공개키 기반의 단일인증 시스템 설계

강형자*, 채수환*, 유일선**

*한국항공대학교, 컴퓨터공학과

** 인터넷 씨큐리티

Design of A PKI-Based Single Sign-On System

Hyung-Ja Kang*, Soo-Hoan Chae*, Il-Sun You**

*Department of Computer Engineering, Hankuk Aviation University

** Internet Security

요 약

공개키 기반 기술의 인기와 웹 기반의 다양한 응용서비스는 기존 단일인증시스템에 대한 새로운 도전이 되었다. 본 논문에서는 단일인증의 편의성과 통합적인 사용자관리 이외에 공개키 기반 구조와의 연계를 통해 강력한 보안기능을 제공하는 단일인증 시스템을 제안한다. 제안된 시스템은 다양한 시스템 환경에 쉽게 적용 가능한 유연성 있는 구조를 가지며 X.509에서 제시된 PMI구조를 기반으로 설계되어서 이기종의 시스템으로 구성되는 분산환경에서 통합된 접근통제 기능을 제공한다.

I. 서론

인터넷사용자의 기하급수적인 증가와 이용확산으로 인하여 전자문서에 기반을 둔 온라인 전자거래가 증가하게 되었으며 그 결과 전자문서의 무결성, 부인방지, 거래자의 신원확인, 전송내용의 기밀성, 접근통제에 대한 보안문제점이 발생하였고 이와 같은 문제를 해결하기 위해 공개키 기반 구조가 제시되었다. 또한 웹 기반의 다양한 응용서비스가 등장함에 따라 기존의 환경과는 달리 접속하게 될 사이트가 증가하게 되었고, 사용자는 사이트별로 서로 다른 아이디(I.D.)와 패스워드를 기억하고 관리해야 하며 보안정책에 따라 패스워드의 최소길이와 형식을 제한 받고 자주 변경해야 하는 부담을 갖게 되었다.

따라서 공개키 기반 구조와의 연계를 통해 강력한 보안기능을 제공하며 다양한 웹 응용 시스템에 쉽게 적용 가능한 단일인증 시스템 개발에 대한 필요성이 제시되었으며 이를 위해 공개키 기반의 커버러스, SESAME, RSA Keon®, Netscape SuiteSpot, WDAI 등과 같은 연구가 이루어져 왔다[3][4][5][6][7][8].

본 논문에서는 다양한 환경을 고려한 유연성 있는 공개키 기반의 단일인증 시스템 SecureSSO를 제안한다. SecureSSO는 통합된 접근통제를 위해 X.509에서 제시된 PMI 기반구조를 지원하며 기밀성, 무결성, 사용자 부인방지, 사용자 사칭차단, PKC(Public Key Certificate)를 통한 사용자 인증 등 공개키 기반의 강력한 보안서비스를 제공한다.

II. PMI (Privilege Management Infrastructure)

PMI는 AC(Atribute Certificate)를 생성하거나 관리, 저장, 배포, 취소하는데 필요한 하드웨어, 소프트웨어, 사람, 정책과 절차의 집합이며 그림 1과 같이 구성된다[2].

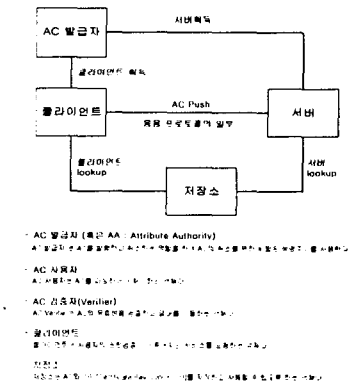

그림 1: PMI 구조

PKC와 AC와의 가장 큰 차이점은 다음과 같

다. PKC의 경우, identity는 공개키와 연결되지만 AC의 경우, 공개키를 갖고 있지 않고 대신에 identity는 속성정보(AC소유자의 소속그룹, 역할, 보안등급 등)와 연결된다.

접근통제 시스템에서 권한정보는 PKC의 확장필드에 저장하거나 혹은 분리된 AC에 저장되어질 수 있다. 그러나 권한정보를 PKC에 저장하는 방법은 권한 정보가 공개키쌍과 같은 생명주기를 갖지 않고 일반적으로 PKC 발급자가 응용서비스에 대한 권한정보 관리 자격을 갖지 못하기 때문에 바람직하지 않다.

그림 2는 AC의 구조를 나타낸다.

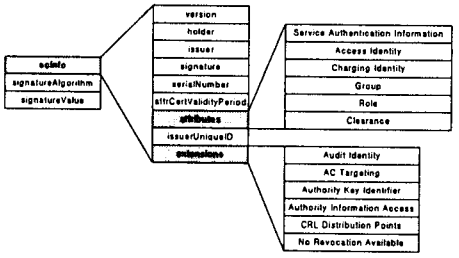

그림 2: AC 프로파일의 구조

III. SecureSSO

본 논문에서 제안하는 SecureSSO는 PMI 구조를 적용하여 공개키 기반의 단일인증 시스템이다.

1. PMI 기반구조

SecureSSO는 사용자의 권한정보를 제공하는 권한 인증서로서 AC를 선택하였고 AC의 생성 및 관리를 위해 PMI 구조를 기반으로 설계된다.

1) 권한서버(Privilege Server)

PKC는 CA가 발급하고 보증한 long-term 형태의 오프라인 인증티켓이므로 PKC를 기반으로 사용자와 응용서버사이에 인증이 이루어 질 때 PKC의 유효성을 증명하기 위한 중앙서버의 개입이 별도로 필요하지 않다. 따라서 SecureSSO는 사용자 인증보다는 사용자의 권한검증을 중앙에서 제어하는 PMI의 AC 발급자와 같은 권한 서버를 중심으로 설계된다.

2) 인증과 접근통제의 분리

SecureSSO는 인증과 접근통제를 분리하여서 앞서 언급하였던 PKC의 확장필드에 권한정보를 두는 방법의 문제점을 해결하고 또한 SESAME의 PAC과 같이 시스템내의 고유한 규격을 사용하기보다는 개방된 표준인 X.509 v2의 AC를 지원함으로써 상호 호환성과 확장성을 제공한다.

3) 인증과 접근통제의 분리

SecureSSO는 권한서버로부터 직접 AC를 받아서 응용서버에게 전송하는 On-Line, Push 모델이다. 그림 3은 PKC와 AC를 이용한 사용자 인증 및 접근통제의 과정을 나타낸다. 사용자는 응용서버에 있는 자원에 접근하기 위하여 PKC와 AC를 함께 응용서버에 제출한다. 이때 AC의 Holder는 baseCertificateID로 선택되며 이 값은 사용자가 AC와 함께 제시한 PKC의 issuer및 serial 값과 매칭 되어야 한다. 응용서버는 제출된 PKC를 통해 사용자를 인증하며 인증이 끝난 후, AC를 통해 권한검증을 한다. 단, 그림 4처럼 응용서버가 단일인증화 될 수 없는 Legacy 시스템을 위해 AC는 Attributes 필드의 Service Authentication Information Type을 이용해서 사용자의 인증 정보를 응용서버에게 제시할 수 있도록 한다.

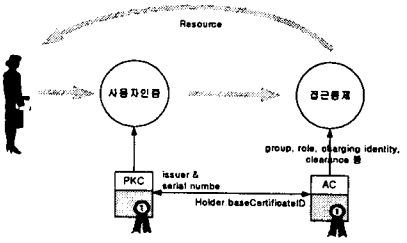

그림 3: 사용자 인증 및 접근통제

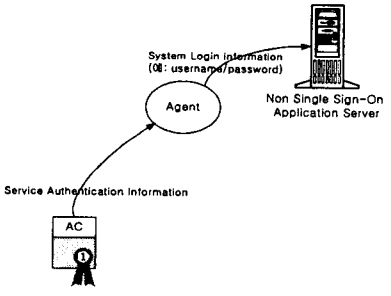

그림 4: Legacy 시스템 지원

4) 인증과 접근통제의 분리

SecureSSO에서 AC의 권한위임은 AC의 확장필드에서 정의된 id-pe-ac-proxying Type의 확장옵션을 사용하여 이루어진다. SecureSSO는 AC의 취소를 위해 특별한 메커니즘을 지원하지 않으며 대신 짧은 생명주기를 갖는 AC를 생성하는 정책을 적용한다. 이를 위해 'No Revocation Available' 확장옵션을 사용한다.

2. 구성요소 및 기능

제안된 SecureSSO의 구조는 그림 5와 같으며 접근 절차는 그림 6과 같다.

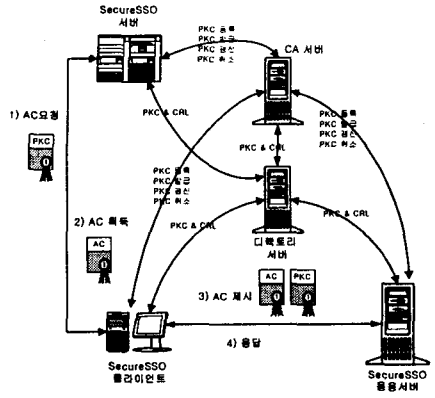

그림 5: SecureSSO의 구조

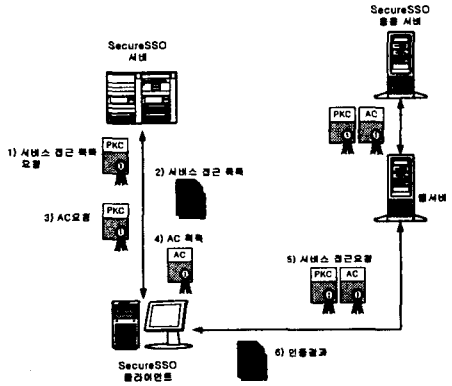

그림 6: SecureSSO의 접근절차

1) SecureSSO 서버

SecureSSO 서버는 사용자가 응용서버에 접속할 수 있도록 AC를 발급해 주는 역할을 한다.

2) SecureSSO 클라이언트

SecureSSO 클라이언트는 사용자의 개인키, PKC, AC등의 정보를 통해 사용자로 하여금 응용서비스를 제공받도록 하는 역할을 하며 이를 위해 사용자의 개인키로 생성된 전자서명과 PKC, AC를 SecureSSO 응용서버에게 제시한다.

3) SecureSSO 응용서버

SecureSSO 응용서버는 사용자의 PKC를 통해 사용자 인증을 수행한 후, AC를 통해 접근통제 결정을 하여 사용자 권한에 맞는 서비스를 제공하는 역할을 한다.

4) CA 서버 및 디렉토리 서버

CA 서버는 SecureSSO 시스템 내에서 사용되어 지는 PKC를 생성하고, 발급, 등록, 취소, 관리하는 역할을 하며 디렉토리 서버는 발급된 PKC와 생성된 인증서 취소목록을 저장하는 역할을 한다.

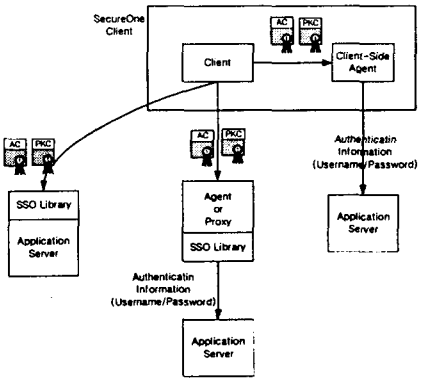

그림 7: SecureSSO의 단일인증 지원방법

3. 단일인증(SSO:Single Sign-On)

1) Legacy System 지원

SecureSSO는 Legacy 시스템에게 사용자의 적절한 인증정보를 제공하기 위해 사용자의 인증정보를 통합 관리하며 AC의 Service Authentication Information Attribute Type 항목을 통해 인증정보를 Legacy 시스템에 전달한다.

2) 유연성 있는 구조

SecureSSO는 단일인증 기능을 지원하기 위해 그림 7처럼 다양한 환경과 요구상황에도 적응할 수 있는 유연성 있는 구조를 갖는다. 그림 7의 세 가지 경우 이외에도 클라이언트 측면에서 클라이언트를 수정할 수 있는 경우와 수정할 수 없는 경우를 고려할 수 있다.

SecureSSO는 이 두 가지 경우를 위해 SecureSSO 라이브러리, 로그인 자동화, 클라이언트 프록시의 세 가지 기법을 지원한다.

IV. 인증 프로토콜 및 기존연구와의 비교

SecureSSO 구성요소간의 인증 프로토콜은 그림 8과 같고 인증 프로토콜의 기호는 표 1과 같다.

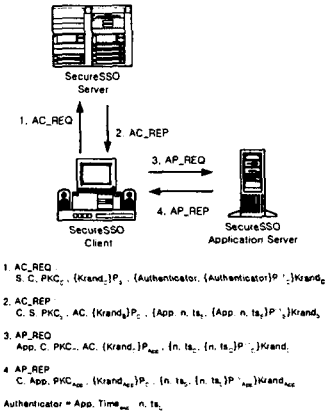

그림 8: SecureSSO의 구성요소간 인증프로토콜

표 1: 인증 프로토콜의 기호

기호	설명
S	SecureSSO 서버
C	SecureSSO 클라이언트
App	SecureSSO 응용서버
Krandx	SecureSSO의 구성요소 X (S, C, App)가 임의로 생성한 대칭키
Px	SecureSSO 구성요소 X (S, C, App)의 공개키
AC	Attribute Certificate
PKCx	SecureSSO 구성요소 X (S, C, App)의 PKC
$Time_{exp}$	SecureSSO 클라이언트가 요청하는 AC의 희망 종료시간
n	nonce
tsx	X에서 보낸 Time Stamp

표 2는 SecureSSO와 기존연구의 비교를 보이고 있으며 이를 통해 SecureSSO가 기존연구에 비해 우수함을 알 수 있다.

표 2: SecureSSO 시스템과 기존연구의 비교

비교항목	A	B	C	D	E	F
통합된 접근통제	○		○		○	○
PMI 기반구조	○					
PKC기반의 사용자 인증	○	○	○	○	○	○
초기인증생략	○			○		
상호인증	○	○	○	○	○	○
부인봉쇄	○	○	○	○		○
Legacy 시스템지원	○					○
유연성있는 SSO 구조	○					○
로그온 자동화 기능지원	○					
통합된 사용자관리 지원	○	○	○	○	○	○
A : SecureSSO, B : 커버리스 C : SESAME, D : SuiteSpot E : WDAI, F : RSA Keon®						

V. 결론 및 추후 연구방향

본 논문에서는 공개키 기반의 단일인증 시스템인 SecureSSO 시스템을 제안하였다. 제안된 SecureSSO는 사용자의 권한정보를 제공하는 권한 인증서로 X.509 v2인 AC를 선택하였고 AC의 생성 및 관리를 위해 PMI 구조를 기반으로 설계되었다. 또한 사용자의 권한검증을 중앙에서 제어하는 PMI의 AC 발급자 역할을 하는 권한서버를 중심으로 동작한다. SecureSSO는 PKC를 통한 사용자 인증, 기밀성, 무결성, 사용자 부인방지, 사용자 사칭차단 등 공개키 기반의 보안서비스를 제공하며 다양한 환경과 요구상황에도 적용할 수 있는 유연성 있는 구조를 갖는다.

추후 연구는 다양한 웹 환경의 Legacy 시스템에 적용 가능한 프록시 형태의 범용 에이전트를 설계하고, 엄격한 정책이 적용되거나 장기간의 오프라인 AC가 적용될 경우를 위해 효율적인 유효성 검증방안을 연구할 것이다.

Acknowledgements

본 논문은 과학기술부.한국과학재단 지정 경기도 지역협력연구센터(RRC)인 한국항공대학교 인터넷정보검색연구센터의 일부 지원에 의한 것입니다.

참고문헌

[1] A. Arsenault, S. Turner, "Internet X.509 Public Key Infrastructure," draft-ietf-pkix-

[2] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization," draft-ietf-pkix-ac509prof-05.txt, 2000.

[3] Jose Kahan, "WDAI : a simple World Wide Web distributed authorization infrastructure," http://decweb.ethz.ch/, 1999.

[4] RSA Security, "RSA Keon® Advanced PKI: A security architecture for enabling e-business solution white paper", http://www.rsasecurity.com/

[5] Netscape, "Single Sign-On Deployment Guide," http://developer.netscape.com/docs/manuals/security/SSO/contents.htm.

[6] M. Sirbu, J. Chuang. "Distributed Authentication in Kerberos Using Public Key Cryptography," Symposium On Network and Distributed System Security, 1997.

[7] B. Tung, C. Neuman, M. Hur, A. Medvinsky, S. Medvinsky, J. Wray, J. Trostle. "Public Key Cryptography for

Initial Authentication in Kerberos", Internet Draft, 1999.

[8] M. Vandenwauver, R. Govaerts, J. Vandewalle, "Overview of Authentication Protocols: Kerberos and SESAME", Pproceedings 31st Annual IEEE Carnahan Conference on Security Technology, pages 108-113, 1997.