보안정책 설계 및 검증을 위한 프레임 설계†

이용석*, 최웅철*, 정광수**, 남택용+, 오승희+

*광운대학교 컴퓨터과학과

**광운대학교 전자통신공학과

+한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀

Frame Design for Security Policy Design and Verification

YongSuk Lee*, WoongChul Choi*, KwangSue Chung, Taek Yong Nam, Seung-Hee Oh

*Department of Computer Science, KwangWoon University

**Department of Electronics Engineering, KwangWoon University

+Information Security Research Division, ETRI

요 약

네트워크에서 보안 기능을 전개하는데 있어 정책 기반 전개 방법이 널리 사용 되고 있다. 본 논문에서는 정책 기반 보안 기능 전개에 있어 정책을 설정하고 검증하기 위한 프레임을 제시한다. 정책 기반 기능 전개에 있어 중요하고도 어려운 문제는 설정한 정책의 정확성(correctness)과 완전성(completeness)을 검증하는 것이지만 이에 관한 기존의 방법은 주로 경험이나 혹은 감시에 의한 끊임없는 정책 갱신이다. 본 연구에서는 기존의 제안된 여러 보안 모델들을 검토해보고 이 모델들로부터 공통적으로 적용할 수 있는 정책의 정확성과 완전성을 위한 제어 프레임을 설계한다.

I. 서론

네트워크 보안은 보안 정책을 중심으로 한 끊임없는 프로세스로 정의할 수 있다[1][2]. 끊임없는 보안정책 프로세스는 보안 대책을 계속하여 갱신하고 재점검한다는 점에서 보안에 있어 효과적이라 할 수 있다. 보안 정책을 실행에 옮기기 전에 필요한 것은 보안 모델을 선택하는 것이다. 보안 모델은 사용자의 네트워크 환경에 고유한 보안 정책을 개발하는 프레임이다. 보안모델은 단순히 점검사항목록이 아니라 네트워크가 속한 기관의 보안에 관한 원칙이다. 즉 효과적인 보안 정책을 설정하고 실행하기 위하여 보안의 대상을 정하고 또 보안 기능을 실행하는 방법 등을 결정하여야 한다. 이러한 일련의 과정들을 체계적으로 수행하기 위하여 보안 모델은 필수적이며 또한 그 영향도 크다 하겠다. 보안 기능 전개를 위한 보안 정책은 궁극적으로 보안 목적에 맞도록 정확(correctness)하여야 하며 완전(completeness)하여야 한다. 이런 관점에서 제안된 보안모델들을 검토함으로써 정확성과 완전성을 어떻게 체계적으로 검증할 수 있는지에 대한 해결책을 구하고자 한다. 즉 본 논문에서는 제안되어진 보안 모델들을 검토하여 체계적으로 보안 정책을 설정하고 검증할 수 있는 프레임을 설계한다. 이 프레임은 현재 진행 중인 프로젝트에 대하여 사용되고 있다.

† 이 연구는 "MIC 고성능 네트워크 정보보호시스템 개발"사업의 위탁과제 연구결과임

II. 보안모델

네트워크 보안과 관련되어 제안된 보안 모델들 중 널리 알려지거나 사용되고 있는 모델들인 NSSC, CISCO SAFE, CERT/CC OCTAVE, RFC 2196, ISO 17799에 대하여 검토한다.

1. NSSC(National Security to Secure Cyberspace)

2002년 9월18일 미 정부는 일반인들의 검토를 위하여 NSSC[5]를 공개했다. NSSC는 개인이나 기관들의 정보자산을 안전하게 하기 위한 조치를 취하자는 것이다. 이 문서 안에는 가상공간상의 보안을 위한 일련의 권고사항들이 담겨 있다. NSSC는 법으로 강제되는 것은 아니지만 상당한 자발적 의무의 필요성을 강조한다. NSSC의 주요 목적중의 하나는 모두의 참여를 통해 개인과 공공기관간의 유대관계를 돈독히 하는 것이다. NSSC는 위협능력에 초점을 맞추기 보다는 취약성에 기반을 둔 접근 방법을 취한다. NSSC에서 사용된 논리는 위협을 수치로 표현할 수 없기 때문에 최악의 시나리오를 대상으로 한다. NSSC는 국가 전략 개발에 있어 새로운 철학이며, 백악관은 그것을 환경이 변함에 따라 바뀌고 진화해 나가는 살아있는 문서로서 다루고 있다. 부시 대통령은 2003년 연방컴퓨터 시스템 보안을 위하여 45억 달러를 의회에 요청해놓고 있다.

NSSC에는 다음의 다섯 개의 기관 레벨이 있다.

- 레벨 1 : 가정 사용자와 소규모 사업체
- 레벨 2 : 대형 사업체
- 레벨 3 : 경제의 주요 부분
- 레벨 4 : 국가적 우선 순위들
- 레벨 5 : 전 세계의 문제점들

다음의 권고 사항들은 상당히 자발적이기는 하지만 NSSC의 강력한 권고사항이다.

● 레벨 1: 가정 사용자와 소규모 사업체

비록 각 개인의 컴퓨터는 중요하지 않다고 할지라도 모든 가정과 소규모 사업체들의 컴퓨팅 능력을 합친 것은 매우 중요하다. 재택근무자 또한 이 그룹에 속하게 되고 그들이 고용주이거나 고용자이거나 간에 주의가 요망된다. 원격으로 접속할 경우에 특별히 주의가 요구된다. 가정 사용자와 소규모 사업체의 사용자들의 보안문제를 간단하게 하기 위해서 NSSC는 서비스와 소프트웨어 제공자들이 자동 업데이트 기능을 제공하도록 하며 이를 통해 능숙하지 못한 컴퓨터 사용자도 안전해질 수 있다.

● 레벨 2: 대형 사업체

NSSC는 메인 프레임 컴퓨터를 갖고 있는 기관을 대형 사업체로 분류(정의)했다. NSSC가 그러한 기관에 대해서 권고한 사항들은 다음과 같다.

1. 기관 내에서 보안 책임의 정도를 높여라.
2. 필요한 경우 적절한 곳에 가상공간 상의 보안을 위한 보안 위원회를 두어라.
3. 다음과 같은 곳에 상당한 주의를 기울여라. - 인증, 구성관리, 교육, 사고 대응, 네트워크와 네트워크 관리와 관련된 기구 등
4. 외부 네트워크와 연결된 네트워크, 메인 프레임 보안, 인스턴트 메시징 등의 위험성을 강조하여라.

● 레벨 3: 경제의 주요 부분

NSSC는 동일 산업 분야 내의 기관들에 초점을 맞추고자 하는데 그 이유는 그들 기관들이 동일한 비즈니스 모델과 IT 인프라를 갖고 있기 때문이다. 또한 그들은 동일한 수요층에 대하여 경쟁하고 동일한 규정을 받기 때문이다. 10개의 주요 산업 분야는 이미 계획서를 이미 개발해 놓은 상태이다.

● 레벨 4: 국가적 우선순위들

이 분야는 NSSC를 구성하는 일반적인 안내이다. NSSC 문서는 공유 시스템을 안전하게 하는 세 가지 주요 기초들에 대해서 매우 자세하게 기술하고 있으며 공적, 사적 협력을 매우 강력히 권장한다는 점을 다루고 있다.

● 레벨 5: 전 세계의 문제점들

(i)북미 중심: NSSC는 미국만이 아니라 북미 전체를 위한 것이다. 캐나다와 멕시코는 미국과 인프라를 공유하고 있으며 이 세 개국은 밀접하게 관련이 되어 있다. 석유와 천연가스 파이프 라인 그리고 통신망이 모두 연결되어 있다. 그러한 관점에서 이 삼개국은 경제적 측면에서는 열려 있지만 테러리스트들에게는 닫혀져 있는 아주 똑똑한 국경선을 만들어야만 한다.

사이버 범죄의 처벌: 백악관 행정부는 유럽 연합의 사이버 범죄 조약을 훌륭한 예로 들면서 다른 나라 정부들도 그 조약을 채택하기를 바라며 최소한 그 나라의 컴퓨터 범죄들을 처벌하기를 바란다.

(ii)인증과 정보공유: 이것은 국제 협력이 필수적인 또 다른 분야이다.

전체적으로 NSSC는 정보보안이라는 세계에서 진보된 것을 나타내고 있다. 그것은 모든 유형의 가상공간 사용자들에 대한 중요한 보안 정보를 제공할 뿐만 아니라 각 개인이나 기관들로 하여금 사이버 공간상의 보안에 있어 중요한 역할을 한다는 것을 깨닫게 한다.

미국 보안전략의 위치를 다음 그림 1 에서 확인할 수 있다.

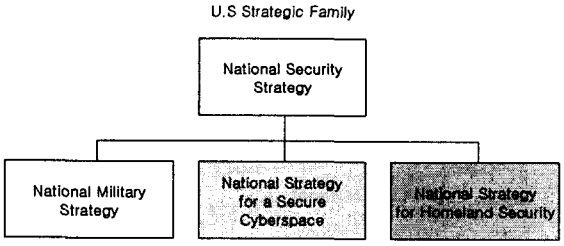

그림 1. 미국 전략 계보

2. SAFE

SAFE[1]는 오늘날 기업체 네트워크의 기능적인 요구사항들을 가능한한 가깝게 애뮬레이트한다. 구현결정은 필요한 네트워크 기능에 따라 달라지지만 다음과 같은 설계 목적들은 의사결정 과정에 대한 가이드라인을 제시한다. 나열된 순서는 우선순위에 따른다.

- 정책에 기반한 보안 및 공격 완화
- 인프라스트럭쳐 전반에 걸친 보안 구현
- 보안관리와 보고
- 중요 네트워크 자원 접근에 대한 사용자 및 관리자의 인증 및 허가
- 중요 자원과 서브넷에 대한 침입탐지
- 네트워크 응용에 대한 지원

무엇보다도 우선 SAFE는 보안 아키텍쳐이다. 그것은 반드시 성공적인 공격으로부터 네트워크 자원을 보호하여야 한다 . SAFE는 또한 신축성이 있어야 하며 기능 확장이 가능해야 한다.

네트워크 설계 과정 중 많은 부분에서 통합된 기능을 가진 네트워크 장치와 특정 기능만을 가진 장비 사이에서 선택을 해야만 한다. 통합된 기능을 가진 장치는 기존의 장치에 설치할 수 있기 때문에 흔히 선택된다. 반면 특정 기능을 가진 장비는 필요한 기능이 아주 특정적이거나 혹은 성능 요구 사항이 특수한 하드웨어를 필요로 할 때에 사용된다. 대부분의 중요한 보안 기능들은 점점 전용 장비로 옮겨가는데 그것은 성능 요구사항 때문이다.

SAFE 아키텍쳐는 모듈러 접근 방식을 사용하는데 그것은 두 가지 장점이 있다. 첫째, 그것은 서로 다양한 네트워크 기능 블록간의 보안 관계를 강조한다. 둘째, 그것은 설계자가 보안 기능을 모듈을 기본으로 하여 구현하고 평가할 수 있게 한다.

SAFE 청사진(SAFE Blueprint)은 보안 청사진을 제공한다. SAFE에서 정의된 계층들은 다음과 같다.

· 인프라스트럭쳐 계층(Infrastructure layer): 라우터, 스위치, 방화벽, 침입탐지 시스템등과 같은 플랫폼에서 제공되는 지능적이며 확장 가능한 보안 서비스들.

· 적용 계층(Appliances layer): 중요 보안 기능들을 모바일 핸드헬드 장치와 원격 PC 클라이언트들에게 적용한 것.

· 서비스 제어 계층: 보안 솔루션들이 서로 밀접하게 동작하도록 하는 보안 프로토콜들과 API들.

· 응용 계층(Applications layer): 중요한 e-비즈니스 응용들의 무결성을 보장하는 호스트 및 응용을 기반으로 하는 보안 요소들

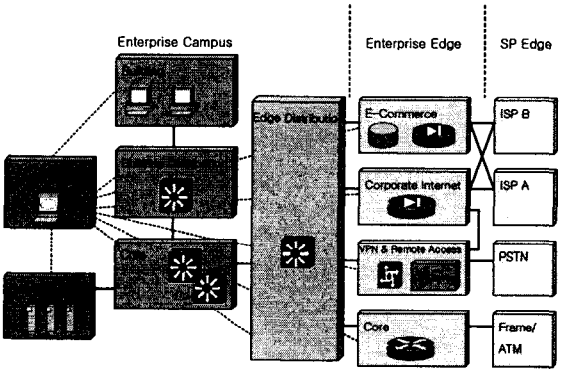

그림 2. SAFE 블럭도

대형 사업체에서 일관성 있고 신속한 보안 기능을 전개할 수 있도록 하게 하기 위하여 SAFE는 각 네트워크 영역에 고유한 요구사항들을 만족하는 모듈들로 구성된다. SAFE청사진을 채택함으로서 보안 관리자들은 새로운 서비스가 네트워크에 추가될 때마다 보안 아키텍쳐 전체를 다시 설계해야 하는 필요성이 없어지게 된다. 모듈러된 템플릿을 사용함으로서 필요한 서비스를 추가할 때마다 그 서비스를 안전하게 하는 것과 전체 보안 아키텍쳐에 통합하는 것이 훨씬 쉽고 비용은 절감하게 된다. SAFE 청사진에 아주 특징적인 것 중에 하나는 어떤 보안 해결책이 네트워크의 어떤 부분에 포함되어야 하는지를, 그리고 왜 그러한 해결책이 사용되어야 하는지를 권고한 최초의 산업 청사진이라는 점이다. SAFE 청사진의 각 모듈은 e-비즈니스를 위해서 최적화된 성능을 제공하도록 설계되었으며 동시에 대형 사업체로 하여금 보안과 통합을 유지할 수 있도록 설계되었다.

3. RFC 2196 : 사이트 보안 요람(The Site Security Handbook)

IETF(The Internet Engineering Task Force)는 사이트 보안 정책을 만들기 위한 보안 요람집을 개발했다. 이 요람집은 Site Security Handbook이라고 불리며 RFC 2196[3]이라고도 알려져 있으며 사이트 관리자가 보안 정책들과 절차들을 개발할 수 있도록 그 과정을 상세히 기술하고 있다. Site Security Handbook의 중요한 점 중의 하나는 유연성을 염두에 두고 설계되었다는 것이다. 이 모델은 아주 많이 다른 네트워크 인프라스트럭쳐를 가진 소규모 사업체에서부터 대규모 사업체에 이르기까지 적용할 수 있다. Site Security Handbook은 보안 정책을 개발하는 절차를 다섯 단계로 나누고 있다.

1. 보안 대상체 식별
2. 보안 대상체로부터 보안 대상 결정
3. 어떤 위협들이 존재하는지 결정
4. 비용효율적으로 자산을 보호할 수 있는 대책 구현
5. 이러한 절차를 항상 검토하고 개선해 나가는 것

Site Security Handbook은 사이트 관리자에게 일반적으로 구현되는 보안 정책들의 실 예를 제공한다. 이러한 실 예들은 맨 처음 계획을 세우고 실천할 때에 어떤 정보들로부터 일을 시작해야 하는지에 대한 가이드를 제공한다. 한 가지 단점은 이것이 1997년도에 쓰여졌다는 점이다. 따라서 몇몇은 문제점이 존재한다. 예를 들면, VLAN 보안, 스위치 보안 혹은 BGP 보안 등과 같은 것은 언급이 없다. 다른 훌륭한 보안 모델과 함께 사용되면 Site Security Handbook은 이러한 미진한 부분을 보충할 수 있으며, 사이트 관리자들로 하여금 정책들을 유연하게 관리할 수 있게 해준다. 다섯 단계 모델에서 네 번째 스텝은 가장 시간이 많이 걸리는 단계이며 다섯 번째 단계는 가장 중요한 단계이다. Site Security Handbook은 특정 하드웨어에 대해서 보안 정책을 개발하는 것을 권고하는 것은 아니고 그 대신 보안 정책은 웹서버, 라우터, 프로토콜등과 같은 디바이스 종류에 대해서 개발이 되어져야 한다. 끝으로 Site Security Handbook은 사용자로 하여금 보안 문제점을 식별하고 처리하고 보고하는 절차를 기록하는데 도움을 주며, 또한 보안 문제 발생 후에 보안 정책을 개발하는데도 도움을 준다.

4. ISO 17799 표준: Global Security Standard

ISO 17799[4]는 2000년 12월 ISO(International Standards Organization)가 제안한 것으로서 현재 가장 널리 정보보호 표준으로 인정되고 있다. ISO 17799는 정보보호에 있어 가장 좋은 실 예들을 모은 종합적인 모음으로 정의된다. 그래서 즉, 현재 ISO 17799는 기관의 규모나 크기와는 무관하게 어느 기관에나 적용할 수 있는 최상의 보안 실 예에 대한 권고사항들을 모은 것이다. 그것은 어떤 구체적인 보안 해결책등을 안내해 주지는 않고 의도적으로 아주 유연한 표준으로 쓰여졌다. ISO 17799의 권고 사항들은 기술 중립적으로 쓰여졌으며 현존하는 보안 대책들을 이해하거나 평가하지는 않는다. 예를 들어 그것은 방화벽의 필요성을 언급할 뿐이지 방화벽의 세 가지 종류라든지 그 각각의 종류들이 어떻게 사용되고 있는지에 대해서는 언급하지 않는다. 따라서 ISO 17799는 상당히 애매하고 너무 느슨하게 구성되어 있다고도 볼 수 있다. 하지만 그것은 의도적이며 빠른 속도로 변화하는 정보기술 분야와 더불어 유연하게 변화되어 질 수 있다. ISO 17799에는 열개의 제어 영역(Control Areas)들이 있다 - 보안정책, 보안기관, 자산제어 및 분류, 개인보안, 물리 및 환경 보안, 통신 및 운용 관리, 접근제어, 시스템 개발 및 유지, 사업관리, 규정준수.

ISO 17799를 준수하는 경우의 장점들은 보안기능이 향상되고 효과적으로 보안을 계획하고 관리할 수 있으며, 소비자 신뢰가 증대되고 보안감사가 훨씬 더 정확하고 믿을 수 있다는 점이다.

5. OCTAVE

CERT/CC는 ISO 15048과 RFC 2196을 기초로 하여 OCTAVE[2]라는 보안 모델을 개발하였다. OCTAVE는 기관으로 하여금 보안 문제점들을 찾아내고 강조하기 위한 절차로서 세 부분으로 접근하였다. 첫째, 자산에 근거한 위험 자료를 만드는 것, 둘째, 인프라스트럭쳐의 취약성을 식별하는 것, 세 번째, 보안전략과 계획을 수립하는 것이다. OCTAVE는 상향식으로 설계되었다. 많은 기관들이 그 기관 자신들의 보안 문제를 발견하고 평가하는 것을 외주를 통하여 해결하고 있는데 이 방법의 문제점은 외부 기관이 그 회사의 보안 위험들을 정확하게 평가할 수 없다는 것이다. 즉, 모든 기관은 핵심 자산이 무엇이냐에 따라 서로 다른 보안 필요성이 있는데 모든 외부 기관은 이러한 핵심 자산을 정확하게 식별해내지 못하므로 그 자산을 보호하는데 흔히 실패하기 때문이다. OCTAVE를 사용하는 것은 어떤 보안 상담의 필요성을 없에는 것은 아니며, 오히려 보안 회사들과의 작업을 쉽게 해줄 수 있다. 또한 보안 회사는 기관과의 대화를 훨씬 더 수월하게 할 수 있다. OCTAVE 방식의 기본은 기관의 크기에 따라

서 세 명이나 다섯 명으로 구성이 되는 핵심 팀이다. 이 팀이 OCTAVE의 세 단계 절차에 따라 회사의 보안 평가 및 지침을 내리게 된다. 이 팀은 IT 부서에서 뿐만 아니고 핵심사업 부서의 인원도 참여하게 된다. 이 핵심 팀은 모든 답을 제공하는 것은 아니지만 답을 위한 정보를 위한 필요한 자원에는 접근할 수 있다. 핵심 팀과 핵심 팀이 수행하는 세 단계 접근 방법이 OCTAVE의 핵심적인 절차이다.

III. 보안정책 설계 및 검증 프레임 설계

모든 보안 경우에 대하여 통할 수 있는 하나의 보안 정책은 존재하지 않는다. 마찬가지로 모든 기관들이 보안 정책을 설계하고 실행하는 데에 있어 동일한 방식을 취할 수도 없다. 따라서 보안 정책 개발 및 전개는 서로 다른 입력과 이에 따른 결과가 나타난다. 그러하므로 보안 정책을 효과적으로 설계하고 적용하기 위하여 체계적으로 개발하고 검증할 수 있는 프레임은 필수적이다. 이를 위하여 여러 보안 모델들을 검토하였고 이를 통해서 보안 정책 설계와 검증에 필요한 체계적인 보안 프레임을 만들 수 있다. 이 보안 프레임은 보안 정책 설계 및 검증뿐만 아니라 보안 정책 수립에 필요한 가이드라인을 제시해 줄 수 있다. 우리는 NSSC와 SAFE 그리고 RFC 2196을 종합하여 보안 정책 설계와 검증을 위한 제어 프레임을 다음과 같이 구성한다.

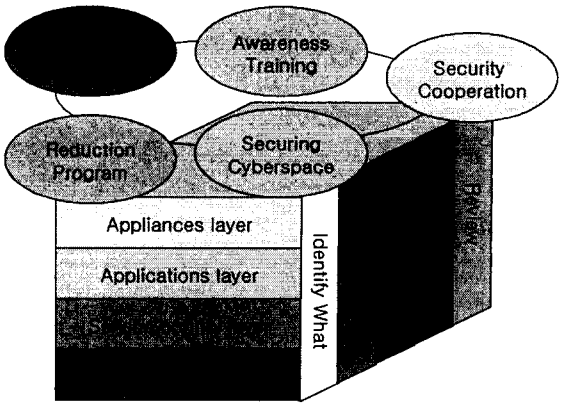

그림 3. 제어 프레임(NSSC+SAFE+RFC2196)

즉 CISCO SAFE 모델은 4개의 계층으로 구성이 되고 RFC2196에서는 보안 정책을 개발하는 과정을 5단계의 과정으로 정의하였다. 그리고 NSSC는 5개의 우선 순위를 정의하게 된다. 이제 그림 3에서 설계된 제어 프레임을 적용하는 예를 살펴보자. 최근 들어 VPN에 관한 응용이 점차 증대되고 있다[6]. 이 VPN을 위한 기능에 대하여 보안 정책을 적용하고 싶은 경우 앞의 SAFE모델 검토에서 살펴보았듯이 VPN을 위한 기능은 Infrastructure 계층으로 구분된다. 그리고 RFC 2196에 의하여 보안 기능의 대상과 기능, 그리고 보안 기능 전개 수단 등을 결정하고 이 결정된 정책을 NSSC의 5개의 우선 순위 관점에서 검토하여 의도한 대로 정책이 개발 되었는지 그렇지 않은지를 판단할 수 있게 된다. 또한 이런 과정을 반복하여 적용하면서 관련된 정책을 개발 할 수 있으며 여러 정책들을 종합적으로 검토하여 의도한 보안 기능들이 정확(correctness)하게 그리고 완전(completeness)하게 개발되었는지를 체계적으로 검토할 수 있게 된다. 이 예는 VPN뿐만 아니라 일반적인 경우에 대해서 보안 정책을 개발하고 검증하는데 사용할 수 있으며 현재 수행중인 보안관련 프로젝트에서도 사용하고 있다.

IV. 맺음말

네트워크 보안을 위한 정책 설계와 분석에서 중요한 것은 보안 정책을 집행하는 보안 모델과 보안 정책을 체계적으로 설계하고 검증할 수 있는 시스템이다. 보안 모델은 보안 정책으로 표현이 된 보안 목적을 구체적으로 변환하고 구현하는 역할을 한다. 그러므로 보안 정책은 그 네트워크에서 이루고자하는 보안 목적을 잘 반영하여야한다. 이렇게 개발된 정책들을 집행하기 위하여 보안 정책들이 올바르게 그리고 완전하게 결정되었는지를 검증하는 것은 매우 중요하다. 본 논문에서는 제안된 보안 모델들을 검토하여 보안 정책 설계 및 검증에 필요한 프레임을 설계하여 제안하였다. 이 프레임은 현재 수행 중인 보안 관련 프로젝트에서 사용되고 있다.

[1] http://www.cisco.com/safe
[2] http://www.cert.org/octave/
[3] RFC 2196
[4] http://www.iso17799software.com/
[5] http://www.whitehouse.gov/pcipb
[6] Xenakis, C., Merakos, L. : On demand Network-Wide VPN deployment in GPRS, IEEE Network, Vol. 16, Issue 6, 2002, pp. 28-37