SPAM 서버를 이용한 초고속 IP 기반의 인증시스템 구축

이재완* · 고남영*

Authentication System Construction in a high-speed IP Infrastructure using Spam Sever

Jae-Wan Lee* · Nam-Young Ko*

이 논문은 2004년도 군산대학교 두뇌한국 21의 연구비를 지원받았음.

요 약

IP기반 초고속인터넷의 인증체계가 전송방식에 따라 인증·무인증 접속체계로 이원화되어 이용자의 적법성 확인, 네트워크의 접속 권환 및 자원 할당에 대한 이용자의 체계적인 인증정보의 관리가 미약했다. 또한 무인증 접속으로 시스템 및 네트워크의 부하 가중과 전송속도 저하로 이용자들의 욕구 충족이 어려운 실정이다. 따라서 본 논문에서는 인증-무인증 접속체계를 단일 인증시스템으로 통합하여 최적의 네트워크 환경을 구축할 수 있는 SPAM 서버를 이용한 인증 시스템 구축 방안을 제시하였다.

ABSTRACT

The authentication system of high-speed internet in IP-infra is not warm enough to administration of systematic authentication information for user's legalization, connection right and resources allocation in order to both methods of authentication-unauthentication connection system according to transmission method. Also unauthentication connection raises a difficulty condition to user's needs satisfaction in order to a load weighting of system and network and a drop of transmission speed. Accordingly, this study brings forth authentication system construction in a high-speed IP infrastructure using spam sever able to construct the suitable network condition according to unifying authentication-unauthentication system for single authentication system.

키워드

Authentication, IP, SPAM, DHCP

Ⅰ. 서 론

고속 네트워킹 기술과 멀티미디어 시스템 구축 기술이 발전함에 따라 다양한 형태의 멀티미디어 응용에 대해 인터넷을 통하여 오디오, 비디오 등과 같이 연속적인 동적 미디어 정보의 실시간 전송이 요구 되고 있다. 따라서 기존의 전화모뎀을 사용한 인터넷 접속방식과는 질적으로 다른 광케이블과 동축케이블이 결합된 고품질 HFC(Hybird

*군산대학교

접수일자 : 2004. 10. 29

Fiber Coaxial)구조의 케이블TV망과 광대역 백본(Backbone)을 이용하여 수 Mbps급의 빠르고 안정적인 초고속 인터넷 환경을 구축하였고, 세계 최고의 초고속 인터넷 인프라를 가진 우리나라에 외국에서도 초고속 인터넷을 벤치마킹 하는 등 초고속 인터넷의 선두주자로 발돋움 하였다.

그림 1에서 국내의 IP기반 초고속 인터넷 서비스의 이용자 추세 분석을 살펴보면은 인터넷 상용화 이후 초기 3년의 성장기를 거쳐 성숙기로 이동하여, 2002년 1,000만을 돌파 하였다.

따라서 초고속 인터넷이 급성장함에 따라 나타나는 문제점은 Hacking, Virus 침투 및 취약한 인증에 따른 시스템 사고 등이다.

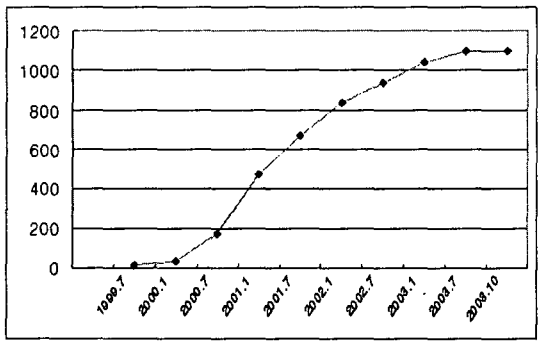

그림 1. 초고속인터넷의 이용자 추세
Fig. 1 User trend in high-speed internet

특히 시스템 침해 사고가 급속히 증가함에 따라 다양한 인증 시스템이 도입 되고 있는 실정이지만, 실제로 인터넷 시스템에서 사용자 인증 자체가 취약성을 보이고 있다. 따라서 기존 초고속 인터넷 이용자의 다양한 욕구를 충족하고 네트워크의 신뢰성과 생존성을 위한 새로운 대안의 인증 시스템 구축이 필요한 시점이다.

본 논문에서는 전송방식에 따라 이원화 되어있는 IP기반 초고속인터넷의 인증·무인증 접속방법을 SPAM 서버를 이용한 새로운 인증 시스템의 구축 모델을 제시하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 IP기반의 인증방법에 대해 기술하고, Ⅲ장에서는 신인증 시스템을 설계한다. 마지막으로 Ⅳ장에서 결론을 맺는다.

Ⅱ. IP기반의 인증 방식

인증은 정상적으로 확인된 이용자에게 다양한 접속 권한을 부여하고, 트래픽에 대한 사용 통계자료를 추출하는 것으로 이용된다. 인증의 기능은 이용자의 적법성을 확인하는 Authentication, 이용자에 대한 서비스 접속 권한 수준 및 자원 할당의 Authorization, 이용자의 사용 통계자료를 추출하는 Accounting 등으로 구분된다.

1. 접속 및 서비스 인증

접속 및 서비스 인증 방식은 그림 2에서와 같이 네트워크 접속 인증과 서버 서비스 인증으로 구분할 수 있다.

접속 인증은 네트워크 접속시 한번의 인증으로 이용자 Profile에 따라 인증 제공(AAA)기능에 의한 Network 접속에 대한 권한이 부여되며, IP- xDSL, CATV등의 초고속인터넷서비스에 이용된다.

서버 서비스 인증은 네트워크와 실제적으로 무관하여 어디서든지 접속 가능하고, 응용 서비스 및 개별 서버별로 인증이 가능한 방식으로Client- Server 기반(VOD, Web Portal 등) 서비스에 이용된다.

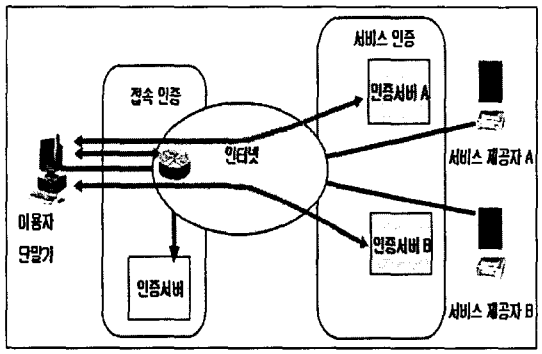

그림 2. 접속 및 서비스 인증 비교
Fig. 2 Comparison in connection and service authentication

2. 인증 방식

가. 무인증 방식

네트워크 상에서 접속 권한을 요구하지 않아 단말기가 접속되어 있으면 언제든지 네트워크 접속이 가능 하지만 이용자의 단말기에 별도의 접속 소프트웨어가 필요해 접속시 네트워크 장애를 유발하고, 부가 서비스 이용을 위해서는 서비스제공자별 인증이 요구된다.

나. 일반 인증 방식

네트워크 기반 서비스 제공으로 무인증 이용자들과 차별화가 가능하며, 위 그림 2에서와 같이 서버 서비스 인증과 통합하여 부가서비스를 가능하게 한다. 또한 이용자 단말에 인증을 위한 접속 프

로그램이 요구되며, 이로 인한 비용 및 유지 보수가 필요하다.

III. 신인증 Algorism

신인증 시스템의 인증 Algorism은 그림 3과 같이 Explicit 인증과 Implicit 인증 방법이 있다.

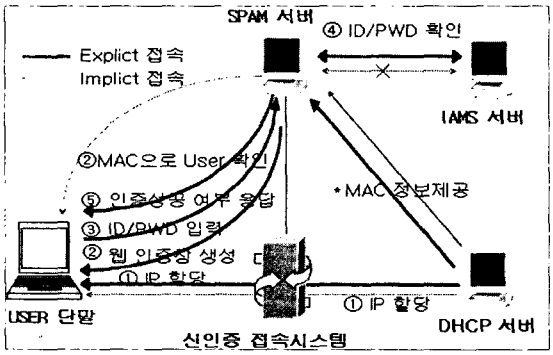

그림 3. 신인증 Algorism
Fig. 3 New authentication Algorism

첫째, Explicit 인증은 일반적 의미의 인증으로 이용자의 ID/Pwd를 확인하여 접속권한을 부여하며, 이용자의 요구에 따라 매 Login시 접속 권한을 부여하는 인증방법이다.

둘째, Implicit 인증은 무인증으로 인식되고 있는 인증 방법으로 시설과 단말기를 확인함으로써 시스템이 내부적으로 인증하는 방법이며, 접속시 User의 MAC Address를 통해 인증함으로써 MAC Spoofing시 시스템의 부하를 가중시킬 수 있고, 부가 자원 사용을 허용할 수 있다.

신인증 Algorism은 최초 접속시 Explicit 접속 방식으로 인증되며, 두 번째 접속부터는 Implicit 접속 방식으로 인증하는 인증 시스템이다.

IV. SPAM 서버를 이용한 인증 시스템 구축

1. 시스템 Architecture

그림 4에서 신인증 시스템은 주 Nod에 SPM 서버, DHCP 서버, Web 서버 및 IAMS 서버로 구성된 Sever Farm이 구성되고, 한 곳의 Sever Farm은 지역 노드(SE800) 5~6곳과 연동되며, 신인증 라우터로 SER(Service Edge Router)과 집선장치(SE800 Router)가 인증 시스템으로 구성된다.

제어 서버인 SPM(Service Police Manager) 서버는 이용자 인증을 Web 또는 One-click으로 수용하며, IAMS(Internet Access Management System)에 대한 Radius(Remote Authentication Dial - In User Sevice) Proxy 기능과 IAMS로부터 획득한 정보를 SE800에 SNMP Set을 통해 Re-authentication을 한다. 또한 접속된 사용자의 세션을 Filter로 연결후 인증 및 Accounting 정보를 전송한다.

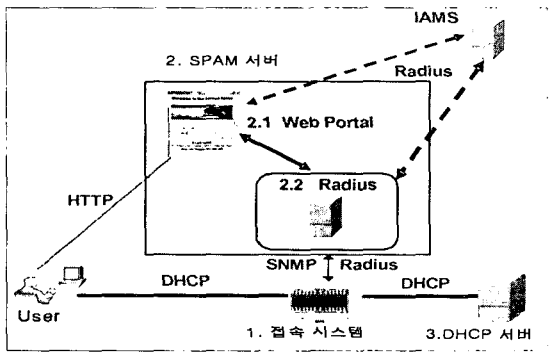

그림 4. 신인증 시스템 Architecture
Fig. 4 Architecture of new authentication system

유동 IP를 할당하는 DHCP(Dynamic Host Configuration Protocol) 서버는 각 호스트의 중요한 Network Parameter들을 DHCP 서버의 setting을 사용하여 원격으로 설정하며, 접속시스템(SE 800)과 제어 서버와의 연동과 User Session 생성, 유지 및 제거를 DHCP Packet type에 의해 수행한다.

2. 신인증 시스템 구축

본 논문에서 제시된 신인증 시스템은 SPAM 서버로 구성된 RADIUS, DHCP, WEB 서버 및 IAMS 서버를 이용한 IP 기반의 신인증 시스템 구축 방안을 제시하였다.

첫째, 이용자 인증은 SPAM 서버에서 원격지 이용자의 접속 요구시 이용자 ID, 패스워드, IP 주소 등의 정보를 통해 이용자 식별과 인증을 수행하며, 인증된 이용자 정보를 바탕으로 이용자의 인터넷 서비스 레벨을 결정한다.

둘째, IP 할당은 DHCP 서버에서 이용자에게 동적으로 IP 주소를 할당하고, SPAM 서버로부터 제공 받은 사용자 정보와 할당된 IP 주소를 필터링 서버인 접속시스템에 전송한다.

셋째, 필터링 서버는 DHCP 서버로부터 제공받은 IP 주소와 이용자 정보를 바탕으로 이용자의 URL 요청시 이용자 이용 레벨에 따라 적절한 필터링을 수행한다.

그림 5는 SPAM 서버를 이용한 신인증 시스템의 접속 모형을 나타내고 있다.

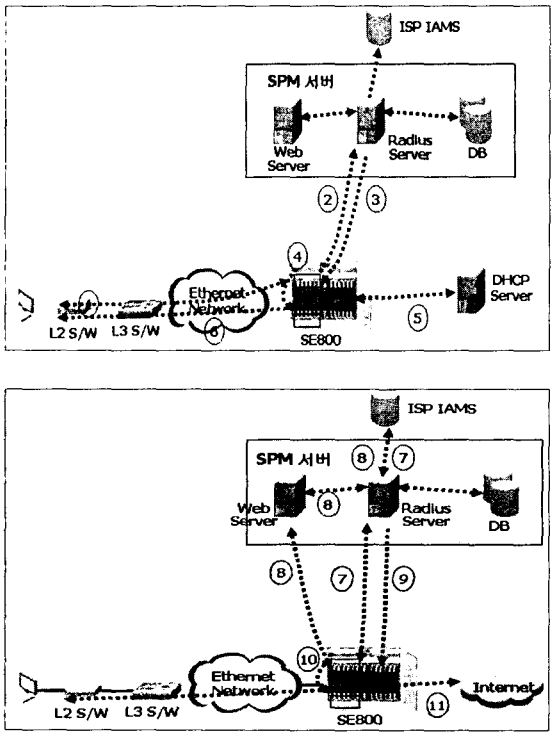

그림 5. 신인증 접속 모형
Fig. 5 Connection model of new authentication

그림 5에서 이용자가 인증을 위한 프로세서 는 열한 개의 단계로 인증 절차를 제시하였다.

① 이용자 PC Booting
② SE800의 이용자 인증 요청
③ 제어서버의 이용자 인증
④ Policy Binding
⑤ IP 요청
⑥ 이용자에 IP 할당
⑦ Radius Access/Accounting
⑧ 이용자 Web 인증
⑨ 이용자 재인증 요청
⑩ 이용자의 해당 서비스 프로파일 적용
⑪ 이용자는 인터넷 및 해당 서비스 이용

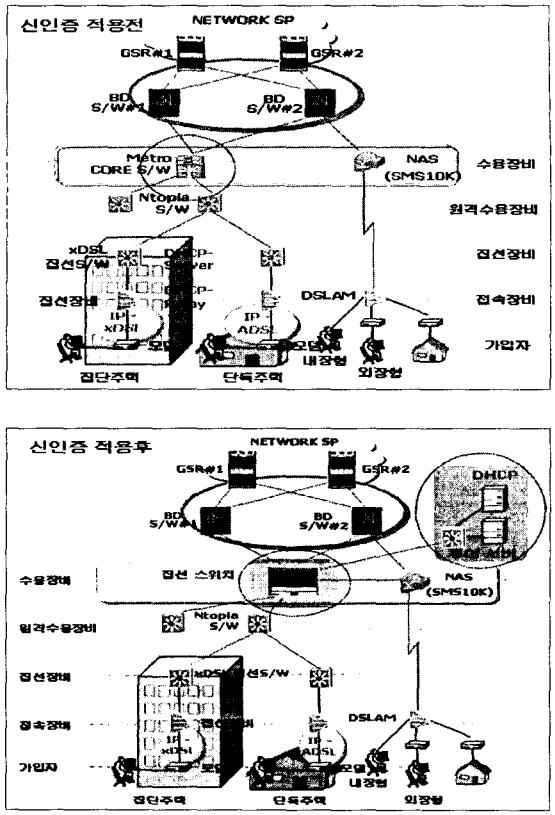

그림 6. 신인증 시스템 구축 모델
Fig. 6 Construction model of authentication system

그림5에서 제세된 신인증 접속 모형에 따라 그림 6에서는 신인증 적용전과 신인증 구축후의 인증시스템 구성도를 보이고 있다.

따라서 본 논문에서 제시된 SPAM 서버를 이용한 신인증 시스템은 IP기반 초고속인터넷 이용자에게 신뢰성 있는 인증 Solution을 구현하고, 접속품질 개선을 통해 이용자별 고품질의 서비스를 제공 할 수 있다. 또한 향후 시스템 인증에 취약한 무선인터넷서비스는 물론, 유무선 통합의 체계적인 인증시스템에 적용 될 수 있다.

IV. 결 론

초고속인터넷의 급성장과 함께 네트워크 및 시스템 보안 사고가 급증함에 따라 다양한 인증 시스템이 도입 되고 있지만 사용자 기반의 보안 및 인증 체계가 취약성을 보이고 있다.

따라서 초고속인터넷 이용자의 다양한 욕구를

충족하고 네트워크의 신뢰성과 생존성을 위한 새로운 신인증 시스템 구축이 필요한 시점이다.

본 논문에서는 전송방식에 따라 이원화 되어있는 IP기반 초고속인터넷의 인증·무인증 접속체계를 보완하여 SPAM 서버를 이용한 새로운 인증 시스템을 설계하고, 이를 기반으로 인증에 필요한 시스템의 접근 절차를 제시하였다.

또한 SPAM 서버를 이용한 신인증 시스템은 IP 기반 초고속인터넷 이용자에게 체계적인 인증 Solution을 구현하고, 새로운 인증 시스템 구축에 적합한 최적의 모델을 제시하였다.

향후 신인증 시스템이 무선 기반의 인증은 물론 유무선 통합의 인증시스템에 적용 될 수 있도록 지속적인 연구가 필요하다.

참고문헌

[1] 김동규, 이상하, 유승화, 손태식, 단일 인증시스템의 인증 기법과 인증 모델 분석, 한국정보보호학회, pp.87-96, 2001.

[2] Douglas E. Comer, Internetworking With TCP/IP Volume 1 : Principles Protocols, and Architecture, Prentice Hall, 2000.

[3] Packet Storm Security Archives, "Distributed Attack Tools", (http://packetstorm.securify.com/Distributed)

[4] 한국전산원, 전산망 보안관리를 위한 지침서, 1995.

[5] http://isis.nic.or.kr/index.html

저자소개

고남영(Name-young Ko)

1973년 광운대학교 공학사
1980년 건국대학교 공학석사
1995년 국민대학교 통신행정학 박사
1996년 Pacific Western Univ. -Communication(Ph.D Com)
1992년 7월~현재 군산대학교 전자정보공학부 교수
※관심분야 : 무선통신, 통신정책, 남북통신

이재완 (Jae-wan Lee)

1989년:전북대학교 공학사
1996년:군산대학교 공학석사
2004년:군산대학교 공학박사
※관심분야 : 초고속인터넷 응용, BCN, 남북통신