인증서를 이용한 정보 보호 서비스 시스템

남보현(*), 채송화(**), 김동규(**)
(*)한국컴퓨터㈜, (**)아주대학교 컴퓨터공학과

Security Service System Using Certificate

Bo-hyun Nam(*), Song-hwa Chae(**), Dong-kyoo Kim(**)
(*)Korea Computer,Inc ,(**) Dept of Computer Engineering, Ajou University

요 약

기업이나 기관등이 인터넷을 사설망 대용으로 사용하는 것은 비용 절감 효과가 크다. 그러나 인터넷은 개방성으로 인해 많은 정보 보호의 취약점을 가지고 있다 따라서 인터넷을 사설망으로 사용하기 위해서는 안전한 하부구조(infrastructure)를 구성해야 한다. 본 논문에서는 인터넷 정보보호를 위한 요구사항과 인터넷상의 전자 ID로 통용되는 인증서에 대해 살펴보고 이를 바탕으로 인증서를 이용한 정보 보호 서비스 시스템의 구성요소를 제안한다

1. 서론

인터넷은 지구상에 현존하는 가장 크고 많이 이용되는 네트워크이다. 인터넷을 통한 통신은 별도의 통신망 시설의 추가 없이 전세계를 묶을 수 있는 가장 효과적인 정책이다 그러나, 사용자가 많으므로 그만큼 위협 요소 또한 많다. 이러한 이유로 인터넷을 통한 무역 혹은 상거래를 활발히 촉진 시키지 못하고 있다 현재 거의 대부분의 은행과 같은 금융 기관 혹은 정부 기관에서는 인터넷 보다는 자체 사설망을 선호하는 경향이 있다. 자체 사설망의 구축은 비용이 상당히 많이 드는 작업이다. 인터넷을 사설망 대용으로 사용하고 암호 장비(하드웨어 혹은 소프트웨어)를 이용하여 가상 사설망(Virtual Private Network)를 구축 한다면 비용 절감 효과는 크다 인터넷의 잠재력을 활용하기 위해 본 논문에서는 인터넷 상에서 전자 ID로 통용 될 수 있는 인증서(Certificate)를 관리하고, 인증기관(CA Certificate Authority)을 설립하고, 인증서를 이용한 응용 프로그램을 작성하기 위한 서비스를 제공하는 시스템에 관한 설계를 제안하고자 한다

2. 정보 보호 요구 사항

2.1 인터넷 정보 보호

인터넷은 최근 몇 년간 네트워크 장비 가격의 하락과 개방된 표준을 수용함으로써 급속히 성장하였다 그러나, 개방적환경을 가지고 있기 때문에 다양한 공격이 이루어질 수 있으며 그에 따른 보안대책을 세우는 일 또한 쉽지않다 또한 암복호화를 위해서 사용되는 키 방식이 공개키 방식과 기밀키 방식 모두가 사용되어야 한다 그러므로 개발되어지는 응용 프로그램이나 API는 이 두 키방식을 모두 지원해야 한다.

2.2 안전한 하부구조(infrastructure)의 요구 사항

인터넷 혹은 네트워크상의 안전한 통신을 위해서는 하부적으로 안전한 구조가 이루어져야 한다 이 절에서는 안전한 하부구조 구축을 위한 요구 사항을 살펴보도록 하겠다

- 인증 사용자에 대한 정확한 인증을 할 수 있어야 한다
- 기밀성: 통신에 있어서 통신 당사자 외의 제 3 자가 도청할 수 없도록 기밀성을 제공해야 한다
- 무결성. 통신을 함에 있어서 주고받은 데이터가 제 3 자에 의해 변조되지 않도록 해야 한다
- 부인 방지 통신을 통해 이루어지는 형태에는 전자상거래, 전자결제 등 돈과 관련되거나 서로 주고 받음이 중요하여야 하는 경우가 비일비재하다 따라서 통신 당사자가 통신 후 그 사실을 부인하지 못하도록 해야 한다

2.3 인증서

인터넷상에서 사용되는 공개키에 대한 신뢰성을 확보하기 위해서는 인증서라는 것이 필요하다 이러한 인증서는 암호학적으로는 개인 또는 어떠한 기관의 공개키를 증명하기 위한 것으로 믿을 수 있는 제 3 자에 의해 발급된다 인증서를 발급한 기관은 발급 뿐만 아니라 계속적으로 관리해야 한다 이러한 역할을 하는 기관을 CA(Certificate Authority)라고 한다 CA는 사용자의 요청에 의해 인증서를 발급하며 유효기간이 경과하면 인증서를 파기 또는 연장 한다 현재 인증서에 관련된 표준으로는 ITU-T 의 X.509 가 대표적이다[1]

3. 인증서

인증서는 ITU-T X.509 에서 그 형태가 정의 되어있다. 이러한 인증서는 ITU-T X.500 의 디렉토리 서비스를 이용하여 사용자가 손쉽게 검색할 수 있다 본 장에서는 인증서가 갖는 의미와 용도를 설명한다

3.1 인증서의 신뢰성

공개키를 신뢰함이란 공개키에 대한 전자 서명을 신뢰하는 것이다. 그러므로, 공개키를 보증선 기관의 신뢰성이 중요한 요소이다 인터넷에서 생각되어질 수 있는 신뢰성 구조는 크게 두 가지가 있다. 첫번째는 PGP(Pretty Good Privacy)에서 사용되는 방식과 같은 "Web of Trust" 방식이다[2] 이는 각각의 사용자가 어떠한 공개키에 대한 보증의 의미로 전자 서명을 하는 방식인데 그러한 공개키의 보증인들을 참조하여 각 개개인이 공개키에 대한 신뢰성 여부를 판단하는 것이다 이 방식은 소규모의 운영 형태에서 적합하나 대규모의 인터넷과 같은 네트워크에서는 신뢰성에 관한 판단이 어렵다. 두번째는 CA

와 같은 신뢰성 있는 제3자가 개인 또는 기관의 공개키에 전자 서명을 함으로써 그 공개키에 대한 신뢰성을 부여하는 방법이다. 이 방식은 대규모의 네트워크에서 공개키의 신뢰성을 검증하기 위해 적당하다. 또한, PGP와 같은 "Web of Trust' 방식에서처럼 여러 사람의 보증을 바탕으로 신뢰성을 검증할 필요 없이 CA의 전지서명만 검증을 하면 신뢰성을 확보할 수가 있다.

그러므로 인터넷과 같은 대규모의 네트워크에서는 CA를 두어 인증서를 발부하는 것이 효율적이다.

3.2 신뢰성 있는 공개키 분배 : 인증서

인증서는 개인이나 기관의 공개키를 확신하기 위한 정보다. 인증서는 다음과 같은 역할을 한다.

- 공개키를 사용자 이름에 바인딩한다.
- 무결성과 식별을 위하여 CA에 의해 전자서명 되어 진다.
- 시리얼 번호를 포함한다.
- 만료기간을 규정한다.
- 인증서 사용에 있어서의 정책을 참조한다.
- 그 밖의 유용한 정보를 제공한다.

인증서는 다음과 같은 정보들을 포함하고 있다.

- 인증서 소유자의 공개키
- 인증서 소유자의 이름 또는 소속 기관
- 키 만료일
- 인증서를 발급한 인증 기관의 이름
- 시리얼 번호
- 정책 정보
- CRL(Certificate Revocation List)의 위치에 관한 정보
- 인증 기관(CA)의 인증서의 시리얼 번호
- 옵션
- 위에 있는 모든 정보에 관한 전자 서명

인증서의 표준인 X.509의 구조를 살펴보면 다음과 같다.

Certificate format version
Certificate serial number
Signature algorithm identifier for CA
Issuer X.500 name
Validity period
Subject X.500 name
Subject public key information
Issuer unique identifier(V2,opt)
Subject unique identifier(V2,opt)
Extension(V3,opt)
CA signature

위와 같이 인증서에는 공개키를 신뢰성 있게 배포할 수 있는 요소들을 갖고 있다.

3.3 인증서의 용도

인증서는 크게 두 가지 용도로 사용된다. 첫번째, 세션키를 암호화하는데 사용된다. 두번째, 전자서명을 검증하기 위해서 사용된다. 이러한 분류는 용도에 있어서 분류이지 인증서의 형태가 다른 것은 아니다. 인터넷에서는 공개키와 기밀키 방식을 모두 사용한다. 공개키 방식은 세션키 분배를 위해서 사용이 되는 한편 전자서명의 검증(확인)을 위해 사용이 되기도 한다. 즉 암호 기능과 인증 기능을 모두 갖춘 것이 공개키이기 때문에 인증서는 위와 같이 두가지 용도로 분류되는 것이다.

4. 인증서 기반의 정보 보호 서비스 시스템

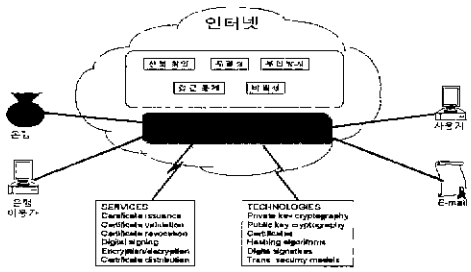
인증서는 공개키에 신뢰성 검증과 분배를 위한 효과적인 수단이다. 이러한 인증서를 바탕으로 인터넷 상에서 안전성을 확보할 수 있다. 본 장에서는 인증서 기반의 정보 보호 서비스 시스템을 고찰한다.

4.1 인증서 서비스

인터넷 응용 프로그램 개발자가 인증서를 이용한 안전한 시스템을 개발하기 위해서는 인증서의 기능을 제공하는 도구(Toolkit)가 있어야 한다. 이러한 도구는 다음과 같은 서비스를 제공하여야 한다.

- 신분확인 (Authentication)
- 접근통제 (Authorization)
- 비밀성 (Privacy)
- 무결성 (Integrity)
- 부인 방지 (Non-repudiation)

위의 서비스는 ISO-7498-2에서도 언급 되었다[3]. 위의 서비스를 바탕으로 인증서를 기반으로 제공 되어 지는 서비스와 이를 구현하기 위한 기술들은 다음 그림과 같다.

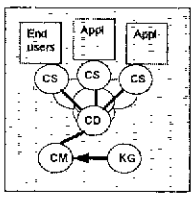


[그림 4-1] 인증서를 이용한 안전한 서비스

4.2 인증서 서비스를 위한 구성 요소 및 환경

인증서를 이용한 안전한 서비스를 제공하기 위해서는 다음과 같은 구성 요소들이 필요하다.

CM/KG	Certificate manager Key Generator
CD	Certificate directory
CS/Server	Certificate Service for application servers
CS/Client	Certificate Service for workstation/PCs



[그림 4-2] 인증서를 이용한 안전한 서비스를 위한 구성 요소

인증서를 이용한 안전한 서비스를 위한 구성 요소들을 살펴보면,

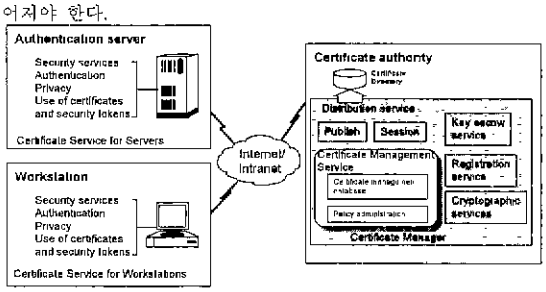
- Certificate Manager/Key Generator 인증서와 암호학적 키를 관리하는 소프트웨어이다. CM/KG는 인증서의 Life-Cycle을 관리한다. 이러한 Life-Cycle의 관리는 인증서의 등록, 발급 분배, 검증, 갱신, 파기, 그리고, 키 위탁 등의 관한 기능을 제공하는 것이다.
- Certificate Directory ITU-T X.500[4] 표준을 따르는 시스템으로 인증서의 체계적인 저장 뿐만 아니라 사용자와 관련된 정보(전자 우편 주소, 일반 주소, 전화 번호, 소속 기관 등)를 저장 하고 있어 사용자들이 쉽게 인증서를 획득 할 수 있는 서비스를 제공한다. 이러한 디렉토리 서비스를 제공 받기 위해서는

LDAP(Lightweight Directory Access Protocol)과 같은 디렉토리 접근 프로토콜을 이용하는 사용자 에이전트가 필요하다[5]

- Certificate Service for Application Server 응용 서버(예 FTP, HTTP 등의 서버) 프로그램에서 사용 되어지는 인증서 조작에 관련된 서비스를 제공한다. 예를 들어, 인증서의 요구 및 검증, 데이터의 암/복호화 등의 서비스를 제공한다 서비스의 제공 방법으로는 IDUP-GSS-API[6]와 GSS-API[7]를 이용한다
- Certificate Service for Application Workstation 개인 사용자가 응용 서버에 안전한 방식으로 접속하고 다른 사용자에게 자신의 인증서를 배포 하기 위한 서비스를 제공한다 서비스의 제공 방법으로는 IDUP-GSS-API 와 GSS-API 를 이용한다

인증서를 기반으로한 서비스를 제공 받기 위해서는 응용 서버와 응용 클라이언트(사용자) 프로그램이 위와 같은 구성 요소들을 이용하여 프로그래밍을 하여야 한다 다시 말해, 응용 프로그램을 위한 인증서 서비스를 위한 툴킷이 제공 되어지고 응용 프로그래머는 이 툴킷을 이용하여 프로그래밍을 한다

인증서 기반의 안전한 서비스는 [그림 4-3]과 같은 환경이 제공되어져야 한다.

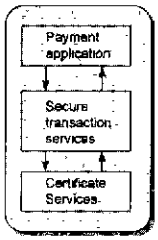


[그림 4-3] 인증시 서비스를 위한 환경

4.3 인증서 기반 정보 보호 서비스 제공

인터넷 상에서 인증서는 공개키의 분배와 검증의 역할을 한다. 이러한 인증서를 이용하여 전자 상거래등 다양한 응용 프로그램에 적용 될 수가 있다. 그러므로, 인증서를 기반으로 한 정보 보호 서비스는 다양한 표준을 수용하여야 한다.

STS(SET)	Secure transaction services for SET
STS(MOSS)	Secure transaction services for MOSS
STS(SMIME)	Secure transaction services for SMIME
STS(PGP)	Secure transaction services for PGP
STS(???)	Secure transaction services for future standard



[그림 4-4] 인증서를 기반으로 한 다양한 표준의 수용

이러한 다양한 표준을 지원하며 응용 프로그레미에게는 손쉬운 방법으로 서비스를 제공하여야 한다 응용 프로그래머에게 이러한 서비스를 제공 하기 위해서는 API(Application Programming Interface)를 라이브러리 형태로 제공하는 것이 가장 효과적인 방법이라 할 수 있다

정보 보호 서비스를 제공하기 위한 API는 또한 두가지 측면을 고려하여야 한다. 하나는 전자 우편과 같은 Store-and-forward 방식의 서비스의 제공이고, 두번째는 session-oriented 방식의 서비스이다

IETF 에서는 이와 같은 두가지 방식을 위한 정보 보호 서비스 인터페이스로 IDUP-GSS-API(Independent Data Unit Protection Generic Security Service API)와 GSS-API(Generic Security Service API)라는 두개의 API 를 표준으로 하고 있다 하지만, IDUP-GSS-API 의 경우는 현재 Internet-draft 상태이다

4.3.1 Store-and-forward 방식을 위한 정보 보호 서비스 API

전자 우편의 전송은 세션을 확립 않고 메일 박스에 긴자 우편을 저장해 두었다가 사용자가 편지를 갖고 가는 형태의 서비스이다 이러한 서비스에서는 세션의 개념이 없기 때문에 편지에 본문을 암호화한 키값을 안전하게 저장하여야 한다 또한 인증서를 첨부하여 편지를 보낸 사람의 신분을 확인하기 위한 전자서명 검증을 할 수 있어야 한다

IDUP-GSS-API 는 전자 우편 뿐만 아니라 개인 파일을 안전하게 저장해야 할 경우 역시 적용될 수 있다.

4.3.2 session-oriented 방식을 위한 정보 보호 서비스 API

TELNET 혹은 FTP 와 같은 인터넷 서비스는 세션을 기반으로 서비스를 제공한다 그러므로, 연결 확립 시 정보 보호를 위한 문맥(Context)를 확립하면 된다 이 문맥 안에는 인증서와 세션키를 포함하고 있다 이러한 서비스는 RFC1508 에서 GSS-API 이라는 이름으로 함수의 프로토타입과 기능이 정의 되어있다 또한, GSS-API 를 공개키 기반으로 구현 하기 위한 하부 메카니즘으로 SPKM(Simple Public Key Mechanism)[8]에 대한 표준이 Internet-draft 상태이다

5. 결론

인증서는 공개키의 신뢰성과 안전한 분배를 위한 수단으로 사용된다. 본 논문에서 제안한 인증서를 이용한 정보 보호 서비스 시스템은 정부 기관, 기업 등에서 각신이 직접 CA 가 되어 정보 보호를 위한 정책을 구성 하고 서비스를 하기 위해 설계된 시스템이다 즉, 각 기관, 기업 마다 정보 보호 정책이 다를 수 있으므로 각 기관에 필요한 요소를 구성할 수 있도록 기본적인 서비스를 대니져 콤포넌트와 API 로 제공 한다 인터넷의 속성상 공개키 방식과 기밀키 방식의 암호 시스템을 함께 사용하여야 하므로 인증서 기술은 인터넷 정보 보호 기술의 핵심이라 할 수 있다. 마지막으로 본 논문에서 제안된 시스템의 상세 설계와 구현을 향후 과제로 남겨둔다

참고 문헌

[1] ITU-T Recommandation X 509(1993) | ISO/IEC 9594-8 1993 Information technology – Open systems Interconnection – The Directory Authentication framework, 1993.

[2] Simson Garfinkel , PGP Pretty Good Privacy, O'Reilly & Associates,Inc,1995

[3] ISO 7498-2 Network Security System Architecture, 1989.

[4] ITU-T Recommandation X 500(1993) | ISO/IEC 9594-1 ,1993, Information technology – Open systems Interconnection – The Directory, Overview of Concepts, Models and Services, 1993

[5] W Yeong, T Howes & S Kille, Lightwegiht Directory Access Protocol(LDAP) Internet RFC 1777, 1995

[6] C. Adams, Independent Data Unit Protection Generic Security Service Application Program Interface(IDUP-GSS-API) . Internet Draft. 1997.

[7] J Linn Generic Security Service Application Program Interface. Version2 Internet RFC 2078 1997

[8] C Adams, The Simple Public-key GSS-Mechanism(SPKM) . Internet RFC 2025 1996