정책기반 무선네트워크 구현에 관한 연구

강오형*, 이지현*, 신성윤*, 박기홍*, 이양원*
*군산대학교 컴퓨터정보공학과
ohkang@kunsan.ac.kr, jhlee@kunsan.ac.kr, s3397220@kunsan.ac.kr, spacepak@kunsan.ac.kr, ywrhee@kunsan.ac.kr

A study on the policy-based wireless network implementation

Oh-Hyung Kang*, Ji-Hyun Lee*, Seong-Yoon Shin*, Ki-Hong Park*, Yang-Won Rhee*
*Dept of Computer Information Engineering, Kunsan National University

요 약

무선네트워크 환경에서 인증과 암호화를 함으로서 보안이 강화되는 효과가 있으나 무선네트워크를 이용하는 이용자들에 대한 권한이 동일하게 부여되면 접근성에 문제점이 대두됨에 따라 이용자 그룹별로 인터넷 이용에 대한 접근권한을 제어함으로서 다양한 학내 구성원, 계약직, 방문자, 시민 등 에게 보안측면과 운영상에 편리성을 가져올 수 있다. 관리자가 정책을 만들어 각각의 액세스포인트에 정책을 적용하고 사용자가 인증을 받을 때 인증서버에서 사용자에 대한 필터아이디를 액세스포인트에 전달해줌으로서 사용자에 대한 정책규칙이 적용된다.

키워드 : 무선 네트워크(Wireless Network), 정책기반(Policy-based), 인증(Authentication), 암호화(Encryption)

I. 서론

취약한 무선랜을 안전하게 보호하기 위해서는 각 사이트의 서비스 환경에 맞는 무선랜 보안 정책의 수립이 필수적이며, 보안 정책에 맞는 무선 보안 기술을 적용하여야만 한다. 이러한 상황에서 안전한 무선랜 서비스를 위해 도입해야할 무선 보안 기술에 대한 연구가 꼭 필요한 시점이다.

무선랜의 보안 취약점이 발생하는 근본적인 원인을 파악하고, 무선랜의 취약점을 이용한 공격에 대한 대비책을 마련해야만 한다. 우선 무선랜 운영자와 사용자에게 현행기술을 이용해 보안성을 제고할 수 있는 관리 및 운영 방안을 제안하고자 한다. 현재까지 제안된 기술만으로도 무선 상에서 보안의 3대 요소라 할 수 있는 인증, 기밀성, 무결성을 보장할 수 있다. 먼저 이러한 무선 보안 기술에 대해 분석하며, 해당 기술의 적용 방법을 파악해 나가야 한다.

하지만 현재까지 무선은 공유 매체라는 한계로 인해 사용자 권한별 접근 제어 정책을 펼 수가 없었다. 각 조직체에는 다양한 권한을 가진 다수의 사용자가 네트워크에 접근하는데, 유선 상에서는 사용자의 위치가 고정되어 있어 권한별 접근 제어가 용이하였다. 그렇지만 무선에서는 각 사용자의 위치가 언제든지 바뀔 수 있고, 이동함에 따라 기존 유선과 같은 접근 제어 정책을 적용하기는 힘들다. 이를 해결하기 위해 무선 상에서 적용할 수 있는 사용자 권한별 접근 제어 방법에 대한 연구가 필요하다[1].

결론적으로 안전한 무선사용을 위해 인증, 기밀성, 무결성을 보장할 수 있는 무선 보안 기술을 분석하여 적용할 수 있도록 하며, 여기에 무선 사용자의 권한에 맞게 접근 제어 정책을 펼 수 있는 기술을 추가하여 완벽한 무선 보안 환경을 구축할 수 있는 기술을 제시하고자 한다.

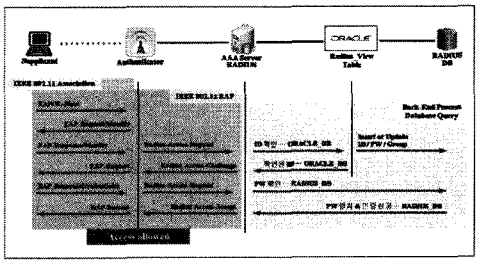
II. 관련 연구

인증 프로세스는 <그림 1>과 같이 크게 클라이언트 PC (Supplicant), 액세스 포인트(Authenticator), RADIUS 서버 (Authentication server)로 나뉜다.

클라이언트 PC는 망에 접근하려는 PC 등의 단말 사용자로 무선인 경우에는 무선 단말기를 말한다.

액세스 포인트는 클라이언트 PC와 RADIUS 서버 간의

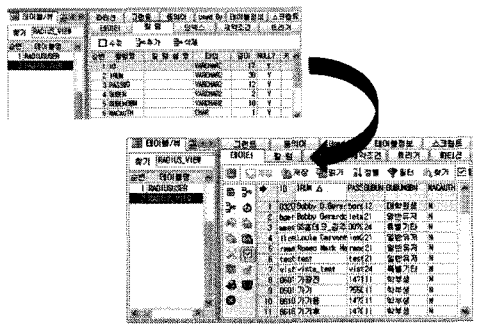
통신을 돕는 경유 장치 역할을 한다. AP와 클라이언트는 EAPOL(EAP Over LAN) 프로토콜을 사용하여 802.1x 메시지를 교환해서 클라이언트 스테이션에서 송신한 메시지가 AP를 거치면서 암호화된 뒤 EAP 확장자를 달아 RADIUS 서버로 전송된다[2].



〈그림 1〉 인증 프로세서 구성도

이 메시지는 대개 RADIUS 서버로부터 응답 EAP 패킷을 받는 즉시 EAPOL 형식으로 해석되어 클라이언트에게로 전송된다. 이제 클라이언트와 RADIUS 서버 사이에 의견 교환이 이루어진다. 인증 과정을 통과한 클라이언트는 자동 키 배포 기능이 있는 EAP 유형인 경우에는 AP로부터 암호화키를 받는다. 인증된 클라이언트는 이후로 이 키를 사용하여 데이터를 암호화한다.

RADIUS 서버는 인증 요구 패킷을 받으면, 접근 한 사용자의 계정 정보에 대한 허가를 위해 〈그림 2〉와 같이 구성된 뷰테이블 정보를 이용하여 ORACLE DB에 허가를 받고 승인이 보내지면 사용자에 대한 링크 필요조건 또는 사용자를 위한 서비스 수준을 정의하는 정책 정보와 같은 추가 정보를 보낸다. 이 뷰테이블은 인사, 학사, 추가등록 사용자 테이블 등을 참조하여 만들어지며 인증 시 구성원을 확인할 때 마다 참조되어진다.



〈그림 2〉 Oracle 데이터베이스 뷰테이블 구성

ORACLE DB의 뷰테이블 정보는 인증서버의 로컬 데이터베이스(SDB)와 SYNC를 통해 정보를 Insert 하거나 Update하며, 〈표 1〉의 형식에 따라 정보가 갱신 된다. 여기에서 GROUPID는 사용자 그룹별 정책에 반영됨에 따라 중요한 역할을 하게 된다.

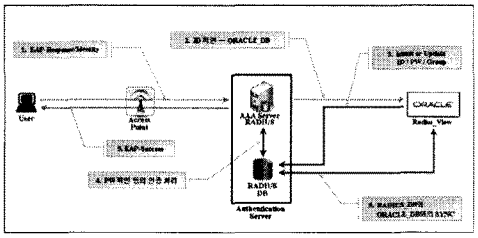
〈표 1〉 인증서버에서 관리되는 사용자 정보 목록

USERNAME	Varchar	NOT	인증클라이언트 사용자의 ID	사용자아이디
USERPASSWD	Varchar	NOT	인증클라이언트 사용자의 PASSWD	사용자패스워드
MACAUTH	CHAR	NOT	인증클라이언트 인증여부 값	MAC인증여부
REALNAME	Varchar		인증클라이언트 사용자의 이름	사용자 이름
GROUPID	Varchar	NOT	인증클라이언트 사용자의 그룹	그룹 아이디
AUTHTYPE	CHAR	NOT	PEAP	인증타입
USERMAC	CHAR		사용자의 아이디	사용자 맥주소
MAXSESS	INT4	NOT	1	최대세션
TPGID	Varchar		NULL	VLAN 아이디
IPADDRESS	Varchar		NULL	IPADDRESS
PHONENO	Varchar		NULL	전화번호
RECTIME	CHAR	NOT	현재시간	등록시간
STARTDATE	CHAR		NULL	시작시간
ENDDATE	CHAR		NULL	종료시간
STATUS	CHAR	NOT	Y	현재상태
ADMIN	CHAR	NOT	3	권한

Default Value

액세스 포인트는 망 접근을 제어하는 장치로 일단은 비제어 포트(Uncontrolled Port)에 접속한 후에, 성공적으로 인증이 되면 제어 포트(Controlled Port)를 이용하여 데이터를 전송 한다. 그래서 인증에 성공하기 전까지, 인증 받지 못한 클라이언트 PC는 AP를 통해 그 LAN의 다른 시스템으로 데이터 트래픽을 보낼 수 없다. 클라이언트 PC가 인증될 때까지 AP가 해당 클라이언트 PC로부터 오는 데이터 트래픽을 전부 차단하기 때문이다.

인증 상태를 불문하고 클라이언트 PC는 항상 암호화되지 않은 802.1x 메시지를 AP와 교환할 수 있다[3]. 이 때 사용자는 네트워크에 로그인하기 위해 사용자명과 암호를 입력하여야 하며, 입력된 사용자명과 암호를 사용하여 클라이언트와 RADIUS 서버 간에 상호 인증을 수행한다. 〈그림 3〉은 Oracle 데이터베이스를 이용한 실시간 사용자 인증 과정을 보여주고 있다.



〈그림 3〉 실시간 사용자 인증과정

RADIUS서버와 클라이언트는 현재의 네트워크 로그인 세션에 대한 WEP 키를 유도하며, 사용자명과 암호와 같은 민감한 모든 정보들은 암호화 처리되는 방식 등으로 인하여 악의적인네트워크 모니터링 및 다른 공격 등으로부터 보호할 수 있다.

또한, 802.1x EAP 기반 사용자 인증이 강력한 무선랜 보안 방식으로 떠오르면서 최근 들어 전문 솔루션들이 시장에 많이 출시되고 있으며, 무선랜을 도입할 때 인증 솔루션을 함께 구축하는 기업도 늘어나고 있다[4].

EAP 사용자 인증 방식에는 인증서를 사용하거나 마이크로소프트 윈도 운영체제에서 지원하는 기술을 이용해 아이디/비밀번호로 인증을 처리할 수 있는 TLS(Transprot Layer Security), TTLS(Tunneled Transport Layer Security),

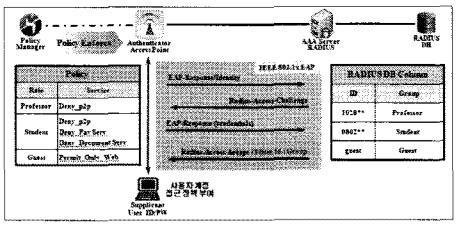
PEAP(Protected Extensible Authentication Protocol)이 있다[5].

주로 대학에서는 인증서버를 기반으로 TTLS와 PEAP이 이용되고 있으며, 사기업에서는 인증서 기반의 TLS도 많이 이용되고 있다. 모두 무선랜 장비에서 지원하고 있음에 따라 사용자 환경과 보안정책에 맞게 적절한 인증 방식을 선택할 수 있다.

III. 사용자 그룹별 보안정책 구성

무선네트워크 환경에서 인증과 암호화를 함으로서 보안이 강화되는 효과가 있으나 무선네트워크를 이용하는 이용자들에 대한 권한이 동일하게 부여되면 접근성에 문제점이 대두됨에 따라 이용자 그룹별로 인터넷 이용에 대한 접근권한을 제어함으로서 다양한 학내 구성원, 계약직, 방문자, 시민 등에게 보안측면과 운영상에 편리성을 가져올 수 있다.

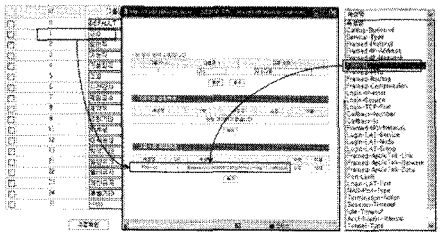
관리자가 정책을 만들어 각각의 AP에 정책을 적용하고, 사용자가 인증을 받을 때 인증서버에서 사용자에 대한 Filter-ID를 AP에 전달해줌으로서 사용자에 대한 정책규칙이 적용된다. <그림 4>은 그룹별 보안정책 구성에 대한 전체적인 구성을 보여주고 있다.



<그림 4> 그룹별 보안정책 구성도

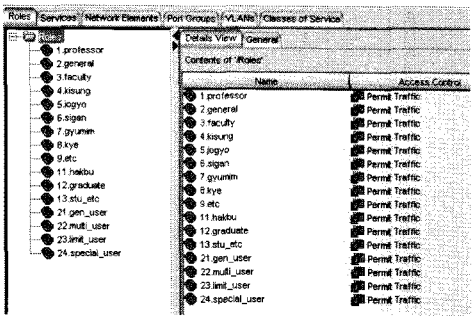
대학 캠퍼스에는 많은 AP(Access point)가 존재함에 따라 네트워크 관리자의 정책을 일관되고 신속하게 적용할 방법이 필요하다. 정책관리자(Policy manager)는 네트워크 관리자가 수립한 사용자 그룹별 정책을 AP에 일관적으로 신속하게 적용함으로서 관리자에게 편리성을 제공한다.

또한 인증서버(Radius Server)는 사용자가 요청한 아이디와 패스워드를 기반으로 인증서버에 인증을 요청하면 인증서버는 Oracle database에 View table 정보를 이용하여 구성원 유무를 판단하고 사용자 인증을 거친 후 인증된 사용자 그룹정보를 이용하여 Filter-ID를 AP에 전달해줌으로서 사용자에 대한 정책규칙이 AP에 적용 되어 차단 및 허용정책이 반영된다. <그림 5>는 인증서버에서 사용자 그룹정보와 Filter-ID 속성 값을 이용하여 AP에 회답해주는 과정을 보여주고 있다.



<그림 5> 인증서버의 Filter-ID 속성값을 이용한 그룹속성 회답

무선네트워크 환경에서 사용자 접근을 제어하기위하여 Netsight policy manager 프로그램을 이용하여 각 그룹에 대한 정책을 반영한다. 그룹정보는 16개로 구분되며 교직원 레벨의 그룹은 교수, 일반직, 기능직, 기성회직, 조교, 시간강사, 겸임교수, 계약직, 기타직원 등 9개로 나뉜다. 또한 학생그룹은 학부생, 대학원생, 기타 3그룹으로 나뉘며, 기타 사용자들을 위하여 4개의 그룹으로 분류된다. 학교에서 직원처럼 근무하고 있는 계약직등을 위한 일반사용자 그룹이 있고, 세미나 및 학술대회 등 큰 행사에 많은 인원이 동시에 무선인터넷을 이용할 수 있도록 멀티사용자 그룹이 있다. 또한 학교를 방문하는 손님과 시민들을 위한 제한사용자 그룹이 있으며, PMP, PSP, PDA 등 암호화를 지원하지 않는 장치들에 대한 인터넷 서비스 지원을 위한 특별 사용자 그룹이 있다. <그림 6>은 Policy manager에서 구성된 16개의 사용자 그룹 롤(Roles)을 보여주고 있다.

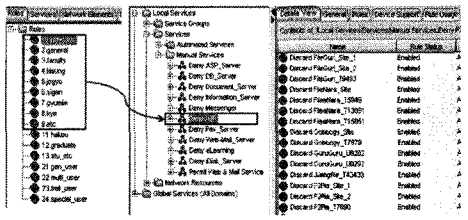


<그림 6> 16개 그룹으로 구성된 Roles

IV. 사용자그룹별 보안정책 구현

교직원 레벨의 그룹은 교수, 일반직, 기능직, 기성회직, 조교, 시간강사, 겸임교수, 계약직, 기타직원 등 9개로 나뉘며 일반적인 서비스는 모두 허용하고 P2P서비스에 대하여 차단정책이 적용된다.

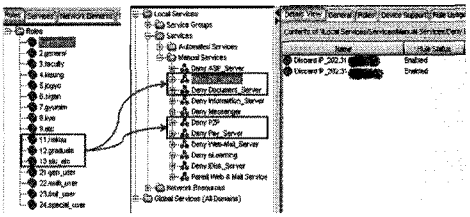
<그림 7>은 교직원 그룹 보안정책으로 P2P서비스는 차단되고 나머지 서비스는 허용되는 내역을 보여주고 있다.



〈그림 7〉 교직원 그룹 보안정책

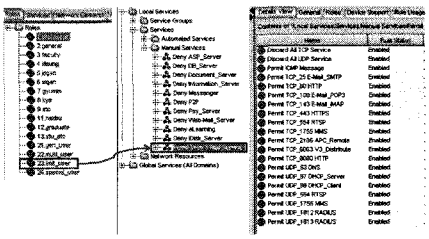
학생그룹은 학부생, 대학원생, 기타 3그룹으로 나뉘며 정보전산원 데이터베이스시스템, 전자문서시스템, 급여시스템, P2P 서비스 등이 차단되고 일반적인 서비스는 모두 허용되는 정책이 적용된다.

〈그림 8〉은 학생그룹 보안정책으로 학생들의 직접적인 접근이 필요 없는 시스템에 대한 접근을 차단함으로서 보안사고 예방에 대처할 수 있다.



〈그림 8〉 학생그룹 보안정책

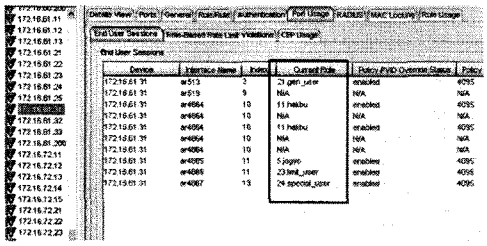
제한사용자 그룹은 사원번호가 없고, 학교에 방문하는 외부인 또는 시민들에게 별도의 사용자등록 절차 없이 무선인터넷 서비스를 이용하고자하는 사용자들로서 기본적으로 모든 서비스는 차단되며 관리자가 허용해주는 서비스에 한하여 이용이 가능하다.



〈그림 9〉 제한사용자 그룹 보안정책

〈그림 9〉는 제한사용자 그룹 보안정책으로 무선네트워크 관리자가 허용해주는 서비스로는 DNS, SMTP, POP3, IMAP, HTTP, HTTPS, Ping, RTSP, DHCP등 이며, 공개된 아이디는 Guest이고 패스워드도 Guest로 무선네트워크 홈페이지에 공지되어 있음에 따라 이용자들이 쉽게 접근이 가능하다.

〈그림 10〉은 특정 AP에 접속된 사용자들의 현재 롤(Roles) 상태를 보여주고 있으며, 사전에 정의된 그룹명에 의하여 관리자의 차단 또는 허용 정책들이 AP에 의해서 제공된다.



〈그림 10〉 AP에 적용된 사용자 Roles

V. 결론

많은 무선랜 운영자들은 무선랜 환경에 대한 막연한 보안 위협을 느끼면서도 실제로는 무선랜이 갖는 보안 취약성에 대해서는 간과하고 있다. 이러한 현상이 일어나는 이유로는 무선랜 정보보호 인식이 그리 높지 않다는 것과 무선랜이 갖는 보안 취약성과 보안 운영 등에 관한 정보가 부족하기 때문이다.

사용자 인증의 강화와 무선 데이터의 암호화 설정을 통한 보안성 증대가 더욱 절실할 것이다. 뿐만 아니라 무선랜 관리자 및 사용자의 보안 정책 수립과 이의 실행 여부 또한 중요하다. 기관에서 수립된 정보보호정책의 원활한 적용과 사용자의 참여의식 고취를 위해 정기적인 정보보호 교육이 필요하고, 이와 더불어 운영자 및 사용자의 철저한 보안 의식이 필요하다.

참고문헌

[1] Changhua He, John C Mitchell, "Security Analysis and Improvements for IEEE 802.11i" Electrical Engineering and Computer Science Departments Stanford University, Stanford CA 94305, 2005.

[2] V.Moen, H.Raddum, and K.J.Hole, "Weakness in the Temporal Key Hash of WPA" ACM SIGMOBILE Mobile Computing and Communications Review, Volume 8, Issue 2, pp. 76-83, 2004.

[3] 이제헌, "차세대무선랜 기술 및 표준화 동향", ETRI-전자통신동향분석, 제23권, 제3호, 2008.

[4] 정계옥, "무선네트워크의 취약점과 대응방안", 국가보안기술연구소, 2006.

[5] 이홍섭, "무선랜 안전운영 가이드", KISA-한국정보보호진흥원, 2004.