익명성과 프라이버시 보장을 위한 효율적인 인증 메커니즘 설계

이동명*, 최효민*, 이옥연**
*고려대학교 정보보호대학원
**국민대학교 자연과학대학 수학과
e-mail : ldmur76@hotmail.com

Design of Authentication Mechanism for Anonymity And Privacy assurance

Dong-Myung Lee*, Hyo-Min Choi*, Okyeon Yi**
*Graduate School of Information Security, Korea University
**Dept. of Mathematics, Kookmin University

요 약

본 논문에서는 인터넷을 통해 다양한 컨테츠 서비스를 사용자가 편리하게 이용할 수 있도록 EAP-TLS 인증 방식과 SKKE(Symmetric-Key Key Establishment)방식을 이용하여 보다 효율적인 인증 메커니즘을 설계하였다. 제안하고 있는 메커니즘에서는 사용자가 인증서 방식을 통해 AS(AAA Server)로부터 인증을 받으면 AS 와 가맹 관계에 있는 CP(Contents Provider)에는 별도의 로그인 과정 없이 서비스를 이용할 수 있는 SSO 서비스, 사용자 익명성, 프라이버시를 제공한다. 사용자가 익명성을 필요로 하는 컨텐츠 서비스를 이용할 경우 사용자의 익명성을 보장 해주고 AS 모르게 사용자와 CP 가 안전하게 서비스를 전송하기 위해 사용 할 세션키를 교환하고 CP 마다 다른 세션키를 사용함으로써 사용자의 프라이버시를 보장해 준다.

1. 서론

인터넷 및 정보통신 기술의 발전으로 다양한 컨텐츠가 개발되고 있으며 누구나 쉽게 웹 사이트에서 제공하는 컨텐츠 서비스들을 이용하고 있다. 컨텐츠 서비스를 이용하기 위해서는 사용자가 개인 정보 등록을 포함하는 가입 절차가 요구된다. 사용자는 개인 신상정보를 입력하여 가입하게 된다. 사용자들은 이렇게 새로운 사이트에 가입할 때 마다 개인정보를 입력하는 것을 매우 불편하게 느끼고 있다. 웹 사이트를 통해 컨텐츠 서비스를 이용하기 위해서는 가입된 개인의 인증정보를 사용해 로그인 절차를 거쳐야 하는데 한번 컴퓨터를 이용할 때 여러 개의 웹 사이트를 방문하는 것이 일반적인 상황에서 매 사이트 마다 로그인 하는 것은 매우 불편한 일이다. 또한 웹 사이트마다 인증과정을 요구하기 때문에 사용자는 웹 사이트를 통해 컨텐츠 서비스를 사용할 때마다 매번 인증을 받아야 하고 사용자가 이용하는 컨텐츠 서비스의 수가 많아 질수록 사용자가 기억하고 관리해야 하는 인증정보 수가 증가하는 문제가 발생한다. 그리고 현재 사용자가 이용 할 수 있는 다양한 컨텐츠 서비스들이 있지만 사용자 측면에서는 컨텐츠 서비스들을 이용할 때 익명성을 보장 받으면서 이용하고 싶은 서비스가 있을 것이고 그런 서비스에 대해서는 익명성을 보장해줘야 할 문제가 있으며 웹 사이트에 등록된 개인정보 유출에 대한 우려가 증폭되고 있는 상황에서 개인 인증정보 도용이나 프라이버시 침해 같은 심각한 문제가 발생 할 수 있다.

본 논문에서는 앞에서 언급한 문제를 해결하기 위해서 사용자 인증 정보를 관리하는 인증서버를 통해 인증된 사용자에만 인증서버와 가맹을 맺고 있는 CP(Contents Provider)에 대해서 또 다른 인증과정 없이 사용자의 익명성을 보장 받으면서 인증서버 모르게

사용자와 CP 간에 서비스 전송을 할 수 있는 인증 메커니즘을 제안하고자 한다. 본 논문은 다음과 같이 구성되어 있다. 2 장에서는 현재 연구되고 있는 인터넷 서비스에 대한 관련 연구를 설명하고 3 장에서는 사용자의 익명성과 프라이버시를 보장 받으면서 컨텐츠 서비스를 이용할 수 있도록 제안한 인증 메커니즘에 대해서 설명한다. 4 장에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

2.1 인터넷 ID 관리 서비스

현재 한국전자통신연구원(ETRI)에서 인터넷 ID 관리 서비스를 제공할 수 있는 시스템을 개발 중에 있다. 이 시스템은 인터넷 ID 관리 서비스 제공자(ID Service Provider: IDSP)를 두고 일반 사용자는 여기에 가입해 ID 와 개인 정보를 등록한 후, 이 ID 를 이용해 인터넷을 이용하도록 하는 서비스이다. 서비스 제공자(Service Provider: SP)는 인터넷 ID 관리 서비스에 가맹하여 IDSP 에게 가입한 사용자들에게 서비스를 제공한다. 인터넷 ID 관리 서비스는 가입자에게 다양한 인증 메커니즘을 지원하는 복합인증 기능, 한번 인증에 모든 사이트 접근을 지원하는 SSO(Single Sign On)서비스 기능, 가입자 ID 정보 생명 주기를 관리하는 ID 관리 기능 및 개인정보의 오남용 방지를 지원하는 개인정보 보호 서비스 기능을 제공하고 가맹사이트에는 가입자의 ID 정보에 대한 열람 기능을 제공하는 ID 정보 열람 기능 등을 제공한다. 인터넷 ID 서비스 기술은 여러 진영에서 개발과 동시에 표준화를 추진하고 있다. 대표적으로 SAML(Security Assertion Markup Language)이 있는데 XML 관련 표준을 주관하는 OASIS 에서 추진하는 인증/인가 정보 전달 방식의 표준화를 위해 고안된 언어로 인터넷 ID 관리 서비스에 사용되는 핵심 기술이다. 또한 리버티는 연방화된 네트워크 ID 관리와 ID 기반의 서비스를 위한 공개표준을 개발할 목적으로 2001 년 9 월에 결성되었고, 2004 년 현재 157 개의 멤버를 가진 조직으로 성장하였다. 한국전자통신연구원에서 개발 중인 인터넷 ID 관리 서비스 시스템은 리버티 ID-FF 1.2 규격을 사용한다.[1][2]

2.2 Kerberos

가장 대표적으로 사용자들에 서비스를 안전하게 이용 할 수 있도록 인증 서비스를 제공하고 있는 커버로스(Kerberos)[3]가 있다. 커버로스는 중앙 집중식 인증 서버를 사용하고, 암호화 방식은 대칭키 암호화 방식을 사용하여 인증을 수행한다. 커버로스가 안전하게 동작하기 위해서는 커버로스 서버, 사용자 그리고 응용 서버로 구성된다. 사용자가 응용 서버에 접근하기 위해서는 커버로스 서버에 티켓-승인 티켓을 신청하여 발급 받고, 티켓-승인 티켓을 사용하여 서비스-응용 티켓을 발급 받은 후에 응용 서버에 접근한다. 각각의 커버로스 구성요소에 접근하기 위해서는 사전에 약속된 패스워드를 기억하고 있어야 한다. 커버로스가 안전하게 동작하기 위해서 영역간의 long-term 키의 교환과 다른 영역의 시스템에 대한 신뢰를 가정하는 것이 커버로스의 제약사항이다. 현재 Kerberos 프로토콜은 버전 4 에서 버전 5 까지 개발되었으며 이는 IETF RFC 1510 과 함께 표준으로 자기 잡고 있다.[4]

커버로스 시스템의 경우에는 티켓을 발행하는 서버가 세션키를 분배해주기 때문에 사용자와 응용 서버 사이에 전송되는 정보를 티켓을 발행하는 서버가 알 수 있는 프라이버시 문제와 익명성이 보장되지 않는 문제가 발생한다. 그러나 본 논문에서는 커버로스 시스템의 문제점을 해결하고 SSO 서비스와 사용자의 익명성, 프라이버시를 보장하면서 컨텐츠 서비스를 제공할 수 있는 새로운 인증 메커니즘을 제안한다.

3. 제안하는 인증 메커니즘

제안한 인증 메커니즘은 AS(AAA Server)와 서비스에 가입한 사용자, 서비스에 가맹한 CP(Contents Provider)로 구성된다. 사용자는 자신의 개인정보를 AS 에 ID 와 패스워드, CA 로부터 받은 인증서를 통해 등록하게 된다. 사용자가 AS 에게 서비스 연결을 시도하면, AS 는 사용자의 접근기기(PC, PDA 등)에 인증 접속 프로그램과 보안 모듈, AS 인증서를 포함한 클라이언트 패키지를 전송한다. CM(Connection Manager)프로그램의 검증을 위한 AS 서버의 서명 값을 포함한다. 인증서를 통해 AS 를 인증한 후에 클라이언트는 CM 의 서명 값을 체크한다. AS 와 CM 패키지가 검증되어지면, 클라이언트 패키지가 사용자의 PC 에 설치되어 안전한 컨텐츠 서비스를 제공한다. CM 은 ID/PW 인증 방식과 인증서 인증 방식이 있는데 본 논문에서는 인증서 인증 방식에 대해서만 이야기 한다. 사용자는 AS 로부터 최초에 인증 받을 때 자신이 원하는 CP 의 서비스를 선택함으로써 AS 로부터 CP 의 신뢰된 공개키와 ID 값을 전송 받아 저장하고 있다.

AS 는 사용자를 인증하는 인증서버 역할도 하지만 포탈서버의 역할도 수행한다. CP 와는 인증서를 통해 가맹을 맺음으로써 비즈니스 관계를 갔고 있으며 CP 들의 신뢰된 공개키를 가지고 있다. 사용자는 CP 의 컨텐츠 서비스를 받기 위해서는 AS 에 인증절차를 걸쳐야 하지만 SSO 서비스를 제공하기 때문에 한번만 인증서 방식의 인증절차를 수행하면 된다.

CP 는 AS 와 가맹을 맺고 있는 비즈니스 관계에 있으며 익명성을 제공하는 컨테츠 서비스를 사용자에게 제공한다. 예를 들어 사용자가 병원 웹 사이트에 접속하여 비뇨기과나 성형외과 같은 곳에서 의료 상담 서비스 받거나 19 세 이상의 영화 서비스 받을 때 사용자는 익명성을 보장 받고 싶어한다. 이런 익명성이 필요로 하는 컨텐츠 서비스에 대해 본 논문에서 제안한 인증 메커니즘은 이런 문제를 해결 할 수 있다. CP 는 AS 의 신뢰된 공개키와 AS 의 ID 값을 알고 있다.

3.1 제안하는 인증 기법

본 논문에서 제안하는 인증 기법은 인증서를 사용한

EAP-TLS[6]기반의 인증 방식과 ANSI X9.63-2001[7]의 HMAC-Matyas-Meyer-Oseas MAC scheme, Matyas-Meyer-Oseas hash function 을 사용한 SKKE(Symmetric-Key Key Establishment)을 수정하여 SSO 서비스 수행과 사용자의 익명성, 프라이버시를 보장해 준다.

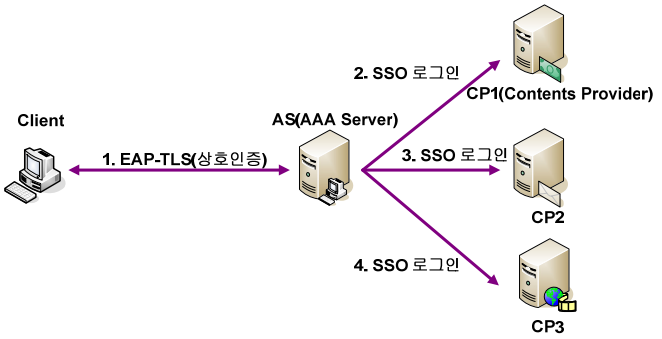

그림 1 인증 과정

그림 1 에서 보는 것처럼 사용자는 CM 을 통해 인증서 방식을 이용하여 AS 에 EAP-TLS(상호인증) 과정을 수행하고 CP 의 컨텐츠 서비스를 이용하게 되는데 추가적인 인증 과정이 없이 CP 에 접속하여 서비스를 이용할 수 있다. 이때 SSO 로그인 과정에서 사용되는 인증기법을 수정한 SKKE 를 사용하게 된다.

SKKE 는 둘간에 사용할 공유키를 나눠가지고 있고 상대방의 ID 를 알고 있다고 가정한다. 그림 2 처럼 U 는 V 에게 임의의 $Random_u$ 값을 전송하면 V 는 자신이 만든 $Random_v$ 값과 U 가 전송해준 $Random_u$, U 의 ID, 자신의 ID, 공유키를 입력 값으로 해서 AES-128bit 를 사용하는 Matyas-Meyer-Oseas hash function 을 이용하면 hash1, hash2 값이 만들어진다. Hash1 값을 MacKey 로 사용하여 MAC1 값을 계산한다. V 는 자신이 만든 $Random_v$ 값과 MAC1 값을 U 에게 전송하면 U 는 V 의 $Random_v$ 값을 이용하여 MAC1 값을 계산한다. V 로부터 전송된 MAC1 값과 비교 하고 U 도 MAC2 값을 만들어서 V 에게 전송한다. V 도 자신이 만든 MAC2 값과 U 로부터 전송된 MAC2 값을 비교하여 맞으면 U 와 V 둘간은 서로 상호인증을 하게 되고 hash1, hash2 값 중 hash2 값을 세션키로 사용한다.

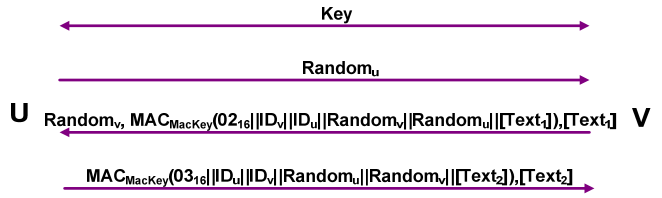

그림 2 Symmetric-Key Key Establishment

여기서 Text1,2 값은 Option 값이고, 02_{16}, 03_{16} 은 MAC 값을 달리 하기 위해서 사용된 값이다. 이렇게 사용된 SKKE 를 본 논문에서는 제안한 인증 메커니즘에 맞게 수정하여 사용하였다.

3.2 전송 프로토콜

제안하고 있는 인증 메커니즘은 그림 3 과 같이 동작한다.

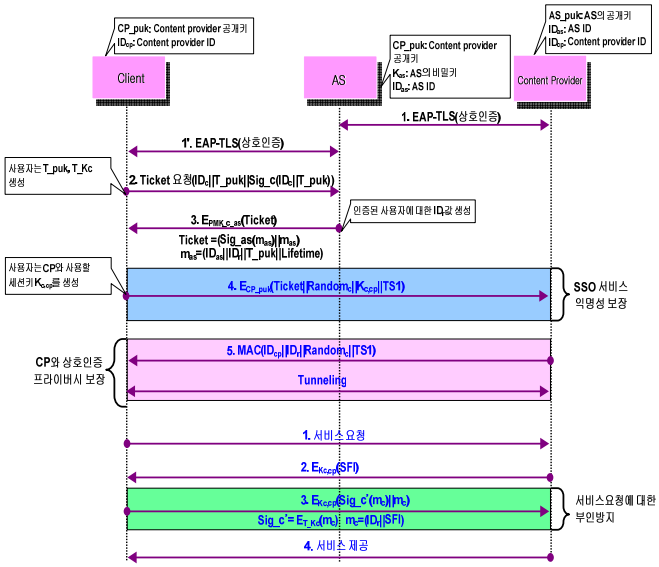

그림 3 제안한 인증 메커니즘

제안한 인증 메커니즘의 동작 절차는 4 단계로 구성한다. 첫 번째 단계는 사용자와 AS 간의 인증단계(1')이고, 두 번째는 Ticket 요청 단계(2~3)이며, 세 번째는 사용자와 CP 간의 인증단계(4~5), 네 번째는 서비스요청(1~4)단계이다.

3.2.1 표기법

전송 프로토콜에 사용할 표기법은 다음과 같다.

- ID_{as}: AS 의 ID
- ID_{cp}: CP 의 ID
- ID_c: 사용자의 ID
- ID_r: 사용자 Random ID
- C_puk: 사용자 공개키
- CP_puk: CP 공개키
- AS_puk: AS 공개키
- T_puk: 사용자가 생성한 임시 공개키
- T_Kc: 사용자가 생성한 임시 비밀키
- PMK_c_as: 사용자와 AS 간의 통신에 사용되는 세션키
- $Random_x$: x 에서 만든 랜덤 값
- TS: 타임 스탬프
- Lifetime: 유효기간
- SFI: 서비스 요금 정보

3.2.2 사용자와 AS 간의 인증단계

1'. 사용자는 CM 프로그램을 이용하여 AS 에 접속하게 되는데 사용자에게 인증서 제출할 것을 요구하고 사용자는 인증서를 제출 함으로써 상호인증을 하게 된다. 컨텐츠 서비스를 이용하기 위해서는 반드시 거쳐야 하는 단계이다.

3.2.3 Ticket 요청단계

2. Ticket 요청(ID_c||T_puk||Sig_c(ID_c||T_puk))
인증된 사용자는 AS 에 Ticket 요청에 앞서 사용자는 임시 공개키와 비밀키를 생성한다. 임시 공개키와 비밀키는 서비스 요청단계에서 서비스 이용에 대한 사용자 부인방지를 막기 위해 필요한 전자서명을 하고 검증할 때 사용된다. 사용자는 자신의 ID 정보와 임시 공개키를 가지고 서명한 값을 이용하여 AS 에게 Ticket 요청을 한다.

3. $E_{PMK\_c\_as}$(Ticket), Ticket =(Sig_as(m_{as})||m_{as}),
m_{as}=(ID_{as}||ID_r||T_puk||Lifetime)
AS 는 Ticket 을 요청한 사용자에게 임의의 ID 값을 부여하여 자신의 정보와 사용자가 보내준 임시 공개키와 함께 전자서명 한 것을 사용자에게 전송한다.
AS 는 사용자가 보내준 Ticket 요청 값과 Random ID 값을 매칭하여 테이블로 저장하고 있다.

3.2.4 사용자와 CP 간의 인증단계

4. E_{CP_puk}(Ticket||$Random_c$||$K_{c,cp}$||TS1)
사용자는 자신이 원하는 CP 에 접속하기 위해 저장하고 있는 CP 의 공개키를 사용한다. Ticket 과 사용자가 만든 $Random_c$ 값, CP 와 사용할 세션키를 생성하고 CP 의 공개키로 암호화해서 안전하게 전송한다. 사용자는 AS 로부터 받은 Ticket 을 유효기간동한 사용하여 자신이 원하는 CP 에 접속할 수 있다. 사용자로부터 암호화된 값을 받은 CP 는 비밀키로 복호화를 해서 Ticket 을 검증하고 AS 가 인증한 사용자로 판단한다.
4 번 단계에서 Ticket 을 이용한 SSO 서비스와 사용자에 대한 익명성 보장을 하고 있다.

5. MAC(ID_{cp}||ID_r||$Random_c$||TS1)
CP 는 사용자로부터 받은 세션키와 $Random_c$ 값을 이용하여 MAC 값을 생성한다. 이때 사용자 ID 값은 AS 가 생성한 Random ID 값으로 사용한다. 사용자에게 자신이 만든 MAC 값을 전송하고 사용자는 CP 가 보내준 MAC 값과 자신이 만든 MAC 값을 비교하여 맞으면 올바른 CP 로 인증함으로써 상호인증 과정이 이루어진다.
5 번 단계에서 상호인증과정이 이루어지고 사용자와 CP 간에 사용할 세션키를 AS 모르게 나눠가짐으로써 사용자에 대한 프라이버시 보장이 이루어진다.

3.2.5 서비스 요청단계

1. CP 와 상호인증과정을 수행 후 사용자는 CP 에게 서비스를 요청한다.

2. $K_{c,cp}$(SFI)
사용자가 요청한 서비스에 대한 요금정보를 사용자에게 전송한다.

3. $E_{Kc,cp}$(Sig_c'(m_c)||m_c), Sig_c'= E_{T_Kc}(m_c), m_c=(ID_r||SFI)
CP 로부터 서비스 요금정보에 대해 사용자는 서비스에 대한 구매결정을 한다. 사용자가 구매결정을 하면 Random ID 값과 서비스 요금정보에 대해 자신이 생성한 임시 비밀키로 전자서명을 해서 CP 에게 전송한다. CP 는 사용자가 인증 요청할 때 사용한 Ticket 을 통해 얻을 수 있는 Random ID 값에 해당한 임시 공개키를 알고 있기 때문에 이것을 이용하여 즉시 전자서명을 검증한다.

4. 검증결과가 타당하면 사용자에게 서비스를 제공한다. 후에 사용자에 대한 서비스 요금청부는 AS 에게 요청한다.

4. 결론 및 향후 연구과제

본 논문에서는 기존의 EAP-TLS 방식과 제안한 인증 메커니즘에 맞게 수정한 SKKE 를 사용하여 AS 에 한 번만 인증을 받으면 AS 와 가맹을 맺고 있는 CP 에 별도의 로그인 과정 없이 서비스를 요청할 수 있는 SSO 서비스를 제공한다. CP 마다 다른 세션키를 사용하여 서비스를 제공 받을 수 있을 뿐 아니라 AS 로부터 인증된 사용자는 AS 모르게 자신이 원하는 CP 와 안전하게 정보를 교환 할 수 있는 세션키를 나눠 가짐으로써 AS 는 사용자와 CP 간의 서비스 정보에 대해서 알 수가 없다. 그렇기 때문에 사용자의 프라이버시를 보장해줄 수가 있고 AS 의 전자서명과 임의의 ID 값을 통해 사용자의 익명성을 보장해준다. 제안한 인증 메커니즘을 익명성과 프라이버시를 보장 받길 원하는 컨텐츠 서비스에 적용하면 보다 효율적으로 활용할 수 있을 것이다.
향후, 제시된 시스템 모델을 구성하고 인증 메커니즘을 구현하여 시뮬레이션을 해서 안전성과 효율성을 측정 해보려고 한다.

참고문헌

[1] 최대선, 조상래, 김승현, 진승헌, 정교일, “인터넷 ID 관리 서비스”, 정보보호학회지, 2004.
[2] 한국전자통신연구원, “인터넷 ID 관리 서비스 기술백서 v1.0”, June 2004.
[3] J. Kohl and C. Neuman, “The Kerberos Network Authentication Service(V5).” RFC 1510, September 1993.
[4] 김은환, 전문석, “공개키를 이용한 커버로스 기반의 강력한 인증 메커니즘 설계”, 정보보호학회지, 2002.
[5] RFC 3588, Diameter Base Protocol, September.
[6] RFC 3748, Extensible Authentication Protocol(EAP), June 2004.
[7] ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry – Key Agreement and Key Transport Using Elliptic Curve Cryptography, American Bankers Association, November 20, 2001. Available from http://www.ansi.org.