

인터넷에서의 시스템 보안은 어떻게 할 것인가?

정태명 / 성균관대학교 전기전자 및 컴퓨터 공학부 교수



인터넷이 보편화되고 있다. 우리나라만 해도 이미 1400만 명이 넘는 인터넷 인구가 있다고 한다. 이러한 인터넷의 성장과 함께 항상 거론되는 것이 인터넷에서의 시스템 보안이다.

아무리 인터넷이 편리하고 좋은 환경을 제공해 준다 할지라도 개인의 정보 혹은 보호되어야 할 시스템 관련 정보가 유출되거나 변조, 혹은 파괴된다면 이는 득보다 실이 많을 가능성이 있다. 따라서, 인터넷과 시스템 보안은 분리시켜 생각 할 수 없는 불가분의 관계에 있다

고 말할 수 있다. 사실상 최근 인터넷에서의 시스템 보안에 관한 여러 가지 위협적인 소식들이 들려오곤 한다. 2000년도 2월에 CNN YAHOO, E-BAY 등의 외국 사이트가 서비스 거부 공격으로 인한 피해를 당한 적이 있다. 국내에서도 얼마 전 강릉의 한 PC방을 거점으로 하여 250여개의 사이트에서 비슷한 서비스 거부 공격을 위한 흔적을 발견한 적이 있을 뿐 아니라, 얼마 전에는 50만 명의 개인 정보가 유출되어서 신문에 보도된 적이 있다. 특히 이번에 일어난 개인 정보의 유출은 대형사고라는 점도 물론 문제가 되지만 경제적인 범죄로 연결되었다는 점에서 더 큰 문제가 있다.

사실상 지금까지의 해킹사건의 많은 것들이 호기심이나 단순한 침입에 그치는 적이 많았으나, 점차

적으로 심각한 경제 범죄로 연결이 되고 있는 추세에 있으며, 이제는 사이버 테러의 목적으로 사용될 것이라고 예측된다. 사이버 테러는 경제적·정치적으로 상당한 피해를 유출 시킬 수 있는 조직적인 범죄 행위이므로 피해자에게 큰 타격을 가져올 것은 자명한 사실이다.

그렇다면 이러한 인터넷에서의 보안 문제를 어떻게 해결할 것인가? 특히 정보가 사용자들 사이에서 공유되는 사이버 아파트나, 대규모 정보를 다루는 공공기관, 해킹의 피해로 경제적인 손실을 가져올 수 있는 전자상거래 업체에서 해결할 수 없는 보안의 문제가 발생한다면, 이는 인터넷의 존재 가치에 대해 회의를 가져오게 할만큼 심각한 상황을 유발할 것임에 틀림이 없다. 따라서 본고에서는 어떻게 인터넷에서 시스템을 보호하고 이러한 피해를 미연에 방지할 수 있을 것인가 하는 것을 생각해 보기로 한다.

시스템의 보안 목적은 우선 두 가지로 정의할 수 있다. 하나는 시스템의 가용성을 유지하여 지속적인 서비스를 제공하기 위한 것이며, 또 다른 하나는 시스템 내의 데이터에 대한 보안을 유지하여 데이터의 유출, 변조, 파괴 등의 피해를 방지하기 위한 것이다. 이러한 보안 목적을 위해서 유기적으로 연결될 수 있는 세 가지 측면, 즉 물리적 보안, 기술적 보안, 관리적 보안의 측면에서 보안 방식을 생각해 보기로 한다.

물리적 보안

우선 물리적 보안이란 시스템이 위치해 있는 환경을 물리적으로 보안하는 것을 말한다. 컴퓨터 시스템의 특성상 컴퓨터에 물리적으로 접근할 수 있으면 그 내부의 데이터는 모두 쉽게 노출될 수 있으므로, 물리적 보안 작업은 단순하지만 아주 중요한 보안 행위이다. 물리적 보안 행위로는 다음과 같은 몇 가지 조치가 있다.

시스템을 외부로부터 격리하고 인가된 자 이외의 출입이나 접근을 통제한다. 시스템을 외부로부터 격리한다는 것은 보호 대상이 아닌 다른 시스템과는 분리해서 설치하여야 한다는 것을 의미한다.

시스템을 재해로부터 보호하기 위한 안전 장치와 전기적 충격으로부터 보호하기 위해 무정전전원공급장치(UPS : Uninterruptible Power System)을 설치하여야 한다. 백업용 마그네틱 테이프나 광저장 장치 등의 미디어는 시스템과 분리하여 보관하며 외부자의 접근을 불허하여야 한다. 특히 백업미디어의 안전한 저장을 간과하는 사람이 많으나, 사실상 백업미디어는 시스템 자체만큼이나 중요하다는 것을 인식하여야 한다.

통신선로상의 중요한 네트워크 장비들의 물리적 보안도 중요하다. 최근에 초고속 인터넷망이 활성화되면서 ADSL이나 VDSL, CATV 등을 이용한 다양한 종류의 네트워크가 형성되고 있다. 이러한 네트워크 장비들은 이제 전산실에 위치하기보다는 사용자로부터 가까운 아파트 단지의 한 곳에 위치하는 경우가 많다. 따라서 물리적인 보안은 이제 전산실로 국한되기보다는 네트워크 장비가 위치하는 곳이면 어디에서나 수행되어야 한다.

기술적 보안

기술적인 보안이란 시스템이 안전하도록 여러 가지 보안 기술을 통해서 시스템을 보호하는 행위를

말한다. 보안을 위해 사용되는 기술은 수십 가지 이상이 있으나, 그 중 대표적인 기술 몇 가지만 살펴보기로 한다.

현재 가장 많이 사용되는 것이 방화벽을 설치해 적용하는 침입차단기술이다. 침입차단기술은 네트워크의 병목에 위치하여 통과시킬 데이터와 그렇지 않은 것을 구분하는 일(필터링)을 수행한다. 통과하는 데이터에 관한 결정은 전적으로 보안관리자에 의해 이루어진다. 또한, 필터링 기술을 이용하여 논리적인 네트워크를 구성할 수도 있다.

침입탐지기술 역시 주목받는 보안 기술이다. 침입탐지기술은 이미 침입하였거나 혹은 침입하려는 시도를 탐지해 내는 기술을 말한다. 기본적으로 네트워크로부터 들어오는 데이터를 살펴보거나 시스템에 기록된 감사 자료를 살펴보는 방법이 사용되며, 때로는 시스템 안에서 일어나는 함수 호출을 살펴보는 기술도 개발되고 있다.

시스템은 침입탐지나 차단 기술처럼 방어하는 기술도 중요하지만 시스템 자체가 보안성을 갖도록 취약점을 제거하는 기술도 중요하다. 그러나 컴퓨터시스템과 인터넷의 특성상 수작업에 의존하여 취약성을 분석하고 제거한다는 것은 거의 불가능하다고 할 수 있다. 따라서, 이러한 분석을 자동적으로 실행할 수 있는 기술이 필요하며, 이를 시스템 취약성 분석 기술이라고 부른다.

바이러스 대응기술은 작년의 CIH 바이러스 사건을 기점으로 유명해진 기술이다. 특히 바이러스의 피해 정도가 점차로 심각해지고 있으며, 변형된 바이러스의 형태가 다양해지고 있으므로 최신 기술의 업데이트가 가장 필요한 기술이기도 하다.

최근에는 데이터를 파괴하고 시스템의 운영 자체를 마비시키는 신종 바이러스가 기승을 부리고 있으므로 바이러스 대응 기술은 철저히 적용되어야 한다.

자료유출 방지 기술은 내부로부터 외부의 사용자에게 중요한 데이터가 유출되는 것을 방지하는 기술을 말한다. 실제적으로 많은 보안 피해 사건은 아직은 내부 사용자에 의해 이루어진다는 것을 기억해야 한다. 따라서 이러한 기술은 중요한 자료가 저장되거나 사용되는 곳에는 필히 설치되어야 한다.

인터넷의 확장과 컴퓨터 기술의 발달은 수작업으로 할 수 있는 일의 범위를 계속적으로 축소시키고 있다. 따라서, 백업과 같은 단순한 작업도 자동화해가고 있으며, 이러한 자동화를 위해서는 먼저 백업 작업이 체계화되어야 할 것이다. 백업의 기술 중 백업데이터의 비밀성과 무결성 보장을 위한 기술 역시 적용되어야 할 것이다.

보안 제품의 자동화와 신속한 대응을 위해 통합된 보안관리기술 또한 적용되어야 한다. 그러나 현실적으로 통합 보안관리기술은 세계적으로 초보의 상태에 있으므로 지속적인 관심을 기울이는 것이 중요하다.

인증기술은 데이터 혹은 사용자를 인증하는 기술로 무결성을 확인하기 위해 주로 사용된다. 데이터 인증은 수신된 데이터와 송신한 데이터가 일치되는 것을 확인하는 것이며, 사용자 인증은 시스템을 사용하려는자의 신원을 확인하는 것이다.

그 밖에도 장애 대처기술이 보안을 위해 필수적이다. 장애 대처 기술은 보안상의 이유로 장애가 일어났거나 일어날 가능성이 있을 때 대처하는 기술로, 우선 보안상의 장애를 사용자에게 알리고 보안 피

해의 경로를 차단하여야 한다. 그 후에 취약점을 제거하고 피해상황을 복구한 후 시스템의 서비스를 재개하게 된다.

권리적 보안

관리적 보안의 영역에는 각종 계정과 데이터를 보안하고, 감사기록을 수집분석하며, 인적자원을 교육하는 일이 포함된다. 뿐만 아니라 보안관리자는 각종 보안 지침과 절차를 수집해서 관리하여야 하며 보안시스템을 운용하고 관리하므로 전체적인 보안의 일차 책무를 담당한다고 볼 수 있다. 다음은 관리적 보안의 영역을 구체적으로 설명한 것이다.

사용자 계정의 비밀성이 항상 유지될 수 있도록 관리하여야 한다. 계정의 관리를 위해서는 비밀번호의 주기적 변경, 추측 불가능한 비밀번호의 선택을 의무화할 수 있는 기능을 제공하여야 한다. 물론, 고급 기술인 홍체 인식, 지문 인식들의 방법을 사용자 인증 방식으로 사용한다면 상기한 방식은 해당되지 않으며, 단지 인증 데이터를 보호하는 것이 필요할 것이다. 감사기록을 수집하고 분석할 뿐 아니라 감사기록 자체를 보안하고 복구하는 작업 역시 시스템 보안을 위해 중요하다. 감사기록을 통해 시스템의 침입 여부를 탐지할 수 있을 뿐 아니라 내부 사용자의 시스템 오남용까지도 찾아낼 수 있기 때문이다.

무엇보다도 시스템 보안에서 중요한 것은 어떻게 보안을 유지할 것인가 하는 것이며 이러한 일은 담당자와 사용자에게 적절한 보안 교육을 실시하면서 이루어진다. 따라서 주기적으로 보안관리자, 시스템 운영자, 사용자에게 보안교육을 펼쳐 실시하여야 할 것이다.

보안지침, 체계 및 백업의 관리 방침을 설정하고 이를 준행하는 일은 시스템 보안과 복구를 위해 필요한 작업이다. 이와 함께 중요한 사항은 보안의 지침은 계속적으로 업데이트 되어야 한다는 것이다. 왜냐하면 시스템 보안에 대한 위협은 계속적으로 변화하며 고급화되고 있으므로, 기존의 보안 체계 및 절차에 안주한다면 곧 쓸모없는 방식으로 전락해 버릴 가능성이 있기 때문이다.

관리적 보안에서 중요한 또 하나는 보안 문제가 발생했을 때의 대처방법을 개발하고 이를 처리할 수 있는 능력을 보유해야한다는 것이다. 일반적으로 보안사고 대처 방법은 다음과 같다.

- 보안 문제의 정도에 따라 필요한 경우 시스템을 통한 서비스를 중지한다.
- 보안 문제의 사항을 모든 관련자에게 알려야하며, 피해 상황을 정보보호센터나 검찰, 경찰 등 관계기관에 알린다.
- 피해 경위와 내용을 정확히 분석하여 피해를 복구하고 재차 피해를 받지 않도록 시스템의 필요한 부분을 수정한다.

이상과 같은 물리적 보안, 기술적 보안, 관리적 보안이 유기적으로 완벽하게 수행될 때 인터넷 상에서의 보안이 가능하게 될 것이다. 어느 한 분야라도 소홀히 된다면 보안의 문제로 인한 심각한 피해를 경험하고, 때로는 복구할 수 없는 폐해를 입게 될 수도 있다.

결론

인터넷은 정보의 변조, 도용, 삭제 등의 침입에 항상 노출되어 있으므로 사실상 인터넷상에서의 서비

스는 범죄의 위협 속에서 실현되는 행위로 볼 수 있다. 때문에 보안의 중요성은 더욱 강조되고 있으며 이를 간과하고는 결코 인터넷 비지니스의 활성화를 기대할 수 없다. 정보통신진흥협회에서는 1999년의 모범상점인증제도를 확대 개편하여 2000년인 올해부터 “인터넷 사이트 안전마크 제도”를 시행하고 있다. 이 제도는 본 고에서 설명하는 시스템 보안의 내용을 준용하는 인터넷 사이트를 선정하고 이를 일반 국민들에게 알려 신뢰할 수 있는 인터넷 세상을 만들고자 하는 데 목적이 있다.

이러한 제도가 정착되고 활성화된다면 누구나 인터넷 안전사이트마크(i-safe mark)를 확인하는 것만으로 부담없이 인터넷을 즐길 수 있게 되리라 생각한다. 그러나 만일 인터넷의 활성화가 이루어지기도 전에 지금처럼 많은 보안 문제가 불거져 나온다면 결국 인터넷은 아무도 사용하지 않는 천덕꾸러기 가 될 가능성도 있다. 따라서 인터넷의 편리성을 계속 유지하기를 원한다면 시스템 보안의 문제는 꼭 해결되어야만 하는 과제이기도 하다.

청소년과 부모·교사가 함께하는

불건전정보차단 소프트웨어 평가대회

사단법인 한국청소년문화연구소에서는 ‘청소년과 부모·교사가 함께하는 불건전정보 차단 소프트웨어 평가대회’를 개최합니다. 청소년과 부모·교사가 한 팀이 되어서 시중에 출시된 차단 소프트웨어를 사용해보고 평가하는 행사입니다. 행사내용과 참가요령은 다음과 같습니다. 청소년과 학부모·교사 여러분의 많은 참여를 바랍니다.

- 일 시 : 2000년 8월 19일(토), 오후 2:00~5:00
- 장 소 : 광운대학교 전산실 (지하철 1호선 성북역 하차)
- 행 사 내용 : 학부모나 교사가 불건전정보차단 소프트웨어를 설치하고 설치된 상태에서 청소년이 인터넷 서핑(학부모, 교사지도아래)→평가서 작성 중·고등학생 1인 + 학부모나 교사 1인
- 참 가 자 격 : 건전 정보문화와 청소년보호에 관심이 있는 분, 컴퓨터 사용능력 무관
- 신 청 : 연구소로 직접 전화접수 ☎(02)734-0701
(선착순 전화접수 마감)