개선된 브로커 기반 SSO 모델 연구

김현진, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[hjkim128, imylee]@sch.ac.kr

A Study on the Improved Broker-based Single Sign-On Model

Hyun-Jin Kim, Im-Yeong Lee
Dept of Computer Software Engineering, Soonchunhyang University

요 약

초고속 인터넷 망이 발달함에 따라 다양한 서비스들에 대한 사용자의 요구가 증가되었다. 보통 사용자들은 여러 서비스 사이트를 이용함에 있어 여러 개의 아이디와 패스워드를 기억하여 사용한다. 이러한 불편함을 해결하고 관리측면에서 효과적인 방법으로 제안된 인증 시스템이 SSO(Single Sign-On)이다. SSO 인증 모델 중 브로커 기반의 경우 중앙집중식 시스템 관리를 사용하여 인증 연산처리의 효율성을 증가시키는 장점을 가지고 있으며, 대표적으로 Kerberos 인증이 있다. 하지만 전통적인 Kerberos 인증은 패스워드 공격 및 재전송 공격에 비교적 심각한 위험성을 가지고 있어 그에 대한 연구가 활발히 진행되었다. 이에 본 논문에서는 기존방식의 문제점을 해결하여 보다 개선된 브로커 기반 SSO 인증 모델을 제안하였다.

1. 서론

최근 초고속 인터넷 망이 발달하게 되었고 급속히 확산함에 따라 과거 인터넷 환경과는 다른 모습을 보이고 있다. 일상생활에서 다양한 인터넷 서비스를 접할 수 있게 되었고, 인터넷 서비스는 우리 생활의 필수요소라 할 수 있다. 많은 사용자가 이용할 수 있는 서비스가 다양해짐에 따라 효용가치도 증가하였다. 또한 휴대성이 편리한 다양한 스마트 기기들의 발전과 보급으로 인해 더 많은 정보와 서비스들이 웹 서비스 형태로 변화되고 있다.

하지만 다양한 웹 서비스들은 각 사용자에게 사용 시 인증 정보를 요구하게 되고, 정당한 사용자로 인증되었을 경우에만 요청 서비스를 제공 받을 수 있다. 이에 따라 사용자측면에서 서비스 별로 개별적인 아이디와 패스워드를 설정하고 기억해야 하는 불편함이 따르게 되었다. 또한 서비스 업체에서 연계된 여러 서비스들을 제공하게 됨에 따라 중복 사용자들의 인증정보를 따로 관리하게 되는 문제점이 발생되었다. 이러한 문제점을 극복하기 위해 한 번의 인증으로 다양한 서비스들을 이용할 수 있는 SSO(Single Sign-On)이라는 개념이 등장하였다[1].

SSO 시스템에서 인증모델은 중요한 요소로써 작용되며, 전체적인 사용자 인증 과정의 안전성과 효율성에 큰 영향을 미친다[2]. 그 중 브로커 기반 모델의 경우 중앙집중식 시스템 관리를 사용하여 이를 통한 인증 연산처리의 효율성을 증가시킨다. 이러한 장점을 가지는 브로커 기반 모델은 Kerberos를 활용하여 인증을 실시한다. 전통적인 SSO 프로토콜의 경우 패스워드 공격 및 재전송 공격에 비교적 심각한 위험성을 가지고 있다. 이에 Jian[3]은 전통적인 SSO 프로토콜에 두 개의 새로운 데이터 흐름을 추가하여 보다 개선된 SSO 프로토콜을 제안하였다. 하지만 불필요한 데이터 생성 및 분배로 인해 비효율적인 단점을 가지고 있다. 따라서 본 논문에서는 Jian의 개선된 SSO 프로토콜 시스템을 기반으로 하여 보다 향상된 브로커 기반 SSO 인증 모델을 제안한다.

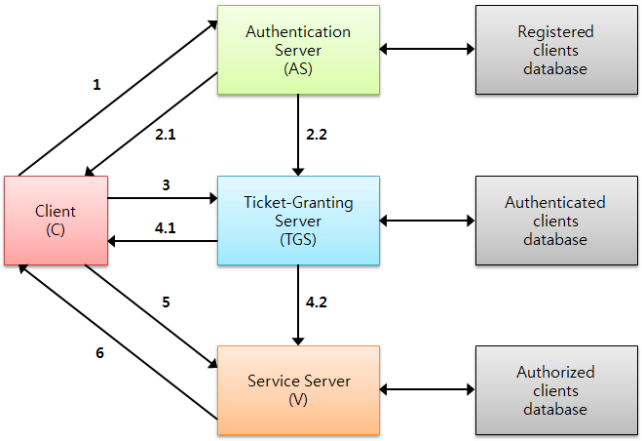
본 논문의 구성은 다음과 같다. 2장에서는 브로커 기반 SSO 인증 모델에 대한 기존 연구들을 살펴보고, 3장에서는 제안 방식에 대해 설명한다. 4장에서는 제안 방식에 대해 분석하고, 마지막으로 5장에서 결론 및 향후 연구 방향으로 마친다.

2. 관련연구

본 장에서는 브로커 기반 SSO 인증 모델 중 대표적으로 사용되는 Kerberos와 개선된 SSO 인증 프로토콜인 Jian의 방식에 대해 분석한다.

2.1 Kerberos

Kerberos는 MIT(Massachusetts Institute of Technology)에서 개발한 Athena 프로젝트의 한 부분으로써 비밀키 인증 프로토콜이다. 개방된 네트워크 환경에서 클라이언트와 서버간의 인증을 제공하기 위하여 중앙에 신뢰된 제3자인 인증 서버를 두고 있다. 이처럼 중앙 집중식 인증 서버를 사용하여 클라이언트와 서버 간에 강력한 인증 기능을 제공한다.



(그림 1) Jian 프로토콜 구조

Needham-Schroeder의 인증 모델을 근거로 하여 설계되었으며, 현재는 Kerberos V4와 V5가 사용되고 있다. Kerberos V5의 경우 문서 표준화 RFC 1510으로 발표되었다[4].

Needham-Schroeder의 인증 모델을 근거로 하여 설계되었으며, 현재는 Kerberos V4와 V5가 사용되고 있다[4].

2.2 Jian 프로토콜

Jian은 Kerberos를 기반으로 하는 전통적인 SSO 프로토콜을 개선한 방식을 제안하였다. 기존 Kerberos 프로토콜의 형태를 따르되, 인증서버와 티켓허가서버, 티켓허가서버와 어플리케이션 서버 간에 새로운 두 가지 데이터 흐름을 추가하였다. 이는 클라이언트에 티켓이 전송되는 과정을 줄임으로써 공격자가 수집한 데이터양을 줄임과 동시에 자동으로 이 단계로의 공격을 감소시키는 효과를 가진다. 또한 처리해야 될 정보감소로 인해 처리 속도를 향상시킨다[3].

하지만 해당 방식의 경우 불필요한 데이터 생성 및 분배 과정을 통해 인증 프로세스가 비효율적이며, 클라이언트 인증자를 복호화 하기 위한 키 값 검색과정이 잘못 설계되어 원활한 SSO 인증이 이루어지지 않는 문제점을 가지고 있다. Jian 프로토콜의 구조는 (그림 1)과 같다.

3. 제안방식

본 제안방식에서는 기존 Jian[3] 방식의 Kerberos 프로토콜 구조를 기반으로 하며, 문제점을 보완하여 보다 개선된 브로커 기반의 SSO 인증 모델을 제안하였다.

3.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

- $*$: 개체 (C : 클라이언트, AS : 인증서버, TGS : 티켓허가서버, V : 서비스 서버)
- ID_* : 해당 개체의 ID
- AD_* : 해당 개체의 IP 주소
- K_* : 사전에 공유된 해당 개체의 비밀키
- $K_{*,*'}$: $*$와 $*'$ 사이에 공유된 비밀키
- AU_C : C가 자신임을 나타내는 인증자
- $Times$: 티켓의 유효시간
- $Ticket_{TGS}$: TGS에게 전송될 티켓허가티켓
- $Ticket_V$: V에게 전송될 서비스티켓
- TS : 현재 시간을 나타내는 타임스탬프
- $Subkey$: C가 정한 V와의 세션키

3.2 사전등록 단계

사용자는 자신의 아이디와 패스워드를 등록하고 일차적으로 사용자를 인증하는데 사용한다. 사용자 등록이 완료되면 AS의 비밀키 K_{AS}를 생성하여 클라이언트에게 분배한다. 또한 서버 간에 티켓 암호화를 위해 사용되는 비밀키 K_{TGS}, K_V를 생성하여 각 서버에 분배한다.

3.3 인증 서비스 교환 단계

Step 1. 클라이언트 C는 티켓허가티켓 발급 및 비밀키 분배를 위하여 인증서버 AS에게 다음과 같은 요청 메시지를 전송한다.

$$C \rightarrow AS: ID_C \| ID_{TGS} \| Times$$

Step 2.1. 인증서버 AS는 응답으로 클라이언트 C와 티켓허가서버 TGS간에 사용될 비밀키를 생성하고 암호화하여 전송한다.

$$AS \rightarrow C: ID_C \| E_{K_{AS}}[K_{C,TGS} \| Times \| ID_{TGS}]$$

Step 2.2. 인증서버 AS는 또한 티켓허가티켓 $Ticket_{TGS}$를 생성하여 티켓허가서버 TGS에게 전송한다.

$$AS: Ticket_{TGS} = E_{K_{TGS}}[K_{C,TGS} \| Times \| ID_C \| AD_C]$$

$$AS \rightarrow TGS: ID_C \| Ticket_{TGS}$$

3.4 티켓 허가 서비스 교환 단계

Step 1. 클라이언트 C는 인증자 AU_C를 생성하고 서비스서버 V와의 비밀키 분배를 위해 다음과 같은 요청메시지를 티켓허가서버 TGS에게 전송한다.

$$C: AU_C = E_{K_{C,TGS}}[ID_C \| TS1]$$

$$C \rightarrow TGS: ID_C \| ID_V \| Times \| AU_C$$

Step 2.1. 티켓허가서버 TGS는 응답으로 클라이언트 C와 서비스서버 V간에 사용될 비밀키를 생성하여 $K_{C,TGS}$로 암호화 하여 전송한다.

$$TGS \rightarrow C: ID_C \| E_{K_{C,TGS}}[K_{C,V} \| Times \| ID_V]$$

Step 2.2. 티켓허가서버 TGS는 또한 서비스티켓 $Ticket_V$를 생성하여 서비스서버 V에게 전송한다.

$$TGS: Ticket_V = E_{K_V}[K_{C,V} \| Times \| ID_C \| AD_C]$$

$$TGS \rightarrow V: ID_C \| Ticket_V$$

3.5 클라이언트-서비스서버 교환 단계

Step 1. 클라이언트 C는 인증자 AU_C를 생성하여 서비스서버 V에게 전송함으로써 서비스를 요청한다. 이때 서비스서버 V와 사용될 $Subkey$를 생성하여 함께 전송한다.

$$C: AU_C = E_{K_{C,V}}[ID_C \| TS2 \| Subkey]$$

$$C \rightarrow V: ID_C \| AU_C$$

Step 2. 서비스서버 V는 클라이언트 C에게 서비스 요청에 대한 응답메시지를 전송한다.

$$V \rightarrow C: E_{K_{C,V}}[TS2 \| Subkey]$$

4. 제안방식 분석

본 제안 방식은 기존 Jian이 제안한 브로커 기반의 SSO 인증 프로토콜에서의 잘못된 프로토콜 설계와 불필요한 데이터 생성 및 분배과정을 개선하였다.

· 잘못된 프로토콜 설계 : 사용자에게 전송된 티켓정보를 복호화 하기 위한 키 값 검색에 있어서 각 서버들은 그 대상이 되는 클라이언트의 ID_C 값을 알 수 없게 설계되어 있다. 그로 인한 정상정인 인증 프로세스가 불가능하므로 이에 대한 개선 방안을 제안하였다.

· 불필요한 데이터 생성 및 분배 : 클라이언트에서 전송되는 요청 메시지에 포함되는 $Nonce$ 값이 불필요하게 생성되어 각 서버에게 전송되고 수신하는 과정을 거치는 문제점이 있다.

5. 결론 및 향후 연구 방향

본 제안방식에서는 Kerberos를 바탕으로 한 개선된 브로커 기반의 SSO 인증 프로토콜을 제안하였다. 기존 Jian 방식에서 잘못된 프로토콜 설계에 대한 보완과 불필요한 데이터 생성 및 분배 과정을 통해 인증 프로세스가 비효율적인 문제점을 해결하였다. 하지만 전체적인 인증 과정이 모두 비밀키 방식을 택하고 있다는 점에서 공개키 방식의 시스템보다 안전성이 미흡하다고 판단된다. 향후 공개키 방식을 활용한 브로커 기반의 SSO 인증 프로토콜에 대한 확장된 연구가 필요할 것으로 판단된다.

참고문헌

[1] A. Volchkov, “Revisiting Single Sign-On:A Pragmatic Approach in a New Context,” IT Professionals, 2001.

[2] 서대희, 이임영, “멀티 에이전트를 이용한 Single Sign-On 인증 모델에 관한 연구,” 한국통신학회논문지, Vol.29, No.7C, pp.997-1006, 2004.

[3] Yang Jian, “An Improved Scheme of Single Sign-on Protocol,” Fifth International Conference on Information Assurance and Security, pp.495-498, 2009.

[4] C. Baliello, A. Basso, and C. D. Giusto, “Kerberos protocol: an overview,” Distributed Systems, 2002.