네트워크 보안성평가 지표개발에 관한 연구

박 동 석* 안 성 진* 정 진 욱*
* 성균관대학 컴퓨터교육과

요 약

네트워크 구축의 각 단계별로 제시하는 분석단계의 정보요구, 기능요구, 성능요구, 보호요구, 접속요구, 다양한 서비스요구와 설계단계의 기능성, 확장성, 서비스계속성, 변경가능성, 네트워크단순성, 실현가능성, 표준 및 시스템과의 호환성 목표 그리고 시험단계의 시기성, 대역폭, 신뢰성, 중요도, 비용 목표 마지막으로 구현 및 운용 단계의 단순성과 간편한 구성, 데이터전송량, 비용 대비 효과, 네트워크 관리 및 통제, 관리가능성, 보안, 교육 등의 목표를 제시하였고 구축된 네트워크의 보안성부문을 평가하기 위한 지표를 제시하고 있으며 지표별로 네트워크 감리 활동에 적용할 수 있는 기준값을 제시하였다.

The Study of Developing an Index for Evaluating the Security of the Network

Park Dong Suck* Ahn Seong Jin* Chung Jin wook*

ABSTRACT

The major goal of this study is to develop an index that can evaluate the quality of the appropriate network in a series of projections that analyze, design, and then build a network. The existing software engineering and/or the methods of developing a system are limited. The process of defining the requirements in building a network, designing the system, and building the network focuses on arranging the methods of building a network. Based upon this, we tried to develop a necessary index to evaluate the security of a network..

1. 서 론

본 연구의 대상은 현재 구축되어 있는 네트워크의 보안성을 위주로 어떻게 평가할 것인가에 관련된 문제를 해결하는 방안을 도출 하고자 하는 것이다. 네트워크 보안성 평가 지표개발의 연구를 실시하게 된 배경과 필요성은 다음과 같이 요약될 수 있다.

첫째, 네트워크 의존도에 따른 네트워크 가용성 확보의 필요성 증대
둘째, 신기술의 도입 및 프로젝트의 대형화에 따른 위험성이 증대
셋째, 네트워크 보안성평가 지표의 부재
넷째, 네트워크 기술분야의 혁신적인 발전속도에 따른 보안성 확보 미흡

본 지표개발연구 주로 관심이 되는 네트워크는 동일한 조직내의 통신망 구조를 지칭하는 것으로 볼 수 있다. 동일한 조직에서는 한 개의 AS(Autonomous System)로 망을 관리 및 운영하므로 단일의 AS를 사용하는 집단의 네트워크가 본연구의 대상이 된다. 대규모 조직의 네트워크일 경우 AS시스템간의 연동이 필요할 경우도 있겠으나, 그러한 예는 매우 드물다고 할 수 있으므로 한 개의 AS는 단일 조직에 의해 관리되고 운영되는 라우터와 네트워크의 집합임을 감안하면, 대상을 한 개의 AS로 국한하여 접근한다 할지라도 별 무리가 없을 것으로 판단된다.

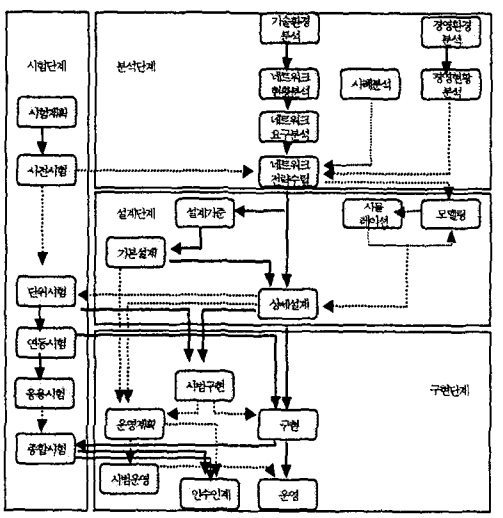
또한 네트워크 보안성지표를 개발하는 과정은 기존의 소프트웨어 공학에서 언급하고 있는 SDLC의 개발방법론인 Method/1, ISACA CobIT, ISO12207등을 참고하여 네트워크 분석/설계/구축과 관련된 추상화된 모형을 도출하고 단계별 목표를 개발하였으며 개발된 목표를 바탕으로 보안성부문에서 다루어야할 지표를 선택하고 제안하였다 그리고 이를 실제 네트워크에 적용한 결과를 바탕으로 검증하는 작업을 수행하였다

2. 네트워크 구축 방법론

2.2 네트워크 구축 방법론

2.2.1 네트워크 구축 방법론의 도출

네트워크 구축 방법론은 다양한 네트워크와 시스템 관련 경험 및 지식을 바탕으로 수립된 표준적 업무절차로 정의할 수 있으며 소프트웨어 개발주기에 비견되는 네트워크 개발주기에 대한 국제적인 표준이나 실제 사례가 없어 기존의 정보시스템 아키텍쳐 분석/설계/구축 모형을 근간으로 하여 도출하였다. 네트워크 구축방법론은 분석단계, 설계단계, 시험단계, 구현단계의 총 4단계로 나누어 볼 수 있다.[1]



(그림1) 네트워크 구축방법 절차도

(1) 분석단계

네트워크 분석단계는 환경분석(경영환경분석과 기술환경분석)과 현황분석(경영현황분석과 네트워크현황분석)으로 나눌 수 있다. 먼저 경영환경 분석은 기업의 경영을 위해 요구되는 Network 특성과 품질 수준을 파악하는 것이며, 업종 특성에 관계된 요구사항과 경영층의 특화

된 요구사항 등이 표현되어야 한다. 기술환경 분석은 상용되고 있거나 상용될 예정인 통신기술 또는 제품을 대상으로 상기의 경영환경 분석에 따른 요구사항을 수용할 수 있는 통신기술 및 제품을 일정과 적용 가능성 등을 포함하여 분석하는 것이다. 경영현황 분석은 Network에 대한 투자대비 경영 및 사용자 관점에서의 효율성을 판단하기 위한 기본 정보로 활용된다. 또한 네트워크 현황 분석은 기업의 현재 네트워크에 관련된 인적, 물리적, 논리적 자원을 파악 및 분석한다 분석단계에서는 환경분석과 현황분석을 바탕으로 네트워크의 전략을 수립하게 된다.

(2) 설계단계

설계단계에서는 모델링과 시뮬레이션을 바탕으로 설계기준에 의한 기본설계와 상세설계를 진행하는 단계이다 먼저 모델링은 아키텍쳐와 설계 기준에서 정의된 네트워크 제자원에 의해 네트워크의 물리적 및 논리적 요소를 개념화한 것이며, 이것은 구현되는 네트워크를 적절한 규모로 축소한 것이다. 이때 축소된 네트워크임에도 불구하고 아키텍쳐와 설계 기준은 유지하여야 한다.

다음 모델링 결과의 적합성은 시뮬레이션에 의해 검증되며, 시뮬레이션 결과에 따라 모델링을 재 설정함으로써 모델의 완성도를 높일 수 있다. 모델링과 시뮬레이션의 반복 순환 작업은 설계 및 구현에서 발생할 수 있는 위험 요소 또는 예외 요소를 최소화할 수 있다. 그리고 기본 설계에는 분석, 계획 등의 선행 프로세스의 내용이 체계적으로 정리되어야 하며 그에 따른 네트워킹의 범위와 설계 방향, 적용 기술 및 표준, 제안서 또는 계약서와의 비교 사항, 상세 설계를 위한 트래픽 분석 등을 표현하여야 한다. 최종단계인 상세설계는 네트워크 구현을 위한 물리적 및 논리적 네트워크 제자원을 정의하고 설계하는 것이며, Low-End까지의 모든 요소를 상세히 표현함으로써 네트워크 구현에 대한 전면 적용이 가능하여야 한다.

(3) 시험단계

시험단계에서는 장비시험과 네트워크시험을 실시하게 되는데 장비는 네트워크를 구성하는 핵심 요소이므로, 기 선정되었거나 선정 예정인 장비에 대해 기능과 성능 등의 장비 특성을 파악하기 위해 장비 시험이 실시되어야 한다. 장비 시험은 장비간의 연동 및 End-to-End의 응용시스템을 시험하는 네트워크시험과 혼용하여 실시될 수 있다. 네트워크 시험은 모델링에서 적용된 네트워크에 대해 적절한 시험 환경을 구성하여 실시될 수 있으며, 장비간의 연동과 End-to-End의 응용시스템 시험을 네트워크 관점에서 실시하는 것이다.

(4) 구현단계

구현단계에서는 제품선정과 시공을 통한 구현, 그리고 운영을 하게 되는데 네트워크설계에 적절한 장비 사양(Specification : 요구 기능, 성능 등)이 정의되어 있으므로 설계에 제시된 구현에 적합한 제품이 선정되어야 한다. 그리고 시공 구현에 있어 대형 네트워크 또는 특별한 요구 사항이 있는 네트워크 등의 경우는 전면적인 구현에 앞서 네트워크의 검증을 위해 별도 설계에 의해 시범 구현이 실시될 수 있다. 교육은 분석 단계에서부터 지속적으로 실시되는 것이 바람직하며, 교육 대상, 기간, 내용 등이 포함된 교육 계획에 따라 실시한다. 인수인계의 경우는 범위와 내용 및 방법 등은 최소한 프로젝트 계획이 완료되기 전에 정의되어야 한다. 시범 운영은 시범 구현된 네트워크의 운영과 운영 Know-How 습득을 위한 부분적 혹은 분야별 운영 등이 있을 수 있다. 전면 운영은 일반적인 네트워크의 운영을 의미하며, 특히 네트워크의 개선 또는 최적화는 운영 단계의 주요 요소이다.[2]

2.2.2 단계별 구현 목표

네트워크 성능에 관련된 평가지표는 2.2.1장에서 제시된 네트워크 구축 방법론을 근간으로 하여 도출되었다. 분석단계에서는 요구사항분석과 수요예측을 통한 네트워크 전략수립에 적용되는 목표를 정의하였으며 네트워크 설계단계에서는 성능 분석, 정보보호요구, 네트워크 규모 산정 등에 해당하는 목표를 정의하였다 이어서 시험단계에서 고려해야할 각종 목표를 도출하였으며 끝으로 네트워크 구현 및 운영과정에서 검토되어야 하는 각종 목표를 제시하였다.

2.2.2.1 네트워크 분석단계의 목표

네트워크 분석 단계에서는 요구사항을 정리하고 비용/효과적 측면과 기술적 타당성 측면에서 가장 효율적인 네트워크를 분석하는 단계이다. 이 단계에서 가장 중요한 사항은 사용자의 요구사항을 정확하게 정의하는 것이다. 관련된 목표는 다음과 같다.

(1) 정보요구(Information requirements)

네트워크 사용자가 자신의 업무를 처리하면서 필요로 하는 정보 및 데이터가 무엇인지를 파악하고 이를 정의하는 것이다. 제반요구사항 중에서 가장 핵심이 되는 요건이다.

(2) 기능요구(Functionality requirements)

네트워크가 각각의 사용자에게 어떠한 서비스를 제공할 수 있는 지에 대한 사항으로서 주로 응용업무시스템으로 구현된다.

(3) 성능요구(Performance requirements)

사용자가 네트워크에 특정한 서비스를 요청하였을 경우, 각 서비스를 어떠한 시간범위 안에서 처리해야 하는 지에 대한 정의로부터 시작한다. 성능요건은 각 사용자의 다양한 정보요건을 처리함에 있어 이를 제한된 시간범위 내에서 처리하기 위하여, 필요한 하드웨어 용량, 데이터베이스 관리시스템, 통신선로의 대역폭, 각 기술별 소요비용 등이 상호 작용됨으로 사전에 설정한 서비스응답시간의 달성여부를 예측하기가 상당히 어려운 한계점을 지니고 있으나 네트워크 설계자는 효율적으로 이를 지원하기 위한 아키텍쳐 설계에 주력해야 한다.

(4) 보호요구(Security requirements)

네트워크를 자산으로 인식하고 이에 대한 여러 가지 위험으로부터 안전하게 보호하기 위하여 구성요소별로 다양한 보안 요건이 존재한다. 구성요소 중 가장 중요한 것이 데이터이므로 이에 대한 각 데이터별 보호수준의 결정, 이에 따른 응용업무시스템 보호대책, 네트워크 보호 및 안전대책 요건이 사전에 설정되어야 한다. 한편 서비스의 계속성을 보장하기 위한 네트워크 중복(Redundancy)설계 및 백업에 대한 요구가 도출되어야 한다.

(5) 접속요구(Interface requirements)

조직외부로부터 필요한 요구가 파악되고 이를 효율적으로 접속하기 위한 방안이 강구되어야 한다. 접속요건은 필요로 하는 정보를 어디에서 어떻게 확보할 것인지에 대한 조사에 해당한다.

(6) 다양한 서비스 요구(Multi services requirements)

현재 텍스트 데이터만을 지원하는 정보시스템을 운영하는 조직일 지라도, 향후 음성, 화상, 동화상 등 멀티미디어 통신에 대한 사용자 요구와 이를 지원하는 다양한 응용시스템의 도입이 일반화되어 있으므로, 분석단계에서부터 사용자의 이러한 서비스에 대한 요구가 식별되어야 한다.

2.2.2.2 네트워크 설계단계의 목표

네트워크의 설계단계에서는 기능성(Functionality),

확장성(Scalability), 서비스계속성(Availability), 변경가능성(Adaptability), 네트워크 단순성(Network Simplification), 실현가능성(Reliability), 표준 및 기존시스템과의 호환성(Compatibility with standards or legacy systems) 등의 목표를 도출할 수 있다.

(1) 기능성(Functionality)

네트워크는 24시간 중단 없이 사용 가능해야 한다. 기능성은 조직의 구성원들이 그들의 업무를 수행하기 위한 가장 중요한 핵심요소이다. 여기서 네트워크를 중심으로 서비스 공급자와 사용자 사이에 서비스 수준에 대한 상호당사자간의 협약(SLA)이 포함된다. 네트워크 설계담당자는 아키텍쳐 관점에서 각 응용시스템의 기능상 요구사항을 파악하여야 한다. 이러한 요구사항에는 응용시스템별 데이터 대역폭, 응답시간, 지연허용시간, 허용데이터 오류율, 데이터유형, 트랜잭션 유형 등이 있다.

(2) 확장성(Scalability)

네트워크는 현재의 정보요건을 충족함은 물론 향후의 정보요건을 충족하기 위하여 확장이 용이해야 한다. 이러한 확장성을 보장하기 위해서는 서브네트워크의 계층적인 구성, 사용하고자 하는 네트워크 프로토콜, 서브네트워크를 통합하는 방법, 전체적인 노드 주소체계 및 스위치 및 라우터 등에 의해 영향을 받는다. 따라서 네트워크 설계자는 향후 네트워크 확장이 용이하도록 현재의 네트워크를 설계하여야 한다. 조직의 규모가 증대됨에 따라, 네트워크를 중심으로한 정보시스템도 이에 상응하는 서비스를 제공할 수 있어야 한다. 따라서 네트워크 담당자는 이의 초기 설계 시 이에 대한 고려를 반드시 하여야 한다.

(3) 서비스 계속성(Availability)

정보시스템의 여타 구성요소 중에서 서비스 계속성이 가장 중요시되는 것이 네트워크이다. 특히 백본망의 경우, 서비스 장애가 발생할 경우 조직 전체의 운영이 중단되는 현상을 초래함으로 대부분의 조직은 백본망을 구성할 경우 Redundancy를 반영하여 한쪽의 회선에서 장애나 네트워크 혼잡이 일어난다 할 지라도 이를 극복할 수 있도록 하고 있다. 한편 각 조직 단위별 LAN 설계 시에도 서비스 중단을 최소화하기 위한 설계방식이 고려되어야 한다. 네트워크 설계자는 사용자 서비스의 중요도 및 서비스의 특성을 고려하여 서비스 계속성을 보장하기 위한 백업 및 이중화가 설계가 반영되도록 해야 한다.

(4) 변경가능성(Adaptability)

변경가능성이란 네트워크가 변화에 대처할 수 있는 정도를 의미한다. 대다수의 경우에, 네트워크를 기반으로 변경가능성이란 시기 적절하고 효율적으로 방법으로 신기술을 네트워크에 반영할 수 있는 정도를 의미한다. 이러한 변경가능성은 네트워크와 관련된 기술의 변화가 엄청난 속도로 진행되고 있기 때문에 네트워크를 설계하고 관리하는 전문가들에게는 매우 중요한 문제이기 때문이다. 비록 조직의 네트워크를 항상 최신의 새로운 기술을 사용하여 구축 운영할 필요는 없지만, 새로 도입할 기술이나 장비로 인한 장애의 최소화를 위해서는 중요한 의미는 지닌다 하겠다.

(5) 네트워크 단순성(Network Simplification)

아무리 성능이 좋고, 선진기술이 도입된 시스템일지라고 향후의 운용 용이성 및 유지보수성을 제고하기 위해서는 가급적 설계하고자하는 네트워크를 단순화할 필요가 있다. 따라서 위에서 언급할 제반 정보시스템 요건을 충족하면서도 네트워크 구조를 단순화하기 위한 고려가 실시되어야 한다.

(6) 실현가능성(Reliability)

네트워크를 설계할 경우에, 아무리 최첨단의 기술이나 장비일지라도 실제 그 네트워크를 도입

하여 사용하는 과정에서 수많은 문제를 야기할 수 있다. 따라서 설계의 대상이 되는 네트워크 구성요소에 대한 충분한 타당성과 사용가능성이 입증되어야 할 것이다.

(7) 표준 및 기존시스템과의 호환성

표준에 대한 고려나 기존시스템과의 호환성 또한 네트워크 설계전문가가 항상 염두에 두어야 하는 사안이다. 특히 정부표준이나 산업표준에 반하는 네트워크의 설계 및 구축은 향후 타 시스템과의 연동에 지장을 초래할 뿐만 아니라, 기존시스템의 특성을 무시한 신규 정보시스템 아키텍처의 도입은 시스템 통합 측면에서 여러 가지 문제점을 가져다 줄 수 있다. 따라서 정보시스템 아키텍처 담당자는 항시 자신과 관련된 표준화 동향을 수시로 파악하고 이를 네트워크 설계에 반영하여야 하며, 기존의 시스템을 수용하는 방향으로 네트워크를 설계하여야 한다.

2.2.2.3 네트워크 시험단계의 목표

네트워크 시험단계에서는 기본적인 시험평가 항목과 사용자중심의 시험평가 항목으로 크게 구분할 수 있으며 기본적인 시험평가 항목에서는 시기성/대역폭/신뢰성을 사용자 중심의 시험평가 항목에서는 중요도/사용자별 QoS수준/비용/보안을 주요한 목표로 도출할 수 있다.

(1) 시기성

네트워크에서 시기성이란 지연과 응답시간 그리고 지터 항목으로 나눌 수 있으며 시기성에 민감하게 반응하는 응용서비스(음성, 동영상)에 영향을 미치게 된다. 지연(Delay)은 정보가 전달되면서 소요되는 시간을 말하며 처리시간과 전파지연시간에 의해 결정되어진다. 시스템 응답시간(System response time)은 정보시스템 요건정의의 성능요건과 직접적으로 관련되어 있으며, 사용자가 서비스를 요청한 후 시스템이 사용자에게 서비스를 응답 또는 제시하기까지의 시간을 의미한다. 많은 사용자가 사용하는 공통의 실시간 온라인 서비스의 경우에 대한 서비스 시간은 향후 시스템 평가에 중요한 요소로 작용한다. 네트워크 전문가는 시스템 응답시간과 관련하여, 각회선별 대역폭, 폭주제어(Congestion control), 각 노드간 전송요구량 등을 바탕으로 성능을 최적화할 수 있도록 고려하여야 한다. 지터(jitter)는 지연 및 시스템응답시간에 의한 변동치를 뜻한다.

(2) 대역폭(bandwidth)

대역폭은 물리적 채널이 가지는 고유한 특성으로 네트워크의 전송용량에 밀접한 영향을 미치게 된다. 대역폭과 전송용량의 관계식은 식(2.1)과 같다.

C(전송용량bps)=W(대역폭hz)log2(1+S(신호)/N(잡음)) (2.1)

(3) 신뢰성(reliability)

Network을 구성하는 물리적, 논리적 요소의 장애(오류)에 의해 Network 서비스가 중단될 때까지의 평균시간을 MTBF(Mean Time Between Failures)라 하며, 장애 또는 유지보수 필요성에 의해 Network 서비스가 중단되는 평균시간을 MTTR(*Mean Time To Repair*)이라 한다. Network의 신뢰성은 이론상 식(2.2)로 나타낸다.[4]

R(신뢰성) = 1 - (MTTR/MTBF) (2.2)

(4) 중요도

중요도란 네트워크를 이용하는 사용자의 관점에서 부여하여 적용되는 멀티미디어 데이터스트림의 여러 가지 *flow level*을 뜻한다

(5) 비용(Cost)

하나의 connection을 설정하거나, 자원을 이용하기 위해 소요되는 건당 비용과 시간이나 데이

터 단위당 비용을 이용자 관점의 비용으로 분류한다.

2.2.2.4 네트워크 구현 및 운용단계의 목표

네트워크 구현단계에서는 단순성과 간편한 구성(Simplicity and easy configuration), 데이터 전송량(Amount of traffic), 비용효과 측면(Cost Effectiveness), WAN 관련된 비용(Cost of WAN resources)이 주요한 목표이며 운용단계에서는 네트워크 관리 및 통제(Network management and control), 관리가능성(Manageability), 보안(Security), 교육(education) 등이 주요한 목표이다.

(1) 단순성과 간편한 구성(Simplicity and easy configuration)

네트워크 구축전문가는 자신의 입장이 아닌 향후 네트워크 운영자 및 사용자의 입장에서 네트워크를 설계하고 구축하여야 한다. 즉 정보시스템을 사용하고 운영하는 사람은 설계자가 아닌 조직에 소속된 일반 전문가들이므로 가급적이면 최대한 단순하고 구성이 용이한 네트워크가 구축되도록 하여야 한다.

(2) 데이터 전송량(Amount of traffic)

네트워크 전문가는 네트워크의 적절한 규모와 여러 가지 구성장비를 선택하기에 앞서 향후 네트워크 상에서 전송될 데이터 량을 정확히 산정하여야 한다. 한편 현재의 데이터 전송량뿐만 아니라 향후 예측 가능한 데이터 증가량을 고려하여 네트워크를 구축하여야 한다.

(3) 비용효과 측면(Cost Effectiveness)

대다수 시스템 구축과 마찬가지로 네트워크의 구축 시에도 비용효과 측면은 가장 중요한 요소로 간주된다. 따라서 현재의 제한된 자원과 예산의 범위 안에서 최적의 네트워크를 설계하고 구현하는 것이야말로 네트워크 구축전문가가 항상 고려해야 하는 요소이다.

(4) WAN 관련된 비용(Cost of WAN resources)

WAN과 관련된 자원을 사용할 경우에는 그 비용이 현재로서는 상당히 크다고 할 수 있다. 따라서 정보시스템을 사용하고자 하는 각 사용자의 그룹의 WAN접속 필요성과 그 사용비용을 비교하여 WAN접속여부를 결정하는 것이 바람직하며, 비용효과측면과 네트워크이중화사이의 상충관계를 고려하여 결정하여야 한다. 오늘날의 대다수 통신환경에서는, 조직과는 거리적으로 떨어져있는 원격지 사무실이나 재택근무자를 수용하는 네트워크를 구성해야 한다. 따라서 조직 내에 이러한 요구사항이 상당히 존재할 경우 이를 수용할 수 있는 네트워크 장비와 회선의 적정한 선택이 요구된다.

(5) 네트워크 관리 및 통제 (Network management and control)

네트워크 구축완료 후, 네트워크 상태를 계속적으로 감시하고, 예방적 유지보수 및 신속한 문제해결을 위하여 네트워크 관리 및 통제에 대한 조직 요건이 식별되어야 한다. 이러한 네트워크 관리는 대규모 시스템의 경우, NMS(Network Management System)등에 이루어지며, 이외에도 부가적으로 네트워크 장비에 대한 데이터베이스 및 자산관리 서비스 등이 요구되어 지기도 한다.

(6) 관리가능성(Manageability)

관리가능성의 목표는 네트워크가 사전에 설정된 목표를 적절하게 달성하도록 하는 관리의 정도를 의미한다. 네트워크 운영담당자로 하여금 네트워크의 운영과 현재의 상태를 항상 정확하게 파악할 수 있도록 하기 위한 도구와 설계가 지원되도록 하는데 그 목적이 있다.

(7) 보안(Security)

접근 통제 및 암호화에 의한 정보접근 예방정도인 기밀성, 조작으로부터 전송데이터를 보호하는 무결성, 송신부인을 금지하는 부인봉쇄 그리고 사용자인증 등이 보안의 주요요소이다.

(8) 교육(education)

TCP/IP프로토콜, SNMP를 활용한 망관리, 방화벽/IDS 보안 등 네트워크운용을 위한 교육이 필수적으로 수행되어야 한다.

3. 네트워크 보안성 평가 지표

2장에서 도출된 네트워크 구축 방법론의 진행 단계별 목표를 바탕으로 네트워크의 보안성부문에 대한 주요한 지표를 개발하였다.

<표 3.1> 네트워크 보안성 평가 주요 의미

평가부문	관련지표 및 의미
보안성	네트워크를 구성하는 각 구성요소의 무결성(integrity), 가용성(availability), 그리고 자원의 비밀성(confidentiality) 확보를 통하여 유형의 정보시스템과 무형의 정보자산을 보호하려는 것

3.1 보안성평가 지표

네트워크에서 보안이란 네트워크를 구성하는 각 구성요소가 무결성(integrity), 가용성(availability), 그리고 자동화된 정보와 이를 등록/저장/처리/ 통신하는데 사용되는 자원의 비밀성(confidentiality)을 보호하는 것이다. 여기에서는 시스템 목적에 알맞는 이용성(usability)을 항상 고려해야 한다.[5] 즉, 상업성 목적이라면 완벽한 보안보다는 성능에 많은 주의를 기울여야 하지만, 특수 목적(국가, 국방, 정부, 회사 기밀을 다루는 시스템)이라면 성능은 떨어지더라도 완벽한 보안에 치중해야 할 것이다.

3.1.1 네트워크보안 목표[6]

(1) 무결성(integrity)

무결성이란 인가된 자(authorized member)만 화일 자료를 사용함으로써 기록된 화일의 재생, 삭제, 변경 등으로부터 보안을 보장하는 것이다. 즉, 비인가자에게는 화일에 대한 접근을 엄격히 제한하는 것이다. 특히, 인가자라 할지라도 화일을 재생하거나 삭제 또는 변경하는 등의 권한을 통제할 수 있는 기능이 제공되어야 한다. 이러한 통제 방법은 암호화를 이용한 데이터 비밀 유지 서비스의 자동 효과로써 실현할 수 있다. 무결성에는 크게 두가지로 분류하는데 첫째는 내용 무결성이며, 둘째는 순서 무결성이다. 내용 무결성이란 전송되는 각각의 메시지에 대해 특정한 값을 첨부하여 전송하면 수신자는 이 메시지를 확인함으로써 무결성을 제고한다. 또한 순서 무결성이란 송신되는 메시지에 일련의 순서를 부여하여 전송할 시 외부의 공격이 탐지됨으로써 무결성을 제공할 수 있다.

(2) 인증성(authenticity)

네트워크를 사용할 시에는 여러가지 방법으로 사용자들을 확인할 필요성이 대두된다. 인증성에는 반드시 사용자만이 인증 대상이 되는 것이 아니고 컴퓨터 시스템 및 각종 응용 프로그램 등도 포함될 수 있다. 이러한 대상들이 실패를 가장해서 네트워크에 침입하는 경우를 대비하여 정확하게 인증 대상을 확인하는 기능이 제공되어야 한다. 특히 데이터 송신은 암호화된 데이터 영역에 송신측 주소의 복사본을 포함시켜 암호화하여 송신하면 수신측은 이를 복호화한 후 주소를 확인함으로써 실현될 수 있다.

(3) 가용성(availability)

네트워크에 연결된 시스템이나 시스템 내부에 있는 자료들은 인가된 사용자에게는 즉시 효과적으로 이용되도록 데이터의 백업, 중복성유지, 물리적 위협으로부터 보안을 유지시킴으로써 가용성을 보장할 수 있는 기능이 제공되어야 한다.

(4) 비밀성(confidentiality)

네트워크에서의 보안 시스템은 시스템 에 대한 비인가자와 불법 침입자의 접근을 제어하고, 비밀 자료의 비밀성이 노출되지 않도록 인가된 자에게만 접근 가능하도록 해야한다.

(5) 이용성(usability)

네트워크에서 보안에 비중을 많이 두면 중요한 정보를 암호화해야 하는 데, 그러한 경우 성능 및 가용성 등이 저하될 수 있으므로 보안뿐만 아니라 전체적인 시스템 성능과의 조화를 이룰 수 있는 기능을 제공하도록 노력해야 한다.

3.1.2 주요지표

(1) 접근 제어(access control) 보안성

네트워크에 저장된 정보를 접근하고자 할 때, 이에 따른 인증은 각 작업에 해당하는 기준이 그 기반이 되어야 한다. 또한 LAN 서버의 보안 체계는 방어적인 접근 제어를 제공해야 할 뿐 아니라, 감사 추적을 할 수 있도록 해야 한다.

<표 3.2> 접근제어 보안성 평가 항목

관련 지표	순서	평 가 항 목	O/×
접근 제어 보안성	1	유저가 시스템으로 로그인 하고자 할 때, 유저 ID와 패스워드를 요구하는가? ※ 필수항목	
	2	서버는 로그인하는 워크스테이션과 그 워크스테이션의 연결 포인트를 확인할 수 있는가?	
	3	모든 자원(프로그램, 데이터, 주변 장치,..)들은 용도에 맞는 적절한 보호가 있는가?	
	4	자원 접근은 허락된 사용자만이 할 수 있는가? ※ 필수항목	
	5	화일 접근의 허락 단위는 화일, 디렉토리, 서브 디렉토리 단위로 되어 있는가?	
	6	화일 접근 권한은 읽기, 쓰기, 실행, 생성, 이름 변경, 삭제, 권한 변경 등으로 세분화 되어 있는가?	
	7	자원 접근은 개인, 그룹, 모두의 세가지 형태, 또는 그 이상 세부적으로 지정이 되어 있는가?	

(2) 패스워드(password) 보안성

패스워드는 사용자에 대한 인증을 위한 가장 처음 단계이자, 보편적으로 가장 많이 쓰이는 방법이다. 패스워드에 대한 평가항목은 다음 표와 같다.

<표 3.3> 패스워드 보안성 평가항목

관련 지표	순서	평 가 항 목	O/×
패스워드 보안성	1	최저 6문자, 최적 8문자, 최고 64문자로 이루어져 있는가?	
	2	대문자와 소문자 또는 문자와 숫자를 혼합해서 사용하는가?	
	3	추측하기 어려운 단어들을 사용하는가?	
	4	패스워드를 주기적으로 변경하는가?	

관련 지표	순서	평 가 항 목	O/×
패스워드 보안성	5	패스워드 문자는 스크린에 디스플레이 되지 않는가? ※필수항목	
	6	새로운 패스워드는 두 번 입력으로 검증을 받는가?	
	7	중요한 화일의 접근은, 비록 암호화되어 있을 지라도, 접근을 위한 추가적인 인증 절차가 요구되는가?	
	8	백도어(back door) 유저 ID 와 패스워드가 없는가? ※필수항목	

(3) 서버(server) 보안성

서버는 네트워크 시스템 구성요소의 가장 중요한 요소로서, 시스템 가용성과 데이터 무결성을 유지할 수 있도록 하여야 하며 다음 표에 의하여 평가할 수 있다.

<표 3.4> 서버 보안성 평가 항목

순서	평 가 항 목	O/×
1	워크스테이션의 세션이 일정기간(관리자가 결정) 동안 사용하지 않을 경우, 이를 사용할 수 없도록 하고, 그 이후 어느 정도의 기간이 다시 지날 경우 완전히 제거되는가?	
2	세션이 끊어진 후에는 개설된 세션에서 수행한 작업내용이 터미널에서 볼 수 없도록 하는가? ※필수항목	
3	권한이 없는 작업을 수행하고자 할 때에는 키보드가 작동되지 않는가?	
4	모든 공유 데이터에 관해서는 트랙잭션 로크를 사용하여 데이터 무결성이 이루어지는가?	
5	소프트웨어의 변경이나 추가는 서버 또는 LAN 관리자에 의해서만 이루어지는가? ※필수항목	
6	서버는 유저에 관한 확인과 인증 작업을 동시에 할 수 있는가?	
7	중요한 자원을 접근하고자 하는 할 때는 추가적인 인증을 거치게 하는가?	
8	중요한 화일(패스워드 화일, 키 화일, 감사용 화일,...)은 암호화된 형태로 유지되는가? ※필수항목	
9	중요한 정보가 있는 화일이나, 암호화된 화일의 백업시 권한 없는 유저의 접근을 막는가?	
10	로그인 실패, 비권한 접근 시도, 우연이나 고의로 인한 접속의 끊김, 소프트웨어와 보안 접근 감사의 변경, 로그인, 로그 아웃, 또는 미리 지정한 다른 행위들에 대해 감사 추적용 로그를 유지하는가?	
11	감사 추적용 로그는 사용 자원, 행위, 유저, 날짜와 시간, 워크스 테이션 ID 와 연결 포인트 등의 항목을 유지하는가?	
12	비정상적인 심각한 행위가 이루어질 경우 자동적으로 경보를 해주는 기능을 제공하는가?	

(4) 백업(backup) 보안성

백업은 네트워크 시스템이 항상 정상적인 상태로 복구될 수 있도록 하기 위한 방법이다. 기본적인 백업 평가 항목은 다음 표와 같다.

<표 3.5> 백업 보안성 평가 항목

관련 지표	순서	평 가 항 목	O/×
백업 보안성	1	백업시 자동적으로 검증이 이루어지는가?	
	2	암호화를 비롯한 보안 측면은 백업을 수행하는 동안 효율적인가?	
	3	백업과 재저장, 복구 기능은 정상적으로 테스트 되는가?	
	4	멀티 서버상의 유저가 정보를 공유하거나, 응용 프로그램이 상호의존적이라면 백업은 적절하게 동기화 되는가?	
	5	네트워크 시스템 전체는 복구 후 정상 가동되는가? ※필수항목	
	6	시스템의 중요도 만큼 시스템 전체 대상의 백업 기간은 짧아지도록 하였는가?	
	7	백업된 내용은 안전한 곳에 위치하며, 백업 매체를 계속 순환적으로 바뀌가며 사용하는가?	
	8	자료의 백업 자체가 중요한 시스템이라면 미러링 시스템을 운영하는가?	

(5) 통신(communication)

통신에 있어서 주요한 보안평가 항목은 다음 표와 같다

<표 3.6> 통신 보안성 평가 항목

관련 지표	순서	평 가 항 목	O/×
통신 보안성	1	원격 접근을 허락하는 대상(유저, 프로그램, 데이터, 트랜잭션 형태, 날짜, 요일, 시간)은 미리 지정되어 있는가?	
	2	확인과 인증 프로토콜은 통신 접근에 관해 효율적(challenge-response, additional passwds등을 사용하여) 인가?	
	3	통신 접근 메시지는 "메시지 인증 코드(message authenticaion codes:MACs)" 나 "디지탈 사인" 등을 이용하여 인증이 되는가?	
	4	모든 통신 접근은 로그 화일로 남는가?	
	5	유저의 통신 접근은 강력한 암호화 알고리즘을 이용하는가?	
	6	통신중의 중요한 정보(패스워드, 데이터,...) 는 전송되는 동안 양방향 암호화가 가능한가?	
	7	원격 접근 포트는 목록화 되어 있고 사용되지 않는 포트는 사용 불가능하게 만들어져 있는가? ※필수항목	
	8	시스템 제작 회사에서 만들어진 원격 접근 포트는 사용을 하지 못하게 하였는가?	

(6) 하드웨어

하드웨어의 보안성 평가 항목은 다음 표와 같다.

<표 3.7> 하드웨어 보안성 평가 항목

관련 지표	순서	평 가 항 목	O/X
하드웨어 보안성	1	모든 장비는 안전한 곳에서 보호되는가? ※필수항목	
	2	전체 장비들의 목록을 유지하는가? ※필수항목	
	3	서버는 잠금 장치가 된 곳에 위치하며, 서버가 있는 위치의 접근은 "카드키 접근 시스템"등을 통해 로그되는가? ※필수항목	
	4	서버가 있는 곳은 물과 불의 위험이 없고 천정까지 연결된 벽이 있는가?	
	5	연결 포인터는 보호되어야 하고 늘 감시되는가?	
	6	jacks, jumpers, cross-connections, routers 등이 보호되는가?	
	7	모든 외부 장치들은 주기적으로 감시되는가?	
	8	케이블은 은닉되는가?	

3.1.3 보안성평가 지표를 활용한 네트워크 품질평가 기준

네트워크 보안성 평가에 사용된 접근제어, 패스워드, 서버, 백업, 통신, 하드웨어 6가지 주요지표의 각 체크항목에 기초하여 네트워크품질의 보안성 부문을 다음 표와 같이 제시할 수 있다.

<표 3.8> 보안성 평가 기준

지 표 명	기준값(%)	필수항목
접근제어	80~90	1.4
패스워드	80~90	5,8
서버	80~90	2,5,8
백업	80~90	5
통신	80~90	7
하드웨어	80~90	1,2,3

표 3.8에서 필수항목은 네트워크의 보안성부분을 만족하려면 필수적으로 요구되어지는 항목이다. 보안성 평가의 해당항목에서 만족되어지는 정도를 이용해 네트워크를 평가하면

우수 = 필수항목 & 분야별 해당항목 만족도 90%이상 (3.1)

양호 = 필수항목 & 분야별 해당항목 만족도 80% ~ 90% (3.2)

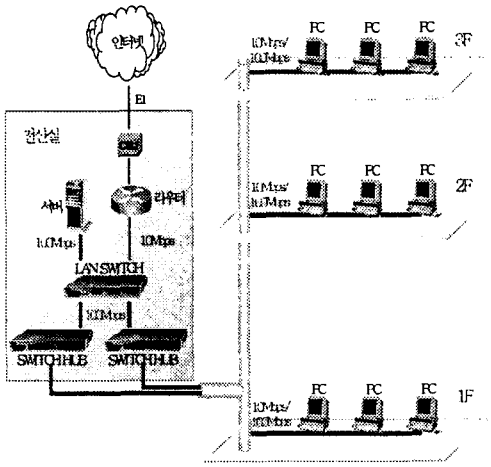
미흡 = 필수항목미비 or 해당항목 만족도 80% 미만 (3.3)

으로 나타낼 수 있다

4. 적용사례

4.1 적용환경

이 논문에서 제시한 보안성평가, 성능평가, 장애평가 각 항목별로 실재 존재하는 네트워크환경을 대상으로 적용성을 실험하였다. 실험에 사용된 네트워크의 구성도는 그림과 같다.



(그림 2) 적용대상 네트워크 구성도

[적용환경]

(1) LAN의 속도는 100Mbps이며 인터넷 속도는 E1이다
(2) 서버는 1대(IBM RS6000 R50)이며 단말기(팬티엄Ⅲ)는 50대이다
(3) 라우터는 cisco2501(1Ethernet 2Serial)이다.
(4) 허브는 백본 역할을 하는 100Mbps(3Com) 스위칭허브 1대와 분배망 역할을 하는 100Mbps(3Com) 스위칭 허브 2대로 구성되어 있다
(5) 실험기간은 2001년 5월 7일 09:00부터 5월 12일 12:00까지이다

4.2 적용결과

보안성평가를 위해 3.1.2에서 제시하고 있는 6가지항목에 대하여 실제 적용한 결과는 다음과 같다.

<표 4.1> 보안성 평가 항목별 체크List

분야	평 가 항 목	O/×
접근제어	유저가 시스템으로 로그인 하고자 할 때, 유저 ID와 패스워드를 요구하는가?	○
	서버는 로그인하는 워크스테이션과 그 워크스테이션의 연결 포인트를 확인할 수 있느가?	○
	모든 자원(프로그램, 데이터, 주변장치,..)들은 용도에 맞는 적절한 보호가 있는가?	○
	자원 접근은 허락된 사용자만이 할 수 있는가?	○
	화일 접근의 허락 단위는 화일, 디렉토리, 서브 디렉토리 단위로 되어 있는가?	○
	화일 접근 권한은 읽기, 쓰기, 실행, 생성, 이름 변경, 삭제, 권한 변경 등으로 세분화 되어 있는가?	○
	자원 접근은 개인, 그룹, 모두의 세가지 형태, 또는 그 이상 세부적으로 지정이 되어 있는가?	×

분야	평가항목	○/×
패스워드	최저 6문자, 최적 8문자, 최고 64문자로 이루어져 있는가?	○
	대문자와 소문자 또는 문자와 숫자를 혼합해서 사용하는 가?	○
	추측하기 어려운 단어들을 사용하는가?	×
	패스워드를 주기적으로 변경하는가?	×
	패스워드 문자는 스크린에 디스플레이 되지 않는가?	○
	새로운 패스워드는 두 번 입력으로 검증을 받는가?	○
	중요한 화일의 접근은, 비록 암호화되어 있을 지라도, 접근을 위한 추가적인 인증 절차가 요구되는가?	○
	백도어(back door) 유저 ID 와 패스워드가 없는가?	○
서버	워크스테이션의 세션이 일정기간(관리자가 결정) 동안 사용하지 않을 경우, 이를 사용할 수 없도록 하고, 그 이후 어느 정도의 기간이 다시 지날 경우 완전히 제거되는가?	○
	세션이 끊어진 후에는 개설된 세션에서 수행한 작업내용이 터미널에서 볼 수 없도록 하는가?	○
	권한이 없는 작업을 수행하고자 할 때에는 키보드가 작동되지 않는가?	×
	모든 공유 데이터에 관해서는 트랙잭션 로그를 사용하여 데이터 무결성이 이루어지는가?	○
	소프트웨어의 변경이나 추가는 서버 또는 LAN 관리자에 의해서만 이루어지는가?	○
	서버는 유저에 관한 확인과 인증 작업을 동시에 할 수 있는가?	○
	중요한 자원을 접근하고자 하는 할 때는 추가적인 인증을 거치게 하는가?	○
	중요한 화일(패스워드 화일, 키 화일, 감사용 화일,...)은 암호화된 형태로 유지되는가?	○
	중요한 정보가 있는 화일이나, 암호화된 화일의 백업시 권한 없는 유저의 접근을 막는가?	○

분야	평가항목	○/×
서버	로그인 실패, 비권한 접근 시도, 우연이나 고의로 인한 접속의 끊김, 소프트웨어와 보안 접근 감사의 변경, 로그인, 로그 아웃, 또는 미리 지정한 다른 행위들에 대해 감사 추적용 로그를 유지하는가?	○
	감사 추적용 로그는 사용 자원, 행위, 유저, 날짜와 시간, 워크스 테이션 ID와 연결 포인트 등의 항목을 유지하는가?	○
	비정상적인 심각한 행위가 이루어질 경우 자동적으로 경보를 해주는 기능을 제공하는가?	×
백업	백업시 자동으로 검증이 이루어 지는가?	○
	암호화를 비롯한 보안 측면은 백업을 수행하는 동안 효율적인가?	○
	백업과 재저장, 복구 기능은 정상적으로 테스트 되는가?	○
	멀티 서버상의 유저가 정보를 공유하거나, 응용 프로그램이 상호 의존적이라면 백업은 적절하게 동기화 되는가?	○
	네트워크 시스템 전체는 복구 후 정상 가동되는가?	○
	시스템의 중요도 만큼 시스템 전체 대상의 백업 기간은 짧아지도록 하였는가?	○
	백업된 내용은 안전한 곳에 위치 하며, 백업 매체를 계속 순환적으로 바꿔가며 사용하는가?	×
	자료의 백업 자체가 중요한 시스템이라면 미러링 시스템을 운영하는가?	×
통신	원격 접근을 허락하는 대상(유저, 프로그램, 데이터, 트랜잭션 형태, 날짜, 요일, 시간)은 미리 지정되어 있는가?	○
	확인과 인증 프로토콜은 통신 접근에 관해 효율적(challenge-response, additional passwds등을 사용하여) 인가?	○
	통신 접근 메시지는 "메시지 인증 코드(message authenticaion codes:MACs)" 나 "디지탈 사인"등을 이용하여 인증이 되는가?	×

분야	평 가 항 목	O/×
통신	모든 통신 접근은 로그 화일로 남는가?	○
	유저의 통신 접근은 강력한 암호화 알고리즘을 이용하는가?	○
	통신중의 중요한 정보(패스워드, 데이터,...) 는 전송되는 동안 양방향 암호화가 가능한가?	○
	원격 접근 포트는 목록화 되어 있고 사용되지 않는 포트는 사용 불가능하게 만들어져 있는가?	○
	시스템 제작 회사에서 만들어진 원격 접근 포트는 사용을 하지 못하게 하였는가?	○
하드웨어	모든 장비는 안전한 곳에서 보호되는가?	○
	전체 장비들의 목록을 유지하는가?	○
	서버는 잠금 장치가 된 곳에 위치하며, 서버가 있는 위치의 접근은 "카드키 접근 시스템"등을 통해 로그되는가?	○
	서버가 있는 곳은 물과 불의 위험이 없고 천정까지 연결된 벽이 있는가?	○
	연결 포인터는 보호되어야 하고 늘 감시되는가?	○
	jacks, jumpers, cross-connections, routers 등도 보호되는가?	○
	모든 외부 장치들은 주기적으로 감시되는가?	○
	케이블은 은닉되는가?	×

해당 지표별로 세부 항목을 체크하여 표 4.2와 같은 결과를 얻을 수 있었다.

<표 4.2> 보안성평가 결과

평가부문	지 표 명	만족도(%)	필수항목 준수여부
보안성	접근제어	85	준수
	패스워드	87.5%	준수
	서버	83%	준수
	백업	75%	준수
	통신	87.5%	준수
	하드웨어	87.5%	준수

이를 바탕으로 적용한 네트워크의 보안성은 전체적으로 볼 때 필수항목을 준수하고 있으며 전체적으로 80%이상의 만족도를 보여 양호하다고 할 수 있지만 백업부분이 75%로서 미흡한 것을 확인 할 수 있다.

5. 결 론

이 논문에서는 먼저 네트워크를 구축하고 관리하는 방법론을 도출하고 그것에 바탕을 둔 지표를 개발하였으며 또한 네트워크를 평가할 수 있는 기준을 제안하여 실제 네트워크 실험을 통해 적용성을 입증하였다.

2장의 네트워크 구축방법론은 학계에서 다양한 연구 진행이 되어 있지 않아 접근하는데 많은 어려움이 있었다. 또한 3장의 보안성평가의 각 세부항목의 기준 값들이 그것을 제시하고 있는 원전에 따라 서로 상이하여 통일성을 기하는데 매우 어려웠다.

2장과 3장에서 제시하고 있는 사항을 다시 한 번 요약하면 네트워크 구축은 분석단계, 설계단계, 시험단계, 구현 및 운용단계로 나눌 수 가 있으며 각 단계별로 제시하는 목표는 분석단계에서 정보요구, 기능요구, 성능요구, 보호요구, 접속요

구, 다양한 서비스요구이며 설계단계에서의 목표는 기능성, 확장성, 서비스계속성, 변경가능성, 네트워크단순성, 실현가능성, 표준 및 시스템과의 호환성이며 또한 시험단계에서의 목표는 시기성, 대역폭, 신뢰성, 중요도, 비용이며 마지막으로 구현 및 운용 단계에서는 단순성과 간편한 구성, 데이터전송량, 비용 대비 효과, 네트워크 관리 및 통제, 관리가능성, 보안, 교육 등의 목표를 달성하도록 하여야 한다. 그리고 구축된 네트워크의 보안성부문 평가를 위해 고려해야할 지표를 제시하고 있으며 지표별로 네트워크 감리 활동에 적용할 수 있는 기준값을 제시하였다. 보안성부문에서는 필수항목을 두어 필수항목을 반드시 만족하도록 하여 네트워크에서 보안의 중요성이 날로 증대되고 있는 현실을 반영하였다.

이 논문은 중·대규모의 네트워크에 적용할 수 있을 것으로 기대된다. 공공기관 및 기업이 계획하고 있거나 구축하고 있는 대다수의 프로젝트는 적용할 수 있을 것으로 보인다. 다만 가정내 홈네트워크의 적용에는 ADSL등의 장비를 다루지 않아 다소 한계가 있을 것으로 판단된다.

본 연구는 네트워크 자체가 대단히 다양하고 복잡하며, 신기술이 급속도로 적용되고 있기 때문에 모든 사항을 전부 정리하지 못하였지만 네트워크 전문가가 네트워크 분석/설계/구축/감리 업무를 수행함에 있어 함께 고려하고 검토해야할 기본적인 지표를 정리하였으므로, 네트워크에 대한 이해를 요하는 관련 종사자에 도움이 될 수 있을 것으로 보인다 향후 네트워크에 대한 다양한 지표를 체계적으로 연구하고자 하는 첫걸음이라 할 수 있다.

참고문헌

[1] 한국정보통신인력개발센터, "삼성SDS, "SI를 위한 방법론 innovator", pp.239-247, 2001.

[2] 정보기술교육원, NETWORK 설계기법, 1998.

[3] 정진욱, 컴퓨터네트워크, 희중당, 1999.

[4] 한국정보통신인력개발센터, "IT-Networker", pp.212-214, 2001.

[5] 김동윤, "근거리통신망(LAN) 구축 지침서",http://ccl.chungnam.ac.kr/QosIP/LANcont/LAN/guide.htm, 1998.

[6] 박동석, The Study of Developing an Index for Evaluating the Quality of The Network, 2000 성균관대학교 석사학위 논문

박 동 석

1995년 서울산업대학교 전자공학과(공학사)
2001년 성균관대학교 정보통신공학과(공학석사)
1999년 정보통신 기술사
1995년 ~ 현재 서울시청 DMC(디지털미디어시티) 추진단
2001년 ~ 현재 성균관대학교 컴퓨터교육과 겸임교수
관심분야 : 네트워크 보안, 도시계획과 정보통신 인프라, 미디어스트리트, 유비쿼터스

안 성 진

1988년 성균관대학교 정보공학과 졸업 (학사)
1990년 성균관대학교 대학원 정보공학과 졸업 (석사)
1998년 성균관대학교 대학원 정보공학과 졸업 (박사)
1990년 ~ 1995년 시스템공학연구소 연구 전산망 개발실 연구원

1996년 정보통신 기술사 자격 취득
1999년 ~ 현재 성균관대학교 컴퓨터교육과 조교수
관심분야 : 네트워크 관리, 트래픽 분석 ,보안관리

정 진 욱

1974년 성균관대학교 전기공학과 학사
1979년 성균관대학교 대학원 전자공학과 석사
1991년 서울대학교 대학원 계산통계학과 박사
1982년 ~ 1985년 한국과학기술 연구소 실장
1981년 ~ 1982년 Racal Milgo Co. 객원연구원
1985년 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부 교수
관심분야 : 컴퓨터 네트워크, 네트워크 관리, 네트워크 보안