情報保護學會論文誌
第12券 第4號, 2002. 8

공개키를 이용한 커버로스 기반의 강력한 인증 메커니즘 설계

김 은 환*, 전 문 석*

Design of a Strong Authentication Mechanism using Public-Key based on Kerberos

Eun-Hwan Kim*, Moon-Seog Jun*

요 약

분산 네트워크 환경에서 커버로스는 사용자와 응용 서버 사이에 인증을 위해서 대칭키를 사용하고 있으며 다른 영역의 시스템을 신뢰할 것을 가정하고 있다. 본 논문에서는 기존의 커버로스에 공개키/개인키를 적용하여 효율적이고 강력한 인증 메커니즘을 설계하였다. 제안하고 있는 메커니즘에서는 사용자 인증을 위해 미리 정해진 long-term 키와 공개키를 통해 교환한 랜덤 수에 MAC 알고리즘을 적용하여 암호화에 사용하는 세션키 값을 매번 바꾸어주기 때문에 안전성을 높였다. 또한, 영역간의 신뢰성을 높이기 위해 전자 서명 기반의 시도-응답(challenge-response) 기법을 통한 상호 인증 방법을 사용하고 있으며, 인증 절차를 간소화하여 사용하는 키의 수를 줄였다.

ABSTRACT

Kerberos is designed to provide strong authentication between client and application servers which are working in distributed network environment by using symmetric-key cryptography, and supposed to trust other systems of the realm. In this paper, we design an efficient and strong authentication mechanism by introducing the public/private-key to Kerberos. In the mechanism, to make a system more secure, the value of the session key is changed everytime using MAC(message authentication code) algorithm with the long-term key for user-authentication and a random number exchanged through the public key. Also, we employ a mutual authentication method, which is used on challenge-response mechanism based on digital signatures, to improve trust between realms, and present a way of reducing the number of keys by simplifying authentication steps.

Keyword : *Kerberos, Public/Private-key, Strong/Mutual Authentication, Challenge-response*

Ⅰ. 서 론

컴퓨터와 정보 통신의 발달로 인해 다양한 응용 서비스들은 계속해서 만들어지고 사용되고 있다. 특히, 인터넷의 빠른 보급으로 인해 통신의 속도가 엄청나게 증가하였으며 이를 이용하려는 사용자들과 서비스도 함께 증가하고 있다. 이런 상황에서 네트워크를 사용하는 사용자들은 더욱 안전한 통신을 원하고 있으며, 통신하려는 상대에 대한 인증을 통한 정보 보호 문제가 심각하게 요구된다. 더군다나 불법 사용자들이 합법적인 사용자를 가장하여 비 인가 자원에 대한 접속으로 인한 피해도 늘고 있다. 이런 개방된 네트워크 환경에서 가장 대표적인 인증 메커니즘으로 커버로스(Kerberos)[3,6,7,11]가 있다. 커버

* 숭실대학교 컴퓨터학과(ehkim@cherry.ssu.ac.kr, mjun@computing.ssu.ac.kr)

로스는 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 구성 요소에 접근하기 위해서는 사전에 약속된 패스워드를 기억하고 있어야 한다. 패스워드는 key-derived function을 통해 long-term 키로 바꾸어 저장하고 티켓을 암호화하거나 세션키로 사용한다. 커버로스의 영역(realm)이 커지면서 외부 영역의 커버로스 서버와도 통신이 가능해야한다.

커버로스가 안전하게 동작하기 위해서 영역간의 long-term 키의 교환과 다른 영역의 시스템에 대한 신뢰를 가정하는 것이 커버로스의 제약사항이다. 그러므로 위와 같은 커버로스의 제약사항을 보완하기 위해서 IETF의 CAT(common authentication technology) Working Group에서는 공개키와 인증서를 기반으로 한 인증 방법에 대한 연구를 시작했다. PKINIT(Public Key Cryptography for Initial Authentication in Kerberos)[2,4] /PKCROSS(Public Key Cryptography for Cross-Realm Authentication in Kerberos)[5]는 공개키와 인증서 기반으로 한 새로운 인증 서비스에 대한 발표이다. 또한, SESAME(Secure European System for Application in a Multi-vendor Environment)[12]는 유럽 보안 시스템 연구 프로젝트로써 비밀키/공개키를 이용한 대표적인 분산 개방형 시스템이다.

PKINIT/PKCROSS와 SESAME는 모두 공개키/개인키와 이를 보증하는 인증서를 발급하는 신뢰할 수 있는 인증 센터[1,8]를 가정하고 있다.

본 논문에서는 기존의 커버로스를 기반으로 인증 센터와 인증서를 사용하지 않고 단지 공개키/개인키를 적용한 강력한 인증 메커니즘을 소개한다. 제안하고 있는 인증 메커니즘은 사용자 인증을 위해 미리 정해진 long-term 키와 공개키를 통해 교환한 랜덤 수에 MAC(message authentication code) 알고리즘을 적용시켜 세션키 값을 매번 다르게 생성한다. 이 세션키를 사용하여 구성 요소간에 전송하는 데이터를 암호화한다. 시스템간의 인증을 위해서 공개키를 통해 전송한 랜덤 수와 전자 서명 기반의 시도-응답(challenge-response) 기법을 적용한 상호 인증(mutual authentication)방법[10]을 사용하여 시스템간에 신뢰성을 강조한다.

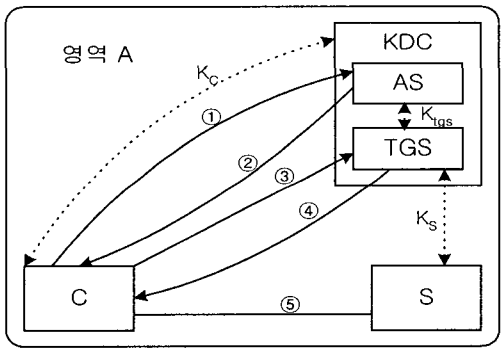
또한, 사용자가 외부 영역의 응용 서버에 접근하기 위한 기존의 커버로스에서의 동작 절차를 축소시킴으로써 사용자의 통신비용을 줄인다.

본 논문의 구성은 다음과 같다. 2장은 기본적인 단일 영역에서의 커버로스 인증 절차와 외부 영역의 커버로스 인증 절차를 소개한다. 또한, 공개키를 이용한 상호 인증 방법도 설명한다. 3장은 제안하고 있는 공개키 기반의 강력한 인증 메커니즘을 설명한다. 4장은 제안한 인증 메커니즘과 기존의 커버로스를 비교 분석하였으며, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 내부 영역의 커버로스

커버로스의 구성 요소는 커버로스 서버(KDC : key distribution center), 사용자(C : client)와 응용 서버(S: application server)로 구성된다. 커버로스 서버는 인증 서버(AS : authentication server)와 티켓 승인 서버(TGS : ticket granting server)로 구성된다. [그림 1]은 커버로스 시스템의 구성을 도식화 한 것이다.



[그림 1] 커버로스 동작 원리 및 절차

실선과 번호는 동작 순서를 나타내고 있으며 점선은 사전에 약속된 long-term 키를 나타낸다. long-term 키는 티켓을 암호화하는데 사용된다. 커버로스의 동작 절차는 다음과 같다.

① C → AS : ID_c || ID_{tgs} || TS1

사용자는 자신의 이름과 TGS 사용을 요구하는 TGS의 이름을 인증 서버(AS)에 전송함으로써 티켓-승인 티켓을 요청한다.

② AS → C : ID_c || $Ticket_{tgs}$ || $E_{Kc}[K_{c,tgs}$ || ID_{tgs} || TS2 || Lifetime]

인증 서버는 사전에 약속된 long-term 키(K_c)를 사용하여 TGS와 통신할 때 사용할 세션키($K_{c,tgs}$) 등을 암호화하여 사용자로 전송한다. 또한, 티켓-승인 티켓($Ticket_{tgs}$)을 발급한다.

③ C → TGS : ID_s || $Ticket_{tgs}$ || $Authenticator_c$

사용자는 티켓-승인 티켓($Ticket_{tgs}$)과 인증자($Authenticator_c$)를 TGS에게 제공함으로써 서비스-승인 티켓을 요청한다.

④ TGS → C : ID_c || $Ticket_s$ || $E_{Kc,tgs}[K_{c,s}$ || ID_s || TS4]

TGS는 서비스-승인 티켓($Ticket_s$)을 사용자에게 발급한다. 서비스-승인 티켓에는 사용자와 응용 서버가 통신 할 세션키를 포함하고 있다. 또한, 사용자와 TGS간의 세션키($K_{c,tgs}$)는 사용자와 응용 서버간의 세션키($K_{c,s}$)등을 암호화한다.

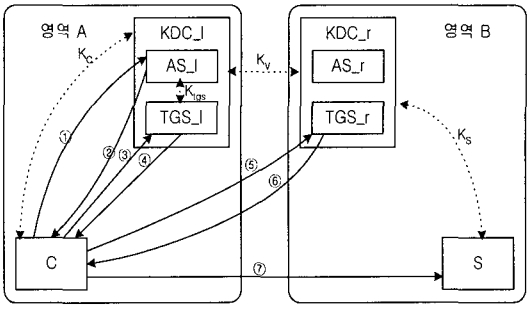
⑤ C → S : $Ticket_s$ || $Authenticator_c$

사용자는 서비스-승인 티켓과 인증자를 응용 서버에 제공함으로써 별도의 승인 과정 없이 응용 서버에 접속한다.

2.2 외부 영역 커버로스

사용자나 응용 서버들이 증가하면서 커버로스 영역이 커지게 된다. 이런 커버로스 영역이 여러 개 생기는 경우에 커버로스와 커버로스간의 신뢰성 있는 통신을 제공해야 한다. [그림 2]는 다중 영역 커버로스[5,9] 동작 과정을 나타낸다.

[그림 2]에서 실선은 외부 영역 커버로스 동작 절차를 나타내고 있으며 점선은 long-term 키를 나타낸다. 외부 영역 커버로스의 동작절차는 다음과 같다.



[그림 2] 외부 영역 커버로스 동작

① C → AS_l : ID_c || ID_{tgs} || TS1

사용자(C)는 지역 AS(AS_l)에게 티켓-승인 티켓을 요청한다.

② AS_l → C : ID_c || $Ticket_{tgs}$ || $E_{Kc}[K_{c,tgs}$ || ID_{tgs} || TS2 || Lifetime]

지역 AS는 사용자에게 티켓-승인 티켓($Ticket_{tgs}$)을 발급하고 세션키(K_c)로 기타 정보를 암호화하여 전송한다.

③ C → TGS_l : ID_{tgs_r} || $Ticket_{tgs}$ || $Authenticator_c$

사용자는 지역 TGS(TGS_l)에게 티켓-승인 티켓을 제시하고 원격 TGS(TGS_r)의 티켓-승인 티켓을 요청한다. 또한, 사용자 자신을 인증하기 위해 인증자를 함께 전송한다.

④ TGS_l → C : ID_c || $Ticket_{tgs\_r}$ || $E_{Kc,tgs}[K_{c,tgs\_r}$ || ID_{tgs_r} || TS4]

지역 TGS는 사용자가 제공한 티켓-승인 티켓으로부터 얻은 세션키($K_{c,tgs}$)를 이용하여 인증자를 확인하고, 원격 커버로스와의 통신에 사용할 새로운 세션키(K_{c,tgs_r})를 생성한다. 그리고 원격 커버로스에 제시할 원격 티켓-승인 티켓($Ticket_{tgs\_r}$)을 약속된 long-term 키로 암호화하여 사용자에게 발급한다. 원격 티켓-승인 티켓에는 새로 생성한 세션키를 포함한다.

⑤ C → TGS_r : ID_s || $Ticket_{tgs\_r}$ || $Authenticator_c$

사용자는 원격 티켓-승인 티켓($Ticket_{tgs\_r}$)을 원격 TGS에 제공함으로써 원격 응용 서버(S)의 서비스-승인 티켓을 요청한다.

⑥ TGS_r → C : $Ticket_s$ || $E_{Kc,tgs\_r}[K_{c,s}$ || ID_s || TS6]

원격 TGS는 원격 티켓-승인 티켓으로부터 세션키(K_{c,tgs_r})를 구하고 사용자를 인증한 후에 사용자와 원격 응용 서버간의 통신에 사용할 세션키($K_{c,s}$)를 생성한다. 원격 TGS는 서비스-승인 티켓($Ticket_s$)을 사용자에게 발급한다. 서비스-승인 티켓에는 새로 생성한 세션키를 포함한다.

⑦ C → S : $Ticket_s$ || $Authenticator_c$

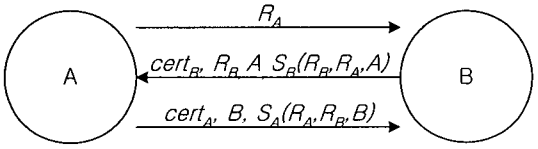
사용자는 서비스-승인 티켓과 인증자를 원격 응용 서버에 제공함으로써 별도의 승인 과정 없이 응용 서버에 접속한다.

제안한 인증 메커니즘에서는 ①번의 사용자 인증 방법을 수정했으며 ④, ⑤, ⑥번 단계를 단순화 시켰다. 그리고 지역 KDC와 원격 KDC간에 직접 통신하는 부분을 첨가하여 전체적인 동작 과정을 줄였다.

2.3 상호 인증 방법

공개키 기반의 인증서를 포함하고 있는 시스템에서 서로가 신뢰할 수 있는 통신을 하기 위해서 전자 서명 기반의 시도-응답(challenge-response) 상호 인증(mutual authentication)방법[10]이 있다. 이 방법은 상호 인증을 하기 위해서 랜덤 수와 전자 서명을 포함하고 있어 상대방을 인증한다. [그림 3]은 랜덤 수를 이용한 상호 인증 방법을 나타낸다.

A는 B에게 랜덤 수(R_A)를 전달한다. B는 자신의 인증서($cert_B$), 랜덤 수(R_B), A의 이름, 그리고 B가 개인키로 서명한 전자서명을 A에게 전달한다. A는 B의 인증서에서 공개키를 얻어 전자서명을 복호화하여 랜덤 수를 확인한다. 그리고 A는 자신의 인증서($cert_A$), B의 이름과 A가 자신의 개인키로



[그림 3] 상호 인증 방법

서명한 전자서명을 B에게 전달함으로써 상호 인증을 한다. 시도-응답 방식에서 랜덤 수를 사용하는 것은 시기 적절성(timeliness)과 유일성(uniqueness)을 보장해준다. 그리고 전자 서명은 상호간의 인증을 보장한다.

제안한 인증 메커니즘에서는 인증서 대신 공개키를 사용한다. 그러므로 공개키/개인키에 대해서만 상호 인증을 한다.

Ⅲ. 제안한 인증 메커니즘

본 논문은 기존의 커버로스 메커니즘 형태를 유지하면서 공개키/개인키를 첨가하여 보다 효율적이고 강력한 인증 절차를 수행하기 위한 새로운 메커니즘을 제안한다.

첫째, 기존의 커버로스는 사용자와 지역 커버로스, 지역 커버로스와 원격 커버로스간에는 반드시 패스워드를 교환하고, 이것을 long-term 키로 만들어 티켓을 암호화하거나 통신에 세션키로 사용한다. 그러나 매번 같은 long-term 키로 암호화를 하기 때문에 사전 공격 등을 통해 키 값이 해독되거나 노출될 가능성이 있다. 제안하고 있는 메커니즘은 공개키를 통해서 사용자와 키를 인증하고 long-term 키와 공개키를 통해 받은 랜덤 수를 이용하여 세션키를 다시 생성한다. 그리고 시스템간에 매번 세션키 값을 바꾸어 줌으로써 안전성을 높이고 사전 공격을 막을 수 있다. 둘째, 기존의 커버로스는 원격 커버로스에 있는 서버나 사용자를 인증 해 주기 위해서 원격 커버로스를 신뢰하고 있어야 한다. 실제로 통신하려는 대상에 대한 인증이 이루어지지 않고 있으며 long-term 키의 노출로 인해 위장 공격을 당할 수 있다. 제안한 메커니즘에서는 공개키/개인키를 이용하여 전자 서명을 주고받아 상호 인증을 시도한다. 또한, 공개키에 해당하는 개인키를 소유하고 있음을 증명하므로 신뢰성을 높이고 위장 공격을 막을 수 있다. 셋째, 기존의 커버로스는 사용자의 입장에서 볼 때 응용 서버가 내부 영역에 있을 때와 외부 영역에 있을 때에 서비스-승인 티켓을 얻기 위한 통신 회수가 다르다. 그러나 제안한 메커니즘은 사용자가 서비스-승인 티켓을 얻기 위해서 영역에 관계없이 지역 TGS에게 티켓-승인 티켓을 제출하는 것으로 일관성 있게 통일시켰으며, 전체적인 통신 회수도 줄였다.

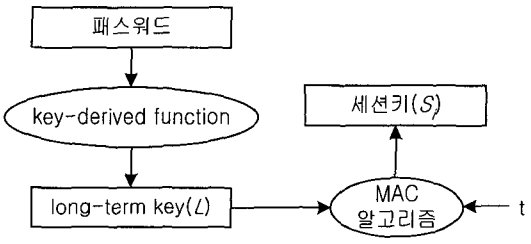
제안한 인증 메커니즘은 사용자, 커버로스가 각각

자신들의 공개키/개인키를 소유하고 있어야만 한다. 공개키/개인키를 이용하여 신뢰성 있는 강력한 인증 메커니즘과 각각의 영역에 존재하는 시스템을 상호 인증하고 동작 절차를 줄일 수 있다.

3.1 제안하는 인증 기법

기존의 커버로스는 사용자가 지역 KDC에 인증을 하기 위해 preauthentication방법을 사용한다. 즉, 사전에 약속된 패스워드를 key-derived function을 사용하여 long-term 키로 만들어 사용한다. 이 때 만들어진 long-term 키는 사용자와 지역 KDC 간의 통신에 세션키와 티켓을 암호화하는 비밀키로 사용한다. 그러나 long-term 키는 계속해서 같은 값의 세션키와 비밀키 기능을 하기 때문에 노출되거나 사전 공격의 위험을 지닌다.

본 논문에서 제안하는 long-term 키를 이용한 세션키 생성 과정은 공개키를 사용하여 사용자와 지역 KDC간에 랜덤 수(t)를 교환하고, 랜덤 수와 long-term 키를 조합하여 통신에 사용하는 세션키나 비밀키의 값을 계속해서 바꾸어 준다. [그림 4]는 제안하는 세션키 생성 과정을 표시한다.



[그림 4] 세션키 생성 과정

(1) 초기 설정 과정

2.3절에서 설명한 랜덤 수(R_A, R_B)와 전자 서명 기반의 시도-응답 방법을 통해서 공개키를 교환하고 공개키(Puk_A, Puk_B)에 해당하는 개인키(Prk_A, Prk_B)의 존재를 전자 서명을 통해 확인함으로 키에 대해서 인증을 한다. A는 교환된 B의 공개키(Puk_B)를 이용하여 B에게 랜덤 수(t)를 암호화하여 전달한다.

A → B : R_A
B → A : Puk_B, R_B, A, Prk_B(R_B, R_A, A)
A → B : Puk_A, B, Prk_A(R_A, R_B, B),
Puk_B(t)

(2) 세션키 생성 과정

B는 자신의 개인키(Prk_B)로 랜덤 수(t)를 복호화 한다. 그리고 처음에 약속된 long-term 키(L)에 대해서 랜덤 수(t)를 키로 사용한 CBC-MAC 알고리즘을 적용하여 S_i를 구한다. 계산된 S_i는 A와 B간의 통신에 대해서 세션키로 사용한다.

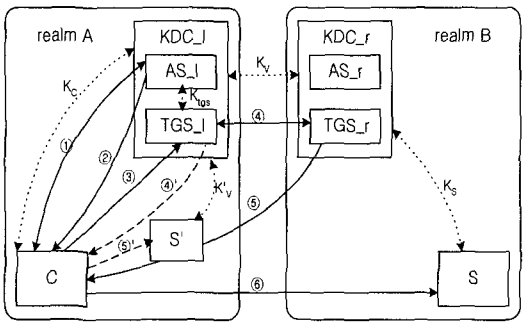
$L = L_1, ..., L_t$ (n비트 블록으로 나눔)
$S_i = E_t(S_{i-1} \oplus L_i)$, $S_1 = E_t(L_1)$,
$2 \le i \le t$, IV = 0

세션키를 생성하기 위해 미리 설정되어 있는 long-term 키를 사용하는 이유는 사용자를 인증하기 위함이다. 또한, 공개키와 개인키를 사용하여 키에 대한 인증과 사용자에 대한 인증을 동시에 한다.

세션키 생성 과정은 사용자와 지역 AS, 지역 TGS와 원격 TGS간에 각각 적용한다.

3.2 전송 프로토콜

제안하고 있는 공개키를 이용한 강력한 인증 메커니즘은 [그림 5]와 같이 동작한다.



[그림 5] 제안한 인증 메커니즘

제안한 인증 메커니즘은 사용자(C), 지역 커버로스(KDC_l)와 원격 커버로스(KDC_r)는 모두 공개키/개인키를 소유한다. 동작 절차는 3단계로 구성한다. 첫 번째 단계는 사용자 인증 단계(①~②)이고, 두 번째 단계는 서비스 승인 단계(③~④′, ③~⑤)이며, 세 번째 단계는 응용 서버와의 데이터 전송 단계(⑤′, ⑥)이다. 두 번째 단계를 모두 끝내면 사용자는 서비스-승인 티켓을 소유하고, 티켓 유효기간 내에 티켓을 사용하여 언제든지 응용 서버(S′, S)와 통신한다.

④′, ⑤′는 내부 영역의 응용 서버(S′)에 접근하는 경우로 기존의 커버로스 동작과 같기 때문에 이 부분에 대해서는 설명하지 않는다.

3.2.1 표기법

전송 프로토콜에 사용할 표기법은 다음과 같다.

- ADx : x의 IP 주소
- C_puk, C_prk : 사용자의 공개키/개인키
- KDC_lpuk : 지역 KDC의 공개키
- KDC_lprk : 지역 KDC의 개인키
- KDC_rpuk : 원격 KDC의 공개키
- KDC_rprk : 원격 KDC의 개인키
- $K_{a,b}$: a와 b간의 통신에 사용할 세션키
- K_a : a에서 사용할 비밀키
- Lifetime : 유효 기간
- ID_X : x의 이름
- R_X : x에서 만든 랜덤 수
- TS : 타임 스템프

3.2.2 사용자 인증 단계

사용자 인증 단계는 사용자(C)와 지역 KDC(AS_l) 간의 인증 과정을 나타낸다. 사용자와 지역 KDC는 각자의 공개키/개인키를 소유하고 3.1절과 같이 강력한 인증 기법을 사용한다.

① 사용자(C)와 지역 KDC(AS_l)간의 상호 인증 과정

- C → AS_l : $ID_{as\_l} \,||\, R_c$
- AS_l → C : KDC_lpuk $||\, R_{as\_l} \,||\, ID_{as\_l} \,||$ Sig_asl
- C → AS_l : C_puk $||\, ID_c \,||$ Sig_c $||\, ID_{tgs\_l} \,||$ TS1 $||\, E_{KDC\_lpuk}[t1]$
  - Sig_asl : $E_{KDC\_lprk}[R_c \,||\, R_{as\_l} \,||\, ID_{as\_l}]$: 지역 KDC의 전자서명
  - Sig_c : $E_{C\_prk}[R_{as\_l} \,||\, R_c \,||\, ID_c]$: 사용자의 전자 서명

② AS_l → C : $Ticket_{tgs\_l} \,||\, E_{K'c}[K_{c,tgs\_l} \,||\, ID_{tgs\_l} \,||$ TS2 $||$ Lifetime]

- $Ticket_{tgs\_l} = E_{Ktgs\_l}[K_{c,tgs\_l} \,||\, ID_c \,||\, AD_c \,||\, ID_{tgs\_l} \,||$ TS2 $||$ Lifetime] : 티켓-승인 티켓

①에서는 사용자와 지역 AS간에 랜덤 수(R_c)와 전자 서명을 이용한 상호 인증 과정을 나타낸다. 그러므로 사용자와 지역 AS는 각각 상대방의 공개키를 소유하고 공개키에 대응하는 개인키의 존재도 전자 서명으로 확인한다. 사용자는 세션키를 생성하기 위한 키 재료인 랜덤 수(t1)를 지역 AS의 공개키로 암호화하여 지역 AS로 전송하고 티켓-승인 티켓을 신청한다. ②는 ①에서 전달한 랜덤 수(t1)를 이용하여 기존의 long-term 키(K_c)를 3.1절과 같은 절차를 거쳐 세션키(K'_c)를 생성하고 이 세션키를 사용하여 서비스-승인 티켓등을 발급할 때 새로 생성한 세션키(K_{c,tgs_l})등을 암호화하여 사용자에게 전달한다. ②과정 후에 사용자는 사전에 약속된 패스워드를 입력하여 3.1절과 같은 과정을 통해 세션키(K'_c)를 얻어 복호화 함으로써 사용자 인증 과정을 완성한다. 이미 사용자에 티켓-승인 티켓이 있는 경우에는 티켓의 유효기간을 계산하여 유효 범위 내에 존재하면 상호 인증 과정을 생략하고 바로 서비스-승인 티켓을 요구할 수 있다. 티켓-승인 티켓을 암호화 한 비밀키(K_{tgs_l})는 지역 KDC내의 long-term 키이다.

3.2.3 서비스 승인 단계

내부 영역에서의 서비스 승인 단계는 기존의 커버로스 동작 절차(③-④′)와 같다. 외부 영역에서의 서비스 승인 단계(③-④-⑤)는 사용자가 원격 커버로스에 있는 응용 서버에 접속하기 위해 서비스-승인 티켓을 발급 받는 과정이다. 이 과정에서 지역 커버로스와 원격 커버로스, 원격 커버로스와 원격 응용 서버와는 약속된 long-term 키가 반드시 존재한다. 제안하는 인증 메커니즘은 지역 커버로스와 원격 커버로스사이에 공개키 개념을 적용 시켜서 세션이 연결 될 때마다 티켓을 암호화하는 long-term 키 값을 변경하여 신뢰성을 높였다. 또한, 지역 커버로스가 원격 커버로스에 직접 서비스-승인 티켓을 요청하고 원격 커버로스가 서비스-승인 티켓을 사용자에게 직접 전달한다. 그러므로 기존의 커버로스 동작 절차를 간소화했다.

③ C → TGS_l : $ID_{tgs\_r} \,||\, Ticket_{tgs\_l} \,||\, Authenticator_{c\_l}$

- $Ticket_{tgs\_l} = E_{Ktgs\_l}[K_{c,tgs\_l} \,||\, ID_c \,||\, AD_c \,||\, ID_{tgs\_l} \,||$ TS2 $||$ Lifetime] : 티켓-승인 티켓
- $Authenticator_{c\_l} = E_{Kc,tgs\_l}[ID_c \,||\, AD_c \,||$ TS3] : 인증자

사용자 인증 과정을 거쳐 획득한 티켓-승인 티켓($Ticket_{tgs\_l}$), 원격 커버로스의 이름(ID_{kdc_r})과 인증자($Authenticator_{c\_l}$)를 지역 TGS에 제공함으로써 원격 서비스-승인 티켓을 신청한다.

④ 지역 TGS(TGS_l)와 원격 TGS(TGS_r)간의 상호 인증 과정

- TGS_l → TGS_r : $ID_{tgs\_r} \| R_{tgs\_l}$
- TGS_r → TGS_l : KDC_rpuk $\| R_{tgs\_r} \| ID_{tgs\_r} \| Sig\_asr$
  - $Sig\_asr : E_{KDC\_rprk}[R_{tgs\_l} \| R_{tgs\_r} \| ID_{tgs\_r}]$: 원격 TGS의 전자 서명
- TGS_l → TGS_r : KDC_lpuk $\| ID_{tgs\_l} \| Sig\_asl \| E_{KDC\_rpuk}[t2] \| Ticket_{tgs\_l\_r} \| Authenticator_{c\_l\_r}$
  - $Sig\_asl : E_{KDC\_lprk}[R_{tgs\_r} \| R_{tgs\_l} \| ID_{tgs\_l}]$: 지역 TGS의 전자 서명
  - $Ticket_{tgs\_l\_r} = E_{K'v}[K_{c,tgs\_l} \| ID_c \| AD_c \| ID_{tgs\_l} \| ID_{tgs\_r} \| TS4 \| Lifetime]$: 티켓-승인 티켓
  - $Authenticator_{c\_l\_r} = E_{Kc,tgs\_l}[ID_c \| AD_c \| ID_{tgs\_l} \| TS4]$: 사용자의 정보를 세션키로 암호화

지역 TGS와 원격 TGS간에 랜덤 수(R_{tgs_l})와 전자 서명을 사용한 상호 인증 과정을 나타낸다. 그러므로 지역 TGS와 원격 TGS는 각각 상대방의 공개키를 소유하고 공개키에 대응하는 개인키의 존재도 전자 서명으로 확인한다. 지역 TGS는 원격 TGS에게 세션키 생성을 위한 키 재료인 랜덤 수(t2)를 원격 TGS의 공개키로 암호화하여 전송한다. 이렇게 전달된 랜덤 수는 long-term 키(K_v)와 함께 3.1절과 같은 절차를 거쳐 티켓을 암호화하는 비밀키(K'_v)를 생성한다. 생성한 비밀키(K'_v)는 원격 티켓-승인 티켓($Ticket_{tgs\_l\_r}$)을 암호화한다. 이 티켓에는 신분 확인을 할 수 있는 세션키(K_{c,tgs_l})를 포함한다. 인증자는 사용자와 지역 TGS를 확인하는 내용을 세션키(K_{c,tgs_l})로 암호화한다. 원격 TGS는 인증자를 복호화하여 신분을 확인하고 원격 TGS와 사용자간의 통신에 사용할 세션키($K_{c,s}$)를 생성한다. 그리고 사용자에게 발급할 서비스-승인 티켓을 생성한다.

⑤ TGS_r → C : $ID_c \| Ticket_s \| E_{Kc,tgs\_l}[K_{c,s} \| ID_s \| ID_{tgs\_r} \| TS5 \| Lifetime]$
- $Ticket_s = E_{Ks}[K_{c,s} \| ID_c \| ID_s \| TS5 \| Lifetime]$: 서비스-승인 티켓

원격 TGS는 사용자에게 직접 서비스-승인 티켓($Ticket_s$)을 발급한다. 서비스-승인 티켓은 원격 응용 서버와 원격 TGS간의 long-term 키(K_s)로 사용자와 원격 응용 서버간에 사용할 세션키($K_{c,s}$)를 암호화한다.

3.2.4 데이터 전송 단계

원격 응용 서버(S)에게 서비스-승인 티켓과 인증자를 제출함으로써 별도의 인증 과정 없이 응용 서버에 접근하여 데이터를 전송할 수 있다.

⑥ C → S : $Ticket_s \| Authenticator_{c\_s}$
- $Ticket_s = E_{Ks}[K_{c,s} \| ID_c \| ID_s \| TS5 \| Lifetime]$: 서비스-승인 티켓
- $Authenticator_{c\_s} = E_{Kc,s}[ID_c \| AD_c \| TS6]$: 사용자의 인증 정보

사용자는 발급 받은 서비스-승인 티켓($Ticket_s$)과 자신의 정보를 포함하는 인증자($Authenticator_{c\_s}$)를 사용하여 원격 응용 서버(S)에 접속한다. 원격 응용 서버는 서비스-승인 티켓으로부터 세션키($K_{c,s}$)를 알아내고 인증자로부터 사용자를 인증하고 접근을 허용한다.

Ⅳ. 제안한 메커니즘의 분석 및 효과

제안한 강력한 인증 메커니즘에 대한 연구는 기존의 커버로스 메커니즘을 최대한 활용할 수 있도록 개선하였다. 기존의 커버로스 메커니즘에 신뢰성, 안전성과 인증 절차의 단순성을 위해서 공개키/개인키 개념을 첨가했다.

(1) 안전성 : 커버로스 시스템에서 처음 티켓-승인 티켓을 받을 때 인증을 성공하면 그 이후에는 티켓-승인 티켓을 사용하여 원하는 서버에 접속할 수 있다. 그러므로 처음 티켓-승인 티켓을 받는 과정이 매우 중요하다. 기존의 커버로스에는

사전에 약속된 패스워드를 key-derived function을 통하여 long-term 키를 생성하여 이를 세션키로 사용한다. 그러므로 매번 같은 세션키를 사용하여 티켓-승인 티켓을 발행하기 때문에 세션키 값을 알아내기가 쉬워진다. 즉, 사전식 공격을 통해 세션키 값을 알아낼 수 있다. 제안하고 있는 공개키 기반의 메커니즘에서는 랜덤 수와 long-term 키에 MAC 알고리즘을 적용하여 세션키를 생성하므로 사용자를 인증 할 때마다 변경되는 세션키 값을 알아내기가 어렵다. 그러므로 사용자의 인증 때마다 변경되는 세션키 값으로 인해 사전 공격에 안전하다. 이 방법은 지역 TGS와 원격 TGS사이의 인증에서도 사용된다.

(2) 신뢰성 : 기존의 커버로스는 상호 영역간, 시스템간의 신뢰성을 가정함으로써 실제 신뢰성이 결여되어 있다. 또한, 사전 공격등으로 long-term 키가 노출되면 인증에 심각한 문제점이 발생하면서 신뢰성이 사라진다. 그러나 커버로스에서는 사용자 인증과 커버로스 서버간 인증에서 사전에 약속된 long-term 키와 함께 공개키를 사용한다면 상호 영역간이나 시스템간에 신뢰성을 높일 수 있다. 본 논문에서는 세션키를 안전하게 관리함으로써 사전 공격을 차단한다. 세션키를 안전하게 관리하기 위해서 공개키 개념을 적용했다. 그러나 공개키 개념은 위장 공격에 취약하다. 위장 공격에 대해서는 공격자가 공개키/개인키를 만들어 공격하는 경우 long-term 키와 랜덤 수의 조합으로 값을 만들어 사용자에게 되돌려 주고, 사용자는 패스워드를 입력해서 이것을 해석해야 하는데 이 부분을 수행 할 수가 없게되므로 위장 공격을 차단할 수 있다. 공개키에 대한 인증은 전자 서명을 통해서 할 수 있으며 상호 인증을 하도록 했다. 공개키에 대한 인증과 long-term키와 랜덤 수의 조합으로 사용자 인증을 확인하고, 사용하는 세션키가 안전하게 관리된다면 영역간, 시스템간의 신뢰성을 높일 수 있다.

(3) 단순성 : 기존의 커버로스는 사용자 측면에서 볼 때 서비스-승인 티켓을 얻기 위해 각각의 TGS에 접근하는 회수가 내부 영역과 외부 영역이 다르다. 그러나 제안한 메커니즘은 사용자 입장에서 영역에 관계없이 서비스-승인 티켓을 얻기 위해서 지역 TGS에 티켓-승인 티켓을 전달하면 서비스-승인 티켓을 얻을 수 있도록 통일 시켰으며, 접근 회수를 줄임으로써 통신비용이 감소한다.

(4) 키관리 : 기존 커버로스에서 사용하는 long-term 키는 모두 4개(K_c, K_v, K_s, K_{tgs})를 사용하며, 세션키도 4개(K_c, $K_{c,tgs}$, $K_{c,v}$, $K_{c,s}$)를 사용한다. 제안하고 있는 메커니즘에서는 long-term 키는 모두 4개(K_c, K_v, K_s, K_{tgs})를 사용하고 세션키는 3개(K'_c, K_{c,tgs_1}, $K_{c,s}$)를 사용하며 공개키를 3쌍(사용자, 지역 KDC, 원격 KDC)을 사용한다.

〔표 1〕은 기존의 커버로스와 제안하고 있는 강력한 인증 메커니즘을 비교 분석한 것이다.

〔표 1〕 메커니즘 비교 분석

분석 / 구분	기존의 커버로스	제안한 인증 메커니즘
안전성	▸티켓 발행할 때 같은 값인 long-term 키를 사용하므로 노출 될 가능성과 사전 공격의 가능성이 있다.	▸티켓 발생할 때 공개키를 이용하여 랜덤 수를 교환하고 이를 이용하여 티켓을 암호화 할 키를 매번 다시 생성한다. 그러므로 long-term 키에 대한 노출과 사전공격에 안전하다.
신뢰성	▸상호 영역간, 시스템간의 신뢰성을 가정함으로써 신뢰성이 결여되어 있다. 또한 사전 공격으로 long-term키가 노출되면 신뢰성이 사라진다.	▸랜덤 수와 공개키를 이용한 전자서명 기반의 시도-응답 기법을 사용하여 공개키/개인키의 존재를 확인하고 상호 영역과 시스템간의 인증을 확인하여 신뢰성을 높이고, 안전하게 세션키를 관리함으로써 사전공격과 위장공격 등을 차단하여 신뢰성을 향상 한다.
단순성	▸사용자 측면에서 서비스-승인 티켓을 얻기위한 내부 영역과 외부 영역에서의 접근 회수가 다르다. (사용자 측면에서의 통신회수: 내부영역-2회, 외부영역-4회)	▸서비스-승인 티켓을 얻기 위한 단계를 축소 시켰기 때문에 사용자 측면에서는 영역에 상관없이 지역 TGS에 접근하여 서비스-승인 티켓을 얻도록 단순화 시켰다. 통신비용도 줄였다.(사용자 측면에서의 통신회수: 내부영역-2회, 외부영역-2회)
키 관리	▸long-term 키 : 4개(K_c, K_v, K_s, K_{tgs}) ▸세션키 : 4개(K_c, $K_{c,tgs}$, $K_{c,v}$, $K_{c,s}$)	▸long-term 키 : 4개(K_c, K_v, K_s, K_{tgs}) ▸세션키 : 3개(K'_c, K_{c,tgs_1}, $K_{c,s}$) ▸공개키 : 3쌍(사용자, 지역 KDC, 원격 KDC)

V. 결 론

본 논문에서는 분산 환경에서의 대표적인 인증 메커니즘인 커버로스를 분석하고 기존의 커버로스에 공개키/개인키 개념을 첨가함으로써 효율적이고 강력한 인증 메커니즘을 제안했다. 기존의 커버로스에서 대칭키를 사용하여 사용자를 인증하고 있기 때문에 보안에 취약한 부분이 발생하였다. 제안한 인증 메커니즘은 공개키/개인키를 사용하여 키에 대한 인증과 사용자에 대한 인증을 시도했다. 사용자에 대한 인증은 사전에 약속된 패스워드 기반의 long-term 키로 충분하지만 이 키를 암호화하는데 사용함으로써 노출될 가능성이 있다. 그러므로 랜덤 수를 사용하여 서비스 할 때마다 암호화하는 키의 값을 바꾸도록 하여 신뢰성을 높였다. 또한, 기존의 커버로스는 응용 서버에 접속하기 위해서 서비스-승인 티켓을 발급 받아야한다. 그러나 사용자 입장에서 볼 때 서비스-승인 티켓을 받아오기 위해서 내부 영역과 외부 영역에서의 TGS에 접근하는 회수가 다르다. 제안하는 메커니즘에서는 사용자 입장에서 내부 영역과 외부 영역에서 각각 서비스-승인 티켓을 얻기 위해 TGS에 접근하는 메커니즘을 동일하게 만들었으며, 전체적인 인증 메커니즘을 단순화 시켜 통신 비용을 줄였다. 인증 절차의 단순화로 인해 사용하는 세션키의 개수도 줄었다.

본 논문은 기존의 커버로스에 공개키/개인키를 적용하여 효율적이고 강력한 인증 메커니즘을 설계하였으며 앞으로 실제 구현하여 소규모 네트워크등에서 활용할 수 있을 것이다.

참 고 문 헌

[1] 신광철, 정진욱, "네트웍 환경에서 안전한 Kerberos 인증 메커니즘에 관한 연구," 정보보호학회 논문지, 제12권 2호, April 2002.

[2] 김철현, 정일용, "PKINIT 기반 새로운 커브로스 인증 메커니즘의 설계," 정보과학회 논문지, 제28권 1호, Mar 2001.

[3] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, September 1993.

[4] B. Tung, C. Neuman, M. Hur, A. Medvinsky, S. Medvinsky, J. Wray, J. Trostle, 'Public Key Cryptography for Initial Authentication in Kerberos," draft-ietf-cat-kerberos-pk-init-15.txt.

[5] B. Tung, B. C. Neuman, M. Hur, A. Medvinsky, S. Medvinsky, "Public Key Cryptography for Cross-Realm Authentication in Kerberos," draft-ietf-cat-kerberos-pk-cross-08.txt.

[6] A. Harbitter and D. Menasce, "Performance of Public Key-Enabled Kerberos Authentication in Large Networks," Proc. 2001 IEEE Symposium on Security and Privacy, Oakland, CA, May 13-16, 2001.

[7] John T. Kohl, B. Clifford Neuman, Theodore Y. T'so, "The Evolution of the Kerberos Authentication System," In Distributed Open Systems, pages 78-94. IEEE Computer Society Press, 1994.

[8] Marvin A. Sirbu, John Chung-I Chuang, "Distributed Authentication in Kerberos Using Public Key Cryptography," Proc. 1997 Symposium on Network and Distributed System Security, 1997.

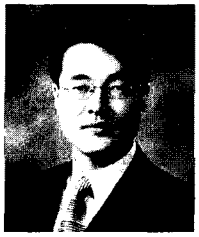
[9] W. Stallings, "Network Security Essentials applications and standard," prentice hall, 2000.

[10] Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone, "Handbook of applied Cryptography," CRC Press, 1997.

[11] J. Steiner, C. Neuman, J. Schiller, "Kerberos: An Authentication Service for Open Network System," Proc. of the Winter 1988 Usenix Conference, Feb. 1988.

[12] T. T. Parker, "A Secure European System for Applications in a Multi-vendor Environment(The SESAME Project)," Proceedings of the 14th American National Security Conference, 1991.

〈著者紹介〉



김 은 환 (Eun-Hwan Kim) 정회원
1990년 2월 : 숭실대학교 전자계산학과 졸업
1997년 8월 : 숭실대학교 컴퓨터학과 석사
2000년 2월 : 숭실대학교 컴퓨터학과 박사수료
1990년 2월~1995년 8월 : 국방과학연구소 연구원
1997년 9월~현재 : 숭실대학교 전자계산원 전임교수
〈관심분야〉 정보보호, 인증 시스템, 네트워크 및 인터넷 보안

전 문 석 (Moon-Seog Jun) 종신회원
1981년 2월 : 숭실대학교 전자계산학과 졸업
1986년 2월 : University of Maryland. Computer Science(석사)
1988년 2월 : University of Maryland. Computer Science(박사)
1989년 : Morgan State Univ. 부설 Physical Science Lab. 책임 연구원
1991년 3월~현재 : 숭실대학교 컴퓨터학부 정교수
〈관심분야〉 침입차단시스템, 인증 시스템, 인터넷 보안, 병렬처리시스템, 전자상거래보안