情 報 保 護 學 會 誌
第 13 券 第 1 號, 2003. 2

신뢰성있는 차세대 네트워크 보안 시스템

남 택 용*, 김 숙 연*, 이 승 민*, 지 정 훈*, 손 승 원*

요 약

차세대 네트워크 보안 시스템(NG-NSS: Next Generation Network Security System)은 현재 네트워크 보안이 가지고 있는 한계를 극복하기 위해 각 지역망에 대한 보호 뿐만 아니라 공중망에 대한 총체적인 보호를 목표로 한다. 본 고에서는 신뢰성있는 차세대 네트워크 보안 시스템 (NG-NSS)을 정의하고 그 특성과 주요 기술을 제시한다. 신뢰성있는 차세대 네트워크 보안 시스템이란 공격, 취약성, 침입에도 불구하고 일정 수준 이상의 차세대 네트워크 보안 서비스를 지속적으로 제공하는 시스템을 의미한다.

신뢰성있는 차세대 네트워크 보안 시스템은 자율적 보호, 자체 복원과 능동적인 대응 특성을 가지며, 네트워크의 보안성, 안정성, 견고성 및 생존성을 높이기 위하여, 시스템 및 네트워크 보안기술과 네트워킹 기술을 통합하여 제공한다. 이러한 신뢰성있는 차세대 네트워크 보안 시스템은 ISP(Internet Service Provider) 등과 같은 공중망이나 증권, 은행, 보험 업계의 전산망 뿐만 아니라, 국방망, 행정전산망과 같은 국가의 중요 네트워크에 적용되어 신뢰성있는 네트워크 환경을 제공할 수 있다.

Ⅰ. 서 론

정보화 사회의 도래와 더불어 다양한 사이버 범죄가 등장하여 개인의 사생활 침해나 경제적 손실은 물론이고 국가 안보와 사회질서를 위협하는 사례까지 발생해 왔음은 잘 알려진 사실이다. 이러한 위협에 대한 대응으로서 해킹이나 바이러스 등으로부터 정보의 파괴와 왜곡을 막는 시스템 보안 기술이 발전하여 왔다. 그러나 전자 상거래, 원격 교육, 홈쇼핑 등 인터넷 기반의 서비스가 확산되고 네트워크를 통한 정보의 유통이 더욱 다양화, 복잡화, 대량화 됨에 따라 시스템 보안만으로는 한계가 있음이 알려졌다. 이에 따라 네트워크 보안의 중요성은 더욱 커지고 있는데, 특히 최근의 1.25 인터넷 대란[1]과 같은 사건은 사이버 공격의 형태가 시스템 위주의 공격에서 네트워크 공격으로 변화하고 있음을 단적으로 보여주고 있다.

네트워크 보안은 네트워크를 흘러다니는 정보를 보호하는 것 뿐만 아니라 네트워크를 통해 시스템을 해킹하거나 바이러스를 유포하는 것을 방지, 탐지, 차단 및 대응하는 것을 포함한다. 네트워크를 흘러다니는 정보를 보호하는 것은 부적절한 사용자가 트래픽을 본다든지 변형한다든지 파괴하는 것을 방지하는 것이다.

현재의 네트워크 보안의 개념은 각 지역망(Local Network)을 개별적으로 보호하는데 초점이 맞추어져 있어 사고를 미연에 방지하기가 어렵고 공중망에 유해 트래픽이 범람함에 따라 보안 사고의 책임 소재가 불분명하다는 한계점들을 지닌다. 이러한 한계점들은 네트워크 보안의 개념을 개별 지역망의 보호가 아닌 전역적인 네트워크 (Global Network) 차원의 보호로 확장함으로써 극복이 가능하다. 따라서 차세대의 네트워크 보안은 공중망을 통과하는 트래픽을 유출, 변조, 파괴, 오용 및 비정상 사용으로부터 총체적으로 네트워크 차원에서 보호하는 개념이 되어야 한다. 이러한 차세대 네트워크 보안을 위해 제안된 차세대 네트워크 보안 시스템(NG-NSS: Next Generation Network Security System)

* 한국전자통신연구원

1) 웜바이러스로 인해 전세계 인터넷 서비스가 동시 다발로 마비된 사태로서 2003년 1월 25일 발생

은 전역적인 네트워크 차원에서의 협력 (Cooperation), 등급별 서비스, 실시간 대응 및 능동적 대응, 기능의 추가 및 변경의 용이성과 다기능 통합 서비스 등의 특성을 지닌다[1].

NG-NSS는 기존의 보안 시스템과 구별되는 많은 특장점을 지니고 있지만 NG-NSS의 보안 서비스가 완벽하게 지속되는 것은 현재의 기술로는 불가능하다. 왜냐하면 시스템이 설치되는 네트워크의 복잡하고도 개방적인 특성이나 시스템 자체의 취약성으로 인하여 시스템의 정상적 가동을 위협하는 요인을 모두 제거하는 것이 어렵기 때문이다. 더구나 기존에 알려지지 않은 새로운 유형의 공격이 속출하는 요즘 같은 상황에서 침입을 완벽하게 봉쇄하는 것은 더욱 어려운 문제가 될 수 밖에 없다. 따라서 공격, 취약성, 침입에도 불구하고 일정 수준 이상의 서비스를 지속적으로 제공하기 위해서는 새로운 접근 방식이 필요한 실정이다.

이를 위하여 신뢰성있는 차세대 네트워크 보안 시스템에서는 시스템 및 네트워크 보안기술과 네트워킹 기술을 통합하여 제공한다. 즉, 네트워크 공격을 사전에 방지하고 침입의 발생시에도 일정 수준의 서비스를 유지하며 능동적인 대응을 통하여 침입의 원인을 원천적으로 제거하기 위해 기존의 보안기술과 네트워킹 기술을 통합하여 제공한다.

이러한 신뢰성있는 차세대 네트워크 보안시스템을 통하여 사용자가 신뢰할 수 있는 네트워크 환경을 제공할 수 있으며, 본 고에서는 신뢰성있는 차세대 네트워크 보안 시스템에 대한 개념과, 주요 특성 및 지원기술에 대하여 기술한다.

2장에서는 NG-NSS에 대해서 설명하고 3장에서는 신뢰성있는 보안의 개념을 제시한다. 4장에서는 신뢰성있는 NG-NSS의 정의, 특성 및 주요 기술을 제시하고 5장에서는 신뢰성 있는 NG-NSS와 관련한 연구를 정리한 후 6장에서 결론을 맺는다.

2. 차세대 네트워크 보안 시스템 (NG-NSS)

2.1 보안 시스템과 네트워크 보안 시스템

보안 시스템 (Security System)이란 보안 서비스를 제공하는 시스템을 말한다. 표 1에 보안 시스템의 예들이 나타나 있다. 보안 시스템들은 물리적으로 독립된 시스템으로서 제품화되어 있을 수도 있지만 PC 보안 제품이나 전자우편 보안 제품 같이 다른 시스템의 부가적 기능으로서 제공될 수도 있다. 본 고에서 특별한 언급없이 보안 시스템이라 함은 물리적으로 독립된 시스템을 의미한다.

〔표 1〕 보안 시스템의 예

항 바이러스 시스템	컴퓨터 바이러스에 의한 시스템 유해요소의 차단과 손상된 시스템에 대한 복구를 수행하는 시스템
침입탐지시스템 (IDS)	네트워크 또는 컴퓨터 시스템에서 내외부 사용자에 의한 불법행위를 실시간으로 탐지하는 시스템
침입차단시스템 (Firewall)	해커 등 비인가자가 내부망으로 침입하는 것을 차단시키는 소프트웨어 또는 하드웨어 시스템
가상사설망 (VPN) 시스템	공공망을 지점간 안전한 터널링으로 설정하여 전용회선을 사용하는 듯한 사설망 기능을 제공해주는 시스템
공개키기반구조 (PKI) 시스템	공개키 암호기술을 이용한 인증 프레임워크로 인터넷과 같은 개방형 환경에서 인증기관이 발행하는 인증서를 통해 전자문서의 무결성, 기밀성, 부인방지 등을 보장해 주는 시스템
데이터보안 (Encryption) 시스템	저장한 파일 내용을 암호화하여 적정한 해독키 없이는 복호화하여 사용할 수 없도록 보안기능을 제공해 주는 시스템
보안관리시스템 (ESM)	여러 형태의 정보보호제품을 통합하여 관리하는 시스템
무선인터넷 보안 시스템	모바일 인터넷의 정보 보안을 해결해 주는 시스템
생체인식 시스템	홍채, 지문, 정맥, 음성, 얼굴 등 개인의 신체적 특성을 이용해 신원확인 및 출입, 접근을 통제 관리하는 시스템

네트워크 보안 시스템은 네트워크 보안 서비스를 제공하는 시스템을 말한다. 네트워크 보안 서비스에 대해서는 다음 절에서 상세히 설명한다. 기존의 네트워크 보안 시스템으로는 침입탐지시스템, 침입차단시스템, 보안관리시스템(ESM: Enterprise Security Management) 등이 있다. 최근에 제안된 NG-NSS는 보안 게이트웨이(Secure Gateway) 형태를 띠기도 하고 라우터나 스위치에 보안 서비스 기능이 부가된 보안 라우터(Secure Router)나 보안 스위치 (Secure Switch)의 형태를 띄기도 한다.

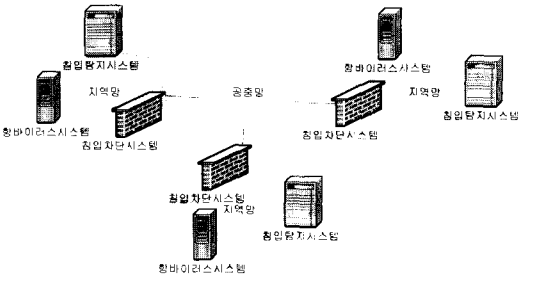
NG-NSS은 기존의 네트워크 보안 시스템들과 달리 다음과 같은 특성을 갖는다. 첫째, NG-NSS들이 전역적인 네트워크 차원에서의 협력을 한다. 즉 분산된 NG-NSS들은 유기적으로 결합되어 함께 동작함으로써 네트워크 보안 서비스를 제공한다. 둘째, 등급별 서비스를 제공할 수 있다. 네트워크 보

안 서비스를 다양화 및 세분화된 형태로 제공함으로써 개별 지역망(예: 기업망)의 요구사항에 부합하는 보안 서비스를 제공한다. 셋째, 실시간 대응 및 능동적 대응을 할 수 있다. 즉 공격의 결과를 수습하는데 그치지 않고 공격의 준비, 착수, 진행의 각 시기에 개입하여 실시간으로 대응할 수 있으며, 침입 패킷을 차단하는 식의 방어적 대응뿐만 아니라 침입자를 역추적하는 등의 능동적 대응을 할 수 있다. 넷째, 정책 기반의 통합적 관리 메커니즘을 가진다. 즉 공중망에 분산적으로 위치하는 NG-NSS들을 통합적으로 제어할 수 있으며 사용자 친화적인 관리도 가능하다. 다섯째, 새로운 기능의 추가 및 변경이 용이하다. 빠른 속도로 변화하는 해킹 및 바이러스의 유형에 대하여 신속 정확하게 대응할 수 있는 유연한 구조를 가진다. 여섯째, 침입탐지, 접근제어, 바이러스 탐지, 가상사설망 등의 기능이 고성능화 및 통합화된 형태로 제공된다. 즉 기존의 보안 장비들이 가진 개별적 기술들이 그 경계나 구분 없이 네트워크 보안이라는 한가지 목표 아래 고성능화되어 통합된다. 일곱째, 기존의 보안 장비들과의 연동이 가능하다.

2.2 네트워크 보안 서비스 (Network Security Service)

네트워크 보안 서비스는 크게 두 가지로 볼 수 있다. 첫째는 협의의 네트워크 보안 서비스로서 각 지역망을 외부의 침입으로부터 보호하는 서비스이고 둘째는 광의의 네트워크 보안 서비스로서 공중망을 총체적으로 보호하는 서비스이다.

먼저 각 지역망을 외부의 침입으로부터 보호하는 서비스에 대해서 살펴보자. 그림 1과 같이 이 서비스는 침입 탐지, 침입 차단, 항바이러스 등의 기능을 하는 시스템들을 활용하여 각 지역망을 외부의 침입으로부터 보호하는 것이다. 이러한 서비스의 예로는 전문 보안업체나 ISP (Internet Service Provider)가 제공하는 보안 관제 서비스를 들 수 있다. 보안 관제 서비스는 불법 해킹이나 바이러스로부터 지역망 내부의 시스템과 네트워크 자원의 손상을 막기 위해 관제가 필요한 모든 시스템을 실시간으로 모니터링하여 적절한 대응을 해주는 것이다. 보안관제 서비스를 이용하는 기업은 보안전문인력의 지원을 받는 것은 물론, 보안 장비 관리와 유지에 드는 비용도 절감할 수 있다. 서비스 항목을 구체적으로 살펴보면 침입 탐지, 접근 제어, 바이러스 탐지, 침입 대응 등이 있다



〔그림 1〕 기존의 네트워크 보안 서비스

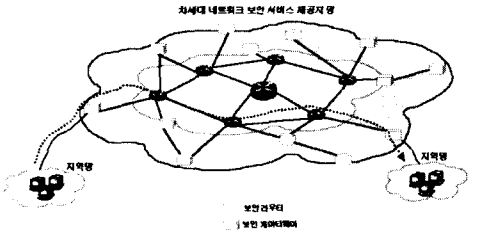
보안 관제 서비스는 각 지역망을 개별적으로 보호하는데 초점이 맞추어져 있어 다음과 같은 한계점들을 가지고 있다. 첫째, 사고의 미연 방지 및 원천 봉쇄가 어렵다. 왜냐하면 각 지역망은 자신을 목적지로 하는 패킷만을 탐지하여 대응하므로, 공격자의 패킷이 다양한 경로와 방법을 통하여 공격을 준비하는 과정에 개입할 수가 없기 때문이다. 둘째, 공중망[2]에 유해 트래픽이 범람한다. 즉 피해자 중심으로 탐지 및 대응을 하므로 공격을 목적으로 하는 유해 트래픽이 목적지 네트워크에 도착할 때까지 아무런 제지 없이 공중망을 통과하게 된다. 셋째, 보안 사고의 책임 소재가 불분명하다. 왜냐하면 공격자는 IP Spoofing이나 TCP 우회 공격 등의 방법으로 네트워크를 광역적으로 활용하는데 반해 피해자는 자기가 속한 망에 국한하여 탐지하므로 공격자를 색출하기가 어렵기 때문이다.

이러한 한계점들을 극복할 수 있는 방안 중 하나가 광의의 네트워크 보안 서비스, 즉 차세대 네트워크 보안 서비스이다. 이는 전역적인 네트워크 차원의 보안을 목표로 공중망을 총체적으로 보호하는 것이다. 즉 각 지역망을 개별적으로 보호하는 것에 그치는 것이 아니라 공중망을 통과하는 트래픽을 파괴, 왜곡, 오용 및 비정상 사용으로부터 총체적으로 보호함으로써 지역망에 대한 보안 서비스도 함께 제공할 수 있다.

차세대 네트워크 보안 서비스의 제공자는 전달망을 소유한 ISP이거나 전달망을 임대한 보안 서비스 업체일 수도 있다. 차세대 네트워크 보안 서비스의

2) 예: ISP망, 초고속 국가망 등

고객은 서비스 제공자의 망을 통해 인터넷과 같은 전달 서비스를 받음과 동시에 보안 서비스를 받는 사이트가 된다. 이러한 고객 사이트는 기업망이거나 가입자망이 될 수 있다. 그림 2는 차세대 네트워크 보안 서비스의 제공자와 고객의 예를 나타낸 것이다. 서비스 제공자 망에는 보안 게이트웨이나 보안 라우터 같은 NG-NSS들이 존재하여 지역망들에게 차세대 네트워크 보안 서비스를 제공한다.



〔그림 2〕 차세대 네트워크 보안 서비스

서비스 제공자는 고객 사이트인 지역망의 접속점을 통과하는 모든 트래픽에 대해서 보안 서비스를 제공한다. 여기서 접속점이라 함은 지역망의 트래픽이 서비스 제공자 망에 진입하는 지점을 말한다. 접속점을 통과하는 모든 트래픽에 대한 보안 서비스는 접근 제어, 침입 탐지, 항 바이러스, 역추적 및 대응뿐만 아니라 가상 사설망 서비스까지도 포함한다. 여기서 가상 사설망 서비스는 Access VPN을 의미하는 것은 아니고 서비스 제공자 망을 통해 논리적으로 연결된 두 개의 원격 사이트간의 Intranet 혹은 Extranet을 의미한다.

광의의 네트워크 보안 서비스의 항목은 협의의 네트워크 보안 서비스의 항목과 유사하게 지역망에 대한 침입 탐지, 접근 제어, 바이러스 탐지, 능동 대응 등이다. 하지만 광의의 네트워크 보안 서비스는 다음과 같은 면에서 협의의 네트워크 보안 서비스와 차별성을 지닌다.

첫째, 서비스의 최종 목표가 개별적인 서비스를 제공하는 것이 아니라 공중망을 통과하는 트래픽에 대한 총체적 보호이다. 둘째, 인터넷 서비스와 같은 기존의 네트워크 서비스에 결합된 형태로 제공된다. 셋째, 각 네트워크 보안 시스템들이 독립적인 기능을 수행함으로써 서비스가 제공되는 것이 아니라, 전체 네트워크 차원에서의 협력을 통해 제공된다. 넷째, 각 서비스 제공자의 망에 국한되어 제공되는 것이 아니라 다수의 서비스 제공자가 연동함으로써 제공된다. 다섯째, 침입탐지, 접근제어, 바이러스 탐지, 가상사설망, 능동 대응 등의 서비스가 개별적인 형태가 아닌 통합된 형태로 제공된다. 여섯째, 각 서비스 항목들은 세분화된 후 적절한 등급별 조합을 형성함으로써 등급별 서비스가 제공된다.

3. 신뢰성 (Reliability) 과 보안 (Security)

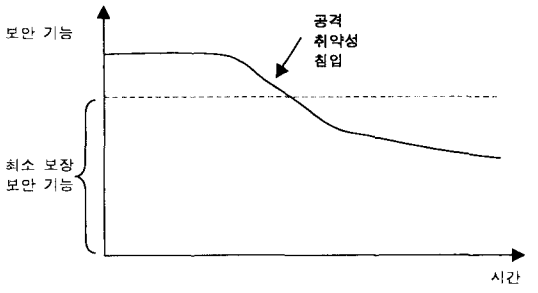
본 절에서는 신뢰성있는 보안(Reliable Security)의 개념과 신뢰성있는 보안을 수행하기 위한 방안을 제시한다.

신뢰성(Reliability)이란 일반적으로 시스템이 사용 환경 하에서 정해진 기간 동안 요구되는 기능을 수행할 수 있는 능력을 나타낸다. 시스템의 신뢰성을 위협하는 사용 환경에는 물리적, 자연적, 기술적, 그리고 인위적인 요소 등이 포함될 수 있다. 따라서 신뢰성있는 시스템은 이러한 사용 환경에도 불구하고 요구되는 기능을 일정기간 동안 지속적으로 제공할 수 있어야 한다.

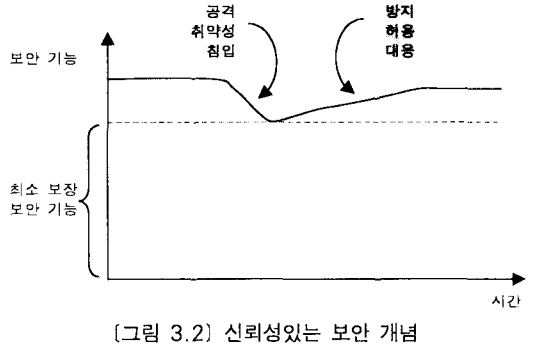
이와 같은 신뢰성의 개념을 보안에 적용하기 위해서는 우선, 보안을 위협하는 사용 환경에 대하여 살펴볼 필요가 있다. 사용 환경으로 첫째, 공격(Attack)을 들 수 있다. 공격이란 악의적인 침입 시도 행위 자체를 의미한다. 둘째, 취약성(Vulnerability)으로서 공격을 위하여 탐색 되는 시스템의 약점 또는 결점을 들 수 있다. 셋째, 침입(Intrusion)으로 외부에서 유도된 의도적이거나 악의적인 침투이며, 공격과 취약성은 침입의 원인이 될 수 있다.

이러한 외부의 공격이나 취약성, 그리고 침입에도 불구하고 일정수준 이상의 보안 기능을 유지하기 위한 방안으로는 방지(Prevention), 허용(Tolerance), 대응(Response) 등을 들 수 있다. 방지는 공격이나 취약성, 그리고 침입의 발생을 사전에 대처하는 것이다. 허용은 공격이나 취약성, 그리고 침입에도 불구하고 보안 기능을 제공 할 수 있는 방법이다. 대응은 침입 이후에 자체 복원이나 역추적 등을 통하여 공격의 근본 원인을 해결하기 위한 능동적인 대처 방안이다.

그림 3.1은 기존의 보안 개념을 나타낸 것으로서 시간이 지남에 따라 외부의 공격, 취약성, 침입 등의 영향으로 초기의 보안 기능이 최소한으로 보장된 보안 기능 이하로 떨어짐을 보여주고 있다.



〔그림 3.1〕 기존 보안 개념



〔그림 3.2〕 신뢰성있는 보안 개념

그림 3.2는 신뢰성있는 보안 개념을 나타낸 것으로서 초기의 보안 기능이 공격, 취약성, 침입 등에도 불구하고 방지, 허용, 대응 등의 기술을 이용하여 최소한으로 보장된 보안 기능을 지속적으로 제공함을 보여주고 있다.

따라서, 본 고에서 다룰 신뢰성있는 보안(Reliable Security)이란 외부의 공격이나 취약성, 그리고 침입에도 불구하고 이를 방지하고 허용하며, 대응할 수 있는 일련의 과정을 통하여 지속적인 보안 기능을 유지함을 의미한다.

4. 신뢰성있는 차세대 네트워크 보안 시스템

본 장에서는 신뢰성있는 차세대 네트워크 보안 시스템(NG-NSS)를 정의하고 그 특성과 주요 기술을 제시한다.

4.1 정의 및 특성

차세대 네트워크 보안 시스템(NG-NSS)은 2.1절에서 언급한 바와 같이 기존의 보안 시스템과 구별되는 많은 특장점을 지니고 있다. 그러나 NG-NSS가 설치되는 네트워크의 복잡하고도 개방적인 성격이나 시스템 자체의 취약성으로 인하여 NG-NSS의 정상적 가동을 위협하는 요인을 모두 완벽히 제거하는 것은 불가능하다. 따라서 NG-NSS의 신뢰성이 절실히 필요한 실정이다. 신뢰성있는 NG-NSS이란 공격, 취약성, 침입에도 불구하고 일정 수준 이상의 차세대 네트워크 보안 서비스를 지속적으로 제공하는 시스템이다.

신뢰성있는 NG-NSS의 대표적인 특성으로는 자율적인 보호 특성, 침입후의 피해를 최소화 할 수 있는 자체 복원 특성 및 침입의 근본 원인을 해결하기 위한 능동적인 대응 특성 등이 있다.

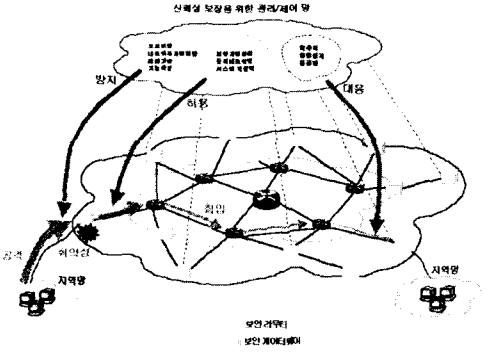
자율적인 보호 특성이란 시스템이 다양한 여러 침입에 대한 자체 보호기능을 갖고 있으며, 차후의 동일한 또는 유사한 공격에 대하여 자동적으로 저항능력을 갖는 것을 말한다. 기존의 네트워크 보안이 주로 침입후의 대처방안에 있어서 수동적인 관리자의 네트워크 설정으로써 대응하는데 반하여, 신뢰성있는 NG-NSS은 시스템 자체의 자율적인 동작으로써 대응한다.

자체 복원 특성이란 공격자의 침입 후에 침입으로 인한 피해를 최소화하고, 최소한의 기능수준을 유지하기 위하여 자체 복원기능을 갖는 것을 말한다. 기존의 보안 시스템에서는 침입후의 피해 복구 단계에서 관리자의 개입에 의하여 유해 프로그램 및 이상 설정에 대한 제거가 이루어지며, 피해가 심각할 경우에는 시스템 운영체제의 재설치와 하드웨어의 교체를 필요로 한다. 이러한 과정은 시스템의 가용성을 떨어뜨리며, 서비스의 단절까지 초래할 수 있다. 이에 반해 신뢰성있는 NG-NSS는 자체 복원 특성을 이용하여, 실시간 온라인으로 피해를 복구하여 서비스의 연속성을 지원한다.

능동적인 대응 특성이란 실시간적으로 침입 징후를 탐지하여 공격의 근원지를 역추적함으로써 공격자를 네트워크로부터 고립시키거나 역공격하는 것을 의미한다. 이러한 능동적인 대응을 통하여, 공격의 피해를 최소화할 수 있으며 보다 효과적으로 이전 서비스의 수준으로 회복할 수 있다.

그림 4는 신뢰성있는 NG-NSS로 구성된 서비스 제공자 망의 예를 보여준다. 서비스 제공자망에는 신뢰성을 보장하기 위한 논리적인 망이 오버레이 형태로 존재하여 NG-NSS들에 대한 관리 및 제어를 담당한다. 이러한 신뢰성 보장을 위한 관리 제어 망에서는 방지, 허용, 대응의 능력을 제공한다. 방지가 공격이 시도되기 전에 효과를 발휘하는 능력이라면

허용이나 대응은 이미 침입이 진행되었을 때 되었을 때의 대처 능력이라 할 수 있다. 허용이 비교적 수동적인 성격을 띄는 반면 대응은 적극적인 성격을 띄게 된다. 그림 4에는 굵은 화살표로 강도 크게 시작된 공격이 방지 능력에 의해서 약화된 형태로 침입으로써 진전하다가 허용 및 대응 능력에 의해서 더욱 약화되어 최소 보장 보안 기능이 성공적으로 수행되는 예를 보여주고 있다.



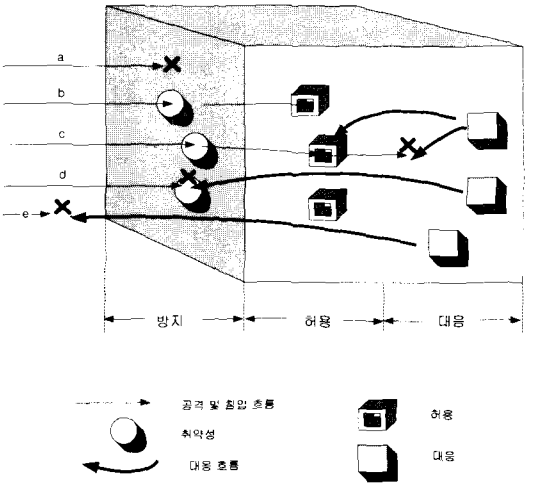
〔그림 4〕 신뢰성있는 NG-NSS로 구성된 서비스 제공자 망의 예

4.2 주요 기술

본 절에서는 신뢰성있는 차세대 네트워크 보안 시스템을 위한 주요 기술들을 크게 방지, 허용, 대응으로 분류하여 설명한다.

방지에는 공격과 취약성으로 인한 침입의 발생을 사전에 차단하는 기술들이 해당되며, 감내에는 침입에도 불구하고 네트워크 보안 서비스를 신뢰성있게 제공할 수 있는 기술들이 해당된다. 대응에는 침입 이후에 역추적등을 통한 공격자 근원지의 파악을 통하여 침입의 근본 원인을 제거하는 과정과 시스템의 취약성등에 대한 복원을 수행하는 기술들이 속한다.

그림 5는 방지, 허용, 대응에 대한 개념에 대한 도식화된 표현으로, a의 경우는 공격이 방지에 의해서 차단되는 것을 보이며, b는 공격이 취약점을 이용하여 침입에 성공하였으나, 허용에 의해서 영향을 미치지 못하는 경우를 보인다. c의 경우에는 허용치를 초과하는 침입의 경우인데 이러한 침입은 대응에 의해서 차단되며, 또한, 해당 허용의 기능은 대응에 의해서 업데이트되어 차후의 침입에 대응한다. d의 경우는 대응에 의해서 취약점이 제거되는 것을 보이며, e의 경우는 대응에 의해서 공격의 근원지 파악과 원인 제거 과정을 보인다.



〔그림 5〕 방지, 허용, 대응의 개념

4.2.1 방지

방지는 공격이나 취약성, 그리고 침입의 발생을 사전에 차단하기 위한 것으로서, 안전한 통신 프로토콜 기술, 네트워크 자원 할당 기술과 보안 기능 측정 기술 등이 있다.

안전한 통신프로토콜 기술

기존의 통신프로토콜에 고비도 암호화, 인증 및 권한인가 기능을 첨가하여, 통신프로토콜의 보안성을 높인다. 이러한 기술은 기존의 통신프로토콜의 취약성과 개방성으로 인하여, 이러한 점을 악용한 여러 공격에 대처하기 위한 것으로 기존의 라우팅, 멀티캐스팅 및 QoS 등의 프로토콜에 적용된다.

네트워크 자원 할당 기술

네트워크 자원을 관리하여 특정 사용자의 가용한 자원을 할당한다. 이러한 기술은 사용자의 무분별한 네트워크 자원 사용을 제한하여 보다 안정적으로 네트워크 서비스를 운용할 수 있도록 지원한다. 이러한 기술을 통하여, DoS (Denial of Service) 와 같은 네트워크 자원 남용을 이용한 공격을 막을 수 있다.

보안 기능 측정 기술

시스템내의 보안 자원과 보안 기능의 정도를 감시하여 보안 자원으로 제공되는 보안 서비스의 질적

수준을 적합한 수준으로 제공하도록 하기 위한 보안 기능별 성능을 평가할 수 있는 기술을 의미한다. 이러한 기술은 사전에 네트워크에서 지원되는 보안 기능의 성능을 측정하여 일정 수준 이상으로 유지함으로써, 보안기능의 오동작 및 성능 저하를 이용한 네트워크 공격을 사전에 차단하기 위한 것이다.

4.2.2 허용

허용은 공격이나 취약성, 그리고 침입에도 불구하고 보안 기능을 제공 할 수 있는 방법을 의미하며, 보안 자원 관리 기술, 동적 네트워킹 기술과 시스템 적응력 기술 등이 해당된다.

보안 자원 관리기술

위험 상황 시에 보안 서비스를 신뢰성있게 지원하기 위하여 보안 자원을 관리하여, 보안 서비스가 적합한 수준으로 원활히 제공될 수 있도록 한다. 보안 시스템의 성능 저하가 발생할 경우에 전체 네트워크 차원에서 동일한 기능을 수행 할 수 있도록, 보안 자원 재할당, 보안 자원 복제와 보안 자원 동적 협동 등이 포함된다.

동적 네트워킹 기술

위험상황에 대처하기 위한 전체 네트워크 차원의 기술이다. 동적 라우팅 설정을 통한 논리적인 보안 overlay 네트워크를 생성 및 네트워크의 신뢰성을 지원하기 위한 네트워크 서비스 자체에 대한 복제 및 분할기술이 해당된다. 여기서의 복제는 위험상황에 대처하기 위한 잉여의 자원을 예비하는 것이며, 분할은 네트워크 침입의 영향이 전체 네트워크 서비스의 안정성에 영향을 미치지 않도록 하기 위한 조치를 의미한다.

시스템 적응력 기술

보안 시스템의 신뢰성을 지원하기 위한 시스템 자체의 동적 적응 기술을 의미한다. 보안 기능의 성능 저하될 경우, 제한된 보안 자원을 최대한 활용하여 보장된 보안 기능을 수행할 수 있도록 한다.

4.2.3 대응

대응은 침입 이후에 자체 복원이나 역추적 등을 통하여 근본 원인을 해결하기 위한 능동적인 대처 방안이다. 이러한 기술로는 공격자 근원지 확인 기술, 침입 평가 기술과 등급화 서비스 기술 등이 있다.

공격자 근원지 확인 기술

침입에 대한 가장 효과적인 대처방안은 침입자의 근원지 파악을 통한 침해원인의 근본적 해결이다. 이를 위하여 네트워크 노드 식별 기법 및 공격자 패킷 경로 확인 등의 기술이 적용되고 있다. 공격자의 근원지를 확인하기 위해서는 네트워크 도매인간의 역추적 정보교환과 제도적인 문제 등이 선결되어야 한다.

침입 평가(Assessment) 기술

보안 시스템 자체에 대한 침입이나 DDoS와 같이 타 시스템에 대한 공격으로 인한 간접적인 영향에 대하여 시스템 차원의 대응을 하기 위해서는 현재 진행중인 침입의 정도를 정확하게 평가 할 수 있는 기술이다.

등급화 보안 서비스(Leveled Security Service) 기술

시스템 차원에서 수행할 수 있는 대응 방법은 다양할 수 있는데, 이를 위해서 사전에 패킷별 등급화가 필요할 수 있다. 예를 들어, 보안 서비스의 등급에 따라 특정 패킷은 폐기하여 원활한 서비스가 수행될 수 있게 한다.

5. 관련 연구

본 장에서는 신뢰성있는 NG-NSS와 관련된 연구에 대해서 살펴본다. DARPA에서 추진중인 FTN (Fault Tolerant Network), ITS (Intrusion Tolerant System)와 OASIS(Organically Assured and Survivable Information Systems) 프로그램에 대해서 살펴보고, 유럽 IST(Information Society Technologies)의 MAFTIA(Malicious and Accidental Fault Tolerance for Internet Applications) 프로그램에 대해서 살펴보기로 한다.

5.1 주요 연구 현황

신뢰성있는 NG-NSS와 관련된 대표적인 연구로 DARPA의 FTN (Fault Tolerant Network) 프로그램[2]을 들 수 있다. FTN 프로그램은 1999년부터 시작된 프로젝트로서, 성공적인 공격의 후에도 지속적인 네트워크의 동작을 지원하기 위한 기술을 개발하는 것을 목표로 하여, ISP 등에서 제공하는 네트워크 기반 서비스의 생존성과 안정성을 보장

하기 위해 글로벌 환경에서 DDoS 공격을 방어 및 대응하기 위한 연구를 진행한다. 해당 프로그램에서는 공격자 침입경로 고립기술, 보안 네트워크, 네트워크 인프라에서의 공격방어 및 생존성 기술, 능동 네트워크 기반 침입대응기술 등에 대한 과제를 진행중이다. 프로그램에서 추진중인 프로젝트의 주요 내용은 표 2에서 살펴볼 수 있다.

시스템의 생존성에 관한 연구로는 우선 DARPA 에서 추진중인 ITS (Intrusion Tolerance Systems) 프로그램[3]을 들 수 있다. 이 프로그램의 목적은 침입에 대한 저항성(Resilience)과 허용성(Tolerance)을 가지는 시스템의 개념, 설계, 개발, 검증 구조와 방법론에 대한 기술을 개발하기 위함이다. 연구 개발 범위는 악의적인 침입에 대한 데이터와 프로그램의 무결성 유지와 서비스 거부 공격에 대한 대응 및 시스템의 가용성 보장에 초점을 두고 있다. 해당 프로그램에서 추진중인 프로젝트의 주요내용은 표 6에서 살펴볼 수 있다.

DARPA의 OASIS 프로그램[4]은 생존성 있는 시스템을 유기적으로 국가정보 방어에 활용할 수 있는 기술과 구조의 개념 정립, 설계, 개발, 구현 및 검증을 목적으로 한다. 이를 위한 기술적 이슈는 유기적으로 생존성 있는 시스템을 구축하기 위하여 다중 허용 계층형태로 3세대 보안 기술을 제공하는 것이다. 3세대 보안 기술은 1세대의 Trusted Computing Bases, Encryption, Authentication과 Access Control 및 2세대의 Boundary Controllers, Intrusion Detection Systems, Public Key Infrastructure 와 Biometrics 보안 기술을 보완한 것을 의미한다.

EC(European Commission)에서는 IST(Information Society Technologies)의 MAFTIA(Malicious and Accidental Fault Tolerance for Internet Applications) 프로그램을 통하여, 시스템의 우연히 발생한 고장이나 악의적인 공격을 포함한 부주의한 행동으로부터 분산된 인터넷 자원의 의존성(Dependability)을 연구하고 있다.

여기서 말하는 의존성은 시스템이 제공하는 서비스에 정당하게 부여되는 신뢰성, 즉 시스템의 믿을 수 있는 정도를 말한다. 의존성을 구성하는 일반적인 속성은 시스템의 사용가능 정도에 대한 척도를 나타내는 가용도(Availability), 서비스가 지속적으로 유지될 수 있는가에 대한 척도를 나타내는 신뢰도(Reliability), 치명적인 재해가 발생하지 않는가에 대한 척도를 나타내는 안정도(Safety), 그리고 사생활을 위협하거나 가치 있는 자산의 손실을 초래하는 사건을 피할 수 있는가에 대한 척도인 보안성(Security) 등이다. 의존성 있는 시스템을 개발하기 위하여 결함(Faults)을 공격(Attack), 취약성(Vulnerability), 침입(Intrusion)으로 정의하고, 이에 대처하기 위한 방안으로 방지(Prevention), 허용(Tolerance), 제거(Removal), 예측(Forecasting)으로 구분하여 연구 개발을 추진하고 있다.

5.2 프로젝트 현황

본 절에서는 DARPA 의 FTN 프로그램과 ITS 프로그램의 주요 프로젝트에 대해서 살펴보기로 한다.

〔표 5〕 FTN 프로그램 관련 프로젝트 주요내용

프로젝트	주요내용
Transitioning Secure BGP into the Internet - BBN	• 목 적 : BGP에 안전성 부여 • 적 용 처 : 인터넷의 라우팅 프로토콜 BGP • 주요기법 - 라우터간 안전한 통신을 위해 IPsec사용 - S-BGP의 참여자간의 권한부여 프레임워크로 PKI (Public Key Infrastructure) 사용 - 인증서(certificates) 및 증명서(attestations)를 이용한 경로 업데이트의 검증
Applications that Participate in their Own Defense (APOD) - BBN	• 목 적 : 취약한 OS나 네트워크 환경상의 어플리케이션 보호 • 적 용 처 : 네트워크 어플리케이션 • 주요기법 - 특권을 독립적으로 가지는 다수개의 보안 도메인 설정 - 공격자의 특권사용에 대한 대응 - 정적 보호와 동적 보호를 융합

〔표 5〕 FTN 프로그램 관련 프로젝트 주요내용 (계속)

프로젝트	주요내용
A Cost-Benefit Approach to Fault Tolerant Communication and Information Access - **Johns Hopkins Univ.**	• 목 적 : 공격자에 대한 모델링, 공격자에 따른 특정 알고리즘 선택, 비용-이득에 관련한 알고리즘적 프레임워크 제시 • 적 용 처 : 네트워크 전반 • 주요기법 - 최적에 가까운 라우팅과 라우팅 정보 분배에 의한 네트워크 레벨의 견고성 - 네트워크에 대한 위협의 증가 시에도 성능이 점진적으로만 감소하도록 중복성을 활용하여 정보 접근의 견고성 확보 - 자원관리와 신뢰성을 통합하는 비용-이득 프레임워크
Denial of Service Attack Assessment - **Johns Hopkins APL**	• 목 적 : 네트워크의 Denial of Service (DoS) 공격을 평가하는데 분석과 시뮬레이션을 사용 • 적 용 처 : 네트워크 전반 • 동 기 - DoS 공격에 대한 견고한 양적 기준 필요 - 미래의 Information Assurance (IA) 설계와 평가 도구에 대한 기반 연구 필요 • 주요기법 - 주요 DOS 공격을 모델링하는데 OPNET사용 - 프로토콜 스택에 걸친 효과, 공격성능에 대한 네트워크 아키텍쳐, 크기와 stochastic behavior의 효과들을 연구하기 위해 모델링한 결과를 분석
Advanced Security Proxies - **NAI Labs**	• 목 적 : 차세대 고속 네트워크(ATM OC-12)를 지원할 수 있는 안전한 고속 방화벽 • 적 용 처 : 방화벽 • 주요기법 - TCP/IP 트래픽 재조합을 위한 방화벽과 프락시의 연동기법
Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) -**Arch. Technology Corp.**	• 목 적 : 애드혹 (ad hoc) 네트워크를 DoS (denial of service) 공격으로부터 방어하는 일반적인 기법들 개발 • 적 용 처: 애드혹 (ad hoc) 네트워크 • 동 기 - 인터넷 라우팅 인프라스트럭춰를 보호하는 기법은 애드혹 네트워크에 부적절 - 노드의 이동성, 네트워크 범위의 유동성, 공격의 새로운 유형과 같은 새로운 문제에 봉착 • 주요 기법: - 애드혹 무선 네트워크에 분산된 방화벽 설치 - 분산된 트래픽 정책 메커니즘 - 침입감내 라우팅
Better Fault Tolerance via Application-Enhanced Networks - **Arizona**	• 목 적: 오류와 공격을 감내해 내는 액티브 라우터의 지역적(local) 자원관리 • 적 용 처: 액티브 네트워크에서 단-대-단(end-to-end) 고장 감내 • 주요기법 - 저장소 특징에 따른 자원관리와 계정관리 - 부적절한 요구를 기부하는 등의 침입 및 고장에 대한 저항성 - 토큰 기반의 동기화

〔표 6〕 ITS 관련 프로젝트 주요내용

프로젝트	주요내용
A Binary Agent Technology for COTS Software Integrity - **InCert Software Corporation**	• 목 적 : COTS(Commercial-off-the-shelf) 소프트웨어의 무결성 • 주요개념 - 에이젼트를 COTS 바이너리에 직접 삽입 - 삽입된 에이젼트가 비정상행위나 데이터 손상을 탐지, 정정, 보고 및 복구 • 주요기법 - COTS 바이너리에 자동 에이젼트 삽입 기법 - 실행중인 응용의 비정상행위 탐지 메커니즘 - 이상 보고 및 정정 메커니즘 및 신속한 복구기법
Agile Objects: Component-based Inherent Survivability - **University of California, San Diego**	• 목 적 : 원천적 생존성을 가지는 컴포넌트 기반의 응용에 대한 프레임워크 제시 • 주요개념 - 응용이 공격에 대해서 유연하게 반응할수 있도록 생존성 부여. • 주요기법 - 분산된 자원에 걸쳐 응용 컴포넌트들이 재설정되는 기법 - 응용의 보안성을 유지하기 위해 컴포넌트와 분산객체의 인터페이스의 자동 설정 변경하는 기법 - 복잡하게 진화하는 침입환경에 대해 동적으로 elusiveness 차원을 관리하는 기법
Containment and Integrity for Mobile Code - **Cornell University**	• 목 적 : 각기 다른 신뢰도를 가지는 컴포넌트들과 호스트들로 구성된 네트워크 정보 시스템에 보안 정책을 실현 • 주요 개념 - 상세한 접근제어에 대한 유연한 지원과 효과적 구현 - 인증에 소스 뿐만 아니라 정보의 내용까지 고려하는 응용레벨의 보안정책
FOUR-A (Agent Adaptation and Assurance) - **Carnegie Mellon University**	• 목 적 : 프로그램 분석, 주석, 조작과 같은 기법에 기반하여 보증된 소프트웨어 시스템의 개발, 분석, 보완의 방법 개발 • 주요개념 - 소프트웨어 신뢰성과 신뢰성의 보증에 대한 도구와 기법을 위한 시험용 어플리케이션 - 자바 프로그램의 개발 및 개량을 위한 프로토타입 도구에 프로그램의 분석, 조작, 주석에 대한 기법을 적용
Integrity Through Mediated Interfaces - **Information Sciences Institute**	• 목 적 : 권한있는 사용자만 공인된 툴을 이용하여 수정할 수 있는 단-대-단(end-to-end) 데이터 무결성 관리. • 주요개념 : 권한있는 사용자가 공인된 툴을 이용하지 않은 수정과 프로그램 오류나 악의적인 공격에 대한 탐지 및 정정. • 주요기법 - 데이터 집합의 모든 변경에 대한 다-대-단 감사기록을 제공하기 위해 프로그램의 동작을 감시하고 기록하는 무결성 관리자 생성 - 데이터 집합이 손상되었을 경우 그들의 변경기록을 이용하여 원래의 데이터 상태로 복구.
PASIS - A Distributed Framework for Perpetually Available and Secure Information Systems - **Carnegie Mellon University**	• 목 적 : 지속적 가용성, 지속적 보안성, 완만한 성능 저하를 가지는 정보저장시스템 생성 • 주요개념 - 가용성, 보안성, 성능간의 트레이드오프를 조절 - 분산된 저장 노드들에 임계점(threshold) 개념 적용 • 주요기법 - 저장 노드들 중 일부분만 손상되고 악의적 사용자의 행위는 즉각 탐지될 수 있음을 가정 - 가용성은 적어도 x개의 고장난 노드에서 보장되어야함. - 기밀성과 무결성은 적어도 y개의 손상된 노드에서 보장되어야 함. - 데이터와 감사로그는 z 주동안 보관되어야 함.

〔표 6〕 ITS 관련 프로젝트 주요내용 (계속)

프로젝트	주요내용
Reconciling Execution Efficiency With Provable Security - **University of California, Irvine**	• 목 적 : 모바일 코드의 기밀성, 무결성 제공 • 주요개념 : 생명력있고 실용적인 모바일 코드 생성을 위하여 원천적 보안 제공 • 주요기법 - 공격자의 악의적 프로그램이 인코드될 수 없는 모바일 프로그램 - 적용 기계에 독립적인 모바일 프로그램
Sandboxing Mobile Code Execution Environments - **Reliable Software Technologies**	• 목 적 : 악의적인 모바일 코드로부터 모바일 코드 호스트 소프트웨어와 호스트 시스템을 보호. • 주요개념 : 현재 보호 기법이 알려지지 않은 악의적 액티브 스크립트로부터 모바일 코드 호스트 보호 • 주요기법 - 액티브 스크립트의 행위를 억제함으로써 정상적 기능만 수행하고 호스트나 시스템을 손상시키지 못하게 함. - 윈도우 플랫폼에 액티브스크립팅 API를 설치하여 호스트의 무결성을 보호 - 소스코드에 대한 접근없이 COTS 소스트웨어에 적용 가능
Scaling Proof -Carrying Code to Production Compilers and Security Policies - **Princeton University and Yale University**	• 목 적 : 단말 시스템의 원천적 생존성을 향상하기 위한 모바일 코드 기반구조 개발 • 주요개념 - Necula and Lee's PCC(Proof-Carrying Code) 프로토타입 프레임워크를 실제 프로그래밍 언어, 컴파일러 및 보안 정책에 적용 - 확장성, 상호운용성, 효율성, 보안정책 적용성 등을 그대로 유지하면서 TCP (Trusted Computing Base) 의 크기를 줄임.
Secure Execution of Mobile Programs - **University of California, Davis**	• 목 적 : 분산된 호스트들 사이에 코드와 데이터의 이동을 지원하는 분산 프로그래밍 환경 개발 • 주요개념 - 프로그램 컴포넌트의 이동을 담당하는 유연한 프로그래밍 모델 - 모바일 코드 프로그램으로부터 호스트 자원을 보호하는 접근 제어 메커니즘 - 프로그램에 호스트의 자원을 할당하는 스케쥴링 알고리즘
Semantic Data Integrity - **Odyssey Research Associates**	• 목 적 : 공격당한 후 손상된 데이터로부터 의미있는 정보를 복구하는 효과를 획기적으로 개선하는 도구와 기법 개발 • 주요 개념 - 중복이 있는 부분집합으로 데이터를 나누어 잠재적인 데이터 복구를 지원. - 핵심 성질을 복구 및 검증하기 위한 워터마킹과 self embedding 방법 - 손상되지 않은 데이터 조각을 효과적으로 분별해 내어 사용 가능한 형태로 재생성하기 위한 새로운 알고리즘

6. 결 론

본 고에서는 신뢰성있는 차세대 네트워크 보안 시스템(NG-NSS) 을 정의하고 특성 및 주요 기술을 제시하였다. 신뢰성있는 NG-NSS이란 공격, 취약성, 침입에도 불구하고 일정 수준 이상의 차세대 네트워크 보안 서비스를 지속적으로 제공하는 시스템이다. 이렇게 서비스를 지속적으로 제공하기 위해서는 공격, 취약성, 침입에 대하여 방지, 허용, 대응을 위한 기술들이 필요하다. 신뢰성있는 NG-NSS의 주요 특성은 자율적 보호, 자체 복원, 능동적인 대응 등이며 주요 기술은 안전한 통신 프로토콜 기술, 동적 네트워킹 기술, 공격지 확인 기술 등이다.

네트워크의 보안성, 안정성, 견고성 및 생존성을 높이기 위하여, 시스템 및 네트워크 보안기술과 네트워킹 기술을 통합하여 제공하는 신뢰성있는 차세대 네트워크 보안 시스템은 ISP(Internet Service Provider) 등과 같은 공중망이나 증권, 은행, 보험업계의 전산망 뿐만 아니라, 국방망, 행정전산망과 같은 국가의 중요 네트워크에 적용되어 신뢰성있는 네트워크 환경을 제공할 수 있다.

신뢰성있는 NG-NSS는 ISP의 망관리시스템

(NMS), 트래픽제어시스템, 경로관리시스템 등과 연계되어 필요로 하는 정보의 공유 및 교류를 통해 전역적인 네트워크 차원에서 협력을 함으로써, 궁극적으로 신뢰성있는 네트워크(Reliable Network)를 구축하는데 활용될 것으로 보인다.

참 고 문 헌

[1] Sook-Yeon Kim, Junghoon Jee, Taekyong Nam, Sungwon Sohn, and Cheehang Park "Framework of network security service for next generation," The International Workshop on Information Security Applications (WISA 2002), Jeju island, Korea, 123-130, 2002.8.28-29

[2] "DARPA 의 FTN 사이트," http://www.iaands.org/iaands2002/ftn/index.html

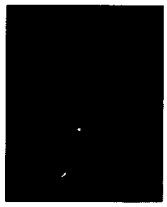
[3] "IST 의 MAFTIA 사이트," http://www.newcastle.research.ec.org/maftia/index.html#partners

[4] "DARPA 의 OASIS 사이트," http://www.tolerantsystems.org/

〈著 者 紹 介〉

남 택 용 (Taek Yong Nam)

1987년 : 충남대학교 계산통계학과 (이학사)
1990년 : 충남대학교 계산통계학과 (이학석사)
1987년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 팀장
관심분야 : 정보보호, 능동보안, 인터넷, 차세대네트워크구조



김 숙 연 (Sook-Yeon Kim)

1991년 : 연세대학교 전산과학과 (이학사)
1993년 : 한국과학기술원 전산학과 (공학석사)
1998년 : 한국과학기술원 전산학과 (공학박사)
1998년~현재 : 한국전자통신연구원 선임연구원
관심분야 : 네트워크 보안, 네트워크 알고리즘, 병렬 처리, 상호연결망

이 승 민 (Seungmin Lee)

1995년 : 고려대학교 산업공학과 (공학사)
1997년 : 한국과학기술원 산업공학과 (공학석사)
1997년~2001년 : 데이콤연구소 연구원
2001년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 연구원
관심분야 : 네트워크 보안, 인터넷, 신뢰성

지 정 훈 (Junghoon Jee) 정회원

1996년 2월 : 한양대학교 전자공학과 (공학사)
1998년 2월 : 한양대학교 전자공학과 (공학석사)
2001년 2월 : 한양대학교 전자공학과 박사과정 수료
2001년 3월~현재 : 한국전자통신연구원 정보보호연구본부 연구원
관심분야 : 네트워크 보안, 이동 코드 기술, 침입탐지기술

손 승 원 (Sung-Won Sohn) 정회원

1984년 : 경북대학교 전자공학과 공학사
1994년 : 연세대학교 산업대학원 전자공학과 공학석사
1999년 : 충북대학교 컴퓨터공학과 공학박사
1983년~1986년 : 삼성전자 연구원
1986년~1991년 : LG 전자(주) 중앙연구소 HI8mm 캠코더 팀장
1991년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장
관심분야 : 네트워크보안, 차세대인터넷, Active Network