네트워크 이중 인증을 통한 역할 기반 개방형 네트워크 접근 통제 시스템의 구현

정회원 이 춘 재*, 조 기 량**

Role-Based Network Access Control System on Open Network Two-Factor Authentication

Chun-jae Lee*, Ki-ryang Cho** ***Regular Members***

요 약

본 논문은 네트워크 기반(L2, MAC ADDRESS)과 어플리케이션 기반(L7, ID/PASSWORD)의 이중 인증 시스템을 구현을 통하여 허용되지 않은 자원과 사용자의 네트워크 접속을 차단할 수 있는 방안을 제시하였다. 인증 게이트웨이 시스템은 중앙 관리 서버로부터 보안/인증 정책을 물려받아 모든 패킷을 허가/차단/제어한다. 사용자의 컴퓨터에 에이전트 없이 모든 클라이언트의 자원(H/W, S/W)을 수집하며 OS 패치 여부 및 바이러스 감염 여부 등을 체크하여 안정적인 네트워크를 운영하고, 침해 사고가 발생한 때에도 신속히 대응 할 수 있는 방안을 제시하였다. 또한 유무선 네트워크의 경우, IEEE802.1x 인증을 요구하는 시스코 NAC에 비해 구축이 용이하고, 비용 절감을 실현할 수 있는 방안을 제시하였다.

Key Words : Two-factor authentication, Authenticating gateway system, Agent

ABSTRACT

This paper proposes a method to shut out all of the not certified network access packet by embodying the two-factor(MAC ADDRESS, ID/PASSWORD) authentication system. The Authenticating Gateway System takes over central server's policy and permit or hold up the packet by inherited policy. And checks the whether or not patched the OS version and getting influenced from computer virus. And takes the information about client's resources(H/W, S/W) without Agent in the client. That makes more stability of network operating circumstance and fast facing the attack from hackers. In the fixed mobile network circumstance, This method provides more simplicity and less expenses than IEEE802.1x authentication system(cisco nac).

Ⅰ. 서 론

IT인프라에 기반을 둔 업무 환경에서 내부보안 공격[1]으로 심각한 재정적인 문제 등을 초래한다.

일반적으로 기존의 맥 어드레스(L2) 기반 네트워크 접근 통제 시스템은 하드웨어 자원에만 접근 권한을 부여하는 단일 인증 방식으로 무선 네트워크 환경 및 대학이나 관공서와 같이 사용자가 수시로 바뀌거나 공용 시스템을 사용하는 개방형 네트워크의 경우에는 불특정 다수의 사용자에 의해 발생하는 침해 사고에 대한 대응[2]이 사실상 불가능하다.

즉, 내부 네트워크 망이 광범위해지고, 내부 사용자수가 급속하게 증가하는 개방형 네트워크 내에서 물리적 자원(PC)인증과 인적 자원(사용자)인증을 통합 관리해야 하는 문제점이 발생하고 있다.

따라서 내부 사용자에 의한 침해 사고를 예방하

* 전남대학교 전자 통신공학과 (jason@nyinfo.co.kr), ** 전남대학교 공학대학
논문번호 : KICS2007-04-196, 접수일자 : 2007년 4월 27일, 최종논문접수일자 : 2007년 7월 18일

기 위해서는 네트워크 접속 권한을 자원별/사용자별로 이중 관리하고, 사용자의 내부 네트워크 접근 발생 시간, 물리적 위치, 사용자 PC상태(바이러스 감염 여부, 보안 패치)에 대한 정보를 중앙관리자가 효율적으로 제어하고, 관리해야만 한다.

본 논문에서는 유동인구가 많은 개방형 네트워크 내에서 맥 어드레스(L2) 인증방식의 단점과 유무선 네트워크 접근제어시스템(NAC)[3]의 단점을 보완하여 불특정 단말기와 사용자를 일치시켜 보다 유연성 있는 네트워크 인증관리 방법을 제시하였다. 또한 내부 보안 공격에 대처하기 위해 네트워크 이중 인증 방식을 통해서 내부 네트워크에 접근하는 자원에 대해 내부 자원/구성원 여부를 판별하며, 또한 각 조직별 그룹에 따른 적절한 정책을 할당하고, 사용자 인증 과정에서 시스템의 보안 패치 상태 점검 및 시스템 자원 수집과 IP 관리 등의 작업을 클라이언트 PC에 에이전트 설치 없이 적절하게 조치할 수 있는 방안을 연구하였다.

Ⅱ. 네트워크 이중 인증 시스템 설계

IEEE802.1x[4]는 무선 랜의 인증에 대한 표준이며, 이는 포트를 기반으로 제어를 수행하는 방식으로써 사용자가 접속하는 네트워크의 물리적인 포트를 제어하므로 가장 강력한 사용자 인증 및 제어 정책에 해당한다. 또한 유선환경에서는 IEEE802.1x 인증 클라이언트의 비용이 무료라는 장점으로 최근 시스코 NAC과 같은 유무선 네트워크 접근제어 인증프로토콜로 사용 되어진다.

그러나 PC에 설치될 IEEE802.1x 클라이언트의 지원을 위해 Windows XP 이전 OS에서는 별도의 전용 에이전트 소프트웨어가 필요하고, IEEE802.1x를 지원하지 않는 액세스 스위치 장비를 업그레이드해야 하는 비용 부담 등의 문제점이 발생 한다. 또한 시스템이 너무 많고 파악조차 되지 않는 개방형의 네트워크에서 각 실 자체적으로 조달하여 사용하고 있는 스위치나 허브, AP 등의 IEEE802.1x 미 지원 호스트들의 예외 처리 문제점들로 인하여 서비스 확산에 커다란 걸림돌로 작용하고 있다.

이러한 문제점들을 해결하기 위하여 본 논문에서는 아이디/패스워드 방식과 맥 어드레스 방식의 2가지 인증 방식을 조합[5]한 유무선 통합 TCP/IP 기반의 네트워크 이중 인증 관리 시스템을 제안하였다.

그림 1은 제안한 네트워크 이중 인증 시스템의 제어 프로세스를 나타낸 것으로 우선, 사용자 컴퓨터가 네트워크 접속을 시도할 때에 발생되는 ARP 패킷을 이용한 L2 기반 1차 시스템 인증 단계[6]를 거치고, 다음에, 웹 브라우저를 통해 특정 목적지 접근을 시도하는 때에 기간 데이터베이스에 등록된 사용자 아이디와 패스워드를 판별하는 L7 기반 2차 사용자 인증 단계[7]로 설계하였다.

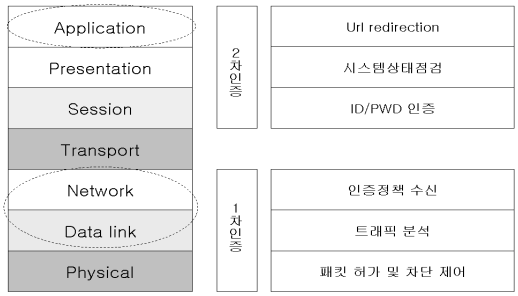


그림 1. 제안한 네트워크 이중 인증 시스템의 제어 프로세스

2.1 이중 인증 관리 시스템 구성

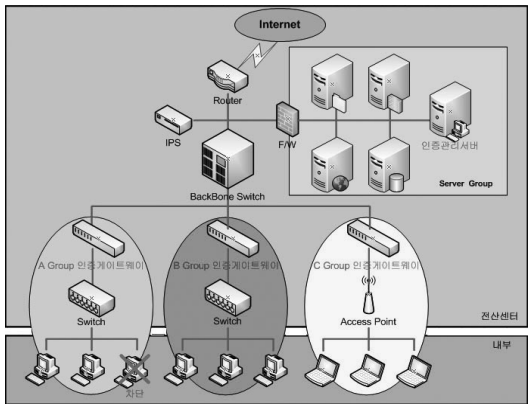


그림 2. 제안한 네트워크 이중 인증 시스템의 구성

그림 2는 본 논문에서 제안한 네트워크 이중 인증 시스템의 구성도를 나타낸 것으로써 중앙관리자에 의해 그룹화 된 서브 네트워크 단위별로 패킷 필터 인증 게이트웨이[8]를 브리지 형태로 각각 서브 네트워크에 위치시키고, 다수의 인증 게이트웨이를 관리하는 인증 관리 서버를 DMZ 구간 안에 위치시켰다.

또한, 인증 그룹은 단위 조직별 또는 지역별로 융통성 있게 적용할 수 있게 하기 위하여 패킷 필터 인증 게이트웨이를 단위 네트워크에 위치 시켰으며, 인증 스케줄(일간, 주간, 월간, 인증 없이 자원 수집)을 통해 보다 융통성 있는 인증 시스템을 구현할 수 있도록 설계하였다.

2.2 패킷 필터 인증 게이트웨이

그림 2에서 백본 스위치의 아래 단(각 그룹 액터의 최상단)에 위치한 패킷 필터 인증 게이트웨이는 브리지 방식의 게이트웨이로서 사용자의 ARP 패킷 검출 및 패킷 차단 필터 제어[9] 등의 기능을 수행한다. 또한 인증을 받지 않은 사용자가 웹 브라우저를 통해 특정 목적지 접근을 시도했을 때에 URL Redirection[10]을 통해 인증 시스템으로 유도하는 역할을 한다.

패킷 필터 인증 게이트웨이는 RAM DISK[11] 방식의 파일 시스템으로 구성하여 안정적이면서 빠른 패킷 필터 처리 속도 확보와 불법 사용자의 시스템 침입 및 변경/조작에 대비하였다. 인증 게이트웨이 시스템은 시스템 기동과 동시에 중앙 관리 서버에서 사용자 인증 정책에 관한 모든 정보를 전달받아 RAM DISK로 인증 정책을 로딩한 뒤에 해당 인증 정책에 의해 내·외부로 지나가는 모든 패킷을 허가, 차단, 제어하는 기능을 수행한다.

2.3 인증 관리 서버

인증 관리 서버는 다수의 패킷 필터 인증 게이트웨이의 시스템 환경 설정 파일과 각각의 그룹별 인증 정책, 패킷 필터 인증 게이트웨이의 각종 로그 등을 관리하고, 모니터링 하며, 실시간으로 사용자의 시스템의 인증, 차단, 허가 등의 작업을 수행한다.

Ⅲ. 제안한 이중 인증 시스템의 인증 절차

3.1 인증 순서

제안한 인증 시스템에서는 클라이언트 PC에 에이전트를 설치하지 않고 네트워크 사용자들을 인증 시스템으로 유도하기 위해 패킷 필터 보안 게이트웨이를 사용하여 2단계 인증 프로세스로 구성하였다. 기본적으로 패킷 필터 인증 게이트웨이는 사전 허가 대상(서버 시스템, 무인 발급기, 공용 프린터 서버 등)을 제외한 모든 시스템의 패킷을 차단하며, 다만 인증 대상의 패킷의 목적지가 인증 서버이면서 80포트인 패킷만 허용한다.

클라이언트가 최초로 IP를 할당 받을 때에 발생하는 ARP 패킷으로 맥 어드레스를 추출하여 사전 차단 및 허가 대상자인지를 판단하는 1차 인증 단계와 차단 대상자가 아니며, 인증 받지 않은 사용자의 HTTP 패킷을 인증 시스템으로 URL Redirection시킴에 따라 사용자를 별도의 조작 없이 인증을 유도하는 2차 인증 단계로 구분한다.

3.2 인증 대상 분류

제안한 시스템에서의 네트워크 인증 대상은 사용자와 시스템을 포괄하여 다음과 같이 4가지로 분류하였다.

① Q검증이 완료된 서버나 증명 발급기/네트워크 프린터/무인 시스템 등과 같은 사전 허가 시스템
② 내부 네트워크 접근 권한이 없는 허가되지 않은 불법 사용자
③ 네트워크 접근 권한이 없지만, 단기간 내부 네트워크에 접근해야 할 임시 사용자
④ 조직 내 네트워크 사용 권한이 부여 받은 인증 사용자

위의 인증 대상별 인증 시스템의 제어 위치는 표 1과 같이 구성하였다.

표 1. 인증 대상별 제어 위치

인증 대상	제어 위치
인증 사용자	L2 / L7 인증 후 허가
임시 사용자	L2 / L7 인증 후 허가
불법 사용자	L2 기반 차단
사전허가 시스템	L2 기반 허가

3.3 인증 정책 적용

광범위한 네트워크 관리 시에는 지역적으로 예외적인 인증 정책을 적용해야 하는 문제점이 발생한다. 이러한 문제점을 해결하기 위하여 중앙 관리자에 의해 인증 대상을 그룹화 하여 각 그룹별로 독립적인 인증 정책을 적용할 수 있도록 하였다.

인증 정책은 그림 3과 같이 일 단위 인증, 주 단위 인증, 월 단위 인증, 자동 인증 후 시스템 상태 점검과 자원 수집의 4단계 정책으로 구성하였다.

- 일간 (매일 시스템 인증 실시)
- 주간 (요일별 시스템 인증 실시)
- 월간 (매월 설정된 날짜별 시스템 인증 실시)
- 자원 수집 인증정책 (자동 인증 후 패치, 자원수집)

그림 3. 인증 정책

3.4 제안한 이중 인증 시스템에 의한 인증 구현

3.4.1 L2 기반 1차 시스템 인증 구현

본 논문에서 제안하는 L2 기반 시스템 인증 방식은 먼저, 패킷 필터 인증 게이트웨이가 기동되고, 중앙관리자가 설정한 인증 정책을 인증 서버로부터 수신한 다음, 시스템 메모리상에 차단/허가 목록을 저장하고, 인증 웹 브라우저로 가는 TCP 80을 제외한 모든 패킷 진입을 차단한다.

다음에, 사용자 시스템이 네트워크 접속을 시도했을 때에 발생하는 ARP 패킷을 분석하여 해당 맥 어드레스를 추출하는 단계와 해당 맥 어드레스의 변조 여부 및 실제 시스템 존재여부를 ARP 패킷을 이용해 판별하는 단계, 아이피 할당 이력을 인증 서버에 기록하는 단계로 구성되어 있다.

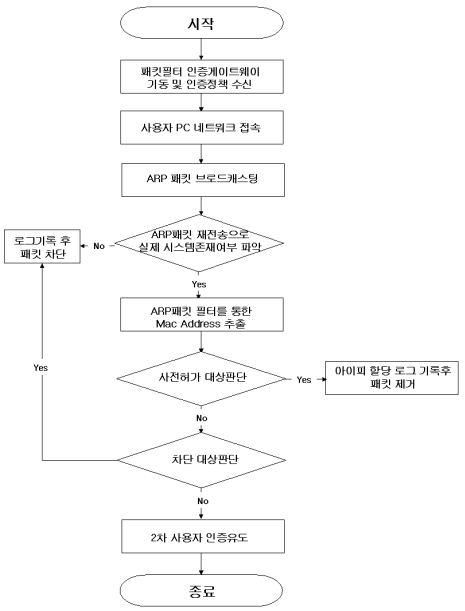


그림 4. L2 기반 1차 인증 프로세스도

아이피 할당이 완료된 시스템의 패킷은 인증 정책에 의한 허가 시스템/차단 시스템과 그 외의 인증 시스템으로 분류되어 허가 시스템의 모든 패킷은 2차 사용자 인증 단계 없이 진입이 허용되며, 차단 시스템 또한 2차 사용자 인증 단계 없이 모든 패킷이 차단이 된다. 차단 및 허가 시스템 이외의 모든 시스템의 80포트의 패킷은 인증 서버로 DNAT되어 2차 사용자 인증 단계(L7)로 이동하도록 되어 있다.

그림 4의 L2 기반 1차 인증 프로세스 도는 이들의 순서를 나타내고 있다.

3.4.2 L7 기반 2차 사용자 인증 구현

L7 기반 사용자 인증 방식은 1차 시스템 인증(L2) 시, 인증 시스템으로 판별된 시스템 사용자가 웹 브라우저를 통해 특정 목적지에 접근을 시도 할 때, 해당 80포트 패킷의 목적지를 변경해 사용자 웹 페이지를 웹 인증 페이지로 URL redirection 시킨다.

인증 페이지는 Active X 기술을 이용하여 사용자 맥 어드레스를 추출하여 1차 인증 단계에서 등록된 맥 어드레스와 일치하는지를 판단하여 비정상적인 패킷 변조에 의한 접근을 사전에 차단한다. 정상 접근이 확인된 사용자 시스템은 바이러스 감염 여부와 OS 패치 여부 등 안전성을 확인 한 후 네트워크 접속 가능 여부를 판단한다. 안전성이 확보되지 않은 사용자 시스템은 적절한 조치 후, 안전성을 재확인을 받게 된다. 안정성이 확인된 시스템은 사용자 아이디/패스워드를 입력받아 2차 사용자 인증을 실시하고, 인증이 완료되면 해당 그룹의 패킷 필터 인증 게이트웨이에 인증 완료 메시지를 보내 사용자 시스템을 실시간으로 허가하는 단계로 구성하였다.

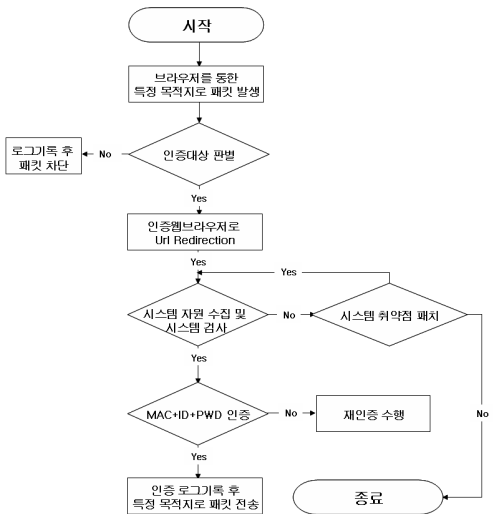


그림 5. L7 기반 2차 인증 프로세스도

L7 기반 2차 사용자 인증은 사용자의 인증뿐만 아니라 사용자의 시스템의 안정성과 보안성을 동시에 검사하여 내부 네트워크에 접근 여부를 판단함으로서 보다 안전하게 내부 네트워크를 운용할 수 있도록 하였다.

그림 5는 L7 기반의 2차 인증 프로세스 순서를 나타내고 있다.

Ⅳ. 이중 인증 시스템의 성능 평가

본 논문에서 제안한 이중 인증 시스템은 재학생 수가 약 3,000명, 4,000명 정도인 지방의 두 대학을 선정하고, 시스템을 적용하기 전과 후의 보안 패치 설치율 변화, 자산 관리, 트래픽 분석 및 시간대별 인증 통계를 통한 트래픽 사용량 분석 등을 통하여 성능 평가 및 효율성을 확인하였다.

4.1 제안된 기법 과 기존기법의 장단점 비교

네트워크 이중인증은 맥 어드레스(L2)인증의 장점이자 NAC 인증의 단점인 네트워크 하드웨어 추가 및 변경 같은 별도의 예외처리 없이 기존 어플리케이션에서 사용하고 있는 아이디/패스워드 인증 방식을 네트워크에 적용하였다. NAC 인증에 비해 에이전트 없이 패킷필터를 통한 URL Redirection으로 사용자와 단말기를 동시에 인증하는 네트워크 이중인증을 구현하였으며 사용자 인증과정에서 시스템의 취약점을 파악하여 네트워크 진입초기에 적절한 조치를 취함으로써 저비용으로 보다 안정적인 네트워크를 구성 할 수 있었다.

4.2 보안성 향상

보안 패치는 바이러스나 악성 코드에 대한 감염될 가능성을 없애기 위하여 설치된다. 네트워크 진입초기에 사용자 인증 웹페이지에서 보안 패치여부를 판단하여 적절한 조치를 취함으로써 안전한 상태의 PC만을 네트워크 접근을 허용한다. 그림 6은 제안한 이중 인증 시스템을 설치하기 전과 후의 보안 패치 설치 정도를 나타내고 있다. 그림에서 알 수 있듯이 시스템 설치 전의 일반적인 대학의 보안 패치 설치는 70~80 (%) 정도이나, 이중 인증 시스템을 설치하여 인증 전에 보안 패치를 검사하고, 자동으로 보안 패치를 설치함으로써 95(%) 이상(설치 전에 비해 20(%) 정도 향상)의 보안 패치 설치율을 나타내고 있다. 단, 제안한 이중 인증 시스템의 설치 후에도 보안 패치의 설치가 100(%)에 이르지 못하는 이유는 전산실에서 운영되고 있는 각종 서버, 특정 어플리케이션이 동작(무인 시스템, 리눅스 및 유닉스 시스템 등)하는 서비스 단말기는 윈도우 서비스 팩 및 보안 패치와의 시스템 충돌 가능성이 때문에 관리자에 의해 지정된 단말기는 패치 대상에서 제외하기 때문이다.

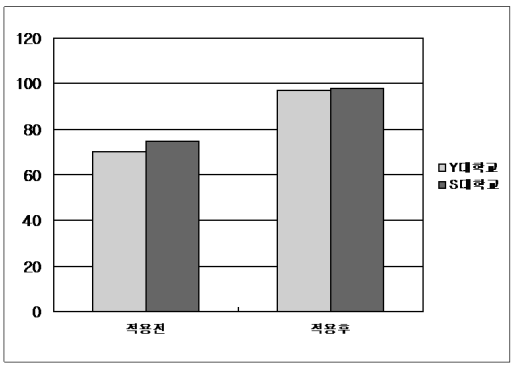


그림 6. 제안한 시스템의 적용 전후의 보안패치 설치율 변화

4.3 효율적인 자산 관리

본 논문에서 제안한 이중 인증 시스템은 사용자 인증 전에 실시되는 시스템 인증 단계에서 사용자 단말기의 보안성을 검사함과 동시에 사용자의 단말기에 설치된 소프트웨어 목록 및 하드웨어 사양을 서버로 전송하여 관리한다. 따라서 사용자 단말기에 에이전트를 설치하지 않고도 에이전트를 설치했을 때와 동일한 효과를 내는 장점이 있다.

그림 7, 8, 9는 제안한 시스템을 이용한 경우의 백신 설치 유형, 컴퓨터에 설치된 사용자의 소프트웨어, OS 등을 분석한 것이다.

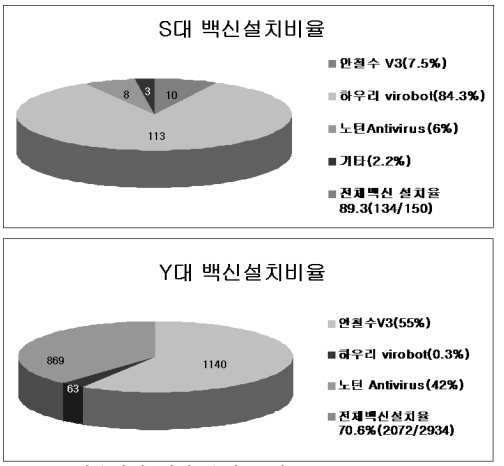


그림 7. 사용자의 백신 유형 분석

그림 8. 사용자의 소프트웨어 분석

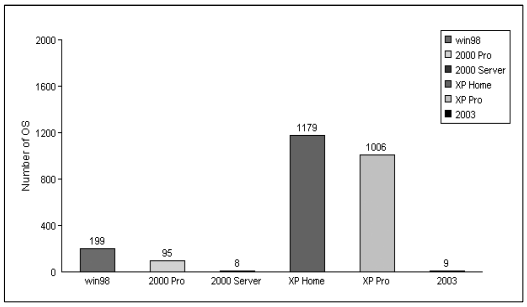


그림 9. 사용자의 OS 분석

4.4 트래픽의 효율적인 분산 관리

기존의 트래픽 관리 시스템과는 다르게 패킷 필터 인증 게이트웨이를 통해 수집된 실시간 트래픽 관리는 유해 트래픽을 유발하는 단말기 및 사용자 위치를 즉시 추적할 수 있다. 또한, 인증 그룹별, 시간대별 로그인 추이 및 최대 트래픽 발생 시간 등을 분석하여 트래픽을 효율적으로 분산 관리 할 수 있다.

소프트웨어 TOP 10 | 트래픽 Read TOP 10 | 트래픽 Write TOP 10

순번	트래픽	맥주소	아이피	아이디
1	681.49 Kbyte	00:16:76:2F:9F:20	168.131.225.48	
2	227.97 Kbyte	00:19:21:56:75:B9	168.131.233.142	
3	175.27 Kbyte	00:13:77:2B:25:19	168.131.232.120	
4	169.66 Kbyte	00:18:F3:E9:D4:2E	168.131.224.174	
5	159.68 Kbyte	00:01:39:04:3F:FE	168.131.221.154	sehui8
6	157.68 Kbyte	00:17:31:1A:26:10	168.131.219.80	
7	140.06 Kbyte	00:0B:6A:B9:20:02	168.131.234.228	mjy
8	134.27 Kbyte	00:14:2A:ED:0F:83	168.131.234.149	
9	126.73 Kbyte	00:1A:92:3C:30:76	168.131.232.59	
10	114.97 Kbyte	00:16:17:B5:E8:98	168.131.225.245	

그림 10. 트래픽 사용 리스트

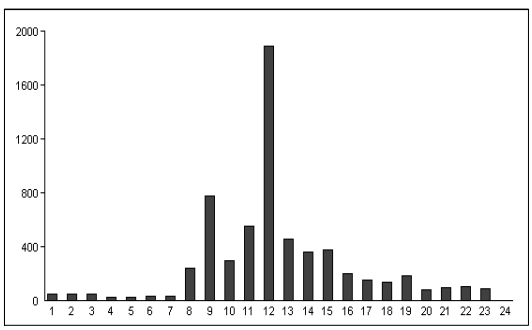
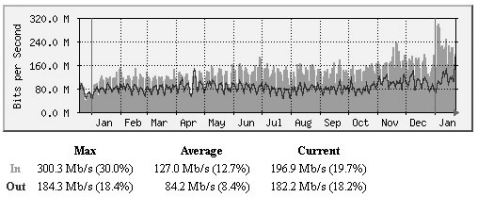


그림 11. 시간대별 평균 인증 통계

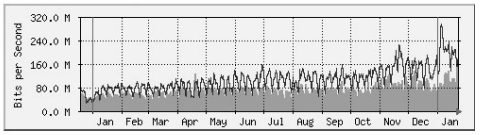
그림 10과 11은 각각 트래픽 사용 리스트와 패킷 필터 인증 게이트웨이를 통해 수집된 시간대별 인증 통계를 나타내고 있다.

그림 12는 이중 인증 시스템의 적용 전과 후의 패킷 필터 인증 게이트웨이를 통해 수집된 실시간 트래픽 현황을 나타낸 것이다. 여기에서는 일간, 주간, 월간, 년간 트래픽 사용 이력을 관리할 수 있다. 또한, 본 논문에서 제안한 시스템 구성 즉, 그림 2와 같이 패킷 필터 인증 게이트웨이를 통해 서브 네트워크별로 분산하여 트래픽을 관리함에 따라 특정 지역에 네트워크 장애가 발생하여도 여타의 단위 네트워크에서는 정상적으로 트래픽 관리를 할 수 있다.



	Max	Average	Current
In	300.3 Mb/s (30.0%)	127.0 Mb/s (12.7%)	196.9 Mb/s (19.7%)
Out	184.3 Mb/s (18.4%)	84.2 Mb/s (8.4%)	182.2 Mb/s (18.2%)

a) 시스템 적용 전



	Max	Average	Current
In	176.2 Mb/s (17.6%)	69.9 Mb/s (7.0%)	175.0 Mb/s (17.5%)
Out	292.2 Mb/s (29.2%)	105.5 Mb/s (10.6%)	190.3 Mb/s (19.0%)

b) 시스템 적용 후

그림 12. 트래픽 분석

V. 결 론

본 논문에서는 내부 보안 공격에 대처하기 위하여 아이디/패스워드 방식과 맥 어드레스 방식의 2가지 인증 방식을 조합한 네트워크 이중 인증 관리 시스템을 제안하고, 재학생수가 각각 약 3,000명, 4,000명 정도인 지방의 두 대학을 선정하여 시스템을 적용하기 전과 후의 보안 패치율 변화, 자산 관리, 트래픽 분석 및 시간대별 인증 통계를 통한 트래픽 사용량 분석 등을 통하여 성능 평가 및 효율성을 확인하였다. 그 결과,

① 바이러스나 악성 코드에 대한 감염될 가능성을 없애기 위한 보안 패치 설치율이 20(%) 이상 높아져 보안성이 향상되었다.

② 모든 인증 대상 시스템은 네트워크를 사용하기 위해 반드시 인증 페이지를 거쳐야 함으로 인증 페이지에서 사용자의 단말기에 설치된 소프트웨어 목록, 하드웨어 사양, 보안 패치 여부를 서버로 전송하여 관리하기 때문에 사용자 단말기에 에이전트를 설치하지 않고도 에이전트를 설치했을 때와 동일한 효과를 낸다.

③ 사전 허가 대상을 제외한 모든 시스템의 패킷

을 인증 전까지는 차단함으로써 불필요한 네트워크의 부하를 줄일 수 있으며, 인증을 통해 사용자 시스템 보안 점검과 적절한 조치를 취함으로써 기존에 보안 패치를 설치하지 않아 발생하던 문제점을 월등히 감소시킬 수 있으며, URL Redirection을 통한 웹 브라우저 인증으로 사용자 컴퓨터에 에이전트 설치의 부담을 줄임으로써 네트워크 사용 인증에 대한 거부감을 최소화할 수 있다.

④ Non 802.1x 기반 유무선 통합 네트워크 이중 인증은 TCP/IP기반 인증 시스템으로 IEEE802.1x 인증을 요구하는 NAC 인증에 비해 상대적으로 구축이 용이하고, IEEE802.1x 미 지원 클라이언트의 예외 처리 문제 및 네트워크 장비 업그레이드로 인한 추가 구축비용이 발생하지 않는다.

⑤ 패킷 필터 인증 게이트웨이를 각 단위 네트워크에 위치시켜 사용자 인증 기반 네트워크 접근 제어를 지역적으로 독립시켰으며, 개방형 네트워크 내의 복잡한 지역적 특성을 융통성 있게 수용하는 사용자 인증 시스템을 구현하였다.

참 고 문 헌

〔1〕 강민균, 김석수, "Design and Implementation of Security Solution Structure to Enhance Inside Security in Enterprise Security Management System", 한국콘텐츠학회논문지 제5권 제6호, pp. 360-36, .2005..

〔2〕 김우한, 최중섭, 홍관희, "정보통신 인프라 침해사고현황 및 대응체계", 한국통신학회지(정보통신) 제21권 9호, pp. 38-47, 2004.

〔3〕 Denise Helfrich, "Cisco Network Admission Control, Volume I : Nac Architecture and Design", CISCO PRESS, 2006.

〔4〕 이상렬, 박용진, "Design of PKI Cryptosystem Enabling Efficient Mutual Authentication on Wireless LAN", 대한전자공학회 논문지 TE 제41권 3호, pp. 69-78, 2004.

〔5〕 Bruce Schneier, "Thinking Sensibly About Security in an Uncertain World-The Failure of Two-Factor Authentication", Beyond Fear, 2005.

〔6〕 김수덕, 김기창, 김병룡, "Marking Algorithm 기반 IP 역추적의 공격 진원지 발견 기법", 한국정보과학회학술발표논문집 제29권 제1호(A), pp. 814-816, 2002.

〔7〕 서대희, 이임영, "A Study on Single Sign-On Authentication Model Using Multi Agent", 한국통신학회논문지, 제27권 7C호, pp. 997-1006, 2004.

〔8〕 김재한, 한기준, 백석철, "인증 게이트웨이를 활용한 ESM시스템의 개발", 한국정보과학회학술발표논문집 제30권 제1호 (A), pp. 509-511, 2003.

〔9〕 박대우, 서정만, "TCP/IP 공격에 대한 보안 방법 연구", 한국컴퓨터정보학회논문지 제10권 제5호, pp. 217-226, 2005.

〔10〕 김태웅, 류호연, 김성조, "RADIUS 서버를 이용한 사용자 인증 기반 URL 필터링 시스템의 설계 및 구현", 한국정보과학회학술발표논문집 제30권 제1호(C), pp. 433-435, 2003.

〔11〕 연준상, 양 오, "Flash disk와 Ethernet을 이용한 백업장치 개발에 관한 연구", 청주대학교 산업과학연구소 산업과학연구 제19권 1호, pp. 259-265, 2001.

이 춘 재 (Chun-jae Lee)

1987년 : 조선대학교 전산통계학과
2003년 : 조선대학교 전산통계학과 공학석사
2004년~현재 : 전남대학교 전자통신공학과 박사과정
멀티미디어 기술사
<관심분야> 적응제어, 네트워크 보안

조 기 량 (Ki-ryang Cho)

1981년 : 광운대학교 통신공학과
1983년 : 건국대학교 대학원 전자공학과 공학석사
2002년 : 일본 오카야마대학 자연과학연구과 공학박사
현재 : 전남대학교 공학대학 교수
<관심분야> 파동 · 압전문제의 수치해석, 최적제어 등