主題

인터넷 보안 이슈와 신뢰 보안기술

한국전자통신연구원 네트워크보안연구부 이 승 민, 남 택 용, 손 승 원, 박 치 항

차 례

1. 서론
2. 인터넷의 취약성 분석
3. 취약성에 대한 보안 이슈와 보안 기술
4. 신뢰 보안기술
5. 결론

1. 서론

최근 인터넷을 이용한 사이버 공격이 단순 시스템 위주에서 특정 서비스를 마비시키는 네트워크 공격으로 변화하고 있다. 인터넷 웜을 이용하여 인터넷 서비스를 마비시킨 지난 1.25 인터넷 대란이 대표적인 사례로 볼 수 있다[1-2]. 이는 사이버 공격이 개인의 사생활 침해를 떠나서 국가적인 경제적 손실은 물론이고, 국가 안보와 사회질서를 위협하기까지 이르렀음을 보여주고 있다.

이에 대한 대응방안으로서 보안기술은, 해킹이나 바이러스 등으로부터 정보의 파괴나 왜곡을 방어하는 기존의 시스템 보안 기술만으로는 많은 한계점을 드러내기 시작하였다[1,4]. 사이버 공격의 형태가 시스템 위주에서 네트워크 공격으로 변화하고 있기 때문이다. 국가의 중요한 서비스와 인프라를 제공하고 있는 인터넷 사업자들이 네트워크 보안성 강화에 많은 노력을 기하고 있는 것도 이 때문으로 볼 수 있다.

공격 유형의 변화에 따른 최근의 보안 기술은 네트워크 기반의 고성능 보안장비, 통합보안 서비스, 그리고 글로벌 네트워크에서 외부의 침입을 능동적으로 탐지하고 대응할 수 있는secure networking 기술[1,9-11]로 발전하고 있다. 나아가서 인터넷을 이용하는 사용자 서비스의 품질을 보장하면서 신뢰성을 강화하고 네트워크의 생존성을 만족시키면서, 새로운 공격 유형에 대해서도 유연하게 대처할 수 있는 신뢰 보안기술의 등장이 예상된다[4].

본 논문에서는 안전하고 신뢰적인 인터넷 서비스를 제공하기 위하여, 인터넷의 취약성을 분석한 후 이에 대한 해결책으로서의 보안 기술을 제시하고자 한다. 이를 통하여 향후 보안 기술의 발전 방향을 짚어보고, 이 가운데 핵심기술로 등장할 신뢰 보안기술의 개념 및 주요 기술을 도출하고자 한다.

2. 인터넷의 취약성 분석

본 장에서는 현재 인터넷의 취약성에 대하여 분석하기로 한다. [그림 1]은 일반적인 인터넷의 모습과 영역별 취약성을 도시한 것이다. 영역별 취약성을 살펴보면 다음과 같다.

• 백본영역[2]

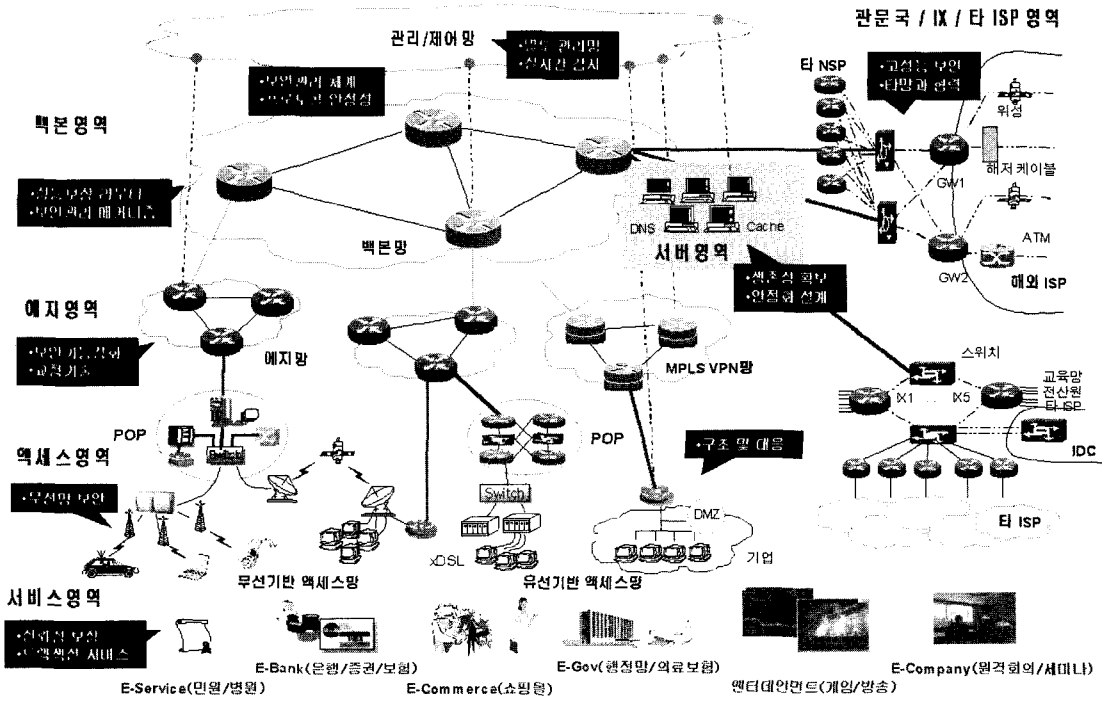
백본영역에서는 성능 보장형의 하드웨어 기반 라우터 부재로 인해 ISP망의 구조적인 병목현상을 유발시키며,

라우터 및 스위치 단에서 멀티캐스트 패킷에 대한 drop 기능 미 설정과 IP 주소 위조 패킷 등 유해 트래픽을 차단할 수 있는 블랙홀(black hole) 및 싱크홀(sink hole) 필터링 기능을 탑재한 네트워크 장비등의 보안 관리 메커니즘이 미흡하다.

또한, 보안관리 전문가 부족, 신속한 대응 및 분석 체계 미흡, 유기적 연동 및 체계적인 유지관리 등의 보안관리 체계가 미흡하며,

인터넷 프로토콜(예:Border Gateway Protocol)의 취약성을 이용한 다양한 공격 가능성이 존재한다.

그리고 라우터의 로그기록 등을 이용한 공격자에 대한 실질적인 역추적 방안이 없으며, 네트워크 노드와 관리시스템간 또는 관리시스템간의 통신 방식이 별도의 전달통로가 없는 in-band 방식을 사용함으로써 트래픽 폭주시 경보 및 제어 신호의 전달이 불가능하다. 또한 악의적인 내부 관리자에 의한 관리시스템으로의 접근은 대부분의 경우 무방비 상태에 놓여 있으며, 실시간 감시 및 조기경보 기능이 취약하다.



[그림 1] 인터넷 구성 및 취약성.

• 서버영역

서버 자체(OS, application 등)에 존재하는 취약성과, DNS 서버, DHCP 서버 등 중요 정보통신 인프라의 안전한 구조 설계 및 가용성 확보(설비 용량 증설, 분산 설치, 백업 체계 구축 등)가 미흡하다.

• 에지영역

에지 라우터의 접속 구조 분산화 및 네트워크 장비의 보안기능, 수용 트래픽량을 고려한 라우터 용량의 증설 및 망 구조의 분산화가 미흡하다. 그리고 스위치 및 라우터 단에서 IP 주소 위조 패킷 등 유해 트래픽을 차단할 수 있는 기능이 적으며, 네트워크 장비에 대한 관리용 포트를 이용한 원격접속(Telnet, FTP, Rlogin 등)에 의한 해킹 가능성이 존재한다. 또한 서비스의 연속성을 방해하는 신속한 복구 방안과 외부 침입에 독립적인 지속적 기능개선으로 시스템의 내성을 강화할 수 있는 방안이 거의 전무한 실정이다.

• 액세스영역

무선영역에서는 무선 단말의 보안과 무선 인터넷 서버의 취약성, 그리고 무선 방송 컨텐츠 보안의 취약성을 들 수 있다. 유선영역에서는 xDSL가입자 수용을 위한 스위치 또는 라우터의 용량 증설, 과다 유입 트래픽의 분산 등 망 접속 구조를 개선하고 보강할 수 있는 방안이 미흡하다[3]. 그리고 ISP와 협약으로 신속한 보안기능 제공 방안이 미흡한 실정이다.

• 서비스영역

사용자의 요구 수준에 따라 사용자가 원하는 서비스를 안전하고 신뢰할 수 있게 보장하는 방안과, 다중 도메인의 트랜잭션 서비스의 시작과 완료시까지 세션의 안전한 유지관리를 위한 보안 관리 기술이 미흡하다.

• 관문국/IX/타ISP 영역

인터넷 기간망 처리 능력은 최고 수십 Gbps임에 반해, 현재의 정보보호 제품의 처리 능력은 최고 수백 Mbps급에 불과하여 성능저하의 우려에 따라 실제 망에 적용하는 데 어려움이 있으며, 타 ISP 및 NSP와 취약성 정보와 외부 침입 정보 등에 대한 공유가 거의 되지 않고 있다. 또한, 역추적이나 패킷 차단 등의 대응 시 타 ISP 및 NSP와의 협력체계가 미흡한 실정이다[2].

3. 취약성에 대한 보안 이슈와 보안 기술

본 장에서는 앞서 살펴본 인터넷의 보안 취약성에 대한 보안 이슈와 이를 해결하기 위한 보안 기술에 대하여 살펴 보기로 한다. 첫째, 매년 인터넷 대역폭의 증가에 따른 주요 백본 라우터의 성능을 통하여 보안 시스템에 요구되는 성능 관점의 이슈를 살펴본다. 둘째, 네트워크 보안 시스템의 기능 관점의 요구 변화를 통하여 향후 보안 이슈로 등장할 교정기술의 필요성을 살펴 보기로 한다. 셋째, 서비스 관점에서 가입자에게 요구될 보안 서비스의 주요 특징을 살펴본다. 넷째, 현재 세계 주요 업체들이 상용화하여 인터넷 백본망에 사용되고 있는 백본용 보안장비에 관하여 적용관점에서 이를 분석하기로 한다.

마지막으로 이렇게 살펴본 취약성에 대한 보안 이슈들을 네트워크 영역관점에서 분류한 후, 이를 통하여 향후 요구되는 보안 기술과 연구 영역을 제시하고자 한다.

3.1 성능 관점의 보안

인터넷 백본망의 대역폭은 1995년 155Mbps에서 2000년 5Gbps로 확장되어 왔으며, 매 2년마다 4배씩 증가하여 2005년에는 100Gbps에 이를 것으로 전망된다. [그림 2]는 년도별 인터넷백본망의 대역폭 증가에 따른 주요 백본 라우터의 성능 예측치와 함께 향후 네트워크 보안 시스템에

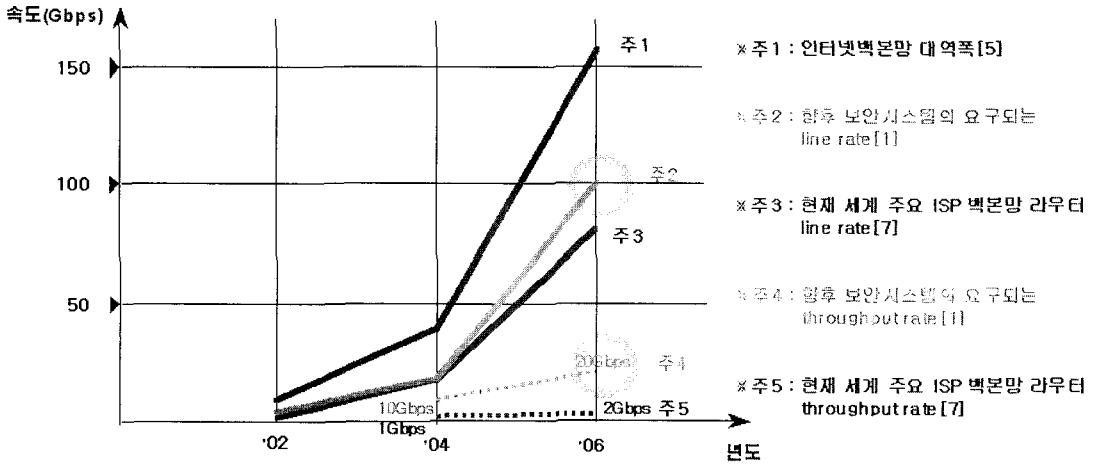
서 요구되는 성능을 예측해 보았다[7].

이에 따라 백본 영역에서는 성능 보장형 보안 시스템의 중요성이 점점 증가하고 있으며, ETRI 대형국책사업의 하나인 "고성능 네트워크 정보보호시스템 개발"사업은 ISP망의 성능 보장형 보안시스템 연구로서 2002년부터 2006년까지 총 5년간 연구개발이 추진되고 있다[1].

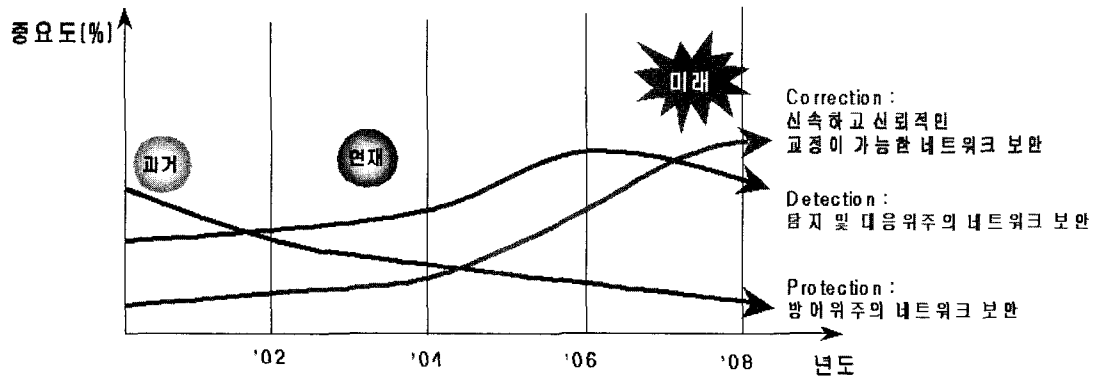
3.2 기능 관점의 보안

인터넷 보안에 대한 기능 관점의 대응 변화는 [그림 3]과 같이 과거에는 외부 공격이나 침입에 대한 방어(예:방화벽) 위주의 네트워크 보안이었다면, 현재는 탐지 및 대응(예:침입탐지시스템)을 통한 네트워크 보안이 주류를 이룬다고 볼 수 있다. 그러나 앞으로는 신속하고 신뢰적인 교정이 가능한 네트워크 차원의 보안 제어기술이 중요한 이슈로 등장할 것이다.

교정기술은 안정적이고 신뢰적인 네트워크를 보장하여 seamless service를 제공하며, 향후 주요 보안 기술의 하나로서 신뢰 보안기술의 근간이 된다.



[그림 2] 인터넷 대역폭 증가에 따른 백본 라우터 및 보안 시스템의 성능 예측.



[그림 3] 네트워크 보안의 기능요구 변화.

3.3 서비스 관점의 보안

인터넷 이용자의 급증과 함께 바이러스, 해킹 등으로 인한 네트워크 침해 사고가 확산되어 서비스에 대한 보안기술의 필요성과 중요성이 증가되고 있으며 책임성 또한 커지고 있다. 그러나 현재의 보안기술은 시스템, 네트워크 수준에서 대응하는 데 그쳐, 안전하고 신뢰성 있는 인터넷 서비스를 제공하는 데 어려움이 있다. 따라서 향후에는 보안이 요구되는 *mission-critical* 서비스에 속하는 사용자 트랜잭션의 안전한 수행과 완료를 보장하기 위해 가변적인 대역폭 할당 및 안전한 다중 경로 제공 기술이 가입자측면의 가장 큰 요구사항으로 등장할 것이다.

이는 사용자 측면의 안정적인 서비스를 보장하기 위한 서비스 관점의 생존성 기술로서, 신뢰 보안기술 가운데 하나이다.

3.4 적용 관점의 보안

주요 업체를 중심으로 인터넷 사업자의 백본망에 적용되고 있는 보안 장비의 특징을 [표 1]과 같이 기능 측면에서 분석해 보았다[12-16]. 현재 주류를 이루는 백본용 보안 장비는 ASIC과 스위치형 하드웨어 기반의 고속 보안 장비라는 점과, 네트워크 기능과 보안 기능의 융합화가 그 특징이다.

그러나, 이와 같은 보안 장비의 적용 관점의 문제는 최소한의 보안 기능(Firewall, VPN 기능 정도)만 제공하고 있으며, 네트워크 차원의 제어 기술과 사용자 서비스에 대한 신뢰성을 보장하지 못하고 있다. 향후에 요구되는 보안기능으로는 침입 트래픽 제어를 위한 성능과 QoS가 보장된 보안 제품으로서, 네트워크 관점의 교정 기술과 사용자 서비스 관점의 신뢰성이 접목 되어야 할 것이다.

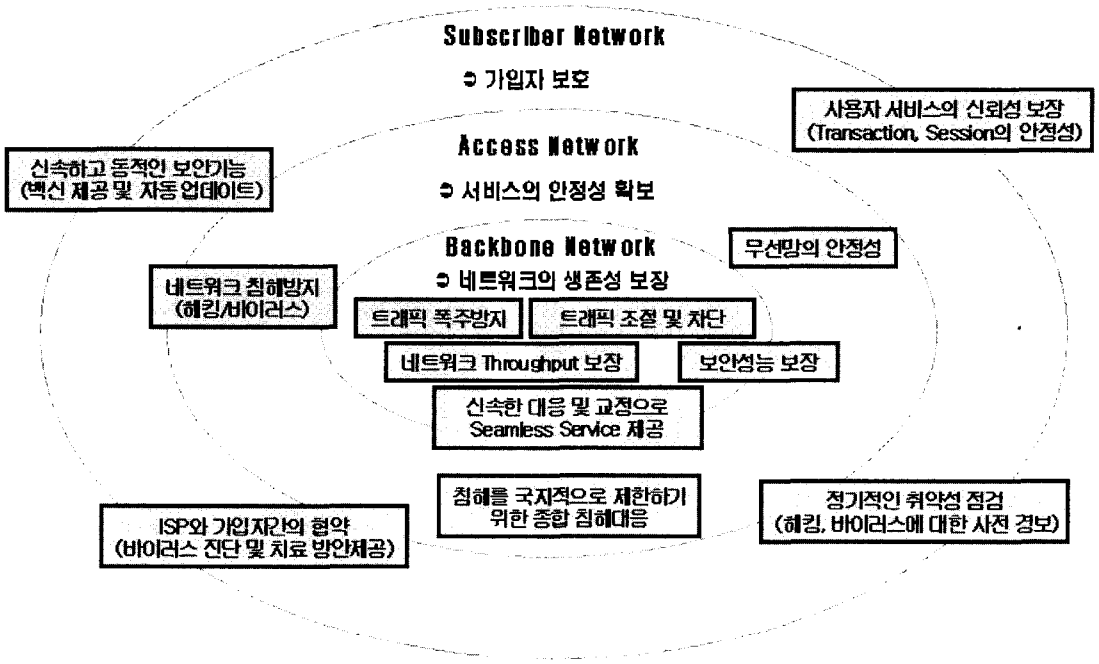
[표 1] 주요 업체별 백본용 보안장비

제품(업체)	주요 기능
Catalyst 6500 (Cisco)	Firewall, IP VPN, MPLS VPN, NAT, ACL, 암호화 등
IP740 (Nokia)	Firewall, VPN, ACL, Secure Administrative Access, SSH, SSL/TLS, Authentication 등
Shasta 5000 BSN (Nortel)	Stateful firewall, IP VPN, MPLS VPN, NAT, DoS Protection, Anti-spoofing, VoIP용 QoS 등
IPSX 9500 Service Processing Switch (CoSine)	Stateful firewall, IP VPN, MPLS VPN, Dial VPN, 안티 바이러스, URL 컨텐츠 필터링, PKI, CAs 등
iQ8000 Service Edge Switch (Quarry)	Stateful firewall, IP VPN, MPLS VPN, NAT, Traffic Classification 등

3.5 네트워크 영역관점의 보안

본 절에서는 지금까지 바라 본 성능, 기능, 서비스 및 적용 관점의 보안 이슈를 포함하여 취약성에 대한 요구사항을 네트워크 영역관점에서 분류 한 후, 보안 기술의 발전방향을 짚어보기로 한다. 이를 통하여 신뢰 보안의 필요성을 제시하고자 한다.

[그림 4]는 네트워크 영역관점의 보안 이슈를 나타낸 것으로, 크게 에지영역과 관문국영역 등을 포함한 백본망과, 액세스망, 그리고 서비스영역을 포함한 가입자망으로 구분하여 각각 요구되는 보안 기술을 제시하였다



[그림 4] 네트워크 영역관점의 보안 이슈

백본망의 경우, 네트워크의 생존성 보장이 가장 핵심적인 보안 이슈로서, 이를 위하여 DDoS 등으로부터 트래픽 폭주 방지, 트래픽 조절 및 차단, 그리고 네트워크의 대역폭 보장 등을 들 수 있다. 그리고 외부 침입에 대한 신속한 대응 및 교정과 성능 보장 보안 제품개발이 또 하나의 보안 이슈로 볼 수 있다.

액세스망의 경우, 가입자의 서비스를 백본망에 안전하게 전달하여 서비스의 안정성을 확보하는 것이 가장 중요한 이슈로 들 수 있으며, 이를 위하여 해킹과 바이러스 등으로부터 네트워크 침해를 방지하고, 국지적으로 침해를 제한하기 위한 대응책이 요구된다. 그리고 무선가입자의 증가에 따른 무선망에 대한 보호가 또 하나의 보안 요구 영역으로 볼 수 있다.

서비스영역이 존재하는 가입자망의 경우, 점점 사용자 서비스에 대한 신뢰성을 보장하는 것이 가장 중요한 보안 이슈로 등장하게 될 것으로 보인다. 이는 유무선 통합과 음성과 데이터의 통합으로 서비스 융합이 본격화 되는 시점에서 가장 핵심적인 요구 사항이 될 것이다[8].

이와 같이 분류한 보안 기술에 대하여 트래픽 폭주방지, 네트워크 throughput 보장, 신속하고 동적인 보안기능, ISP와 가입자간의 협약, 정기적인 취약성 점검 등은 현재 ISP와 주요 장비업체에서 개발 및 상용화가 활발히 진행 중에 있으며, 무선망의 안정성등에 대해서는 확대개발 추진해야 할 분야로 볼 수 있다. 네트워크 생존성 보장을 위한 트래픽 조절 및 차단, 보안 성능 보장, 네트워크 침해방지, 침해를 국지화 하기 위한 종합 침해대응 등의 기술은 secure networking 기술분야로서 ETRI를 비롯하여 여러 기관에서 활발한 연구가 진행되고 있다[1,9-11].

그리고 seamless service 제공을 위한 네트워크 차원의 신속한 대응 및 교정과 사용자 서비스의 신뢰성 보장을 포함하는 "신뢰 보안기술"은 신규 연구가 필요한 개발 분야로서 4 장에서 논의하기로 한다.

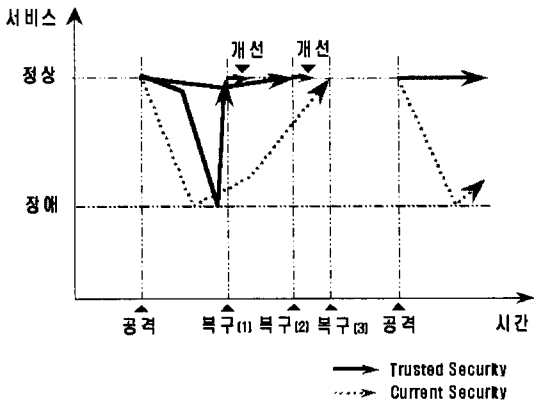
4. 신뢰 보안기술

현재의 인터넷은 DDoS등의 공격으로 인한 네트워크내 트래픽 폭주가 발생할 때, 신속하고 정확한 대응을 위한 제어가 불가능한 태생적인 한계를 지니고 있으며, 이에 대응하기 위한 현재의 보안 기술은 시스템과 네트워크 수준에서 대응하는 데 그쳐, 안전하고 신뢰성 있는 인터넷 서비스 제공이 어렵다. 따라서, 사용자 서비스 레벨의 신뢰성 제공 기술과, 인터넷 마비 사태에 대한 신속한 교정을 가능하게 하는 네트워크 차원의 제어기술의 필요성이 증가하고 있다.

신뢰 보안기술이란 이와 같이 외부의 공격이나 침입, 취약성에도 불구하고 사용자 서비스에 대한 신뢰성 보장과, 네트워크의 생존성을 보장하기 위한 보안기술로 정의할 수 있다. 단, 본 장에서는 신뢰 보안기술 가운데 사용자 서비스의 신뢰성 부분을 제외한 네트워크 차원의 생존성 보장 부분을 중심으로 신뢰 보안의 개념과 주요 기술을 설명한다. 즉, 신뢰 보안을 위한 네트워크 차원에서 제공해야 할 교정기술을 중심으로 살펴보기로 한다.

4.1 신뢰 보안의 개념

신뢰 보안을 위한 네트워크 차원의 교정기술은 복구(recovery) 기술과 개선(improvement) 기술을 이용한 네트워크 생존성 기술이며 네트워크의 가용성 보장을 위한 제어기술로 정의할 수 있다.



[그림 5] 신뢰 보안기술의 개념

[그림 5]는 신뢰 보안을 보장하기 위한 네트워크 차원의 복구기술과 개선기술의 개념을 나타낸 것으로서 기존 보안과의 차이를 보여준다.

기존 보안기술로는 외부의 공격이나 침입 등으로부터 급격한 네트워크 마비 사태를 초래하여 서비스 장애를 유발시키며, 정상 서비스로 복구되는 데 비교적 긴 시간이 소요된다. 또한 네트워크 마비를 초래한 공격이나 침입이 지속되거나 재발할 경우에도, 이에 대한 적절한 대응 방안이 없이 안정적인 서비스를 보장하지 못하는 한계점이 있다.

반면, 신뢰 보안 기술은 외부의 공격이나 침입 상황에서도 네트워크 차원에서 정상적인 서비스를 제공할 수 있는 생존기술과, 대처가 불가능하여 서비스 장애를 초래했다고 하더라도 이에 대한 빠른 서비스의 복원을 가능하게 하고, 기능 개선을 통하여 재발 방지를 포함하는 개념이다.

복구기술은 시스템 복구를 포함한 네트워크 차원의 복원기술로서, 외부의 공격이나 침입, 취약성 등으로 인한 네트워크의 비가용성을 최소화하기 위하여, 네트워크 차원에서 여분의 차원을 활용하여 최대한의 네트워크 서비스를 보장할 수 있도록 하는 네트워크 생존성 기술([그림 5]의 복구[2] 참조)과, 생존성 기술로는 대처가 불가능

하여 네트워크 시스템의 장애가 발생한 경우, 빠른 서비스 복원을 가능하게 하는 네트워크 제어 기술([그림 5]의 복구[1] 참조) 이다.

개선기술은 복구기술의 한계를 보완하는 기술로서 네트워크의 비가용성을 초래하는 외부의 공격이나 침입이 지속되거나 재발할 경우에도 이를 방지할 수 있도록 한다([그림 5] 참조). 구체적으로 외부 시스템으로부터 네트워크의 가용성을 저하시킨 원인을 전달 받아 시스템의 기능을 동적으로 변경하여 개선하거나, 시스템 내부에 침입 평가 및 제어기능을 가지고 동일한 침입에 대한 자체 방어기능을 보유하고 있다.

4.2 신뢰 보안의 주요기술

본 절에서는 신뢰 보안기술을 구현하기 위한 주요 기술을 복구기술과 개선기술로 분류하여 살펴보기로 한다.

복구기술은 외부의 공격이나 침입, 취약성과 같은 서비스의 장애요인으로부터의 네트워크 차원의 생존성 기술로서 시스템 컴포넌트 랩핑기술, 보안자원 관리기술, 동적 네트워킹 기술, 시스템 적응력기술, 프로파일 저장 및 미러링기술 등이 있다.

- 컴포넌트 랩핑기술
  시스템 내 주요 기능을 수행하는 소프트웨어 컴포넌트에 대해 랩핑기술을 적용하여, 컴포넌트의 생존성을 보장하는 기술이다.
- 자원 관리기술
  위험 상황시에 보안 서비스를 신뢰성 있게 지원하기 위하여 주요 자원을 관리하며, 보안 서비스가 적합한 수준으로 원활히 제공될 수 있도록 한다. 시스템의 성능 저하가 발생할 경우에 전체 네트워크 차원에서 동일한 기능을 수행 할 수 있도록, 자원 재할당, 자원 복제와 자원 동적 협동 등이 포함된다.
- 동적 네트워킹기술
  위험상황에 대처하기 위한 전체 네트워크 차원의 기술이다. 동적 라우팅 설정을 통한 논리적인 보안 overlay 네트워크 생성 및 네트워크의 신뢰성을 지원하기 위한 네트워크 서비스 자체에 대한 복제 및 분할기술이 여기에 해당된다. 여기서의 복제는 위험상황에 대처하기 위한 여분의 자원을 예비하는 것이며, 분할은 네트워크 침입의 영향이 전체 네트워크 서비스의 안정성에 영향을 미치지 않도록 하기 위한 조치를 의미한다.
- 시스템 적응기술
  시스템의 신뢰성을 지원하기 위한 시스템 자체의 동적 적응 기술을 의미한다. 성능이 저하될 경우, 제한된 자원을 최대한 활용하여 최대한의 기능을 수행할 수 있도록 한다.
- 프로파일 저장 및 미러링기술
  시스템의 장애가 발생할 경우를 대비하여, 시스템의 중요 프로파일 저장 및 재설정을 위한 미러링기법을 이용하여 빠른 복구를 가능하게 한다.

개선기술은 복구기술의 한계를 보완하여 네트워크의 비가용성을 초래하는 외부의 공격이나 침입으로부터 장애발생 요인을 제거하여 방지하는 기술로서, 보안 수준 측정기술, 침입평가기술, 데이터 마이닝기술, 동적 기능 적용기술 등이 있다.

- 보안 수준 측정기술
  시스템내의 보안 자원과 보안 기능의 상태를 감시하여, 보안 자원으로 제공되는 보안 서비스를 질적으로 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 초

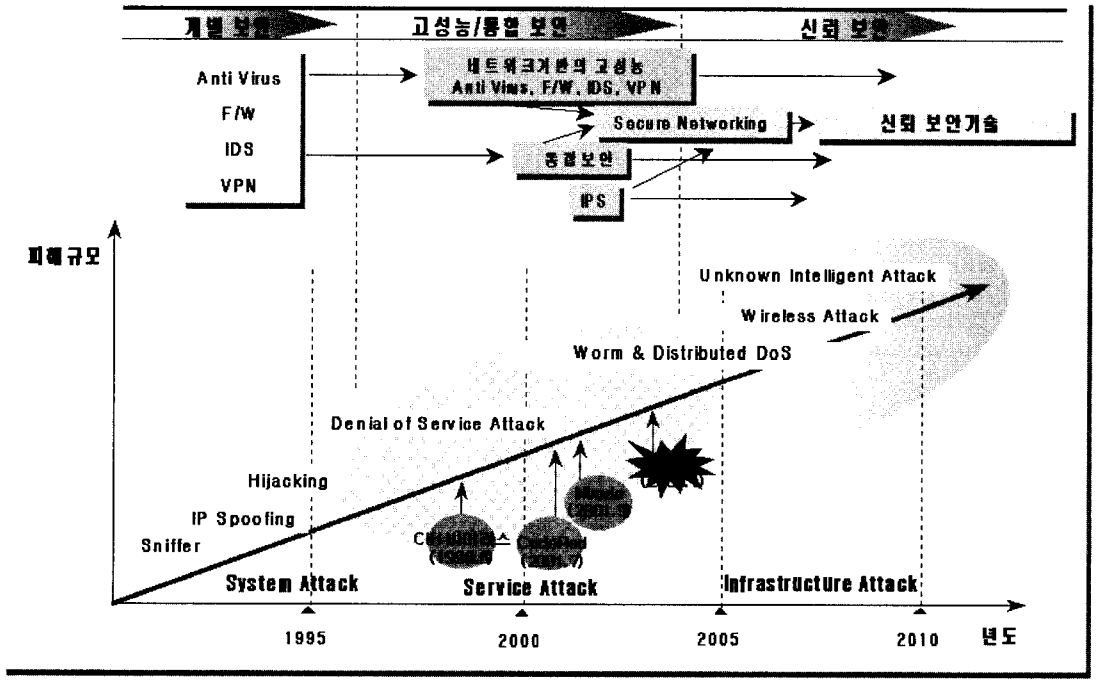
래한 네트워크 공격을 사전에 차단하기 위한 것이다.

- 침입 평가기술
  보안 시스템 자체에 대한 침입이나 타 시스템에 대한 공격으로 인한 간접적인 영향에 대하여 시스템 차원의 대응을 하기 위해서는 현재 진행중인 침입의 정도를 정확하게 평가하는 기술이다.
- 데이터 마이닝기술
  외부 시스템(취약성 분석, 침입탐지, 망관리, ESM 등)으로부터 네트워크의 개선 정보를 전달 받아, 이를 분석하여 시스템에 적용하기 위한 데이터 분석 및 상관관계 판별 기능을 제공한다.
- 동적 기능 적용기술
  시스템의 기능과 성능을 지속적으로 개선하기 위하여 Open API, 동적보안플랫폼을 제공하여 동적으로 기능적용이 가능한 환경을 제공한다.

4.3 향후 전망

보안기술은 인터넷에 대한 외부의 공격이나 침입, 네트워크의 취약성 등에 대한 방어기술로서 발전하여 왔다. [그림 6]은 이를 나타낸 것으로서, 시대흐름에 따른 공격형태의 변화가 1990년 중반까지 시스템 공격이 주류를 이루었으나, 1990년 후반부터 최근까지 공격유형은 서비스 마비를 목적으로 하는 인터넷 웜이나 DDoS 공격이 등장하게 되었다. 2003년 이후로는 이러한 공격을 포함하여 서비스를 전달하는 네트워크 인프라 자체에 대한 피해를 초래하는 새로운 공격 유형이 등장할 것으로 보인다.

이러한 공격에 따른 대응차원의 보안기술은 초기에 방화벽, 침입탐지시스템, 가상사설망 등의 개별보안이 주류를 이루었으나, 1990년대 중반 이후부터는 네트워크 기반의 고성능 장비의 출현



[그림 6] 바이러스, 해킹 대응을 위한 보안기술의 발전추세

과 통합보안, 침입방지 등의 형태로 발전하였다. 2002년 이후로는 이러한 보안 기술들이 글로벌 네트워크 환경에서 네트워크에 대한 침입을 능동적으로 탐지하고 대응할 수 있는 secure networking 기술로 진행되고 있다. 대표적인 secure networking 관련 기술은 ETRI의 대형사업 가운데 하나인 "네트워크 종합 침해대응시스템(사업명:고성능 네트워크 정보보호시스템개발"을 들 수 있다. 그 뒤를 이어 신뢰 보안기술은 사용자 서비스에 대한 신뢰성을 보장하고 네트워크의 생존성을 동시에 만족시키면서, 새로운 유형의 공격에 대해서도 유연하게 대처할 수 있도록 진화할 것으로 예상된다.

5. 결론

본 논문에서는 안전하고 신뢰적인 인터넷 서비스를 제공하기 위하여, 인터넷의 취약성을 분석하고, 이에 대한 해결책으로서의 보안 기술을 살펴보았다. 그리고 이를 통하여 향후 보안 기술의 발전 방향을 짚어보고, 이 가운데 핵심기술로 등장할 신뢰 보안기술의 개념 및 주요 기술에 대하여 살펴보았다.

신뢰 보안기술은 크게 e-government, e-commerce, e-bank, e-company, e-service 등에 활용되어 특히, 사용자 서비스에 대한 신뢰성을 보장하고, 네트워크의 생존성을 보장하며, 향후 ISP망 등과 같은 공중망이나 증권, 은행, 보험업계의 전산망뿐만 아니라, 국방망, 행정전산망과 같은 국가의 주요 기간망에 적용되어 신뢰할 수 있는 네트워크 환경을 제공할 수 있을 것으로 기대된다.

참고문헌

[1] 정통부, "고성능 네트워크 정보보호시스템 개발계획," 2003.4.

[2] 정통부, "네트워크 기반 정보보호체계 구축 계획(안)," 2003.2.

[3] 정보통신망침해사고합동조사단, "정보통신망 침해사고 조사결과," 2003.2.

[4] 남택용, 김숙연, 이승민, 지정훈, 손승원, " 신뢰성 있는 차세대 네트워크 보안 시스템," 정보처리학회지, 제13권, 제 1호, 2003.02.

[5] "차세대 통합 네트워크기술 워크샵," NGcN 2002.10.

[6] 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), p.123-130, Jeju island, Korea, 2002.8.

[7] J.Pescatrore, M. Easley, R.Stiennon, "Network security platform will transform security markets," Gartner, Nov. 2002.

[8] "State of the NGN : Carrires and vendors must take security seriously," Gartner, March 2003.

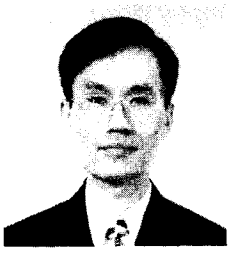
[9] DARPA FTN, http://www.iaands.org/iaands2002/ftn/index.html.

[10] DARPA OASIS, http://www.tolerantsystems.org.

[11] IST MAFTIA, http://www.newcastle.research.ec.org/maftia/index.html#partners.

[12] Cisco, http://www.cisco.com/en/US/products/hw/switches/ps708/index.html.

[13] Nokia,
http://www.nokia.com/product_catalog/pc_subcategory/1,6935,38669,00.html.
[14] Nortel,
http://wwww.nortelnetworks.com/products/01/shasta/index.html.
[15] Cosine,
http://www.cosinecom.com/switches/index.html.
[16] Quarry,
http://www.quarrytech.com//products/iq8000.shtml.

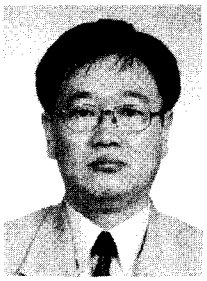


이 승 민
1995년 : 고려대학교 산업공학과 공학사
1997년 : 한국과학기술원 산업공학과 공학석사
1997년~2001년 : 데이콤 종합연구소 연구원
2001년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 연구원

관심분야 : 네트워크보안, 인터넷, NGN

남 택 용
1987년 : 충남대학교 계산통계학과 이학사
1990년 : 충남대학교 계산통계학과 이학석사
1987년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 팀장

관심분야 : 정보보호, 능동보안, 인터넷, 차세대네트워크구조



손 승 원
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 Internet

박 치 항
1974년 : 서울대학교 응용물리학과 이학사
1980년 : 한국과학기술원 전자계산학과 이학석사
1987년 : 파리6대학 전자계산학과 공학박사
1974년~1978년 : 한국과학기술연구소 연구원
1978년~현재 : 한국전자통신연구원 정보보호연구본부 본부장
관심분야 : 네트워크보안, 멀티미디어시스템, 미들웨어, 모바일 에이전트 구조