논문 2005-42TC-2-5

패스워드를 변경 가능한 효율적인 패스워드 기반의 인증된 키 교환 프로토콜

(Efficient Password-based Authenticated Key Exchange Protocol with Password Changing)

이 성 운*, 김 현 성**, 유 기 영*

(Sung-Woon Lee, Hyun-Sung Kim, and Kee-Young Yoo)

요 약

본 논문에서는 안전하지 않은 통신상에서 사람이 기억할 수 있는 패스워드를 이용하여 클라이언트와 서버 간에 서로를 인증하고 세션키를 공유하기 위한 패스워드 기반의 인증된 키 교환 프로토콜을 제안한다. 제안된 프로토콜은 인증된 사용자가 자유롭게 자신의 패스워드를 변경할 수 있는 기능을 제공한다. 또한 다양한 공격들에 안전하고 완전한 전방향 보안성을 제공하도록 설계되었다. 더욱이 제안된 프로토콜은 같은 보안 요구 사항을 가지는 기존의 잘 알려진 패스워드 기반의 키 교환 프로토콜들과 비교하여 좋은 성능을 제공한다.

Abstract

In this paper, we propose a password-based authenticated key exchange protocol which authenticates each other and shares a session key using only a small memorable password between a client and a server over an insecure channel. The proposed protocol allows an authenticated client to freely change a his/her own password. The protocol is also secure against various attacks and provides the perfect forward secrecy. Furthermore, it has good efficiency compared with the previously well-known password-based protocols with the same security requirements.

Keywords : Cryptography, Authentication, Password, Key exchange, Key agreement

I. 서 론

인터넷과 같은 개방된 통신 환경에서 안전하게 통신을 하기 위해서는 인증과 메시지 암호화가 필요하다. 이때 메시지 암호화를 위해서는 대칭키 암호화 시스템이 가장 널리 이용되는데 통신에 참여하는 참여자들 사이에 키의 공유가 반드시 선행되어야 한다. 한편, 사용자를 인증하는 방법은 여러 방식이 있지만 패스워드를 이용한 인증은 별도의 장비가 필요 없고 패스워드만을 기억하면 되기 때문에 현재 가장 널리 이용되고 있다. 그러나 이 방법은 사람이 기억할 수 있는 낮은 엔트로피를 가지는 패스워드를 이용하기 때문에 패스워드 추측 공격에 취약할 수 있다.

패스워드 기반의 인증된 키 교환 프로토콜은 안전하지 않은 통신상에서 통신에 참여하는 참여자들 사이에 패스워드를 이용하여 서로를 인증하면서 앞으로의 통신을 암호화하기 위한 세션키를 공유하는 프로토콜이다. 일반적으로 클라이언트-서버 환경에서 사용자는 패스워드를 기억하여 사용하고 서버는 패스워드로부터 유도된 값인 검증자를 패스워드 파일에 미리 저장해두어 프로토콜 수행 중에 해당 클라이언트에 대한 인증을 위한 검증 데이터로 사용한다. 이 방식은 패스워드 파일이

* 정회원, 경북대학교 컴퓨터공학과
(Dept. of Computer Engineering, Kyungpook National Univ.)
** 정회원, 경일대학교 컴퓨터공학과
(Dept. of Computer Engineering, Kyungil Univ.)
※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었음
접수일자: 2003년10월8일, 수정완료일: 2005년2월11일

노출되더라도 공격자는 직접적으로 이 검증자를 이용하여 클라이언트로 위장할 수 없다는 장점을 제공한다.

본 논문에서는 안전하지 않은 통신상에서 사람이 기억할 수 있는 패스워드만을 이용하여 클라이언트와 서버 사이에 서로를 인증하고 세션키를 공유하기 위한 패스워드 기반의 키 교환 프로토콜을 제안한다. 패스워드 기반의 키 교환 프로토콜은 프로토콜 안전성의 대부분을 패스워드에 의존하고 있다. 그러므로 인증된 사용자는 언제든지 자신의 패스워드를 자유롭게 선택하고 변경할 수 있어야 한다. 그러나 대부분의 키 교환 프로토콜들에서는 패스워드 변경에 관하여 고려하지 않기 때문에 별도의 패스워드 변경 프로토콜(예를 들어 Unix의 passwd 명령)을 이용할 수밖에 없다. 그러나 만약 이 패스워드 변경 프로토콜에 취약점이 존재한다면 공격자는 이를 이용하여 키 교환 프로토콜의 안전성을 해칠 수 있다. 제안된 프로토콜은 사용자가 자유롭게 자신의 패스워드를 변경할 수 있는 기능을 제공한다. 더욱이 제안된 프로토콜은 여러 가지 다양한 공격들, 즉 중간 침입자 공격(Man-in-the-middle attack), 패스워드 추측 공격(Password guessing attack), Denning-Sacco 공격, Stolen-verifier 공격, 그리고 서비스 거부 공격(Denial of service)에 안전하며, 완전한 전방향 보안성(Perfect forward secrecy)을 제공한다. 또한 기존의 잘 알려진 패스워드 기반의 키 교환 프로토콜들과 비교하여 좋은 성능을 제공한다.

Ⅱ. 보안 요구사항

패스워드 기반의 키 교환 프로토콜을 다양한 공격들에 대하여 안전하도록 설계하기 위해서는 다음과 같은 보안 요구 사항들이 고려되어야 한다.

① 중간 침입자 공격에 안전해야 한다. 공격자는 통신선로 중간에서 정당한 사용자로 위장하거나 전송 메시지들을 도청, 변경, 반송, 재전송하여 공격할 수 있다. 키 교환 프로토콜은 이러한 공격들에 세션키에 관한 정보를 노출해서는 안되며 잘못된 세션키의 생성을 탐지할 수 있어야 한다.

② 패스워드 추측 공격에 안전해야 한다. 패스워드 추측 공격은 온라인 패스워드 추측 공격과 오프라인 패스워드 추측 공격으로 나뉠 수 있다. 온라인 패스워드 추측 공격은 패스워드 인증 실패 횟수를 제한함으로써 쉽게 막을 수 있다. 그러나 공격자는 안전하지 않은 통신상의 메시지를 가로채거나 정당한 사용자로 가장하여 다른 사용자와 세션키를 공유하는 과정 중에 발생하는 정보들을 저장해두고 오프라인으로 패스워드에 관한 정보를 알아내려고 할 수 있다. 이러한 오프라인 패스워드 추측 공격은 패스워드를 사용하는 키 교환 프로토콜들에 있어서 가장 큰 위협이다.

③ Denning-Sacco 공격에 안전해야 한다. 즉 공격자가 임의의 세션키를 알았다 할지라도 그 동안 통신상에서 도청한 메시지들을 이용하여 패스워드에 관한 정보를 알 수 없어야 한다.

④ Stolen-verifier 공격에 안전해야 한다. 서버는 보통 클라이언트의 패스워드를 검증하기 위한 검증자(Verifier)를 패스워드 파일에 저장한다. 클라이언트가 패스워드를 안전하게 유지한다할지라도 서버의 패스워드 파일의 손상에 대한 위협은 여전히 존재할 수 있다. Stolen-verifier 공격은 서버로부터 패스워드 검증자를 훔친 공격자가 직접적으로 합법적인 사용자로 위장하려는 공격을 의미한다.

⑤ 완전한 전방향 보안성을 제공해야 한다. 공격자가 참여자의 패스워드를 알아내었다 할지라도 이전에 사용된 세션키에 관한 정보는 알 수 없어야 한다.

패스워드 변경 프로토콜은 인증된 사용자가 자신의 패스워드를 변경할 수 있는 프로토콜이다. 패스워드를 변경하는 프로토콜은 위에 언급된 공격들 이외에 다음과 같은 공격에도 안전해야 한다.

⑥ 서비스 거부 공격에 안전해야 한다. 서비스 거부 공격은 통신 시설의 정상적인 사용이나 관리를 불가능하게 하는 공격이다. 예를 들어 공격자는 이 공격을 수행하여 서버가 특정 사용자의 로긴 요청을 계속적로 허용하지 못하게 할 수 있다.

Ⅲ. 제안된 프로토콜

본 장에서는 클라이언트-서버 환경에서 패스워드를 이용하여 서로를 인증하고 세션키를 공유하며 클라이언트가 자유롭게 자신의 패스워드를 변경할 수 있는 패스워드 기반의 키 교환 프로토콜을 제안한다.

표 1. 기호
Table 1. Notation.

기호	설명
p	큰 소수 (보통 최소 1024 bit)
q	q	p-1인 상대적으로 적은 소수 (보통 160 bit)
G_q	곱셈군 Z_p^*의 부분군 (q order)
A, B	각각 클라이언트와 서버에 대한 식별자
g	G_q 의 생성자 (Generator)
π	클라이언트의 패스워드
v_1, v_2	서버에 저장되는 패스워드 검증자(Verifier)
a, b	G_q 상의 임의의 원소
h_1, h_2, h_3	Collision-free 일방향 해쉬 함수
$\oplus$	비트 Exclusive-OR 연산
K	세션키
$[M]_k$	암호화 키 k를 이용한 대칭키 암호화 연산

1. 초기설정

제안된 프로토콜에서 사용할 기호들은 [표 1]과 같다. 프로토콜이 시작하기 전에 클라이언트 A는 패스워드 π를 기억하고 있고 서버 B는 A를 인증하기 위한 검증자 $v_1 = h(A, B, \pi)^{-1}$과 $v_2 = g^{h(A,B,\pi)-1}$를 패스워드 파일에 저장하고 있다고 가정한다. 'mod p' 연산 표기는 생략하기로 한다.

2. 프로토콜의 수행

제안된 프로토콜은 다음과 같이 수행한다.

단계 1. A는 임의의 정수 a를 선택하고 $v_1 = h_1(A, B, \pi)$과 $X_A = g^a \oplus v_1$를 계산하여 자신의 ID와 X_A를 B에게 전송한다. 그리고 B의 응답을 기다리는 동안 $t = h_2(A, B, \pi)$를 계산한다.

단계 2. A로부터 메시지를 받으면 B는 패스워드 파일로부터 A의 검증자 v_1과 v_2를 검색하고 임의의 정수 b를 선택하여 $X_B = (v_2)^b \oplus v_1$를 계산한 후 X_B를 A에게 전송한다. 그리고 B는 A의 응답을 기다리는 동안 $K_B = (X_A \oplus v_1)^b = g^{ab}$와 $V_B = [B, X_A]_{K_B}$를 계산한다.

단계 3. B로부터 X_B를 받으면 A는 $K_A = (X_B \oplus v_1)^{at} = g^{ab}$와 $V_A = [A, X_B]_{K_A}$를 계산하고 V_A를 B에게 전송한다.

단계 4. B는 A로부터 V_A를 받은 후에 K_B를 사용함으로 V_A를 복호화하고 메시지의 송신자와 X_B가 정확한지를 검사하고 정확하다면 V_B를 A에게 전송한다.

단계 5. A는 B로부터 V_B를 받은 후에 K_A를 사용하여 V_B를 복호화하고 X_A가 정확한지를 검사한다.

단계 6. 마지막으로 A와 B는 각각 세션키 $K = h_3(A, B, K_A) = h_3(A, B, K_B) = h_3(A, B, g^{ab})$를 계산한다.

제안한 프로토콜의 수행을 간단히 요약하면 [그림 1]과 같다. [그림 1]에 있는 '{ }'안의 내용은 클라이언트 A가 필요시에 자신의 패스워드를 변경하는 과정이다. 즉 A가 패스워드를 변경하고자 한다면 위 프로토콜의 3단계와 4 단계를 다음과 같이 수행한다.

단계 3. B로부터 X_B를 받으면 A는 $K_A = (X_B \oplus v_1)^{at} = g^{ab}$를 계산한다. 또한 A는 패스워드를 변경하기 위하여 새로운 패스워드 π'를 선택하고 새로운 검증자 $v_1' = h_1(A, B, \pi')$와 $v_2' = g^{h_2(A,B,\pi')-1}$를 계산한다. 그리고 $V_A = [A, X_B, \{v_1', v_2'\}]_{K_A}$를 계산하여 B에게 전송한다.

단계 4. B는 A로부터 V_A를 받은 후에 K_B를 사용함으로 V_A를 복호화하고 A, X_B, v_1', v_2'를 구한다. 메시지의 송신자와 X_B가 정확한지를 검사하고 정확하다면 새로운 검증자 v_1'와 v_2'를 패스워드 파일에 저장한다. 그리고 V_B를 A에게 전송한다.

Ⅳ. 안전성 분석

프로토콜에 참여하는 참여자들 사이의 모든 통신은 공격자의 제어 하에 있다고 가정하자. 그리고 제안된 프로토콜은 DES나 AES와 같은 안전한 대칭키 암호화 시스템을 사용한다고 가정한다. 또한 이산대수 문제와 Diffie- Hellman 문제[8]를 다항식 시간에 풀 수 있는 확률이 각각 무시할만하다고 가정한다.

1. 중간 침입자 공격

공격자는 정당한 사용자로 위장하거나 통신 선로 중간에서 전송 메시지들을 도청하거나, 변경, 반송, 재전송하여 공격할 수 있다. 첫째로, 공격자는 전송 메시지들을 도청하여 $X_A = g^a \oplus h_1(A,B,\pi)$, $X_B = g^{b \cdot h_2(A,B,\pi)^{-1}} \oplus h_1(A,B,\pi)$, $V_A = [A, X_B, \{v_1', v_2'\}]_{K_A}$, $V_B = [B, X_A]_{K_B}$를 얻을 수 있다. 그러나 공격자가 이 값들을 획득한다 하더라도 패스워드 π와 세션키 K를 계산할 수 있는 방법은 존재하지 않는다. 둘째로, 공격자가

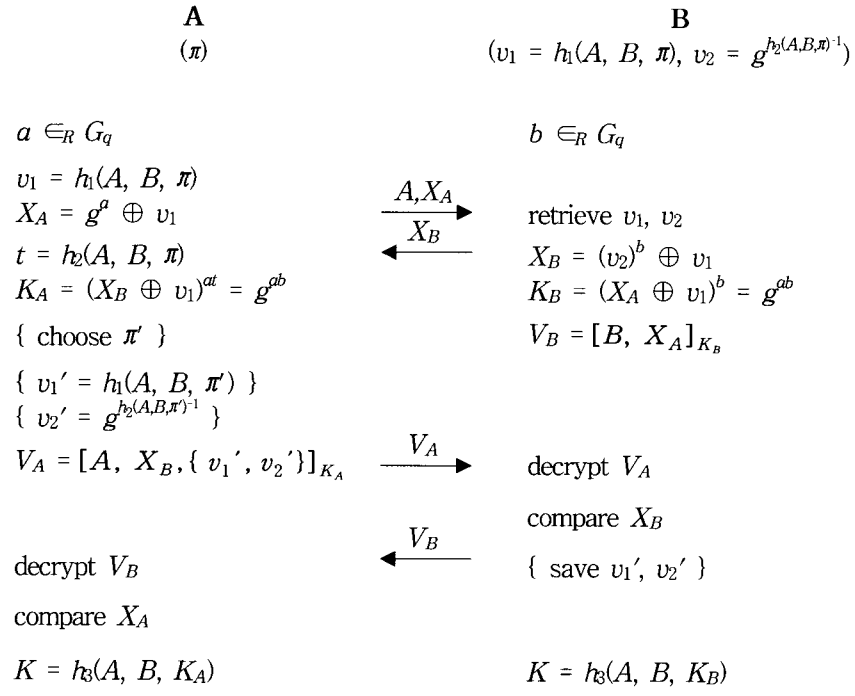

그림 1. 제안한 프로토콜
Fig. 1. The proposed protocol.

X_A와 X_B를 중간에서 수정하여 상대에게 전송한다면, 이 위조된 값들은 A와 B에 의해 K_A와 K_B를 생성하는 데 각각 사용되게 된다. 그러나 A는 임의의 정수 $a \in_R G_q$를 사용하여 K_A를 계산하고 B는 임의의 정수 $b \in_R G_q$를 사용하여 K_B를 계산하기 때문에 K_A와 K_B의 값이 같게 될 확률은 무시할만하다. 결국, 이 공격은 K_A와 K_B를 다르게 만들므로 검증 시에 각 참여자가 정확한 X_A와 X_B를 얻을 수 없어 탐지될 수밖에 없다. 셋째로, 이전 세션의 전송 메시지들을 저장해 두었다가 이후 세션들에 이용하는 재전송 공격을 고려하자. 그러나 매 세션마다 각 참여자들은 새로운 임의의 난수 a와 b를 생성하여 사용한다. 공격자가 이 난수들을 알 수 있는 확률은 무시할 만하다. 넷째로, 공격자는 합법적인 참여자로 위장하여 정상적인 방법으로 다른 참여자와 세션키를 공유하려고 할 수 있다. 그러나 이러한 위장 공격은 공격자가 패스워드를 알지 못하기 때문에 합법적인 참여자가 생성한 정확한 세션키를 생성할 수 없어 검증 시에 탐지될 수밖에 없다. 결국 제안한 프로토콜들은 중간 침입자 공격들에 안전하다.

2. 오프라인 패스워드 추측 공격

첫 번째로 도청한 메시지만을 이용하는 수동적인 오프라인 패스워드 추측 공격을 고려하자. 공격자는 먼저 메시지 X_A, X_B, V_A, V_B를 도청하여 저장하고, 패스워드로 사용될 수 있는 π'를 추측한다. 그리고 π'를 도청한 값들에 적용하여 그 값들을 비교함으로 추측한 π'가 정확한 값인지를 검증한다. 이를 모든 패스워드 범위에 대하여 반복 수행함으로써 추측한 π'가 참여자들이 사용하고 있는 정확한 π인지를 확인할 수 있어야 한다. 그러나 제안된 프로토콜에서는 전송 메시지인 X_A, X_B, V_A, V_B에 π'를 적용하여도 π'가 정확한지를 검증할 방법이 존재하지 않는다.

두 번째로 공격자가 정당한 참여자로 위장한 적극적인 오프라인 패스워드 추측 공격을 고려해 보자. 공격자가 A로 위장한다면 자신이 만든 a와 g^a, 그리고 B로부터 받은 $g^{b \cdot h_2(A,B,\pi)^{-1}} \oplus h_1(A,B,\pi)$를 얻을 수 있다. 그러나 이 값들을 이용하여 추측한 π'가 정확한지를 검증할 방법이 존재하지 않는다. 또한 만약 공격자가 B로 위장한다면 자신이 생성한 b와 g^b, 그리고 A로부터 받은 $g^a \oplus h_1(A,B,\pi)$와 $[A, g^b]_{(g^b \oplus h_1(A,B,\pi))^{a \cdot h_2(A,B,\pi)}}$을 얻을 수 있다. 그러나 이 값들을 이용해서도 추측한 π'가 정확한지를 검증할 방법이 존재하지 않는다. 그러므로 제안된 프로토콜은 오프라인 패스워드 추측 공격에 안전하다.

3. Denning-Sacco 공격

Denning-Sacco 공격은 세션키가 노출되었을 때 공

표 2. 관련 프로토콜들과의 효율성 비교
Table 2. Efficiency comparison with the related protocols.

분석요인 / 프로토콜	통신횟수	랜덤정수 생성횟수	지수연산 횟수			해쉬연산 횟수	대칭키 연산 횟수
			A	B	병렬		
B-SPEKE	4	3	3	4	6	4	4
SRP	4	2	3	3	4	7	0
SNAPI-X	5	5	5	4	7	7	0
PAK-X	3	3	4	4	8	10	0
AMP	4	2	2	3	3	9	0
AuthA	3	2	3	3	5	8	4
제안된 프로토콜	4	2	2	2	3	2	4

격자가 패스워드에 관한 정보를 얻고자 하는 공격이다. 제안된 프로토콜들에서 공격자가 임의의 세션에서 도청을 통해 X_A, X_B, V_A, V_B를 얻었고, 세션키 $h(A, B, g^{ab})$가 공격자에게 노출되었다고 가정하자. 그러나 공격자는 이 값들로부터 패스워드 π를 계산하거나 추측한 패스워드의 정확성을 검증할 방법은 존재하지 않는다.

4. Stolen-verifier 공격

Stolen-verifier 공격은 서버로부터 패스워드 검증자를 훔친 공격자가 직접적으로 합법적인 사용자로 위장하려는 공격을 의미한다. 제안된 프로토콜에서 서버에 저장된 패스워드 검증자는 $v_1 = h_1(A, B, \pi)$와 $v_2 = g^{h_2(A,B,\pi)^{-1}}$이다. 그러나 이 값들을 훔친 공격자는 새로운 세션의 3단계에서 사용해야 하는 t를 구할 수 없으므로 직접적으로 사용자로 위장할 수 없다.

5. 완전한 전방향 보안성

완전한 전방향 보안성을 제공하기 위해서는 패스워드가 공격자에게 노출되었다 할지라도 이전의 세션키들은 안전해야 한다. 제안된 프로토콜에서 공격자에게 패스워드 π가 노출되었다고 하자. 공격자는 도청을 통해 X_A, X_B, V_A, V_B를 얻을 수 있다. 그러나 공격자가 이산대수 문제나 Diffie-Hellman 문제를 풀지 않고는 이 정보들로부터 g^{ab}를 구할 방법은 존재하지 않는다.

6. 서비스 거부 (Denial of Service) 공격

제안된 프로토콜에서 공격자가 서버로 하여금 계속적으로 특정 사용자에 대한 인증을 거부하도록 하려면 사용자가 의도하지 않은 패스워드 검증자를 서버가 저장하도록 할 수 있어야 한다. 그러나 공격자는 세션키를 알지 못하기 때문에 패스워드 검증자를 자신이 생성한 값으로 대체시킬 수 없다.

V. 효율성 분석

키 교환 프로토콜의 효율성은 통신 부하와 계산 부하 측면에서 평가될 수 있다. 통신 횟수는 통신 부하를 측정하는 기준이고 랜덤 정수 생성 횟수, 지수 연산 횟수, 해쉬 연산 횟수, 대칭키 연산 횟수는 계산 부하를 측정하기 위한 기준들이다. 이들 중에서 지수 연산은 다른 연산들에 비해 상대적으로 많은 수행 시간(해쉬 연산이나 대칭키 연산에 비해 100 ~ 1000 배 느림)을 필요로 하므로 프로토콜의 성능 측정에 있어서 가장 중요한 요소라 할 수 있다. 일반적으로 대칭키 연산과 해쉬 연산의 속도는 비슷하다고 여겨진다. [표 2]는 제안된 프로토콜을 IEEE P1363.2[1]에 제출된 PAK-X[2], AMP[3], B-SPEKE[4], SRP[5], SNAPI-X[6], AuthA[7]들과 비교한다. 비교되는 이 프로토콜들은 모두 패스워드를 변경하는 기능을 제공하지 않음으로 공정한 비교를 위해 제안된 프로토콜에서 패스워드를 변경하는 과정에 필요한 연산들은 이 비교에서 제외한다.

[표 2]는 제안된 프로토콜이 계산 부하 면에서 가장 효율적임을 보여준다. 특히, 제안된 프로토콜의 지수 연산 횟수는 가장 작다. 프로토콜의 전체 수행시간을 비교하기 위해 지수 연산의 병렬 수행 횟수를 고려해 보자. 지수 연산 병렬 수행 횟수는 두 참여자 사이에 비슷한 시간에 수행되는 지수연산 횟수를 의미한다. 제안된 프로토콜은 두 참여자 사이에 병렬로 지수 연산을 세 번 수행한다. 이것 또한 다른 프로토콜들에 비하여 AMP와 함께 가장 효율적이다.

제안된 프로토콜은 통신 횟수 측면에서 4회의 통신을 한다. 몇몇 프로토콜들은 통신비용을 줄이기 위해 3

번의 메시지 교환을 채택하고 있다. 그러나 이 방법은 통신비용은 줄일 수 있지만 두 참여자 사이의 연산 수행을 직렬화시킨다. 즉 한 참여자의 응답을 받은 후에야 자신의 다음 연산을 수행할 수 있다. 그래서 프로토콜의 전체 수행 시간은 길어질 수밖에 없다. 이러한 이유로 제안된 프로토콜에서는 4번의 메시지 교환을 채택하였다. 그러나 제안된 프로토콜을 적은 통신 부하를 요구하는 응용들을 위하여 3회의 통신을 수행하는 프로토콜로 변형하기는 매우 쉽다. 연산에 대한 수정 없이 통신 흐름만을 $A \xrightarrow{A, X_A} B \xrightarrow{X_B, V_A} A \xrightarrow{V_B} B$ 형태로 변형하면 된다.

VI. 결 론

패스워드 기반의 프로토콜은 사람들이 패스워드와 같은 작은 지식만을 기억하면 되기 때문에 널리 이용되고 있다. 본 논문에서는 클라이언트-서버 환경에서 사용될 수 있는 상호 인증 가능하고 한 개의 세션키를 생성하는 패스워드 기반의 키 교환 프로토콜을 제안하였다. 이 프로토콜은 다양한 공격에 안전하고 완전한 전방향 보안성을 제공하도록 설계되었다. 더욱이 기존의 패스워드 검증자 기반의 프로토콜들과 비교하여 좋은 효율성을 제공한다.

참 고 문 헌

[1] IEEE. Standard Specifications for Public Key Cryptography, *IEEE1363*, 2002.

[2] V. Boyko, P. MacKenzie and S. Patel. "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," *Advances in Cryptology-EUROCRYPT*, pp. 156-171, 2000.

[3] T. Kwon. "Ultimate Solution to Authentication via Memorable Password," *IEEE P1363a*, May 2000.

[4] D. Jablon. "Extended password key exchange protocols," *WETICE Workshop on Enterprise Security*, 1997.

[5] T. Wu. "Secure remote password protocol," *Internet Society Symposium on Network and Distributed System Security*, pp. 97-111, 1998.

[6] P. MacKenzie, S. Patel, and R. Swaminathan. "Password-authenticated key exchange based on RSA." *ASIACRYPT*, 2000.

[7] M. Bellare and P. Rogaway, "The AuthA protocol for password-based authenticated key exchange," *IEEE P1363a*, 2000.

[8] D. R. Stinson, *Cryptography Theory and Practice*, CRC, 1995.

저 자 소 개

이 성 운(정회원)

1993년 전남대학교 전산통계학과 학사 졸업.

1996년 전남대학교 전산통계학과 석사 졸업.

2005년 경북대학교 컴퓨터공학과 박사 졸업.

<주관심분야 : 정보보호, 암호 프로토콜, 네트워크 보안>

유 기 영(정회원)

1976년 경북대학교 수학교육과 학사 졸업.

1978년 한국과학기술원 컴퓨터공학과 석사 졸업.

1992년 Ph.D. degree in computer science from Rensselaer Polytechnic Institute, New York, U.S.A.

1980년~현재 경북대학교 컴퓨터공학과 교수

<주관심분야 : 정보보호, 암호학, 암호칩 설계, 유비쿼터스 보안>

김 현 성(정회원)

1996년 경일대학교 컴퓨터공학과 학사 졸업.

1998년 경북대학교 컴퓨터공학과 석사 졸업.

2002년 경북대학교 컴퓨터공학과 박사 졸업.

2002년~현재 경일대학교 컴퓨터공학과 교수

<주관심분야 : 정보보호, 암호칩 설계, 네트워크 보안>