시키기 위해서 자연어를 사용한다. 이는 변수들에 대한 적절한 네이밍(naming)과 주석을 통해서 실현할 수 있으며, 정확하게 정의된 규정은 사용자로 명확한 의미를 해설할 수 있게 도와준다.

또한, Z-Notation은 정제의 특징을 갖고 있다. 설계모델의 구성과 요구된 행위를 인지하기 위해서 간단한 수학적 데이터 타입을 사용해서 시스템을 개발한다. 이들에 대한 정제 과정을 통해서 설계의 적절성을 파악하고, 시스템 구현을 용이하게 할 수 있다. 마지막으로 침입차단시스템을 대상으로 통합보안관리 과정에서 발생할 수 있는 정책 충돌을 검출하고 해결하는 알고리즘을 제시하였다.

본 연구는 보안정책 모델링과 정책 충돌에 대한 개념과 침입차단시스템으로 구성된 소규모 네트워크에서 정책 충돌을 정의하고 검출하는 과정을 언급하였다. 따라서 대규모의 Real환경에서 다른 보안시스템과의 연동에서 발생하는 다양한 정책 충돌에 대한 보다 심층적인 연구가 필요하다고 사료됩니다.

참 고 문 헌

1. J. Zao, L. Sanchez, et el, “Domain based Internet security policy management,” DARPA Information Survivability Conference and Exposition, 2000, DISCEX ’00, Proceedings, Vol.1, pp. 41-53, Jan., 1999.
2. L. Lewis, “Implementing policy in enterprise networks,” IEEE Communications Magazine, Vol. 34, Iss.1, pp. 50-55, Jan., 1996.
3. D. Y. Lee, D. S. Kim, K. H. Pang, H. S. Kim, T. M. Chung, “A Design of Scalable SNMP Agent for Managing Heterogeneous Security Systems”, NOMS (Network Operations and Management Symposium)2000, pp. 293-294. April 2000.
4. 이동영, 김동수, 정태명, “이종의 보안시스템 관리를 위한 정책 기반의 통합보안관리시스템의 계층적 정책모델에 관한 연구”, 한국정보처리학회논문지 C 제8-C권 Vol. 5호, 2001년. 10월
5. G. Patz, M. Condell, et el, “Multidimensional security policy management for dynamic coalitions,” DARPA Information Survivability Conference & Exposition Ⅱ, 2001, DISCEX ’01. Proceedings, Vol. 2, pp. 41-54, Feb., 2001.
6. J. Moffett, Morris S. Sloman, “Policy Conflict Analysis in Distributed System Management”, Journal of Organizational Computing, Vol. 4, No. 1, pp. 1-22, Ablex Publishing, 1994.3.
7. D. Schnackengerg, H. Holliday, et el, “Cooperative Intrusion Traceback and Response Architecture (CITRA),” DARPA Information Survivability Conference & Exposition Ⅱ, 2001. DISCEX ’01, Proceedings, Vol. 1, pp. 56-68, Jan., 2001.
8. R. Barruffi, M. Milano, et el, “Planning for security management,” IEEE Intelligent Systems [see also IEEE Expert], Vol. 16, Iss.1, pp. 74-80, Feb., 2001.
9. G. Patz, M. Condell, et el, “Multidimensional security policy management for dynamic coalitions,” DARPA Information Survivability Conference & Exposition Ⅱ, 2001, DISCEX ’01. Proceedings, Vol. 2, pp. 41-54, Feb., 2001.
10. Dong-Young Lee, “A Study on the Centralized Databas of the Multi-agents Based Integrated Security Management System for Managing Heterogeneous Firewalls”, KES2005,

Lecture Notes in Computer Science (LNAI3682), Springer-Verlag, 2005. 9. pp. 1036-1042.
11. Gary N.Stone, Bert Lundy, and Geoffrey G. Xie, “Network Policy Languages: A Survey and a New Approach”, IEEE Network January/February, pp. 10-21, 2001.
12. Spivey, J. M., ‘The Z Notation - A Reference Manual’, Prentice-Hall, second edition, 1992.
13. Jim Woodcock, Jim Davies, ‘Using Z : Specification, Refinement, and Proof’, Published by Prentice-Hall, 1996.
14. Nicole Dunlop, Jadwiga Indulska, Kerry Raymond “Dynamic Conflict Detection in Policy-Based Management Systems” in Sixth International Enterprixe Distributed Computing Conference, 2002.

이 동 영 (dylee@mail.mjc.ac.kr)

1993 동아대학교 전자공학과(학사)
1998 성균관대학교 정보공학(석사)
1993～1997 기아자동차 중앙기술연구소 연구원
2002 성균관대학교 컴퓨터공학(박사)
2003～현재 명지전문대학 정보통신과 교수

관심분야 : 네트워크보안, 홈 네트워크, USN

서 희 석 (histone@kut.ac.kr)

2000 성균관대학교 산업공학과(공학사)
2002 성균관대학교 전기전자및컴퓨터공학과(공학석사)
2004～2005 (주)정보감리평가원 선임연구원
2005 성균관대학교 전기전자및컴퓨터공학과(공학박사)
2005～현재 한국기술교육대학교 인터넷미디어공학부 정보보호전공 교수

관심분야 : 네트워크보안, 보안 시뮬레이션, USN

김 태 경 (tkkim@stu.ac.kr)

1997 단국대학교 수학교육과(이학사)
2001 성균관대학교 정보통신공학과(공학석사)
2005 성균관대학교 전기전자및컴퓨터공학과(공학박사)
2006～2008 서일대학 정보기술계열 정보전자전공 교수
2008～현재 서울신학대학교 교양학부 교수

관심분야 : 네트워크보안, 그리드 네트워크, USN