韓國 OA學會 論文誌
第3卷 第4號, 1998. 12.

98-3-4-3-7

효율적인 네트워크 보안시스템 구축에 관한 연구

정 한 열*

A Study for the Efficient Constructure on Network Security System

Han-yeol Jeong*

요 약

기업 업무 효율이나 정보화를 위하여 우리나라의 기업, 대학등에서는 네트워크망을 구축하고 있는데, 대부분 보안에 대한 자문없이 시공회사에서 획일적인 솔루션을 제공하고 있다. 이로 인해 여러 가지 보안 문제가 발생하고 있다. 본 연구에서는 차단시스템, 암호화시스템, 인증시스템 등 세 가지 정보 보안 시스템을 중심으로 효율적인 네트워크 보안시스템 구축 방법을 기술해보았다.

Abstract

Many Company or college construct the network for the office efficient and information but they construct the total solution from vendor without security consultant. It makes many security problems. In this paper, I expalaned the network security system method from the three information security system that block system, encryption system, authentication system

* 경원전문대학 사무자동화과 겸임교수
논문접수 : 98.11.12. 심사완료 : 98.12.16.

1. 서 론

인터넷이나 원거리 사용자 Dial-In을 통해 사설 네트워크와 외부 네트워크 사이에 양방향 통신을 할 수 있는 길이 열리면서, 민감한 내부 자원의 보안을 위해 견고한 보안 정책이 필요해지고 있다. 특히 연구소나 기업 등의 시스템이나 네트워크망까지 불법 침입 및 침입 후 시스템에 대한 여러 가지 불법 행위 사례들이 종종 발생하고 있기에 개방된 네트워크인 인터넷을 기반으로 정보 시스템을 구축하려면 안정적인 정보보안시스템이 뒷받침되어야 한다.

이 때문에 정보 보안은 전자상거래를 구현하기 위한 핵심 기술로 인식되고 있으며, 인터넷 보안 관련 시스템 중에서도 특정 기관의 보안 사고를 막을 수 있는 차단 시스템, 암호화 기술, 인증 기술에 대한 연구 개발 및 구축이 활발하게 진행되고 있다.

미국 시장 조사업체인 제라드 클라우어 마티슨사는 방화벽 소프트웨어 시장은 오는 2천년까지 매년 평균 1백% 이상의 고속 성장을 지속, 2천년초에는 연간 4백만 달러에 이르는 시장규모를 형성할 것으로 전망하고 있다. 또 암호화와 인증 소프트웨어 시장도 방화벽 분야와 비슷한 속도로 시장이 급성장, 2천년대 보안 소프트웨어 시장은 적어도 연간 1억달러 이상의 시장 규모를 형성할 것으로 예측했다.

보안 소프트웨어 시장에 대해 이처럼 낙관적으로 보는 것은 수요의 기반이 되는 전자상거래와 인터넷/인트라넷 등 정보통신 부문의 성장이 앞으로 지속적인 성장세를 탈 것으로 예상되고 있기 때문이다.

본 고에서는 외부 망과의 접속시 내부 망을 보호하기 위한 종합적인 대책을 제시해보고자 한다.

2. 정보보안 기술

정보보안 기술로는 차단기술, 암호화기술, 인증기술 등 크게 세 가지로 구분할 수 있다.

2.1 차단 기술

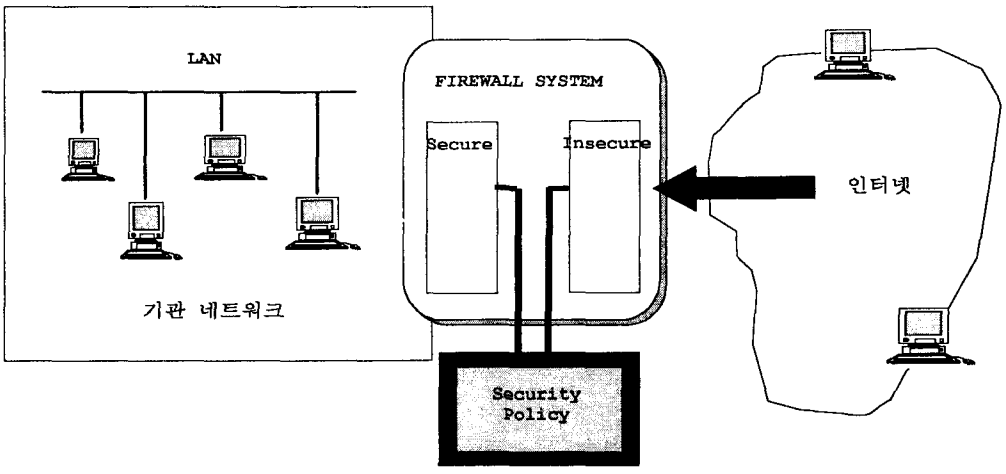

그림 1. 방화벽 시스템
Fig 1. Firewall System

2.1 차단 기술

차단 기술은 네트워크에 대한 불법적인 침입을 사전에 차단하기 위한 소프트웨어 기술로 대표적인 것이 방화벽(Firewall)이다. 방화벽의 사전적 의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는 것을 의미한다. 즉, 인터넷과 LAN 등으로 구축된 네트워크에 인가되지 않은 사용자들이 침입하는 것을 사전에 방지하여 주요 정보를 보호하기 위한 기능을 구현하는 것이다. 물론 방화벽을 구현하는 것만이 완벽한 보안을 보장하는 것은 아니나, 가장 효과적이면서도 비용이 저렴한 방법이라고 할 수 있다.

방화벽 시스템의 기본 목표는 네트워크 사용자에게 가능한 한 투명성을 보장하면서 위험 지대를 줄이고자 하는 적극적인 보안 대책을 제공하는 것이다. 그림 1의 경우는 외부와 내부 네트워크간의 유일한 경로에 방화벽 시스템을 둠으로써 방화벽 시스템이 보안 서비스를 제공하여 불법적인 트래픽을 거부하거나 막을 수 있게 하고 있다. 투명성을 보장하지는 않지만 내부 네트워크를 안전지대로 만들 수 있는 것이다.

방화벽은 이를 구현하는 방법에 따라 패킷 필터링(Packet Filtering) 방식과 애플리케이션 레벨 게이트웨이(Application Level Gateway) 방식으로 나뉘며 최근에는 두 가지 방식이 혼용된 하이브리드 방식, 커널 프록시 방식 등이 있으나 두 방식 모두 기본적으로 패킷 필터링 방식과 애플리케이션 레벨 게이트웨이 방식을 혼용하거나 네트워크 검색을 한 단계 낮은 수준에서 처리하기 때문에 두 방식과 커다란 차이가 없다고 볼 수 있다.

패킷 필터링 방식의 방화벽은 네트워크 접속을 시도하는 모든 경우에 표준 인터넷 프로토콜인 IP주소와 포트 번호를 점검한 다음 필터 테이블로 불리는 규칙을 적용, 인가되지 않은 접근일 때 이를 원천 차단하는 기술이다. 이와 관련, 전체 7계층으로 구성된 TCP/IP Stack 가운데 네트워크 계층에서는 data를 보내는 IP 주소와 목적지 주소를 점검하며, transport 계층은 포트 번호를 확인하고 네트워크 관리자가 정한 필터 테이블의 규칙을 적용해 네트워크 접속 허용 여부를 판단하게 된다. 패킷 필터링 방식은 단순한 보안 방식으로 처리속도가 빠르고 가격이 저렴한 반면 시간대별, 사용자별 특정 애플리케이션 접근 금지와 같은 정교한 네트워크 통제 기능을 제공할 수 없으며 해커가 허가된 네트워크로부터의 패킷을 분석, 발신처 IP를 도용하여 마치 자신이 허가된 네트워크 상의 사용자인 것처럼(IP spoofing) 접근해올 수도 있다. 현재 가장 많이 쓰이는 방식이기도 하다.

애플리케이션 레벨 게이트웨이 방식의 방화벽시스템은 네트워킹중 컴퓨터의 중간에 자리잡고 프록시 서버와 같은 역할을 하면서 보호 대상이 되는 네트워크를 외부로부터 차단해주는 기술이다. 패킷 필터링 방식이 내부와 외부 컴퓨터간 직접적인 통신을 허용하는데 반해 게이트웨이 방식은 안전한 중간자 프록시서버를 통해 양자가 정보를 주고받도록 하고 있는것이 특징이며, IP주소를 외부에 노출시키지 않고 보안기능을 강화할 수 있다는 장점을 가지고 있다. 또한 내부 주소가 외부에 노출되지 않기 때문에 전산팀에서 원하는 숫자를 사용할 수도 있기 때문에 시간과 비용을 절감할 수 있다. 또한 웹(HTTP), 텔넷, FTP, 전자우편 등 원하는 애플리케이션만을 통과시킬 수 있게 트래픽을 제어할 수 있다. 한 걸음 더 나아가서는 특정 애플리케이션을 허용하거나 거부할 수도 있다. 방화벽 차원에서 정교한 통제기능을 제공해주기 때문에 애플리케이션 분배와 같은 특정기능만을 실행하도록 할 수 있으며, 시간대별 사용자별로 특정 애플리케이션에 접근하는 것을 제한할 수도 있다.

따라서 애플리케이션 레벨 게이트웨이 방식의 방화벽은 허용된 애플리케이션마다 특별한 프록시를 요구한다. 예를 들어 실시간 플러그인 리얼 플레이어와 같은 애플리케이션의 경우 별도의 프록시가 없으면 방화벽을 통과할 수 없기 때문에 사용에 불편이 따른다.

결과적으로 이 방식은 유연성이 떨어지고 불편하지만 보안성을 강화시켜주는 장점을 가지고 있다.

2.2 암호화 기술

방화벽과 함께 정보보안의 핵심 요소로 떠오르고 있으며, 문자 생기기 이전부터 개발되어 왔다고 할 수 있을 정도로 오랜 역사를 갖고 있다. 즉, 정보를 보호하고자 하는 인간의 욕구가 그만큼 오랜 역사를 지니고 있다고 볼 수 있다. 이 때문에 암호화 기술 분야에 대해서는 대부분 일정 수준의 대책을 갖고 있는 상황이다.

암호화 기술은 구현 방법에 따라 일정한 약속에 의한 난수표 등을 이용해서 문서를 암호화하는 대칭키 방식과 암호와 복호에 서로 다른 키를 사용하는 공개키 방식, 그리고 hash 알고리듬 등을 이용한 디지털 서명방식 등이 주로 이용되고 있다.

2.3 인증 기술

인증 기술은 네트워크에 Access해 오는 사용자의 신원을 확인한 후 사용 권한을 결정하는 과정을 자동으로 구현하는 것을 말하며, 때에 따라서는 특정 자원에 접속할 수 있는 권한과 접속 시간 등을 강제로 규정할 수도 있다. 인증 과정은 크게 사용자가 미리 알고 있는 것과 사용자가 갖고 있는 것, 고유한것 등 세 가지를 통해 이뤄진다. 사용자가 미리 알고 있는 것을 이용하는 인증 기술로는 대표적인 예가 패스워드방식이다며, 사용자가 갖고 있는 것을 이용하는 인증 기술로는 카드가 있고, 고유한것으로는 지문처럼 신체를 이용하는 방식이다. 이밖에 공인기관으로 부터 토큰을 발급 받는 것도 인증기술의 또 다른 방법이라 할 수 있다.

3. 보안 시스템 구축

3.1 방화벽

방화벽 시스템의 가장 중요한 목적인 내부 네트워크의 보호라는 관점에서 다음의 고려 사항을 염두에 두고 방화벽의 설계 및 사양을 작성하거나, 구현 혹은 설치를 어떻게 할 것인지를 판단해야 한다.

첫째, 해당 조직이 어떻게 시스템을 운영할 것인지에 대한 정책을 반영하는 것으로서, 매우 중요한 네트워크에서의 작업을 제외하고는 접속을 거부하는 시스템을 운영할 것인가 아니면 덜 위협적인 방법으로 접속해 오는 트래픽에 대해 조사하고 점검하는 방식으로 시스템을 운영할 것인가라는 선택한다.

둘째, 어느 정도 수준의 감시, 백업 및 제어를 원하는가 라는 문제이다. 첫번째 문제로서 기관이 받아들일 수 있는 위험 수준이 세워졌다면, 이제 어떤 것을 감시하고, 허용하고, 거부할 것인가라는 체크리스트를 작성해야 한다. 즉, 기관의 전체적인 목적을 결정하고 위험 평가에 근거한 필요성 분석을 하며, 구현하고자 계획하여 사양을 마련했던 목록과 구별될 수 있는 문제점을 가려낸다.

셋째, 경제적인 문제이다. 구매하는데 드는 비용과 유지보수에 드는 비용까지도 정확하게 산출하는 것이 중요하다.

넷째, 기술적인 측면에서 기관 내부의 네트워크와 네트워크 서비스 제공자 사이에서의 고정적 트래픽 라우팅 서비스 등에 대해서 결정해야 한다. 트래픽 라우팅은 라우터에서의 IP 수준의 스크린 규칙이나 혹은 프록시게이트웨이나 서비스에서의 응용 수준 등에서 구현되어야 한다.

다섯째, telnet, ftp, news 등의 프록시를 설치되는 외부에 노출된 기계가 외부 네트워크에 둘 것인가 혹은 하나 이상의 내부 기계와 통신을 허용하는 필터링으로서의 스크린 라우터를 만들 것인가를 결정해야 한다. 프록시는 요구되는 서비스 마다 따로 설계되어야 하며, 편리성과 보안에 드는 비용은 상대적이다.

3.2 암호화

일반적으로 방화벽이 정보교환의 인프라에 해당하는 네트워크 시스템에 불법 접속하는 것을 차단하는 기술이라면 암호화는 정보내용 자체를 보호하는 기술이라고 할 수 있다. 즉, 그림 2와 같이 어떤 기관의 네트워크가 인터넷을 통하여 여러 지역으로 분산되어 있을 경우에 두 지점 사이를 암호 장비를 이용하여 가상 가설 링크(VPL : Virtual Private Link)를 만들어 운영하면 된다.

이러한 암호화 방법으로는 비밀 숫자나 키를 이용해서 단순 텍스트로 구성된 메시지를 암호화 텍스트로 바꿔주는 것을 들 수 있는데, 송수신자가 3라는 암호화키를 서로 나눠 갖고 메시지를 원래 알파벳 순서보다 3자리 앞이나 뒤의 문자(예 HMP→KOR)로 표기해 전송하는 방법을 들 수 있다.

이 방법은 암호와 복호 과정에서 모두 같은 키를 사용하기 때문에 흔히 대칭형 암호화 방식이라고 하며, DES 알고리듬, RC2, RC4 알고리듬이 있다. 그러나 대칭형 암호화 기술은 송수신자가 똑같은 키를 갖고 있어야 하기 때문에 암호화키를 나눠 갖고 보관하는 과정에서 키가 유출될 수 있는 위험이 있으며, 이같은 위험을 줄이기 위해 나온 기술이 송수신자가 서로 다른 암호화키를 나눠 갖는 비대칭형 암호화 방식이다. 즉 암호화 키를 주고받는 위험을 가능하면 줄이기 위해 송수신자가 암호와 복호를 위한 서로 다른 개인 키를 갖게 되며 이와는 별도로 누구나 자유롭게 주고받을 수 있는 별도의 공개키를 갖고 키를 확인하게 된다. 암호와 복호를 위해 송수신자가 갖는 개인키가 다르기 때문 누군가 공개 키를 갖게 되더라도 개인 키가 없으면 암호를 알아낼 수 없게 된다. 대표적인 비대칭형 암호화 알고리듬은 RSA 알고리듬을 꼽을 수 있다.

3.3 사용자 인증

인증 기술은 사용자 신분을 확인해 네트워크 사용 권한을 결정하고 이행하는 과정을 결정하게 된다. 사용자는

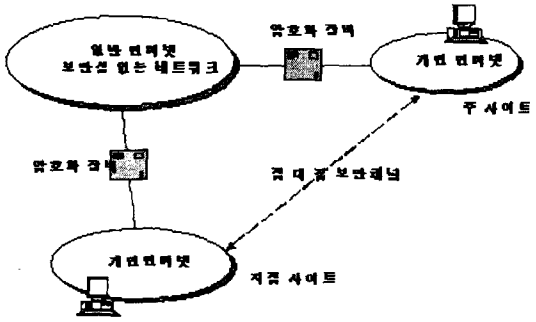

그림 2. 암호 장비
Fig 2. Encryption Devices

인증 확인 절차를 거쳐 접속시간 및 환경에 따라 특정 자원에 접속할 수 있는 권한을 부여받게 된다. 한 예로 네트워크 관리자가 인증과정을 거쳐 회계 담당자가 근무시간에 회계자료를 볼 수 있는 권한을 부여하지만 업무외 시간에는 자료를 열람하거나 인사자료와 같은 업무와 관련없는 정보에의 접근을 금지한다. 그러나 경영자는 언제든 모든 정보에 접근할 수 있는 권한을 부여한다. 따라서 전자신분 시스템의 핵심은 사용자들의 신분을 정확히 확인하는 능력에 달려 있다고 볼 수 있다. 인가된 사용자의 신분을 위조할 수 있다면 누구나 정보에 접근할 수 있게 된다.

패스워드를 이용한 인증시스템이 일반적이지만 유출가능성이 가장 높기에 최근에는 일회용 패스워드 방식이 사용되기도 한다. 물리적인 장치는 패스워드 방식보다 안전하다고 할 수 있지만 분실이나 복사우려가 있다. 일단 네트워크 접속을 시도한 사용자가 접속장치를 훔치거나 혹은 복사했는지를 확인하는 것이 불가능하기 때문이다.

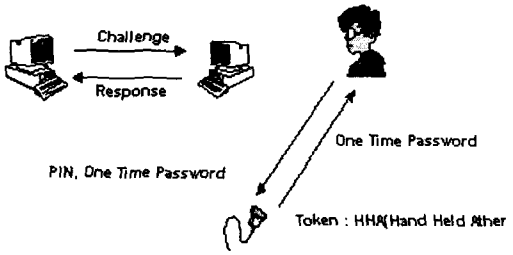

그림 3. 일회용 패스워드 인증 시스템
Fig 3. One Time Password Authentication System

최근에 개발된 지문인식시스템은 물리적 장치와 사용자를 결합하기 위한 시도라고 볼 수 있지만 기술 자체가 초기단계에 있기 때문에 비용에 비한 활용도가 낮다고 볼 수 있다.

각각의 인증 방법마다 장단점이 있기 때문에 두 가지 이상의 인증 요소를 결합해서 인증 기능을 강화하는 것이 바람직하다. 이렇게 되면 불법 인증 확인을 얻기 위해서는 두 개의 독립적인 인증 시스템을 파괴해야만 하기 때문에 그만큼 침투가 어려워지는 것이다. 즉, 패스워드와 물리적 장치를 결합하는 방법이 가장 보편적이라 할 수 있다. 최근 인터넷에서 관심을 끄는 전자 인증은 신뢰성 있는 단체에서 거래 객체의 신분을 확인해준다는데 초점을 맞추고 있다. 서로 상대방의 신분을 확인할 수 있다면 얼마든지 믿고 거래할 수 있기 때문이다.

4. 결 론

지금 까지 차단기술, 암호화 기술, 인증 기술에 대한 네트워크 보안 시스템에 대해 알아보았다. 어떤 기관 내부의 중요 자원을 보호하기 위해서는 보안 시스템을 효과적으로 운용할 수 있는 철저한 보안 대책이 수립되어야 한다. 보안 대책을 세우기 위해서는 무엇보다도 보호할 대상의 선정, 위협요소, 구현 가능한 방법 등을 분석한 올바른 보안 정책을 세우는 일이다. 보안 정책에 따라 네트워크에 대한 관리적, 기술적, 물리적인 보안 대책 뿐 아니라 각 연동 대상별로의 보안 대책을 포함하는 종합적인 보안 체계를 구축해야 한다.

참고문헌

[1] 류경춘, 이요섭, 전문석, 이철희, "가상사설망의 침입탐지 방화벽의 구성", 한국정보과학회 봄 학술 발표논문집 vol. 24. No. 1, 1997

[2] 신훈, 임휘성, 임채호, "인터넷 해킹 수법의 이해 및 대책", 정보과학회지 제15권 제 4호 1997.4
[3] 송의, 김남욱, 이병만, 송관호, "TIS-FWTK를 이용한 방화벽 구현", 정보과학회비 제15권 제4호, 1997. 4
[4] 이성만, 이필중, "방화벽시스템의 구현모델과 취약점", 정보통신보호학회지 제 6권 제4호, 1996, 12
[5] D. Brent Chapman, "Network Security Through IP Packet Filtering", In Proceeding of the USENIX Security Symposium, september, 1992
[6] Karanjit S. Siyan, Chris Hare, "Internet Firewalls and Network Security". NRP, 1995
[7] Professor Ronald L.Rivest "Network and Computer Security", MIT, 1995
[8] Steve Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, vol, 19, no 2, 1989

저자소개

정한열

경기대학교 대학원 경영학과 졸업 (경영학석사)
현재 : 경기대학교 대학원 경영학과 박사과정
현재 : 에스엠컨설팅 수석연구원
현재 : 경원전문대학 사무자동화과 겸임교수