韓國 컴퓨터情報學會 論文誌
第8卷 第1號, 2003. 3.

2003-8-1-1-9

인증 메커니즘을 이용한 CA-VPN 설계에 관한 연구

김 도 문* 전 정 훈** 전 문 석**

A Study on CA-VPN Design using Authentication Mechanism

Do-moon Kim* Jeong-hoon Jeon** Mun-seok Jun***

요 약

인터넷의 보편화와 보안 장비의 개발이 활발히 진행되고 있다. 그러나 보안 방식에 따른 여러 형태의 장비들에 따른 프로토콜의 다양화로 인해 호환성과 장비의 가용성에 따르는 문제점들이 나타나고 있다. 일부 업체의 표준화 작업을 위한 독과점식 보안장비의 판매로 효율성을 고려하지 않은 문제점들을 야기시킬 수 있다. VPN 게이트웨이 장비의 사용에 있어 동일 장비임에도 불구하고, 상호 장비들의 확인과정 없이 통신장비 판매에만 치중하고 있는 것이 현실이다. 이러한 문제는 업체들마다의 다량 판매에 급급한 나머지, 특정 장소의 네트워크 환경에 맞는 장비 설정과 장소 내에서 상호 인증과정을 통해 장비에 대한 확인과정을 고려하지 않은 채 구현되어, 악의를 가진 공격자로부터 동일 장비를 이용한 공격에 대해 무방비 상태로 있게된다. 그러므로 이에 대한 대책이 필요한 것이 사실이다. PKI 기반의 인증시스템을 통해 VPN 게이트웨이 장비간의 상호 인증과정을 수행함으로써, 제 3의 공격자가 공격을 시도할 지라도, 허가된 사용자가 아님으로 물리적 공격으로부터 CA-VPN 게이트웨이를 이용으로 보안성과 인증성이 기존의 VPN 연결보다 안전하게 사용자를 보호할 수 있다.

Abstract

Now the development of using a internet and security equipment is processed actively. But It is presented problems about compatability and availability between variable equipment as several protocol. It is able to occur the problem which is not considered efficiency as monopoly security equipment for the standardization of some vendor. As a using of VPN gateway equipment, the same equipments have been actually used only for sale a communication equipment which are not confirmed(authenticate) between of

* 동우대학 컴퓨터그래픽과 교수
** 숭실대학교 대학원 박사과정
*** 숭실대학교 정보과학대학 교수

접수일자 : 2003. 1.25
심사완료 : 2003. 3.15

mutual equipments. These problem is remain which are not considered suitable network environment and position by mutual authentication processing. Because it is considered for only sale a equipment of several vendor. And you will be remain where is unable to protect from attack of using the same equipment. and you will need a actually protected method. By authentication system of base on PKI, although there is an intended attack from the third intruder, users can be protected with safe from the physical attacks since he is not a permitted user by employing CA-VPN gateway that is more viable than the previous VPN connection in its security and certification.

I. 서론

인터넷의 보편화와 신뢰성 있는 통신요구 등 보안에 대한 중요성이 날로 증가하고 있다. 이러한 문제를 해결하기 위한 대처방안으로 공중 데이터 통신망을 이용해 마치 개인이 구축한 통신망과 같이 이를 직접 운용 및 관리할 수 있는 기술인 VPN(Virtual private Network)이 많이 사용되어지고 있다. 그러나 이 방법도 상존하는 취약점으로 인해 날로 심각해지는 해킹으로부터 안전하지 못하며, 취약점을 개선한 보다 안전하고 향상된 기능의 보안방법이 절실히 필요한 실정이다. 이에 본 논문에서는 기존 VPN장비들의 취약점을 개선한 PKI 기반하의 보안성 향상을 위한 CA-VPN(Security-VPN) 게이트웨이 시스템 설계 구조를 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 VPN의 개요에서 기존의 VPN이 갖는 보안상의 취약한 문제점을 기술하였으며, 3장에서는 본 논문에서 제안하는 제안한 CA-VPN 시스템 설계에 따른 PKI 인증기관 (CA: Certification Authorit 게이트웨이(GA: GateWay)의 동작 절차 및 보안성과 능 향상을 위해서 CA-VPN에 PKI의 적용에 따른 성능분석을 기술하였다. 마지막으로 4장에서는 인증 메커니즘을 이용한 CA-VPN에 대한 결론와 차후 연구방향 등을 기술한다.

II. 가상 사설망(VPN, Virtual Private Network)

2.1 VPN의 개요

VPN은 인터넷과 같은 공중망을 이용하여 가상의 사설망을 구성하는 기술로 기존의 전용선을 이용한 사설망에 비해 저렴한 비용으로 외부와의 네트워크 정보 교환이 안전하게 구성할 수 있다는 면에서 각광을 받기 시작하였다. VPN은 상호 네트워킹 시나리오에 따라 통상 인트라넷 기반의 VPN, 엑스트라넷 기반의 VPN, 원격 접속 기반의 VPN이 있다. 구현 기술로는 터널링, 암호화 및 인증, 액세스 제어로 구분할 수 있다. 그리고 불특정 다수의 인터넷 사용자에 대한 접근통제이고, VPN의 주요내용은 암호기술을 이용한 사설 망을 인터넷으로부터 차단됨과 동시에 정보의 보안에 있다. 따라서 IPsec의 무결성, 인증을 보장하는 HA, 무결성을 보장하는 ESP 헤더 및 키 보안 연계의 안전이 가상 사설망의 필요성이다.

2.2 VPN의 문제점

VPN이란 기업이 공중망(인터넷)을 이용하여 경제적이고 안정적으로 통신망을 운영할 수 있도록 하는 솔루션을 의미한다. VPN의 핵심 기술로서 사용되어지는 터널링 기술은 인터넷 상에서 외부의 영향을 받지 않는 가상적인 터널을 형성해 정보를 주고받도록 하는 기술로서, 시작지점에서 목표지점까지 상호 약속된 프로토콜로 세션을 구성하게 된다.

현재 많은 VPN 제품에서 터널링 기법으로 계층 2와 3에서 사용되고 있는 몇몇 프로토콜들이 있다. 현재로서는 IPSec을 표준으로 하고 있지만, 아직까지는 특정 업체에서 개발한 프로토콜들을 사용하고 있는 추세이기 때문에 각각의 프로토콜의 문제점들을 고려해보기로 한다.

① IPSec과 PPTP, L2TP의 완벽한 호환성 문제 : VPN에서 사용하는 터널링 프로토콜은 지역적인 것이 아닌 세계적인 표준형태로서 이루어져야한다. 만약 IPSec의 유럽방식과 북미방식의 차이가 발생한다면, VPN 사용자에 대한 혼선을 야기 시킬 수 있고, 또한 PPTP와 L2TP, IPSec 사이의 이 기종 프로토콜과의 통신문제를 야기 시킬 수 있다.

② 터널링 프로토콜의 암호화 규칙의 전세계적 표준안 제시 문제 : 터널링 프로토콜은 서로 다른 프로토콜간의 호환은 전혀 되고 있지 않고 있다. 그러므로, VPN 장비간의 암호화 표준에 따른 운영이 시급하다.

③ 세션 당 패킷 수 증가로 인한 트래픽 발생문제 : 세션을 성립시킬 때마다 발생하는 패킷 전송량 문제는 세션 성립마다 발생할 수 있는 트래픽의 문제 또한 심각한 네트워크 장애를 발생할 수 있으므로 빠른 대처방안이 필요하다.

④ VPN의 무결성(Integrity) 유지 문제 : 데이터의 메시지 다이제스트를 거쳐 각각 일정크기의 데이터에 대한 해쉬 값 생성으로 데이터의 변경 유무를 확인함으로써 데이터에 대한 전송 중 발생할 수 있는 손실 및 데이터 변경 유무를 확인할 수 있다. 알고리즘은 역추적이 가능하게 된 상태임에도 불구하고, 보안제품에서 무결성 확인을 위해 사용 중이어서 이에 대한 확실성을 떨어뜨리고 있는 상황이다.

⑤ VPN의 사용자 인증 문제 : VPN 사용자 상호간의 인증은 키 교환을 통한 세션 연결을 수행하고 있다.

예를 들면 ISAKMP(Internet Security Association and Key Management Protocol)와 같은 프로토콜 이용으로 자동 키 교환을 수행하고 있지만, 자동 키 분배 및 생성과정에서 교환될 키를 스니핑 함으로써 해킹 가능성을 내포하고 있다.

또한 메일이나 그 밖의 통신수단을 통한 수동모드 키 교환은 키 값의 노출 가능성으로 상대편에 대한 오인 가능성이 있다. 일반적으로 사용자의 편의를 위해 고정된 암호화 알고리즘 및 터널링 프로토콜, 교환 키 값을 이용한 침입가능성은 VPN 장비 사용자의 사용자 인증이 필요하다.

⑥ VPN의 키 관리와 쿠키 교환방식의 문제점 : 기존의 VPN 키 관리를 통해 교환된 데이터는 해킹기술 중 스니핑(도청: Sniffing)을 통한 공격방법으로 개인의 신상정보 및 사용자 ID와 암호를 알아낼 수 있었다. 인증기관으로부터 신뢰된 키를 사용하여 보다 안전한 통신을 고려하여야만 한다.

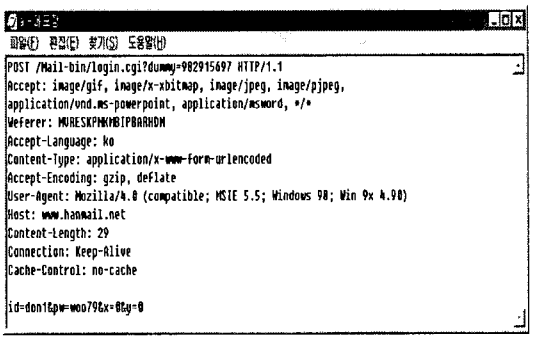

그림 1. 해킹 된 개인신상정보1

또한, 쿠키(Cookie) 교환방식은 암호화되지 않은 쿠키 정보, 키 교환 등에 따른 취약점을 보완하고자 VPN에 세션연결에 필요한 키 관리 및 전송(Transport) 모드의 개선은 앞으로의 취약점으로 남겨질 수 있을 뿐만 아니라, 치명적인 요소로 남을 수 있다. 그 예로서 다음 〔그림 1〕은 세션 성립을 위해 상호 교환되어야할 신상정보 및 시스템 정보를 담고 있는 쿠키파일의 내용을 보여주고 있다.

쿠키파일을 통해 신상정보 및 시스템 정보의 내용을 상호교환 중에 정보를 도청 당하는 화면이다. 이는 인증정보 교환의 취약점을 이용한 암호 및 신상정보에 대한 해킹기법에서 실제 사용하고 있는 스니핑 방법으로 〔그림 2〕는 통신자간의 정보를 스니핑을 통해서 신상정보를 얻어낸 결과이다.

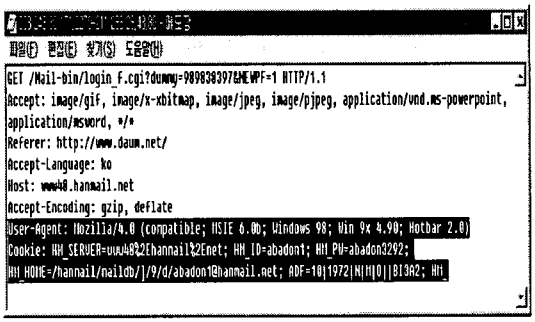

그림 2. 해킹 된 신상정보2

Ⅲ. 인증 메커니즘을 이용한 CA-VPN 시스템 설계

3.1 CA-VPN에서 게이트웨이 시스템 설계

본 논문에서 제안하는 CA-VPN에서 게이트웨이란 PKI를 기반으로 한 VPN 인증기관(CA) 및 게이트웨이(GW)를 말한다.

CA-VPN에서 게이트웨이는 VPN의 급성장으로 인한 보편화 추세에 발맞추어, 보다 안전한 전자상거래와 신뢰성 있는 데이터의 교환을 위해, 취약점으로 알려진 호환성 문제 및 키 관리, 암호화 알고리즘의 통합 등의 공격

가능성을 보완하기 위한 VPN 전용 인증 시스템 및 게이트웨이를 제안하는 것이다.

CA-VPN에서 게이트웨이 운용관리시스템은 추적 및 관리와 방어를 함께 응용할 뿐만 아니라, 모든 VPN 사용자의 실시간 관리를 목적으로 하고 있다.

CA-VPN에서 게이트웨이 운용관리시스템의 제안은 보안분야의 향후 VPN 확장 가능성을 고려한 제안으로 날로 심해지는 보안침해사고 등을 대비한 것이라 할 수 있겠다.

CA-VPN에서 게이트웨이의 기능으로는 VPN기능과 PKI기능의 장점들을 결합한 상호보완 된 보안기능들로 보다 안전한 데이터 송수신 및 관리를 할 수 있는 보안시스템을 구성한다.

또한, CA-VPN에서 게이트웨이의 제안은 앞으로의 VPN 사용자 급증과 오용가능성을 고려한 것이다. CA-VPN의 장점으로는 키 교환의 취약성을 이용한 해킹 가능성을 방지하고, 신뢰된 사용자의 관리를 통해 안전한 전자상거래를 구축할 수 있다는 것이다.

또한 인증기관으로부터의 인증서 관리를 통해 특정 기간별, 사용자별 제한을 통해 공격자의 접속을 차단할 수 있다. 그밖에 사용자들의 접속로그 기록들을 관리하여, 상대방의 접속 지점을 확인함으로써, 추적 가능하다. 그리고 VPN 통신을 원하는 사용자간의 암호화방법에 있어서, 암호화 알고리즘의 연결을 제한함으로써, 인증기관으로부터 인증을 받지 못한 사용자와는 통신할 수 없도록 통제도 가능하다.

3.1.1 CA-VPN에서 게이트웨이 구조와 동작 절차

CA-VPN 인증기관 게이트웨이 설계구조의 [그림 3]는 공개키를 기반으로 한 인증 시스템의 구현원리와 마찬가지로, 마스터 인증기관에서 총괄적인 CA-VPN의 관리를 수행하고, 각각의 CA-VPN은 하위 인증기관(Sub CA)과 CA-VPN 등록기관(RA)을 통해서 VPN게이트웨이의 총괄적인 관리 감독 및 게이트웨이의 역할을 수행할 수 있다.

각 VPN 게이트웨이의 등록정보는 CA-VPN 하위 인증기관과 CA-VPN의 등록기관간의 교환과 마스터 인증기관의 데이터베이스에 저장되어 마스터 인증기관에서 총괄하게 된다.

마스터 인증기관에서는 각 하위 등록기관 및 하위 인증기관으로부터 등록된 VPN 게이트웨이 정보를 총괄적으로 관리하며, 감사기록을 남김으로써 부인방지(Nono-Repudiation)역할 함께 수행하게 된다.

하위 인증기관에서는 등록기관의 등록정보를 마스터 인증기관에 전달하고, 설정내용 및 사용자의 세션 키 관리와 터널링 프로토콜 등의 정보를 전달해준다.

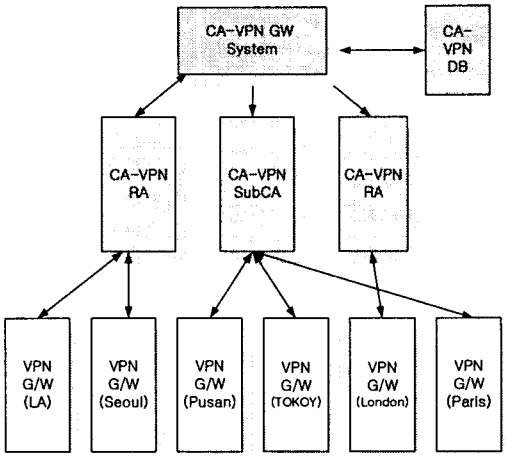

그림 3. CA-VPN의 설계구조

또한 등록기관의 관리를 수행함으로써 마스터 인증기관의 부하를 감소시키는 역할을 수행한다. 등록기관은 VPN 게이트웨이의 등록을 대행하는 기능을 수행하고, 연결에 관련한 터널링 프로토콜, 암호화 알고리즘, 세션 키 등을 실제적인 상호 연결 관리를 하여, VPN 사용자에 대한 정보를 감사기록 한다. 또한 감사기록 된 내용을 상위 등록기관 또는 하위인증기관에 전달해 줌으로써 인증서 발급을 대행하여 준다. 다음 [그림 4]는 CA-VPN의 동작 화면을 도식화 한 것이다.

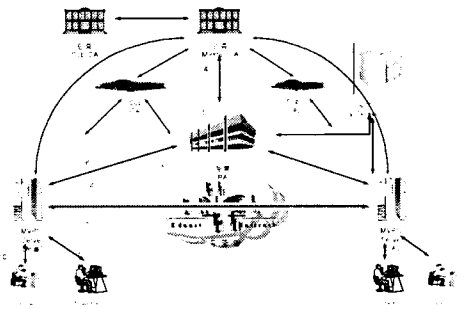

그림 4. CA-VPN의 동작 모델

동작과정(1-2)은 키의 생성과 인증기관의 인증서를 요청한다. 동작과정(3-4)은 등록기관이 클라이언트로부터의

요청을 받아 등록한 후 인증서 발행을 인증기관에 요청한다. 동작과정(5-6)은 인증기관이 등록기관의 요청에 따라 인증서를 하위 인증기관을 통해 발행한다. 동작과정(7-8)은 인증서의 저장과 인증서 폐지 목록(CRL)의 유효성체크를 수행하고, CA-VPN 인증기관 게이트웨이로부터 부여받은 세션 키를 사용해 세션연결을 수행한다. 마지막으로 동작과정(9-10)은 CA-VPN 터널링을 구축한 후 데이터의 암호화와 복호화를 통해 데이터를 송수신한다.

3.1.2 보안성 향상을 위한 PKI 적용

PKI의 인증 시스템 적용으로 VPN장비간의 인증과 확인으로 키 교환으로서 사용자에 대한 인증의 역할이나 시스템간의 교환해야할 정보에 따른 공격가능성 때문에 키 교환에 따르는 문제점과 취약성, 성능 개선 문제를 해결하기 위한 노력이 계속되고 있다.

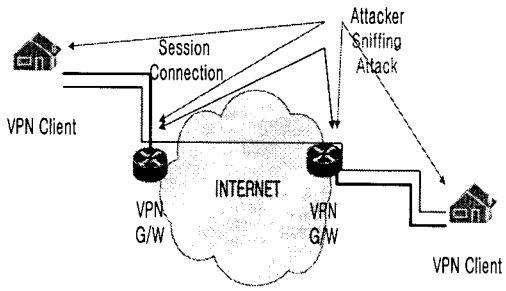

그림 5. IPSec 트랜스포트 모드 공격 형태

기존의 키 교환방법이 아닌 인증기관을 통한 신뢰성 있는 사용자 인증과 세션을 성립에 따르는 정보 유출가능성을 배제하기 위해 공개 키 기반의 인증 시스템을 통한 응용에 대해 해결책을 제안하고자 한다. 이러한 키 관리의 취약성에 따른 보안과 사용자에 대한 인증을 위하여 PKI를 응용한 인증 키의 교환 및 인증서 발급을 통해 보안성 및 안전성을 향상시킬 수 있다. 인증기관으로의 사용자 인증 정보의 등록과 동시에 부여받게 되는 공개키 값의 2가지 경우의 활용방안을 제안한다.

첫째로, 인증기관으로부터 부여받게 되는 공개키를 VPN의 세션연결 키로써 활용하는 방법이다. 키의 생성 및 저장과 재발급에 관한 모든 통제를 인증기관 게이트웨이에서 받도록 한다. 여기서 인증기관 게이트웨이란 본 논문에서 제안하는 CA-VPN의 인증기관/게이트웨이를 의미한다. 이렇게 CA-VPN 게이트웨이에서 키의 생성 및 저장과 재발급에 관한 모든 통제를 함으로써, 차후에 발생할 수 있는 해킹공격 및 변경된 자료에 대한 추적이 가능하다. 그리고, 기존의 VPN 장비에서 세션 키의 생성으로 인한 시간소요 및 교환에 있어 지연되는 시간을 등록된 사용자에 한하여서는 효과적인 연결을 할 수 있다.

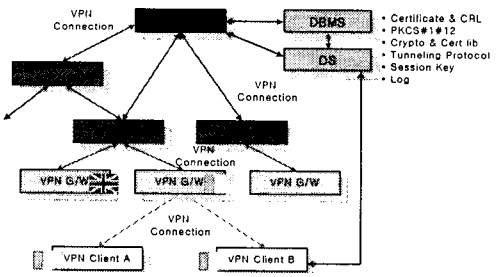

그림 6. 인증관리 설계 모델

둘째로, 인증기관으로부터 부여받게 된 공개키를 사용자 인증에서만 사용하는 방법이다. 이 방법은 PKI를 응용한 인증방법을 그대로 적용하는 것으로써, 사용자에 대한 신분확인과 데이터의 암호화에 사용한다. 여기서 부여받게 된 공개키는 VPN의 ESP를 암호화하는데 사용할 수 있다. 이러한 방법은 기존의 VPN에서 사용하는 키 생성과정을 보다 신뢰성 있는 사용자의 신분확인을 제공할 수 있게 된다.

제안한 활용방안들은 기존의 VPN에서 개선한 PKI 적용과는 달리 세션연결에 관한 키 관리뿐만 아니라, 별도의 인증기관(CA)의 기능을 첨가하여, 통합 운영 관리를 하고자 한다.

3.1.3 CA-VPN 게이트웨이 운용 관리

VPN 게이트웨이의 설정과 프록시(Proxy) 서비스의 IP별 설정을 통해 VPN 게이트웨이를 통합관리 할 수 있다. 관리내용은 VPN G/W의 IP 및 로그 기록관리 접속현황을 통해 실시간 연결상태를 감사할 수 있다.

(1) 인증 운용의 관리기능

사용자에 대한 인증서 발급 및 키 분배를 함으로써 신뢰성 있는 통신을 이룰 수 있도록 통합 관리하는 기능을 수행한다. 인증서의 발급으로 등록된 사용자가 아닌 임의의 침입자로부터 보호할 수 있는 관리기능을 수행한다.

(2) 접속자 관리기능

〔그림 6〕은 실시간 상호 통신자에 대한 연결상태를 관리하고, 연결상태 종료 후에도 사용자간의 로그기록을 통해 확인할 수 있는 기능을 수행한다. 접속자의 접속시간, 세션 키, 암호화 알고리즘, 터널링 프로토콜, 전송시간, 목적지/출발지주소 등에 대한 정보를 등록기관 또는 하위 인증기관에 전송하고, 주기적으로 마스터 인증기관 데이터베이스에 보관한다. 차후 부인방지를 위한 감사기록 로그로써 활용할 수 있다.

(3) CA/RA 인증기관의 운용관리

인증기관 및 등록기관 관리를 수행한다. 하위인증기관과 등록기관들을 통합 운용관리 함으로써 인증서 및 인증서 폐지 목록 관리, 키 등의 인증에 사용하는 데이터를 일괄적으로 관리하고, 마스터 인증기관에 전송하여 DBMS에 저장 보관하도록 한다. 데이터베이스의 구성 형태는 〔표 1〕과 같다.

〔표 1〕의 DBMS의 내용에 대한 인증과 관련된 내용을 간단하게 기술하면 다음과 같다.

① 인증서(Certificate)

- 인증서 폐지목록과 인증(CRL & Certification) : 인증서의 유효기간 및 인증서를 체크하여, 불법적인 접근을 통제하는 자료로 사용된다.
- 하위 인증기관과 등록기관(Sub CA/RA) 정보 : 하위 인증기관과 등록기관의 공인성을 증명할 수 있는 정보들을 저장한다. 또한 하위 인증기관과 등록기관의 네트워크 정보를 함께 포함하고있다.

② 암호화 목록(Crypto Set)

- 암호화 알고리즘 : 다양한 암호화 알고리즘 중 사용자의 사용알고리즘에 대한 정보 및 데이터의 접속시간 및 송수신 된 데이터의 크기 등이 기록된다.
- 인증헤더(AH) 알고리즘 : 데이터의 인증에 필요한 알고리즘의 정보를 기록하게 되며, 사용자의 IP와 접속시간에 대한 정보를 포함하게 된다.

③ 세션 키

- 키 관리 : VPN 통신을 하고자하는 사용자간의 세션연결을 위한 세션 키의 사용자별, 네트워크 주소별 등의 정보를 포함하게 된다.
- 키 생성 및 저장 : 세션연결에 필요한 세션 키의 생성을 인증서와 함께 사용자에게 분배한 시간과 유효성을 함께 포함하는 정보를 기록한다.
- 키 로그 저장 : 키에 관한 모든 접속 로그 및 사용자로그 기록을 총괄하여 저장한다.

표 1. DBMS의 구성 형태

구 분	기 능
Certificate	CRL& Certificate Sub CA/RA information
Crypto Set	Cryto Algorithm AH Algorithm
Session Key	Key Manage Key Create/store Key log store
Log	Connection log Source/Destination IP & Port Keychange Algorithm
Tunneling Protocol	Tunneling Protocol Set Connection Port Set
Proxy Seting	Service Port Set Flag Set Realtime Status

④ 로그

- 연결상태 로그 : 연결상태에 있는 사용자간의 전송되는 데이터에 대한 연결 상태의 로그를 저장하여 보관한다.
- 출발지/목적지 IP * Port : 목적지와 출발지 및 경유하게 된 CA/RA에 대한 정보를 저장한다.

⑤ 터널링 프로토콜

- 터널링 프로토콜 집합(Tunneling Protocol set) : 터널링 프로토콜의 종류와 연결확인에 대한 정보를 저장하게 된다.
- 연결모드(Connection mode) : 터널링 및 전송모드의 선택에 따른 데이터 정보를 저장하게 된다.

⑥ 프록시 설정(Proxy Setting)

- 서비스 집합(Service Set) : 통신 프로토콜 서비스의 허용과 차단에 따른 로그기록 및 서비스 사용중인 내용에 대한 정보를 포함한다.
- 플래그 집합(Flag Set) : ECN, SYN차단, 자바 크립트 등에 관련한 추가 옵션기능의 로그정보를 저장한다.
- 실시간 상태 : 실시간 통제 감사로그기록을 저장함으로써 연결상태 시에도 통제함으로 인해 발생하는 로그기록을 저장하게 된다.

3.2 CA-VPN의 성능 및 분석

현재 VPN 장비간의 상호 확인기능에 있어 발생 가능한 신분을 위장한 공격방법들에 있어 제안한 CA-VPN은 공개키와 개인키를 활용한 PKI 방식의 인증을 제공함으로써, 동일장비로의 해킹가능성과 로그인 정보의 유출에 의한 기존의 공격기법들로부터 보다 안전한 인증성을 제공할 뿐만 아니라, VPN장비간의 연결상황 및 설정상황을 통합관리 할 수 있어, 침입유무에 관계없이 모든 감사기록을 통해 접속에 따른 설계 성능 및 분석은 다음과 같다.

첫째, 인증성은 동일 장비를 이용하여, 동일 설정을 이용한 공격가능성으로부터 강력한 인증성을 제공함으로써, CA-VPN 게이트웨이로부터 접속이 차단된다.

둘째, 감사추적기능은 VPN장비를 이용한 해킹 및 접속시도에 따른 감사기록을 관리할 수 있어 침입경로 및 침입패턴으로 추적이 가능하다.

셋째, 키 분배메커니즘의 보안성에 따른 문제를 해결할 수 있다. 현재 사용중인 키 분배 메커니즘의 사용자정보의 유출가능성으로부터 CA-VPN을 통해 스니핑 공격으로부터 보호될 수 있다.

넷째, 다음 [표2]은 각종 공격으로부터 기존의 VPN과 CA-VPN의 분석을 나타낸 것이다.

이러한 비교분석의 토대를 고려해 볼 때, 보안의 중요성이 증가하며, 개인정보의 중요성도 부각되고 있다. CA-VPN에서 게이트웨이는 다양한 분야에서 응용 및 활용되어질 수 있다.

표2. VPN과 CA-VPN의 비교분석

구분	기존의 VPN	CA-VPN
사용자 인증성	미흡	탁월
Sniffing attack	가능	불가능
동일장비 공격	가능	불가능
사용자 위장공격	가능	불가능
키 유출가능성	가능	불가능
감사 추적	불가능	가능
알고리즘 통합관리	불가능	가능
다중 연결관리 및 통제	불가능	가능

즉, 보안을 필요로 하는 공공단체 및 금융기관 그리고 기업체의 인트라넷과 익스트라넷, 국제적 교류가 많은 곳에서도 사용이 가능하다. 네트워크 망에서 안전한 데이터의 전송뿐 만 아니라, 상대 통신자의 확실한 신분확인을 함께 수행함으로써 보다 신뢰성 있는 통신망 구조를 구축할 수 있다.

Ⅳ. 결 론

인터넷 시장의 광범위한 확산과 이에 따른 보안문제의 심각성이 대두되고 있으며, 보다 안전하고 신뢰성 있는 네트워크 구축에 대해 요구하는 수요자들을 만족시키기 위한 노력이 계속되고 있다. 제안하는 CA-VPN의 설계에 관한 VPN의 장점과 VPN에서의 취약점으로 고려되었던 키 관리 문제를 PKI를 활용하여 보다 향상된 방안을 제시하였다.

향상될 보안성에 대해서 첫째, 세션 연결 시 개인정보의 유출 가능성을 배제와 동일장비를 이용한 해킹공격으로부터 장비에 대한 인증을 수행한다. 둘째, VPN 사용자의 감사기록으로 추적정보를 생성과 인증서 발급을 통해 사용자의 신뢰성을 보장한다. 셋째, VPN은 공개키와 비밀키로 운영이 되기 때문에 불법적인 사용을 하고자 하는 내부자라 할 지라도 사용할 수 없다. 넷째, 인증서 만료를 통해 연결 후 불법적인 침입시도를 차단할 수 있고, 데이터의 암호화를 위한 키 생성에 공개키 또는 개인 키를 사용할 수 있다.

즉, CA-VPN의 게이트웨이 의한 설계로 PKI를 통해 개인정보 및 인증정보에 대한 노출을 방지함으로서, 신뢰성 있는 통신을 수행하고, 접근통제의 기능을 부여함으로써, 동일장비를 통한 VPN 연결 공격을 막을 수 있다.

또한 VPN 장비 사용자들에게 인증서를 발급함으로써, 사용자 및 VPN 장비에 대한 모니터링과 감사를 수행함으로서 기존의 VPN을 통합 관리할 수 있다. 제안한 CA-VPN에서 게이트웨이 운용 시스템에서는 추적 및 관리와 방어를 함께 응용할 뿐만 아니라, 모든 VPN 사용자의 실시간 관리를 목적으로 하고 있다.

날로 커져만 가는 사이버 테러 및 해커들로 인한 사생활 침해에 대한 대안으로 CA-VPN은 현시점에서보다 앞으로 VPN 시장의 확장을 겨냥한 미래의 통합 운용 관리 시스템이라고 할 수 있다. 침입차단의 기능뿐만이 아니라, VPN 게이트웨이로서 사용되어질 CA-VPN의 제안은 앞으로 적용성을 확대하여 신분확인, 접속자 통제, 패킷 필터링, 감사기록 등의 기능을 함께 수행할 수 있음으

로써, 기존의 침입차단 시스템보다 보안성 향상에 크게 기대된다.

그러나 문제점은 다중의 사용자 접속시 로그의 저장방법에 대한 처리문제와 CA-VPN에서 CA·RA 통합 시스템이 설치 운영될 하드웨어의 뒷받침 또한 중요한 문제로써 남아 있다.

참고문헌

[1] David McDysan , "VPN Applications Guide : Real Solutions for Enterprise Networks" Jonhn Wiley & Sons, Inc, 2000

[2] William Stallings, "Network Security Essentials : Applications and Standards " Prentice-Hall, Inc, May 1999

[3] S. Kent, R.Atkinson, "IP Encapsulating Security Payload(ESP)", 1998

[4] RFC 2408 Internet Security Association and Key Management Protocol(ISAKMP)

[5] Modelling a Public-Key Infrastructure : Ueli Maurer

[6] AES Key Agility Issues in High-Speed IPSec Implementatins : Doug Whiting, Bruce Schneier, Steve Bellovin

[7] IBM/Tivoli Technical Evangelist : Laura

[8] A Cyptographic Evalution of IPSec : Ferguson, Bruce Schneier

[9] Performance Comparison of the Submissions : Bruce Schneier, John Ke Doug Whiting, David Wagner, Chris Hall

[10] PKI and VPNs-Enabling Security in Increcasingly Networked World, ALCATEL,

저자소개

김 도 문

계명대학교 컴퓨터학과 졸업
숭실대학교 대학원 컴퓨터학과 공학석사
숭실대학교 대학원 컴퓨터학과 (박사과정수료)
현재 동우대학 컴퓨터 그래픽과 조교수
관심분야 : 네트워크보안, 암호학, 컴퓨터그래픽

전 정 훈

숭실대학교 컴퓨터학과 졸업
숭실대학교 대학원 컴퓨터학과 공학석사
숭실대학교 대학원 컴퓨터학과 (박사과정)
현재 : 매직캐슬 정보통신 근무
관심분야 : 네트워크 보안, 암호학, 정보통신

전 문 석

숭실대학교 전자계산학과 졸업
University of Maryland, Computer Science(석사)
University of Maryland, Computer Science(박사)
Morgan State Univ. 부설 Physical Science Lab. 책임 연구원
현재 : 숭실대학교 컴퓨터학부 부교수
관심분야 : 네트워크 보안, 암호학, 컴퓨터 알고리즘