익스트라넷 환경에서 상호 연동을 통한 단일 인증 서비스에 대한 연구

손태식°, 이건희, 유정각, 이규호, 박종운, 김동규
아주대학교 정보통신공학과
{tsshon, icezzoco, kagi, perry, hizcool, dkkim}@madang.ajou.ac.kr

A Study on Single Authentication Service through Inter-working in Extranet Environments

Tae-Shik Shon°, Gun-Hee Lee, Jeong-Gak Yoo, Kyoo-Ho Lee,
Jong-Wun Park, Dong-Kyoo Kim
Dept. of Information Communication Engineering, GSIC, AJOU

요 약

익스트라넷 환경에서는 인트라넷 환경에서 고려되는 보안 문제는 물론이고, 이와 함께 익스트라넷 환경 내의 여러 조직사이에 공유되는 자원의 관리 및 사용자에 대한 접근 제어에 있어 많은 문제를 가지고 있다. 본 논문에서는 익스트라넷 환경에서의 보안 문제를 해결하기 위해 익스트라넷 내부의 여러 도메인을 PKI(Public Key Infrastructure)를 기반으로 상호 연동하는 방안을 제안한다. 또한 상호 연동된 여러 도메인 사이의 상호 인증을 통해 익스트라넷 사용자에 대한 단일 인증 서비스를 제공하는 방안을 제안한다. 각 도메인 내부에는 도메인의 사용자 정보를 가지고 있는 사용자 관리 서버를 두고, 이 사용자 관리 서버에서는 사용자에 대한 인증과 응용 서버에 접근하여 응용 서비스를 제공받을 수 있는 서비스 티켓을 발급한다. 사용자 관리 서버에서 부여된 권한 정보가 담긴 서비스 티켓을 통하여 각 응용 서버는 응용 서버 자신의 보안 정책에 맞는 권한 속성을 접근하는 사용자에게 부여한다. 따라서 사용자의 인증은 PKI 기반으로 상호 연동되어 있는 도메인내의 사용자 관리 서버에서 한번 이루어지며 이때 발급한 서비스 티켓의 권한 정보를 통하여 사용자는 권한에 맞는 권한 속성에 따라 응용 서비스를 각 응용 서버에서 독립적으로 제공받을 수 있다.

I. 서 론

현재의 네트워크 환경은 인터넷 기술을 근간으로 하는 인트라넷의 증가와 함께 인트라넷을 확장한 익스트라넷 기술을 사용하여 같은 목적을 가지는 기관, 기업 그리고 학교 등이 서로 하나의 네트워크를 구성하여 사용하고 있다. 하지만 이러한 익스트라넷을 기반으로 하는 네트워크 환경에서 무엇보다도 자원의 공유에 있어서 많은 보안상 어려움을 가지고 있다. 또한 익스트라넷을 구성하는 집단사이에서 혹시 발생할 수 있는 이익 문제와 같은 여러 문제에 의해 익스트라넷 구성원에 대한 접근 통제 역시 필수 불가결하다.[1][2][3][4][7]

따라서 본 논문에서는 여러 도메인으로 구성된 익스트라넷 환경에서 상호 연동을 통해 도메인 간 상호 인증을 제공하여, 사용자에게는 한번의 인증을 통한 단일 인증의 간편함과 관리자에게는 네트워크 내에 공유된 자원에 대한 접근 권한 제어를 수행 할 수 있는 기반을 마련해 준다. 본 논문은 다음과 같이 구성된다. 제2절에서는 익스트라넷 환경의 도메인간 상호 연동 기능에 대해서 서술하며, 제3절에서는 도메인간 상호 인증 기능에 대해서 서술하며, 제4절에서는 도메인 내의 단일 인증 기능에 대해서 서술한다. 제5절에서 본 논문의 결론을 제시한다.

II. 상호 연동 기능

도메인간 상호 인증의 기반이 되는 상호 연동은 PKI 기반 구조의 인증 체계를 통하여 도메인간 사용자 관리 서버들이 신뢰 관계를 구축하는 것이다. 각 도메인의 사용자 관리 서버들은 비밀키를 공유하기 위해서 공개키를 사용한 키 분배 방법을 사용한다. 이때 비밀키를 분배하는 주체에 대한 인증은 비밀키를 보내온 메시지에 포함된 인증서의 발급 경로를 검증하여 공인 인증기관이 인증하는 범위까지의 인증 경로가 타당한지를 확인함으로써 이루어진다. 이렇게 비밀키를 보내온 도메인의 검증된 인증서는 계속해서 리스트 구조로 연결되어 여러 도메인 사이의 신뢰성을 보장해주며 또한 신뢰 관계를 나타내는 하나의 수단이 된다. 결국 이러한 검증된 인증서 리스트는 서로 신뢰하는 도메인들간에 비밀키를 공유하는 기반이 되고 여러 도메인들 간의 연동을 가능하게 한다. 다음의 과정은 [그림 1]의 PKI를 기반으로 하는 상호 연동 과정에 대한

설명이며, 관련 기호는 [표 1]을 참조한다.

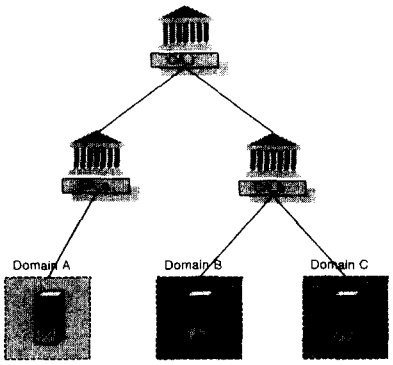

그림 1. 공개키 기반 구조의 상호 연동과정의 간략한 예시

1) 도메인 A와 도메인 B사이의 공개키 이용 비밀키 분배와 인증서 검증 과정

Domain A -> Domain B :

E_{b_pub}[mk, $Sign_{a\_pri}$(mk)] || Admin_A_Cert

(도메인 A에서 비밀키를 도메인 B에 보낸다.)

Domain B :

Verify(CA_A_Cert)

= $Verify_{ca\_r\_pub}$($Sign_{ca\_r\_pri}$(ca_a_pub))

Verify(Admin_A_Cert)

= $Verify_{ca\_a\_pub}$($Sign_{ca\_a\_pri}$(a_pub))

D_{b_pri}(Encrypted Secret key)

= D_{b_pri}[E_{b_pub}[mk, $Sign_{a\_pri}$(mk)]]

Verify(Sign value of Secret key)

= $Verify_{a\_pub}$($Sign_{a\_pri}$(mk))

2) 도메인 B와 도메인 C사이의 공개키 이용 비밀키 분배와 인증서 검증 과정

Domain B -> Domain C :

E_{b_pub}[mk, $Sign_{a\_pri}$(mk)] || Admin_A_Cert || Admin_B_Cert

(도메인 B에서 비밀키를 도메인 C에 보낸다. 이때 암호화된 메시지 뒷부분의 연결된 인증서 리스트가 검증된 후에 자신이 알고있는 신뢰하는 리스트가 된다.)

Domain C :

Verify(CA_B_Cert)

= $Verify_{ca\_r\_pub}$($Sign_{ca\_r\_pri}$(ca_b_pub))

Verify(Admin_B_Cert)

= $Verify_{ca\_b\_pub}$($Sign_{ca\_b\_pri}$(b_pub))

Dc_pri(Encrypted Secret key)

= D_{c_pri}[E_{c_pub}[mk, $Sign_{b\_pri}$(mk)]]

Verify(Sign value of Secret key)

= $Verify_{b\_pub}$($Sign_{b\_pri}$(mk))

III. 상호 인증 기능

본 논문에서는 도메인간 상호 인증 기능을 검증하기 위하여 사용자는 자신이 속한 도메인(도메인 A)에서 발급 받은 서비스 티켓을 사용해 다른 도메인(도메인 B)에 있는 응용 서비스를 요청한다고 가정한다.

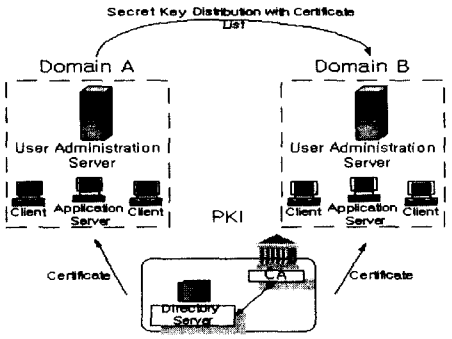

그림 2 도메인간 상호 연동 및 상호 인증 개념도

이때 도메인 B에 속한 응용 서버는 사용자의 서비스 요청에 대하여 사용자 관리 서버(도메인 B)에 사용자 인증을 요청한다. 이때 맨 먼저 서비스 티켓에서 서비스 티켓에 포함되어 있는 서비스 티켓을 발급한 사용자 관리 서버의 인증서가 자신이 신뢰하는 인증서 리스트에 포함되어 있는지를 확인한다. 확인 과정이 끝나고 서비스 티켓을 발급한 사용자 관리 서버의 도메인(도메인 A)이 신뢰 관계에 있는 도메인이라면, 도메인간 사용자 관리 서버의 비밀키로 암호화되어 있는 사용자 인증 정보를 복호화하고, 사용자 관리 서버(도메인 A)의 개인키로 서명되어 있는 사용자 인증 정보의 서명 값을 서비스 티켓에 있는 인증서의 공개키(도메인 A의 사용자 관리 서버의 공개키)로 검증하여 자신의 도메인에 속한 사용자가 아닐지라도 부가적인 사용자 등록 과정 없이 도메인간 신뢰 관계에 의하여 도메인 상호간에 인증이 성립 할 수 있다. 이러한 도메인간 상호 인증 기능은 각 도메인의 사용자 관리 서버가 상호 연동 과정에서 신뢰 관계를 바탕으로 유일한 비밀키를 공유함으로써 성립된다. 결국 앞서 검증된 도메인간의 상호 연동에서 PKI를 기반으로 구축된 신뢰 관계는 도메인간의 상호 인증을 성립시켜주는 바탕이 된다. 다음의 과정은 도메인간 상호 인증 과정에서 사용되는 비밀키와 서명 값 검증 과정이다.

1) 서비스 티켓에서 사용자 정보 복호화

D_{mk}(user authentication information)

= D_{mk}(E_{mk}[m, $Sign_{a\_pri}$(m)])

(여기서 mk는 도메인간 사용자 관리 서버의 비밀키)

2) 서비스 티켓에서 서명 값 검증

Verify(Admin_A_Cert)

= $Verify_{ca\_pub}$($Sign_{ca\_pri}$(a_pub))

Verify(UAI sign value)

= D_{a_pub}($Sign_{a\_pri}$(m))

(여기서 a_pub는 도메인 A의 사용자 관리 서버의 인증서에 얻어낸 공개키)

* UAI = User Authentication Information

표 1. 인증 프로토콜 기호 설명

기호	설명
App_Server_N	응용 서버 N
ux_pub	사용자 x의 공개키
ux_pri	사용자 x의 개인키
ca_x_pub	인증서 발급 기관의 공개키
ca_x_pub	인증서 발급 기관의 개인키
x_pub	사용자 관리 서버 x의 공개키
x_pri	사용자 관리 서버 x의 개인키
Rand	임시 난수 값
E_{mk}	사용자 관리 서버간의 비밀키
Sign(m)	메시지 m의 사인 값
TSN	서비스 티켓 시리얼 번호
TVT	서비스 티켓 유효 기간
PUP	사용자 프로파일 정보
IDI	서비스 티켓 발부 식별자
User_ACI	사용자의 접근 권한 정보
E_{kx}	응용 서버 x와 사용자 관리 서버의 비밀키로 암호화
D_{kx}	응용 서버 x와 사용자 관리 서버의 비밀키로 복호화
Admin_X_Cert	사용자 관리 서버 X의 인증서
Client_X_Cert	사용자 X의 인증서
Domain_X_UAS	도메인 X의 사용자 관리 서버

IV. 단일 인증 기능

응용 서버에 서비스를 요구하는 사용자에 대한 단일 인증은 도메인 내의 사용자 관리 서버에서 이루어진다. 이때 사용자 관리 서버에서 인증이 성공하는 경우 사용자 인증 정보를 포함하는 서비스 티켓이 사용자에게 발급된다. 이때 서비스 티켓의 사용자 인증 정보와 사용자 인증 정보에 대한 사용자 관리 서버의 서명 값은 도메인간 사용자 관리 서버들의 비밀키로 암호화되어 있다. 서비스 티켓을 가지고 있는 사용자가 새로운 응용 서버에서 서비스를 요청하는 경우 응용 서버는 이 서비스 티켓을 사용자 관리 서버에게 넘겨주고 사용자 관리 서버는 자신의 비밀키로 암호화되어 있는 사용자 인증 정보를 복호화 한다. 복호화 한 사용자 인증 정보와 사용자 인증 정보의 서명 값을 비교함으로써 서비스 티켓을 가지고 있는 사용자에 대한 인증이 이루어지며 이러한 과정에서 사용되는 사용자 관리 서버의 비밀키와 서명 값의 검증을 통해 사용자에게는 부가적인 인증 정보 요청이 없는 단일 인증 기능이 제공된다. 단일 인증에 사용되는 비밀키와 전자 서명 기법의 정당성은 PKI를 기반으로 다중 도메인간에 상호 연동을 통한 신뢰 관계를 구축함으로써 보장된다. 다음의 과정은 비밀키와 전자 서명을 통해 단일 인증 기능이 수행되는 과정에 대한 검증 과정이다.

1) 사용자 인증 후 발급 받은 서비스티켓

Ticket = E_{mk}[m, Signa_pri(m)] || Appl || Admin_A_Cert

(m = [TSN, TVT, PUP, IDI],

Appl = E_{ka}[PUP, User_ACI])

2) 사용자 관리 서버의 서비스티켓 복호화

Dmk(user authentication information)

=D_{mk}(E_{mk}[m, $Sign_{a\_pri}$(m)])

3) 사용자 관리 서버의 서명 값 검증

Verify(UAI sign value)

= D_{a_pub}($Sign_{a\_pri}$(m))

V. 결 론

본 논문에서는 현재 널리 사용되는 익스트라넷 환경에서 여러 응용 서비스에 대한 단일 인증 서비스를 제공하며 사용자 시스템의 투명성 제공, 중앙 집중적인 사용자 관리와 권한 부여 그리고 분산화 된 권한 속성 조절을 통해 기존의 SESAME나 Kerberos와 같은 분산 환경에서의 인증 시스템들[5][6]에 비하여 각 응용 시스템마다의 독립적인 보안성, 효율성 그리고 편리성이 강화되었다. 또한 다중 도메인 환경에서 도메인간 상호 인증을 위해 PKI 기반 신뢰 관계를 이용하여 여러 도메인들을 상호 연동하였다. 따라서 다중 도메인 환경에서 상호 연동되어 있는 각 도메인의 사용자 관리 서버들이 비밀키를 공유함으로써 도메인간 상호 인증이 가능하다.

향후에는 익스트라넷 환경에서 상호 인증에서 사용되는 비밀키의 안전한 관리, 스마트 카드 등을 사용한 서비스 티켓의 보안에 대한 연구가 필요하다.

참 고 문 헌

[1] Richard Au, "Towards a New Authorization Paradime for Extranets", *in Proceeding of information security and privacy*, ACISP 2000, 2000.06

[2] Barry, "Extranet Security : What happens if your partner turns against you?", Computer Security Institute, 2000

[3] Richard Power, "Intranet Security", Computer Security Institute, 2000

[4] Camilloi, "Unified Single Sign-On", *in Proceeding of Helsinke Univ of Technology*, Seminar on Netwokr Security, 1998

[5] Anonymous, Kerberos: *The Network Authentication Protocol*, Massachusetts Institute of Technology, 1998, http://web.mit.edu/kerberos

[6] Mark Vandenwauver. 1995. *SESAME V3*.http://www.esat.kuleuven.ac.be/cosic/sesame3_2.html

[7] 손태식, 김동규 외, "단일 인증 시스템의 인증 기법과 인증 모델 분석", 정보보호학회, 정보보호학회 학회지, Vol. 11, No. 4, 2001.08