공인인증기반 가상사설망(VPN)에서의 문제점과 해결방안에 관한 연구

김재홍* 유인태* 윤정원**

*경희대학교, 정보통신대학원 정보통신망관리학과

**한국전산원 정보연계인증부

Comprehension Analysis on PKI-Based VPN Architecture

Jaehong Kim* Intae Ryoo* Jeongwon Yoon**

*Network Management Engineering, Kyung-Hee University

**National Computerization Agency

요 약

인터넷은 확장성과 사용상의 편의성을 바탕으로 급격한 확산을 가져오게 되었다. 그러나 인터넷의 개방성과 확장성으로 인해 보안상 취약성이 나타나게 되었다. 이에 따라 인터넷 환경에서 저렴한 비용으로 전용 사설망과 같은 보안성을 보장해주는 가상사설망(VPN)의 도입이 활성화되고 있다. 전자상거래와 재택근무등 가상사설망 구축의 범위가 커지면서 사용자 인증과 키관리 및 분배 자동화를 위하여 공개키기반의 공인인증서비스를 적용한 VPN구축이 필요하게 되었다. 본 글에서는 공인인증서비스를 적용한 VPN구축사례를 통해 공인인증서비스의 적용시 문제점과 그 해결방안에 대해 알아본다.

I. 서론

오늘날 정보통신기술의 발전은 인터넷기술의 급진전을 가져왔다. 인터넷은 확장성과 사용상의 편의성을 바탕으로 전자상거래, 온라인 뱅킹, 온라인 쇼핑, 온라인 주식거래등의 급격한 확산을 가져왔으나, 일부 사용상의 문제점이 나타나게 되었다. 그것은 인터넷의 개방성과 확장성으로 인한 보안상 취약성이 드러났고, 네트워크 공유로 인한 속도저하 등의 서비스 질(QoS: Quality of Service)이 불확실해진 것이다. 또한 해킹기술등의 발전으로 인하여 정보의 유출, 변조, 도용 등의 보안상 문제점이 심각하게 대두되었고, 네트워크를 공유함에 따라 자원의 독점이 불가능하므로 원하는 시간에 원하는 만큼의 정보를 전송할 수 있는 기능을 보장할 수 없게 된 것이다. 이러한 문제점을 해결하기 위하여 가상사설망(VPN: Virtual Private Network)이 나타나게 되었다.

VPN(Virtual Private Network)이란 글자그대로 물리적으로 존재하지 않는 사설망(Private Network)을 가상(Virtual)으로 구축하여 전용망처럼 사용하는 것을 말한다. 즉, 사설망을 물리적으로 새로이 구축하지 않고 기존의 인터넷망과 같은 공중망(Public Network)을 이용하여 자신의 사설망처럼 이용하는 것을 의미한다. 가상사설망(Virtual Private Network)은 기존의 전용선의 문제점인 고비용과 확장의 어려움을 극복하면서도 전용망과 같은 서비스의 질과 보안기능을 제공하여 줌으로써 새롭게 대두되고 있다. 이러한 VPN은 본사와 지사를 연결하는 intranet, 협력사와 연결되는 extranet, 그리고 최근들어 급증하고 있는 이동근무자와 재택근무자들의 원격접속등이 늘어나면서 강력한 사용자인증과 키관리 및 분배의 자동화를 이룰 수 있는 공개키기반의 공인인증서비스의 적용을 가져오게 되었다. 본 글은 공개키기반 공인인증서비스 기반의 가상사설망(Virtual Private Network)의 구축과 사용상의 문제점과 그 해결방안에 관하여 알아보고자 한다.

II. VPN기술 개요

VPN은 터널링 기술을 이용하여 송신자가 보내는 데이터 패킷에 보안 헤더를 추가하여 원래 패킷을 캡슐화하는 방식으로 수신자 외에는 알아볼 수 없도록 패킷을 전송하는 기술을 말한다. 대표적인 터널링 프로토콜은 Layer 2에서 사용되는 PPTP, L2TP등과 Layer 3에서 쓰이는 IPsec등으로 구분할수 있다. 현재는 많은 표준화 노력과 호환성의 문제등으로 인해 L2TP와 IPsec이 대표적인 터널링 프로토콜로 자리를 잡고 있다.

1. 주요 프로토콜

1) L2TP(Layer 2 Tunneling Protocol)

L2TP는 마이크로소프트사의 PPTP와 시스코의 포워딩(L2F)기술이 결합된 것이다. L2TP는 클라이언트와 프락시 서버간 터널을 생성해 주기 위한 목적으로 사용되며 보안 기능과 직접적인 관련은 없으나 연결성을 좋게 하므로 IPsec프로토콜의 암호, 인증부분을 적용하여 함께 사용한다.

표1 : 계층별 VPN 프로토콜

Security GateWay	OSI Layer	Security Protocol (VPN 프로토콜)
Application Proxy	Application Layer	
	Presentation Layer	
Session Layer Proxy	Session Layer	Socks V5, SSL
	Transport Layer	
Packet Filtering	Network Layer	ATMP, VTP, IPsec
	Data Link Layer	L2F, PPTP, L2TP
	Physical Layer	

2) IPsec(Internet Protocol Security)

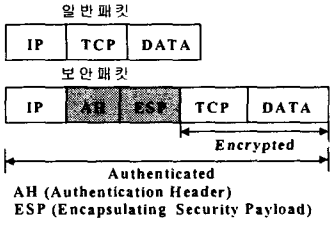
IPsec은 IP망에서 안전하게 정보를 전송하는 표준화된 계층3 프로토콜로서, IPsec과 관련된 프로토콜과 구조에 대한 표준화는 거의 완료된 상태이다. IPsec은 전송모드와 터널 모드 2가지가 있다. 전송모드는 IP페이로드를 암호화하여 IP헤더

M	H	0	0	0	0	Overall Length	Vender ID
Attribute							Value
Until overall length is rdached							

<그림 1> L2TP 패킷 형식

로 캡슐화한다. 터널모드는 IP패킷을 모두 암호화하여 인터넷으로 전송한다. 터널 모드 IPsec은 터널의 종단점과 첫번째 라우터 사이는 암호화되지 않은 평문으로 전송되고 라우터와 라우터 사이만 암호화되기 때문에, 주로 망간 연결에 사용한다. IPsec은 AH(Authentication Header)와 ESP(Encapsulation Security Payload)의 두가지 IP헤더를 가진다. AH는 인증 데이터와 순서번호(sequence number)를 가져서, 송신자를 확인하고, 메시지가 송신되는 동안 수정되지 않았음을 보장(데이터 인증)하며, 데이터의 암호화는 제공하지 않는다. ESP는 IP페이로드를 암호화하여 데이터 기밀성(confidentiality)을 제공하고 제3자가 데이터를 캡처하는 것으로부터 데이터를 보호한다.

IPsec 프로토콜의 구성요소는 다음과 같다.



<그림 2> 보안 패킷구조

Next header	Payload length	Reserved
Security Parameters index(SPI)		
Sequence Number		
Authentication Data(MD5, SHA-1) (Variable length of 32 bit words)		

<그림 3> AH 패킷구조

IPSec의 인증헤더인 AH는 IP 데이터그램에 대한 인증과 무결성을 보장하기 위한 메커니즘으로 리플레이 방지 기능을 포함하고 있다. 세부 기능을 살펴보면 IP 데이터그램 기반의 connectionless 무결성 제공, 인증알고리즘(MD5, SHA-1)을 이용한 데이터 출처 인증, 일련번호(sequence)를 이용한 리플레이 공격 방지, 비밀키 공유와 키관리 기술인 IKE(Internet Key Exchange) 메카니즘을 이용하여 안전한 통신 보장 등을 지원한다.

IPSec의 ESP는 IP 데이터그램의 무결성과 기밀성을 제공하는 메카니즘으로서 주요 기능은 안전한 키교환 메커니즘과 함께 데이터 기밀성을 위한 암호화 기능 제공, connectionless 무결성에 대한 인증과 데이터 출처에 대한 인증, 일련번호(sequence)를 이용하여 리플레이 공격 방지등의 기능을 한다.

A	Security parameters index(SPI)	
A	Squence Number	
A, E	Payload Data (Variable length of 32 bit words)	
A, E	Padding(0~255bytes)	
	Pad length	Next header
S	Authentication Data(Variable length)	

A: Authenticated, E: Encrypted

<그림 4> ESP 패킷구조

현재 IPsec통신은 IKE SA에 의하여 생성된 터널 내에서 이루어진다. IKE는 두 개의 키 관리 프로토콜인 Oakley와 SKEME으로부터 생성된 Hybrid방식의 프로토콜이며 Internet Security Association Key Management Protocol(ISAKMP) [RFC2408]라는 언어로 정형화된 프로토콜이다. IKE는 그 동작 방식에 따라 Phase 1(Main, Aggressive mode)과 Phase 2(Quick mode)로 구분되어진다. Phase 1은 IKE SA를 생성하는 방식으로 협의를 시작하는 쪽의 ID정보 및 보안터널의 생성방식에 대한 합의점을 찾게 되고, Phase 2는 IPsec SA를 생성하는 방식으로 Phase 1에서 얻은 정보 외에 목적지 주소정보와 그 밖의 정책을 수행하기 위한 제반 정보를 얻게 된다.

Ⅲ. 공인인증 서비스의 적용

1. 필요성

1) 키관리상의 문제점

VPN의 가장 핵심기술인 터널링을 위해서는 암호화가 필수이며 PKI기반의 암호화를 위해서는 데이터를 주고받는 두 개체간에 대칭키를 공유하고 있어야 한다. 그러나 대칭키로 암호화하기 위해 모든 노드가 통신하고자 하는 각 노드별로 고유한 키를 각각 공유하고 있어야 한다. 따라서, 노드가 추가되면 필요한 키의 수는 통제가 불가능한 수준으로 급격히 증가한다. 이 경우 관리자가 모든 노드에게 키를 안전하게 분배하기란 결코 쉽지 않다.

표2 : 노드 개수별 키의수

노드수	2	3	4	5	6	7	8	9	10	11	...	N
키의 수	1	3	6	10	15	21	28	36	45	55	..	N(N-1)/2

이에 대한 해결책이 바로 공개키기반인 PKI (Public Key Infrastructure)를 적용하는 것이다. 공개키기반의 방식은 암호화 키와 복호화 키를 분리하여 암호화 키는 송신하려는 모든 통신 참여자에게 공개하고, 복호화 키는 각자가 비밀리에 관리하는 방법이다.

2) 사용자 인증의 문제점

공인인증기관에서 발급하는 인증서는 신분확인을 거치기 때문에 이 인증서를 이용하여 VPN의 사용자 및 정보자원에 대한 인증도 할 수 있다. 인증이 필요한 사용자와 정보자원은 공인인증기관으로부터 받은 인증서를 통하여 VPN 환경에서 인증을 받고 안전하게 데이터를 주고받을 수 있다. 이러한 공인인증서를 이용하면 규모가 큰 네트워크에서 특정 다수의 사용자를 인증하는데 있어 VPN시스템 관리자에게 부하를 주지 않고 사용자 인증을 수행할 수 있다.

2. 공인인증기반 VPN의 장점

기존의 VPN은 관리자가 수동으로 암호화에 쓰일 키를 관리하였으나 PKI기반의 VPN은 공개키기반이라 손쉽게 키교환 및 관리를 할 수 있어 네트워크 규모가 확장되더라도 키관리가 매우 용이하고 또한 네트워크 규모가 G2G, G2B, B2B 등으로 확대되고, 이 기종 VPN과 연동을 할 경우에도 매우 용이하게 대처가능하며, 전자서명을 통한 사용자 인증과 제 3의 공인인증기관(CA)을 통한 안전 · 신뢰성 확보가 가능하다

표3. 기존 VPN과 PKI기반 VPN의 비교

VPN 구분	기존VPN	PKI기반 VPN
적용환경	소규모 네트워크에 적합	대규모 네트워크에 적합
키관리 및 배포	· 관리자에 의한 수동방식 · 어려움(확장시)	· 자동키 분배방식 · 매우 용이
확장성	어려움	매우 용이
이기종간 상호연동	불가	가능
이용자 등록	한번의 등록으로 가능	공인인증센터와 VPN센터 모두에 등록 필요

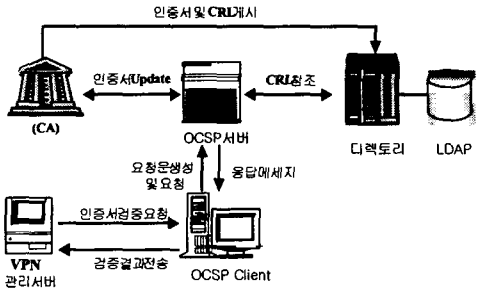
IV. 공인인증 적용시의 문제점

VPN서비스에서 사용자의 인증부분을 제 3자인 공인인증기관 대신하여 줌으로써. 규모가 큰 네트워크에서 특정 다수의 사용자를 인증하는데 있어 VPN시스템 관리자에게 부하를 주지 않고 사용자 인증을 수행할 수 있다. 인증서 검증시 VPN서버는 검증 시간 단축을 위해 인증기관으로부터 CRL(폐지목록)을 다운받아 저장하고, 인증서의 일련번호가 이 CRL(폐지목록)에 들어있는지를 확인하는 절차를 통해 인증서의 유효성을 검증하게 된다. 그러나 인증기관에서 다운받는 이 CRL(폐지목록)은 24시간안에 인증기관이 임의로 시간을 정해 갱신 함으로써 문제가 발생하게 되었다.

즉, 실시간 인증이 이루어질 수 없다는 문제가 발생하게 된 것이다. 현재의 시스템 구조에서는 사용자의 인증서를 폐지하거나 문제가 발생하여 인증서의 정보가 바뀌어도 CRL이 다시 게시되기 전에는 아무문제 없이 VPN서비스를 이용할 수 있다. 또한 현 공인인증기반 VPN에서는 접속시에 인증서가 유효하다고 판단하여 접속이 이루어지면 접속후 인증서에 문제가 생겨도 그 세션을 계속 유지하고 있게 된다. 즉, 누군가에 의해 인증서와 인증서 비밀번호를 도난 당하였다면 도난당한 인증서를 이용해 사용하고 있는 VPN 서비스를 중간에 차단할 수 있는 사용자 관리상의 사용자 차단 방법이 없다. 이러한 문제점을 해결하기 위한 하나의 방법으로 VPN관리서버를 이용해 연결된 모든 사용자들에 대한 일정시간마다 인증절차를 다시 거치도록 할 수 있다. 그러나 이런 방법은 인증기관의 디렉토리에 게시되는 CRL(폐지목록)의 주기와 VPN서버의 부하가 증가하여 사용자 수에 비례하여 접속속도 및 관리 기능의 저하등의 이유로 실현이 불가능 하다.

V. 해결방안

VPN 사용자의 실시간 검증이 이루어져야 만이 다른 사용자의 인증서를 도용한 공격에 대한 시스템 접근의 차단과 올바른 사용자 인증이 이루어질 수 있다. 이러한 문제점을 해결할수 있는 방법으로 현재 각 공인인증기관에서 추진중인 OCSP (Online Certificate Status Protocol, 실시간 인증서 상태조회 프로토콜)를 이용하는 방법이 있다. OCSP는 CA DB에서 Action이 일어날때마다 생성되는 Revoked Table을 검색하여 인증서의 실시간 상태를 검증하는 역할을 하도록 설계되어 있다.

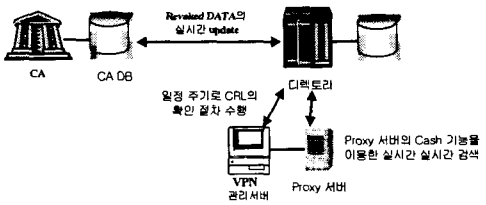


<그림 5> OCSP의 구조

따라서, VPN서버에 OCSP Client를 설치한 후 신원확인에 대한 모든 작업을 OCSP Client를 이용하여 처리하는 모델을 구현한다면 OCSP 서버가 CA DB에서 Action이 일어날때마다 추가되는 Revoked Table데이터와 인증서 사용자의 CA 접속시 상태를 검색하여 인증서의 상태변화를 실시간으로 VPN서버에 알림으로써 사용자 인증의 실시간 처리가 가능하게 된다.

이것은 현 VPN서비스 이용자의 신원확인 과정에서 일어날 수 있는 사용자 도용등의 문제를 해결함으로써 네트워크의 보안성 강화를 가져오는 결과를 낳는다. 그러나 인증기관의 어플리케이션 프로그램에 너무 의존적일 수밖에 없다는 문제점을 안고 있다.

즉, 공인인증기반의 VPN증가와 사용자 증가시 처리능력의 한계로 인하여 응답메시지의 지연을 가져올수 있고 이로 인하여 접속중인자의 정기적인 인증서 검증시 서비스 속도의 저하를 가져올 수 있다. 따라서 현재의 구조처럼 OPENDB(디렉토리 시스템)을 이용하여 처리 하여 줌으로써 인증기관의 부담을 덜어 줄수 있다. OCSP에서 이루어지고 있는 실시간 데이터 update를 디렉토리로 해줌으로써 인증기관의 어플리케이션 프로그램의 의존성에서 벗어날 수 있으며, 실시간 검증에는 문제가 없는 모델을 구현 할수 있다.



<그림 6> 디렉토리의 실시간 UPDATE시의 구조

참고문헌

[1] 가상사설망(VPN) 기술과 동향, 한국전산원, 2000

[2] PKI기반의 원내 인트라넷 VPN시스템 구축 제안서, 퓨처시스템, 2001

[3] 가상사설망 기술 및 표준화 동향. ETRI 결과정리 및 효과

[4] 송명원, 윤병남, 한국전산원 정보인증센터 정기점검 2002년8월

[5] 신순자, 공인인증기반 가상사설망(VPN) 구축, 통신학회, 2001년 11월

[6] PKI and VPNs-Enabling Security in an Increasingly Networked World, ALCATEL, 2000

[9] RFC#2401 Security Architecture for the Internet Protocol

[10] RFC#2409 The Internet Key Exchange(IKE)

[11] RFC#2411 IP Security Document Roadmap

[12] Virtual Private Network Security Components, CHECKPOINT, 1998