MIS 환경하의 취약점 보완 및 해킹방지 시스템 설계 방안 연구

조만영
고려대학교 정보통신대학원 컴퓨터공학과
e-mail:natural@korea.ac.kr

Designing the System of Crackingproof and Preventing Vulnerability in the MIS

Man-Young Cho
Dept of Computer Engineering, Graduate School of Information Communication, Korea University

요 약

인터넷의 급속한 확산으로 인해 인터넷을 통한 정보교환은 일상생활에서부터 군사 영역에 이르는 특수분야까지 광범위하게 사용되고 있다. 인터넷과 네트워크를 통한 정보의 교환이 일반화 됨과 동시에 정보보호와 정보보안이 큰 사회적 이슈로 대두되고 있다. 본 논문은 기업의 정보소통의 근간인 경영정보시스템(MIS)의 관점에서 정보보안을 바라본다. 인간과 기계를 통틀어 경영정보 시스템의 일부로 생각하며 정보유출의 관점뿐만 아니라 외부 공격으로 인해 전산자원이 낭비되거나 비정상적으로 작동되고 있는지를 파악하기 위한 시스템을 구축하는 방법에 대해 연구하고자 한다. 이에 패킷 스캐닝 방식의 방화벽과 어플리케이션 스캐닝 방식의 방화벽을 상호 비교하여 각각의 작동원리와 장단점을 파악하여 각 기업 고유의 환경에 적용하기 위해 어떤점들을 취사 선택할 것인지 연구한다.

1. 서론

경영정보시스템 보안 관리는 '경영정보시스템(MIS)이 관리자들에게 정보를 제공하기위하여 조직 내의 운용과 경영 및 관리자의 의사결정기능을 지원하는 종합적인 사용자-기계시스템(man-machine system)을 운영하는데 있어서 컴퓨터의 하드웨어, 소프트웨어, 수작업 절차, 분석 및 계획모형, 통제와 의사결정 및 데이터베이스, 모델, 정보통신 등을, 관련 S/W와 H/W를 활용함으로써 MIS가 운영 추구하는 주체의 정보를 보호하고 관리하고 원활케 하는 기능을 수행하는 것'을 말한다.

인터넷의 급속한 확산으로 지금 우리는 과거에 비해 훨씬 많은 정보 속에 살고 있다. 현재는 인터넷을 통해 각종 상품의 정보를 파악하고 정보획득과 동시에 구매도 가능하며 TV, 라디오, 신문에서 제공해 주던 정치, 경제, 스포츠. 사회전반적인 소식들도 인터넷을 통해 실시간으로 제공받을 수 있게 되었다. 이는 우리가 정보의 홍수 시대에 살고 있다고 해도 과언이 아니다. 이러한 환경은 우리의 생활을 예전에 비해 훨씬 풍요롭게 해주고 있다.

그러나 정보가 풍부해진 것이 반드시 정의 효과만이 있는 것은 아니다. Karanjit Siyank & Chris Hare의 연구에서 "근거가 불분명하고 잘못된 정보들로 인해 합리적인 의사결정에 저해받기도 하며 많은 정보들 속에서 정작 우리가 필요한 정보들을 간과할 우려가 있다고 하였다.[1] 특히 해커들의 침입으로 정보가 유출되고 파괴되는 일이 발생되면서 사회에 악영향을 미치고 있다.

2. 정보보안

기업경영에 있어서 정보 보안이란 무엇이며 정보를 보호하기 위한 통제수단은 무엇인가? 불과 얼마 전까지만 해도 정보보안이란 단순히 MIS를 공격하는 해커나 정보 사냥꾼에 대해서만 언급해왔다. 그러나 현재의 정보는 대부분 컴퓨터 즉 인터넷을 통해 제공되며 기업의 입장에서는 경영정보 시스템을 통해 제공되므로 정보보안, 컴퓨터 보안, 정보시스템 보안 즉 기업이나 공공기관에서 생성된 정보를 잘 지키고 유출을 막는 것도 점점 더 중요한 과제로 떠오르고 있다.

D. Brent Chapman & Elizabeth D. Zwicky는 경영정보 시스템 보안의 정확한 개념과 이의 보완을 위한 여러 가지 방안의 모색이며 경영정보 시스템 보안이라 하면 대개 다음과 같이 3가지 요소를 포함한 일체의 경영정보관리 시스템을 말하며 아래와 같은 내용들이 주요한 요소들이라 할 수 있다고 구체적인 사례를 예시했다.[2]

첫째, 사용자-기계시스템(man-machine system)의 안정적인 관리이다. 경영정보시스템은 컴퓨터 등의 정보기술만을 의미하는 것이 아니라 인적자원도 포함하는 개념으로 특정과업은 인간에 의해서 다른 과업은 컴퓨터에 의해 수행되며, 특히 이들을 결합하여 운용하는데 그 특징이 있고 이의 안정성 확보및 보안은 그런 면에서 중요하다.

둘째, 정보이용에 관한 성과적 측면에서뿐만 아니라 자원의 낭비를 방지하기 위한 종합적인 정보시스템계획을 중심으로 한 종합시스템의 성격을 갖는다. 자원의 낭비란 MIS 관할권내에 운영되는 전체 시스템의 효율적 관리와 소프트웨어적인 압축, 해제, 보존을 적절한 선에서 조절하여 운영되는 시스템의 물리적 소프트 웨어적 과도한 설비나 장치및 이에 대한 투자에 대해 적절한 유효성에 입각한 설비및 운영의 합리점을 찾는 것이다.

셋째, 위에서 언급한 경영정보시스템이 종합시스템으로서의 역할을 수행하기 위해서는 자료의 종합관리 및 처리를 가능케 하는 데이터 베이스가 있다. 데이터 베이스의 보안은 얼마 전에도 중국의 구글에서 우리나라 국민의 주민등록번호 데이터베이스가 나와서 말썽이 났는데 데이터베이스의 보안은 현 컴퓨터 운영자 측에서 가장 중요하게 여겨야할 종목이다.[3] 넷째, 경영정보시스템은 데이타베이스의 자료를 기초로 하여 경영의사 결정 모형을 이용하여 의사 결정 업무를 수행하며, 경영자에게 회사 경영에 있어 경영성과에 버금가는 가장 타당성 있는 자료를 제시한다. 다섯째, 경영정보시스템은 포괄적 의미에서 조직의 기능과 경영과정을 광범위하게 지원하는 것으로서 자료 처리시스템을 포함한다.

위의 설명과 같은 경영정보시스템에 대한 입장에서 경영정보시스템(MIS), 정보보안(ISS)이라는 동일 용어를 통해 이론적인 접근하에 기업경영에 필요한 정보시스템의 구축과 정보보안에 대해 정리해 보고자 한다.

3. MIS의 보안관리제안

우리는 전술한 바와 같이 컴퓨터가 없는 세대에 하루도 살수 없으며 또 전세계 수십억이 사용하고 있는 컴퓨터를 보안이 취약하다해서 피하고 사용안할수도 없는 상황에 있다. Marcus J. Ranum,은 이러한 보안관리에 대해서 어떤 기관 내 정보시스템의 위험 관리로서 이해해야 한다고 파악하였다.[4] 보안 대책이란 넓은 의미에서는 하나의 위험 관리적인 측면이 있다. 이것은 마치 시스템 수명(Life Cycle)과 같이 순환적으로 실행되고 관리되어야 하는 것이다.[5] 순서에 맞게 하나씩 보안관리 및 위험 분석을 진행한 후, 이를 구현하고 교육과 인지를 통해 관리하다가 정기적 혹은 비정기적으로 감사 및 사후 관리를 실시하여 적절하게 다시 수정 발전하게 되는 것이다.

여기서의 방화벽 호스트의 구축 방법은 여느 방화벽 프로그램을 분석하여 TIS Firewall Toolkit, Bellcore's S/Key등의 추가 기능을 위한 프로그램을 재료로 방화벽 프로그램의 컴파일과 설치및 프로그램 소스 코드의 수정과 추가, 프로그램 소스 코드의 컴파일링, 프로그램의 설치를 통해 설정 환경을 세팅해보고 패킷 스캐닝 방식의 구축으로 마무리 하려 한다. 정보보안의 허가되지 않은 접근을 막을 수 있는 가장 효과적인 보안 대책은, 허가된 사용자 이외의 모든 접근을 차단하도록 구현된 방화벽을 네트워크 경로에 설치하는 것이다. 아울러 접근이 허용된

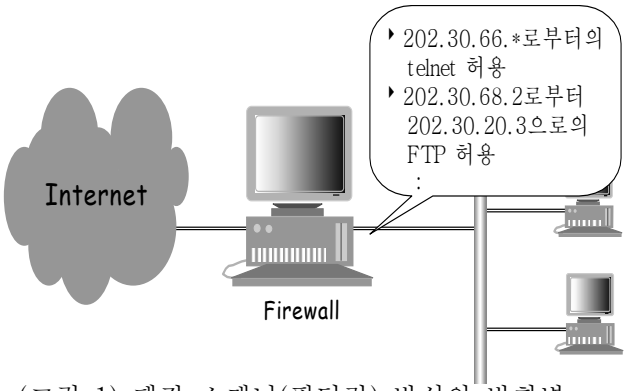
사용자에 대해서도 접근이 이루어진 후의 활동을 감시하고 로그하는 등의 내부 통제가 필요하다. 여기서 논하는 것은 TCP/IP 패킷의 발신지 어드레스와 목적지 어드레스, 요청 서비스를 분석하여 허용 여부를 결정하고, 추가로 사용자 인증 알고리듬을 사용하여 정당한 사용자인지를 판단하는 방법이 사용되고 있는데, 다만 허가되지 않은 사용자가 정당한 사용자로 위장하여 침입을 시도할 경우에 대한 차단 방법을 함께 생각해 보아야 할 것이다.

방화벽은, 일반적으로 네트워크 서비스별로 해당 서비스를 요구한 호스트의 IP 주소와 포트 번호, 사용자 인증에 기반을 두고 외부 침입을 차단하게 된다. 방화벽은 허용된 네트워크 사용자에게 원하는 서비스를 제공하면서 허용되지 않은 사용자에게는 서비스를 차단하고, 해당 서비스의 허용 또는 실패에 대한 기록을 남긴다. 이렇게 서비스를 제공함에 있어서, 방화벽의 종류와 특성에 따라 네트워크 사용자에게 투명성을 보장하지 않을 수도 있으므로 적용 네트워크의 성격에 따라 가장 알맞은 형태의 방화벽을 선정하는 것이 매우 중요하다 할 수 있겠다.

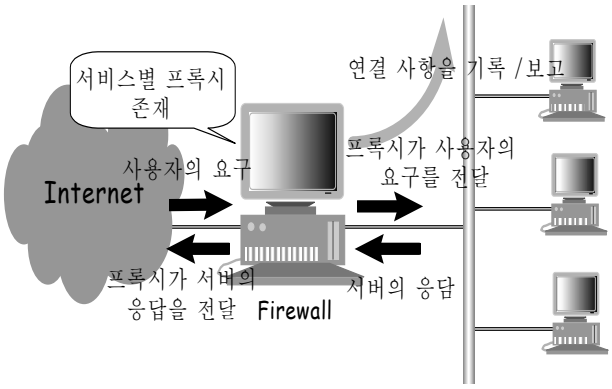
본 논문에서는 외부 네트워크와 연결된 유일한 창구인 Gateway를 통해 들어오는 서비스의 접속 및 거부, 사용자 인증, 내·외부 상호 접속된 네트워크에 대한 트래픽 감시, 기록을 중심으로 정보보안 시스템을 구축하는 방안을 제시한다.

4. 기존 프로그램에 연동 가능한 Packet Scanning(Filtering)의 구축

본 논문에서 연구하고자 하는 방식은 패킷 스캐너 방식이다. 흔히 스캐닝(필터링) 방식이라고도 말하는데 여기서는 네트워크의 OSI 모델에서 네트워크층(IP 프로토콜)과 전송층 (TCP 프로토콜)층에서 패킷을 스캐닝(필터링)하는 기능을 하면서, 패킷에 대한 경로 배정을 위한 자체 프로토콜을 함께 사용하는 형태의 방화벽 시스템으로의 구축이다. 패킷 스캐닝(필터링) 방식의 방화벽은 스크리닝 라우터와 구성하며, 베스천 호스트와 패킷 스캐닝(필터링) 소프트웨어의 양측을 모두 사용할 수 있게 구축하려 시도하려 한다.



(그림 1) 패킷 스캐닝(필터링) 방식의 방화벽



(그림 2) 어플리케이션 스케닝 방식의 방화벽

구현코자 하는 스캐닝 방식의 시스템 기능은 Source / Destination IP Address를 이용한 호스트별, 네트워크별 접근 제어를 가능케 하고 TCP / UDP 포트를 이용한 응용 서비스별 접근 제어, TCP, UDP, ICMP 등 프로토콜별 접근 제어, TCP Sync 비트를 이용한 최초 접근 제어를 가능케 할 수 있다.. 기대되는 시스템의 장점을 살펴보면 패킷 스캐닝(필터링) 방식의 방화벽은 접근 통제 기능이 제 3, 4 계층에서 처리되기 때문에 처리 속도가 상대적으로 빠르고, 사용자에게 투명성을 제공하며, 새로운 서비스에 대해 비교적 쉽게 연동할 수 있는 유연성이 있다. 또한 이제까지 실현되었던 기존의 패킷 블록 방식이나 제어방식보다 구축이 용이하고 기존의 응용 서비스 프로그램에 대한 수정이 필요치 않다는 좋은 점이 있다. 그러나 반대로 생각하면, 제 3, 4 계층에서 처리되기 때문에 모든 트래픽이 IP 패킷 형태로 되어 있어 내부 시스템과 외부 시스템이 직접 연결된다, 데이터가 IP 수준에서 처리되

기 때문에 데이터의 내용에 대한 분석이 불가능하다, 접근 제어를 위한 복잡한 규칙으로 인해 운영상 어려움이 있다, IP 패킷 헤더 내에는 소스, 목적지 주소 및 포트 번호에 관한 정보 등이 들어 있는데, 이들 정보는 해커에 의해 조작이 가하다, (IP 스푸핑 등의 공격 방법), 로깅 및 사용자 인증 기능에 한계가 있다, 한번 공략된 경우 전체적인 보안 규칙이 무너지기 쉬우며, 이러한 경우 전체 네트워크에 미치는 영향이 있을 수 있는 등의 단점이 나올 수가 있다.

모든 방화벽이 치명적인 단점과 장점을 가지고 있다. 적절한 환경과 문제점을 짚어 보고 그 기업이나 자신에게 알맞은 구축시스템은 효율성을 따져 필수적이다. 그림 2에서는 어플리케이션의 방어벽인데 방화벽의 성능이 비교적 떨어지며, 또한 사용자에게 투명한 서비스를 제공하기 어렵다는 치명적인 단점이 있다. 즉 사용자에게 접속 절차의 변경을 요구하거나 (Modified Procedure), 방화벽에서 새로운 서비스를 제공하기 위해서는 새로운 프락시가 추가되어야 하므로 새로운 서비스에 대한 유연성이 떨어진다고 할 수 있는데 이러한 장단점들을 비교하여 설치하는 것도 효율면에서 상당히 고려되어야 할 사항이다.

그래서 이 논문에서 제시하는 패키지 스캐닝 구축 방법을 각 기업이나 기관이 운영하는 시스템의 환경에 맞게 본 논문에서 제시한 시스템의 장단점을 살펴 구축할 때에 고려 사항으로 제시하면 좋을 것이며 이 시스템의 단점에 대한 문제가 없는 기업이나 MIS에서의 활용은 구축비용등에 상대적 경쟁력이 있어 고려해 볼만한 시스템이 될 것이다.

참고문헌

[1] Karanjit Siyank & Chris Hare, *"Internet Firewalls and Network Security"*, New Riders Publishing, 1995, pp 24-34.

[2] D. Brent Chapman & Elizabeth D. Zwicky, *"Building Internet Firewalls"*, O'Reilly & Associates, Inc., 1995, pp 123-135.

[3] 연합통신 , 구글, 중국 정부에 무릎 꿇다 , 2006, 1, 17

[4] Marcus J. Ranum, *"Thinking About Firewalls", Trusted Information Systems,* 2001, pp 56-59

[5] William Stallings, *"Internet Security Handbook", I*DG Books *Worldwide,* Inc., 1996, pp 123-142 / Frederick M. Avolio, *"A Network Perimeter with Secure External Access"*, Trusted Information Systems, 1994, pp 66- 86