일반논문-08-13-2-09

그룹 사용자간 안전한 콘텐츠 전송을 위한 검증자를 이용한 패스워드 기반 다자간 키 교환 프로토콜

권 정 옥[a)], 정 익 래[a)], 최 재 탁[a)], 이 동 훈[a)‡]

Verifier-Based Multi-Party Password-Authenticated Key Exchange for Secure Content Transmission

Jeong Ok Kwon[a)], Ik Rae Jeong[a)], Jae Tark Choi[a)], Dong Hoon Lee[a)‡]

요 약

본 논문에서는 서로 다른 패스워드를 가지는 그룹의 구성원들이 자신의 패스워드만을 사용하여 공통된 그룹 키(세션 키)를 공유할 수 있는 패스워드의 검증자(verifier)를 이용하는 두 개의 패스워드 기반 다자간 키 교환 프로토콜을 제안한다. 공유된 키는 그룹 사용자간 안전한 콘텐츠 전송을 위해 사용될 수 있다. 제안 프로토콜들은 서버의 DB가 노출되었을 경우에 기존의 스킴들보다 강한 안전성을 제공하도록 설계되었다. 첫 번째 제안 프로토콜은 전방향 안전성(forward secrecy)과 기지 키 공격에 대한 안전성(known-key secrecy)을 제공하며, 두 번째 제안 프로토콜은 추가적으로 서버에 대한 키 기밀성(key secrecy)을 제공한다. 제안 프로토콜들은 상수 라운드를 가지며 표준 모델(standard model)에서 안전성이 증명되었다. 기존에 서버의 DB 노출공격에 안전한 패스워드 기반 다자간 그룹 키 교환 프로토콜이 제안된 적이 없으며, 본 논문에서 처음으로 제안한다.

ABSTRACT

In this paper, we present two verifier-based multi-party PAKE (password-authenticated key exchange) protocols. The shared key can be used for secure content transmission. The suggested protocols are secure against server compromise attacks. Our first protocol is designed to provide forward secrecy and security against known-key attacks. The second protocol is designed to additionally provide key secrecy against the server which means that even the server can not know the session keys of the users of a group. The suggested protocols have a constant number of rounds are provably secure in the standard model. To the best of our knowledge, the proposed protocols are the first secure multi-party PAKE protocols against server compromise attacks in the literature.

Keywords : Verifier-based group password key exchange, dictionary attack, forward secrecy, known-key secrecy

I. 서 론

1. 패스워드 기반 다자간 키 교환

인터넷과 같이 안전하지 않은 네트워크에서 안전한 통신을 하기 위해서는 세션 키(session key)를 안전하게 교환

a) 고려대학교 정보경영공학전문대학원 정보보호기술연구센터
Graduate School of Information Management & Security CIST, Korea University
‡ 교신저자 : 이동훈(donghlee@korea.ac.kr)
※ 이 연구에 참여한 연구자 중 일부는 '2단계 BK21사업'의 지원비를 받았으며 다른 일부는 '지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업 (IITA-2008-(C1090-0801-0025))'의 지원비를 받았음.

하는 것이 필수적이다. 공유된 세션 키는 기밀성(confidentiality)이나 데이터의 무결성(integrity)과 같은 안전성 목적을 이루기 위해 사용될 수 있다. 패스워드 기반 키 교환은 인간이 기억하기 쉬운 패스워드만을 사용해서 두 명 또는 그보다 많은 특정 사용자 사이에 세션 키를 공유할 수 있도록 한다. 패스워드 기반 키 교환은 사용자의 편의성과 이동성, 키 값을 저장하기 위한 저장장치를 필요로 하지 않는다는 면에서 많은 장점을 지니기 때문에 이에 대한 연구가 활발히 진행되고 있다. 특히, 패스워드 기반 다자간 (그룹) 키 교환 프로토콜은 무선 네트워크 환경과 같은 환경에서 사용될 수 있다. 예를 들면 화상 회의, 개인 네트워킹, 군사 작전, 위급 구조와 같은 안전한 그룹 통신이 필요한 무선 네트워크 환경에서는 상대적으로 적은 자원을 사용하여 효율적으로 키 교환이 이루어져야 한다. 패스워드 기반 그룹 키 교환 프로토콜은 그룹의 사용자를 인증하는 방법을 제공하고, 공개키 기반 구조(PKI: Public Key Infrastructure)와 같은 기반 구조가 마련되어 있지 않은 환경에서도 단지 패스워드만을 이용하여 암호학적으로 안전한 키를 교환할 수 있는 방법을 제공하기 때문에 무선 환경에서 적합하게 사용될 수 있다.

또한 모바일 기기는 제한된 메모리와 프로세싱 능력을 갖고 있고, 무선 네트워크는 대역폭이 제한되어 있기 때문에, 실제 무선 환경에 패스워드 기반 그룹 키 교환 프로토콜이 사용되기 위해서는 적은 라운드의 수와 계산 시간 그리고 전송되는 메시지의 크기가 작아야한다. 특히, 그룹 사용자의 수가 많거나 그룹 키가 자주 변경되어야 하는 경우에 라운드의 수는 매우 중요한 요소이다.

기존의 패스워드 기반 그룹 키 교환 기법은 그룹 구성원의 동일한 패스워드 공유를 가정한다. 하지만 그룹 구성원이 동일한 패스워드를 공유하는 경우, 각 구성원은 자신이 속한 그룹의 수만큼의 패스워드를 기억하고 있어야하는 문제가 발생한다. 이러한 문제를 해결하기 위한 방법으로 제시된 것이 서버를 이용하는 모델이다. 서버를 이용하는 모델에서는 구성원은 자신의 패스워드 하나만을 기억하면 되고, 다른 구성원과 패스워드를 공유할 필요가 없다. 단, 구성원은 자신의 패스워드를 서버에 등록을 하여야 한다. 구성원들의 패스워드를 DB에 저장하고 있는 서버는 서로 다른 패스워드를 가지고 있는 그룹의 구성원들이 동일한 세션 키(그룹 키)를 공유할 수 있도록 도와주는 역할을 한다.

2. 서버를 이용하는 패스워드 기반 키 교환 프로토콜에서의 사전공격

다른 암호 프로토콜의 안전성 모델과 비교할 때, 패스워드 기반 키 교환 안전성 모델의 가장 특별한 차이점은 패스워드 기반 키 교환 프로토콜은 반드시 사전공격(dictionary attack) 또는 추측공격(guessing attack)에 안전해야 한다는 점이다. 패스워드는 사람이 쉽게 기억할 수 있는 4개에서 8개의 문자로 구성된다. 따라서 가능한 패스워드의 집합이 작기 때문에 상대적으로 쉽게 추측이 가능하다. 보통 사전공격은 온라인(on-line)과 오프라인(off-line) 사전공격으로 구분된다.

온라인 사전공격에서, 공격자는 키 교환 프로토콜에 참여하여 추측한 패스워드를 사용한다. 만약 프로토콜이 실패하면, 공격자는 다른 패스워드를 추측 후에 이것을 사용하여 새로운 프로토콜을 수행한다. 이러한 온라인 공격은 공격자가 직접 프로토콜에 참여하여 추측한 패스워드를 사용하는 것을 요한다. 오프라인 사전적 공격에서 공격자는 패스워드 사전(dictionary)에서 패스워드를 선택하고, 오프라인 방식으로 추측한 패스워드를 검증한다. 즉, 공격자는 성공적으로 실행된 프로토콜의 메시지 값들만 사용하여 추측한 패스워드가 맞는지 틀리는지를 검증한다. 그렇기 때문에 이러한 오프라인 공격은 탐지가 불가능하다. 온라인 사전공격은 항상 가능 하지만, 이러한 공격은 접속 실패의 횟수를 관측함으로써 쉽게 막을 수 있기 때문에 심각한 위협은 되지 않는다. 그러나 오프라인 사전공격을 방지하기는 더욱 어렵다. 왜냐하면, 주고받는 메시지에 아주 적은 잉여 정보(redundancy information)라도 존재한다면, 공격자는 추측한 패스워드의 옳고 그름을 검사하기 위한 검증자로서 잉여 정보를 사용할 수 있기 때문이다.

서버를 이용하는 패스워드 기반 키 교환 모델에서는 서버를 패스워드 검증 오라클(oracle)로 사용하여 패스워드에 대한 잉여 정보를 얻을 수 있기 때문에 온라인 사전공격에 좀 더 주의를 기울여야한다. 만약 온라인 패스워드 추측공

격이 서버에 의해 탐지될 수 없는 경우, 이러한 공격을 탐지할 수 없는 온라인 사전공격(undetectable on-line dictionary (UDOD) attack)이라고 한다. 탐지할 수 없는 온라인 사전공격을 방지하기 위해서는 서버에게 키 교환 요청이 왔을 때, 서버 자신이 패스워드 검증 오라클로 사용되는 것인지, 아니면 사용자가 정당한 요청을 한 것인지를 구분할 수 있어야한다.

또한 정당한 그룹 사용자가 자신의 패스워드를 이용해서 다른 그룹 구성원들의 패스워드를 알아내려고 시도하는 악의적인 내부 사용자를 고려해야한다. 패스워드 기반 키 교환 스킴의 주된 안전성 목표는 공격자가 단지 온라인 사전공격만 할 수 있도록 하는 것이다.

3. 서버를 이용하는 패스워드 기반 키 교환 프로토콜에서의 키 기밀성

키 교환 프로토콜의 가장 기본적인 안전성 요구사항은 키 기밀성(key secrecy)이다. 유한한 계산 능력을 지닌 공격자는 정직한 사용자 간의 통신을 도청하거나, 공격자가 프로토콜에 참여함으로써 정직한 사용자에게 메시지를 전송할 수 있다. 키 기밀성은 이러한 공격자가 세션 키에 대한 어떠한 정보도 얻을 수 없어야 한다는 것이다. 키 교환 프로토콜에 요구되는 다른 안전성은 전방향 안전성(forward secrecy)과 기지 키 공격에 대한 안전성(known-key secrecy)이다.

전방향 안전성은 사용자의 롱텀 키(long-term key)인 패스워드를 알고 있는 어떠한 공격자라도 정직한 구성원 간에 성공적으로 확립된 이전의 세션 키에 대한 어떠한 정보도 얻을 수 없어야 함을 의미한다. 기지 키 공격에 대한 안전성은 여러 세션에서 얻은 여러 개의 세션 키를 이용해도 다른 세션의 키 비밀성에는 영향을 주지 않아야 함을 의미한다. 또한 기지 키 공격에 대한 안전성은 공격자가 정직한 구성원 사이에 성공적으로 확립된 세션 키로부터 오프라인 사전공격을 통해서 패스워드를 알아낼 수 없어야 함을 의미한다.

서버를 이용하는 패스워드 기반 키 교환 모델에서 추가적으로 요구되는 안전성은 악의적인 서버(malicious server)에 대한 키 기밀성이다. 이것은 서버가 그룹 구성원들이 공통된 세션 키를 공유하도록 도와주는 역할을 하지만, 그룹 구성원들 간의 통신을 도청할 경우에 세션 키에 대한 어떠한 정보도 없을 수 없어야 함을 의미한다. 따라서 서버에 대한 키 기밀성이 제공된다면, 서버가 도청을 하여 그룹의 구성원들의 세션 키를 알 수 있는 경우보다 서버의 신뢰 의존도를 낮출 수 있다. 서버는 그룹 구성원들의 패스워드를 가지고 있기 때문에 물론 사용자를 가장할 수 있다. 이 모델에서는 서버를 수동적 공격자(passive adversary)로 가정한다.

4. 서버를 이용하는 패스워드 기반 키 교환 프로토콜에서의 무정지성

안전하고 확장이 용이(scalable)하면서 안정적(reliable)인 그룹 키 교환에 관해서 많은 연구가 진행되고 있다. 본 논문에서는 서버가 존재하는 모델에서의 네트워크 구성이 완료되지 않았거나(misconfigurations) 라우터의 고장 등으로 발생하는 네트워크 오류에 의해 사용자들이 네트워크 접속에 실패하는 상황을 고려한다.

그룹의 특정 사용자들이 네트워크에 정상적으로 접속할 수 없는 경우에도 다른 사용자들이 어떠한 추가적인 메시지 전송없이도 세션 키를 공유할 수 있으면, 그 키 교환 프로토콜이 무정지성(fault-tolerant)을 제공한다고 한다.

II. 연구배경 및 관련연구

1. 연구배경

구성원들이 서로 다른 패스워드를 가지는 다자간 키 교환 모델에서 종래 기법은 그룹 구성원과 서버 간 인증을 수행하기 위해서 구성원과 서버는 동일한 패스워드 정보를 이용한다. 각 그룹 구성원과 서버 간 인증에 사용되는 패스워드 정보가 동일한 형태를 가지기 때문에 이러한 모델을

대칭적인 모델(symmetric model)이라 부른다. 대칭적인 모델의 문제점은 서버 DB 노출 공격(server compromise attack)에 취약하다는 것이다. 그 이유는 이 모델에서의 프로토콜들은 서버의 DB에 저장된 구성원들의 패스워드가 노출된 경우에 대한 안전성을 제공하지 못하기 때문이다. 즉, 서버의 DB가 노출되자마자 어떠한 오프라인 사전공격(off-line dictionary attack) 없이도 공격자는 구성원들의 패스워드를 이용하여 곧바로 서버에게 정당한 구성원으로 위장 가능하다.

본 논문에서는 DB노출 공격에 취약한 기존 대칭적인 모델의 문제점을 해결하기 위해서 검증자 기반 모델(verifier-based model)에서의 다자간 키 교환 프로토콜을 연구한다. 검증자 기반 모델에서는 각 그룹 구성원과 서버 간 인증에 사용되는 패스워드 정보가 서로 비대칭적(asymmetric) 이다. 검증자 기반 모델에서는 흔히, 키 교환을 위해 그룹의 각 구성원은 패스워드를 이용하고, 서버는 DB에 패스워드를 그대로 저장하는 것이 아니라 패스워드에 일방향 함수(one-way function)를 적용하여 생성된 패스워드의 검증자를 저장한다. 따라서 서버의 DB가 노출되는 경우, 공격자가 어떠한 패스워드 사전공격 없이 구성원의 패스워드를 이용하여 곧바로 서버에게 정당한 구성원으로 위장할 수 없게 된다. (물론 DB가 노출되면 노출된 패스워드의 검증자를 이용하여 사용자에게 서버로는 항상 위장 가능하다.) 공격자는 노출된 DB로부터 오프라인 사전공격을 통해서 패스워드를 알아낼 수는 있지만, 오프라인 사전공격을 수행하여야 하기 때문에, 이것은 서버가 DB가 노출된 것에 대한 대처를 할 수 있는 시간적 여유를 벌어주게 된다는 관점에서 기존의 대칭적 모델에서 프로토콜보다 안전성이 강화된 것이라고 볼 수 있다.

본 논문에서는 DB노출에 안전하도록 패스워드의 검증자를 이용하며, 구성원들이 서로 다른 패스워드를 가지는 다자간 패스워드 기반 키 교환 프로토콜인 VB-PAMKE1과 VB-PAMKE2를 제안한다. 제안 프로토콜들은 검증자 기반 모델에서 처음으로 제안되는 프로토콜들이다. VB-PAMKE1는 전방향 안전성(forward secrecy: FS)과 기지 키 공격에 대한 안전성(known-key secrecy: KK)을 제공하며, VB-PAMKE2는 추가적으로 서버에 대한 키 기밀성(key secrecy against server: KSS)을 제공한다. 표 1은 제안 프로토콜들의 효율성과 안전성 비교를 나타낸다. 표에서 메시지 길이는 각 사용자가 전송하는 메시지의 전체 비트 수를 의미한다. 제안 프로토콜들의 수학적 연산은 모두 Z_p^*군(group)에서 수행되며 p는 소수이다. $|\tau|$는 MAC (message authentication code) 값의 길이를 의미한다.

표 1. 제안 스킴의 계산량과 안전성 분석
Table 1. Efficiency and security analysis

스킴	VB-PAMKE1	VB-PAMKE2
라운드 수	3	5
지수승 (각 사용자)	4	7
메시지 길이	$\|p\|+\|\tau\|$	$2\|p\|+2\|\tau\|$
제공 안전성	· 기지 키 공격에 대한 안전성, 전방위 안전성 · 온라인 사전공격에 대한 안전성 · 탐지할 수 없는 온라인 사전공격에 대한 안전성	· 기지 키 공격에 대한 안전성, 전방위 안전성 · 서버에 대한 키 기밀성 · 온라인 사전공격에 대한 안전성 · 탐지할 수 없는 온라인 사전공격에 대한 안전성
가정	표준모델	표준모델

2. 관련연구

현재까지 여러 패스워드 기반 다자간(multi-party) 키 교환 프로토콜들이 제안되었다[2, 3, 4, 8, 1]. 그러나 [4]의 스킴만이 구성원들이 서로 다른 패스워드를 가지는 모델이며 (다른 스킴들은 그룹의 구성원이 동일한 패스워드를 가지는 모델이다), 대칭적인 모델을 따르는 프로토콜이다. [4]에서 Byun과 그 외는 두 개의 프로토콜을 제안하였다. 하나는 그룹의 구성원의 수가 n일 때, 유니캐스트 네트워크에서 $O(n)$ 라운드를 가지는 N-party EKE-U 스킴이고, 다른 하나는 멀티캐스트 네트워크에서 상수 라운드를 가지는 N-party EKE-M 스킴이다. 그러나 N-party EKE-U 스킴은 오프라인 사전공격에 취약하다. (이에 대한 공격은 [11] 논문에 제시되었다.) 그리고 [11] 논문에서 제안된 공격을 방어하기 위해 개선된 N-party EKE-U[5] 스킴 또한 오프라인 사전공격에 취약하다. (이에 대한 공격은 [10] 논문에 제시되었다.) N-party EKE-M 스킴은 이상적인 암호(ideal cipher)

와 이상적인 해쉬(ideal cipher) 모델 하에서 키 기밀성에 대한 안전성이 증명되었다. 하지만 이 두 스킴은 서버에 대한 키 기밀성을 제공하지 않으며, 대칭적인 모델에서의 프로토콜이기 때문에 서버 DB 노출공격에 취약하다는 단점이 있다.

III. 안전성 모델

본 장에서는 키 교환 프로토콜을 깨려는 공격자가 수행할 수 있는 공격유형을 모델링하기 위한 쿼리(query)의 종류를 정의한다. 다음 정의에서 G를 그룹의 구성원들의 집합, G_u를 세션 키를 교환하고자 하는 그룹의 구성원들의 집합, S를 서버, U_i를 인덱스 i를 가지는 사용자로 정의한다. 프로토콜의 참여자 P (사용자이거나 서버)는 동시에 여러 개의 세션을 수행할 수 있기 때문에 세션을 구분하기 위해, P^s를 s번째 세션에서의 참여자로 정의한다.

- Execute(G_u,S^t): 이 쿼리는 공격자의 수동적 공격(passive attack)을 모델링한다. 이 쿼리를 통해 공격자 A 는 G_u와 S^t 사이의 정상적인 프로토콜 수행으로 발생하는 모든 메시지(transcript)를 얻을 수 있다.
- SendUser(U_i^s, m): 이 쿼리는 사용자를 대상으로 하는 공격자의 능동적 공격(active attack)을 모델링한다. 이 쿼리를 통해 공격자 A 는 사용자 U_i^s에게 메시지 m을 전송할 수 있고, U_i^s로부터 이에 대응되는 응답을 받을 수 있다. 여기서 공격자 A 는 메시지를 변경하거나 새로 생성하거나 또는 어떠한 변경 없이 단순히 메시지를 전송할 수도 있다.
- SendServer(S^t, m): 이 쿼리는 서버를 대상으로 하는 공격자의 능동적 공격을 모델링한다. 이 쿼리를 통해 공격자 A 는 서버 S^t에게 m을 전송할 수 있고, S^t로부터 이에 대응되는 응답을 받을 수 있다.

IV. 서버 DB 노출에 안전한 다자간 키 교환 프로토콜

본 장에서는 제안하는 두 가지 다자간 패스워드 기반 키 교환 프로토콜인 VB-PAMKE1 과 VB-PAMKE2에 대해 설명한다. 제안 프로토콜은 브로드캐스트 채널과 P2P채널을 가정한다. $|G|=N$이고, 그룹 키 교환이 G의 서브집합인 G_u 내의 구성원들에 의해 수행된다고 가정한다.

1. VB-PAMKE1 프로토콜

VB-PAMKE1은 다음 세 가지 주요 단계들로 구성된다: 그룹의 각 사용자와 서버의 키 교환을 위한 이자간 검증자 기반의 패스워드 기반 키 교환 단계, 온라인 사전공격과 탐지할 수 없는 온라인 사전공격의 시도를 확인하기 위한 단계 그리고 이자간 검증자 기반의 패스워드 기반 키 교환 단계에서 공유한 세션 키를 이용해서 서버가 각 사용자들에게 임의의 비밀키를 분배하는 단계. 이자간 검증자 기반의 패스워드 기반 키 교환 단계 에서는 VB-PAMKE1은 [7]에서 제안된 이자간 검증자 기반의 패스워드 기반 키 교환 스킴을 사용한다.

공개정보. 다음은 프로토콜 참여자에게 공개되는 정보에 대한 표기이다.

표 2. 표기
Table 2. Notion

G	Z_p^*내의 그룹의 오더가 q인 유한 순환군
p, q	소수 ($p=2q+1$을 만족)
g_1, g_2	오더가 q인 생성자 (g_1과 g_2의 이산대수 관계성이 알려져서는 안 된다.)
$H : \{0,1\}^* \rightarrow \mathcal{C}_q^*$	해쉬함수
$M=$ $(KEY.G, MAC.G, MAC.V)$	MAC (message authentication code) 알고리즘. KEY.G는 키kmac을 생성한다. MAC.G 는 kmac을 사용해서 메시지 M에 대한 MAC 태그인 $\tau = MAC.G_{k_{mac}}(M)$를 생성한다. MAC.V은 kmac을 사용해서 메시지와 태그 쌍을 검증한다. 만약 태그가 유효하면 1을 출력하고, 그렇지 않으면 0을 출력한다.
F	의사난수 함수

초기화 단계. 각 사용자 $U_i \in G$와 서버 S가 패스워드 pw_i에 대한 검증자인 $v_{i,1} = g_1^{H(U_i \| S \| pw_i)} \bmod p$와 $v_{i,2} = g_2^{H(U_i \| S \| pw_i)} \bmod p$, 공개정보 그리고 G_u에 대한 정보를 안전하게 공유하였다고 가정한다.

이자간 패스워드 기반 키 교환 단계.

1. 각 사용자 $U_i \in G_u$는 임의의 난수값 $x_i \in \mathcal{C}_q^*$를 선택하고, $X_i = g_1^{x_i} \cdot v_{i,2} \bmod p$를 계산한다.
2. 각 사용자 U_i는 $(U_i \| X_i)$를 S에게 전송한다.
3. 각 사용자 $U_i \in G_u$에 대해서 S는 난수 $y_i, z_i \in \mathcal{C}_q^*$를 선택하고, $Z_i = g_1^{z_i} \cdot v_{i,2} \bmod p$와 $Y_i = g_1^{y_i} \cdot v_{i,1}^{z_i} \bmod p$를 계산한다.
4. S는 $(S_i \| Y_i \| Z_i)$를 각 사용자 U_i에게 전송한다.
5. $(S_i \| Y_i \| Z_i)$를 전송받은 후, 각 사용자 U_i는 $T_i = (Z_i / v_{i,2})^{H(U_i \| S \| pw_i)} \bmod p$와 $k_i = (Y_{i,s} / T_i)^{x_i} \bmod p$를 계산한다.
6. $(U_i \| X_i)$를 전송받은 후, S는 $k_i = (X_i / v_{i,2})^{y_i} \bmod p$를 계산한다.

온라인 패스워드 사전공격 및 탐지할 수 없는 온라인 패스워드 사전공격의 시도 여부 확인 단계.

1. 각 사용자 U_i는 $\tau_{S,i} = MAC.G_{k_i}(U_i \| S \| X_i \| Y_i \| Z_i)$를 계산하고 $(U_i \| \tau_{i,S})$를 S에 전송한다.
2. 각 사용자 $U_i \in G_u$에 대해, S는 $(\tau_{S,i}) = MAC.G_{k_i}(S \| U_i \| X_i \| Y_i \| z_i)$를 계산하고 $(S \| \tau_{s,i})$를 U_i에게 전송한다.
3. $(S \| \tau_{s,i})$를 전송받은 후, 각 사용자 U_i는 $MAC.V_{k_i}(\tau_{S,i})$를 계산한다. 만약 $MAC.V$이 0을 출력하면 각 사용자 U_i는 프로토콜을 종료한다. 그렇지 않은 경우, 다음 단계를 수행한다.
4. $(U_i \| \tau_{i,S})$를 전송받은 후, 각 사용자 $U_i \in G_u$에 대해서 S는 k_i를 사용해서 $\tau_{i,s}$의 유효성을 확인한다. S는 MAC 검증 과정을 모두 통과한 사용자들의 아이디의 집합으로 $G_u^1 = \{U_1, ..., U_{|G_u^1|}\}$를 만든다.

키 분배 단계. S는 {0,1}l 로부터 랜덤하게 K를 선택한다. 각 $i \in G_u^1$에 대해서 S는 $K_i = K \oplus H(G_u^1 \| k_i)$를 계산한다. S는 $(G_u^1 \| U_1 \| K_1 \| ... \| K_1 \| ... \| U_{|G_u^1|} \| K_{|G_u^1|})$를 브로드캐스팅한다.

키 계산 단계. 각 사용자 U_i는 세션 키 $sk = F_K(G_u^1 \| sid)$를 계산한다. 여기서 $sid = (K_1 \| ... \| K_{|G_u^1|})$.

2. VB-PAMKE1 프로토콜의 분석

무정지성(Fault-tolerant). VB-PAMKE1는 무정지성을 제공한다. 만약 사용자들 중 누군가가 네트워크 오류로 인해 네트워크에 접속할 수 없는 경우, 그외 다른 사용자들은 어떤 추가적인 메시지 전송이나 지연 없이 세션 키를 교환 할 수 있다. 만약 $\tau_{i,s}$를 전송후에 사용자 U_i가 네트워크에 여전히 연결되어 있을 경우에 그 사용자는 서버로부터 K_i를 전송 받을 수 있기 때문에 세션 키를 계산할 수 있다. 물론 만약 서버의 브로드캐스트 메시지가 전송 실패하면 서버는 메시지를 다시 전송하여야 한다.

온라인 사전공격과 탐지할 수 없는 온라인 사전공격에 대한 안전성. VB-PAMKE1은 온라인 사전공격과 탐지할 수 없는 온라인 사전공격에 안전하도록 설계되었다. 만약 패스워드 추측공격이 서버나 사용자에 의해 탐지 가능하다면, 그러한 공격들은 더 이상 가능하지 않을 것이다. 탐지할 수 없는 온라인 사전공격을 탐지하기 위해서 제안하는 기법은 각 사용자가 서버로부터 키 교환을 위한 정보를 받기 이전에 자신이 패스워드에 대한 정보를 알고 있음을 증명하도록 하고, 서버는 이를 검증하도록 한다. 만약 검증이 통과하면 서버는 각 사용자에게 세션 키를 계산할 수 있도록 하는 정보를 보내준다. 이것은 시도-응답(challenge-response) 메커니즘이다. 패스워드에 대한 정보를 알고 있음을 증명하는 방법으로 임시적인 디피-헬만(ephemeral Diffie- Hellman) 값을

키 값으로 사용하는 MAC을 사용한다. 만약 MAC 검증이 실패하게 된다면 서버는 사용자의 패스워드가 탐지할 수 없는 온라인 사전공격의 대상이 되고 있음을 알아차릴 수 있다. 만약 기존 정해진 실패 횟수를 초과하는 경우 서버는 공격 대상이 되는 사용자에게 더 이상 패스워드를 사용하지 말고 패스워드를 교체하도록 한다. 온라인 사전공격을 방지하기 위해서 위와 같은 시도-응답 메커니즘을 사용하는데 이것은 키 확인(key confirmation)의 형태로 볼 수 있다. 만약 MAC 검증이 실패한다면, 사용자는 자신의 패스워드가 온라인 사전공격의 대상이 되어 위험에 노출되었다는 사실을 알아차릴 수 있다. 기존 정해진 실패 횟수를 초과하는 경우 사용자는 더 이상 패스워드를 사용하지 않고 패스워드를 교체하게 된다.

위와 같은 검증 단계들을 통과하기 위해서 공격자는 다음 3가지 방법 중 하나를 취할 수 있다: 공격자가 실패횟수를 초과하지 않는 범위에서 패스워드를 올바르게 추측하는 방법 (그러나 이것은 패스워드 공간의 크기 때문에 성공할 확률이 일반적으로 매우 낮다). 또는 DDH(decisional Diffie-Hellman) 문제를 풀거나 MAC 알고리즘을 깨는 방법.

다음 정리는 VB-PAMKE1이 오프라인 사전공격에 안전하고, 전방향 안전성과 기지 키 공격에 대한 안전성을 제공함을 보인다.

정리 1 G를 DDH문제가 어려운 순환 군이라고 하고, F가 안전한 의산난수 함수라고 가정한다. 그러면 VB-PAMKE1은 PAKE-KK&FS 프로토콜이다. (PAKE-KK&FS 프로토콜이라는 것은 기지 키(KK) 공격에 대한 안전성과 전방향 안전성(FS)을 제공하는 패스워드 기반 키교환 프로토콜을 말한다.)

$$Adv_{VB-PAMKE1}^{PAKE-KK\&FS}(k,t) \le (4|G|+4|G|\cdot N_s)\cdot Adv_G^{DDH}(t)+ 4Adv_F^{PRF}(k,t,q,h)+\frac{2(q_{se}^U+q_{se}^S)}{PW}+ \frac{|G|(q_{ex}+q_{se}^U+q_{se}^S)^2}{q},$$

t는 공격자의 수행시간을 나타내며, q_{ex}는 공격자의 Execut 쿼리 수이고, q_{se}^U는 SendUser 쿼리의 수 그리고 q_{se}^S는 SendServer 쿼리의 수이다. N_s는 공격자가 만드는 최대 세션 수이고, PW는 패스워드 공간의 크기를 나타낸다.

증 명. 본 정리의 증명은 페이지 제한으로 생략하며, 오프라인 사전공격에 대한 안전성과 전방향 안전성 그리고 기지 키 공격에 대한 안전성에 대해서 간략히 살펴본다. 공격자는 프로토콜을 깨기 위해서 패스워드를 하나씩 선택해서 확인해보는 온라인 사전공격 밖에 할 수 없고, 오프라인 사전공격은 MAC을 위조하거나 DDH문제를 풀어야 하는 공격자의 계산능력의 한계 때문에 수행할 수 없다. 따라서 VB-PAMKE1은 오프라인 사전공격에 안전하다. 만약 공격자에게 롱텀 키인 패스워드가 주어졌다 하더라도 이전 세션의 세션 키에 대한 정보를 알아내기 위해서 공격자는 DDH문제를 풀어야하기 때문에 VB-PAMKE1은 전방향 안전성을 제공한다. 매 세션에 계산되는 세션 키는 해당 세션에서 생성되는 난수 값을 이용해 계산된다. 따라서 각 세션의 세션 키는 독립적이기 때문에 제안 프로토콜은 기지 키 공격에 안전하다.

3. VB-PAMKE2 프로토콜

VB-PAMKE2는 악의적인 서버로부터 안전하도록 설계되었다. 즉, 서버는 수동적인(passive) 공격으로 그룹의 사용자들이 공유하는 세션 키에 대한 정보를 알 수 없다. 이러한 안전성을 만족하도록 설계하기 위해 본 스킴은 VB-PAMKE1과 다른 방법을 사용한다. VB-PAMKE1은 서버가 세션 키를 분배해주는 방법을 사용하였지만, VB-PAMKE2는 MAC 키 분배와 MAC을 사용한 인증된 다자간 키 교환 방법을 사용한다. 이 스킴은 여전히 상수 라운드를 요한다. 이러한 방법을 통해 세션 키는 서버에 의해 결정되는 것이 아니라 모든 사용자들에 의해 결정된다. VB-PAMKE2는 VB-PAMKE1에서 사용한 이자간 검증자 기반의 패스워드 키 교환과 온라인 사전공격과 탐지할 수 없는 온라인 사전공격의 시도 여부를 확인하기 위한 기법을 사용한다. 그리고 MAC 키 분배와 MAC을 사용한 인증된 다

자간 키 교환 기법으로 Burmester와 Desmedt의 그룹 키 교환 기법[6]을 이용한다. VB-PAMKE2는 다음 부분들을 제외하고는 VB-PAMKE1과 동일하다.

온라인 패스워드 사전공격 및 탐지할 수 없는 온라인 패스워드 사전공격의 시도 여부 확인 단계.

1. S는 $\tau_{s,i}=MAC.G_{k_i}(U_i \| S \| X_i \| Y_i \| Z_i)$을 계산하고, $(S \| \tau_{s,i})$를 U_i에게 전송한다.
2. $(S \| \tau_{s,i})$를 전송 받은 후에, 각 사용자 U_i는 $MAC.V_{k_i}(\tau_{Si})$을 계산한다. 만약 $MAC.V$가 0을 출력하면, 각 사용자 U_i는 프로토콜을 종료하고, 그렇지 않은 경우 다음 단계를 수행한다. 각 사용자 U_i는 임의의 난수값 $r_i \in Z_q^*$를 선택하고 $\tau_{s,i}=MAC.G_{k_i}(U_i \| S \| X_i \| Y_i \| Z_i \| g^{r_i})$를 계산한다. 그리고 $(U_i \| \tau_{i,S} \| g_1^{r_i})$를 S에게 전송한다.
3. $(U_i \| \tau_{i,S} \| g_1^{r_i})$를 전송 받은 후에, 각 $i \in G_u^1$에 대해, S는 K_i를 사용해서 $\tau_{i,S}$의 유효성을 검증한다.
4. S는 MAC 검증이 통과한 사용자의 아이디만으로 G_u^1을 정렬하여 구성한다. $|G_u^1|=n$ 이고 $G_u^1=\{U_1,...,U_n\}$라고 가정하자.

MAC 키 분배와 MAC을 사용한 인증된 다자간 키 교환 단계.

1. S는 $KEY.G$를 사용하여 MAC 키인 k_{mac}를 생성한다. 각 $i \in G_u^1$ 마다, S는 $K_i=k_{mac} \oplus H(G_u^1 \| k_i)$와 $\sigma_{1,i}=MAC.G_{k_{mac}}(U_i \| \alpha_i)$를 계산한다. 여기서 $\alpha_i=g_1^{r_i} \bmod p$ 이다.
2. S는 $1 \le j \le n$마다, $(G_u^1 \| U_1 \| K_1 \| \cdots \| U_n \| K_n)$와 $(U_{j+1} \| U_{j+(n-1)} \| \alpha_j \| \sigma_{j,1})$를 브로드캐스트한다. 여기서 $j=j \bmod n$이다.
3. S의 브로드캐스트 메시지를 전송받은 후, 각 사용자 U_i는 K_i로부터 K_{mac}을 계산한다. 그리고 $MAC.V_{k_{mac}}(U_{i-1} \| \alpha_{i-1})$ 과 $MAC.V_{k_{mac}}(U_{i+1} \| \alpha_{i+1})$ 을 계산한다.
4. 만약 MAC 검증이 모두 통과하면 각 사용자 U_i는 다음 단계를 수행한다. 그렇지 않은 경우, 프로토콜을 종료한다.
5. 각 사용자 U_i는 $\beta_i=(\alpha_{i+1}/\alpha_{i-1})^{r_i} \bmod p$ 를 계산하고 $(U_i \| \beta_i \| \sigma_{2,1}= MAC.G_{k_{mac}}(U_i \| \beta_i))$ 를 브로드캐스트한다.
6. 사용자들로부터 브로트캐스트 메시지를 전송받은 후, S는 G_u^1 내의 모든 사용자들로부터 메시지가 모두 잘 전송되었는지를 확인한다. 만약 그렇지 않다면, S는 분실된 메시지의 소유자에게 메시지 재전송을 요청한다.
7. $(U_i \| \beta_i \| \sigma_{2,1})$를 전송받은 후, $U_i \in G_u^1 (j \neq i)$마다, 각 사용자 U_i는 K_{mac}을 사용하여 $\sigma_{2,1}$의 유효성을 검증한다.
8. 만약 모든 검증이 성공적으로 완료되면, 각 사용자 U_i는 $\gamma_i=(\alpha_{i-1})^{nr_i} \cdot \beta_i^{n-1} \cdot \beta_{i+1}^{n-1} \mathrm{L}\ \beta_{i-2} \bmod p$ 를 계산한다. 그렇지 않은 경우는 프로토콜을 종료한다.

키 계산 단계. 각 사용자 U_i는 세션 키 $sk=F_{ri}(G_u^1 \| sid)$를 계산한다. 여기서 $G_u^1=(U_1,\cdots,U_n)$이고, $sid=(\boldsymbol{K} \| \alpha \| \sigma_1 \| \beta \| \sigma_2)$, $\boldsymbol{k}=(K_1 \| \cdots \| K_n)$, $\alpha=(\alpha_1 \| \cdots \| \alpha_n)$, $\alpha_1=(\alpha_{1,1} \| \cdots \| \alpha_{n,1})$, $\sigma_1=(\sigma_{1,1} \| \cdots \| \sigma_{n,1})$, $\beta_1=(\beta_1 \| \cdots \| \beta_n)$, $\sigma_1=(\sigma_{1,2} \| \cdots \| \sigma_{n,2})$이다.

3. VB-PAMKE2 프로토콜의 분석

정확성(Completeness). 만약 VB-PAMKE2의 모든 단계들이 정상적으로 완료된다면, U_i에 의해 계산되는 세션 키는 $sk = F_{\gamma_i}(G_u^1 \| sid)$ 이다. 여기서 $\gamma_i=g_1^{r_1r_2+r_2r_3+\ldots+r_nr_1} \bmod p$ 이다.

무정지성(Fault-tolerant). VB-PAMKE2는 완전한 무정지성을 제공하지는 않는다. 만약 사용자들 중 누군가가 네트워크 오류로 인해 네트워크에 접속할 수 없는 경우, 세션 키 교환이 이뤄지지 않을 것이다. 왜냐면 MAC 키 분배와 MAC을 사용한 인증된 다자간 키 교환 단계에서 모든 사용자들은 링(ring) 형태로 모두 정상적으로 연결되어있어야

세션 키가 올바르게 공유될 수 있기 때문이다. 링 구조가 완성되기 이전까지는 다자간 키 교환이 지연될 것이다.

정리 2 G를 DDH문제가 어려운 순환 군이라고 하고, F가 안전한 의산난수 함수, 그리고 M이 위조 불가능한 MAC 알고리즘이라 가정한다. 그러면 VB- PAMKE2는 안전한 PAKE-KSS&KK&FS 프로토콜이다. (PAKE-KSS&KK&FS 프로토콜이라는 것은 서버에 대한 키 기밀성(KSS)과 기지 키(KK) 공격에 대한 안전성, 그리고 전방향 안전성(FS)을 제공하는 패스워드 기반 키 교환 프로토콜을 말한다.) 여기서 파라미터들은 정리1에서와 같이 정의된다.

$$Adv_{VB-PAMKE2}^{PAKE-KSS\&KK\&FS}(k,t) \le (8|G|+4|G|\cdot N_s)\cdot Adv_G^{DDH}(t)+6Adv_F^{PRF}(k,t,q,h)+4|G|\cdot Adv_M^{SUF}(k,q_{se}^U)+\frac{2(q_{se}^U+q_{se}^S)}{PW}+\frac{|G|(q_{ex}+q_{se}^U)^2}{q}.$$

증 명. 본 정리의 증명은 페이지 제한으로 생략한다. 오프라인 사전공격에 대한 안전성과 전방향 안전성 그리고 기지 키 공격에 대한 안전성은 VB-PAMKE1에서와 동일하다. VB-PAMKE2는 VB-PAMKE1이 제공하는 안전성에 추가적으로 서버에 대한 키 기밀성(KSS)을 제공한다는 점에서 차이가 난다. 이를 위해, MAC 키 분배와 MAC을 사용한 인증된 다자간 키 교환 단계에서 서버는 MAC 키를 선택해서 각 사용자에게 분배한다. 서버로부터 전달 받은 MAC 키를 이용해서 각 사용자는 서버의 개입 없이 자신들만이 알 수 있는 세션 키를 교환하기 때문에 악의적인 서버는 수동적인 공격을 통해서는 그룹 사용자들이 맺는 세션 키에 대한 정보를 알 수 없다.

V. 결 론

본 논문에서는 패스워드 기반 다자간 키 교환 모델에서 서버 DB노출공격에 안전한 두 개의 프로토콜들을 처음으로 제안하였다. 두 제안 프로토콜들은 랜덤 오라클의 사용 없이 표준 모델에서 안전성이 증명되었으며, 모두 상수 라운드를 가진다. 첫 번째 제안 프로토콜은 키 교환 프로토콜에서 만족되어야 하는 전방향 안전성과 기지 키 공격에 대한 안전성을 제공하며, 두 번째 제안 프로토콜은 추가적으로 악의적인 서버에 대한 키 기밀성을 제공한다. 서버 DB 노출공격에 안전하도록 두 프로토콜들은 모두 패스워드에 대한 검증자를 이용한다.

참 고 문 헌

[1] M. Abdalla, E. Bresson, O. Chevassut, and D. Pointcheval. Password-based Group Key Exchange in a Constant Number of Rounds, In Proc. of PKC '06, LNCS 3958, pages 427-442 , 2006.

[2] N. Asokan and P. Ginzboorg. Key Agreement in Ad-hoc Networks, Journal of Computer Communications 23(17), pages 1627-1637, 2000.

[3] E. Bresson, O. Chevassut, and D. Pointcheval. Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks, In Proc. of ASIACRYPT 2002, LNCS 2501, pages 497-514, Springer-Verlag, 2002.

[4] J. W. Byun and D. H. Lee. Password-Authenticated Key Exchange between Clients with Different Passwords, In Proc. of ACNS '05, LNCS 3531, pages 75-90, 2005.

[5] J. W. Byun and D.H. Lee. Comments on Weaknesses in Two Group Diffie-Hellman Key Exchange Protocols, IACR ePrint Archive, 2005/209, 2005.

[6] M. Burmester and Y. Desmedt. A Secure and Efficient Conference Key Distribution System, In Proc. of EUROCRYPT '94, LNCS 950, pages 275-286, Springer-Verlag, 1995.

[7] J. O. Kwon, I. R. Jeong, D. H. Lee. One-Round Protocol for Two-Party Verifier-Based Password-Authenticated Key Exchange, In Proc. of CMS 2006, LNCS 4237, pages 87-96, Springer-Verlag, 2006.

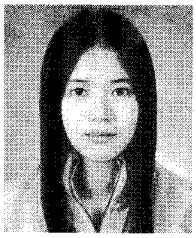
[8] J. O. Kwon, I. R. Jeong, D. H. Lee. Provably-Secure Two-Round Password-Authenticated Group Key Exchange in the Standard Model, In Proc. of IWSEC '06, LNCS 4266, pp. 322-336, 2006.

[9] S. M. Lee, J. Y. Hwang and D. H. Lee. Efficient Password-Based Group Key Exchange, In Proc. of TrustBus '04, LNCS 3184, pages 191-199, Springer-Verlag, 2004.

[10] Raphael C.-W. Phan and B.-M Goi. Cryptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange Using Different Passwords, In Proc. of ACNS '06, LNCS 3989, pp. 226-238, Springer-Verlag, 2006.

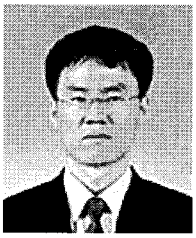
[11] Q. Tang and L. Chen. Weaknesses in Two Group Diffie-Hellman Key Exchange Protocols, IACR ePrint Archive, 2005/197, 2005.

저 자 소 개



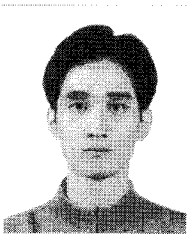
권 정 옥

- 2000년 2월 : 동덕여자대학교 전자계산학과 졸업
- 2003년 2월 : 고려대학교 정보보호기술협동과정 석사 졸업
- 2007년 2월 : 고려대학교 정보경영공학전문대학원 박사 졸업
- 2007년 3월~2007년 8월 : 고려대학교 정보보호기술연구센터 박사후연구원
- 2007년 9월~현재 : 고려대학교 BK21 유비쿼터스 정보보호 사업단 연구교수
- 주관심분야 : 암호프로토콜, 암호이론



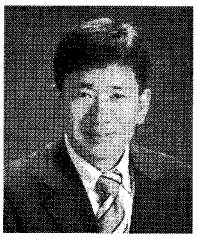
정 익 래

- 1998년 2월 : 고려대학교 전산학과 학사 졸업
- 2000년 2월 : 고려대학교 전산학과 석사 졸업
- 2004년 8월 : 고려대학교 정보보호대학원 박사 졸업
- 2006년 6월~2008년 2월 : 한국전자통신연구원 암호기술연구팀 선임연구원
- 2008년 3월~현재 : 고려대학교 정보경영공학부 조교수
- 주관심분야 : 암호프로토콜, 암호이론, 계산이론



최 재 탁

- 2002년 2월 : 충북대학교 수학과 학사 졸업
- 2005년 8월 : KAIST 수학과 석사 졸업
- 2005년~현재 : 고려대학교 정보경영공학전문대학원 박사과정
- 주관심분야 : 암호이론, 암호프로토콜



이 동 훈

- 1983년 8월 : 고려대학교 경제학과 학사 졸업
- 1987년 12월 : Oklahoma University 전산학과 석사 졸업
- 1992년 5월 : Oklahoma University 전산학과 박사 졸업
- 1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
- 1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
- 2001년 2월~현재 : 고려대학교 정보경영공학전문대학원 교수
- 주관심분야 : 암호프로토콜, RFID/USN 보안, 프라이버시 보호기술