情報保護學會論文誌
第13券 第1號, 2003. 2

서로 다른 패스워드를 가진 사용자간의 패스워드 인증 키 교환 프로토콜

변 진 욱*, 정 익 래*, 이 동 훈*

Password-Authenticated Key Exchange between Clients with Different Passwords

Jin Wook Byun*, Ik Rae Jeong*, Dong Hoon Lee*

요 약

논문에서 언급되어지는 대부분의 패스워드 인증 키 교환 프로토콜은 사전 분배된 패스워드를 기반으로 해서 서버와 사용자간의 인증된 키 교환을 제공한다. 현대 통신 환경의 빠른 변화에 의해, 기존의 서버와 사용자간의 패스워드 인증 키 교환 프레임워크(framework)와는 틀린, 사용자와 사용자간의 안전한 종단간 인증(end-to-end authentication) 구축이 요구되어진다. 본 논문에서는 어떤 사전 비밀 값 분배 없이, 오직 사용자들간의 서로 다른 패스워드를 기반으로 한 사용자간의 패스워드 인증 키 교환 프레임워크인, C2C-PAKE(client-to-client password-authenticated key exchange)를 제안한다. 새로운 프레임워크에 적합한 안전성 개념들과 공격형태들이 정의된다. 또한 제안된 스킴이 정의되어진 공격들에 대해 안전함을 보인다. 본 논문은 두 개의 안전한 C2C-PAKE 스킴을 다중 영역(cross-realm) 환경과 단일서버(single-server) 환경에서 각각 제안한다.

ABSTRACT

Most password-authenticated key exchange schemes in the literature provide an authenticated key exchange between a client and a server based on a pre-shared password. With a rapid change in modern communication environments, it is necessary to construct a secure end-to-end channel between clients, which is a quite different paradigm from the existing ones. In this paper we propose a new framework which provides a password-authenticated key exchange between clients based only on their two different passwords without any pre-shared secret, so called Client-to-Client Password-Authenticated Key Exchange(C2C-PAKE). Security notions and types of possible attacks are newly defined according to the new framework. We prove our scheme is secure against all types of attacks considered in the paper. Two secure C2C-PAKE schemes are suggested, one in a cross-realm setting and the other in a single-server setting.

Keyword : *서로다른 패스워드 인증, 인증 된 키 교환 다중 영역 인증, Kerberos 시스템 사전 공격*

Ⅰ. 서 론

패스워드에 의존하는 인증은 그 쉬운 암기 성질로 인해 클라이언트-서버구조(client-server)상에서 널리 사용되는 사용자 인증 방법이다. 하지만 패스워드는 작은 공간에서 암기하기 쉬운 형태로 선택되어지기 때문에 공격자에게 오프라인 사전공격을 허용할 수 있는 심각한 약점이 존재한다. 이러한 영구적인 공격을

* 고려대학교 정보보호기술연구센터(CIST)({byunstar, jir}@cist.korea.ac.kr, {donghlee}@korea.ac.kr)

막고, 안전하고 효율적인 패스워드 인증 키 교환을 달성하기 위해 다양한 프로토콜들이 각각 다른 암호학적 가정(cryptographic assumption)들을 기반으로 하여 제안되어졌다[1~7].

패스워드 인증 키 교환 프로토콜은 두 개체가 패스워드를 오프라인을 통해 사전에 미리 가지고 있음을 가정한다. 두 개체는 패스워드를 이용하여, 공통의 세션 키를 만들고 형성된 세션 키에 대한 키 확인 과정을 수행한다. 논문에서 다루어지는 대부분의 패스워드 인증 키 교환 프로토콜들은 사용자와 서버간의 동일한 패스워드에 관한 인증된 키 교환만을 고려한다.

모바일 네트워크, 홈 네트워킹 등의 통신환경의 다양성으로 인해, 종단간(end-to-end) 안전성은 중요한 관심사 중의 하나로 간주되고 있다[8,9]. 예를 들어, 모바일 환경에서, 셀(cell) A에 속한 사용자와 셀 B에 속한 사용자(혹은, 동일한 셀 A에 속한 다른 사용자) 간의 안전한 종단간 채널 형성은 중요한 관심사이다. 또한 이는 사용자의 관점에서 네트워크 요소(component)들 간의 통신량을 최소화시킬 수 있다.

본 논문의 주요 목적은 사용자들간에 사전의 비밀값 분배 없이, 서로 다른 패스워드를 기반으로 하여 안전한 사용자들간의 패스워드 인증 키 교환 프레임워크(C2C-PAKE)를 설계하는 것이다. 프레임워크를 설계함에 있어서, 사용자들은 자신들이 등록된 서버를 이용한다.

새로운 프레임워크에 적합한 안전성 개념들과 공격 형태들이 정의되며, 제안된 스킴이 정의되어진 공격들에 대해 안전함을 보인다. 두 개의 안전한 스킴이 다중 영역 환경과 단일 서버 환경에서 각각 제안되어진다. 제안된 스킴들은 효율적인 다중 영역 커버로스(Kerberos) 인증 시스템에 기반하고 있다[10].

[관련연구와 연구 업적]

관련된 연구내용과 제안된 스킴을 실용적인 측면(practical use)과 오프라인 사전공격(dictionary attack)의 관점에서 비교해 봄으로써 본 논문의 실용성을 살펴본다.

- **실용적인 측면** 다중영역에서의 C2C-PAKE 스킴은, 처음으로, 다중영역에서 사용자들간의 서로 다른 패스워드를 이용한 인증을 제공해준다. 서로 다른 패스워드를 가진 임의의 사용자들은 자신들이 암기하고 있는 패스워드만을 가지고, 다른 영역에 있는 사용자들과 인증을 할 수 있다. 단일영역 환경에서 서로 다른 패스워드를 가진 사용자들간의 인증 프로토콜은 Steiner 등이 제안한 3-Party EKE가 있었다[11]. 하지만 3-Party EKE는 다중 영역간 환경에서의 인증은 고려하지 않았다.
- **오프라인 사전 공격** 커버로스 시스템에서 가장 심각한 문제 중의 하나는 사용자 패스워드에 대한 사전공격이 가능하다라는 점이다. 이 공격을 막기 위해 커버로스 버전 5(V5)에서는 타임스탬프를 암호화한 형태를 가지는 사전인증(pre-authentication) 개념을 도입하였다. 하지만, 이러한 구조도 사용자 패스워드의 오프라인 사전공격에 대한 완전한 해결책을 제시하지 못하였다[12]. 이 문제는 1996년, Jaspan이 사용자와 커버로스 서버 사이에 DH-EKE 스킴을 적용한 PA-ENC-DH를 제안함으로써, 사용자의 패스워드에 대한 사전공격을 막을 수 있었다. 또한 Jaspan은 제안된 스킴을 이용해서, 아래의 커버로스의 단점 세 가지를 해결 할 수 있었다[13]. (1) 사전공격의 취약성, (2) 시간 동기화의 문제점, (3) 패스워드 연결(password-chaining) 문제.

하지만 PA-ENC-DH 스킴은 오직 사용자와 커버로스 서버간에만 패스워드 공유를 가정할 뿐, 응용서버와 커버로스 서버간에는 대칭 키 공유를 가정한다. 만약 응용서버와 커버로스 서버간의 사전 공유된 대칭 키가 패스워드로 변환되어졌을 때, PA-ENC-DH 스킴은, 사전공격을 쉽게 허용한다. 다시 말하면 PA-ENC-DH는 커버로스 서버에 등록된 두 개체(사용자, 응용서버)가 모두 패스워드를 이용해서 통신하려고 할 때에 적용되어서 사용되어질 수 없다. 그 원인은 두 개의 패스워드와 여러 개의 세션 키 존재로 인한 새로운 안전성 개념들과 공격들이 존재하기 때문이다. 본 논문의 C2C-PAKE는 효율적인 커버로스 시스템을 기반으로 하여 이러한 문제를 해결한다. 더 나아가 (2),(3)항목을 해결한다.

II. 준비 단계

본 장에서는 제안된 스킴에 필요한 모델과 정의를 소개한다. 먼저 패스워드 인증 키 교환 프로토콜을 두 가지 모델로 분류한다.

[Shared Password-Authentication Model]

이 모델은(이하, SPA) 사용자 A와 서버 B사이의

사전 분배된 공통의 패스워드에 대한 인증된 키 교환을 제공한다. 또한 이 모델은 사용자 A가 패스워드를 가지고 있으며, 서버 B는 그에 해당하는 패스워드 확인자(password-verifier)를 안전한 채널을 통해 저장하고 있음을 가정한다. 대부분의 패스워드 인증 키 교환 프로토콜은 이 모델을 기반으로 하고 있다.

[Different Password-Authentication Model]

이 모델은(이하, DPA) 사용자 A_1과 사용자 A_2 사이의 서로 다른 패스워드를 이용하여, 인증 된 키 교환을 제공해 준다. 이 모델은 다중 영역(cross-realm) 환경과 단일 서버(single-server) 환경으로 나누어진다. 다중 영역 환경에서는 사용자 A_1, A_2와 두 개의 서버 B_1, B_2로 구성된다. 단, A_1, A_2는 각각 서버 B_1, B_2에 등록된 사용자이다. 단일 서버 환경에서는 두 개의 사용자 A_1, A_2와 하나의 서버 B로 구성되어 있으며, 사용자 A_1, A_2는 서버 B의 사용자이다. 사용자 A_1, A_2는 다중 영역 환경에서는 서버 B_1, B_2의 도움을 받아서, 또는 단일 서버 환경에서는 B의 도움을 받아서 사용자간의 서로 다른 패스워드를 이용하여 인증된 키 교환을 한다. 본 논문에서 제안된 스킴은 이 모델에 기반하고 있다.

SPA에서는 오직 하나의 공통된 패스워드가 사용되는 반면에, DPA에서는 두 개의 패스워드들이 인증 과정에 관여한다. 대부분의 논문에서는 안전성과 공격의 개념 및 정의가 SPA 환경에서만 논의되어진다. DPA 모델의 안전성 개념을 다루기 위해서, 관련된 안전성 개념들이 모델의 정의에 따라 새롭게 정의되어져야 한다. 다음절에 이 부분에 관해서, 형식을 갖추지 않고(informal) 소개한다.

2.1 정의와 가정

먼저, SPA 모델에서 perfect forward secrecy의 정의를 살펴본 다음, DPA 모델 상에서 perfect forward secrecy를 정의한다.

(정의 1)

롱텀(long-term) 비밀 값(패스워드)의 분실이 롱텀 비밀 값 분실 이전에 생성된 프로토콜 P의 세션 키 분실을 의미하지 않는다면, 프로토콜 P는 *SPA 모델에서 perfect forward secrecy*를 만족한다라고 말한다.

DPA 모델에서는 SPA 모델보다 관여되는 롱텀 비밀 값의 개수가 많다. 이러한 추가된 롱텀 비밀 값에 대한 perfect forward secrecy 개념이 정의에 포함되어져야 한다.

(정의 2)

프로토콜 P의 모든 참여자들의 롱텀 비밀 값들의 분실이 롱텀 비밀 값들의 분실이전에 생성된 프로토콜 P의 모든 세션 키의 분실을 의미하지 않는다면, 주어진 프로토콜 P는 *DPA 모델에서 perfect forward secrecy*를 만족한다고 말한다.

정의 1과 정의 2에 의해서, 만약 프로토콜 P가 DPA 모델에서 perfect forward secrecy를 만족한다면, SPA 모델에서 perfect forward secrecy를 만족함을 알 수 있다(단, 그 역은 만족하지 않는다.).

다음은, SPA 모델에서의 Denning-Sacco 공격에 대해서 살펴보고[14], DPA 모델에서 이 공격을 정의한다. 아래에 정의하였듯이, DPA 모델은 많은 세션 키들이 존재하므로, Denning-Sacco 공격의 정의는 이러한 개념들이 포함되어져야 한다.

(정의 3)

공격자가 세션 키를 이용해 공통 패스워드에 대해서 사전 공격이 불가능해야 하고, 또한 이전 세션 키를 이용해서, 이 후 프로토콜 P에 속하는 개체들을 가장할 수 없다면, 프로토콜 P는 *SPA 모델에서 Denning-Sacco 공격*에 강하다라고 말한다.

(정의 4)

공격자가 프로토콜 P에서 사용되는 모든 세션 키들을 이용하여 프로토콜 P의 롱텀 비밀 값들에 대한 사전공격이 불가능해야 하고, 또한 모든 이전 세션 키를 이용해서 이후에 프로토콜 P에 속하는 사용자들을 가장할 수 없다면, 이후에 프로토콜 P는 *DPA 모델에서 Denning-Sacco 공격*에 강하다라고 말한다.

SPA 모델에서의 패스워드 기반 프로토콜은 항상 오프라인 사전 공격에 강해야 하며, DPA 모델에서의 패스워드 기반 프로토콜 역시 이러한 성질을 만족해야 한다. 하지만 DPA 모델의 사전공격에서 고려되어져야 하는 패스워드가 SPA 모델보다 많다. 그러므로 DPA 모델에서의 사전공격을 다음과 같이 정의한다.

(정의 5)

프로토콜 P가 다음 두 가지를 만족하면, *DPA 모델에서 사전공격*에 안전하다라고 말한다. 먼저 프로토콜 P에 속하는 모든 패스워드에 대해서 사전공격이 불가능해야 한다. 또한 공격자에게 하나의 패스워드가 주어졌을 때, 그것을 제외한 다른 패스워드에 대한 사전공격이 불가능해야 한다.

SPA 모델에서의 패스워드 기반 프로토콜에서는 이를 제외한 많은 공격들이 존재한다. 예를 들면, 중간공격(man-in-the-middle attack), 재생 공격(replay attack) 등이 그 대표적인 예이다. 하지만, 이러한 공격들은 수정 없이 SPA 모델에서 DPA 모델로 적용되어질 수 있다. 다음은 DPA 프로토콜의 안전성에 대해서 논한다.

[DPA 프로토콜의 안전성]

다항식 시간(poly-time)의 공격자 E가 주어진 프로토콜을 잘 알려진 공격 방법들을 이용하여 공격한다고 가정하자. 온라인 사전공격의 경우, E는 로그인(log-in) 단계에서 가능한 모든 패스워드들을 시도해 볼 것이다. 만약 서버가 공격자 E가 선택한 패스워드에 대해서 수락하면 공격자의 패스워드에 대한 추측은 성공한 것이고, 거부하면 공격자 E는 패스워드 사전으로부터 해당 패스워드를 삭제 할 수 있게 된다. R번의 서버의 연속적인 거부 후에 공격자 E가 패스워드 추측을 성공하게 되는 확률은 $1/(|D|-R)$이 된다.(단, |D|는 패스워드의 사전 크기이다.) 실제적으로 온라인 사전 공격은 피할 수 없는 것이며, 그 성공 확률은 어떠한 공격자가 주어진 프로토콜을 공격함에 있어서 최하위 이점(lower bound advantage)이 되어야 한다. 다시 말하면, 만약 공격자 E가 프로토콜 P를 공격하는 이점이 다음과 같이 결정되어 질 때 프로토콜 P는 DPA 모델에서 안전하다라고 말한다.

$$ADV_E^{DPA}(k) \le O(1/(|D|-R)) + \varepsilon(k)$$

(단, ε(k)는 negligible 함수, R은 로긴 단계에서 거부되는 횟수, k는 안전성 파라미터, 부등식 오른 쪽의 두 번째 텀은 DPA 모델에서 정의된 공격들에 대한 공격자 E의 이점이다.)

[계산적 가정]

본 논문에 제안된 스킴 들은 수학적인 가정과 계산적인 가정에 기반하고 있다. p, q를 $q|p-1$를 만족하는 충분히 큰 소수라고 하고, G를 위수가 q인 Z_p^*의 서브그룹이라 하자. 초기화 단계동안 생성자, $g \in G$와 해쉬 함수(H_1, H_2, H_3, H_4, H_4)는 공개되어진다. 본 논문에 나타난 모든 프로토콜들은 이산 대수 가정(DLA)과 Diffie-Hellman 가정(DHA)에 기반을 둔다. 이 가정들은 다음과 같이 정의된다

(정의 6) [Discrete Logarithm Assumption]

모든 다항식 시간 알고리즘 A에 대해서 다음이 성립한다.

$$\Pr[A(p,g,y) = x \; s.t \; y = g^x \bmod p] \le \varepsilon(k)$$

여기서 $\varepsilon(k)$는 무시할수 있는 함수이고, $x \in Z_q$이다.

(정의 7) [Diffie-Hellman Assumption]

모든 다항식 시간 알고리즘 A에 대해서 다음이 성립한다.

$$\Pr[A((p,g,y),(g^a, g^b)) = \alpha \; s.t \; \alpha = g^{ab} \bmod p] \le \varepsilon(k)$$

여기서 $\varepsilon(k)$는 무시할수 있는 함수이고, $x \in Z_q$이다.

본 논문에서 사용하는 표기를 요약하면 다음과 같다.

〔표 1〕 표 기

표 기	의 미
Alice, Bob	정직한 사용자 혹은 클라이언트
ID_A, ID_B	Alice와 Bob의 identity
pwa, pwb	Alice와 Bob의 패스워드
E_x E_x: $\{0,1\}^l \rightarrow \{0,1\}^l$	대칭키 암호 알고리즘
H_1, H_2, H_3, H_4, H_5 H_i: $\{0,1\}^* \rightarrow \{0,1\}^l, 1 \le i \le 5$	암호학적 해쉬 함수 (예, SHA-1)
$Ticket_B$	사용자 A가 서버 B의 서비스를 받기 위한 커버로스 티켓

Ⅲ. 다중 영역에서의 커버로스 인증 시스템

커버로스는 대칭키 암호를 이용한 인증 시스템으로 MIT의 Athena 프로젝트의 일부로써 개발되었다[15].

커버로스 시스템은 사용자와 응용서버 S 간의 세션 키 분배가 인증 서버(AS:authentication server)와 티켓 승인 서버(TGS:ticket granting server)가 포함된 커버로스 서버의 개입으로 인해 수행된다. 완전 서비스(full service)를 제공하는 커버로스 시스템은 다중 영역에서의 인증을 제공한다. 이 단락에서는 다중 영역에서의 커버로스 시스템에 대해서 간략히 살펴본다. 그리고 커버로스 시스템의 변형인, Fake Ticket Protocol이라 불리는 효율적인 다중 영역 인증 프로토콜도 살펴본다. 이 인증 프로토콜은 효율적인 다중 영역 프레임워크를 제공하며, 여러 영역간의 전송 복잡도를 줄였다.

3.1 다중영역에서의 Kerberos 인증 시스템

먼저 다중 영역 환경에서의 커버로스 인증시스템을 살펴본다. 다중 영역 환경은 영역 A에 속한 사용자 Alice가 영역 B에 속하는 응용서버 S의 접근을 가능하게 한다. 다중 영역에서의 커버로스 인증 시스템의 자세한 기술은 [그림 1]에 나타내었다. 단계 (1)에서 Alice는 자신이 속한 인증 서버 AS_A에게 TGT_A를 요청한다. Alice의 요구를 받은 AS_A는 Alice에게 TGS_A에 접근할 수 있는 TGT_A를 단계 (2)에서 발급한다. 단계 (3)에서 Alice는 TGS_A에게 TGS_B와 통신에 사용되는 TGT_B를 요청한다. TGT_A를 검증 후, TGS_A는 $K_{TGS_A,\,TGS_B}$로 암호화된 TGT_B를 Alice에게 발행한다. TGT_B를 가진 Alice는 TGS_B에게 티켓을 요청하고, TGS_B는 응용서버 S와 통신할 티켓을 발행한다.

[그림 1] 다중영역에서의 커버로스 인증 시스템

(1) $Alice \rightarrow AS_A$	: ID_A
(2) $AS_A \rightarrow Alice$	: $TGT_A, E_{K_A}(K_{A,TGS_A}, T)$
(3) $Alice \rightarrow TGS_A$	: $ID_A, ID_S, TGT_A, E_{K_{A,TGS_A}}(T)$
(4) $TGS_A \rightarrow Alice$	: $TGT_B, E_{K_{A,TGS_A}}(T, K_{A,TGS_B})$
(5) $Alice \rightarrow TGS_B$	: $ID_A, TGT_B, E_{K_{A,TGS_B}}(T)$
(6) $TGS_B \rightarrow Alice$	: $Ticket_S, E_{K_{A,TGS_B}}(K_{A,S}, T)$
(7) Alice $\rightarrow$ S	: $ID_A, Ticket_S, E_{K,S}(T)$

각 영역은 인증서버(AS)와 티켓 승인 서버(TGS)로 구성되어 있다. TGT_A는 Alice가 TGS_A에 접근하기 위해 사용되는 티켓이다. K_A와 K_B는 Alice와 AS_A, 서버 S와 AS_B 간에 각각 공유된 대칭키이다. T는 재생공격을 방지하는 타임스탬프이다. 나머지 표기는 다음과 같다.

$TGT_A = E_{K_{TGS_A,AS_A}}(ID_A, K_{A,TGS_A})$
$TGT_B = E_{K_{TGS_A,TGS_B}}(ID_A, K_{A,TGS_B})$
$Ticket_S = E_{K_S}(ID_A, ID_S, K_{A,S}, L)$

3.2 Fake Ticket 프로토콜[5]

Cresenzo와 Kornievskaia는 다른 영역에 있는 Alice와 Bob사이의 효율적인 다중영역 인증 프로토콜, Fake Ticket Protocol을 제안했다[10]. 이 스킴은 커버로스 인증 시스템의 변형으로써, 그 인증과정을 간략히 살펴보면 다음과 같다([그림 2]).

로긴 단계에서 Alice는 KDC_A로부터 TGT_A를 얻는다. TGT_A를 가진 Alice는 KDC_A에게 서비스 티켓을 요청하면, 메세지 (4)에서 KDC는 랜덤한 세션 키, $K_{A,B}$를 생성해서, 훼이크(fake) 티켓(FTKT)을 Alice에게 발급한다. 메세지 (5)에서 Alice는 받은 FTKT를 Bob에게 전달한다. 메세지 (8)에서는 FTKT를 가진 Bob이 KDC_B에게 티켓(TKT)을 요청하고, KDC_B는 Alice와 통신에 사용될 TKT를 Bob에게 발급한다. 나머지 부분은 다중영역의 커버로스 인증 시스템과 동일하다.

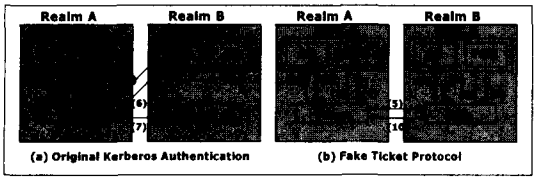
영역간의 통신 시 인터넷 서비스가 사용되고, 영역내의 통신 시 인트라넷 서비스가 사용된다고 가정했을 때, 인터넷 통신 속도가 인트라넷 통신 속도보다

[그림 2] Fake Ticket Protocol.

I. Alice의 KDC_A 로긴 단계	
(1) $Alice \rightarrow KDC_A$	: ID_A
(2) $KDC_A \rightarrow Alice$	: $TGT_A, E_{K_A}(K_{A,TGS_A}, T)$
II. FTKT 발행 단계	
(3) $Alice \rightarrow TGS_A$	: $ID_A, ID_B, TGT_A, E_{K_{A,TGS}}(T)$
(4) $TGS_A \rightarrow Alice$	: $FTKT, E_{K_{A,TGS}}(T, K_{A,B})$
(5) $Alice \rightarrow Bob$	: $ID_A, FTKT, E_{K_{A,B}}(T)$
III. Bob의 KDC 로긴 단계	
(6) $Bob \rightarrow KDC_B$	: ID_B
(7) $KDC_B \rightarrow Bob$	: $TGT_B, E_{K_B}(K_{B,TGS_B}(T))$
IV. Real Ticket 발행 단계	
(8) $Bob \rightarrow TGS_B$	: $FTKT, TGT_B, E_{K_{B,TGS}}(T)$
(9) $TGS_B \rightarrow Bob$	: $TKT, E_{K_{B,TGS_B}}(T)$
(10) $Bob \rightarrow Alice$	: $TKT, E_{K_{A,B}}(T, H_1(TKT))$

기호 $K_{X,Y}$는 개체 X와 Y사이에 공유하는 대칭키를 의미한다. 기본적인 표기 원칙은 [그림 1]과 동일하다. 나머지 표기는 다음과 같다.

$TGT_A = E_{K_{TGS,AS}}(ID_A, K_{A,TGS_A})$
$TGT_B = E_{K_{TGS_B,AS_B}}(ID_B, K_{B,TGS_B})$
$TKT = E_{K_B}(ID_A, ID_B, K_{A,B}, L)$
$FTKT = E_{K_{TGS,TGS_B}}(ID_A, K_{A,B})$



〔그림 3〕 커버로스 시스템과 Fake Ticket Protocol의 일반적인 도식

더 느리기 때문에, 영역간의 통신 량을 줄이는 일은 의미 있는 일이라 할 수 있다. [그림 3]에서 보듯이 원래 커버로스 인증 시스템은 영역간 인증 시 3번의 통신량(flow)을 요하는 반면에, Fake Ticket Protocol에서는 2번의 통신 량을 요한다. 또한 영역 B에 있는 다른 사용자와 통신하려 할 때에도 Fake Ticket Protocol은, 다중영역에서의 커버로스 시스템과는 달리, 영역 B의 TGS를 거치지 않으므로 보다 적은 영역간의 통신량을 요한다.

Ⅳ. 다중 환경에서의 C2C-PAKE

본 장에서는 새로운 사용자간의 패스워드 인증 키 교환 프로토콜인 다중 영역환경에서의 C2C-PAKE를 제안한다. 제안된 스킴은 Fake Ticket Protocol의 프레임워크를 기반으로 하여 구축되어진다. 분산된 환경에서, 서버 KDC_A가 Alice와 Bob사이의 세션 키 공유 시 항상 참여한다는 것은 비효율적이다. 제안된 스킴은 티켓 구조를 사용함으로써, 오픈 네트워크 상에서 KDC_A의 개입을 가능한 줄였다. $Ticket_B$를 사용하여, Alice는 KDC_A의 개입 없이 오직 암기 가능한 패스워드를 이용하여 세션 키를 형성할 수 있다.

4.1 프로토콜 기술

[그림 4]에서 기술된 C2C-PAKE 는 크게 두 단계로 나누어진다. 첫 단계는 티켓 발행 단계이고((1)-(2)), 나머지 단계는 상호 인증과 세션키 형성 단계((3)-(8))이다. 먼저, KDC_A는 티켓 발행 단계에서 $Ticket_B$를 발행한다. 티켓은 미리 발행되고, 유효기간을 포함하고 있으므로 KDC_A는 모든 세션 키 형성과정에 참여할 필요가 없다. Alice는 Bob과 세션 키를 형성하기를 원할 때, 유효기간 L 이내에 발행 받은 티켓을 이용하여 공통의 세션 키를 얻을 수 있다.

[프로토콜 초기화]

프로토콜 실행을 위한 준비 단계는 다음과 같다.

1. g, p와 q는 프로토콜 참여자들에 의해 공유되는 광역(global) 파라미터이다.
2. Alice는 패스워드 pwa를 선택하고, 자신의 서버 KDC_A에게 안전한 채널을 이용하여 전달한다. Bob 역시 자신의 서버 KDC_B에게 pwb 를 선택하여 전달한다. KDC_A와 KDC_B는 각각 (ID(A),pwa)와 (ID(B), pwb)를 저장한다.

[프로토콜 설명]

KDC_A와 KDC_B는 공개키 암호 방법을 이용하여 안전하게 대칭 키 K를 공유한다고 가정한다. 그 대표적인 방법으로 PKCROSS가 있다[16]. 패스워드, pwa로 암호화 함은 pwa가 일방향 함수에 의해서 1비트의 크기로 변형되어 암호화됨을 의미한다. 또한 pwa가 지수승에 사용됨은 q의 치역을 갖는 일방향 함수에 의해 변형되어 사용됨을 의미한다.

(1) Alice는 랜덤하게 $x \in Z_q$를 선택한 다음, $E_{pwa}(g^x)$를 계산하여 KDC_A에게 ID_A, ID_B와 함께 보낸다.

(2) KDC_A는 $E_{pwa}(g^x)$를 복호화 하여, g^x를 얻는다. 그리고 $y, r \in Z_q$을 랜덤 하게 선택해서 $g^{pwa \cdot r}$과 $E_{pwa}(g^y)$를 계산한다. 또한 티켓의 유효기간, L을 정한 다음, KDC_A는 티켓($Ticket_B$)을 만들어, $E_{pwa}(g^y)$, $E_R(g^{xy} \oplus g^r, ID_A, ID_B, L)$, $Ticket_B$,를 Alice에게 전달한다. KDC로부터 이 메시지를 받은 Alice는 세션 키 $R(=H_1(g^{xy}))$을 계산할 수 있으며, $E_R(g^{xy} \oplus g^r, ID(A), ID(B))$를 복호화 해서, g^r을 구할 수 있다.

(3) Alice는 $Ticket_B$를 Bob에게 전달한다.

(4) Bob은 $x' \in Z_q$를 선택하고, $E_{pwb}(g^{x'})$를 계산한다. 그리고 KDC_B에게 $Ticket_B$와 함께, ID_A, ID_B, $E_{pwb}(g^{x'})$를 전달한다.

(5) KDC_B는 $Ticket_B$를 복호화하여, $g^{pwa \cdot r}$을 얻을 수 있으며, 또한 $r' \in Z_q$을 랜덤하게 선택하여 $g^{pwa \cdot r \cdot r'}$를 계산한다. KDC_B는 또 하나의 랜덤 값 $y' \in Z_q$를 선택하여 $R'(=H_2(g^{x'y'}))$를 계산한 다음, $E_{R'}(g^{pwa \cdot r \cdot r'} \oplus g^{x'y'}, ID_A, ID_B)$를 만들어 $E_{pwb}(g^{y'})$, $E_{H_1(g^{pwa \cdot r})}(g^{pwb \cdot r \cdot r'})$와 함께 Bob에게 전달한다.

(6) Bob은 $E_{pwb}(g^{y'})$을 복호화 하여, $g^{y'}$를 얻어서 R'를 계산 할 수 있으며, R'를 이용하여 $E_{R'}(g^{pwa \cdot r \cdot r'} \oplus g^{x'y'}, ID_A, ID_B)$를 복호화 한다. Bob은 궁극적으로 $g^{pwa \cdot r \cdot r'}$를 얻을 수 있으며,

$cs(=H_5(g^{pwa\cdot pwb\cdot r\cdot r'}))$를 만들 수 있다. Bob은 새로운 랜덤 값 $a\in Z_q$를 만들어 낸 다음, $E_{cs}(g^a)$를 계산하여, $E_{H_4(g^{pwa\cdot r})}(g^{pwb\cdot r\cdot r'})$와 함께 Alice에게 보낸다.

(7) Alice는 $H_4(g^{pwa\cdot r})$를 자신의 pwa와 g^r을 이용하여 만들어 낸다. 그리고 Alice는 이를 이용하여 $E_{H_4(g^{pwa\cdot r})}(g^{pwb\cdot r\cdot r'})$를 복호화 해 낼 수 있으며, $g^{pwb\cdot r\cdot r'}$를 얻는다. 또한 Bob과 마찬가지로 $g^{pwb\cdot r\cdot r'}$를 이용해, cs값을 계산할 수 있다. 마지막으로 랜덤 값 $b\in Z_q$를 선택하여, $sk(=H_3(g^{ab}))$를 만들어 낸다. Bob에게 세션 키 확인을 위해 $E_{cs}(g^b)$, $E_{sk}(g^a)$를 보낸다.

(8) $E_{cs}(g^b)$, $E_{sk}(g^a)$를 받은 후, Bob은 g^b를 얻을 수 있으며, 자신이 선택한 랜덤 값 a를 이용하여 세션 키 $sk(=H_3(g^{ab}))$를 형성한다. Bob은 세션 키 확인을 위해, $E_{sk}(g^b)$를 Alice에게 보낸다. 이를 받은 Alice는 자신의 세션 키로 g^b를 확인함으로써 세션 키 확인을 마친다.

〔그림 4〕 다중환경에서의 C2C-PAKE

I. 티켓 발행 단계

(1) $Alice \rightarrow KDC_A$: $ID_A, ID_B, E_{pwa}(g^x)$

(2) $KDC_A \rightarrow Alice$: $E_R(g^{xy}\oplus g^r, ID_A, ID_B, L)$ $E_{pwa}(g^y), Ticket_B$

II. 상호 인증 및 세션 키 형성 단계

(3) $Alice \rightarrow Bob$: $Ticket_B, ID_A, L$

(4) $Bob \rightarrow KDC_B$: $Ticket_B, E_{pwb}(g^{x'}), ID_A$ ID_B, L

(5) $KDC_B \rightarrow Bob$: $E_R(g^{pwa\cdot r\cdot r'}\oplus g^{x'y'}, ID_A, ID_B)$ $E_{H_4(g^{pwa\cdot r})}(g^{pwb\cdot r\cdot r'}), E_{pwb}(g^{y'})$

(6) $Bob \rightarrow Alice$: $E_{cs}(g^a), E_{H_4(g^{pwa\cdot r})}(g^{pwb\cdot r\cdot r'})$

(7) $Alice \rightarrow Bob$: $E_{sk}(g^a), E_{cs}(g^b)$

(8) $Bob \rightarrow Alice$: $E_{sk}(g^b)$

기본적인 표기 원칙은 [그림 1]과 동일하다. R과 R'와 sk는 각각 Alice와 KDC_A, Bob과 KDC_B 그리고 Alice와 Bob사이에 공유되는 세션 키이다. K는 KDC_A와 KDC_B사이에 공유되는 대칭 키이다. 티켓은, $Ticket_B = E_K(g^{pwa\cdot r}, g^r, ID(A), ID(B), L)$로 표시한다.

[티켓의 재사용]

Alice는 유효기간 안에 티켓을 재 사용할 수 있다. 티켓인, $Ticket_B$를 소유한 Alice는, 자신의 영역에 속한 KDC_A의 접속을 거치지 않고 또한 영역간의 전송량을 줄이면서, Bob에게 $Ticket_B$를 전달한다. 이 과정을 통해 Alice는 Bob과 궁극적인 세션 키 sk를 공유하게 된다. 그 과정은 **(3)-(8)**과정을 따른다.

4.2 C2C-PAKE의 안전성 분석

본 단락에서는 제안된 다중 영역 환경에서의 C2C-PAKE 스킴이 새롭게 정의된 공격들에 대해 안전함을 보인다. 공격자 E는 확률적 다항식 시간인 $E(1^k,m)$로 표현된다.(단, 1^k는 안전성 파라미터이고, m은 공격자에게 주어지는 유용한 정보이다.) 또한 공격자 E는 이산대수 문제와 Diffie-Hellman 문제를 푸는 것이 불가능하다라고 가정한다. 그러므로 어떠한 (some) negligible 함수 $\epsilon(k)$에 대해 $\Pr[Forge_{DLP}(k)]$, $\Pr[Forge_{DHP}(k)]\le\epsilon(k)$라고 할 수 있다.

■ DPA 모델에서의 perfect forward secrecy.

$Adv_E^{P/S}$를 공격자가 C2C-PAKE를 DPA 모델에서 perfect forward secrecy를 공격하는 이점이라 했을 때, $Adv_E^{P/S}\le\Pr[Forge_{DHP}(k)]$임을 보인다.

(경우 1)

공격자 E에게 pwa가 주어진다고 가정하자. $E(1^k,pwa)$는 $E_{pwa}(g^x), E_{pwa}(g^y)$를 복호화해서, g^x, g^y를 구할 수 있다. 하지만 g^x, g^y를 가진 $E(1^k,pwa, g^x, g^y)$는 Diffile-Hellman 문제를 풀 수 없으므로 여전히 $R(=H_1(g^{xy}))$을 결정할 수 없다. 만약 E에게 R까지 주어진다면, 공격자는 cs를 얻을 수 있고, g^a, g^b를 얻을 수 있다. 하지만, $E(1^k,pwa, g^x, g^y, g^a, g^b R, cs)$는 DHA를 깨지 못하는 한 여전히 $sk(=H_3(g^{ab}))$를 구할 수 없다. 그러므로 공격자의 perfect forward secrecy에 대한 이점은 $\Pr[Forge_{DHP}(k)]$에 의해 결정되어진다. 프로토콜 내의 모든 세션 키들은 DHA에 기반하고 있으므로, 이 결과는 자연스럽다.

(경우 2)

공격자 E에게 pwb가 주어진다고 가정했을 때, 경우 1과 마찬가지로, 공격자는 $g^{x'}, g^{y'}$를 얻을 수 있지만, R'를 얻을 수 없다. 또한 공격자에게 R'까지 주어질지라도, $E(1^k,pwa, g^x, g^y, g^a, g^b, R', cs)$는 DHA를 깨지 못하는 한 세션 키 sk를 구할 수 없다.

(경우 3)

공격자에게 pwa, pwb 모두 주어졌다고 가정했을

때도 경우 1과 경우 2와 동일하게 적용된다. 즉, $E(1^k, pwa, pwb, g^x, g^y, g^a, g^b, R, R', cs)$가 $sk(=H_3(g^{ab}))$를 구하는 것은 DHA를 깨는 것과 같다.

경우 1,2,3에 의해서 $Adv_E^{P/S} \le \Pr[Forge_{DHP}(k)]$임을 보였다. ■

■ DPA 모델에서의 Denning-Sacco 공격

$Adv_E^{P/S}$를 DPA 모델에서 공격자가 Denning -Sacco 공격을 하게 되는 이점이라 가정했을 때, $Adv_E^{D/S} \le \varepsilon(k)$임을 보인다. 공격자를 두 가지의 형태로 분류하는데, 하나는 외부(outsider) 공격자이고, 또 하나는 내부(insider) 공격자이다. 외부 공격자는 pwa나 pwb를 얻지 못하는 공격자이며, 내부 공격자는 둘 중 하나를 가지고 있는, 시스템에 등록된 정당한 사용자이다.(예, Alice 혹은 Bob)

(경우 1) 외부 공격자 $E(1^k, R, sk, R')$.

패스워드가 아닌, R, sk, R'를 얻은 외부 공격자를 가정했을 때, 공격자는 $ID_A, ID_B, L, g^{xy} \oplus g^r, g^a, g^b$를 위의 정보를 이용하여 얻을 수 있다. 하지만, 이러한 정보는 공격자에게 pwb 혹은 pwa를 사전 공격하는데, 아무런 도움을 주지 못한다. 공격자가 선택한 패스워드 pwa', pwb'검증하기 위해서는 $g^x, g^y, g^{x'}, g^{y'}$를 얻어야 한다. 하지만 x, y, x', y'값은 매 세션 마다 선택되어지는 랜덤 한 값이므로, 이 값을 추측할 확률에 의존하여 사전 공격이 가능하게 되고, 이 확률이 공격자 E의 Dennig-Sacco 공격의 이점으로 결정되어진다. 그러므로 $Adv_E^{D/S} \le 1/q$이며, 이는 곧 $Adv_E^{D/S} \le \varepsilon(k)$이다.(단, p는 충분히 큰 소수)

(경우 2) 내부 공격자 $E(1^k, pwa, R, sk, R')$

pwa를 알고 있는 정당한 사용자 A에게 R, sk, R'가 주어졌다고 가정하자. pwa, R, sk, R'를 지닌 정당한 내부 공격자가 pwb에 대한 사전공격이 불가능함을 보이려 한다. 먼저, E는 R'를 이용하여 $g^{pwa \cdot r \cdot r'} \oplus g^{x'y'}$를 얻을 수 있다. 하지만, E는 해쉬함수의 일방향 성질에 의해 $R'(=H_2(g^{x'y'}))$에서 $g^{x'y'}$를 얻을 수 없으므로, $g^{pwa \cdot r \cdot r'}$를 구할 수 없다. $g^{pwa \cdot r \cdot r'}$는 아주 중요한 의미를 지니는 값으로, 만약 내부 공격자에게 $g^{x'y'}$값이 알려져서, $g^{pwa \cdot r \cdot r'}$값을 구할 수 있게 된다면, 다음과 같은 방법으로 인해 pwa에 대한 사전공격이 가능하게 된다.

(단계 1)

E는 pwa와 $g^{pwa \cdot r \cdot r'}$를 이용하여, $g^{r \cdot r'}$를 얻어낸다.

(단계 2)

E는 pwa와 g^r을 이용하여 $g^{pwb \cdot r \cdot r'}$ 값을 $E_{H_4(g^{pwa \cdot r})}(g^{pwb \cdot r \cdot r'})$의 복호화로 인해 얻어낸다.

(단계 3)

공격자는 pwb에 대한 후보 패스워드 pwb'를 선택한 다음, $g^{pwb' \cdot r \cdot r'}$를 계산한 다음, 이 값을 $g^{pwb \cdot r \cdot r'}$와 비교한다. 결국에는 두 값의 비교작업을 통해, pwb에 대한 후보 패스워드 사이즈의 크기를 줄 일 수 있으므로, 사전공격이 가능하다. 즉, 사전공격에 안전하기 위해서는 $g^{pwb \cdot r \cdot r'}$값을 $g^{x'y'}$에 의한 블라인드(blind) 과정을 거쳐야 한다. $g^{x'y'}$를 추측할 확률만큼, 사전 공격을 가능하게 하므로, 이 확률이 Denning-Sacco 공격의 이점을 결정한다. 그러므로 $Adv_E^{D/S} \le 1/q$이다. (단, p는 충분히 큰 소수)

(경우 3) 내부 공격자 $E(1^k, pwb, R, sk, R')$

공격자 E가 pwb를 가지고 있는 정당한 공격자라고 가정하자. 공격자 E에게 R, sk, R'를 주어져도 pwa에 대한 사전공격이 불가능함을 보이려 한다. 먼저, E는 R을 이용하여 $g^{xy} \oplus g^r$를 얻을 수 있다. 하지만 E는 g^{xy} 값을 모르기 때문에, g^r 값을 얻을 수 없다. 만약 공격자 E가 g^{xy}를 추측해서, g^r값을 구할 수 있다면, 다음과 같은 방법으로 인해, pwa에 대한 사전공격이 가능하게 된다.

(단계 1)

공격자는 R과 g^{xy}를 알고 있기 때문에 $E_R(g^{xy} \oplus g^r)$를 복호화 하여 g^r을 얻는다.

(단계 2)

공격자는 $E_{R'}(g^{pwa \cdot r \cdot r'} \oplus g^{x'y'})$를 복호화 할 수 있으며, $g^{x'y'}$를 이용하여, $g^{pwa \cdot r \cdot r'}$를 계산해 낼 수 있다.

(단계 3)

E는 pwa에 대한 후보 pwa'를 선택하여 $H_4(g^{pwa' \cdot r})$를 계산한 후, $E_{H_4(g^{pwa' \cdot r})}(g^{pwb \cdot r \cdot r'})$를 복호화 해서, 어떤 r_1, r_2에 대한 $g^{pwb \cdot r_1 \cdot r_2}$를 구할 수 있다. 공격자는 $g^{pwb \cdot r_1 \cdot r_2}$에서 pwb를 제거할 수 있으며, $g^{r_1 \cdot r_2}$

에서 선택한 pwa'를 지수 승하여, $g^{pwa' \cdot r_1 \cdot r_2}$를 계산한 다음 단계 2에서의 $g^{pwa \cdot r \cdot r'}$와 비교함으로써 사전 공격을 수행할 수 있다. 즉, 두 값이 일치하면, pwa'가 pwa이므로 추측이 성공한 것이고, 다른 경우는 해당 패스워드 사전 크기를 줄 일 수 있다. 그러므로 g^r를 적절히 블라인드(blind)하는 과정은 필수적이다. 공격자는 g^{xy}를 추측하는 확률로 g^r을 구할 수 있으며, 이 확률이 이 경우의 Denning-sacco 공격의 이점을 결정한다. 정의에 나타난 사용자를 가장하는 문제는 a, b가 항상 랜덤 하게 뽑아져서 세션 키 확인 과정이 수행되므로 이전 세션 키를 이용하여 이후 세션에서 이용할 수 없다.

경우 1,2,3에 의해서 $Adv_E^{D/S} \leq \Pr[Forge_{DHP}(k)]$임을 보였다. ■

■ DPA 모델에서의 사전 공격.

$Adv_E^{D/A}$를 공격자 E가 DPA 모델에서 사전 공격을 수행 할 이점이라 했을 때, $Adv_E^{D/A} \leq \varepsilon(k)$임을 보이려 한다. 분석은 Denning-Sacco 공격과 유사하며, 내부 공격자와 외부 공격자의 두 가지 경우로 나누어서 분석한다.

(경우 1) 외부공격자의 경우

사전공격의 외부공격자라 함은 pwa 혹은 pwb를 소유하지 않고 프로토콜의 전송 내용만을 보고 pwa, pwb에 대한 사전공격을 수행하려 하는 공격자를 의미한다. 그러므로 외부 공격자가 세션 키들을 획득할 수 없음을 가정한다. 각각의 패스워드는 $g^x, g^y, g^{x'}, g^{y'}$를 암호화한다. x, y, x', y' 은 Z_q에서 랜덤 하게 뽑혀지는 값이므로 사전공격이 가능할 확률은 이 값을 추측할 정도의 이점을 가진다. 나머지 프로토콜의 전송내용은 공격자가 세션 키를 획득할 수 없으므로 사전공격에 아무런 도움을 주지 못한다. 만약 q가 충분히 큰 소수라면, 외부공격자의 사전공격의 가능성은 무시할 수 있는 이점을 가진다.

(경우 2) 내부공격자의 경우

사전공격의 내부공격자라 함은 pwa 혹은 pwb 중 하나의 패스워드만을 알고 다른 패스워드에 대한 사전공격을 수행하려 하는 공격자를 의미한다. 경우 1과 마찬가지로 내부공격자의 세션 키 소유의 문제는 가정하지 않는다. 공격자의 능력을 세션 키의 획득까지 포함한 안전성 분석은 DPA 모델에서의 Denning-Sacco 공격을 참조한다. 경우 2는 오직 pwa를 소유한 공격자와 pwb를 소유한 공격자로 다시 나눌 수 있다. 먼저 pwa를 소유한 공격자는 세션 키 R 정보를 알지 못하는 한 pwb에 대한 사전공격에 관한 아무런 자료를 얻지 못한다. 비록 세션 키 R을 얻더라도 DPA 모델에서의 Denning-Sacco 공격에서 분석하였듯이 사전공격은 불가능하다. 그러므로 pwa를 소유한 내부 공격자는 x'을 추측할 확률로 사전공격의 이점을 결정짓게 된다. 이는 경우 1에서 분석하였듯이 무시할 수 있는 확률을 가진다. pwb를 소유한 내부 공격자의 경우, 역시 위의 분석 내용과 동일하게 적용되어진다.

경우 1,2에 의해서, $Adv_E^{D/A}$가 negligible함을 알 수 있다. ■

■ 온라인 추측 공격.

이 공격은 로그인 실패 횟수를 정함으로써 막을 수 있다. 하지만, 공격자의 입장에서 보면, 실패 횟수 만큼 패스워드 사전 크기를 좀 더 줄일 수 있다. 그러므로 서버가 횟수 R만큼 거부(reject) 했을 때, 공격자가 패스워드를 추측할 수 있는 확률은 $1/|D| - R$ 이다. ■

■ 중간 공격 및 재생 공격.

중간 공격(man-in-the-middle attack)은 공격자 E가 양쪽 개체를 합법적으로 가장하거나, 혹은 속이는(fool) 공격을 의미한다. 공격자 E는 프로토콜 내의 모든 대화내용(conversation)을 이용하더라도, pwa 혹은 pwb를 모르는 한, 세션 키 확인 과정을 통과하지 못한다. 양쪽 개체를 합법적으로 가장하기 위해서는 pwa 혹은 pwb를 아는 사용자만이 가능하다. 재생 공격(replay attack)은 이전에 사용됐던 대화내용 등을 이용하여, 다음 세션에 사용하여, 성공적으로 사용자를 가장하거나, 키 확인 과정을 통과하는 공격을 의미한다. 하지만, 모든 메시지들은 매 세션마다 랜덤(random) 혹은 즉시적(ephemeral)으로 만들어지기 때문에, 공격자의 이 공격에 대해서 얻을 수 있는 이점은 negligible 하다.

위의 분석에 의해서, 다음과 같은 결론을 내릴 수 있다.

$$Adv_E^{DPA}(k) < O(1/|D| - R) + Adv_E^{F/S}(k) + Adv_E^{D/S}(k) + Adv_E^{D/A}(k) + \varepsilon(k)$$

온 라인 추측 공격은 패스워드 인증 키 교환 프로토콜에서 피할 수 없는 공격이다. 그러므로 이 이점이 공격자가 DPA 모델에서 C2C-PAKE 프로토콜을 공격함에 있어서, 성공 확률의 하한 값이 되어야 한다. 본 절에서 $Adv_E^{F/S}(k), Adv_E^{D/S}(k), Adv_E^{D/A}(k)$가 negligible함을 보였기 때문에, C2C-PAKE는 II장의 안전성 정의를 만족한다. ■

V. 단일 서버환경에서의 C2C-PAKE

본 장에서는 단일 서버 환경에서 C2C-PAKE 스킴을 살펴본다. 단일 서버 환경은, II장에서 설명하였듯이, 동일한 서버내의 다른 사용자간의 패스워드 인증 키 교환을 제공한다. 본 단락에서는 더 나아가 단일 서버환경을 단일 서버 티켓 환경과 단일 서버 티켓리스(ticketless) 환경으로 나눈다. 먼저 단일 서버 티켓리스 환경에서의 C2C-PAKE를 소개한다.

5.1 단일 서버 티켓리스 환경에서의 C2C-PAKE

3-Party EKE[11]는 단일 서버 티켓리스 환경으로 분리되는 스킴으로, 각 사용자는 자신의 패스워드를 이용하여 제 삼의 신뢰기관(KDC)과 통신함으로 사용자간의 패스워드 인증된 키 교환 프로토콜을 제공한다. 다음의 [그림 5]는 3-Party EKE의 변형으로써, 그 구조가 간단하다.

[그림 5]에서 보듯이, KDC는 패스워드를 오직 저장하고 있는 전달 센터의 역할을 한다. Alice가 동일한 KDC에 등록된 Bob과 통신하기를 원할 때, Alice는 $E_{pwa}(g^a)$를 KDC에게 전달한다. KDC는 pwa를 알고 있기 때문에, 복호화 해서, g^a를 얻는다. 랜덤 값, $s \in Z_q$를 선택하여, $E_{pwb}(g^{a \cdot s})$를 계산한 다음, Bob에게 전달한다. Bob은 $b \in Z_q$를 선택하여 $sk(=H_1(g^{abs}))$를 계산한다. 또한 Bob은 $E_{pwb}(g^b)$를 KDC에게 보내면, KDC는 s값을 적용하여, $E_{pwa}(g^{b \cdot s})$를 Alice에게 전달한다. Alice 역시 Bob과 마찬가지로 세션 키, $sk(=H_1(g^{abs}))$를 계산한다. [그림 5]는 패스워드를 이용한 키 교환만을 제공하고, 형성된 세션 키에 대한 키 확인 과정은 포함하지 않고 있다. 하지만 프로토콜에 추가적인 세션 키 확인 절차를 첨가시킴으로써, 이를 설계할 수 있다.

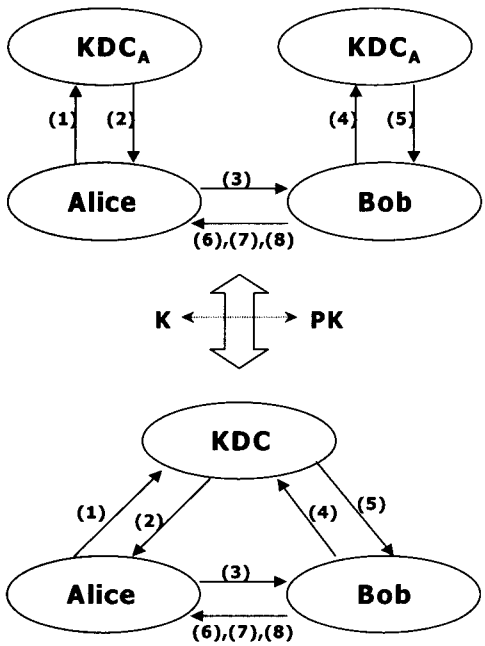
[그림 5] 단일서버 티켓리스 환경에서의 C2C-PAKE

(1) $Alice \rightarrow KDC$	: $ID(A), ID(B), E_{pwa}(g^a)$
(2) $KDC \rightarrow Bob$	: $ID(B), E_{pwb}(g^{a \cdot s})$
(3) $Bob \rightarrow KDC$	: $ID(A), E_{pwb}(g^b)$
(4) $KDC \rightarrow Alice$	: $ID(A), E_{pwa}(g^{b \cdot s})$

단일 서버 티켓 리스 환경은 [그림 5]를 비롯해서, 3-Party EKE를 변형한 많은 스킴 들이 존재 할 수 있다.

5.2 단일 서버 티켓 환경에서의 C2C-PAKE

본 장에서는 다중 서버 환경에서의 C2C-PAKE 스킴을 이용하여 단일 서버에서의 C2C-PAKE 스킴을 소개한다. 단일 서버 티켓 환경에서의 C2C-PAKE는 다중영역의 C2C-PAKE를 변형함으로써, 쉽게 구축할 수 있다. 다중영역의 C2C-PAKE는 커버로스 영역간의 안전한 통신을 위해 대칭 키, K를 안전한 공개키 방식으로 공유한다. [그림 6]에서 보듯이, 이러한 사전 대칭키 K를 KDC의 개인 키(PK)로 변환함으로써, 단일 서버 티켓 환경의 C2C-PAKE를 구축한다. 티켓의 구조가 PK를 사용하여 암호화 한 형태인 $Ticket_B = E_{PK}(g^{pwa \cdot r}, g^r, ID(A), ID(B), L)$ 인 점을 제외하고 나머지 부분은 다중 서버 환경에서의 C2C-PAKE 구조와 동일하다. 단, K와 마찬가지로 PK도 항상 안전하게 보관됨을 가정한다.



[그림 6] 단일서버 티켓리스 환경에서의 C2C-PAKE

V. 결 론

본 논문에서는 서로 다른 패스워드를 가지는 사용자간의 패스워드 인증 키 교환 프로토콜을 다중영역 환경과 단일 서버 환경으로 나누어서 각각 제안하였다. 패스워드 기반 프로토콜 설계의 가장 큰 어려움은 패스워드에 대한 사전공격 뿐 아니라, 잘 알려진 공격들에 대한 안전성을 보장해야 한다는 것이다. 본 논문은 잘 알려진 두 가지 가정(DHA, DLA)을 기반으로 하여 안전하고 효율적인 C2C-PAKE 프로토콜을 설계하였다.

제안된 스킴은 사용자간의 암기 가능한 서로 다른 패스워드를 가지고, 안전한 채널을 형성하기를 원하는 유·무선 모든 환경에 적용되어져 사용 될 수 있다.

참 고 문 헌

[1] S. Bellovin and M. Merrit, "Encrypted key exchange: password based protocols secure against dictionary attacks", In Proceedings of the Symposium on Security and Privacy, pp. 72~84, IEEE, 1992.

[2] S. Lucks, "Open key exchange: How to defeat dictionary attacks without encryting public keys", The security Protocol Workshop '97, pp. 79~90, 1997.

[3] T. Wu, "Secure Remote Password Protocol", In Proceedings of the Internet Society Network and Distributed System Security Symposium, pp. 97~111, 1998.

[4] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks", Eurocrypt'00, LNCS, Vol. 1807, pp. 139~155, Springer-Verlag, 2000.

[5] V. Boyko, P. MacKenzie, and S. Patel, "Provably Secure Password-Authentica ted Key Exchange Using Diffie-Hellman", Eurocrypt'00, LNCS Vol. 1807, pp. 156~171, Springer-Verlag, 2000.

[6] J. Katz, R. Ostrovsky and M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords", Eurocrypt'01, LNCS, Vol. 2045, pp. 475~494, Springer-Verlag, 2001.

[7] O. Goldreich and Y. Lindell, "Session-Key Generation Using Human Passwords Only", Crypto'01, LNCS Vol. 2139, pp. 408~432, Springer-Verlag, 2001.

[8] V. Varadharajan and Y. Mu, "On the Design of Security Protocols for Mobile Communications", In Proceedings of Twelfth Annual Computer Security Applications Conference, pp. 78~87. IEEE Computer Society Press, 1996.

[9] C. Boyd and A. Mathuria, "Key establishment protocols for secure mobile communications : A selective survey", ACISP'98, LNCS, Vol. 1438, pp. 344~355, Springer-Verlag, 1998.

[10] G. D. Crescenzo and O. Kornievskaia, "Efficient kerberized multicast in a practical distributed setting", ISC'01, LNCS, Vol. 2200, pp. 27~45, Springer-Verlag, 2001.

[11] M. Steiner, G. Tsudik, and M. Waider, "Refinement and extension of encrypted key exchange", ACM Operation Sys. Review, Vol. 29, No. 3, pp. 22~30, 1995.

[12] T. Wu, "A Real-World Analysis of Kerberos Password Security", In Proceedings of the Internet Society Network and Distributed System Security Symposium, 1999.

[13] B. Jaspan, "Dual-workfactor encrypted key exchange: Efficiency preventing password chaining attacks", In Proceedings of the sixth annual USENIX security conference, pp. 43~50, July 1996.

[14] D. Denning and G. Sacco, "Timestamps in key distribution protocols", Communications of the ACM, Vol. 24, No. 8, pp. 533~536, 1981.

[15] S. P. Miller, B. C. Neuman, J. I. Schiller, J. H.Saltzer, "Kerberos Authentication and Authorization System", Section E.2.1, Project Athena Technical Plan, M.I.T. October 1988.

[16] M. Hur, B. Tung, T. Ryutov, C. Neuman, A, Medvinsky, G. Tsudik, and B. Sommerfeld, "Pulbic key cryptography for cross-realm authentication in kerberos", Internet draft, May 2001.

〈著者紹介〉

변 진 욱 (Jin Wook Byun) 학생회원
2000년 2월 : 고려대학교 전산학과 학사
2000년 3월~현재 : 고려대학교 정보보호대학원 석사과정
<관심분야> 암호 프로토콜, 암호이론

정 익 래 (Ik Rae Jeong) 학생회원
1998년 : 고려대학교 전산학과 학사
2000년 2월 : 고려대학교 전산학과 석사
2000년 3월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 암호이론, 암호 프로토콜, 정보이론

이 동 훈 (Dong Hoon Lee) 정회원
1984년 : 고려대학교 경제학과 졸업
1987년 : Oklahoma Univ. 전산학과 석사
1992년 : Oklahoma Univ. 전산학과 박사
1993년~현재 : 고려대학교 전산학과 교수
2000년~현재 : 고려대학교 정보보호 대학원 교수
<관심분야> 암호이론, 암호 프로토콜, 정보이론