Journal of Next-generation Convergence Information Services Technology Vol.4, No.2, December (2015), pp. 65-82
차세대컨버전스정보서비스기술논문지

교육기관에서의 효율적인 네트워크 보안관리 모델에 관한 연구

A Study on Effective Network Security Management Model of Education Institute

구천열[1], 김용성[2]*

Cheon-Yel Ku[1], Yong-Sung Kim[2]*

요약

오늘날 인터넷 접속과 사용률은 기하급수로 증가되고 있고, 인터넷 서비스에 따른 해킹과 바이러스의 위험부담은 상대적으로 증가했지만, 네트워크 시스템을 구축하고, 관리하는 인원과 예산은 매우 빈약한 수준이다.

따라서 지속적인 국가 교육 정보화 사업 확대에 따라 각종 보안 문제가 대두됨에 따라 이러한 문제점을 보완하기 위해서 효율적인 교육 기관 성격별, 보안 유형별 대책 마련이 내·외적으로 필요하게 되었다. 보다 효율적인 전산 보안 관리시스템이란 사용자 기반의 서비스를 가능하게 하고, 적은 인원의 관리자로 시스템의 구축 및 관리가 가능하기 때문에, 본 논문에서는 이를 합리적으로 수행할 수 있는 방안을 수립하여 적용하는데 목적이 있다.

핵심어 : 보안, 보안모델, 해킹, 해커, 바이러스, 보안 관리 시스템, 네트워크 보안 관리 모델

Abstract

Increasing Internet connections and computerization causes side- effects like exposure on cracking and viruses, although it have improved the network security management system in education. But, in fact, there is no outstanding solution for schools to cope with its security problems and possible derived risks.

Based on investigation - how schools understand security, how they 're currently prepared, and what makes security difficult for schools to deal with - we will consider the number of security technologies, and would like to suggest an effective network security management model that is compatible with schools. We hope that this model will be able to guide the schools on considering their security system construction.

Keyword : Security, security model, hacking, hackers, viruses, security management system, network security management model

1 Department of Computer Engineering, Chonbuk National University 664-14 DuckJinDong, DuckJin-Gu, Jeonju, Korea e-mail : cyku@jbnu.ac.kr

2 Department of Computer Engineering, Chonbuk National University 664-14 DuckJinDong, DuckJin-Gu, Jeonju, Korea e-mail: yskim@jbnu.ac.kr (Corresponding author)

Received(June 22, 2015), Review(July 16, 2015), Accepted(December 02, 2015), Published(December 31, 2015)

ISSN: 2384-101X JNCIST

1. 서론

교육 정보화 사업에는 성적관리, 생활기록부 관리, 교과 과목 관리, 클럽활동, 학급회의, 단체 활동 등의 중요한 교육 정보 자료를 취급한다. 이런 중요한 정보는 사용과 관리 못지않게 중요한 문제점은 해킹이나 바이러스 등 같은 외·내부 침입에 대한 보안의 문제이다. 오늘날과 같은 급속한 정보 사회에서는 안정적인 통신 환경과 주요 교육 정보 자원들의 손실 및 유출의 방지를 예방하기 위한 방안이 수립되어야 한다. 특히, 오늘날에는 보안사고가 자주 발생되고 있기 때문에, 정보 보안 관리 시스템을 체계적으로 관리할 필요성이 그 어느 때 보다도 증대되고 있다. 그러나 국내에서는 보안관리 관리 체계가 선진국에 비하여 빈약할 뿐만 아니라 관련 기술, 인력 등이 부족하여 효율적이고 실용적인 보안관리가 이루어지기 어려운 실정이다[1]. 따라서, 본 논문에서는 효율적인 네트워크 보안관리 체계를 위한 내·외부 보안의 시스템의 구축 방안을 제시하고, 이를 교육계에 활용할 수 있도록 하는데 연구의 주목적이 있다.

이를 위해 국내 주요대학 초, 중, 고 교육행정기관들의 전산 보안 현황을 조사 분석하여 교육기관의 내적이고 외적인 전산 보안 시스템의 문제점을 파악하여, 교육기관에서 효율적인 네트워크 보안관리 모델을 제시하고, 이를 설계 구현하고 평가하는데 본 논문의 의의가 있다.

2. 관련연구

2.1 전산보안

보안의 출발점은 자신이 가지고 있는 정보를 보호하려는 차원에서 보안이라는 개념이 도입되었다[2]. 보안의 의미는 여러 가지로 해석할 수 있으나 그 중에서 정보시스템과 관련하여 보안의 정의를 내리면 다음과 같다. 허가 받은 사용자들은 정보 시스템에 접근하여 원하는 정보를 얻을 수 있고 일부 정보들은 데이터의 안전과 공동체의 이익을 위하여 이러한 정보의 접근은 제한되어야 한다. 즉, 사용자들에게는 최대한의 편의를 제공하면서 시스템과 정보에 대해서는 안전을 기하는 것을 의미한다.

전산 보안을 지켜지기 위해서는 가용성, 무결성, 비밀성의 3가지 조건이 만족되어야 한다[3].

첫째, 가용성(availavility)은 특정조건이나 환경에 관계없이 효율적으로 서비스를 제공하고 데이터에 접근할 수 있도록 하는 시스템의 능력이다. 이것은 문제 발생 후 얼마나 신속하게 복

구가 가능한가에 따라서 평가되어 진다.

둘째, 무결성 (Integrity)은 사용자들에게 정확한 정보를 제공하고 유지하기 위한 시스템의 능력이다. 또한 이것은 하드웨어, 소프트웨어 또는 허가 받지 않은 사용자에 의해 데이터가 훼손되지 않을 것이라는 것을 확신시켜주는 에러 체크 기능 등을 포함하고 있다.

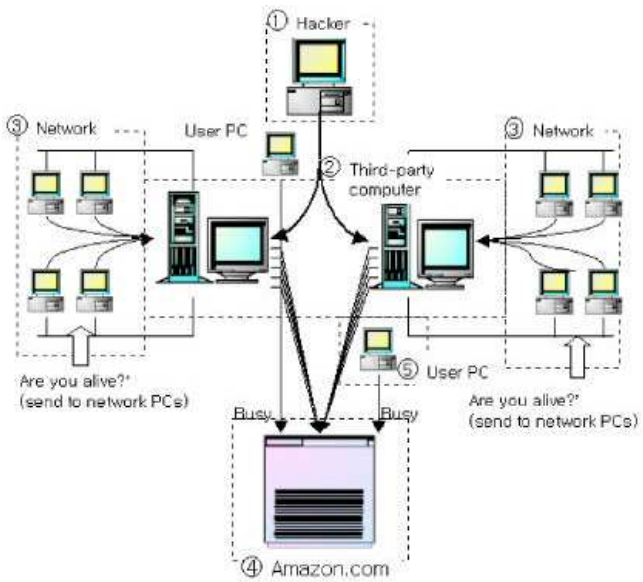
셋째, 비밀성 (Privacy) 은 정보가 허가 받지 않은 사용자에 의해 누설되거나 공개되어지는 것을 방지하는 시스템의 능력을 말한다.

위와 같은 조건들이 만족되었을 때 전산 보안이 이루어졌다고 할 수 있다.

2.2 해킹

해킹은 권한이 주어지지 않는 사용자가 사용 권한이 없는 기능들을 사용하기 위해서 불법적인 행위를 하는 것을 의미한다. 해킹의 대표적인 공격 방법으로는 IP Spoofing, Packet Sniffing, NFS attacks, E -mail related Attacks, Network Scanning 등이 있다.

최근 발생한 해킹 사례로서 전자 상거래 업체로 유명한 Amazon의 사례를 들어본다. 사실 Amazon 뿐만 아니라, Yahoo, Buy , eBay , CNN, ZDNet , E*Trade, DATEK, EXcite 등의 세계 유명 웹사이트가 같은 방법으로 해킹을 당한 사건으로 [그림 1]은 해킹 방법을 모형화 한 것이다[4].



[그림 1] 아마존 해킹 모형도

[Fig. 1] Amazon hacking models

2.3 전산보안의 기법

2.3.1 방화벽 (Firewall)

방화벽은 일반적으로 외부로부터의 불법적인 접근이나 해커의 공격으로부터 내부의 네트워크를 효과적으로 방어해주는 시스템을 말한다.

방화벽의 구성은 두개의 네트워크 사이에서 두 네트워크 간에 이루어지는 접근에 대해 제어할 수 있는 기능을 지닌 소프트웨어 및 하드웨어로 구성된다[5]. 이러한 방화벽은 외부의 공격이나 해킹으로부터 내부 네트워크의 자원 및 정보를 효과적으로 보호해주면서 또한, 내부 네트워크로부터 외부 네트워크로의 불필요한 접근을 효과적으로 제어해줄 수 있다.

방화벽이 모든 보안을 완벽하게 지원하는 것은 아니다. 방화벽 시스템은 내부 사용자가 내부 네트워크에 존재하는 중요한 정보를 디스크 혹은 테이프와 같은 매체를 통해 가지고 나가는 것은 방어하지 못한다. 또한 외부 네트워크로부터 바이러스 혹은 정보 지향적인 공격에 대해서는 방어하지 못한다.

따라서 방화벽 시스템은 보호하고자 하는 네트워크의 자원이나 정보들을 완벽하게 불법 침입자로부터 보호할 수 없으며, 다만 외부 네트워크에서 내부 네트워크로의 진입을 1차로 방어해주는 기능을 수행하므로 방화벽만으로 모든 보안 기능을 수행 할 수 없다. 방화벽 시스템의 기능을 지원하기 위해서는 사용자 인증, 접근제어, 트래픽 암호화, 트래픽 로그, 감사 추적 기능과 같은 정보보호 서비스가 필요하다.

2.3.2 암호화

암호화 (Encryption)는 자료의 기밀성 (cryptography) 을 보장하는 방법이다. 암호화는 원래의 자료 (Message) 와 그것을 암호화하는 키 (key) 와 암호화된 자료 (CryptedMessage) 와 그 암호화된 자료를 원래의 자료로 복원시키는 키 (key) 등으로 구성된다[6][7].

일반적으로 정보보호의 목적 달성을 위한 방법 중 가장 강력한 기술로서 암호 시스템의 활용을 들 수 있다. 즉, 암호 시스템의 합리적인 사용을 통하여 정보시스템과 정보통신망에서 유통되는 다양한 정보에 대한 비밀성과 무결성을 확보 할 수 있으며 더 나아가 정보기술 환경의 가용성의 확보가 가능하다.

2.3.3 사용자 계정과 암호

사용자 계정과 암호는 어떠한 시스템의 인증을 받는 중요한 보안 방법이다[8]. 안전한 시스템을

구축하는데 있어서 사용자의 신원 확인 및 인증은 매우 중요한 요소이다. 정보에 대한 접근, 자원에 대한 접근, 소프트웨어의 개발, 그리고 어플리케이션의 사용 등에 앞서 모든 사용자는 반드시 신원이 확인되어야 하며 인증 절차를 거쳐야 한다. 이러한 과정은 보안시스템을 구축하는 첫 번째 단계라고 볼 수 있다.

3. 네트워크 보안관리 시스템 분석

3.1 조사방법

본 논문에서는 교육기관에서 네트워크 보안관리 시스템의 보안 관리방안을 제시하기 위해서 인터넷이 연결된 교육기관을 대상으로 계단 총화 추출방법에 의해 초, 중, 고 32개교, 대학교 16개교, 교육청 160개 곳을 대상으로 하고, 설문지 참여 대상은 각 기관 전상망 운영자와 그 기관의 일반 사용자로 조사대상자를 정한다.

3.2 설문지 요구사항 추출

교육 전산 시스템의 사용자를 사용 목적에 따라서 크게 두 가지 부류의 사용자로 분류할 수 있다. 서비스를 사용하고자하는 일반 사용자들과, 사용자들의 요구사항을 서비스 해주고 시스템을 관리하는 시스템 관리자들로 구분하였다.

첫째, 사용자와 관리자 공동 모니터링 항목은 네트워크 사용시간, 해킹의 의미, 보안이 필요한 이유 네트워크에서 중요한 서비스와 형태, 그리고 시간 등의 요목이다.

둘째, 컴퓨터 시스템 일반 사용자와 모니터링 항목은 개인 PC 에 대한 바이러스와 해킹의 감염 여부와 대체방안, 보안 사고에 대한 대비책, 다른 사용자의 접근과 허용, 계정과 암호의 변경 주기 등에 대한 항목 등이다

셋째, 전산관리자 모니터링 항목은 네트워크 전반에 대한 것으로 하드웨어 구성요소, 보안실태와 보안 점검요소, 외부보안을 알아보기 위한 항목, 보안 설치요소와 활용법, 내부보안 점검과 시스템 지원요소, 정보보안 방법과 절차 등 보안 관리시스템의 전반적인 요소에 대한 항목들이다.

3.3 현황분석

각 교육기관의 전산시스템 규모가 다르고, 취급하는 정보의 중요성과 관리방법이 다르기 때문에

각 교육기관을 분리해서 현황을 분석한다.

3.3.1 분석결과

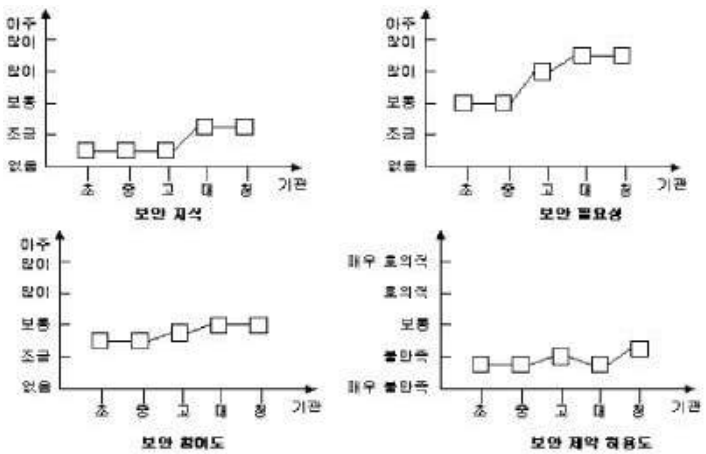
설문지 응답자는 관리자 68명과 일반 사용자 136명으로 중, 고교가 다른 곳보다 다소 낮은 편이다.

[표 1] 설문지 조사 응답률
[Table 1] Respondents of the survey

구 분		초등학교	중학교	고등학교	대학교	교육청
관리자	인원	12	12	12	16	16
	응답	4	3	3	12	10
	응답률	66.6%	25%	25%	75%	62.5%
일반 사용자	인원	24	24	24	32	32
	응답	8	6	6	24	20
	응답률	66.6%	25%	25%	75%	62.5%

가. 일반 사용자

일반 사용자에 대한 설문지 모니터링 항목으로는 보안에 대한 기본적인 지식과 보안의 필요성을 인식하고 있는가를 모니터링 하였을 뿐만 아니라, 보안의 참여도와 보안 시 가해지는 통신 시스템 사용 제약의 허용도를 모니터링 하였다.

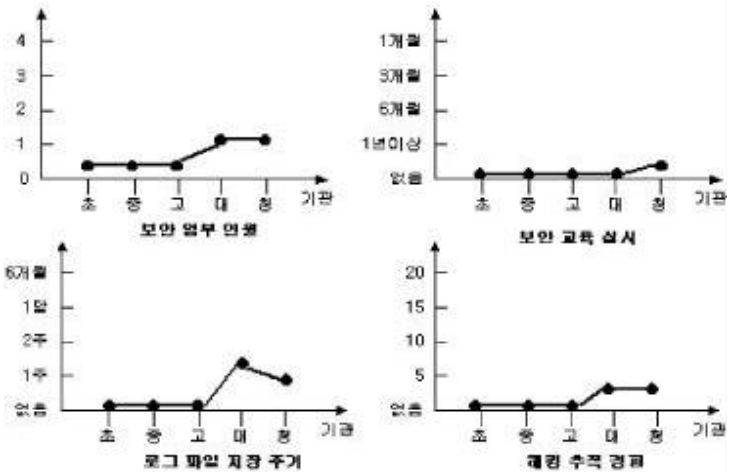


[그림 2] 일반 사용자 보안 의식
[Fig. 2] General security-conscious users

나. 관리자

관리자 설문조사의 모니터링은 보안 실태 파악과 내부 보안, 외부 보안으로 나누어서 모니터링 하였다.

① 보안 실태 파악



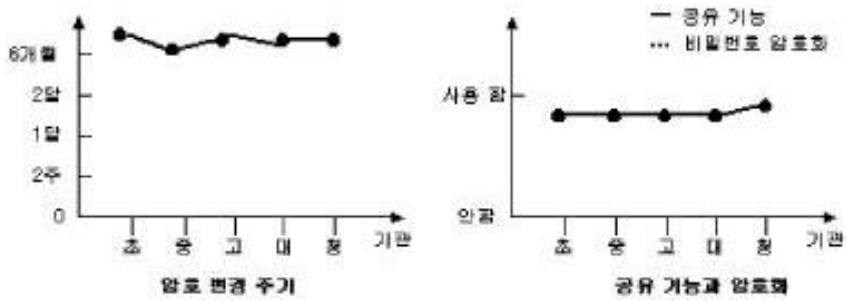
[그림 3] 보안 실태 파악

[Fig. 3] Actual conditions of security

각 기관의 보안 업무 인원이 1명을 넘지 못하고 있다. 보안 문제에 관한 관리자의 부족이 각 기관마다 나타나고, 이러한 관리자의 부족으로 보안교육은 거의 이루어지지 않고 있고, 특히 초·중·고등학교의 관리자인 경우 컴퓨터 환경에 대한 전반적인 지식이 부족한 것으로 나타나고 있다. 기본적으로 로그 파일도 저장하지 않고 있다.

② 내부 보안

서버 루트 (root , Administrator) 의 암호의 변경 주기는 모든 기관이 거의 변경하지 않는 것으로 나타나고 있고, 공유 기능을 많이 사용하고 있지만, 이렇게 중요한 데이터를 암호화는 하지 않는 것이 매우 큰 문제점이다.



[그림 4] 내부 보안

[Fig. 4] Internal security

3.3.2 현행 전산보안 시스템의 문제점

현행 전산 보안 시스템의 분석결과 주요 문제점을 도출하여 정리하면 다음과 같다.

첫째, 개방성의 문제 - 일반적으로 보안보다는 개방에 의한 이용 효과가 우선적이어야 한다. 그러나 개개의 구성 호스트를 자체의 기본적인 접근 제어나 암호들로는 불충분하다.

둘째, 금전적인 제한 - 보안을 위한 방법에 있어서 인적, 물적 자원에 대하여 충분하지 못하다. 보안 도구의 경우 새로 개발 한다던가 상용 제품을 구입하는데 많은 제약이 따른다.

셋째, 관리자 부재 - 교육망 전체에 대한 보안 행위의 책임자는 정해질 수 있지만, 구성하는 내부 망들에 대해서는 각각에 대한 책임 및 관리자를 지정하기 힘든 경우가 대부분이다.

넷째, 사용자 교육 - 사용자들은 그 사용에 있어서 구속이나 책임이 가해지기 힘든 학생들이 다수이고, 이들에 대한 보안 교육이 이루어지기 힘들다.

다섯째, 암호화 - 일반 사용자나 관리자 모두 중요한 데이터가 발생해도, 암호화를 하지 않고 평문 상태의 데이터를 전송하거나, 컴퓨터에 저장하고 있다. 이것은 해커가 컴퓨터에 침입했을 때, 아무런 제약 없이 중요 데이터의 정보를 알 수 있기 때문에 암호화가 필요하다.

여섯째, 데이터 백업 - 해킹이나 바이러스에 의해서 서버가 파괴된 경우 중요 데이터나 서비스의 복구를 위해서 데이터를 백업해야 한다.

4. 효율적인 네트워크 보안 관리 시스템 모형

네트워크을 통한 정보유출, 파괴 등으로부터 막을 수 있는 전산망 보안문제를 기관의 유형별로 현황을 파악하고 문제점을 제기하기 위해서, 유형별 교육기관에서 전산망 관련 업무에 종사하는

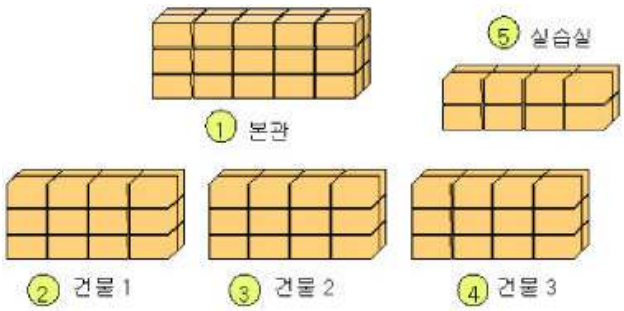
사람들의 의견을 종합하여 기관의 성격별 적정한 전산망 보안 모델을 제시하고자 한다.

4.1 시스템구성

전산망에 대한 적절한 보안정책을 수립하기 위해서는 먼저 전산망의 특성을 파악 한후, 이에 따른 보안 목표와 그에 따른 보안 수준을 정해야한다. 전산 보안은 전산망 자체의 성격과 특수성에 따라 꼭 필요한 선택 보안 기능과 선택적인 보안 기능 그리고 불필요한 보안 기능들이 존재한다.

4.1.1 네트워크 보안관리 시스템 환경 설정

네트워크 보안관리 시스템 모형을 설정하기 위한 테스트 베드는 인원 500정도의 하나의 단과대학을 대상으로 다음 환경을 가정하여 모형을 설계 한다.



[그림 5] 가상 건물 모델
[Fig. 5] Virtual building model

[가정 1] 전산망을 설계하기 위해서 [그림 5]과 같이 총 5개 건물로 구성된 가상 건물 모델을 설정한다.

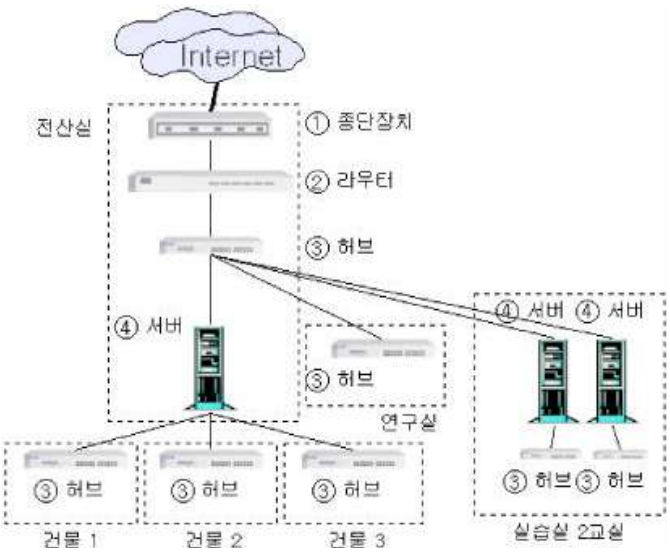
[가정 2] ①번 건물은 본관이다. 본관에는 전산소가 존재하고, 전산소에 네트워크 서버가 존재하며, 내부 네트워크를 관리하고 인터넷과 연결된다. 그리고 교수연구실들의 PC에 LAN이 연결된다.

[가정 3] ② ~ ④번은 3층 건물 세 동이 있다. 이 건물의 1층에는 학생들이 수시로 인터넷이나 교내에서 제공하는 서비스를 사용할 수 있도록 10대의 PC에 통신이 가능하도록 한다.

[가정 4] ⑤번 건물은 실습실이다. 실습실은 2곳이고 이곳에는 각각 W/S 이 존재하며 학생의 실습을 위해서 통신에 연결된 PC를 40대로 가정한다.

4.1.2 네트워크 보안관리 시스템 구성

4.1.1의 가정에서 전산망에 대한 백본망을 설계하기 위해서 본 논문에서는 다음과 같은 사항을 고려하면 [그림 6]와 같다.



[그림 6] 네트워크 백본망

[Fig. 6] Network backbone

첫째, 네트워크 장애로 인한 시스템의 중단 없도록 백업망을 구성하고, 장애시 백업망으로 우회가 가능하도록 네트워크 안전성 및 신뢰성을 고려한다.

둘째, 네트워크 장비의 통합 관리 장애 예방 및 복구가 가능해야 한다.

셋째, 네트워크 장비의 호환성을 고려한다.

넷째, 전원 이중화 등 주요 장비의 장애 대책 및 예비 장비를 확보해야 한다.

4.2 제안하는 보안관리 시스템 모형

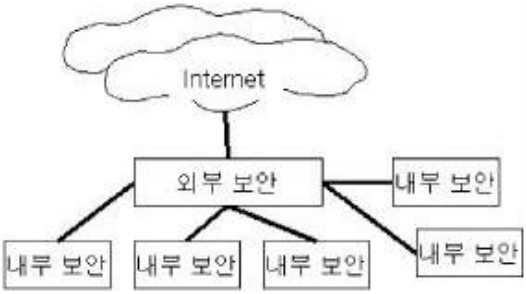
제안하는 보안관리 시스템의 전체 모형은 다음 [그림 7] 과 같다.

4.2.1 내부보안

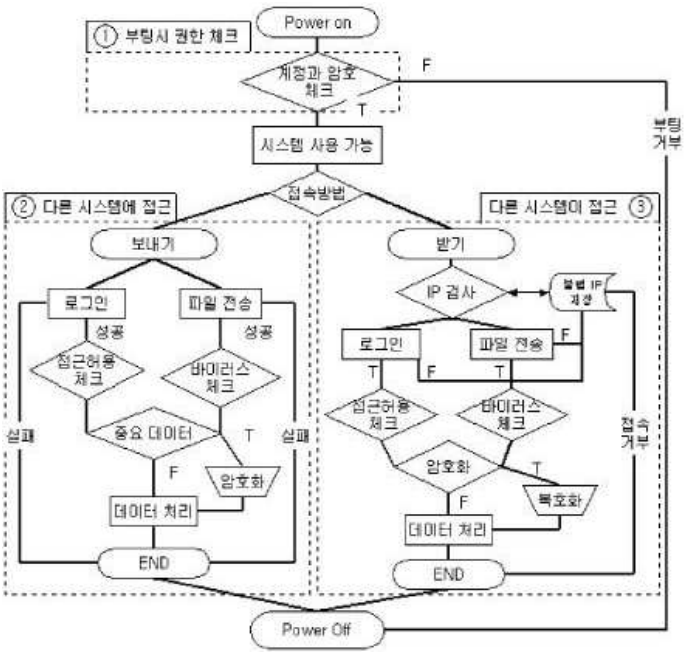
내부 보안은 자체 네트워크의 보안에 관한 내용이다. [그림 6]에서 설계한 백본망에서의 건물 1, 2, 3과 연구실, 그리고 실습 교실 2곳과 서버에 해당하는 부분이다. 내부보안은 시스템을 작동시키

는 것에서부터 사용이 완료되고 시스템의 동작이 완료할 때까지의 보안이다. 내부 보안의 경우에는 개인 PC가 주를 이루기 때문에 부팅시의 계정을 체크하는 부분과 다른 시스템에 접속하는 부분, 그리고 다른 시스템이 접속을 해오는 경우로 나누어 보안을 생각 할 수 있다.

[그림 7]은 내부 보안을 하는 방안을 도식한 것이다. [그림 8]에서 ①은 부팅 시 권한을 체크하는 부분이고, ②은 다른 시스템에 접속하는 경우 ③은 다른 시스템이 접속을 해오는 경우이다.



[그림 7] 전체 보안 모형도
[Fig. 7] Complete security model



[그림 8] 내부보안 모델 플로
[Fig. 8] Internal security model flow

(1) 부팅 시 권한 체크

[그림 7]의 ①번 부분의 알고리즘을 살펴본다. 시스템이 처음 작동을 시작하면 운영체제가 작동을 시작한다. 이 보안의 운영체제가 완전히 작동되기 전에 권한을 체크하는 부분이다. 이 기능은 각 시스템의 CMOS 셋업에서 설정을 할 수 있지만, Board의 스위치를 조정함으로서 삭제가 가능하므로 S/W로 구현하면 부팅 시 권한 체크 알고리즘은 [그림 9]와 같다.

```
입력 : 사용자 계정, 암호
출력 : 시스템 가동

chkBootAdmin ( char login, char password )
{
   time timer = 0
   if (timer < 30) {
      if (계정 = "login" AND 암호 = "password") {
         System Start
         break();
      }
      else {
         "에러 메시지"
         repeat;
      }
   else
      system shutdown
      break
   }
}
```

[그림 9] 부팅 알고리즘

[Fig. 9] Booting algorithm

```
입력 : 평문 데이터, 사용자 키
출력 : 암호화 데이터

const c1 = 52847
const c2 = 22719

encrypt ( char content, int key )
{

   byte i
   char tmpCont
   for (i=1; i <= length(content); i++)
   {
     tmpCont = tmpCont + char(byte(content[i]) xor (key shr 8))
     key = (byte(tmpCont[i] + key) * c1 + c2;
   }
   result(tmpCont)
}
```

[그림 10] 암호화 알고리즘

[Fig. 10] The encryption algorithm

```
입 력 : 접속IP, 계정, 암호
출 력 : 접근 허용

chkConnect ( login, password, ConnectIp )
{
   int i = 0
   query('select Ip from wrongIpTable')

   while not query.EOF
   {
     if (ConnectIP = Ip)
        "접속할 수 없는 IP 에러"
        connect out
   }

   if (i < 5) {
      if (계정 = "login" and 암호 = "password") {
         System Start
         break();
      }
      else {
         i++;
         "에러 메시지"
         repeat;
      }
   else
      insert into wrongIpTable values ('ConnectIp')
      connect out
      break;
   }
}
```

[그림 11] 불법 IP 체크 알고리즘

[Fig. 11] Illegal IP check algorithm

```
입 력 : 암호화 데이터, 사용자 키
출 력 : 평문 데이터

const c1 = 52847
const c2 = 22719

decrypt ( char content, char key )
{

   byte i
   char tmpCont
   for (i=1; i <= length(content); i++)
   {
     tmpCont = tmpCont + char(byte(content[i]) xor (key shr 8))
     key = (byte(content[i] + key) * c1 + c2;
   }
   result(tmpCont)
}
```

[그림 12] 복호화 알고리즘

[Fig. 12] Decryption algorithm

(2) 다른 시스템에 접속

[그림 7]의 ②는 시스템의 사용 중 다른 시스템으로의 접근에 관한 것이다. 사용자가 다른 시스템으로 접근하는 경우를 2개로 분리해서 처리하였다. 처리하는 데이터가 중요 데이터인지를 체크해서 암호화 처리를 통해서 데이터를 송신한다. 파일의 송신인 경우에는 바이러스 체크를 먼저해서 상대편 시스템에 바이러스가 걸리지 않도록 주의한다.

여기에서 중요한 것은 암호화 부분이다. 통신을 하다 중요한 데이터를 사용할 때 암호화를 한 다음에 데이터를 전송한다. [그림 10]는 암호화에 관한 알고리즘으로 encrypt ()함수를 선언하였다. 이 함수는 인자로 내용 (content) 과 비밀 키 (key) 를 입력받는다. 이 알고리즘은 비밀 키 알고리즘을 사용하고 있다.

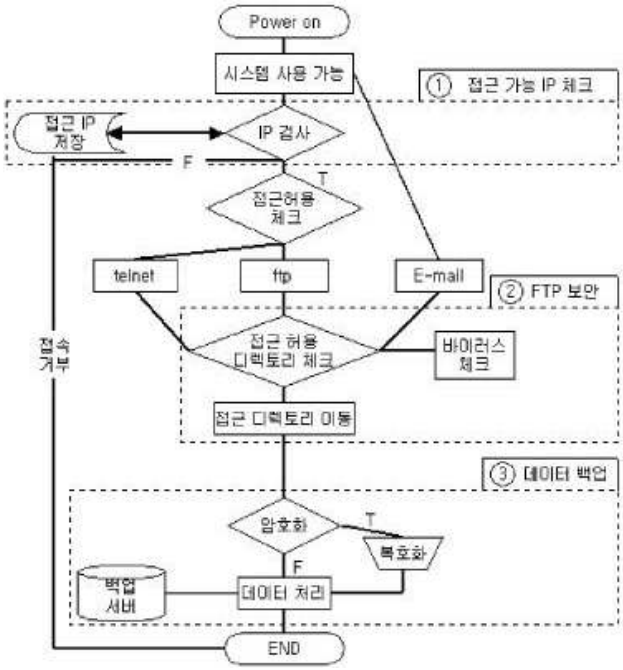
(3) 다른 시스템이 접근

[그림 7]의 ③은 시스템의 사용 중 다른 사용자가 접근해 오는 것에 관한 것이다. 다른 사용자가 시스템으로 접근하는 또한 2가지 경우를 분리해서 처리하였다. 제일 먼저 접근하는 IP를 체크한다. 악의를 가진 사용자가 접근하는 경우 사용자 계정과 암호를 직접적으로 알 수 없고, 허가를 가지고 있는 사용자도 실수로 계정과 암호의 입력이 틀릴 수 있다. 그래서 만약 계정과 암호의 입력이 5회 이상 틀리면 접근하는 IP를 불법 IP 테이블에 저장하고, 접근해오는 IP가 이 테이블에 존재하면 바로 접근할 수 없도록 한다. 그리고 사용자 계정과 암호가 일치하면 접근을 허용한다. 만약 인증될 수 있는 사용자의 IP가 실수로 저장되면 관리자에게 문의해서 불법 IP 테이블에서 삭제를 요구하는 방법으로 다시 사용할 수 있게 한다. 다른 하나의 처리는 사용자가 암호화된 데이터를 보내면 암호화된 데이터를 복호화하고 데이터를 사용한다. [그림 11]은 불법 IP 체크 알고리즘이다.

[그림 12]는 암호화되어 전송된 데이터를 평문 데이터로 복호화 하는 과정이다. 이 알고리즘에서 사용되는 사용자 키는 암호화 과정에서 사용한 사용자 키와 일치해야만 복호화가 가능하다.

4.2.2 외부보안 관리시스템 모형

[그림 13]은 외부 보안을 도식화 한 것이다.



[그림 13] 외부 보안 플로

[Fig. 13] External Security Flow

(1) 접근 가능 IP 체크

[그림 12]의 ① 접근 가능 IP 체크 부분의 알고리즘을 살펴본다. ①의 가장 안전한 방법은 서버 시스템으로 접근하는 모든 포드와 IP로의 접근을 차단해서 서버 시스템으로의 접근을 근본적으로 할 수 없게 만 드는 것으로 접속가능 IP 체크 알고리즘은 다음과 같다.

```
입 력 : 접속 IP
출 력 : 로그인 화면

chkServerConnect (char ConnectIp)
{
   int i = 0
   int count = 0
   query('select Ip from connectIpTable')

   while not query.EOF
   {
     if (ConnectIP = Ip)
        count++
   }

   if (count < 1)
   {
     "접근 에러 메시지"
     connect out
   }
   else
     if (계정 = "login" and 암호 = "password") {
        System Start
        break();
      }
      else {
        "에러 메시지"
        repeat;
      }
   }
}
```

[그림 14] 접근가능 IP 체크 알고리즘

[Fig. 14] Accessible IP check algorithm

(2) FTP 보안

[그림 12]의 ②는 ftp 보안에 관한 내용이다. 일반 사용자가 인정된 IP로 계정과 암호로 인증을 부여받은 후 권한을 행사한다. 사용자가 자신의 홈 부분의 디렉토리 이동을 가능하게 하고, 그 외의 나머지 부분은 접근조차 할 수 없도록 사용자 등록 시 설정한다.

(3) 데이터 백업

[그림 12]의 외부 보안에서 ③ 데이터 백업에서는 두 가지 종류의 기능이 존재한다. 하나는 만약 데이터가 암호화되어 있으면 데이터를 복호화 하는 것이다. 만일의 경우에 시스템의 고장이나 해킹이나 바이러스로 인해 문제가 발생하면 이를 즉시 복구하는 해결책이다. 주 서버에 문제가 발생하면 [그림 6]의 백본망에서 실습실에 존재하는 서버로 서비스를 복구한다. 백업에는 특정의 디렉

토리와 파일을 보존하는 소규모의 백업과 파일시스템 (파티션) 전체를 보존하는 대규모의 백업이 있다. 이 부분의 관리자가 데이터의 중요도에 따라서 백업을 한다.

5. 결론

본 논문에서는 교육 기관 시스템의 효율적인 네트워크 보안관리 모델을 구축하고 평가하는데 목적이 있다. 이를 위해서 교육 전산망의 특징적인 문제점을 파악하기 위해서 설문지를 일반 사용자와 보안을 관리하는 관리자 유형 2가지로 분리해서 전자메일을 사용하여 설문을 실시하고, 이 결과를 분석하여 현행 교육전산 보안시스템의 문제점을 파악하였다. 이 조사에서 발견된 보안 문제점들을 해결하기 위해서 가상 네트워크 모형을 설계했고, 이 모형을 대상으로 네트워크 보안관리 모델을 내·외부로 분리해서 설계하고 구현하여 효율적인 네트워크 보안관리 모델을 제안하였다.

내부 보안은 부팅 시 사용자 계정과 암호를 체크하는 부분과 다른 시스템에 접근 시 바이러스 체크, 중요 데이터 발생 시 암호화하는 보안 기법을 사용했고, 다른 시스템이 접근 해오는 경우는 접근 IP를 검사해서 불법 IP 저장 테이블에 존재하면 접근을 거부한 후 사용자 계정과 암호를 물어보고, 파일 전송 시 바이러스 체크, 암호화 데이터가 존재하면 복호화를 실시한다.

외부 보안은 시스템 접근 시 접근 IP 저장 테이블에 IP를 검사해서사용자 계정과 암호를 체크한 후 접근을 허용한다. FTP 보안으로는 접근 사용자의 홈 디렉토리 이외에는 접근을 허용하지 않고, 전자메일은 바이러스를 체크한다. 암호화 데이터는 복호화를 실시하고, 일정기간이 지나면 주기적으로 데이터 백업을 한다.

향후 연구로는 본 논문의 전산 기관 시스템의 효율적인 네트워크 보안관리 모델은 가상의 소규모의 단과 대학을 대상으로 구성하였기 때문에 본 논문에서 제안한 모델의 확대 적용과 효율성과 정확성을 체크하기 위한 모니터링 시스템 구축하고 운영하여, 그 효율성을 검증하는 것이다.

ISSN: 2384-101X JNCIST

References

[1] http:// www.certcc.or.kr/, Retrieved: Nov 10, **(2015)**.

[2] C. Brenton, "Mastering Network Security", **(1998)**.

[3] D. M. Kienzle, "Practical computer security analysis", Thesis (Ph. D.), University of Virginia, 1998. Includes bibliographical references (leaves 141- 148), **(1998)**.

[4] "Hunting the Hackers", Newsweek, **(2000)** February 21, pp. 36-42.

[5] M. R. Haake, "Firewall implementation", Computers: Computer security . Security . Network access policies . Firewall. Computer industry, **(1999)**.

[6] W. Bellingham, "Security and watermarking of multimedia contents II", **(2000)** January 24- 26, San Jose, California.

[7] http://home.ahnlab.com/, Retrieved: Nov 10, **(2015)**.

[8] B. K. Kim and T. M. Chung, "Current Trends and Prospects in Intrusion Detection Technology", Korea Information Science Security, vol. 18, no. 1, **(2000)**, pp. 29-39.