네트워크 서비스 기반의 단일 웹 인증 설계

이재완* · 반경식* · 김형진**

*군산대학교·**익산대학

A Design for Single Web Authentication at Network Service Foundation

Jae-wan Lee* · Kyung-sig Ban* · Hyoung-jin Kim**

*Kunsan National University

**Iksan National College

E-mail : oneuni@paran.com, hjkim@iksan.ac.kr

요 약

최근 초고속통신망의 발달로 네트워크 보안 및 시스템 침해 사고에 대응하기 위한 다양한 인증 및 접근 제어 시스템이 도입되고 있다. 하지만 초고속인터넷 환경에서 보안 자체가 취약성을 보이고 있다. 따라서 인터넷 이용자의 다양한 욕구를 충족하고, 보다 안전하고 신뢰성있는 새로운 인증 시스템 도입이 필요한 시점이다.

본 논문에서는 다원화된 네트워크 환경에서 기술방식에 따라 차별적으로 적용하는 기존의 다양한 인증 체계를 하나로 통합하여 네트워크 보안을 강화하고, 보다 안정적인 서비스 제공 기반을 마련하기 위하여 단일 웹 인증 설계를 통한 새로운 인증 체계 방안을 제시하고자 한다.

ABSTRACT

Recently, Network companies have introduced security solutions to protect the network from intrusions, attacks and viruses but the network has still weakness and vulnerability.

It is time to bring more stable and reliable authentication system that would meet the Internet user's need. In this study, Current broadband networks don't have hierarchic and stable authentication solutions. And so, an integrated and hierarchic system is needed to provide a various kinds of application services.

키워드

인증, 라우팅, VRRP

Ⅰ. 서 론

최근 통신 인프라는 여러 가지 방법으로 사용자 데이터베이스를 관리하고, 보안 강화를 시도하고 있지만 자원관리, 접근 권한 등의 관리가 서로 다원화되어 있는 환경에서 다양한 사용자 관리의 어려움으로 인해 접근 인증과 같은 네트워크 보안에 취약점이 발생되고 있다.

기존의 접근방법은 네트워크 접근 허용 여부를 판단하는 단순 접근 인증만을 기반으로 네트워크 시스템에 일관된 자원 및 네트워크의 보안 체계 구축하여 서비스를 제공하였다. 따라서 이러한 네트워크 환경의 신뢰성을 높여 중요한 자원들의 안전성 보장 및 관리가 필요하다는 인식을 통해 보안성 높은 접근 권한을 가진 사용자에 의해서만 접근이 가능토록 해야 한다. 즉 다양한 환경에서 네트워크 관리를 위해 사용자 인증 기반의 세분화된 접근 관리의 필요성이 부각되고 있다.

따라서 로밍이나 유·무선 통합 및 단말 이동성 등을 기반으로 하는 고부가 기능들을 도입하여 사용자의 신원을 확인하고 이용 가능한 자원을 할당하는 일련의 절차를 통해 접속 가능한 단말

의 수, 접속 장소, 데이터 전송속도, 이용 가능한 서비스를 통제해야 한다. 디시말해 안정성과 신뢰성을 확보할 수 있는 새로운 접근 제어 및 인증 시스템 구축이 필요 하다.

본 논문에서는 초고속 인터넷 환경에서 기술방식에 따라 차별적으로 적용하는 기존 인증·무인증 기반을 하나로 통합한 단일 웹 인증 기반이라 정의하고 이를 기반으로 통합하여 접근 보안을 강화하고 보다 안정성이 고려된 새로운 인증 체계 개선 방안을 제시하고자 한다.

따라서 이를 위해 라우터 간 이원화된 운용 체계를 VRRP(Virtual Router Redundancy Protocol) 프로토콜을 이용하여 단일 웹 인증 체계를 설계하고자 한다.

이를 위해 본 논문에서는 2장에서는 기존의 인증 체계를 설명하고 3장에서는 제안 기법에 대해 설계한다. 마지막 4장에서 결론을 맺는다.

Ⅱ. 본 론

그림 1은 OSI 각 계층마다 그 계층에서 가장 효율적으로 제공 가능한 기본적인 보안 서비스 6가지와 그 서비스들을 수행하는데 필요한 8가지 주요 메커니즘을 보이고 있다.

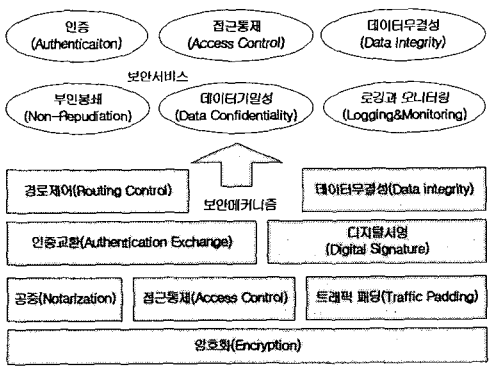

그림 1. 네트워크 인증

따라서 그림 1에서 보이는 거와 같이 네트워크 인증은 보다 안전한 통신을 위하여 인증, 접근통제, 데이터 기밀성, 데이터 무결성, 로깅과 모니터링의 6가지 기본적인 서비스를 통하여 각각의 보안서비스는 부당한 위협으로부터 네트워크를 보호하기 위하여 지원되는 여러 가지 보안메커니즘들로 구성된다.

예를 들면 식별과 인증 서비스는 접근사용자를 식별하고 접근권한의 유무를 검사하여 네트워크의 부당한 사용을 막을 수 있도록 한다.

2.1 네트워크 접근 제어

접근 제어는 사용자의 식별 정보, 인증, 권한 제어, 계리 및 IP 할당 등의 서비스 제공을 위한 것을 말한다. 따라서 접근 제어는 네트워크 보안 통제를 통해 응용 서비스 계층에 대한 네트워크 계층의 수직 결합을 유도하는 것으로 네트워크 가치를 높인다. 최근 네트워크 접근망은 전통적인 네트워크 접근·전달 서비스로부터 인터넷 응용의 접근·전달 서비스로의 패러다임 분계점이 분화되고 있다. 첫째, 접근 제어는 응용 서비스 계층과 네트워크 계층의 수직 결합을 유도하는 효과적인 수단으로 응용 서비스로의 확장이 용이하다. 둘째, 통신망 설비 및 서비스 장치를 사업자 영역에서 제어하고 통제하는 수단으로 각 서비스 영역의 동기화를 유지하면서도 서비스 제공자에 대한 의존성을 높일 수 있다. 셋째, 서비스 이용자와 서비스 제공자가 충분한 서비스 효용성을 인지하는 보장형 서비스 사업에 대한 정교한 통신망 제어 능력을 제공하는 수단으로 활용된다.

2.2 네트워크 인증

유·무선 환경에서 이용되고 있는 네트워크 접근 인증 방식을 비교하면 크게 인증 방식과 무인증 방식으로 구분할 수 있다.

인증 접근은 네트워크 기반의 인증 서비스를 제공하므로 기존 서비스들과 차별화가 가능하며, 서비스 인증과 통합하여 차별화된 서비스 제공이 가능하다. 그러나 사용자가 인증을 받기 위해 네트워크 인증 응용 프로그램이 요구되고, 네트워크 인증 응용 프로그램으로 인한 비용 및 유지 보수가 필요한 단점이 있다.

무인증 접근은 네트워크 접근 권한이 필요하지 않아 사용자가 네트워크를 통해 언제든지 웹 서비스 이용이 가능하다. 그러나 사용자를 위한 서비스의 차별화가 어려운 단점을 가지고 있다.

따라서 본 논문에서는 기존 인증 방식 및 무인증 방식에서 나타난 문제점을 해결하기 위해 네트워크 접근 장치를 이용해서 웹 기반의 인증 서버를 구현하여 사용자 요구사항을 능동적으로 수용할 수 있는 단일 웹 인증 설계를 구현하고자 한다.

Ⅲ. 단일 웹 인증 설계

3.1 웹 인증 방식

사용자의 PDA, 무선인터넷, PC등 서비스에 접근이 가능한 유·무선 환경의 어떤 기기와도 상관없이 접근하는 사용자를 인증하는 통합 인증 기능과 사용자의 권한을 통합하여 다양한 서비스의 선택이 가능한 인증 방식을 말한다.

따라서 사용자가 쉽게 선택하고 사용할 수 있는 다양한 서비스들을 제공할 수 있어야 한다. 또한 사용자가 필요에 따라 단 한 번의 네트워크 인증을 통해 필요한 정보를 얻을 수 있어야 한다.

접근 형식에 따라 인증 알고리즘은 explicit, implicit 인증 및 무선인증으로 구분한다. explicit 인증은 일반적 의미의 인증으로 웹 서버를 이용

하여 이용자의 ID·password를 확인하여 접속권한을 부여하고, 이용자의 요구에 따라 매 login시 접속권한을 부여하는 수동 인증 방법이다.

implicit 인증은 무인증으로서 인식되고 있는 자동인증 방법으로 시설과 단말기를 확인함으로써 시스템이 내부적으로 인증하는 방법이다. 그리고 접속 시 이용자의 MAC 주소를 통해 인증함으로써 MAC 스프핑시 시스템의 부하를 가중시킬 수 있고, 부가서비스 자원의 사용을 허용할 수 있다. 무선인증은 웹 서버를 사용하지 않고 MAC 주소와 EAP-MD5 인증 방식을 적용한다.

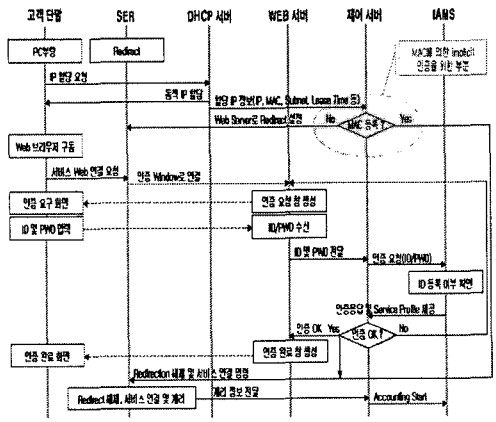

그림 2. 단일 웹 인증 절차

따라서 단일 웹 인증 방식은 사용자의 단말기의 MAC 주소를 등록 후 IP 할당 시 인지된 정보를 기반으로 implicit 인증 방법과 웹을 통하여 ID·PWD로 접속하는 explicit 인증 방법을 통합 적용한다. 그림 2는 단일 웹 인증 절차이다.

3.2 VRRP 프로토콜

동적 라우팅은 라우팅 프로토콜을 사용해 최단의 거리를 자동으로 설정해 주므로 네트워크가 커진 경우에 상당히 편리한 작용을 하지만 계속적인 라우팅 정보를 갱신하기 때문에 부하가 커지기도 한다. 정적 라우팅은 프로토콜을 설정해주는 것이 아니라 어떤 패킷이 들어올 경우에 패킷을 지정된 장소로 보내는 것으로, 정적 라우팅 환경에서는 한 개의 라우터가 잘못되었을 경우에 그것을 통해 나가는 모든 호스트들은 통신장애가 발생한다. 이러한 통신장애가 발생했을 경우에 백업기능으로 구현된 것이 VRRP 프로토콜이다.

VRRP는 LAN상에서 정적으로 설정된 기본적으로 하나의 라우터를 사용하고 있을 때, 하나 이상의 또 다른 백업 라우터를 가질 수 있는 방법을 제공하는 인터넷 프로토콜의 하나이다.

네트워크 구성에서 가장 일반적인 배치는 근거리통신망 상의 호스트 그룹으로부터 전달되는 패킷들을 하나의 라우터가 관리하고 서비스하도록 설정하는 것이다. 그러나 만약 이 라우터가 고장이 나면, 다른 라우터를 백업으로 사용할 수 있는 방법이 없다. VRRP를 사용하면 하나의 가상 IP 주소가 기본으로 설정된다. 가상의 IP 주소는 하나는 마스터 라우터로, 다른 것은 백업들로 지정되는 라우터들 간에 공유된다. 마스터 모드에 문제가 발생하는 경우에 가상 IP 주소는 백업 라우터의 IP 주소로 바로 천이된다.

또한 VRRP는 네트워크 부하조절에도 사용될 수 있으며, 대상 프로토콜은 IPv4와 IPv6 모두에 적용된다.

VRRP 기본 구성도는 그림 3과 같다.

그림 3에서 보면 router1 과 router2는 VRRP 그룹으로 구성돼 클라이언트들에게 라우팅 서비스를 제공한다. VRRP 에서는 마스터·백업 개념이 사용되며 동일한 VRRP 그룹에 속하는 라우터 그룹은 priority 등의 우선권으로 각각 마스터 또는 백업 동작을 결정하게 된다. 또한 VRRP는 이더넷 인터페이스에서 사용할 수 있는 기능이며, 멀티캐스트 기반의 프로토콜이다.

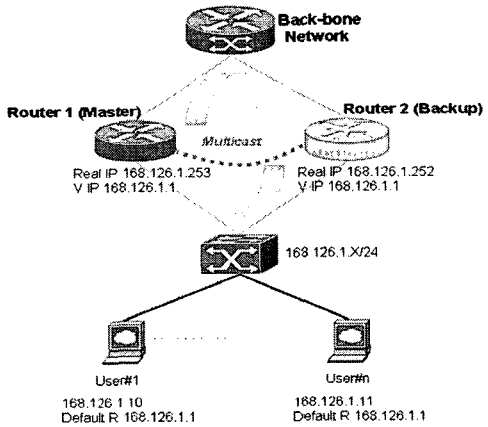

그림 3. VRRP 기본 구성도

따라서 본 논문에서 VRRP 구현을 위한 단일 웹 인증 기반의 인증 시스템 설계는 그림 4와 같다. 또한 이 테스트베드 스몰 망의 SER - RS38K 라우터간 라우팅 프로토콜은 BGP/IS-IS를 적용하였다

본 논문에서 제안한 절차는 다음과 같다.

① 망 모형에서 SER - RS38K 라우터간 VRRP 그룹을 구성한다.

② 라우팅 프로터콜(BGP,IS-IS)을 적용하고, SER - RS38K 라우터간 인터페이스 config 작업을 수행한다.

③ VRRP 그룹 구성 후 트래픽 라우팅 흐름을 측정·비교한다.

④ 웹 stress를 이용한 트래픽 발생, 점유 및 흐름을 비교·분석한다.

⑤ 시뮬레이션 수행 후 결과를 확인·분석한다.

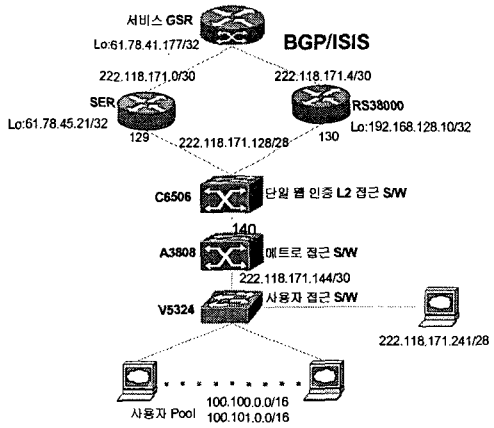

그림 4. VRRP 스몰 망 설계

본 논문에서는 단일 웹 인증 기반의 SER - RS38K 라우터간 물리적으로 이원화된 체계를 VRRP 기반에서 최적의 단일 웹 인증 체계를 설계하고자 하였다.

Ⅳ. 결 론

본 논문에서는 단일 웹 인증 기반에 적합한 Test Bed 스몰 망을 구성하여 접근·인증 절차를 제시하고, VRRP 프로토콜을 활용하여 Test Bed 시험 망을 설계하였다.

따라서 본 논문에서 제시한 단일 웹 인증 방식은 네트워크 로드 밸런싱은 물론 자동 장애복구가 가능하고 보안성, 안전성 및 신뢰성을 확보할 수 있는 인증 체계이다.

향후 연구과제로 VRRP를 적용하여 트래픽 흐름을 시뮬레이션을 통해서 측정·분석하여 최적의 인증 체계 방안을 지속 연구하고자 한다.

참 고 문 헌

[1] http://www.mic.go.kr.

[2] Korea Information Security Agency, "An Introduction Computer Security:The NIST Handbook(NIST Special Publication 800-12)", 1999.1.

[3] Meyer C.H., and S. M. Matyas, "Cryptography: A New Dimension in Computer Data Security", John Wiley & Sons. 1982.

[4] Murray W.H., "Security Considerations for Personal Computers". Tutorial:Computer and Network Security, Oakland, 1986.

[5] National Institute of Standards and Technology. "Guideline for the Advanced Authentication Technology Alternatives", October 1994.

[6] National Institute of Standards and Technology, "Data Encryption Standard", Federal Information Processing Standard Publication 46-2. December 1993.

[7] Denning P., and D. Denning, "The Clipper and Capstone Encryption Systems", American Scientist, 81(4), 1993.

[8] Rivest R., A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, 1978.

[9] Schneier B., "A Taxonomy of Encryption Algorithms", Computer Security Journal, Vol. 9, No 1, 1993.