인터넷기반 서비스 보안요구분석

○
성장렬, 김봉회, 박진섭
대전대학교 컴퓨터공학과

An Analysis of Security Requirements on the Internet-based Services

○
Jang-Ryeol Seong, Bong-Hoi Kim, Jin-Sub Park
Dept. of Computer Engineering, Taejon University

요 약

많은 분야에서 계획이나 정보기술전략으로 인터넷에 근거한 서비스를 제공하거나 이용한다. 본 논문에서는 여러 가지 요인들과 함께 조직체들의 업무에서 정보보호에 필요한 사항들을 분석하고 접근하기 위한 방법들을 고려한다. 특히, 인터넷 기반하에서 지원되는 중요 서비스들과 이들 서비스들을 보호하는데 이용 가능한 보안제어수단과의 연계성을 원격접근, 전자상거래, R&D, 인터넷의 가용성 측면에서 보안요구사항을 분석한다.

1. 서 론

대부분의 조직체들은 조직체들간이나 그들의 고객과의 통신지원, 업무의 비용절약, 업무의 자동화를 위한 방법으로 인터넷에 근거한 서비스를 사용한다. 그러므로, 인터넷연동으로 발생할 수 있는 사건들에 대처할 수 있도록 보안요구사항을 고려해야 한다. 여기에서는 인터넷 기반하에 지원되는 중요 서비스들과 이 서비스들을 보호하는데 필요한 보안제어 사항들을 분석한다.

2. 원격접근

사업체들은 점점 더 그들의 정보시스템에 원격접근을 필요로 한다. 이것은 직원이 메일을 읽거나 재택근무, 고객들로부터 원격주문/판매를 가능하게 한다. 그러나, 컴퓨터 시스템에 원격접근을 허용하는 것은 인트라넷으로의 접속점의 증가로 인하여 취약성이 높아진다.

원격접근에서 고려해야 할 내용으로 '원격접근서비스', '원격제어', '원격노드운용' 등이 있으며 각 특징은 다음과 같다.

- 『원격접근서비스』는 일반적으로 전자우편처럼 하나의 서비스를 사용하는 원격작업으로 제한한다. 이런 형태로의 운용방식이 가장 안전하다.
- 『원격제어』는 보안 소프트웨어 프로그램으로 원격사용자를 제한한다. 뿐만 아니라 몇몇 멀티유저를 갖는 원격제어제품은 향상된 감사기능

과 로깅 수준을 지원한다.

- 『원격노드운용』은 원격사용자에게 모든 네트웍 서비스들을 지원하므로, 원격제어소프트웨어를 사용할 필요가 없다. 편리한 원격접근방법이긴 하지만 공동의 시스템들에서 취약성이 높다.

이들 원격접근의 형태는 전화접속, 텔넷 세션을 사용하거나 이동컴퓨팅을 지원하는 소프트웨어제품을 사용하여 이루어진다.

2.1. 전화접속네트워킹

전화회선을 이용한 전화접속은 일반적인 원격접근방식으로 원격컴퓨터는 자동응답모뎀을 다이얼하는 아날로그/디지털모뎀을 사용한다. 이 접속방법은 정보를 보호하기위해서 접속번호를 제어하고 인증하는 수단이 필요하다.

- 전화접속번호의 제어인식 - 이 접근방법은 전화 번호, 위치, 로그 모뎀의 블록들을 검색하는 자동-다이얼 모뎀을 사용하는 소프트웨어의 단순한 부분으로 인해 War dialer(전화번호의 리스트를 호출하고 기록하는 크래킹 툴)에 의한 공격에 취약하다.
- 사용자명과 패스워드 - 내부 네트웍상에서 스니퍼를 이용하거나 사회공학적수단을 이용하는 비기술적인 방법으로 패스워드를 쉽게 획득하거나 추측할 수 있다.
- 향상된 인증 - 패스워드를 보완하거나 교체하는 방법들로는 다이얼-백모뎀, 원타임패스워드, 위치에 기초한 인증 등이 있다. 다이얼-백모뎀은 사용자에게 사용자명과 패스워드를 입력하도록 요구하고 서비스 제공자의 모뎀은 원격모뎀으로 전화를 걸고 접속을 개시한다. 이 접근법은 포워딩 공격에 취약하다. 원 타임 패스워드는 암호법에 기초한 응답시스템을 사용하여 사용자에게 소프트웨어/하드웨어적인 패스워드 생성기를 운용하게 한다. 이 방법을 사용할 때는 세션을 빼앗는 공격에 취약하다. 위치에 기초한 인증은 사용자가 인증된 위치로부터 접속하지 않는다면 접근은 거부된다. 이 기술은 발전 단계에 있고 복잡하고 고가이지만 많은 어플리케이션을 위해 사용된다. 취약점은 공격자가 허위의 위치정보를 가질 수 있다는 것이다. 이런 공격유형을 방어하기위해 암호기법을 사용한다.

2.2. 텔넷

텔넷과 원격 로그인 명령은 네트웍을 통하여 원격적으로 컴퓨터들에 로그인을 하는 수단을 제공하고 많은 PC들은 텔넷이 가능한 TCP/IP 소프트웨어가 설치된다. 텔넷은 필수적으로 원격 클라이언트로부터 호스트컴퓨터에 텍스트지향의 원격제어접속을 제공한다. 텔넷은 보통 사용자명과 패스워드를 네트웍을 통하여 보내는데 이것이 중요 보안 약점이다.

2.3. 이동 컴퓨팅

최근 휴대용 컴퓨터의 보급 및 활용이 보편화되고 있는 추세이다. 시장조사연구기관 「International Data Cooperation」의 보고서에 의하면 모든 컴퓨터의 25%는 휴대용 컴퓨터를 사용하는 사업체에 의해서 구입 되었다고 한다. 대부분의 휴대용 컴퓨터는 고속모뎀과 통신 소프트웨어를 장착하고 있다.

휴대용 컴퓨터를 사용하여 전화접속, 텔넷 같은 접속 메커니즘을 사용하는 동안에 발생할 수 있는 취약점은 다음과 같다.

- 원격컴퓨터의 위치가 자주 변경되기 때문에 다이얼-백 모뎀은 접근을 관리하기가 어렵다.
- 원격컴퓨터를 사용하는 동안에 Shoulder surfing을 통하여 패스워드나 신분 증명번호 같은 정보들이 유출된다.
- 정보가 저장된 원격 컴퓨터를 잃어버렸을 때 분실에 대한 보고가 늦어져 잃어버린 원격컴퓨터로부터 부정한 원격접속이 가능하다.
- 휴대용 컴퓨터들에 내장된 모뎀을 사용하여 사무실의 전화라인을 통한 승인되지 않은 다이얼-

인이나 다이얼-아웃 접속을 위해 사용된다.

- 이동컴퓨팅에 무선통신을 사용하는 것은 도청될 수 있으며 취약성의 수준이 높아진다.

3. 전자상거래

컴퓨터들 및 네트웍들의 사용은 일반적으로 다음의 목적에 주로 사용한다.

- Back Office 자동화 - 광고, 재정, 인원 같은 재정 상태와 정보를 유지한다.
- Front Office 자동화 - PC와 LAN의 출현은 워드프로세싱, 거래추적, 재정평가 등의 사무기능을 컴퓨터를 통하여 해결한다.
- 고객 지원 자동화 - 회사와 가정에서 PC의 영역 확대와 저 비용은 어느 곳에서나 쉽게 인터넷의 접속을 지원하여 회사와 그들의 고객간 업무처리가 용이하다.

이렇게 나아가기 위해서는 전자상거래가 필수적이다. 전자상거래는 전자우편, 정보발간, 전자데이터 교환, 정보·재정 트랜잭션의 내용을 포함한다.

3.1. 전자우편

전자우편을 사용하여 업무를 처리하는 것은 적은 비용으로 고객들, 공급자, 파트너들과 통신을 할 수 있기 때문이다. 하지만 쉽고 편리한 만큼 사용하는 데에는 다음과 보안 취약성이 있다.

- 인터넷 전자우편주소를 쉽게 속일 수 있기 때문에 전자우편주소로만 근거하여 전자우편 메시지를 보내거나 송신한 사람의 정보를 신뢰할 수는 없다.
- 인터넷 전자우편 메시지가 중간에 부정 사용자에 의해서 변경될 수 있다.
- 중요한 정보가 수록된 전자우편 메시지의 내용은 계획되지않은 수령인에 의해서 읽혀질 수 있다.

이런 취약성들은 조직들이 업무를 처리하는데 전자우편을 이용할 것인지 정책을 결정하는데 중요한 영향을 미치고 해결방안이 강구되어야 한다.

3.2. 정보 발간

인터넷을 이용하여 다수의 목적을 가진 사람이나 조직에게 정보를 쉽게 제공할 수 있다. 오늘날 미국에서는 가정의 대략 35%가 PC를 가지고 있고 이들 가정 중에서 반정도가 인터넷에 연결이 가능하다. 이런 이유로, 전자 출판은 출판계에 상당한 영향을 주고 있다.

정보발간에는 두 가지 주된 종류가 있는데 PUSH 형과 PULL 형이다. 잡지를 예약 구독하는 것이 푸쉬형 정보발간의 예이며 이때 정보는 정기적으로 구독자에게 보내어진다. 거리의 가판대에서 신문이나 잡지를 얻는 것이 풀형 정보발간의 예이다. 독자는 정보를 얻기 위해 주도권을 가진다.

푸쉬형 정보발간에 전자적으로 상당하는 것은 모든 가입자에게 정보를 보내는 메일링 리스트를 만드는 것이다. 전형적으로 리스트서버소프트웨어는 메시지 전송, 가입자를 추가/변경/삭제할 수 있다. 리스트서버 사용자는 정보를 얻기 위해 조직의 네트웍에 접속할 필요가 없으므로 안전하다. 그러나 다음과 같은 몇 가지 취약성이 있다.

- 리스트서버소프트웨어가 사용자를 추가/제거하고 리스트에 대한 정보를 관리할 수 있어야 한다. 관리가 제대로 되지 않을 때 부정한 사용자는 계획하지 않은 작동이나 버퍼 오버플로우를 시도하려고 유닉스 명령어들이나 매우 큰 입력 문자열들을 보낼 수 있다.
- 만일 서버의 구성이 정확하지 않다면 리스트서버소프트웨어는 전체 가입자주소의 리스트가 각 가입자에게 노출될 수 있어 부정한 서비스나 공격들을 받는다.

보통 인터넷에서 이용하는 풀형 정보 발간에 두 가지 전자적으로 상당하는 것은 FTP서버와 WWW

서버들이다. FTP 서버들은 Unix 운영체제, 많은 MS Windows가 실행되는 어떤 컴퓨터든지 바로 설치하고 실행할 수 있다. FTP 서버들은 패스워드가 필요없는 완전한 익명 로그인을 허용하거나 정당한 사용자명과 패스워드를 요구하도록 설치할 수도 있다. FTP 서버들은 표준화된 Unix 파일 디렉토리와 닮은 간단한 인터페이스를 지원하다. 만약 FTP 서버가 정확하게 구성되지 않았다면 호스트 컴퓨터의 어떤 파일이라도 찾고 액세스가 가능하다. 심지어 호스트에 연결된 네트웍을 통하여 다른 서버의 접근까지도 가능하다. FTP 서버들은 제한된 디렉토리 영역으로만 접근할 수 있도록 구성하여야 한다.

웹 서버는 텍스트/그래픽/오디오/비디오가 포함된 정보들을 저 비용으로 제공할 수 있다. HTML과 HTTP 표준을 사용하는 것은 다양한 종류의 클라이언트 플랫폼을 가진 사용자들에 의해서 Web에 기초한 문서들을 쉽게 접할 수 있도록 한다. FTP 서버들과 유사하게 웹 서버들은 정확하게 구성되지 않는다면 대규모 네트웍에 중요한 보안 취약성을 가진다.

3.3. 전자데이터교환

표준화된 포맷에서 아주 단순한 형태의 전자데이터교환(EDI)은 관계된 두 회사간에 정보를 전자적으로 교환한다. 교환의 기본적인 단위는 일반적으로 구매주문이나 고객송장 같은 표준화된 사업문서에 관계된 트랜잭션 세트이다. X.9 와 UN/EDIFACT 같은 표준화된 몸체를 통하여 개발된 트랜잭션 집합은 각 데이터 요소를 위한 포맷들과 절차들로 기술된 데이터 성분들의 광범위한 집합이다.

사업체들은 공급자와의 거래 시간과 비용을 줄이는데 EDI를 사용한다. EDI는 거대한 문서량을 줄이고 현재의 데이터베이스를 유지하는데 필요한 시간과 노력을 단축한다. 부가가치망은(VAN)은 전형적으로 EDI 트랜잭션의 전송에 사용된다.

인터넷은 비용절약을 위해 부가가치망을 통하여 EDI를 지원한다. 그러나 인터넷은 EDI를 위해 필요한 보안 서비스(무결성, 기밀성, 비부인성)를 지원하지는 않는다. 인터넷에서 전자우편과 유사하게 EDI 트랜잭션들은 인터넷을 통하여 전송할 때 중간에 변경되거나 노출될 수 있다. 이런 경우에 암호기법을 사용하여 이런 취약성을 제거한다.

3.4. 정보 트랜잭션

정보제공은 상거래에서 중요하고 그 종류에는 다양한 형태의 서비스가 있다. 역사적인 정보 같은 정적인 데이터,전호번호/주소와 같은 공용정보, 생산정보, 뉴스/정기 간행물/데이터 베이스 /주식시세검색 같은 유료 정보서비스 등이 있다. 이들 서비스를 제공하는데 인터넷을 이용하는 것은 대체로 팩스, 전화, 우편 서비스를 사용하는 것보다 비용이 적게 든다. 잠재적인 고객들은 고가의 고객지원 서비스를 이용할 필요 없이 정보를 찾고 검색할 수 있다.

전형적으로 정보 서비스들은 정보를 제공하기위해 기초를 이루는 메커니즘으로 WWW을 사용한다. 정보의 무결성과 유효성의 제공은 보안 제어와 정책에 관계한 보안문제해결의 관건이다.

3.5. 재정 트랜잭션

다양한 형태에서 컴퓨터들과 네트웍들은 재정상의 트랜잭션을 처리하는데 사용되어 왔다. 이들 트랜잭션들의 보안유지는 항상 비공개적인 네트웍들을 통하여 전송하거나 데이터 암호화표준을 사용하여 암호화한다.

주요 지불메커니즘을 요약하면 표 1.과 같다.

	사업체-사업체	사업체-고객	고객-고객
지폐		Primary	Primary
수표	Primary	Secondary	Secondary
직불		Secondary	
신용		Secondary	
EFT	Secondary		

표 1. 재정 트랜잭션 종류

이들 트랜잭션 전송에 인터넷을 사용하는 것은 전자적으로 동등하게 지폐/수표, 직불/신용카드를 대체한다.

- 지폐 - 모든 방법들은 디지털통화가 안전하게 저장된 안전한 디지털「지갑」을 만드는데 암호화기법을 사용한다. 전자지폐의 이체는 금융기관을 거칠 필요가 없다.
- 수표 - 금융산업은 전자검사를 위한 표준을 개발하고, 전자수표 자체에는 전자메시지가 포함되어 있는데 전자수표에서 전달되는 정보를 어떻게 정의할 것인지를 결정해야 한다. 전자수표는 자금이체를 위해서 항상 금융기관을 통해야 한다.
- 직불 카드 - 스마트카드와 가치 저장형 카드는 다양한 방법으로 전자통화를 예금한다. 각 트랜잭션은 카드에 예금된 통화가 소모될 때까지 사용한 총액을 지불한다. 가치 저장형 카드는 중재자로 금융기관이 필요 없다.
- 신용카드 - 주요 업체들(비자, 마스터카드, 아메리칸 익스프레스 등)은 공공네트웍을 통한 신용카드 트랜잭션을 수행할 수 있는 표준을 개발하였다. 잘 알려진 SET 표준은 구매자, 판매인, 신용카드채무자(전형적으로 은행)사이의 3-way 트랜잭션을 지원한다. SET을 사용하는 전자신용카드 트랜잭션은 항상 금융기관을 통한다.
- 전자자금이체(EFT) - EFT는 은행들과 다른 금융기관사이의 자금이체를 보호하는데 암호화기법을 사용한다. 고객들은 고객을 위한 EFT를 통하여 금액을 불입/지불한다.

전자자금 트랜잭션의 각 형태는 무결성, 기밀성, 인증, 비부인성을 지원하는데 암호화기법을 이용하고 있다.

4. R&D

인터넷을 통한 R&D는 일반적으로 원격서버로부터 정보를 탐색하고 받기 위해 FTP, Gopher, WWW 클라이언트 소프트웨어 사용한다. R&D를 위해서 인터넷을 사용할 때 언급되는 중요 취약성은 바이러스나 다른 부정한 소프트웨어가 내포되었을 가능성이다. 다음으로 중요한 취약성은 클라이언트 소프트웨어가 인터넷 정보 서버들을 탐색할 때 남는 로그이다. 대부분의 서버소프트웨어는 클라이언트의 IP 어드레스를 로그하는 능력을 가지고 있으며, 웹 서버 소프트웨어는 사용하는 브라우저의 종류, 마지막으로 방문했던 사이트, 브라우저에서 사용되는 전자우편 주소 등의 정보를 로그하기 때문이다.

5. 인터넷 가용성 및 편의성

인터넷을 이용하는 것은 사업운영에 중대한 영향을 미치고, 인터넷 접속을 보호하는 보안제어는 높은 유용성과 연속적인 운영을 위한 요구사항을 지원하는데 필요하다. 이들 요구사항은 흔히 보안정책에서 주요한 쟁점 사항이다. 예를 들면, Firewall 시스템이 다운된다면, 인터넷으로의 접속은 복구될 때까지 불가능하다. 낮은 위험률을 가진 조직의 입장에서 정책은 복구가 끝날 때까지 위험요소를 포함한 고장 난 Firewall 시스템을 허용한다. 그러나, 높은 위험률을 가진 조직의 입장에서는 보조 Firewall 시스템을 사용해야 한다. 매우 큰 조직을 위해서는 Firewall 시스템과 인증서버 같은 다중보안제어시스템을 사용해야 하며 또한, 다중인증서버가 필요할 것이다.

높은 가용성을 제공하기 위해서 첫째로 최대 수용량을 계획해야 한다. Firewall 시스템을 설치하여 세밀게 보안제어를 하면 성능을 떨어뜨리게 된다. 그러므로, 조직의 규모에 맞게 보안제어를 계획해야 한다. 둘째로 Firewall 시스템과 인증서버의 백업은 필수이다. 마지막으로 문제가 발생했을 때 복구를 위해서 하드웨어와 소프트웨어구성을 분석하고 최신/패치 버전을 적용해야 한다.

인터넷에 연결된 많은 시스템의 사용자 집단은 다양한 분야의 사람들로 구성된다. 이들에게 자주 요구되는 것은 모든 응용프로그램은 사용하는 것이

평이해야 한다는 것이다. 이것은 사용자가 시스템에 인증되는데 걸리는 시간을 줄이고 사용자 집단의 역량에 맞도록 보안을 제어하는 인터페이스를 설계하여 해결해야 한다.

6. 결과 분석

인터넷연동에 의해서 지원되는 중요 서비스들의 보안제어수단과의 연계성을 요약하면 표 2.와 같다. '√' 표기가 된 것은 주어진 서비스들을 보호하는데 필수적인 보안제어 수단을 의미한다.

	검증/인증	액세스 제어	Firewall 시스템	소프트웨어 도입 제어	암호화	아키텍처	사고 대응	관리차원
원격 접근	√	√	√		√			√
전자 우편	√			√	√			√
정보 발간		√	√			√		√
R&D		√	√	√		√		√
전자상거래	√	√	√	√	√	√	√	√
가용성						√		√
편의성						√		√

표 2. 보안제어와 서비스간의 연계성

7. 결론

보안과 사용의 편의성은 서로 배반적이다. 사용자 편의성을 높이면 보안의 취약점의 수준이 높아지고 보안의 수준을 높이면 편의성이 떨어진다. 그러므로, 효율적인 보안정책을 만들고 각 시스템과 체제에 맞는 보안기술개발은 필수이다.

보안제어방법은 크게 물리적/기술적/관리적/법·제도적인 방법 등으로 분류가 되는데, 여기서의 논의는 기존의 기술적인 보안방법을 바탕으로 한 관리적 측면의 보안관리 방법에 초점을 맞추었다. 특히, 인터넷 적용업무별 보안요구사항을 분석하고 관리적 보안제어수단을 요약한 것이다. 추가적으로 연구해야 할 사항은 "중요한 내용을 전자우편을 통하여 보낼 때에는 반드시 암호화해야 한다."는 식으로 적용업무의 구체적인 보안제어항목별 관리방법이 깊이 있게 연구/개발되어야 한다.

참 고 문 헌

1. 한국전산원, "전산망 보안을 위한 위험분석 프로그램에 관한 연구", 1995.
2. 김기윤, 나관식, 김종석, "LLNL 체크리스트를 이용한 정보시스템 취약성 평가", 통신정보보호학회지 제6권 제4호, 1996.12.
3. Baskerville, R., "Information System Security design Method : Implications for Information System development", ACM Computing surveys, Vol.25, No.4, Dec. 1993.
4. NCSA, "NCSA Firewall Policy Guide", 1995.
5. M. Fites, P. Kratz, and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.
6. Moses, R., "Risk Analysis and Management", Computer Security Reference Book, CRC Press, Inc., 1992.
7. Otwell, K. and Aldridge, B., "The Role of Vulnerability in Risk Managenet", Computer Security Journal, Vol VI, No.1, 1989.
8. Ozier, W., "Issues in Quantitative Versus Qualitative Risk Analysis", Datapro Reports on Information Security, Risk Analysis, Mar. 1992.
9. 한국정보보호센터, "Firewall 시스템 총서", 1996. 10.
10. 한국정보보호센터, "방화벽 FAQ", 기술문서 CERT-KR-TG-96-002, 1996.