보안정보 통합관리 시스템의 설계

김주한, 문기영
ETRI 전자정부보안연구팀

A Design of Integration Management System for Security Information

Ju-Han Kim, Ki-Young Moon
ETRI E-Government Security Research Team

요 약

현재의 보안정보에 관리는 크게 공개키를 기반으로 공개키 쌍의 관리만이 표준화된 형식으로 사용되고 있을 뿐, 다양한 시스템들 및 사용자들이 필요한 대부분의 보안정보들은 시스템별 혹은 사용되는 보안 서비스들의 따라 달리 관리되고 있다. 본 논문에서는 여러 종류의 보안정보들을 통합 관리하는 보안 정보 통합 관리 시스템을 설계하였다.

1. 서론

최근에 인터넷은 모든 컴퓨터 사용자들이 매일 접하는 일종의 문화가 되어 가고 있다. 사용자들은 e-mail, 전자 상거래, 온라인 뱅크, 온라인 주식거래, 그룹웨어, 온라인 게임, 멀티미디어 서비스 같은 인터넷과 연결되어 사용되는 수 많은 응용 프로그램들을 이용한다.

이러한 응용 프로그램들은 다시 이용하는 PDA, 이동 전화 등의 무선 단말 및 기존의 유무선 단말 등의 미디어 및 환경이 따라 다시 다양하게 발전되어 가고 있다.

위의 다양한 응용 프로그램들, 다양한 환경 및 다양한 미디어에 따라 사용되는 대부분의 보안 서비스들은 각기 다른 형태의 보안 정보들은 요구한다. 응용 프로그램, 미디어 및 환경에 따라 사용할 수 있는 보안 서비스의 종류가 다르고, 또한 같은 보안 서비스라 하더라도 서로 다른 종류의 보안 정보들을 요구하는 경우가 대부분이다.

멀티미디어 서비스를 위해 필요한 보안 정보들의 경우를 보더라도, 해당 서비스들 제공하는 업체에서 사용자를 인증하기 위한 ID 및 패스워드가 일단 필요하며, 성인 멀티미디어 서비스의 경우에는 개인 정보도 필요하다. 또한, 지급 결제를 위한 보안 정보들이 필요하며, 경우에 따라서는 PKI가 사용자 인증으로 사용됨으로 공개키 쌍이 필요하다. 그리고, 멀티미디어의 암호화 전송을 위한 비밀키가 필요하며, 그룹 전송 시에는 그룹키도 필요하다. 여기에 무선 단말을 위한 서비스들을 제공한다고 하면, 무선 단말을 위한 인증 정보, 접근 제어 정보, 결제 정보, 비밀키, 그룹키 및 기타 보안 정보들이 다시 또 다른 형태로 요구된다. 대부분의 경우에 기존 유선에서 사용되는 보안 서비스들과 무선 단말에서 사용되는 보안 서비스들의 단말의 제한 때문에 다른 형태를 가지며,

요구하는 보안정보들의 형태가 다르다.

같은 목적을 가진 또 다른 업체라 하더라도 같은 보안 서비스들 사용하는 경우는 회사의 시스템, OS 환경 및 플랫폼에 따라 다양한 보안 서비스들과 보안 정보들을 요구하게 된다.

본 논문에서는 응용 프로그램, 미디어 및 환경에 따라 달라지는 수 많은 보안정보들을 효과적으로 관리하는 통합 보안 정보 관리 시스템에 대해 설계한다.

2. 관련연구

2.1 PKI

PKI(공개키 기반 구조)는 인터넷 상에서 사용자의 인증, 문서나 메시지의 무결성 등의 기능을 제공하는 대표적인 보안 서비스이다.

RA(등록소)에서 사용자를 등록하여 공개키쌍을 할당받아, 공개키를 디렉토리에 저장하고, CA(인증기관)를 통하여 인증서의 유효를 검증하고, 서명을 검증하는 절차 등으로 이용된다.

이에 관련된 보안 정보들은 개별 PKI 관련 제품들을 만든 회사에서 제공하는 관리 시스템을 사용한다.

2.2 XKMS

XKMS(XML 기반 키 관리 시스템)은 일종의 PKI 기반의 응용 프로그램이다. 대부분의 PKI 클라이언트는 복잡하고 무거운 프로토콜을 사용한다. XKMS는 클라이언트오 인증기관 사이에 XKMS 서버를 두어 복잡하고 무거웠던 프로토콜 대신에 XML 기반의 가볍고 편리한 프로토콜을 사용하는 시스템이다. 이 시스템 역시 개별 보안 정보 관리 시스템을 이용한다.

2.3 기타 보안 서비스들

문서나 메시지의 암복호에 관련된 보안 서비스, 인터넷 상의 자원에 대한 접근 제어에 대한 보안 서비스, 기본적인 사용자 인증 서비스인 ID, 패스워드 기반의 보안 서비스, 생체 정보를 위한 인증 서비스 등의 다양한 보안 서비스들이 있다.

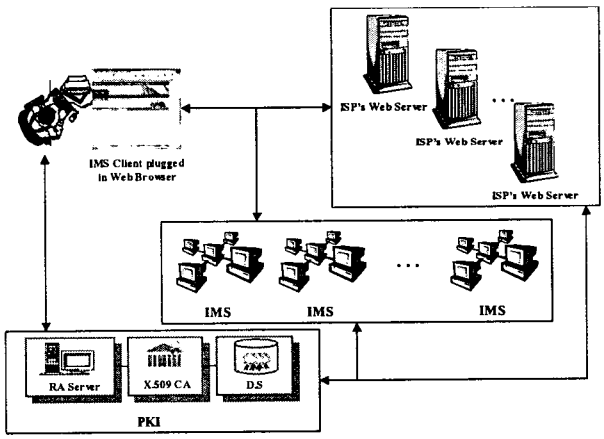
지금까지 이러한 보안 서비스들에서 필요한 보안 정보들의 관리는 각 보안 서비스를 제공하는 업체나 각 보안 서비스를 만든 업체의 관리 시스템 등을 이용하여 개별적으로 이루어져 왔다.

이상에서와 같이 대부분의 보안정보들은 개별적으로 관리되어 왔기 때문에, 사용자는 수 많은 보안정보들을 제대로 관리할 방법이 없으며, 업체의 경우에는 각 보안 서비스 및 보안 정보들을 관리하기 위한 부담을 가질 수 밖에 없었다. 따라서, 본 논문에서는 이러한 문제점을 해결하기 위해 보안정보 통합관리 시스템을 제안한다.

3. 보안정보 통합관리 시스템의 설계

3.1 개요

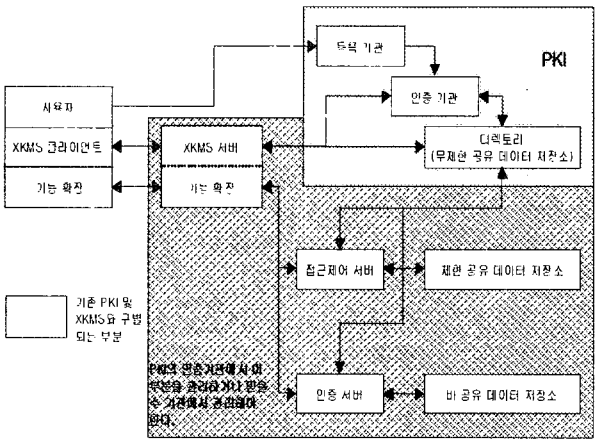
본 연구에서 설계하는 통합관리 시스템(IMS)은 인터넷 상에서 보안정보들만을 관리하는 별도의 시스템을 둔다. 이 시스템은 사용자 및 업체에서 관리하고자 하는 보안정보들을 받아 통합적으로 표준화된 방법으로 관리한다.



[그림 1] 보안정보 통합관리 시스템

3.2 시스템 내부 구조

본 논문에서 제안하는 시스템은 인터넷 상에서 사용하는 보안정보들을 XML 기반의 표준화된 방법으로 분류, 저장, 및 공유 설정/해제, 삭제, 및 수정 등의 관리를 하는 보안정보 통합관리 시스템이다. 또한, 관리되는 보안정보에 대한 접근을 위해 위치정보 제공하며, 인증 및 인가된 사용자 및 시스템에게 보안정보를 제공한다.



[그림 2] 보안정보 통합관리 시스템 구조

본 시스템은 XKMS를 확장하여 보안정보 관리 프로토콜에 사용된다. 즉, 기존의 XKMS는 공개키 쌍 관련한 키 관리를 위한 것이고, 이 시스템에서의 XKMS 확정 서버는 기존의 XKMS 서버를 확장하여 XML 기반으로 표시 가능한 모든 보안정보들을 대상으로 관리하는 프로토콜을 제공한다.

이 시스템은 크게 XKMS 확장 서버, 접근제어 서버, 인증 서버, 제한공유 데이터 저장소 및 비공유 데이터 저장소 등으로 구분된다. XKMS 확장 서버는 XKMS 확장 클라이언트에서 들어오는 요청들을 분석하여 어떤 보안정보에 관한 것인지 분석하여, 해당 보안정보들을 관리하는 접근제어 서버 혹은 인증 서버로 요청을 분산한다. 또한, 이 과정에서 사용자의 인증을 1차적으로 담당한다.

접근제어 서버는 공유가 제한적으로 가능한 보안정보들에 대한 관리를 하며, 이 정보들에 공유 설정/해제에 관한 접근제어 정책들을 사용자의 요청에 맞춰 자동적으로 생성/수정/삭제 등을 한다. 사용자는 자신이 가진 보안정보에 다른 사람이나 시스템 등에 접근 권한을 줄 수 있다. 접근 권한을 받은 사람은 접근제어 서버에서 인가를 받은 후에 보안정보를 접근할 수가 있다.

인증서버는 XKMS 확장서버에서 일차 인증된 사용자들의 비공유 데이터 저장소에 대한 접근을 허가하는 역할을 한다. 이 인증서버를 통해 관리되는 정보들은 통상적으로 아주 중요한 보안정보들이 대부분이다. 따라서, 인증서버에서는 XKMS 확장서버의 사용자 인증보다 강화된 인증을 한다.

제한공유 데이터 저장소는 통상적으로 일부 사람이나 그룹에게 공유 가능한 보안정보들을 저장한다. 비공유 데이터 저장소는 타인과 공유할 수 없는 보안정보들을 저장한다.

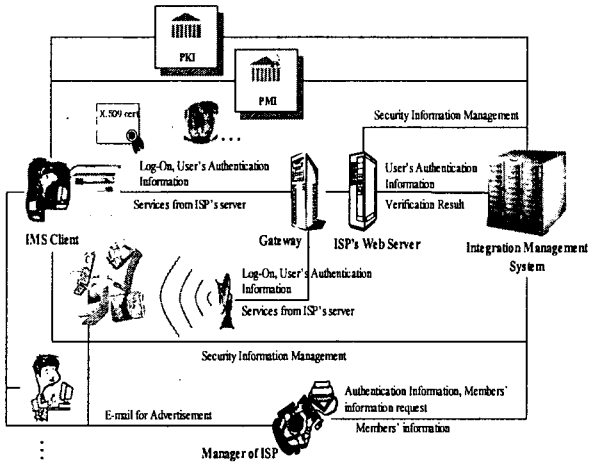
3.3 보안정보 종류

보안정보의 분류는 공유 성격으로 분류하면 세 가지 타입으로 분류할 수 있다. 인증서와 같이 모든 사람들에게 공유가 가능한 보안정보가 있다. 두번째 타입으로는 문서나 메시지를 암복호하기 위한 비밀키, 그룹전송을 위한 그룹키, 속성을 표시하는 속성 인증서, 가입된 인터넷 서비스 제공회사들에 제공하는 개인 정보, 기존의 ID 및 패스워드(개인과 회사간에 공유로 볼 수 있음), 등처럼 의도된 사람 및 그룹에 공유 가능한 제한공유 보안정보가 있다. 마지막으로 개인키와 생체정보 등의 공유가 불가능한 비공유 보안정보가 있다. 제한공유가 가능한 보안정보들은 이 시스템에서 제한공유 데이터 저장소에 저장되며 접근제어 서버를 통해 관리된다. 비공유 보안정보들은 비공유 데이터 저장소를 통해 저장되며 인증서버를 통해 관리된다.

3.4 시스템의 운용 및 활용

보안정보에도 중요도에 따라 구분되는 것처럼 본 시스템의 운용도 중요도에 따라 구분되어 지는

것이 필요하다. 생체정보같이 한번 노출되면 바꿀 수 없는 정보들은 정부나 정부가 주도하는 공인인증 기관에서 운영하는 것이 필요하다. 기타 업체에서 필요한 보안정보들에 관리는 업체가 현행 공인인증 기관을 확장하여 본 시스템까지 같이 운영하는 것이 바람직하다.



[그림 3] 시스템의 활용도

활용의 측면에서 보면 본 시스템은 다양한 환경 및 미디어에 상관없이 특성화된 통합정보 통합관리 시스템을 만들거나 혹은 기존의 시스템을 이용하여 쉽게 보안 서비스들을 구성할 수 있도록 하는 장점이 있다. 또한, 어떤 기관이나 단체에서 본 시스템을 운영을 하더라도, 요구되는 보안정보들을 프로토콜의 변경없이 그대로 적용할 수 있는 장점이 있으며, 새롭게 추가되는 보안정보들에 대해서도 변경없이 쉽게 추가할 수 있는 장점이 있다.

4. 결론

본 논문에서 설계한 보안정보 통합관리 시스템은 인터넷 상에서 사용되는 보안정보들을 분류하여 특성에 맞게 관리하며, 필요한 때에, 필요한 곳에 필요한 보안정보를 제공할 수 있는 장점을 갖는다. 사용자의 입장에서는 수 많은 보안정보들을 편히 관리할 수 있으며, 불필요한 보안정보 관련된 입력 및 관리를 줄일 수 있다. 업체의 입장에서는 기존의 보안 서비스 및 보안정보 관리에 들어가는 비용 및 노력을 줄일 수 있다. 정부의 입장에서도 전자 정부 등에 들어가는 국민의 중요한 보안정보들을 보호할 수 있고, 전자정부등에 응용하면 다양한 미디어 및 환경에서 전자정부를 사용할 수 있도록 하는 보안적인 토대를 마련할 수 있다.

[참고문헌]

[1] XML Key Management(XKMS2.0) Requirement(W3C Not), May-2003.

[2] XML Key Management Specification Version 2.0 (W3C Working Draft), April-2003.

[3] OASIS, "Web Services Security (WS-Security) Version 1.0,http://www-106.ibm.com/developerworks/library /Ws-secure/, Apr. 2002

[4] OASIS, "OASIS extensible Access Control Markup Language (XACML) Working Draft 14, http://www.oasis-open.org/committees/xacml/docs/, Jun. 2002

[5] OASIS, "Security Assertion Markup Language, http://www.oasis-open.org/committees/security/, Jan. 2003

[6] W3C, "The Platform for Privacy Preferences 1.0 Specification.,http://www.w3.org/TR/P3P, Apr. 2002

[7] Takeshi Imamura, Blair Dillaway and Ed Simon, "XML Encryption Syntax and Processing", http:// www.w3.org/ TR/xmlenc-core/, 2002