KSIAM IT series Vol.10, No.1, 61-69, 2006

Single Sign-On을 이용한 인증 관리 기법에 관한 연구
(A Study on Authentication Management Technique Used of SSO)

최진탁
(Jin-Tak Choi)

요 약

SSO (Single Sign On), which allows users to have an access to a various systems through a single authentication, has been receiving much attention from many enterprises due to the user convience through a single authentication and the recent security features based on PKI. An emerging authentication management system called EAM has further enhanced the efficiency and stability of the enterprise IT infrastructrure systems. In this article, the basic concept and characteristics of the existing SSO sytems are analyzed and a new SSO model, based on PKI where authentication load is balanced via multiple circulators, is presented.

단 한 번의 인증으로 여러 시스템을 자유롭게 사용할 수 있는 SSO(Single Sign-On)기술은 단일 인증이라는 편이성과 최근 PKI기반의 강력한 보안 기능까지 갖추게 되어 기업에게 주목 받는 대상이 되었다. 최근에는 SSO기술을 기반으로 한 EAM이라는 권한관리 시스템이 등장하여 현재의 기업 IT 인프라 시스템의 효율성과 안정성을 증대시켰다. 본 논문에서는 SSO 기본 개념과 기존 SSO시스템의 특징을 분석하고, 다중 순환자를 통해 인증시 부하를 분산시킨 PKI 기반의 SSO 모델을 제안한다.

1. 서 론

기하급수적인 인터넷 사용자의 증가와 발전으로 우리는 업무나 일상생활에서 수많은 인터넷 서비스를 접하게 되었고, 이제 인터넷은 우리 생활의 필수 불가결적인 요소가 되었다. 그런데 이러한 여러 인터넷 서비스들은 사용자들의 개인 정보를 요구하고, 사용자가 이를 제공해주는 경우에만 아이디를 발급하여 필요한 정보들을 얻을 수 있게끔 하고 있다. 이와 같은 이유 때문에 사용자들은 그 수많은 서비스들 각각에 해당하는 자신의 인증 정보를 기

* "이 논문은 인천대학교 2003년도 자체연구비 지원에 의하여 연구되었음".
주제어: SSO, Single Sign-On

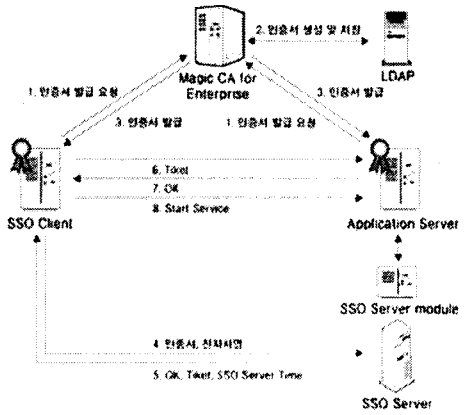
억해야만 하는 불편함을 가지고 있다. 그래서 어떤 사람은 아이디와 패스워드를 따로 관리하는 목록을 만들거나 아이디와 패스워드를 관리하는 소프트웨어를 사용하거나 모든 아이디와 패스워드를 하나로 통일에서 사용하는 사람도 있다. 그러나 이런 현상은 보안의 관점에서 보면 상당한 취약성을 가지고 있다. 서비스 업체들에 제공된 개인 정보들이 유출되어 악용되는 문제점을 가지고 있는 것이다. 만일 아이디와 패스워드의 목록이 다른 사람에게 노출된다면 그 사람이 사용하고 있는 모든 아이디와 패스워드를 변경해야 한다. 시스템의 아이디와 패스워드의 잦은 변경은 기업의 생산력을 떨어뜨리는 원인들이 되며 또한 보안상의 상당한 취약성을 가지고 있다. 이러한 보안상의 취약성과 생산력 저하를 극복하기 위해서 싱글사인온(Single Sign On, 이하 SSO)이란 개념이 나오게 되었다.

본 논문에서는 다중의 순환자를 두어 인증시의 부하를 분산시킨 PKI 기반의 SSO 모델을 제안하고, 모델의 성능을 평가한다.

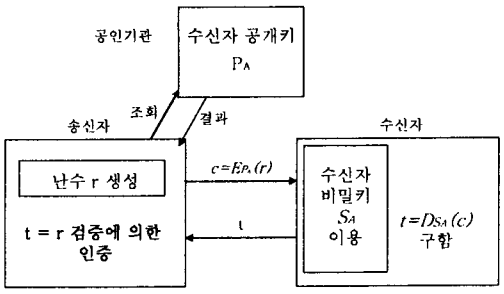
2. 관련 연구

2.1. SSO(Single Sign On)

SSO는 한번의 로그인을 통해 모든 서버에 접속할 수 있는 권한을 갖는 시스템이다. SSO 시스템을 도입하면 각각의 시스템마다의 인증 절차를 밟지 않고도 사용자에 부여된 1개의 계정만으로 다양한 시스템에 접근할 수 있어 사용자 편의가 대폭 높아지고, 관리자 입장에서도 인증정책의 변경이나 권한 설정이 수월해져 관리비용 및 수고를 크게 덜 수 있다.



〔그림 1〕 Single Sign On의 개념도



〔그림 2〕 공개키에 의한 상대 인증

2.2. SSO 구성요소

강력한 인증 기법을 이용한 SSO 시스템에는 인증서에 의한 인증 메커니즘, LDAP에 의한 접근제어 및 내부사용자 정보관리, 클라이언트와 서버 간의 데이터 암호화를 위한 통신보안 기술등이 필요하다.

2.2.1. 사용자 인증 메커니즘

공개키 기법에 의한 상대 인증은 각 이용자가 비밀로 보유하고 있는 비밀키와 그것에 대한 검증용 공개키가 있어야 이용자는 자기의 비밀 정보를 밝히는 것이 아니고, 검증자와 통신교환에 의해 공개키에 대응하는 비밀키를 갖고 있는 것을 증명하는 기법이다. 공개키 기법에 의한 상대 인증은 공개키 암호방식, 영지식 증명을 이용한 방식, 3교신 프로토콜, ID에 근거한 인증방식 등이 있으면 공개키 암호화 원리는 다음과 같다.

〔1〕 키생성 및 등록 : 이용자 A는 자신이 비밀로 관리하는 비밀키 SA와 공개키 PA의 쌍을 정해진 방법으로 생성한다. A는 PA를 공개키 디렉토리에 등록한다.

〔2〕 암호화 : 다른 이용자 B가 A에게 암호화 하는 경우를 생각한다. B는 공개키 디렉토리를 사용해 A의 공개키 PA를 검색한다. 다음으로 메시지 m을 PA를 사용하여 암호화 한다. 여기에서 암호문 c를 EPA(m)으로 표시한다.

$$c(\text{암호문}) = EPA(m) \tag{1}$$

〔3〕 복호화 : 암호문 c를 받은 A는 자신만이 알고 있는 비밀키 SA를 이용해 c로부터 m=DSA(c)를 복호한다. m=DSA(EPA(m))이 성립하는 것에 의해 복호가 행하여진다.

$$m(\text{평문}) = DSA(c) = DSA(EPA(m)) \tag{2}$$

또한 공개키를 이용한 상대 인증 방식은 그림 2의 절차와 같다.

〔1〕 공개키를 사용하는 모든 사용자는 공인된 기관에 자신의 공개키 PA를 등록해 둔다.

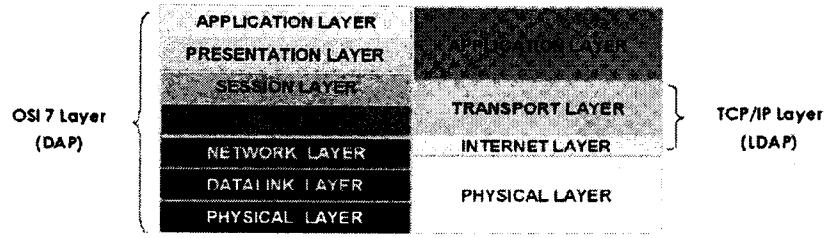
〔2〕 수신자는 난수 r을 생성해서 수신자의 공개키 PA를 이용하여 r을 암호화 한다. 그리고 암호문 c=EPA(r)을 이용자에게 보낸다.

〔3〕 수신자는 자신만이 아는 비밀키 SA를 이용하여 t=DSA(c)를 구함으로써 송신자를 인증하고, 다시 t를 자신의 키로 암호화하여 송신자에게 보낸다.

〔4〕 송신자는 t = r 인지 검증하고 성립하면 정당한 사용자로 인증한다.

2.3. LDAP(Lightweight Directory Access Protocol)

LDAP는 모든 형태의 디렉토리형 자료를 표준화된 방식으로 저장하고 검색하기 위한 통신 규약으로서 미국 미시간 대학에서 ITU-T의 X.500 을 근거로 개발되었다. LDAP은 X.500을 기반으로 개발된 통신 규약이며, X.500은 인터넷 사용이 가능한 곳이라면 전 세계 어디에서라도 이용이 가능하도록 나라, 기관, 사람, 기계 등과 같은 객체들을 관리하고 정보를 제공하는 디렉토리 서비스 표준이다.



〔그림 3〕 LDAP의 구조도

3. 기존의 SSO 시스템

3.1. 커버러스 구조

PKI 기반의 커버러스 구조는 기존의 대칭기 기반 구조에서 공개키 기반 구조로의 변환을 시도하면서 대칭키 기반의 구조에서 커다란 부담이었던 키관리 비용을 최소화하도록 하였고 공개키 기반 구조가 제공하는 강력한 보안서비스를 적용하고자 하였다. 특히 PKINT은 인증서를 사용하여 KDC에 초기인증을 할 수 있는 방안을 제시하였고 PKDA는 중앙의 인증서버인 KDC의 개입없이 직접 클라이언트와 서버사이에서 이루어 지는 인증프로토콜을 제시하여 사용자인증의 부담을 분산화했다. 그러나 PKI기반의 커버러스 구조는 기존의 프로토골과 호환성을 유지하기 위하여 불필요한 절차를 제거하지 못하거나 여전히 대칭키를 공유하는 등 대칭키 기반 구조의 한계성을 극복하지 못하였다.

3.2. SESAME

SESAME는 기존 커버러스 구조를 유지하면서 권한 서버를 통해 대규모의 분산된 이기종 환경에서 역할기반의 통합된 접근통제 기능을 제공한다 또한 공개키 기반 구조를 적용하여 초기인증이 보다 강화되었고 응용 시스템 서버의 키관리 부담을 줄였다 그러나 SESAME는 공개키 기반 기술을 적용함에도 불구하고 PKI기반의 커버러스처럼 대칭키 기반 구조의 한계를 벗어나지 못하였고 접근통제를 위해 를 추가함으로써 구조가 복잡해지는 문제점을 갖게 되었다. 또한 Legacy 시스템의 SSO를 위한 확장성있는 구조를 고려하지 않았다.

3.3. RSAKeon

RSAKeon은 사용자의 권한정보를 PKC(X.509 v3의 인증서)의 확장필드에 저장하는 구조를 갖는 PAC을 통해 사용자인증 아니라 중앙에서의 통합적인 접근통제가 가능하도록 하였으며 PAC 기법을 적용하여서 Legacy 시스템에 대한 확장성있는 구조를 제시하였다. 또한 커버러스나 SESAME 처럼 불필요한 대칭키 기반의 구조를 갖고 있지 않고 구조가 SESAME에 비해 단순하다. 그러나 RSA Keon은 응용 시스템 서버 측에 에이전트가 가능하지 않을 경우에 대한 확장성을 고려하지 못하였고 사용자의 공개키 정보와 권한정보를

함께 갖는 PAC을 새로운 접속요구가 있을 때마다 온라인으로 발급해야 하기 때문에 PAC을 발급할 때마다 공개키 쌍을 생성해야하는 부가적 비용이 존재한다.

3.4. SuitSpot

SuitSpot은 PKDA처럼 인증서버의 개입없이 클라이언트와 응용 시스템 서버와의 인증이 가능하도록 하는 비교적 단순한 구조를 제시하였다. 그러나 통합적인 접근통제를 고려하지 않았고 Legacy시스템의 SSO를 위한 확장성 있는 구조를 고려하지 않았다.

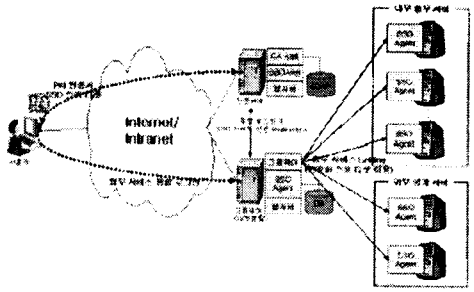
〈표 1〉 SSO 시스템 비교

비교항목	Kerberos	SESAME	RSAKeon	SuiteSpot
통합된 접근통제		O	O	
PKC기반의 사용자 인증	O	O	O	O
초기인증 생략				O
상호 인증	O	O	O	O
부인 봉쇄	O	O	O	O
Legacy시스템 지원			O	
유연성 있는 SSO구조			O	
통합된 사용자 관리 지원	O	O	O	O
주문형 인터페이스			O	

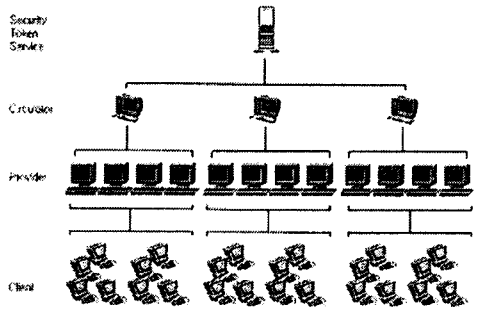
4. 제안 시스템

4.1. PKI기반의 동적 토큰 SSO

동적 토큰 SSO는 중앙에 하나의 순환자가 클라이언트의 첫 접속시 클라이언트의 인증 및 순서가 토큰 발행하고 그것을 저장하고 클라이언트가 공급자를 통해 토큰을 서명과 함께 제시하면 해당 토큰의 다음을 예측할 수 있는, 인증서 발행 및 검증 알고리즘보다 훨씬 계산이 빠르고 간소한 해쉬 알고리즘을 공급자에게 전달함으로써 이후에 클라이언트 인증을 공급자 수준에서 검증하게 하여 순환자와 공급자 간의 네트워크 트래픽을 최소화하였다. 그러나 순환자가 중앙에 하나이므로 많은 수의 공급자와 클라이언트와 함께 시스템을 구성할 경우 인증서 저장, 검증 그리고 토큰 발행, 저장, 최근 사용한 토큰을 공급자로부터 수집 및 배분하는 등의 부하가 동시에 커질 것을 쉽게 예측할 수 있다.



〔그림 4〕 PKI기반 동적 토큰 SSO 개념도



〔그림 5〕 실험 시스템 구성도

이를 해결하기 위해 순환자를 여러 대를 두되 클라이언트 첫 인증 이후 순환자가 토큰 수집을 위해 공급자와의 연결이 많으므로 되도록 공급자에 가까운 곳에 배치한다. 또한 공급자는 하나의 순환자와 통신하도록 한다.

가장 최근에 사용한 토큰이 해당 순환자에게서 발견되지 않으면 다른 순환자에 질의를 한다. 타 서버에서 발견 시 이를 해당 순환자도 복사하여 저장하고 해당 공급자에게 이를 넘긴다.

아래 조건들은 제안하는 SSO 시스템을 충족시키기 위한 보안 요건들이다.

1) 내부 업무 서비스의 접근은 기존 그룹웨어 포탈을 통해서만 접속토록 한다.

2) 인트라넷 및 인터넷을 통해 그룹웨어 포탈에 대한 로그인은 암호화 기능을 적용한다.

3) 그룹웨어 포탈 접속 후 그룹웨어 포탈에서 제공하는 타 업무 서비스 접속 Linking 시 사용자 ID 정보는 암호화한다.

본 제안한 다중 순환자 아키텍쳐는 공급자와 클라이언트 사이에 프락시를 두었던 시스템과 비교하여 동적 토큰 SSO가 우위였던 것에 착안하여 여러 대의 공급자를 프락시 개념의 순환자를 도입하였다.

5. 평가 및 결과

제안한 다중 순환자를 이용한 동적 토큰 SSO 시스템의 효율성 확인을 위해 단일 순환자를 두었을 경우와의 성능을 비교하는 시뮬레이션을 수행하였다.

5.1. 실험 시스템 구성도

실험 시스템을 구성하는 구성요소로는 인증서를 발행하는 보안토큰서비스, 토큰을 발행 및 관리하는 순환자, 서비스를 동급하는 공급자, 서비스를 사용하는 사용자로 구성이 되며 그림5와 같다.

5.2. 실험 절차

먼저 시스템을 구성하는 클라이언트, 공급자, 순환자, 보안토큰 서비스들 간에 일어나는 이벤트 시나리오를 살펴보면 크게 키쌍 생성, 인증서 발행, 토큰 발행, 인증, 검증으로 나

늘 수 있다.

5.3. 실험 환경

실험에서는 Payword의 개념을 이용한 SHA-1 해쉬 함수로 토큰을 생성하고 1000개의 토큰을 하나의 토큰 체인으로 발행토록 하였다. 모바일 상에서의 QKfms 인증을 위해서 ECDSA 알고리즘을 이용하여 키 쌍 생성과 인증을 수행하도록 하였다. 구현을 위한 프로그래밍 언어로는 Java를 사용하였다.

먼저 단일 순환자를 이용하였을 경우를 클라이언트와 공급자의 비율을 1:10으로 하고 공급자와 단일 순환자간 평균 전송 지연시간을 10ms로 하였다. 공급자에 대한 인증 및 토큰 발행 업무 처리 등을 감안하여 단일 순환자의 처리 평균 응답 시간을 측정한 결과는 다음과 같다.

〈표 2〉 단일순환자 평균 응답 속도

보안 토큰 서비스	클라이언트	공급자	순환자	순환자당 공급자수	순환자 평균 응답속도
1	1,000	100	1	100	328
1	10,000	1,000	1	1,000	450
1	100,000	10,000	1	10,000	650

단일 순환자의 실험 환경과 같이 클라이언트와 공급자의 비율을 1:10으로 하고 공급자와 단일 순환자간 평균 전송 지연시간을 5ms, 최근 사용 토큰 타순환자 평균 질의 시도 빈도율을 3%로 하고, 순환자당 공급자수를 10배로 하여 실험한 결과는 다음과 같다.

〈표 3〉 순환자당 공급자수 10배의 다중 순환자

보안 토큰 서비스	클라이언트	공급자	순환자	순환자당 공급자수	순환자 평균 응답속도
1	1,000	100	1	10	315
1	10,000	1,000	1	10	380
1	100,000	10,000	1	10	498

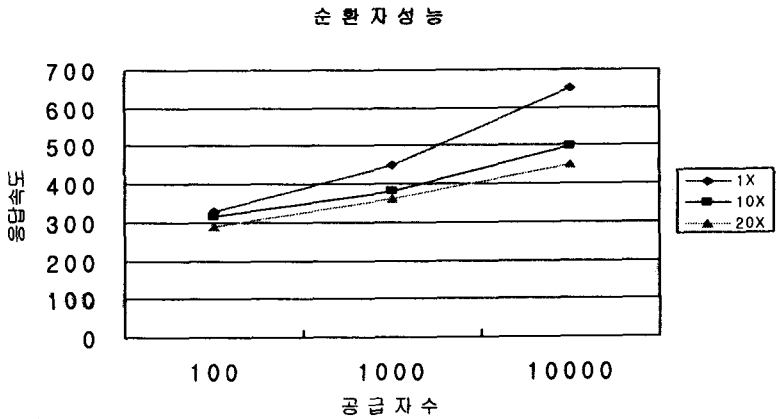
위의 다중 순환자 실험 조건과 같은 환경에서 순환자당 공급자수를 20배로 하여 실험한 결과는 다음과 같다.

〈표 4〉 순환자당 공급자수 20배의 다중 순환자

보안 토큰 서비스	클라이언트	공급자	순환자	순환자당 공급자수	순환자 평균 응답속도
1	1,000	100	1	20	289
1	10,000	1,000	1	20	360
1	100,000	10,000	1	20	450

위의 실험 결과들을 종합하여 단일 순환자, 순환자당 공급자수를 10배일 때, 순환자당 공급자수를 20배일 때의 결과를 하나의 그래프로 나타내면 다음과 같이 된다.

실험결과 그래프를 통하여 단일 순환자를 이용할 경우 공급자에 대한 평균 응답 속도는 공급자의 수에 거의 비례하여 느려지고 다중 순환자를 이용할 경우 공급자에 대한 평균 응답 속도는 공급자수의 증가에 비해 완만히 느려지는 것을 확인할 수 있다. 그러므로 단일 순환자에 비하여 다중 순환자는 공급자에 대한 보다 빠른 평균 응답 속도와 보다 나은 시스템 확장성을 제공한다고 말할 수 있다.



〔그림 6〕 공급자에 대한 순환자 평균 응답 속도

6. 결 론

SSO 기술은 인터넷 시대를 지나 유비쿼터스 시대에 접어든 우리의 전반적인 정보서비스 분야에 많은 개선점과 편리함을 제공해주는 요소기술이다. 사용자 측면에서는 시스템마다 인증절차를 밟을 필요 없이 단 한 번의 인증으로 여러 시스템에 접근할 수 있고, 관리자 측면에서는 인증정책의 변경이나 권한 설정을 편리하게 적용할 수 있어 비용 절감 및 업무 효율을 증대시키는 효과를 가져온다.

본 논문에서는 PKI 기반구조와 페이워드를 모바일 기기에 적합하도록 결합한 방식을 소개하였다. 여기에는 모바일 기기를 대신하여 인증서를 저장하고 순서대로 사용해야만 하는 토큰을 발행하는 순환자를 두었다. 아울러 PKI인증서를 통해 언제 어디서나 내부 업무 정

보 서비스를 이용할 수 있게 되었다. 향후에는 신규인증이 아닌 타 순환자에 있는 인증서를 효과적으로 질의하여 얻어올 수 있는 방법에 대한 연구가 필요하다.

참 고 문 헌

1. 오영선, "안전한 WWW를 이용한 CAI 구축 방안의 설계 및 구현", 홍익대학교, 석사학위 논문, 1997. 12.
2. 손태식, 김동규 외, "단일 인증 시스템의 인증 기법과 인증 모델 분석", 정보보호학회, 정보보호학회 학회지, Vol. 11, No. 4, 2001. 08.
3. Mark Becker, "So You Want Single Sign On", Syntegra, Mar. 2002.
4. Philip Carden, "The New Face of Single Sign-On", Network Computing, Mar. 1999.
5. BioNetrix, "Enterprise Single Sign-On: Balancing Security & Productivity", BioNetrix, 2002.
6. Datamonitor, "Single sign-on enterprise access made secure and easy", http://www.datamonitor.com, Sep. 2002.

최 진 탁(Jin Tak Choi)
· choi@incheon.ac.kr
· 인천대학교 컴퓨터공학과 교수
· 전공 및 연구분야 : 데이터베이스, 전산통계,
· 보안 · 암호학