情報保護學會論文誌
第14券 第5號, 2004. 10

IPSec-VPN 시스템에서의 속성 인증서를 이용한 사용자 접근 제어 방안

강 명 희[a)†], 유 황 빈[b)‡]
(주) 퓨쳐시스템[a)], 광운대학교[b)]

An User Authorization Mechanism using an Attribute Certificate in the IPSec-VPN System

Myung-hee Kang[a)†], Hwang-bin Ryou[b)†]
Future System, Inc.[a)], KwangWoon University[b)]

요 약

Client-to-Gateway 형태의 IPSec-VPN 시스템에서 IPSec-VPN 클라이언트에 대한 사용자 접근 제어를 위해서는 통상 ID/Password 검증 방식 또는 IPSec-VPN 클라이언트가 인증되면, 묵시적으로 IPSec-VPN 게이트웨이가 IPSec-VPN 클라이언트에 대한 사용자 접근 제어가 수행된 것으로 간주하는 묵시적 사용자 접근제어 방식이 있다. 그러나 ID/Password 검증방식은 ID/Password 정보의 전송 방법이 용이하지 않고, 묵시적 사용자 접근제어 방식은 보안상 취약점이 있기 때문에 보다 효과적인 사용자 접근제어 방안이 필요하다. 본 논문에서는 Client-to-Gateway 형태의 IPSec-VPN 시스템에서의 효과적인 사용자 접근제어 방안으로써, 속성 인증서를 이용한 사용자 접근제어 방안을 제안하고, 사용자 접근제어 엔진을 설계, 구현하였다. 본 논문에서 제안한 IPSec-VPN을 위한 사용자 접근제어 방안은 기존의 IPSec-VPN 시스템에 구현이 용이하고, 다른 IPSec-VPN 시스템과의 상호 호환성이 보장되는 장점을 가지고 있다. 또한 본 논문에서 설계, 구현한 사용자 접근제어 엔진은 속성 인증서를 이용한 임의적 접근제어, 역할기반 접근제어 뿐만 아니라, SSO(Single Sign-On) 기능을 제공할 수 있다.

ABSTRACT

To authorize IPSec-VPN Client in Client-to-Gateway type of the IPSec-VPN system, it can be normally used with ID/Password verification method or the implicit authorization method that regards implicitly IPSec-VPN gateway as authorized one in case that the IPSec-VPN client is authenticated. However, it is necessary for the Client-to-Gateway type of the IPSec-VPN system to have a more effective user authorization mechanism because the ID/Password verification method is not easy to transfer the ID/Password information and the implicit authorization method has the vulnerability of security. This paper proposes an effective user authorization mechanism using an attribute certificate and designs a user authorization engine. In addition, it is implemented in this study. The user authorization mechanism for the IPSec-VPN system proposed in this study is easy to implement the existing IPSec-VPN system. Moreover, it has merit to guarantee the interoperability

접수일 : 2004년 1월 26일 ; 채택일 : 2004년 9월 6일
† 주저자 : mhkang@future.co.kr
‡ 교신저자 : ryou@kw.ac.kr

with other IPSec-VPN systems. Furthermore, the user authorization engine designed and implemented in this paper will provide not only DAC(Discretional Access Control) and RBAC(Role-Based Access Control) using an attribute certificate, but also the function of SSO(Single-Sign-On).

Keywords : *IPSec-VPN, User Authorization, Attribute Certificate, SSO, IKE*

Ⅰ. 서 론

IPSec-VPN 시스템은 네트워크 경계점에서 라우터에 연결되는 IPSec-VPN 게이트웨이간에 가상 사설망을 구성하는 Gateway-to-Gateway 형태의 IPSec-VPN 시스템과 IPSec-VPN 게이트웨이와 사용자간에 가상 사설망을 구성할 수 있는 Client-to-Gateway 형태의 IPSec-VPN 시스템이 있다. Gateway-to-Gateway 형태의 IPSec-VPN 시스템은 사용자 측면에서는 IPSec-VPN 구성에 따른 부가적인 프로그램의 설치, 변경 등의 작업이 전혀 필요 없는 장점이 있고, Client-to-Gateway 형태의 IPSec-VPN 시스템은 실질적인 단대단 보안 서비스를 제공할 수 있으며, 사용자가 재택근무 또는 외부 출장지에서의 사내망과의 IPSec-VPN 구성 등의 Remote Access VPN 서비스를 제공할 수 있는 장점을 갖는다. 그러나 Client-to-Gateway IPSec-VPN 시스템을 이용한 Remote Access VPN 서비스를 제공하기 위해서는 사용자 인증, 통신 메시지 암/복호화 뿐만 아니라, 사용자 접근 제어 기능이 요구되고 있으나[1,2,8], IETF의 IPSec 표준 문서들에서는 통신하는 개체들 사이의 상호 인증 및 키 교환 기법에 대해서는 명확하게 규정하고 있지만, 사용자에 대한 접근제어 기능과 관련해서는 구체화 되어 있지 않다. 그리하여, Client-to-Gateway 형태의 IPSec-VPN 시스템들에서는 IPSec-VPN 클라이언트에 ID/Password를 부여하여, ID/Password를 IPSec-VPN 게이트웨이에서 이를 검증하는 방법과 IPSec-VPN 클라이언트에 대한 상호 인증이 성공적으로 통과되면, 묵시적으로 접근을 허용하는 묵시적 접근제어 방법을 사용하고 있다. 그러나 ID/Password 검증 방법 IKE 교섭 과정에서 ID/Password 정보의 전송 방법이 용이하지 않고, 묵시적 접근제어 방법은 사용자가 접근 불가인 상황이 발생하더라도, IPSec-VPN 시스템이 보호하는 내부 영역에 접근할 수 있는 가능성 있기 때문에, 보다 효과적인 사용자 접근제어 방안이 요구되어지고 있다.

본 논문에서는 IPSec-VPN 시스템을 위한 효과적인 사용자 접근제어 방안으로써, 속성 인증서를 이용한 사용자 접근 제어 방안을 제안하고, 사용자 접근제어 엔진을 설계, 구현하였으며, 본 논문에서의 설계, 구현한 사용자 접근제어 엔진은 속성 인증서를 이용한 임의적 접근제어, 역할기반 접근제어 뿐만 아니라 SSO(Single Sign-On) 기능을 제공할 수 있다.

본 논문의 구성은 2장은 관련 연구로써, IPSec-VPN 시스템에서의 사용자 접근 제어 필요성과 공인 인증서의 식별번호를 이용한 사용자 접근 제어 방법에 대하여 기술하고, 3장에서는 본문에서 제안한 시스템에 대하여 기술하였으며, 4장에서는 본 논문에서 제안한 접근 제어 방법에 대한 시스템 분석을 다루었으며, 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 사용자 접근 제어 필요성

IPSec-VPN 시스템에서는 상호 인증 및 키 분배를 위해서 주로 전자 서명 방식의 상호 인증 및 키 분배 방식을 사용하고 있는데, 이를 위해서는 비밀키와 공개키 인증서가 필요하다. IPSec-VPN 시스템에서는 공개키 인증서를 발급받아 사용하기 위해서, IPSec-VPN 시스템 구성 요소 자체에서 공개키 인증서를 생성할 수 있는 Embedded CA 방식과 외부 PKI 사용방식을 사용한다. 그러나 공개키 인증서는 통신하는 개체사이의 상호인증만을 위해서 사용되기 때문에, IPSec-VPN 시스템에서는 IPSec-VPN 게이트웨이에서 클라이언트의 ID/Password를 검증하는 방법과 IPSec-VPN 클라이언트의 IKE 교섭이 성공하면, 묵시적으로 접근을 허용하는 묵시적 접근제어 방법 등을 사용하고 있다. 그러나, ID/Password 검증 방식은 IKE 교섭과정에서 ID/Password 정보 전송이 용이하지 않고, 묵시적 접근제어 방법은 IPSec-VPN 클라이언트 사용자가 더 이상 접근 불가인 상황이 발생하더라도, 외부 PKI로부터 발급된 유효한 인증서를 가지고 IKE 교

섭을 수행하여, 상호인증이 성공되면, IPSec-VPN 시스템이 보호하는 내부 영역에 접근할 수 있는 보안상의 취약점을 가지고 있다. 또한 외부 PKI로부터 사용자가 발급받은 인증서에 대해서는 사용자 자신 이외에는 취소가 불가능하기 때문에, 외부 PKI를 이용하여 IKE를 교섭을 수행할 때는 보다 효과적인 IPSec-VPN 시스템을 위한 사용자 접근 제어 방안이 요구되어 진다.

2.2. 공인 인증서를 이용한 접근 제어 방안

국내 공인 인증 체계에서는 공인 인증서의 확장 필드에 식별 번호 정보를 포함시켜 사용자 접근 제어를 수행할 수 있도록 하고 있는데, 식별번호 정보(주민등록번호 혹은 사업자등록번호)와 난수 값을 연접시켜, 해쉬 알고리즘을 적용하여 나온 결과 값(VID : 가상 식별번호)을 SubjectAltName 확장필드에 포함시켜 인증서를 발행하여 사용하고 있다[10,11,12]. 공인 인증서의 식별번호를 이용한 사용자 접근 제어를 수행하는 과정은 응용 서비스의 운용 환경에 따라 3가지 방법으로 사용자 접근 제어를 수행할 수 있으나, 이 방법은 자연인을 대상으로 하는 응용에서는 유리하지만, IPSec-VPN과 같은 시스템 개체에는 주민등록번호와 같은 식별번호가 없기 때문에, IPSec-VPN을 위한 별도의 식별번호 부여가 공인 인증 체계에서 요구된다. 또한 IPSec-VPN을 위한 별도의 식별번호가 부여되더라도, IPSec-VPN 시스템 내부에서 부여된 식별번호를 유지하거나, 기존의 ISAKMP/IKE 표준 프로토콜을 수정하여야 하는 단점을 가지고 있다. 따라서 공인 인증서의 확장 필드에 식별번호 정보를 포함시킨 접근 제어 방법은 IPSec-VPN 시스템에서 사용하기에는 부적합 한점이 있다.

Ⅲ. 시스템 설계

3.1. 시스템 구조

IPSec-VPN 시스템에서 전자서명방식의 상호인증을 위해서는 공개키 인증서를 발급, 관리할 수 있는 PKI가 요구되는데, IPSec-VPN 관리 시스템에 자체 PKI 기능을 탑재한 Embedded CA 방식과 외부 PKI로부터 공개키 인증서를 발급받아 사용하는 방식이 있다. Embedded CA 방식은 직접 IPSec-VPN 게이트웨이와 클라이언트에 공개키 인증서를 발급할 수 있기 때문에, 전자서명 알고리즘, 전자서명 알고리즘의 서명키 길이 등의 설정에 있어, 외부 PKI와는 달리, 보다 유연성이 있다. 반면, 외부 PKI로부터 IPSec-VPN 게이트웨이와 클라이언트가 공개키 인증서를 발급받는 경우에는 IPSec-VPN 시스템에 부가적인 공개키 인증서 관련 서비스가 필요 없고, 단지 외부 PKI로부터 발급받은 공개키 인증서를 IPSec-VPN 게이트웨이와 IPSec-VPN 클라이언트에 Import 하는 기능 정도만 필요하므로, IPSec-VPN 관리 시스템을 비롯한 게이트웨이, 클라이언트 모두 공개키 인증서의 발급, 갱신, 폐지 등의 PKI 서비스를 구현할 필요가 없다. 본 논문에서는 Embedded CA 환경과 외부 PKI 사용 환경 모두에서 효과적인 Client-to-Gateway IPSec-VPN 시스템을 위한 사용자 접근제어 방안을 제안한다.

3.1.1. Embedded CA 환경에서의 사용자 접근 제어

다음 그림 1은 Embedded CA 환경에서의 사용자 접근 제어를 위하여, 공개키 인증서 및 속성 인증서가 발급되고, 공개키 인증서와 속성인증서를 이용하여, 사용자 접근 제어가 수행되는 시스템 구조이다.

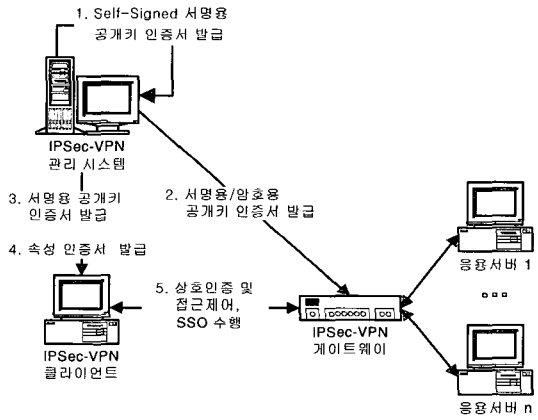

그림 1. Embedded CA 환경에서의 사용자 접근제어

1. IPSec-VPN 관리 시스템은 IPSec-VPN 게이트웨이, IPSec-VPN 클라이언트의 인증서를 발급해주기 위한 목적으로 자신의 Self-Signed 서명용 공개키 인증서를 발급한다.
2. IPSec-VPN 관리 시스템은 IPSec-VPN 클라이언트와 게이트웨이 상호간의 IKE 교섭 시, 필요한 IPSec-VPN 게이트웨이의 서명용

공개키 인증서를 발급한다. 또한 IPSec-VPN 클라이언트가 특정 응용서버에 접속하는데 필요한 ID/Password 정보를 안전하게 속성인증서에 명시하기 위한 목적으로, IPSec-VPN 게이트웨이에 암호용 공개키 인증서 또한 발급한다. 이때, 서명용 공개키 인증서가 암호화 용도로 사용될 수 있으면, 암호용 공개키 인증서는 별도로 발급받을 필요는 없다.

3. IPSec-VPN 관리 시스템은 IPSec-VPN 클라이언트와 게이트웨이 상호간의 IKE 교섭 시, 필요한 IPSec-VPN 클라이언트의 서명용 공개키 인증서를 발급한다.
4. IPSec-VPN 관리 시스템은 IPSec-VPN 클라이언트에 대한 속성 인증서를 발급하고, IPSec-VPN 클라이언트는 발급받은 자신의 속성 인증서를 시스템 내부에서 유지한다. 속성 인증서의 세부 속성 정보는 IPSec-VPN 클라이언트가 접속하고자 하는 응용 서버의 서비스 정보, 접속 ID 정보, 그룹 정보, 역할 정보 등을 속성 인증서 내부의 속성 필드에 명시한다. 이때, 접속 ID 정보와 Password 정보와 같이 비밀성이 요구되는 정보는 해당 IPSec-VPN 게이트웨이의 암호용 인증서를 이용하여, 암호화한다. 속성 인증서의 갱신 과정은 속성 인증서 발급과정과 동일하며, 속성 인증서의 유효기간은 1주 정도로 짧게 설정하고, 속성 인증서의 폐지 과정을 없앰으로써, 인증서의 폐지 목록 발행 및 검증에 따른 오버헤드가 발생하지 않도록 한다.
5. IPSec-VPN 클라이언트와 게이트웨이는 발급받은 서명용 공개키 인증서를 이용하여, IKE 교섭을 수행하고, IKE 교섭 과정 마지막 시점에서 IPSec-VPN 클라이언트는 자신의 속성 인증서를 IPSec-VPN 게이트웨이에 제출하고, IPSec-VPN 게이트웨이는 이를 검증함으로써, 사용자 접근 제어를 수행한다. IPSec-VPN 게이트웨이는 클라이언트의 속성 인증서 내부의 Service Authentication Information, Access Identity 필드의 정보를 검색하여, 검증함으로써, SSO(Single-Sign On) 기능을 수행한다.

3.1.2 외부 PKI 사용 환경에서의 사용자 접근 제어

다음 그림 2는 외부 PKI 사용 환경에서의 사용자

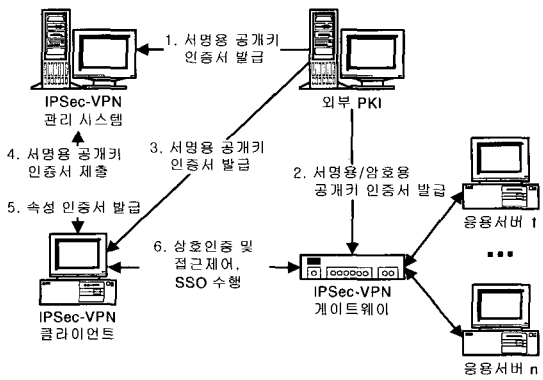

그림 2. 외부 PKI 사용 환경에서의 사용자 접근제어

접근 제어를 위하여, 공개키 인증서 및 속성 인증서가 발급되고, 공개키 인증서와 속성인증서를 이용하여, 사용자 접근 제어가 수행되는 시스템 구조이다.

1. IPSec-VPN 관리 시스템은 IPSec-VPN 클라이언트의 속성 인증서를 발급해주기 위한 목적으로 외부 PKI로부터 서명용 공개키 인증서를 발급받는다.
2. IPSec-VPN 게이트웨이는 IKE 교섭 시, 필요한 서명용 공개키 인증서를 외부 PKI로부터 발급 받는다. 또한 IPSec-VPN 클라이언트가 특정 응용서버에 접속하는데 필요한 ID/Password 정보를 안전하게 속성인증서에 명시하기 위한 목적으로, IPSec-VPN 게이트웨이는 외부 PKI로부터 암호용 공개키 인증서 또한 발급한다. 이때, 서명용 공개키 인증서가 암호화 용도로 사용될 수 있으면, 암호용 공개키 인증서는 별도로 발급받을 필요는 없다. 통상 IPSec-VPN 게이트웨이는 하드웨어 전용 장비인 경우가 많기 때문에, 외부 PKI로부터 공개키 인증서를 발급받는 과정을 IPSec-VPN 관리 시스템이 대신 수행할 수 있다.
3. IPSec-VPN 클라이언트는 IKE 교섭 시, 서명용 공개키 인증서를 외부 PKI로부터 발급받는다.
4. IPSec-VPN 클라이언트는 자신의 속성 인증서를 발급받기 위하여, 외부 PKI로부터 발급받은 서명용 공개키 인증서를 IPSec-VPN 관리 시스템에 제출한다.
5. IPSec-VPN 관리 시스템은 IPSec-VPN 클라이언트가 제출한 서명용 공개키 인증서 정보

를 이용하여, 속성 인증서를 발급한다. 속성 인증서의 세부 속성 정보 설정 및 속성 인증서의 갱신 과정, 유효기간 설정 등은 Embedded CA 사용 환경과 동일하다.

6. IPSec-VPN 클라이언트의 상호 인증 및 접근 제어, SSO 기능 수행 과정은 Embedded CA 사용 환경과 동일하다.

3.1.3 속성 인증서 프로파일 구조

본 논문에서 제안한 시스템에서 사용되는 속성 인증서 프로파일은 IETF의 RFC 3281 표준 규격을 기본적으로 준용하였다[2]. 다음 표 1은 본 논문에서 사용되는 속성 인증서 프로파일을 나타낸 것이다.

속성 인증서의 속성 정보 필드 내부에는 Service Authentication Information, Access Identity, Group, Role 속성으로 구성된다.

- **Service Authentication Information** : IPSec-VPN 클라이언트가 접속하고자 하는 응용 서버와 서비스 이름을 설정하고, ID/Password 정보를 기술한다. 이때 Password 정보를 보호하기 위하여, IPSec-VPN 게이트웨이의 공개키 인증서를 이용하여, Password 정보는 암호화한다. 이 필드는 IPSec-VPN 클라이언트에 대한 임의적 접근제어 및 SSO 기능 수행을 위하여 사용된다.
- **Access Identity** : Service Authentication Information 속성 정보와 유사하게 IPSec-VPN 클라이언트가 접속하고자 하는 응용 서버와 서비스 이름을 설정하지만, Password와 같은 인증 정보는 설정하지 않는다. 이 필드는 IPSec-VPN 클라이언트에 대한 임의적 접근제어 및 SSO 기능 수행을 위하여 사용된다.
- **Group** : 해당 IPSec-VPN 클라이언트가 속한 그룹을 설정한다.
- **Role** : Role 속성 정보는 해당 IPSec-VPN 클라이언트의 역할 정보를 설정한다. 이 필드는 IPSec-VPN 클라이언트에 대한 역할 기반 접근 제어를 위하여 사용된다.

본 논문에서 준용한 RFC 3281 표준에서는 위에서 열거한 속성 정보를 정의하였으나, 이들 속성 정보를 포함하여, 속성 인증서를 발행하기 위한

표 1. 속성인증서 프로파일

세부 필드	프로파일 내용
version	v2(1)
holder	baseCertificateID : 공개키 인증서의 issuer와 serial number로 구성
issuer	IPSec-VPN 관리 시스템의 subject name 값을 적용
signature	속성 인증서 서명 알고리즘 명시, IPSec-VPN 관리 시스템의 공개키 인증서의 공개키 정보의 알고리즘 정보에 따라 결정
serialNumber	속성 인증서 일련번호
attrCertValidityPeriod	속성 인증서 유효기간 : 1달로 적용하며, 속성 인증서의 만료 시점은 항상 공개키 인증서의 만료 시점 이전으로 설정
attributes	Service Authentication Information
	Access Identity
	Group
	Role
extensions	No Revocation Available : Null 값으로 설정
signatureAlgorithm	IPSec-VPN 관리 시스템의 공개키 인증서에 명시된 공개키에 부합되는 서명 알고리즘
signatureValue	속성 인증서에 대한 서명값

Attribute ASN.1 코드가 구체적이지 못하다. 즉, RFC 3281 표준의 부록에서 명시된 ASN.1 모듈에서는 Attribute를 정의하지 않고, RFC 2459의 Attribute를 import하여 사용하도록 되어 있으나, RFC 2459에서 정의한 Attribute의 세부 필드인 AttributeValue는 ANY로 정의되어 있기 때문에, 실제 구현상에 있어서는 모호성이 존재한다. 다음은 RFC 2459에서 정의되어 있는 Attribute에 대한 ASN.1 코드를 나타낸 것이다.

```
Attrubute :: SEQUENCE {
  type      AttributeType,
  values SET OF AttributeValue
     -- at least on value is required -- }

AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY -- 모호성 존재 --
```

RFC 3281 및 2459 표준의 Attribute에 대한 실제 구현상의 모호성을 해소하기 위하여 본 논문에서

는 다음과 같이 AttributeValue를 재정의 하였다.

```
AttributeValue ::= CHOICE {
  svcAuthInfo       [0]  SvceAuthInfo,
  accessIdentity    [1]  SvceAuthInfo,
  chargingIdentity  [2]  IetfAttrSyntax,
  group             [3]  IetfAttrSyntax,
  role              [4]  RoleSyntax,
  clearance         [5]  Clearance }
```

본 논문에서 재 정의한 AttributeValue ASN.1 코드를 RFC 3281 부록에서 명시한 속성인증서 ASN.1 모듈에 포함시키고, 이를 SNACC ASN.1 도구를 이용하여, 속성인증서의 생성/검증 모듈을 구현하였다[4,5,9]. 다음 그림 3은 SNACC ASN.1 도구를 이용하여, 본 논문에서 구현한 속성 인증서의 내부 속성 정보를 나타낸 것이다.

3.1. 접근 제어 및 SSO 수행 과정

본 논문에서 제안한 접근 제어 및 SSO 수행과정은 IPSec-VPN 관리 시스템으로부터 속성 인증서를 발급 받은 IPSec-VPN 클라이언트는 IPSec-VPN 게이트웨이와 IKE 교섭 과정 중 Phase 1 단계의 마지막 시점에서 속성 인증서를 제출하고, IPSec-VPN 게이트웨이는 제출 받은 속성 인증서를 검증하여, IPSec-VPN 클라이언트에 대한 접근 제어 및 SSO 기능을 수행한다.

IPSec-VPN 게이트웨이의 내부 모듈 구성은 IPSec 엔진, IKE 엔진, 접근제어 및 SSO 엔진으로 구성된다. 각각의 기능은 다음과 같다.

- **IPSec 엔진** : IPSec-VPN 클라이언트와 송/수신하는 IPSec 패킷에 대한 암/복호화를 수행한다.
- **IKE 엔진** : IPSec-VPN 클라이언트와의 IKE 프로토콜을 수행하여, 상호 인증 및 키 분배를 수행한다. IKE 프로토콜 수행 과정에서 IPSec-VPN 게이트웨이는 IPSec-VPN 클라이언트의 속성 인증서를 제출받아, 접근 제어 및 SSO 엔진에 전달하여, IPSec-VPN 클라이언트에 대한 접근제어 및 SSO을 수행할 수 있도록 한다.
- **접근 제어 및 SSO 엔진** : IKE 엔진으로부터 IPSec-VPN 클라이언트의 속성 인증서를 전달받고, 속성 인증서의 유효성을 검증하고,

```
attributes { -- SEQUENCE OF --
  { -- SEQUENCE --
    type {1 3 6 1 5 5 7 10 1},
    values { -- SET OF --
      svcAuthInfo { -- SEQUENCE --
        service dNSName
'6e65746c6162312e6b77616e67776f6f6e2e61632e6b72'H --
"netlab1.kwangwoon.ac.kr" --
        ident rfc822Name '6d686b616e67'H -- "mhkang" --
        authInfo octets
'b38a2776c66a8dbb988ed7f10e4567eda57f223c7'H -- "퀼V?똦댒
□.?~???랳IDM랳" --
      },

      svcAuthInfo { -- SEQUENCE --
        service dNSName
'6e65746c6162322e6b77616e67776f6f6e2e61632e6b72'H --
"netlab2.kwangwoon.ac.kr" --
        ident rfc822Name '6d686b616e67'H -- "mhkang" --
        authInfo octets
'b38a2776c66a8dbb988ed7f10e4567eda57f223c7'H -- "퀼V?똦댒
□.?~???랳IDM랳" --
      }
    }
  },

  { -- SEQUENCE --
    type {1 3 6 1 5 5 7 10 2},
    values { -- SET OF --
      accessIdentity { -- SEQUENCE --
        service dNSName
'6e65746c6162312e6b77616e67776f6f6e2e61632e6b72'H --
"netlab1.kwangwoon.ac.kr" --
        ident rfc822Name '6d686b616e67'H -- "mhkang" --
      },

      accessIdentity { -- SEQUENCE --
        service dNSName
'6e65746c6162322e6b77616e67776f6f6e2e61632e6b72'H --
"netlab2.kwangwoon.ac.kr" --
        ident rfc822Name '6d686b616e67'H -- "mhkang" --
      }
    }
  },

  { -- SEQUENCE --
    type {1 3 6 1 5 5 7 10 4},
    values { -- SET OF --
      group { -- SEQUENCE --
        values { -- SEQUENCE OF --
          octets '4e6574776f726b204c61626f726174f7279'H -- "Network
Security Laboratory" --
        }
      }
    }
  },

  { -- SEQUENCE --
    type {2 5 4 72},
    values { -- SET OF --
      role { -- SEQUENCE --
        roleName uniformResourceIdentifier
'61646d696e697374726174f72'H -- "administrator" --
      }
    }
  }
}
```

그림 3. 속성 인증서내의 속성 정보 예

속성 인증서 내의 속성 필드를 검색하여, 접근 제어 및 SSO 기능을 수행한다. 접근 제어 및 SSO 엔진의 내부 모듈 구조는 속성 인증서 검증 모듈, 접근제어 수행모듈, SSO 수행 모듈로 구성된다. 속성 인증서 검증 모듈은 제출

된 IPSec-VPN 클라이언트의 속성 인증서의 유효기간, 서명값, 공개키 인증서와의 연결성이 유효한지 검증하는 모듈이다. 접근제어 수행 모듈은 제출된 IPSec-VPN 클라이언트의 속성 인증서 내의 Group 속성 정보, Role 속성 정보를 검색하여, IPSec-VPN 게이트웨이의 보안 정책과의 일치 여부를 판단하는 모듈이다. SSO 수행 모듈은 속성 인증서 내의 Service Authentication Information 속성 정보와 Access Identity 속성 정보를 검색하여, IPSec 엔진에 전달하고, IPSec 엔진은 이들 정보를 이용하여 사용자 대신 응용 서버에 로그인을 수행할 수 있도록 한다.

3.2.1 사용자 접근제어 과정

본 논문에서 제안한 사용자 접근제어는 전자 서명 방식의 Main Mode/Aggressive Mode로 운영되는 IKE 교섭 과정에서 속성 인증서가 제출되고, 검증하는 과정을 통해서 이루어진다. 다음 그림 4는 전자 서명 방식의 Main Mode에서 접근제어가 이루어지는 과정을 나타낸 것이며, Aggressive Mode에서도 Initiator가 공개키 인증서를 전송할 때, 속성인증서도 같이 보내면, Main Mode와 동일하게 접근제어가 수행된다. 그림 4에서 사용되는 기호는 RFC 2409 IKE 표준에서 사용되는 기호를 사용하였다[3,6,7].

- HDR : ISAKMP의 헤더 정보이다.
- HDR* : HDR* 이후의 후속 데이터 Payload는 암호화 되어 전송됨을 의미한다.
- SA : SA(Secuirity Association) Payload로써, 개체인증방식, ISAKMP 메시지에서 사용할 암호 알고리즘, PRF 함수, SA의 Lifetime, Diffie-Hellman 계산에서 사용하는 그룹 등을 정의한다.
- KE : Key Exchange Payload로써, 키 분배를 위한 Diffie-Hellman Key Agreement를 위한 공개키 값을 나타낸다.
- Ni, Nr : Nonce Payload로써, Initiator, Responder에서 생성한 각각의 난수값이다.
- IDii, IDir : Identification Payload로써, SA를 맺고자 하는 Initiator의 ID(IDii)와 Responder의 ID(IDir)을 나타낸다.
- SIG_I, SIG_R : Initiator / Responder에서 각각 생성한 전자서명 값을 나타낸다.

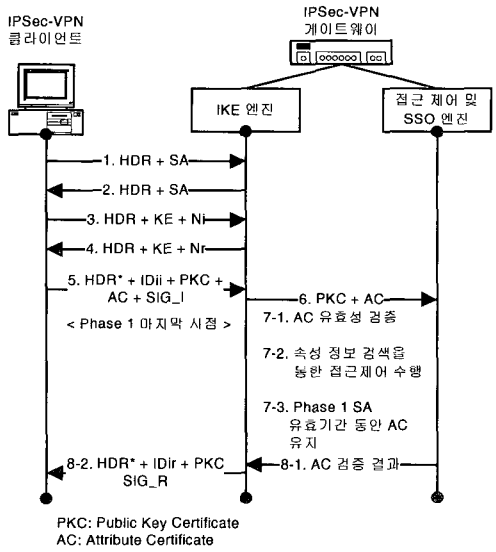

그림 4. IKE 교섭과정에서의 속성인증서 제출/검증 과정

1. IPSec-VPN 클라이언트는 IPSec-VPN 게이트웨이에 SA 정보를 헤더정보(HDR)와 함께 전송한다.
2. IPSec-VPN 게이트웨이는 IPSec-VPN 클라이언트에 SA 정보를 헤더정보(HDR)와 함께 전송한다.
3. IPSec-VPN 클라이언트는 IPSec-VPN 게이트웨이에 Diffie-Hellman 공개키 값(KE, 예 : g^x), 난수값(Ni)를 헤더정보(HDR)와 함께 전송한다.
4. IPSec-VPN 게이트웨이는 IPSec-VPN 클라이언트에 Diffie-Hellman 공개키 값(KE, 예 : g^y), 난수값(Nr)을 헤더정보(HDR)와 함께 전송한다.
5. IPSec-VPN 클라이언트는 IPSec-VPN 게이트웨이에 자신의 ID 정보(IDii), 공개키 인증서(PKC), 속성 인증서(AC), 서명값(SIG_I)을 Diffie-Hellman 교섭키(예 : g^{xy})를 이용하여, 암호화하여, 헤더정보(HDR)와 함께 전송한다.
6. IPSec-VPN 게이트웨이의 IKE 엔진은 Diffie-Hellman 교섭키를 이용하여, 헤더 다음의 본체 부분 정보들을 복호화 한후, IPSec-VPN 클라이언트의 서명값과 공개키 인증서를 검증한다. 서명값과 공개키 인증서가 유효하면, 공개키 인

증서(PKC), 속성 인증서(AC)를 접근제어 및 SSO 엔진에 전달한다.

7. IPSec-VPN 게이트웨이의 접근제어 및 SSO 엔진은 IKE 엔진으로부터 전달받은 IPSec-VPN 클라이언트의 공개키 인증서와 속성 인증서를 이용하여, 속성 인증서의 유효성을 검증한다. 속성 인증서의 서명값, 유효기간, 공개키 인증서와의 연결 등이 유효하면, IPSec-VPN 클라이언트의 속성인증서 내부의 Group 속성 정보, Role 속성 정보가 있을 경우에는 이들 속성 정보를 검색하여, IPSec-VPN 게이트웨이의 보안 정책에 일치 여부를 판단한다. 보안 정책과 일치하면, 해당 IPSec-VPN 클라이언트와의 Phase 1 SA 유효기간 동안 해당 속성 인증서의 상태 정보를 유지한다.
8. 접근 제어 및 SSO 엔진은 IPSec-VPN 클라이언트의 속성 인증서의 검증 결과를 IKE 엔진에 전달하고, 속성인증서가 유효하면, IPSec-VPN 클라이언트에 자신의 ID 정보(IDir), 공개키 인증서(PKC), 서명값(SIG_R)을 Diffie-Hellman 교섭키를 이용하여, 암호화하여, 헤더 정보(HDR)와 함께 IPSec-VPN 클라이언트에 전송한다. IPSec-VPN 클라이언트는 Diffie-Hellman 교섭키를 이용하여, 헤더 다음의 본체 부분 정보들을 복호화 한후, IPSec-VPN 게이트웨이의 서명값과 공개키 인증서를 검증한다. 서명값과 공개키 인증서가 유효하면, 비로소 IKE Phase 1 교섭이 이루어지는 것이다.

3.2.2 SSO 수행 과정

IKE Phase 1, Phase 2 교섭이 성공적으로 이루어지고 나면, IPSec 통신을 수행하게 되는데, 이 시점에서 접근제어 및 SSO 엔진에서는 속성 인증서의 Service Authentication Information, Access Identity 속성 정보를 이용하여, 응용 서버에 접속하는 SSO 기능을 수행한다. IPSec-VPN 게이트웨이는 Service Authentication Information, Access Identity 속성 필드를 검색하여, 해당 응용 서버 접근에 필요한 ID/Password 정보를 얻은 후, 해당 응용서버에 접속을 시도한다. 이때, 암호화된 Password 정보 등은 IPSec-VPN 게이트웨이의 비밀키로 복호화한 후, 해당 응용서버에 접속을 시도한다. 다음 그림 5는 IPSec-VPN 게이트웨이가 IPSec-VPN 클라이언트와 응용 서버에 사이에 위

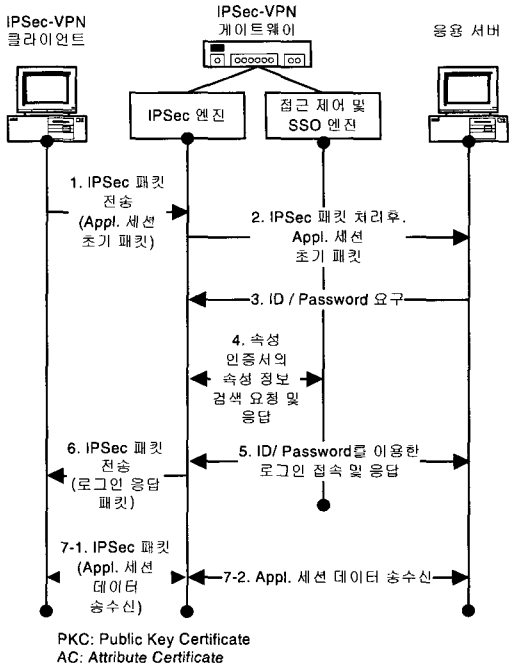

그림 5. SSO 수행 과정

치하여, IPSec 통신 단계에서의 SSO 기능이 수행되는 과정을 나타낸 것이다.

1. IPSec-VPN 클라이언트는 응용 세션 초기 패킷을 IPSec 패킷화 하여, IPSec-VPN 게이트웨이에 전송한다.
2. IPSec-VPN 게이트웨이의 IPSec 엔진에서는 암호화된 IPSec 패킷을 복호화 처리 후, 응용 세션 초기 패킷을 응용 서버에 전달한다.
3. 응용 서버는 IPSec 엔진에 로그인을 위해 ID/Password 정보를 요구한다.
4. IPSec 엔진은 접근제어 및 SSO 엔진에 해당 IPSec-VPN 클라이언트의 속성 인증서의 속성 정보 검색 요청 및 응답 메시지를 통하여 해당 응용 서버에 대한 ID/Password 정보를 습득한다.
5. 습득된 ID/Password를 이용하여, IPSec 엔진은 해당 응용 서버에 로그인을 하고, 그에 대한 응답 패킷을 응용 서버로부터 수신한다.
6. IPSec 엔진은 응용 서버로부터 수신한 로그인 응답 패킷을 IPSec 패킷으로 암호화하여, IPSec-VPN 클라이언트에 전송한다.
7. IPSec-VPN 클라이언트와 게이트웨이 사이에

서 실제 응용의 세션 데이터 패킷을 IPSec 암/복호화 통신을 수행하여, 사용자는 해당 응용 서버와의 안전한 서비스를 제공 받는다.

Ⅳ. 시스템 설계

4.1. 시스템 구현

본 논문에서는 IPSec-VPN 게이트웨이의 IPSec 엔진, IKE 엔진은 Linux Redhat 9.0에서 Free S/WAN 공개 소프트웨어를 기반으로 하는 것을 가정하였으며, 접근 제어 및 SSO 엔진은 Linux 환경에서의 데몬 형태로 구현하여, IKE엔진, IPSec 엔진과는 TCP/IP 로컬 소켓 통신을 수행할 수 있도록 하였다. IPSec-VPN 관리시스템의 공개키 인증서 및 속성 인증서를 생성 부분은 윈도 환경의 DLL 형태로 구현하였다. 또한 공개키 인증서, 속성 인증서의 생성 및 검증, 세부 필드 검색 등의 구현을 용이하게 하기 위한 공개 소프트웨어인 SNACC ASN.1 도구를 이용하였다. 다음 그림 7은 SNACC ASN.1 도구를 이용한 접근 제어 및 SSO 엔진의 구현 구조를 나타낸 것이다. 본 논문에서 공개키 인증서 및 속성 인증서 생성, 검증 과정에서 필요한 암호 관련 알고리즘은 RSA(1024키), SHA1, AES를 사용하였다. 다음 그림 8은 IPSec-VPN 클라이언트의 속성 인증서를 나타낸 것이며, 속성 인증서 보기 프로그램은 별도로 윈도환경에서 MS-Visual C++ 도구를 이용하여 구현하였다.

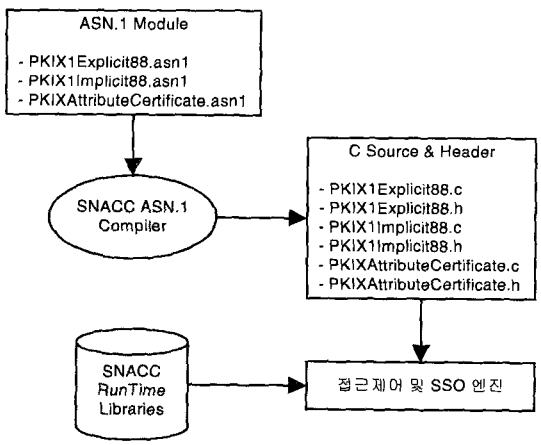

그림 7. SNACC ASN.1 도구를 이용한 접근 제어 및 SSO 엔진 구현 구조

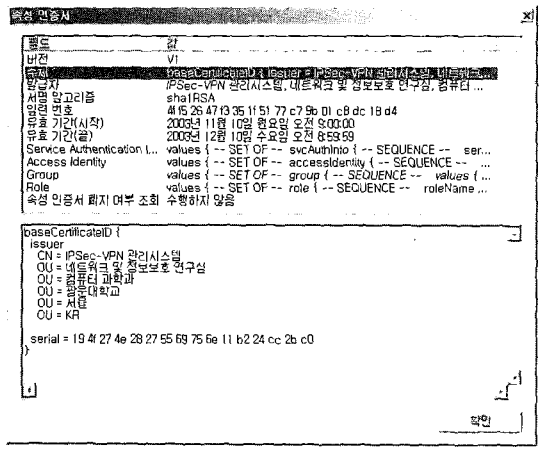

그림 8. IPSec-VPN 클라이언트의 속성 인증서

4.2. 시스템 분석

다음 표 2는 본 논문에서 제안한 속성 인증서를 이용한 접근 제어 방안과 국내의 공인 인증서의 식별번호를 이용한 접근 제어 방법을 비교 분석한 것이다[10-12].

공인 인증서의 식별번호를 이용하는 방법은 자연인의 식별번호(예 : 주민등록번호)를 기반으로 접근 제어를 수행하기 때문에, 자연인을 대상으로 하는 응용에서의 접근제어가 보다 유리한 측면이 있으나, IPSec-VPN과 같은 시스템 개체에는 식별번호가 없다. 통상, IPSec-VPN 시스템 관리자의 식별번호(예 : 주민등록번호) 등을 이용하여 공인 인증서를 발급 받아 사용하는 방안을 고려해볼 수 있으나 관리

표 2. 공인 인증서를 이용한 접근제어 방법과의 비교

공인 인증서의 식별번호를 이용한 접근제어 방법	속성 인증서를 이용한 접근제어 방법
자연인을 대상으로 하는 응용에 적합	IPSec-VPN과 같이 시스템을 대상으로 하는 응용에 적합
식별정보를 이용한 임의적 접근제어 수행	임의적 접근제어, 역할기반 접근제어 등의 섬세한 접근 제어 수행 가능
접근제어 정보(식별번호 또는 식별번호의 해쉬코드) 유지 및 질의 문제 야기	속성인증서의 유효성 검증 및 속성 정보와 보안 정책 정보 검색만으로 접근제어 수행
표준 ISAKMP/IKE 프로토콜의 수정 필요	표준 ISAKMP/IKE 프로토콜의 수정 불필요

자가 여러 대의 IPSec-VPN 시스템을 관리하는 경우에는 인증 및 접근제어에 문제점이 발생하므로, 공인 인증체계에 IPSec-VPN 시스템을 위한 별도의 ID 체계가 요구되고, ID 정보를 IKE 교섭 프로토콜 상에서 IPSec-VPN 게이트웨이에 전달하는 것이 용이하지 않다. 또한 속성 인증서의 유효기간은 1달 또는 1주일 정도로 공인 인증서와 비교하여 상당히 짧기 때문에 사용자의 신분 변동(예 : 소속 변경)이 발생할 경우에 공인 인증서를 사용하는 경우와 비교하여 보다 유리한 측면이 있다.

공인 인증서를 이용하는 방법은 단순한 식별정보 확인 과정을 통한 임의적 접근제어 만을 수행할 수 있는 반면에, 속성 인증서를 이용한 방법은 임의적 접근제어 방법 및 역할 기반 접근 제어 등의 섬세한 접근 제어를 수행할 수 있다.

공인 인증서를 이용하는 방법에서는 제출된 공인 인증서와 연관되는 접근제어 정보(식별번호 또는 식별번호의 해쉬코드)를 유지, 관리하여야만 접근 제어를 수행할 수 있다[10,11,12]. IPSec-VPN 관리 시스템에서 접근제어 정보를 유지, 관리하는 경우에는 IPSec-VPN 게이트웨이가 IKE 교섭과정에서 항상 IPSec-VPN 관리 시스템에 공인 인증서와 연관되는 접근 제어 정보를 질의하여야 하는 오버헤드가 있다. 개별적으로 모든 IPSec-VPN 게이트웨이에 접근 제어 정보를 유지하는 방법 또한 저장 공간 및 관리 문제와 더불어 확장성 측면에서 많은 문제점이 야기된다. 반면, 속성 인증서를 이용한 방법은 IPSec-VPN 게이트웨이에서는 보안 정책 정보와 IPSec-VPN 관리 시스템의 공개키 인증서만을 유지하면서, 제출된 속성 인증서의 유효성을 검증하고 속성 정보를 검색하여 접근 제어를 수행하므로, IKE 교섭과정에서 매번 IPSec-VPN 관리 시스템에 질의하여야 하는 부담도 없으며, 확장성 측면에서도 공인 인증서를 이용하는 방법 보다 우수하다고 볼 수 있다.

표준 ISAKMP/IKE 프로토콜에서는 공인 인증서의 식별번호를 이용한 접근제어 과정에서 전송되는 공인 인증서 이외의 ID 정보, 난수 정보, ID 정보와 난수정보의 해쉬코드 정보 등을 전송하기 위해서, ISAKMP/IKE 프로토콜의 수정이 필요하지만, 속성 인증서를 이용한 방법은 표준 ISAKMP/IKE 프로토콜에서는 이미 AC Payload가 이미 정의되어 있기 때문에, 표준 ISAKMP/IKE 프로토콜을 수정할 필요가 없어, 기존의 IPSec-VPN 시스템과의 상호 호환성을 보장할 수 있다.

V. 결 론

본 논문에서는 Client-to-Gateway 형태의 IPSec-VPN 시스템에서의 효율적인 사용자 접근 제어를 지원할 수 있도록 제안하였으며, 시스템을 설계, 구현하였다. 본 논문에서 설계, 구현한 속성인증서를 이용한 사용자 접근 제어 방법은 기존의 ISAKMP/IKE 표준 프로토콜을 그대로 준용하면서, 사용자 접근 제어를 수행할 수 있으며, SSO (Single Sign-On) 기능을 수행할 수 있다. 또한 IPSec-VPN 시스템에서는 국내의 공인 인증서 내부의 식별번호 정보를 이용한 사용자 접근 제어 방법보다 여러 가지 장점을 가지고 있다고 볼 수 있다.

참 고 문 헌

[1] American National Standard for Financial Services X9.45, "Enhanced Management Controls Using Digital Signatures and Attribute Certificates", February 1999.

[2] S. Farrell and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002. available on line at http://www.ietf.org/rfc/rfc3281.txt.

[3] D. Harkins and D.Carrel, "The Internet Key Exchange", RFC 2409, November 1998. available on line at http://www.ietf.org/rfc/rfc2409.txt

[4] ITU-T Recommendation X.208, "Specification of Abstract Syntax Notation One (ASN.1)", 1988.

[5] ITU-T Recommendation X.209, "Specification of Basic Encoding Rules for Abstract Syntax Notation One(ASN.1)", 1988.

[6] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998. available on line at http://www.ietf.org/rfc/rfc2401.txt

[7] D. Maughan, M. Schertler, M. Schneider and J. Turner, "Internet Security

Association and Key Management Protocol", RFC 2408, November 1998. available on line at http://www.ietf.org/rfc/rfc2408.txt
[8] Joon S. Park and Ravi Sandhu, "Binding Identities and Attributes Using Digitally Signed Certificates", IEEE Communication Magazine, September, 2000.
[9] Michael Sample, "Snacc 1.2rj : A High Performance ASN.1 to C/C++/IDL Compiler", July, 1993.
[10] 박종욱, 윤재호, 김승주, 이재일, 이홍섭, 박상준, "X.509 인증서내 식별번호를 이용한 본인 확인 메커니즘", 제 13회 통신 정보 합동 학술대회, April 2003.
[11] 박종욱, 김승주, 이재일, 이홍섭, "X.509 인증서내 식별번호를 이용한 본인 확인기술 표준화 동향", 한국정보보호학회 학회지 제 14권 2호, April 2004.
[12] 한국정보보호진흥원, "식별번호를 이용한 본인확인 기술규격 v.1.11", September 2002.

〈著者紹介〉

강 명 희 (Myung-hee Kang) 정회원
1996년 2월 : 광운대학교 컴퓨터 과학과 석사
1996년 2월~1998년 5월 : 백두정보기술/주 EP&C팀 주임연구원
1998년 6월~현재 : (주) 퓨쳐시스템 암호체계센터 선임연구원
2001년 8월~현재 : 광운대학교 컴퓨터과학과 박사과정
〈관심분야〉 무선 네트워크 보안, 유비쿼터스 보안

유 황 빈 (Hwang-bin Ryou) 정회원
1989년 2월 : 경희대학교 대학원 전자공학과 졸업(박사)
1981년 2월~현재 : 광운대학교 컴퓨터공학부 교수
2004년~현재 : 한국정보보호학회 비상임 부회장
〈관심분야〉 네트워크 보안, 유비쿼터스 정보보호