□사례발표□

Internet Firewall (방화벽)

김 정 훈†

◈ 목 차 ◈

요 약

인터넷이란 거대한 네트웍들의 네트웍을 가리킨다. 즉, 각 네트웍들은 개방된 채로 서로서로 연결되는 것이다. 따라서, 이러한 인터넷의 개방성으로 인해 인터넷은 여러 사용자가 손쉽게 자료를 교환하고 자기가 원하는 자료를 찾을 수 있었다. 하지만, 이에 따라 이를 악용하는 해킹의 사례는 점점 더 증가하고 있다. 이러한 해킹 등을 막기 위한 방편으로는 여러 가지가 있지만, 그 중 가장 안전하고 확실한 보안 방안으로써 방화벽이 사용되고 있다. 방화벽 또한 여러 가지 종류가 있지만, 그 중 가장 안전한 방식은 프록시 애플리케이션 방식이다. 이 방식을 사용하는 TIS 사의 건틀릿의 실제 구축 사례에 대해 기술하겠다.

1. 머리말

인터넷 (Internet) 이란 거대한 네트웍들이 모인 것이다. 즉, 네트웍들의 네트웍이다. 인터넷은 원래 미 국방성에서 제안한 알파넷 (ARPANET)에서 시작되었다. 이를 토대로 구성된 TCP/IP (Transmission Control Protocol / Internet Protocol) 프로토콜이 이러한 네트웍들의 표준 프로토콜이 됨에 따라 전세계적인 네트웍이 되었다. 이러한 이유로 인해 인터넷은 몇 가지 특징을 가지고 있고 그에 따라 여러 가지 문제점을 가지게 되었다.

첫째, 개방성이다. 원래 인터넷은 학술 연구의 목적으로 만들어진 네트웍이기 때문에, 모든 사람에게 개방되어 있다. 즉, 모든 사용자는 어떠한 네트웍의 어떠한 호스트에도 접속할 수 있고, 그 호스트의 자료를 사용할 수 있다. 가령 예전의 각 기관들은 guest, sonnim 등의 계정을 만들어 자신의 시스템을 모든 사용자들이 사용할 수 있도록 하였었다. 하지만, 이를 침입자가 이용하여 악의적인 목적으로 사용하는 일이 발생하기도 한 것이다. 더구나 국경 없는 전세계의 전산망으로써 여러 국가들 사이에 문제가 발생할 소지를 가지고 있기도 하다.

둘째, UNIX, TCP/IP 등의 소스 코드가 개방되어 있다. IBM의 SNA 등의 프로토콜은 업체만이

† 정회원 : 콤텍시스템 네트워크팀 사원

보유하고 있으므로, 보안에 큰 문제가 없지만, TCP/IP 프로토콜이나 UNIX 시스템은 많은 학교나 연구소 등에서 소스 코드를 보유하고 있고, 서점에서도 교재로 판매하고 있을 뿐만 아니라, 인터넷에서 이러한 문서들을 무료로 배포하고 있다. 즉, 이러한 문서들이 개방되어 있음으로 인해 악의의 침입자가 소스 코드를 분석해서 보안 상의 취약점을 찾아내 침입할 수 있는 것이다.

셋째, 상호 정보 교환이 쉽다. 인터넷에서는 검열이라는 것이 불가능할 정도로 많은 게시판(BBS)과 온라인 정보 교환을 위한 방법들이 제공되므로, 새로운 침입 방법들이 침입자들간에 손쉽고 은밀하게 서로 교환되어 사용되는 것이다. 또한 어떤 경우에는 정상적인 관리자들을 위해 어떻게 해킹을 당할 수 있다는 경고의 문서를 개방하기도 하는데, 이것이 오히려 침입자들에게 도움이 되는 경우도 있다.

이러한 인터넷의 취약점을 이용하는 침입자들을 보통 해커 (Hacker) 라고 부르는데, 실제로 해커란 네트웍이나 시스템에 대한 전문가를 가리키는 말이었지만, 이 의미와는 다르게 해석되고 있으므로, 보통 악의를 가진 침입자들을 불법 침입자 (Intruder, Cracker) 라고 부르기도 한다. 하지만, 악의의 침입인지 실수에 의한 침입인지 알 수 있는 방법이 없으므로, 보통 침입자를 불법 침입자로 가정하는 것이다.

침입을 방지하기 위한 인터넷에서의 보안의 목표는 아래와 같다.

- 정보의 비밀성 / Information Confidentiality
  - 정보는 안전하고 보안이 유지된 상태에서 전송되어 져야 한다
- 정보의 무결성 / Information Integrity
  - 정보는 전송 도중이나 저장 상태에서 임의로 악의적으로 변경되어 져서는 안된다.
- 정보의 가용성 / Information Availability
  - 정보는 인증된 사용자라면 쉽고 간편하게 사용할 수 있어야 한다.
- 부인 봉쇄 / Non-Reputation
  - 정보의 전송자나 수신자가 자신이 전송/수신을 했음을 부인할 수 없는 메커니즘을 가져야 한다.
- 추적성 / Auditability
  - 시스템에 접속한 실제 사용자가 누구인지 알 수 있어야 한다.

불법 침입자라고 알려진 해커들은 이 중에서 주로 첫번째인 비밀성을 위반하는 경우이다. 비밀성이나 무결성과 가용성은 서로 상충되는 부분이 있어서 비밀성이나 무결성을 보장하려면 가용성이 낮아지게 된다. 그 반대도 마찬가지이다. 이들을 위반한 가장 잘 알려진 해킹 사건은 다음과 같다.

- 스파이 해킹 사건 : 서독 해커들이 서방국의 기밀 정보를 빼내 KGB로 넘긴 사건
- 인터넷 웜 사건 : 자유로이 돌아다니는 바이러스에 7500대 컴퓨터가 감염되어 정지한 사건
- 존 메카트닉 사건 : 2, 3년간 타인을 위조하여 정보를 팔거나 돈을 빼낸 사건
- 씨티은행 침입 사건 : 러시아 해커가 씨티 은행의 계좌를 불법 인출한 사건

이러한 해킹 사례는 외국 뿐만이 아니라, 최근 국내에서도 급격히 증가하고 있는 추세이다 이는 국내의 환경이 열악하기도 하지만, 아직은 관리자들의 인식이 부족하고 보안 시스템에 대한 투자가 적어서 제대로 된 보안 시스템을 갖춘 곳이 거의 없기 때문이기도 하다. 하지만, 이러한 보안 시스템을 아무리 잘 갖춘다고 해도 관리자의 인식이 부족하다면 무용지물이 되고 만다.

2. 구 성

여러 가지 보안 시스템 중 가장 효과적이고 비용이 비교적 저렴하게 드는 방법으로 구현된 것이 바로 방화벽이다.

2.1 보안 시스템의 종류

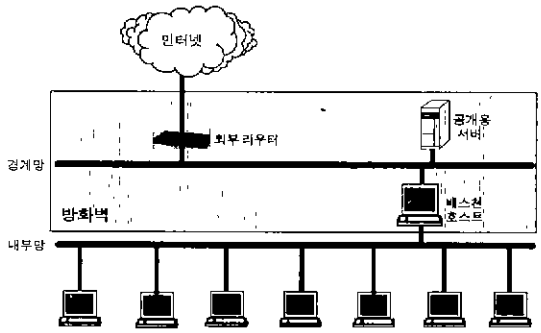
보안 시스템에는 여러 가지 종류가 있다. 가장 간단한 예가 라우터(Router)인데, 라우터의 패킷 필터링(Packet Filtering) 기술을 이용하는 것이다. 이를 이용해서 Router를 통과하는 패킷들의 헤더(Header) 내용을 보고 이 패킷들을 통과시킬 것인지 아닌지를 결정하는 것이다. 하지만, 라우터만으로는 제약점이 많고, 패킷 필터링 규칙이 매우 복잡하므로 라우터만으로 보안 시스템을 구현하는 경우는 매우 드물다.

두 번째로, UNIX나 Windows NT, IntranetWare 같은 네트웍 운영 체제에서도 일부 보안 기능을 제공하고 있다. 현재 대부분의 네트웍 운영 체제들이 보안 표준의 하나인 C2 레벨을 지원한다고 주장하고 있지만, 실제로 완전한 C2를 지원하는 운영 체제는 없는 셈이나 마찬가지이다. 또한, 이런 운영 체제들은 대부분 버그를 가지고 있고, 이러한 버그는 곧 불법 침입자에게 침입하기 쉬운 구멍(Hole)이 될 가능성이 있다.

세 번째로, 단순한 패스워드 인식 기법을 사용하는 UNIX 시스템 같은 인증 방법이 아니라, 보다 강력한 사용자 인증을 위한 사용자 인증 시스템이 있다. 주로 일회용 패스워드(One-Time Password)가 이에 해당된다. 일회용 패스워드란 매번 사용자가 로그인(Login)을 시도할 때마다 새로운 패스워드를 이용하는 것인데, 이렇게 하면 패스워드가 불법 침입자에게 발각되더라도 다음 번 로그인 시에는 다른 패스워드를 사용하게 되므로, 시스템은 안전하게 보호된다.

그리고, 어떤 기관의 네트워크가 공중망을 통해 여러 지역으로 분산되어 있을 때, 두 지점 사이를 암호 장비를 이용하여 가상 사설 망(Virtual Private Network)을 만들어서 운영하는 암호화 장비가 있다.

마지막으로 가장 안전하고, 효과적인 방화벽 시스템이 있다. 물론 위에서 언급한 시스템들은 보통 개별적으로 사용되지 않고 방화벽과 함께 사용되므로, 방화벽 시스템의 한 구성 요소로 간주하기도 한다. 방화벽 시스템은 아래와 같이 구성하는 것이 가장 바람직하다.



외부 인터넷과는 라우터로 연결하고, 경계망과 내부망 사이에 배스천 호스트를 구성하여 내부로 들어가는 트래픽(Traffic)은 반드시 배스천 호스트를 거쳐야 하며 배스천 호스트에서는 허용된 트래픽만을 통과시킨다. 여기서 배스천 호스트가 일반적으로 말하는 방화벽 제품을 가리키는데, 실제로는 라우터와 경계망을 구성하는 허브(Hub), 그리고 경계망에 위치시킬 수 있는 공개 서버와 배스천 호스트를 통칭해서 방화벽이라 한다.

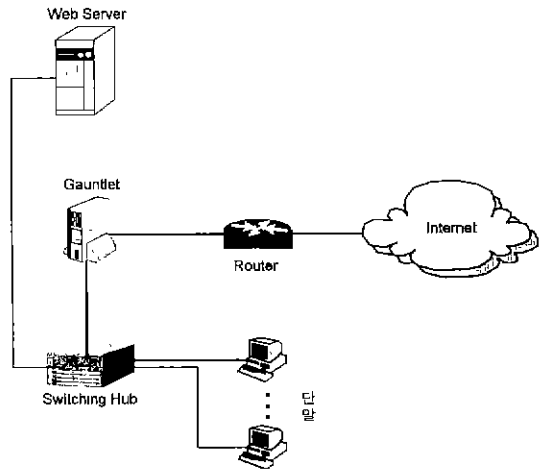
방화벽의 종류에는 패킷 필터링 게이트웨이(Gateway), 서킷(Circuit) 게이트웨이, 프록시/애플리케이션(Proxy/Application) 게이트웨이 그리고 하이브리드(Hybrid) 게이트웨이가 있다. 패킷 필터링 게이트웨이는 앞에서도 언급했던 라우터와 같은 장비의 패킷 필터링 기법을 사용하는 방화벽이다.

저렴하고 뛰어난 성능(Performance)를 제공하기는 하지만, 보안 기능에 제한이 많고, 패킷 필터링 규칙이 복잡해서, 실수로 보안 구멍(Hole)을 만들 가능성이 많다. 서킷 게이트웨이는 주로 내부에서 외부로 나가는 트래픽만을 허용하도록 구성되는 방화벽으로써, TCP(Transmission Control Protocol) 패킷을 처리한다. 방화벽과 내부망의 클라이언트(Client)들이 통신하기 위해서는 특별한 프로토콜을 사용할 수 있도록 클라이언트 소프트웨어를 모두 수정해야 하는 어려움이 있다. 프록시 애플리케이션 게이트웨이는 가장 안전한 방화벽으로써, FTP, Telnet 등의 서비스를 위하여 내부망에 직접 접속하지 못 하도록 하는 프록시를 사용한다. 그리고, 모든 사용자 요청과 응답 등은 로그(log) 화일에 모두 저장되므로, 해킹이 의심될 경우, 그 근원지를 추적할 수 있다. 마지막으로 하이브리드 게이트웨이는 위의 세 가지 게이트웨이를 혼합 구성한 게이트웨이를 가리킨다. 따라서, 이 게이트웨이는 강력한 성능을 제공하기는 하지만, 복잡한 구성과 고가인 것이 단점이다.

이 외에 보안 기능을 도와 주는 도구들이 있다. 이러한 도구들의 종류와 기능은 아래와 같다.

2.2 실제 구성

서울우유의 경우, 앞에서 언급한 점들을 고려해서, 인터넷과의 연동 시에 문제점이 발생할 것으로 판단하고, 방화벽을 설치하기로 하였다. 서울우유의 실제 구성은 아래와 같다.



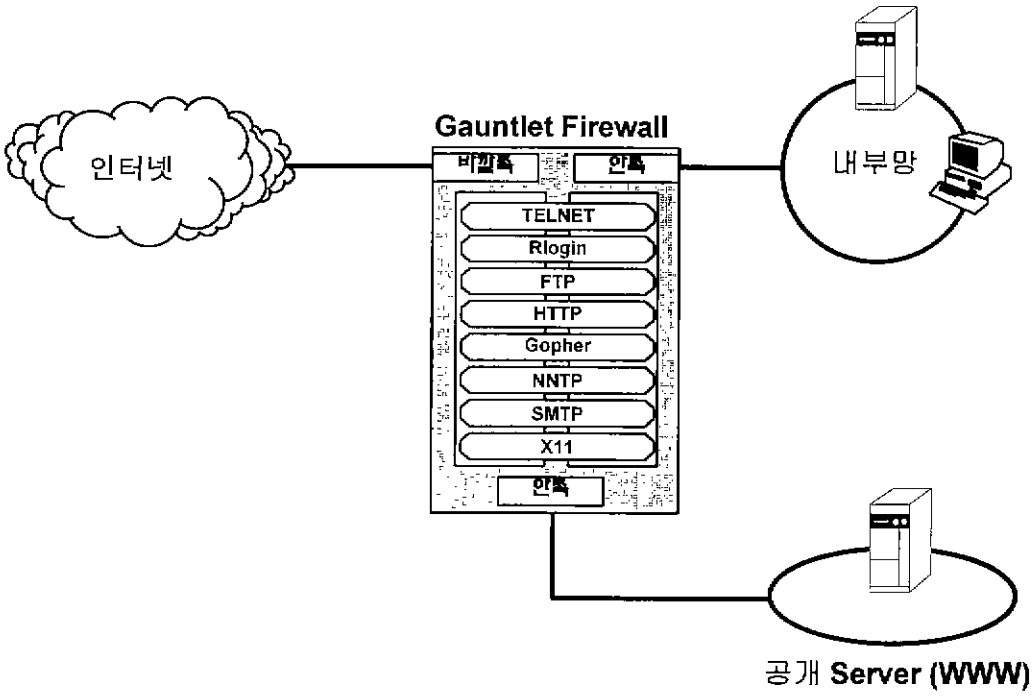
서울우유에서는 따로 경계망을 두지 않고, 내부망을 구성하는 스위칭 허브(Switching Hub)에서 직접 방화벽을 연결한다. 스위칭 허브에서 직접 연결한 것은 단말들이 외부망으로 나가는 통로를 방화벽 방향 하나로 단일화함으로 인해 많은 트

도 구 명	기 능
COPS	일반적인 시스템 보안 점검 및 보고
Tripwire	파일 시스템 무결성 검사
ISS	Internet Security Scanner. 네트워크 호스트 공격 대상 분석
SATAN	네트워크 취약점 공격
Tcpwrapper	네트워크에서의 접근 제어
Crack	패스워드를 알아내는 도구
Sniffer	네트워크상의 패킷 감청/보고
CPM	LAN 모니터링
Swatch	시스템 로그 분석 및 보고 시스템

래픽이 방화벽에 집중되기 때문에, 이를 보완하기 위한 것이다. 하지만, 방화벽으로의 트래픽보다는 라우터에서 외부망 인터넷 등 까지의 속도가 아무리 빠른 링크를 사용한다 하더라도 내부망의 속도보다 빠를 수 없으므로, 실제 방화벽에서의 트래픽 집중으로 인한 병목 현상은 거의 발생하지 않는다. 그리고, 실제로 단말들은 직접 스위칭 허브에 연결되는 것이 아니라, 스위칭 허브로부터 10Mbps를 할당받은 스태커블 허브(Stackable Hub)에 연결된다. 서울우유의 경우, 인트라넷을 위한 웹 서버를 운영하고 있으므로, 방화벽에서는 이것 역시 고려해서 구성해야만 한다.

서울우유에 사용된 방화벽 건틀릿의 내부 구성은 아래와 같다.

건틀릿의 경우, 랜 카드(LAN Card)를 세 개까지 지원하므로, 하나는 외부망 연결용으로 사용하고, 하나는 내부망, 하나는 경계망 용으로 사용할 수 있다. 하지만, 일반적으로 경계망은 방화벽에서 연결하지 않고, 방화벽과 라우터 사이에 구성한다. 서울우유의 경우, 인트라넷 서버가 내부망 내에 있으므로, 아래쪽의 공개 서버는 존재하지 않는다. 따라서, 바깥쪽의 외부망과 안쪽의 내부망 용 카드만을 사용했다. 외부망 인터넷 에서 들어온 패킷들은 건틀릿의 바깥쪽 랜 카드(LAN Card)를 통해 건틀릿 내부의 일치되는 프록시를 통과해서 안쪽으로 전달된다. 이를 위해 방화벽은 패킷의 헤더 안에 있는 서비스 종류에 따라 일치되는 프록시로 패킷을 통과시킨다. 이것은 안쪽에서 바깥쪽으로의 패킷들도 마찬가지이다. 즉, 모든 패킷들은 반드시 건틀릿이 제공하는 프록시를 통과해서 인증을 받아야만 통과될 수 있다. 그래서, 보통 이러한 애플리케이션 게이트웨이 방식을 프록시 게이트웨이 방식이라고 부르기도 한다. 혹은



프록시/애플리케이션 게이트웨이 방식이라고 부른다. 이렇게 할 경우, 어느 정도의 성능 저하가 발생한다. 하지만, 여기서 발생하는 성능 저하는 전체 성능의 약 10% 정도이다. 이 수치는 일반 사용자들은 거의 느낄 수 없는 부분이다. 앞에서 언급했듯이 여기서의 성능 저하보다는 라우터에서 외부망의 링크 속도가 더 큰 성능 저하의 원인이다.

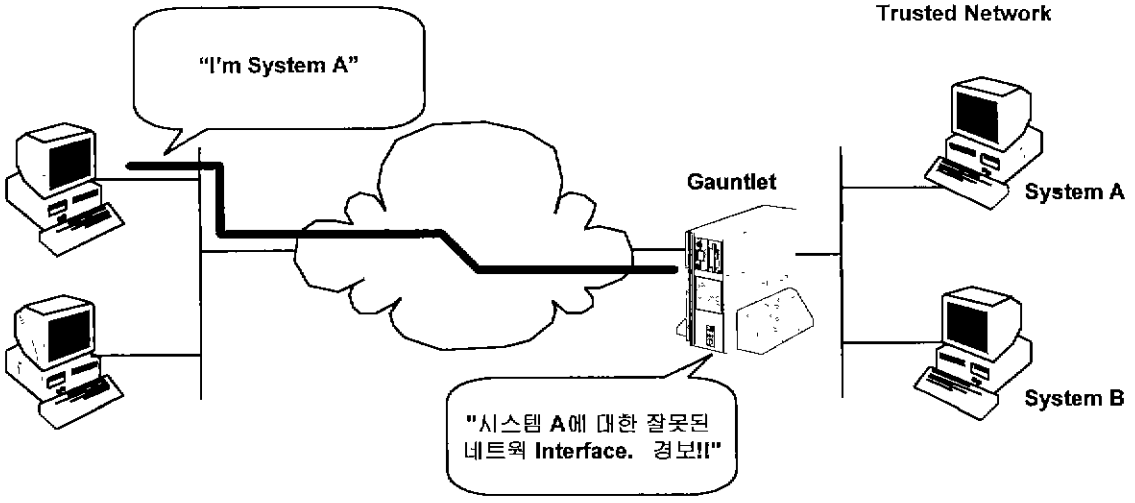
서울우유에 사용된 건틀릿 인터넷 방화벽의 주요 특징은 아래와 같다.

첫째로, 건틀릿은 동등한 네트웍 간에 모든 트래픽을 투명(Transparent)하게 암호화하는 암호화 기능을 제공한다. 하지만, 국내에서 통신 시에 암호화를 하는 것은 허용되지 않으므로, 이 기능을 하는 부분은 실제로 빠져 있다. 둘째로, 클라이언트 상에서 어떤 코드의 변경도 필요하지 않고, 사용자는 실제 건틀릿의 존재 자체를 모른 체 외부망을 사용하도록 구성할 수 있다. 그리고, 건틀릿이 라우팅 요청을 가로채 트래픽을 가로채서 자동적으로 프록시 서비스를 불러낸다. 프록시 서비스는 "가로채기"가 발생한 순간을 인식하고, 자동적으로 연결을 구성한다. 세째로, 대화형 프록시들을 위한 사용자 위주의 승인으로 사용자 권한을 제어한다. 즉, 한번만 사용할 수 있는 암호 등을 제공한다. 그리고, 아래와 같은 IP 스푸핑 (Spoofing) 방어 기능을 제공한다.

즉, 외부망의 한 시스템이 내부망의 한 시스템인양 위장해서 패킷을 전달하려는 경우, 이를 찾아내서 막는다. 다섯번째로, 아래와 같은 다양한 프록시들을 제공한다.

- Terminal Service : TELNET, Rlogin, TN3270
- File Transfer : FTP Proxy
- E-mail : SMTP, POP3 Proxy
- WWW : HTTP, SSL, SHTTP Proxy
- Gopher Proxy
- X-Window System : X11 Gateway
- NNTP Proxy
- R emote Exection : RSH Proxy

- Printing Proxy
- RealAudio Proxy
- Sybase SQL



- Remote Shell
- Authentication Circuit Gateway (다른 Protocol을 위하여 사용자가 제어하는 Circuit)
- Plug Gateway
  - Configuration 설정시 단순한 서비스를 위한 Patch Panel처럼 동작하는 Proxy로서 다음과 같은 서비스를 지원한다.
    - ✓ Finger
    - ✓ Usenet news (NNTP)
    - ✓ Whois
    - ✓ HTTP Proxy Supports Java Guard

마지막으로,. 그래픽 사용자 인터페이스(GUI : Graphical User Interface)를 제공함으로써, 관리자가 손쉽게 건틀릿을 관리할 수 있다.

3. 맺음말

현재 국내 환경이 보안에 대한 관심은 많지만, 아직은 이를 구축하기 위한 기본 지식이나 전반적인 의식이 확립되지 않은 상황이다. 따라서, 지금까지 국내에서 구축된 방화벽은 그렇게 많지 않은 실정이다. 이것은 어떤 방화벽을 설치했는가 하는 것 자체가 보안 사항이기 때문에 잘 알려지지 않은 것도 그 이유이다. 하지만, 점점 더 인터넷에 대한 관심이 높아지고 있고, 각 기업이나 금융권 또는 연구소에서 해킹의 위험 또한 높아짐으로 인해 방화벽을 설치하려는 업체 또한 늘어나고 있다. 하지만, 방화벽을 설치하는 것만으로는 보안이 완벽하게 이루어지지는 않는다.

보안에는 7 단계의 지침이 있다. 첫번째가 외부망과 연결된 통신선로/하드웨어의 보안이고, 두번째가 내부와 외부망 사이의 패킷 필터링을 가리킨다. 세번째는 내부와 외부망의 유일한 통로의 게이트웨이이고 네번째는 내부의 LAN과 LAN 간의 격리이며, LAN 상의 모든 호스트에서의 보안 대책이 다섯번째이다. 여섯번째는 관리자와 사용자 보안 교육 및 인지도 향상이고, 마지막 일곱번째는 인터넷 보안 정책을 수립하는 것이다. 이중 첫번째부터 네번째까지가 OSI 계층의 요구 사항을 만족하는 사항이고, 나머지는 관리자가 관리 대상을 설정하고 그에 따른 보안 대책을 직접 설정하는 부분이다. 이중 가장 중요한 것은 물론 보안 정책을 제대로 수립하는 것이다. 보안 정책이 제대로 되어 있지 않으면, 아무리 강력하고 안전한 시스템을 구축한다 하더라도 보안에 구멍이 생기기 마련이다. 두번째로 중요한 것은 관리자나 사용자의 보안에 대한 교육과 인지도 향상을 위한 노력이다. 실제 중요한 자료의 유출이나 해킹은 내부 사용자에 의한 것이 전체의 2/3가 넘는다. 따라서, 이것이 실제 보안에는 가장 중요하다고 말하는 사람들도 있다. 나머지는 모두 정책 수립과 보안 인식이 제대로 된 이후에라야 제대로 그 기능을 발휘할 수 있다. 하지만, 앞에서도 언급했듯이 국내에는 아직 이러한 환경이 제대로 확립되어 있지 않은 상황이므로, 이런 부분에 대한 고려가 먼저 심각하게 수행되어야 할 것이다.

이러한 부분들이 제대로 확립이 되어 있다면, 좀 더 나은 성능의 방화벽을 구축하려는 관리자의 노력이 또한 필요하다. 서울우유에 설치된 건틀릿의 경우, 애플리케이션 게이트웨이의 가장 큰 단점인 성능과 투명성의 결여를 해결한 매우 유연한 방화벽이다. 방화벽 설치 자체가 보안 사항이므로, 이 수치가 아주 정확하다고 말할 수는 없지만, 건틀릿의 시장 점유율은 전세계의 약 40%를 육박한다. 그리고, TIS 사가 같이 제공하고 있는 방화벽 툴 키트(tool kit)는 전 세계의 방화벽을 제작하려고 하는 업체의 표본이 되고 있다. 그리고, 건틀릿의 경우, 소스 코드를 함께 제공하므로,

요즘 국내에서 우려하고 있는, 방화벽 제작자만이 알고 있는 방화벽 내의 구멍(hole)에 대한 것을 소스 코드를 분석해 봄으로써 이 우려를 불식시킬 수 있다. 또한 이를 이용해서 조직에 알맞은 방화벽으로 그 구성을 조정할 수 있다. 그래서, 현재 국내의 몇 개 업체에서 건틀릿 툴 키트를 이용해서 방화벽을 제작하고 있다. 즉, 이런 소프트웨어 분야에서의 외국에의 높은 의존도를 해결할 수도 있다.

이상과 같이 우선은 보안 정책을 정확하게 수립하고, 그 후 관리자나 사용자 모두 교육을 통해 보안에 대한 인식을 높여야 하며, 그런 후에 알맞은 방화벽을 선정하고 설치해야 할 것이다.

참고문헌

[1] Bellovin, Steve - Security Problems in the TCP /IP Protocol Suite, Computer Communication Review 19(2), 1989; a comment by Stephen Kent appears in volume 19(3), 1989.

[2] Dan Farmer, Wietse Venema, 시스템 공격을 통한 보안 개선 방향

[3] Ranum, Marcus, Firewalls internet electronic mailing list, Sept 1993.

[4] Shimonura, Tsutomu, private communication.

[5] Thompson, Ken, Reflections on Trusting Trust, Communication of the ACM 27(8), 1984.

[6] Trusted Information Systems, Gauntlet Internet Firewall 3.1 Administrator Guide.

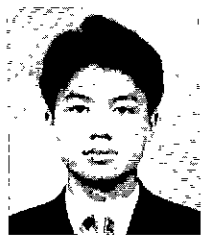
[7] 관리자를 위한 인터네트 보안 지침서 version 1.1~1.3, 시스템 공학 연구소, 1995.

[8] 운영, 보안 그리고 유닉스 Second Edition, 포항 공대 전산소, 1994.

[9] 임채호, *인터네트 보안* 월간 네트워크 타임즈, 1995.1~1995.7.

[10] 전산망 보안을 위한 위험 관리 지침서, 한국전산원, 1994.

[11] 정보화 역기능 현황 및 분석, 한국 전산원, 1994.



김 정 훈

1994년 성균관대학교 정보공학과 졸업 (학사)
1996년 성균관대학교 대학원 정보공학과 졸업 (석사)
1997년-현재 콤텍시스템 네트워크팀 근무