IEEE Std 802.1x 사용자 인증을 위한 분할된 패스워드 인증 기반 EAP

EAP Using Split Password-based Authenticated Key Agreement Protocol for IEEE Std 802.1x User Authentication

유 종 호* 서 동 일** 염 흥 열***
Ryu, Jong Ho Seo, Dong Il Youm, Heung Youl

요 약

EAP(Extensible Authentication Protocol)는 IEEE Std 802.1x 무선 근거리 통신망 및 RADIUS/DIAMETER 프로토콜을 기반으로 각 개체에 대한 인증을 제공하며 인증의 수단으로 인증서, 패스워드, 이중방식(패스워드 및 토큰) 등을 이용한다. 인증된 키교환을 위한 패스워드 기반 인증 방식은 특정 하드웨어 장치 없이도 암기하기 쉬운 간편성, 편리성, 이동성으로 인해 상당히 많이 이용되는 사용자 인증 방식이다. 본 논문에서는 개방형 네트워크를 통해서도 사용자를 인증하고 안전한 암호통신용 세션키 교환에 적합한 패스워드 기반 인증된 키교환 프로토콜 SPAKE(Split Password-based Authenticated Key Exchange)을 제안한다. 더불어 제안된 SPAKE를 토대로 안전한 EAP 인증 프레임워크 EAP-SPAKE를 제시한다.

Abstract

EAP provides authentication for each entity based on IEEE Std 802.1x Wireless LAN and RADIUS/DIAMETER protocol, and it uses certificate, dual scheme(e.g., password and token) with the authentication method. The password-based authentication scheme for authenticated key exchange is the most widely-used user authentication method due to various advantages, such as human-memorable simplicity, convenience, mobility. A specific hardware device is also unnecessary. This paper discusses user authentication via public networks and proposes the Split Password-based Authenticated Key Exchange (SPAKE), which is ideal for both authenticating users and exchanging session keys when using a subsequent secure communication over untrusted network. And then we provides EAP authentication framework EAP-SPAKE by using it.

☞ Keyword : EAP Password Authentication Key Agreement

1. 서 론

2003년 독일 하노버(Hannover)에서 개최된 CeBIT (Center for Bureau, Information, Telecommunication)에서의 이슈는 셀룰러 폰과 무선인터넷 제품의 통합이였다. 예로 사용자의 개인휴대 단말기 PDA가 인터넷 사업자(ISP)들이 설치한 핫스팟(hotspot) 지역의 AP(Access Point)와 통신이 가능하다면 누구라도 공중 무선랜(Public Wireless LAN) 서비스를 제공받을 있게 된다. 04년 말에 들어서는 국내연구기관 ETRI가 이와 같은 국제적 대세를 선도하고 기존 유/무선 인터넷의 단점, 즉 유선 인터넷의 공간적 제약과 모바일 인터넷 서비스의 낮은 전송속도를 극복한 초고속 휴대용 인터넷 서비스 2.3GHz WiBro(Wireless Broadband) 30MBps 시제품을 개발하게 된다.

일반적으로 공중 무선랜은 일반 기업내의 무선랜과 다르게 AAA(Authentication, Authorization, Accounting)[RFC3539], 접근제어, 사업자간 로밍 등 여러 가지 고려해야 할 사항들이 많이 존재한

* 정 회 원 : 한국전자통신연구원 정보보호연구단 연구원
ryubell@etri.re.kr(제1저자)
** 정 회 원 : 한국전자통신연구원 정보보호연구단 팀장
bluesea@etri.re.kr(공동저자)
*** 정 회 원 : 순천향대학교 산학연컨소시엄센터 소장
hyyoum@sch.ac.kr(공동저자)
[2004/12/30 투고 - 2005/03/14 심사 - 2005/05/27 심사완료]

다. 특히 공개된 무선매체에 대한 보안성이 가장 중요한 부분으로 인식하고 있다.

2001년 IEEE Std 802.11 작업반에서는 무선 랜 시스템의 보안성을 개선하기 위하여 인증 개념을 포함하는 포트 기반 네트워크 인증(port based network authentication)의 802.1x 규격을 정립하였다. 가입자와 인증서버 사이의 인증 데이터를 전달하기 위하여 802.1x에서는 EAP(Extensible Authentication Protocol)[RFC2284]를 표준 프로토콜로 이용하고 있으며, 현재 EAP 방식들로는 패스워드 기반의 EAP-MD5(EAP Message Digest 5)[RFC2284], EAP-SRP(EAP Secure Remote Password)[1], 인증서 기반의 EAP-TLS(EAP Transport Layer Security)[RFC2716] 그리고 패스워드와 인증서를 모두 사용하는 EAP-TTLS(EAP Tunneled TLS)[2], EAP-PEAP(EAP Protected EAP) 등으로 분류할 수 있다[3,4].

본 논문에서는 새롭게 제안된 분할된 패스워드 기반 인증된 키교환 프로토콜 SPAKE(Split Password- based Authenticated Key Exchange)을 기반으로 EAP에 적합한 EAP-SPAKE 방식을 제안한다. 제안된 방식은 기존 제안 방식 EAP-SRP 보다 보안성 및 효율성이 개선되었다.

1.1 패스워드 기반 인증된 키교환 프로토콜

패스워드는 암기하기 쉬운 간편성 및 편리성으로 인하여 개방된 네트워크에서 주로 이용되고 있는 사용자 인증 수단이다. 그러나 패스워드는 인간의 짧은 기억에 의해 유지됨에 따라 다양한 추측공격에 노출된다. 즉 패스워드의 엔트로피(entropy)는 컴퓨팅 능력에 비해 상대적으로 작은량이며 동시에 패스워드 변화 패턴은 한계를 지니고 있기 때문에 다양한 유형의 공격에 노출될 확률이 높다[5-11].

1992년 Bellovin과 Merritt가 EKE(Encrypted Key Exchange)[10]로 알려진 논문을 발표한 것을 필두로, 추측공격에 강하게 저항하도록 패스워드 정보와 공개키 암호 알고리즘인 DLP(Discrete Logarithm Problem) 기반의 DH(Diffie-Hellman), RSA, 타원곡선(Elliptic Curve) 공개키 알고리즘, 그리고 램덤 오라클(random oracle) 모델인 일방향 해쉬함수 등을 접목시킴으로써 안전성을 향상시켜왔다.

PAK[5], SRP[11], AuthA[12] 등 에서는 클라이언트와 서버가 서로 간에 비동일 정보를 기억하는 검증자-파일(verifier-file)기반 프로토콜들을 제안하였다. 추측공격(guessing attack)을 배제한 경우에, 공개키 암호방식과 접목된 이들 방식들은 검증자-파일로부터 패스워드를 유도하는 것이 계산적으로 불가능하다. 그러나 만일 공격자(adversary)에 의해 서버의 검증자-파일이 타협된다면 검증자-파일 기반 프로토콜조차 여전히 추가적 사전 추측공격(additional dictionary guessing attack)을 허용하게 된다[8]. 이 문제에 대한 해결책으로 가장 좋은 방법은 첫째로 AMP[6,7,9] 및 EPA[8]에서와 같이 검증자-파일을 서버의 비밀키로 암호화하여 보관하거나, 또는 둘째로 [13,14]에서와 같이 서버의 검증자-파일을 임계치 비밀분산 방식(threshold secret sharing scheme)을 통해 분배시키는 것이다[6]. 첫 번째 방법에 있어서의 AMP와 EPA는 비대칭적인 모델로 각 클라이언트는 패스워드만을 지니고 이에 대응되는 서버는 확대된 패스워드 파일(amplified password file, AMP[6]에서 소개)을 이용함으로써, 서버의 패스워드 파일이 타협되었다하더라도 추가적 사전 추측공격 및 서버가장(server impersonation) 공격에 대하여 안전하도록 설계한 것이다. 특히 TP-AMP(Three-Pass AMP)[9]과 EPA는 이전에 제안된 프로토콜들[5,6,7,11]의 보안 요구사항(security requirement)을 모두 만족시키면서도 더 작은 계산 용량 및 통신 부하용량을 지닌다. TP-AMP에서는 4-단계 통신 교환 횟수의 AMP[6,7] 프로토콜을 좀더 복잡한 메커니즘을 지닌 3-단계 프로토콜로 개선한 것이다. EPA는 통신 교환 횟수 및 멱승(exponentiation) 연산량을 줄이기 위하여 변형 확대된 패스워드 파일(modified amplified password file) 개념을 도입하고 서로 다른 두 순환군(cyclic group)

을 바탕으로 설계되었다. 이 EPA는 통신 교환 횟수, 총 멱승 계산량, 그리고 교환 데이터 크기 측면에서 기존 제안된 방식 보다 효율적이기는 하지만, 두 개의 생성원(generator)을 사용해야 한다는 점이 응용에 있어서 제한을 두게 만든다.

앞서 설명된 사항과 별도로 패스워드를 분할하여 처리하는 사례를 [7,15], 그리고 [16]에서 찾아볼 수 있다. [15]는 다수의 서버들을 통해 RSA 알고리즘을 구동하는 실제적인 VSTP(Virtual Software Token Protocol)을 제시함과 동시에 특정 유형의 패스워드 분할 방식은 이른바 분할 온-라인 공격(split on-line attack)에 취약하다는 점을 보여주었다. [15]에 제시된 VSTP는 기본적으로 클라이언트의 분할된 패스워드 $\pi = \pi_1 \| \cdots \| \pi_m$과 분할된 패스워드에 대한 각 서버들 $S_i (i = 1, \cdots, m)$의 검증자-파일 v_i간에 일대일 대응관계를 맺도록 구성되며 프로토콜 수행시 병행(parallel)으로 처리된다. [16]에서는 서로 다른 터미널(terminal)을 사용하는 로밍(roaming) 사용자가 단순히 패스워드 인증만을 통해 크리덴셜(credential) 서버에 접근한다면, 문제(즉 패스워드 추측 공격)가 발생할 수 있음을 설명하고 동시에 이에 대한 해결책을 제시하였다. 우선적으로 이 프로토콜에서 다수의 서버들 $S_i (i = 1, \cdots, m)$은 클라이언트와 협력하여 패스워드 π로부터 각 서버 고유의 고정 패스워드 R_i을 생성한다. 보안특성에 의해 이후 어떠한 서버도 모든 R_i 및 패스워드 π을 유도할 수는 없다. 클라이언트는 R_i을 이용하여 강한 비밀정보 $K_i = KDF(R_1, \cdots, R_m, i)$을 생성한 후 이 값을 통해 서버들 S_i에게서 인증을 받는다. 여기에서 KDF는 키유도 함수(key derivation function)이다. [15]는 사용자가 패스워드를 분할한 다음 이를 이용하여 각 서버들과 독자적인 프로토콜을 수행(즉 병행 처리)하는 반면, [16]은 각 서버가 저장한 연관 정보 R_i로부터 $K_i = KDF(R_1, \cdots, R_m, i)$을 유도한 다음 이를 이용하여 인증을 수행하게 된다.

1.2 SPAKE의 제안

지금까지 기술된 사항을 토대로 본 논문 3장에 제안된 패스워드 기반 인증된 키교환 프로토콜 설계목표는 Bellare와 Rogaway가 AuthA[12]에서 제시한 "패스워드 기반 키교환 방식의 설계에서 고려해야할 요구사항"을 만족시키는 새로운 프로토콜 SPAKE을 설계하는 것에 있으며, 또한 다음과 같은 특성을 지니도록 한다.

(1) 키동의 구조는 DH 키동의를 바탕으로 구성되며, 안전성은 DLP에 기반 하여 설계된다.

(2) 검증자-파일 기반 인증구조(즉 비대칭적인 모델)로 구성하고 서버 파일 타협에 의한 서버가장 공격 및 오프라인(off-line) 사전추측 공격에 강인하도록 설계한다. 이를 위하여 AMP[6]와 같이 서버의 파일을 암호화하여 보관한다. 이것은 [6]과 [17]에서 지적한 것처럼 안전한 저장장치(예, 스마트카드)에 보관된 암호화 키가 만일 저성능 장치에 의하여 통제된다면 컴퓨팅의 병목현상이 야기 될 수 있다. 그러나 서버 암호화 키가 타협되지 않는다면 이는 검증자-파일 보관에 있어서 가장 안전한 구조이기도 하다. 서버의 파일을 암호화하는 방식으로는 AMP[6,7,9]와 EPA[8]를 대표적으로 들 수 있다. 본 논문에서 제안된 방식 역시 이와 같은 보안 구조를 지니게 때문에 AMP 및 EPA와 유사한 방식으로 볼 수 있다. 그러나 본 논문에서 제안 프로토콜은 패스워드를 분할하여 구성한다는 차이점을 지닌다.

(3) 패스워드 검증자-파일의 램덤성(randomness)을 증가시키기 위하여, 패스워드를 분할한 후 이에 대한 각 패스워드 파일을 확대(amplification)하는 구조로 설계한다(패스워드 분할한 사례는 [7,15,16]을 참조, 또한 확대 개념은 [6-9]를 참조). 단 분할된 패스워드 파일들의 확대는 공격자가 더 많은 정보를 분석해야 함을 의미 할뿐 패스워드 엔트로피(entropy)의 증가를 의미하는 것은 아니다.

1.3 EAP-SPAKE : SPAKE을 적용한 EAP 인증

패스워드 기반 인증 방식을 적용한 EAP 방식들로는 대표적으로 EAP-MD5 그리고 EAP-SRP을 들 수 있다. 본 논문 4장에 제안된 EAP-SPAKE는 1.2절에 언급된 SPAKE을 EAP 인증 유형으로 확장한 것이라 여길 수 있으며 다음과 같은 특성을 지닌다.

(1) 인증 프로토콜은 제안된 패스워드 기반 인증 방식인 SPAKE을 적용한다. SPAKE는 [5-11]에 제시된 보안 요구사항을 만족시키면서도 메시지 교환, 지수승, 난수 생성 등 연산 측면에서 SRP보다 효율적이기 때문에, 제안된 방식 EAP-SPAKE는 SRP를 이용한 EAP-SRP 보다 효과적인 실현이 가능하다.

(2) EAP-SPAKE 패킷 형식(packet format)은 기본적으로 EAP-SRP 패킷 형식을 따르도록 한다. 단 SRP 인증 방식과 SPAKE 인증 방식의 차이점으로 인하여 Subtype 필드(field) 및 Subtype-Data 필드는 서로 다른 형식을 적용하게 되나 상세 사항은 본 논문에서 설명하지 않을 것이다.

(3) 기존 알려진 공격에 강하게 저항하도록 한다. EAP-SPAKE는 서버의 검증자-파일을 암호화하여 보관하기 때문에 기존 알려진 공격에 상대적으로 가장 강인하다. 반면 EAP-MD5는 단순한 오프라인 사전공격에도 취약하고, EAP-SRP은 서버 파일 타협에 의한 추가적 사전공격에 취약하다.

1.4 논문의 구성

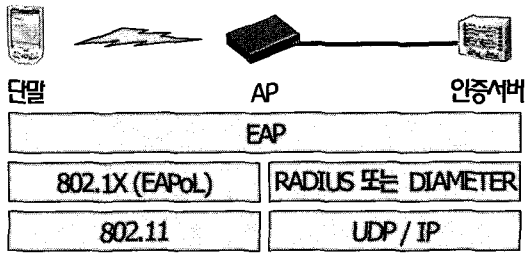
언급된 내용을 기술하기 위하여 우선적으로 2장에서는 802.1x 대한 개요 및 EAP 인증 유형을 설명하다. 3장에서는 제안된 패스워드 기반 인증 및 키교환 프로토콜 SPAKE 대하여 논하고, SPAKE의 안전성 및 효율성에 대하여 분석한다. 4장에서는 SPAKE에 바탕 둔 새로운 무선 근거리 통신망 인증 방식 EAP-SPAKE을 제안하며, 제안된 방식의 보안 특성 및 연산량에 대하여 검토한다. 마지막 5장에 향후 연구 방향 및 결론을 기술한다.

2. IEEE Std 802.1x 기반 무선통신 및 EAP 인증 유형

2.1 IEEE Std 802.1x 기반 무선통신

IEEE Std 802.1x는 무선랜 가입자의 상호인증 방법과 무선 접속구간 보안에 필요한 마스터 세션 키를 랜덤하게 생성하기 위한 방법을 정의한 규격이며, 무선 클라이언트와 인증 서버 간에 EAP를 통해 인증 정보를 교환하는 내용을 골자로 하고 있다.

802.1x의 목표는 수행된 인증과정을 통해 사용자들의 개별적인 과금 정책이나, 사용제한, 대역할당 등 망 접근에 있어 개인별로 제어할 수 있도록 한다. 802.1x 규정에 따르는 시스템 구성요소는 그림 1과 같이 단말(supplicant) 기능을 수행하는 클라이언트와 인증자(authenticator) 기능을 수행하는 브리지 또는 AP, 그리고 인증자와 연결된 인증서버(AS, Authentication Server, 보통 RADIUS [RFC2865]/DIAMETER[RFC3588] 인증서버)로 구성되며 단말과 인증서버 간 인증 프로토콜은 기본적으로 EAP를 사용한다. LAN 구간에서는 EAPoL(EAP over LAN) 프로토콜로 EAP 패킷이 앤캡슐(encapsulation)되어 AP로 전달되고, AP는 이 EAPoL 프레임의 EAP 부분을 인증서버에 전달한다.



〈그림 1〉 IEEE Std 802.1x 기반 무선통신의 개요

2.2 802.1x 프로토콜 동작

802.1x 프로토콜의 동작은 클라이언트(단말)가 먼저 접속을 시도하는 경우에 EAPoL-Start 메시지를 AP에게 보낸다. AP는 EAPoL-Start메시지를 받으면 가입자 인증에 필요한 가입자 신원(ID, identity)정보를 클라이언트에게 요청한다. 클라이언트로부터 받은 신원정보는 AAA EAP-속성(attribute) 메시지에 담겨져서 인증서버에게 전달되고, 최종적으로 AP는 인증서버로부터 인증 성공/실패 메시지(Access Accept/Failure)를 받으면 인증과정이 종료된다. 이때 인증과정에서 생성된 마스터 세션키(master session key)는 Access-Accept 메시지에 담겨져서 AP로 전달된다. 그 다음 AP는 EAPoL-Key 메시지를 이용하여 단말과 키교환을 수행함으로써 키 사용 시점을 동기화 한다. 그 후 EAP-Success 메시지를 통해 동기된 키로 암호화 하여 보냄으로써 802.1x를 이용한 무선랜 접속이 허용되었음을 단말에게 알린다[3].

2.3 EAP 인증 유형[3,4]

802.1x를 구현하는 방식에는 EAP에 따라 여러 방식(EAP-TLS, EAP-TTLS, EAP-SRP, EAP-MD5)으로 분류된다. 본 절에서는 이 방법들에 대해 설명하고 장단점을 비교한다. 표 1은 이 방식들에 대한 특성을 비교한 것이다.

(1) EAP-TLS[RFC2716]

EAP-TLS 방식의 802.1x 프로토콜은 인증서 기반의 가장 일반적인 인증 방식이다. EAP-TLS 프로토콜은 인증서를 기반으로 하는 무선 클라이언트와 인증 서버 간의 세션키를 만드는 상호인증을 지원한다. EAP-TLS를 사용했을 때 장점은 최종 사용자의 신원을 확인하는 방법으로 인증서를 사용한다는 것이다. 그러나 이는 규모가 큰 WLAN을 설치하는 경우 복잡한 인증서 관리 체계를 지녀야 한다.

(2) EAP-TTLS[2]

EAP-TTLS 방식은 EAP-TLS방식과 CHAP (Challenge Handshake Authentication Protocol) [RFC1994] 또는 OTP(One Time Password) [RFC2284]와 같은 전통적인 암호 기반의 결합 방식이다. 이 방식은 무선 클라이언트에서 인증서가 아닌 패스워드를 사용한다. 인증서는 오직 TTLS 서버에서만 필요하기 때문에 인증서의 개수를 줄일 수 있는 동시에 관리도 간소화할 수 있다.

TLS 터널은 처음에 무선 클라이언트와 인증서버 간에 만들어진다. 무선 클라이언트는 TTLS 서버로부터 부여되는 인증서를 인증함으로서 연결되는 네트워크를 인증한다. 일단 인증된 터널이 만들어지면 최종 사용자에 대한 인증이 수행되며 기존 RADIUS/DIAMETER 서버와도 연동 가능하다.

(3) EAP-SRP[1]

Thomas Wu는 검증자-파일 기반 SRP[11][RFC 2945]프로토콜을 제안하였다. SRP는 비대칭형(검증자-파일 기반, verifier-based) 메커니즘의 키분배 프로토콜로서 분할 공격(partition attack)에 안전하고 부분군 제한 공격에도 강한 특성을 지닌다. SRP는 인증서버가 검증자-파일 v를 알고 있고 있는가에 대한 확인과정과 클라이언트가 패스워드를 알고 있는가에 대한 확인과정이 시도-응답 방법으로 처리된다. SRP에 바탕 둔 EAP-SRP는 상호인증 및 전방향 안전성(forward secrecy)을 제공하는 패스워드 기반 인증된 키교환으로서 개체인증 및 세션키 생성이 동시에 이루어진다. EAP-SRP 인증서버는 인증서 대신 가입자의 패스워드 검증자-파일만을 저장하기 때문에 인증서 관리에 따르는 성능 저하를 막을 수 있으나 단말측에 많은 연산을 필요로 한다.

〈표 1〉 각 EAP 인증 방식의 비교

		TLS	TTLS	SRP	MD5
인증서요구	클라이언트	필요	불필요	불필요	불필요
	서버	필요	필요	불필요	불필요
WEP 키관리		예	예	예	아니오
인증 속성		양방향	양방향	양방향	일방향
상대적 보안 수준		상	중	중	하

(4) EAP-MD5[RFC2284]

EAP-MD5 인증 방식은 패스워드 기반의 네트워크 인증 방식이다. EAP-MD5는 인증서버에 사용자 이름과 패스워드 데이터만 관리함으로서 관리의 편리성을 제공하는 반면 무선 LAN에서 암호화 키를 만들지 않아 다른 EAP 방식보다 보안에 취약하다.

3. SPAKE 프로토콜의 제안 및 안전성/효율성 분석

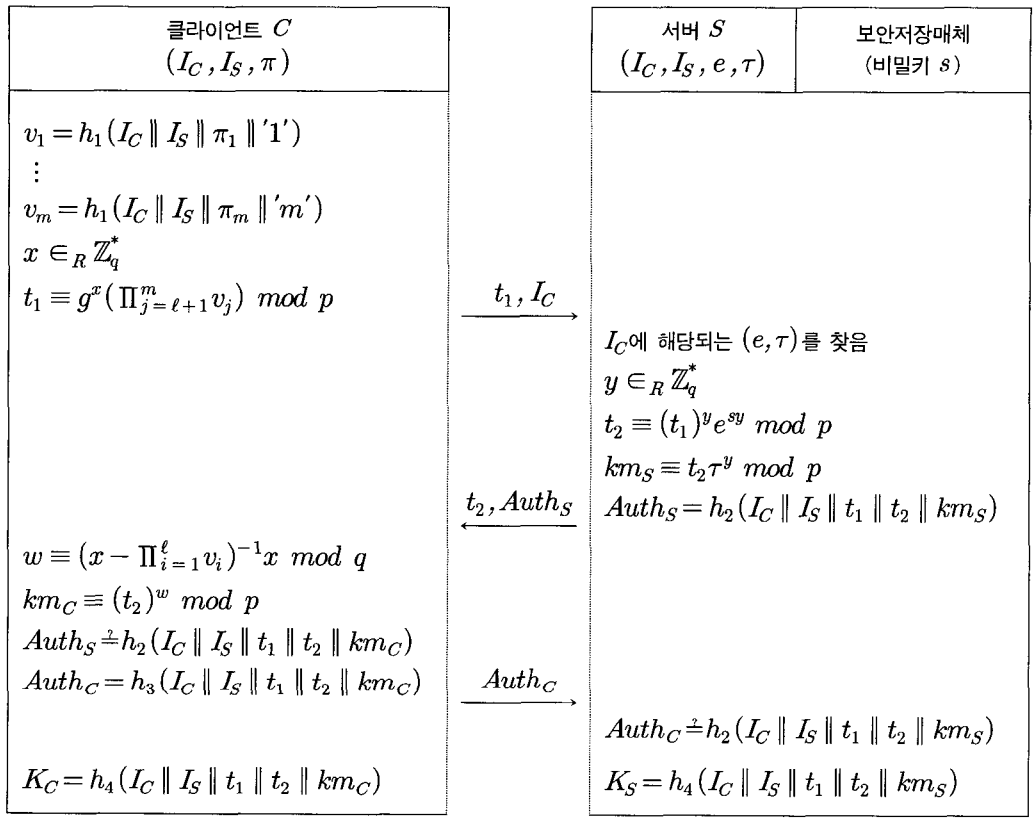
본 장에서는 두 참여자간의 패스워드 기반 인증 및 인증된 DH 키교환 프로토콜을 제안한다. 제안된 프로토콜은 수동적 도청자 및 능동적 공격자에 대한 저항성을 지니며 또한 전방향 안전성(forward secrecy)[19]이 제공된다. 제안된 프로토콜의 설명에 앞서 우선 몇 가지 시스템 공통 파라미터에 대하여 정의를 내린다.

- p와 q는 큰 소수이고 $q \mid p-1$을 만족시킨다. 위수가 q인 원시근 g는 GF(p)중의 한 원소이며 유한 순환부분군 $\mathbb{G}=\langle g\rangle$를 이룬다. 시스템 파라메터 p,q,g는 참여자들 모두에게 공개된다.
- $f:\{0,1\}^* \rightarrow \{0,1\}^{\bar{k}}/\{0\}^{\bar{k}}$는 충돌회피성 일방향 해쉬함수이며 랜덤 오라클과 같이 동작된다고 가정한다. 단 $\bar{k} < \log_2 q$이고 $q < p$이다. [6] 및 [18]에 기술된 사항을 토대로 몇 가지 해쉬함수 출력 유형을 다음과 같이 설정 한다:
  - $h_1(x) = f(00 \parallel x \parallel 00)$
  - $h_2(x) = f(01 \parallel x \parallel 01)$
  - $h_3(x) = f(01 \parallel x \parallel 10)$
  - $h_4(x) = f(10 \parallel x \parallel 10)$
- I_C는 클라이언트의, I_S는 서버의 ID(identity)이다.
- $a^{-1} \bmod m$는 법 m에 대한 a의 곱셈역원을 표기하고 $\in_R$은 우측의 집합(set)에서 좌측의 원소(element)를 랜덤하게 생성함을 의미한다. 기호 $\stackrel{?}{=}$는 좌우 정보의 동일성 여부를 판단하는 기호이다.

3.1 SPAKE 프로토콜의 제안

본 논문에서 제안된 SPAKE 프로토콜의 기본 아이디어는 패스워드를 분할한 후 분할된 각각의 패스워드 지식을 랜덤하면서도 높은 엔트로피를 갖는 정보, 즉 공개키 암호방식 및 해쉬함수와 함께 묶여 있게 함으로서 패스워드에 대한 추측을 낮추고자 하는 것에 있다. 또한 [6-9]에서와 같이 서버가 유지하는 패스워드 검증자-파일을 암호화하여 보관함으로서 만일 서버의 검증자-파일이 해커와 같은 공격자에 의해 타협되었다 하더라도 서버의 검증자-파일 암호화용 키가 타협되지 않는 한 패스워드 검증자-파일을 안전하게 보관하도록 하는 것에 있다.

제안된 SPAKE 프로토콜은 3-단계(3-pass) 통신 교환으로 이루어지며 그림 2에 도시되어 있다. 클라이언트는 자신의 패스워드 π를 $\pi_1 \parallel \cdots \parallel \pi_m$로 분할한 후, 각각의 패스워드 분할값에 대하여 $v_k = h_i(I_C \parallel I_S \parallel \pi_k \parallel k)$을 계산한다. 여기에서 k는 단지 분할된 패스워드의 고유 번호일 뿐이며 $k=1,\cdots,m$ 이다. 서버는 이에 대한 검증자-파일로서 $e \equiv (g^{-\prod_{i=1}^{\ell} v_i} \prod_{j=\ell+1}^{m} v_j^{-1})^{s^{-1}}$ 및 $\tau \equiv g^{\prod_{i=1}^{\ell} v_i} \bmod p$를 계산하여 프로토콜 수행 전에 저장하고 있어야 한다. 단 $1 < \ell < m$이며, ℓ과 m은 두 참여자가 사전에 규정했음을 가정한다. $s(\in \mathbb{Z}_q^*)$는 검증자-파일을 암호화하는 서버의 비밀키이며 [6]에서와 같이 누설되지 않도록 보안성이 높은 안전한 저장매체에 보관한다. 예로 스마트카드 또는 비밀분산 방식을 적용하여 서버들간에 공유하는 것을 들 수 있다. 그림 2에서 최상단 부분의 소괄호 영역은 각 참여자들의 사전지식이다. 만일 프로토콜이 상호간에 정확한 3가지 정보, 즉 패스워드 π, 이에 대한 검증자-파일 (e,τ), 그리고 보안저장매체에 비밀스럽게 저장한 비밀키 s을 사용하여 수행된다면, 세션값(key material) km_C 및 km_S은 Diffie-Hellman 키동의 기법에 바탕을 둔 g^{xy}가 된다.



〈그림 2〉 제안된 SPAKE

각 참여 개체는 상호인증 및 상호 키확신을 제공하기 위하여 클라이언트에서는 $Auth_C$의 계산을 그리고 서버에서는 $Auth_S$의 계산을 반드시 수행하여야 한다. 최종적으로 두 참여자 모두가 상호인증과 상호 키확신 검사를 통과하였다면 동의된 세션키 $(K_C = K_S)$를 생성한다.

제안된 SPAKE에 대한 특성은 다음과 6가지로 정리할 수 있다.

(1) 클라이언트 C는 그림 2의 SPAKE 프로토콜 수행 전 자신에게 해당되는 검증자-파일 (e,τ)을 서버 S에게 미리 등록하여야 한다. 이를 위한 간단한 방법으로 공개키 암호시스템(DH 키교환, PKI)을 활용하면 되며, 편의상 상세사항은 생략하기로 한다.

(2) $Auth_C$ 및 $Auth_S$의 계산 과정은 영지식 증명이 포함된 키확신(key confirmation)을 제공하기 위하여 삽입된 것이며, 만일 $Auth_C$와 $Auth_S$의 계산이 없다면 키확신을 통한 키인증[19]을 제공하지 못한다. 1장에서 언급된 사항과 더불어 지금까지 제안된 프로토콜들 중에는 여러 가지 증명가능한 프로토콜들이 제안되어져 있다. 대표적인 프로토콜로서 EKE2[18], AuthA[12], PAK[5], AMP[6,7] 등이 이에 해당되며 제시된 프로토콜들은 상당히 높은 증명가능한 접근을 제시한다. 특히 AuthA는 여러 이전 프로토콜로부터 유도된 것이지만 강한 증명가능한 방법을 제시하였다[6]. 따라서 본 논문에서는 AuthA에서 제안된 키확신 방법을 SPAKE 방식에 삽입하여 키인증을 제공하였다.

(3) $Auth_S$ 계산의 목적은 서버가 정확한 패스워드 검증자-파일 (e,τ)를 알고 있고 또한 정확한

세션값 $km_S \equiv g^{xy} \bmod p$를 계산했음을 클라이언트에게 증명(인증 및 키확신에 대한 증명)하기 위한 것이다. 마찬가지로 $Auth_C$는 클라이언트가 정확한 패스워드 π를 알고 있고 또한 세션값 $km_C \equiv g^{xy} \bmod p$에 대하여 정확하게 계산했음을 서버에게 증명하기 위한 것이다. $Auth_C$와 $Auth_S$의 계산 및 검증은 지금까지 알려진 공격에 대한 증명가능한 보안성을 제공한다. 알려진 공격에 대한 안전성은 3.2절에서 논증할 것이다.

(4) 프로토콜에서 만일 t_1이 e^{-s} 형태로 전달되어 올 경우, 서버는 프로토콜 세션을 강제적으로 종료하고 $t_1 = e^{-s}$ 이외의 값으로 재시도 하기를 요청해야 한다. 이것은 서버의 km_S는 τ^y가 되고 클라이언트의 km_C는 1 (즉 $km_C \neq km_S$)이 되기 때문이다. 이와 같은 경우는 AMP과 PAK에서도 발생할 수 있다.

(5) 수동적 도청자는 프로토콜에서 어떠한 정보도 얻을 수 없다. 이에 대한 사항은 3.2절 보안분석에서 논증할 것이다. 만일 능동적 공격자가 서버의 비밀키 s를 제외한 (e,τ)만을 타협시킨 경우, 이 정보들에서 패스워드 π를 유도하는 것은 DLP 해결과 동일하게 된다. 그러나 만일 강한(strong) 능동적 공격자가 서버의 비밀키 s까지 타협시킨다면 오프-라인 사전공격을 통해 패스워드 π가 노출될 수 있다.

(6) 이와 별도로 그림 2의 SPAKE 프로토콜에서와 같이 패스워드를 분할하는 경우에, 만일 분할된 패스워드 정보의 일부가 노출된다면 전체 패스워드에 대한 추측 공격이 가능해진다. 예로 능동적 공격자가 패스워드의 일부 정보 $\Pi_{j=\ell+1}^{m} v_j^{-1}$을 알고 있다면 공격자는 서버와 메시지를 주고받은 후 또 다른 일부 정보 $\Pi_{i=1}^{\ell} v_i$에 대한 추측 공격을 수행한다. 이와 같은 문제점은 [15]에 상세히 지적되어 있다. 따라서 그림 2의 프로토콜에 대한 선제조건은 분할된 패스워드값 $(\pi_1,\cdots,\pi_m)$ 및 $(v_1,\cdots,v_m)$에 대한 어떠한 정보도 노출되지 말아야 할 것이며 더불어 매 세션 교환 정보들에 대한 구별불가능성(indistinguishability)을 제공하기 위하여 x와 y는 각 이벤트(event) 확률이 동일한 집합에서 랜덤하게 선택되어야 한다.

최종적으로 두 참여자가 상호인증 및 상호 키확신 검사를 통과하였다면 서로 동의된 세션키 $(K_C = K_S)$를 생성한다.

3.2 SPAKE 프로토콜의 보안분석 및 효율성

본 절에서는 SPAKE의 특징, 기존 알려진 공격에 대한 SPAKE의 안전성 분석, 그리고 효율성 분석을 기술한다.

(1) 패스워드의 분할

패스워드의 분할은 패스워드 검증자-파일의 추측가능성 및 랜덤성(randomness)을 증가시키기 위한 것이다. 왜냐하면 패스워드 분할하여 인증 프로토콜을 수행한다면, 공격자 입장에서 그에 따른 검증자-파일 추측 계산량 역시 증가하게 된다. 이것은 공격자가 더 많은 정보를 분석해야 함을 의미한다. 그러나 패스워드에 대한 분할도가 높아지게 된다면, 그에 따른 클라이언트의 계산량 역시 증가하게 된다.

1장에서 설명된 바와 같이 분할된 패스워드 방식으로 [15]와 [16]이 제안되었다. SPAKE 방식과 [15,16]의 차이점은 기본적으로 서버가 단독으로 존재하는가 다수로 존재하는가에 있다. [15]에서 제시된 방식은 클라이언트의 분할된 패스워드 값들 $\pi_1 \| \cdots \| \pi_m$과 분할된 패스워드에 대한 각 서버들 $S_i (i = 1,\cdots,m)$의 검증자-파일 v_i간에 일대일 대응관계를 맺고 있음에 따라 프로토콜 수행 시 병행으로 처리되는 반면, 본 논문의 SPAKE 방식은 패스워드의 분할 수에 관계없이 항상 일정하게 일대일 클라이언트와 서버관계로 유지된다. 또한 [15,16]은 서버가 단순히 검증자-파일만을 저장함으로서 서버 파일 타협에 의한 서버가장 공격 및 오프라인 패스워드 추측 공격에 노출 될 수 있으나, 본 논문의 SPAKE 방식은 검증자-파일을 서버 비밀키 s로 암호화함으로서 서버가장 공격 및 추가적 사전 공격에에 대해 강한 저항성을 지닌다.

(2) 수동적 도청자(passive eavesdroper)에 대한 안전성

제안된 프로토콜이 수행되는 동안 세션값에 대한 어떠한 지식도 수동적 도청자에게 노출되지 않는다. 즉 수동적 도청(passive eavesdropping)에 대한 보안이 DLP에 바탕을 두고 있음을 증명한다. 여기에서 수동적 도청자는 참여자간에 교환되는 메시지를 도청할 수 있고 그들 사이에서 공유된 세션키를 구하려고 시도하는 공격자라 정의하자. 단 수동적 도청자는 임의의 메시지를 바꾸거나 삭제하거나 삽입하는 것은 불가능하다라고 가정한다. 논증에 앞서 $km_C = km_S = g^{xy}$는 편의상 km이라 표기한다.

제안된 방식의 세션값 교환 과정에서, 도청자가 프로토콜의 시스템 파라메터 (p,q,g) 그리고 서버와 클라이언트 교환정보 $t_1 = g^x(\Pi_{j=\ell+1}^{m} v_j)$ 및 $t_2 = (t_1)^y e^{sy}$를 알고 있다 하더라도, 도청자가 세션값 g^{xy}를 알아내는 것은 적어도 DLP를 해결하는 것만큼 어렵다. 이와 같은 결론을 증명하기 위하여 우선 다음과 같은 알고리즘을 정의한다[17,20,21].

- $Adv_A()$: 다항식 시간 알고리즘 A으로 공통 파라메터 그리고 t_1 및 t_2과 같이 프로토콜 수행 중에 노출되는 교환정보를 입력 값으로 하여 세션값 $km = g^{xy}$을 계산하는 알고리즘이다.
- $Adv_{DLP}()$: DLP를 계산하는 알고리즘으로 공통 파라메터 그리고 $a \in \mathbb{Z}_p^*$를 입력 값으로 하여 $\log_g a \in \mathbb{Z}_q^*$를 구하는 것이다. 즉 $Adv_{DLP}(p,q,g,a) = \log_g a \bmod q$.
- $Adv_{DHP}()$: DHP(Diffie-Hellman Problem)를 계산하는 알고리즘으로 공통 파라메터 그리고 $a,b \in \mathbb{Z}_p^*$를 입력하여 $a^{\log_a b \pmod q} \in \mathbb{Z}_p^*$를 구하는 것이다. 즉 $Adv_{DHP}(p,q,g,a,b) = a^{\log_a b} \bmod p$.
- $Adv_{DHDP}()$: DHDP(Diffie-Hellman Decision Problem)[21]는 $g^a, g^b, g^{c'} \in \mathbb{Z}_p^*$가 입력으로 주어지고 $c' \equiv a'b' \bmod q$인지를 결정하는 문제이다. 만일 $c' \neq a'b'$이라면 $c' \equiv a'b' \bmod q$으로 간주할 수 있고, 균일한 확률 분포 갖는 $\mathbb{G}_p = \langle g \rangle$상에서 g^z (단 $z \in \mathbb{Z}_q$)의 분포는 통계적으로 구별불가능하게(indistinguishable) 된다. 더불어 입력값들 $(g^a, g^b, g^{c'})$의 분포 역시 $\mathbb{G}_p^3$상의 균일한 확률 분포에 통계적으로 구별불가능하게 된다.

DLP, DHP, 그리고 DHDP는 모두 계산적으로 등가를 이룬다. 즉 DLP의 해결이 무시할 만한 확률을 갖는다면 DHP 및 DHDP 역시 무시할 만한 확률을 지닌다[20]. 주어진 알고리즘을 다음과 같은 절차로 수행한다.

- 3.1절에서 해쉬함수는 $f: \{0,1\}^* \rightarrow \{0,1\}^{\bar{k}} / \{0\}^{\bar{k}}$ (단 $\bar{k} < \log_2 q$ 이고 $q < p$)로 정의했기 때문에, $\Pi_{i=1}^{\ell} v_i$은 $\Pi_{i=1}^{\ell} v_i : \{0,1\}^{\bar{k}} \in \mathbb{Z}_q^*$으로 $\Pi_{j=\ell+1}^{m} v_j$는 $\Pi_{j=\ell+1}^{m} v_j : \{0,1\}^{\bar{k}} \in \mathbb{Z}_p^*$으로 가정할 수 있다. 이에 따라 t_1은 $t_1 \equiv g^x(\Pi_{j=\ell+1}^{m} v_j) \equiv g^{x+z_1} \bmod p$로 또한 t_2는 $t_2 \equiv g^{y(x-\Pi_{i=1}^{\ell} v_i)} \equiv g^{yz_2} \bmod p$로 놓을 수 있다. 여기에서 $1 < \ell < m$이고 $z_1, z_2 \in \mathbb{Z}_q^*$이다.
- 정의에 의해 $Adv_A(p,q,g,g^{x+z_1}, g^{yz_2}) = g^{xy}$가 다항식 시간 안에 계산될 수 있다.
- $a' = x + z_1$, $b' = yz_2$, $c' = a'b'z_2^{-1} - yz_1 = xy$라 정의할 경우, 위 $Adv_A()$알고리즘이 성립한다면 $Adv_{DHDP}(p,q,g,g^a, g^b, g^{c'}) =$ "가능(true)"이 된다. 즉 DHDP알고리즘이 성립되면, $\{x, y, z_1, z_2 \leftarrow \mathbb{Z}_q^* : (g^a, g^b, g^{c'})\}$을 구별(즉 계산) 있음을 의미한다. 따라서 이 같은 경우에는 DLP 알고리즘 $Adv_{DLP}(p,q,g,g^{x+z_1}) = x + z_1$을 출력하고 $Adv_{DLP}(p,q,g,g^{yz_2}) = yz_2$를 출력한다. 결과적으로 도청자가 위에서 정의한 알고리즘을 사용하고 주어진 절차에 따라 정확히 수행한다면 세션값 $km = g^{xy}$을 구할 수 있다.

결론적으로 만일 알고리즘 $Adv_A()$가 가능하다면 $Adv_{DHDP}()$가 존재할 수 있고, $Adv_{DHDP}()$가 가능하다면 $Adv_{DLP}()$가 존재할 수 있다. 따라서 제안된 프로토콜에서 세션값 km를 구하는 것은 $Adv_{DLP}()$를 계산할 확률과 비슷하며 DLP를 해결하는 것

만큼 가능하게 된다.

(3) 능동적 중간자 공격(positive man-in-the-middle attack)[19] 및 재생공격(RA, Replay Attack) [19]에 강인하다.

능동적 중간자 공격은 공격자가 양쪽 개체를 합법적으로 가장하거나 혹은 클라이언트와 서버 사이에서 존재하여 두 참여자의 메시지를 가로챈 다음, 공격자와 클라이언트, 공격자와 서버 사이에서 각각 다른 세션값을 만들어내는 공격이다. 이 공격은 가장공격(impersonation attack)과 유사하다. 제안된 SPAKE 프로토콜에서 공격자는 프로토콜 내의 모든 대화내용을 이용하더라도 패스워드를 모른다면 $Auth_S \stackrel{?}{=} h_2()$ 및 $Auth_C \stackrel{?}{=} h_3()$ 검사를 통과시키지 못하기 때문에 이 공격은 불가능하다.

재생공격은 공격자가 클라이언트의 메시지(즉 t_1)를 서버에게 재전송 하여 이미 정상적인 클라이언트에 의해 생성된 이전키(old session key)를 다시 생성하기 위한 공격이다. 그러나 모든 통신 메시지들은 매 세션마다 균일한 확률 분포에서 랜덤하게 생성되어짐을 가정하기 때문에 이 공격에 대한 공격자의 성공 확률은 무시 할만하다. 즉 클라이언트 및 서버가 각 키동의 세션 프로토콜마다 $x \in_R \mathbb{Z}_q^*$ 및 $y \in_R \mathbb{Z}_q^*$를 생성하고 그 선택 확률이 모두 균일한 확률 분포 $1/\phi(q)$를 갖는다면, 공격자의 성공확률은 대략 $\Pr[Adv_{RA}()] \leq 1/\phi(q)$가 된다. 여기에서 $Adv_{RA}()x$는 RA 공격을 수행하는 알고리즘이다.

(4) 전방향 안전성의 제공

롱텀(long-term) 비밀값(패스워드)의 타협이 이전 세션값 km의 타협을 의미하지 않는다면, 프로토콜은 전방향 안전성를 만족한다라고 정의한다 [17,19]. 패스워드가 주어졌다고 가정했을지라도, 공격자는 $t_1 \equiv \Pi_{i=1}^{\ell} v_i \mod p$와 $t_2 \equiv \Pi_{j=\ell+1}^{m} v_j \mod q$만을 구할 수 있을 뿐이다. 즉 t_1와 t_2에서 세션값 km을 구하는 것은 $Adv_A(p,q,g,t_1,t_2) = g^{xy}$가 존재함을 의미하며, 이것은 $Adv_{DLP}(p,q,g,t_1)$와 $Adv_{DLP}(p,q,g,t_2)$가 존재함과 동일한 의미이다. 따라서 다항식시간 알고리즘 A을 해결하는 것만큼 전방향 안전성이 훼손되게 된다.

(5) 오프라인(off-line) 사전추측 공격[19]에 대한 저항성을 지님

저항성이란 프로토콜 수행 중에 노출되는 정보들을 이용한 오프라인 사전추측 공격이 불가능해야 함을 의미한다. 이 공격은 클라이언트와 서버 간에 서로 주고받는 정보 t_1과 t_2에 대한 DLP를 해결해야만 패스워드에 대한 사전공격이 가능하게 됨에 따라 $\Pr[Adv_{DLP}()]$와 비슷한 확률을 갖게 된다[6,17].

이와 별도로 제안된 프로토콜은 서버 파일 타협에 의한 오프라인 사전추측 공격에도 저항성을 지닌다. 즉 제안된 프로토콜은 AMP[6,7,9] 및 EPA[8]에서와 같이 검증자-파일을 서버의 비밀키로 암호화하여 보관하기 때문에 공격자는 타협된 파일로부터 어떠한 정보도 얻을 수 없다.

(6) Denning-Sacco (DS) 공격[22]은 불가능.

이 공격은 이전 세션키를 안다고 할 때 패스워드를 알아내는 공격이다. 그러나 본 논문에 제안된 방식은 세션키가 공개되어도 패스워드는 노출되지 않을 뿐만 아니라 참여자로 가장할 수 없다.

즉 공격자가 t_1, t_2, km을 얻을 수 있어도, 이들 정보에서 패스워드 π 및 검증자-파일 (e,τ)를 계산하는 것은 불가능하다. 더욱이 $e \equiv (g^{-\Pi_{i=1}^{\ell} v_i} \Pi_{j=\ell+1}^{m} v_j^{-1})^{s^{-1}} \mod p$는 서버의 비밀키 s로 암호화 되어 있어 이 문제를 더욱 불가능하게 만든다. 공격자가 패스워드를 얻기 위해서는 $\{t_1, t_2, km\}$로부터 $\{(x, y, v_1 \leftarrow \mathbb{Z}_q^*), (v_2 \leftarrow \mathbb{Z}_p^*)\}$을 구별할 수 있어야 하고 이 문제는 DLP를 해결 할 수 있어야 한다. 따라서 DS 공격을 수행하는 알고리즘을 $Adv_{DS}()$라 할 경우, 제안된 프로토콜에서의 DS 공격 성공률은 $\Pr[Adv_{DS}(g,p,q,t_1,t_2,km)] \approx \Pr[Adv_{DLP}()]$와 같이 이루어지게 된다. [6,17]에서 언급한 것과 같이 이 값은 무시할만한 값이다.

(7) 효율성 분석

효율성 비교를 위한 다른 프로토콜들로 IEEE Std P1363.2에 제출된 B-SPEKE, SRP, AMP 및 SPAKE와 비교한다. 제시된 표 2는 AMP[6]

〈표 2〉 메시지 교환 횟수, 지수승 횟수, 그리고 교환 메시지의 크기 및 기타 사항에 대한 비교

	메시지 교환 횟수	지수승 횟수			교환 메시지 크기	추가적 사전 추측공격에 대한 저항성[8]	패스워드 분할 여부	생성원 개수
		클라이언트	서버	합계				
B-SPEKE	4	3	4	7	$3\|p\|+2\bar{k}$	취약	비분할	1개
SRP	4	3	3	6	$2\|p\|+2\bar{k}+\|q\|$	취약	비분할	1개
AMP	4	2	2.4	4.4	$2\|p\|+2\bar{k}$	강함	비분할	1개
EPA	3	2.2	2	4.2	$2\|p\|+2\bar{k}$	강함	비분할	2개
제안방식 SPAKE	3	2	2.4	4.4	$2\|p\|+2\bar{k}$	강함	분할	1개

및 EPA[8]에 제공된 자료를 토대로 메시지 교환 횟수, 지수승 횟수, 교환 메지의 크기에 대하여 비교한 것이다. 지수승 연산은 효율성을 위하여 다중 병렬 멱승법(simultaneous multiple exponentiation)[23]을 취한다. 이 방법은 $g_1^{e_1}g_2^{e_2}$을 계산함에 있어 $g_1^{e_1}$ 및 $g_2^{e_2}$을 각각 계산할 필요가 없으며, $g_1^{e_1}g_2^{e_2}$ 및 $g_1^{e_1}g_2^{e_2}g_3^{e_3}$는 $g_1^{e_1}$보다 곱셈이 평균적으로 20% 및 40% 이상 연산을 필요로 한다[6,8]. 제시된 표 1의 연산은 이를 근거로 집계되었다. 표 2에서 $|p|$와 $|q|$는 각각 법 p 및 법 q의 의한 합동값의 비트 길이이며, $\bar{k}$는 해쉬함수의 출력 비트 길이이다.

3-메시지교환(3-pass) 프로토콜 EPA는 두 개의 생성원을 이용함으로써 상대적으로 적은 지수승을 갖기 때문에 메시지 교환 횟수, 지수승 횟수, 그리고 교환 메시지 크기 측면에서 기존 제안된 방식보다 가장 효율적인 방식으로 볼 수 있다. 그러나 두 개의 생성원을 사용해야 한다는 점은 응용에 있어서 제한을 갖게 된다.

[8]에 제시된 추가적 사전 추측공격은 만일 공격자(adversary)에 의해 서버의 검증자-파일이 타협된다면 검증자-파일 기반 프로토콜조차 추측공격에 노출됨을 의미한다. 제안방식 SPAKE는 검증자-파일을 안전한 저장매체에 저장함으로써 이와 같은 공격을 피할 수 있다.

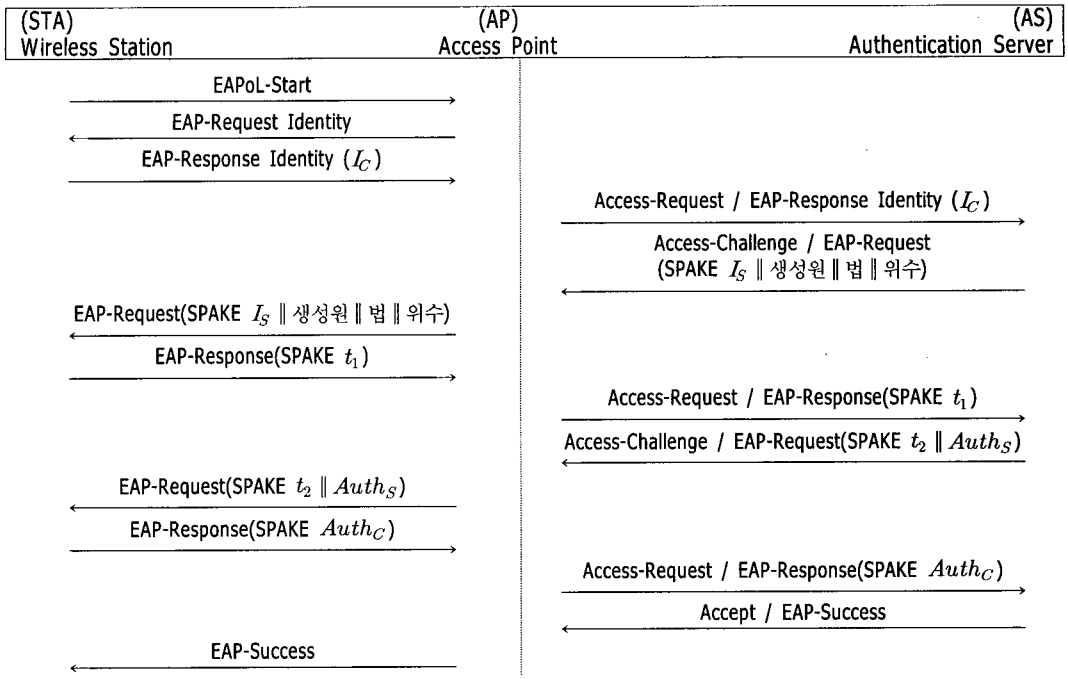
제안방식 SPAKE에서 클라이언트는 패스워드 π를 $\pi_1 \| \cdots \| \pi_m$로 분할한 후 각각의 패스워드 분할값에 대하여 $v_k = h_1(I_C \| I_S \| \pi_k \| k)$을 계산하여야 한다. 단 $k=1,\cdots,m$ 이다. 이와 같은 연산은 클라이언트의 계산 부담을 증가시킬 수 있다. 따라서 실질적인 구현시에는 $m=2$인 경우가 효율적이며, 이 경우의 제안방식 SPAKE는 AMP와 전체적으로 등가인 연산 효율성을 갖는 반면 3-메시지교환을 갖는다.

4. SPAKE에 바탕둔 새로운 무선 근거리 통신망 EAP-SPAKE 방식

본 장에서는 2장의 SPAKE 프로토콜을 EAP에 적용한 새로운 인증 방식을 제안하며 상세 사항은 그림 3에 도시되어 있다. 그림 3은 무선랜 통신 접속을 위한 802.1x 규격 메시지 전달 과정과 SPAKE을 이용한 상호인증 과정을 담고 있다. 제안된 EAP-SPAKE 인증 형태는 3.1절의 SPAKE를 이용하여 EAP 상호인증을 수행한다. SPAKE는 [5-11]에 제시된 보안 요구사항을 만족시키면서도 메시지 교환, 지수승, 난수 생성 등 연산 측면에서 SRP[11][RFC2945]보다 효율적이기 때문에, EAP-SPAKE는 SRP를 이용한 EAP-SRP[1]보다 효과적인 실현이 가능하다.

4.1 EAP-SPAKE 패킷 형식 및 특성

EAP-SPAKE 패킷 형식은 아래와 같이 EAP-SRP[1] 패킷 형식을 따른다. Code 필드(field)는 Request 또는 Response을 지시하며, Identifier 필드는 각 Request/Response 값들을 구별하는 식



〈그림 3〉 EAP-SPAKE 기반의 인증절차

별 번호이다. 여기에서 한 쌍의 Request/Response 만이 동일한 식별번호를 갖는다. Length 필드는 전체 필드들의 EAP-SPAKE 패킷 길이를 기록한다. Type 필드는 EAP-SPAKE 이용을 의미하는 고유번호가 기입된다. Subtype 필드는 각 Request/Response 메시지 내용에 따라 별도로 규정된 필드형태를 지시하며 이에 따른 데이터는 Subtype-Data 필드에 담기게 된다. 전체 패킷 형식은 아래 그림 4와 같다.

[RFC2284]에서는 EAP Identity Request/Response 사용이 권고되고 있으므로, AS는 그에 따라 STA의 Identity을 획득한 후에만 Challenge 패킷을 보내게 된다. 여기에서 AS는 RADIUS 또는 DIAMETER 인증서버로 여길 수 있다.

Code	Identifier	Length
Type	Subtype	Subtype-Data ···

〈그림 4〉 EAP-SPAKE 패킷 형식

STA에게서 EAP-Response Identity (I_C)을 수신한 AS는 아이디 I_C에 해당되는 검증자 (e,τ), 소수인 법(prime modulus) p, 생성원 g, 그리고 위수 q을 찾는다. 검증자-파일 (e,τ)은 SPAKE 프로토콜 수행시 필요한 정보들이며, AS는 그림 3의 EAP-Request(SPAKE I_S ‖ 생성원 ‖ 법 ‖ 위수)와 같이 아이디 및 패스워드만을 기억하는 STA 이용자에게 (g,p,q)을 제공하여야 한다.

EAP-Response(SPAKE t_1)는 EAP-Request (SPAKE I_S ‖ 생성원 ‖ 법 ‖ 위수)에 대한 Response로서, 랜덤하게 선택된 $x \in_R \mathbb{Z}_q^*$에 대해 $t_1 \equiv g^x(\Pi_{j=\ell+1}^{m} v_j) \bmod p$을 계산한 후 이를 탑재한 것이다. 3.1절의 SPAKE에서는 t_1 및 I_C가 동시에 전달되도록 되어있으나, 그림 3의 EAP-Response Identity (I_C)에서 I_C가 이미 전달되었기 때문에 I_C의 전달은 생략된다. EAP-Response(SPAKE t_1)를 수신한 AS는 $y \in_R \mathbb{Z}_q^*$, $t_2 \equiv (t_1)^y e^{sy} \bmod p$, $km_S \equiv t_2 \tau^y \bmod p$, 그리고 $Auth_S$을 차례로 계산한 후, EAP-Request (SPAKE t_2 ‖ $Auth_S$)를 전송한다. STA는 이에 대

〈표 3〉 패스워드 기반 인증에 바탕 둔 EAP 인증 방식별 특성

		EAP-MD5	EAP-SRP	제안방식 EAP-SPAKE
신원보호		미제공	미제공	미제공
기반둔 패스워드 인증 모델		대칭형 모델	비대칭형 모델	비대칭형 모델
STA의 사전지식		패스워드 및 STA ID	패스워드 및 STA ID	패스워드 및 STA ID
AS의 사전지식		패스워드, STA 및 AS ID	검증자 $(salt, v)$, STA 및 AS ID	검증자 (e, τ), 비밀키 s, STA 및 AS ID
암호적 안전성 기반		램덤 오라클 모델	램덤 오라클 모델 및 DLP	램덤 오라클 모델 및 DLP
양방향 인증의 제공 여부		미제공 (서버 인증 미제공)	제공	제공
세션키 생성 및 키확신		미생성 및 미제공	생성 및 제공	생성 및 제공
EAP Request/Response 메시지 통신량 (단 EAPol-Start 제외, EAP-Success 포함)		3회	5회	4회
멱승 계산량	서버	없음	3번	2.4번
	클라이언트	없음	3번	2번
난수생성 계산량	서버	1번	1번	1번
	클라이언트	없음	1번	1번
사전공격에 대한 저항성		사전공격에 취약	추가적 사전공격에 취약	추가적 사전공격에도 강함
전방향 안전성 제공		제공	제공	제공

한 응답 EAP-Response(SPAKE $Auth_C$)를 전송하기 위해 먼저 $w \equiv (x - \Pi_{i=1}^{\ell} v_i)^{-1} x \mod q$ 및 $km_C \equiv (t_2)^w \mod p$의 계산하고 $Auth_S$ 검증한다. STA로부터 EAP-Response(SPAKE $Auth_C$)을 수신한 AS는 $Auth_C$을 검사한 후 만일 정확하다면 EAP-Success를 STA에게 전송한다. 이를 통해 STA 및 AS는 상호인증을 완료하게 되며 최종적으로 상호간에 동의된 키 $K_C = K_S$을 얻게 된다.

4.2 보안 특성 및 연산량 검토

EAP 인증 방식에서 패스워드를 이용한 방법으로 EAP-MD5[RFC2284] 및 EAP-SRP[1]를 들 수 있다. 패스워드 기반 사용자 인증이란 관점에서 EAP-MD5는 평가등가(대칭형 모델)로서 AS와 STA는 쌍방간에 동일한 패스워드 π을 기억한다. 이에 반하여 EAP-SRP는 검증자-파일 기반(비대칭형 모델)으로서 STA는 패스워드 π만을 기억하는 반면, AS는 π를 검증할 수 있는 검증자-파일 $(salt, v = g^{f(salt, \pi)})$만을 지닌다. 표 3는 제안된 방식과 이들 방식에 대한 특성을 비교한 것이다.

(1) 신원보호(identity protection)[24] : 가입자가 AP로부터 ID 요청을 받으면 자신의 ID 대신 $f(ID, g^{\beta})$을 전송하여 수동적 공격자들이 가입자의 신원을 알수 없게 하는 것이다. 여기에서 g^{β}는 AS의 static 비밀키 β에게 대한 공개키이다. EAP-MD5, EAP-SRP, 그리고 제안된 EAP-SPAKE는 패스워드 기반 인증방식이기 때문에 모두 이 특성을 제공하지 못한다.

(2) 세션키 생성 및 키확신(key confirmation) : EAP-SRP과 EAP-SPAKE에서의 개체들은 랜덤한 난수에 기인한 세션키를 생성하기 때문에 키의 랜덤성과 신선도(freshness)을 제공하며 이에 따라 재생공격(replay attack)에 강인하다. 또한 EAP-SPAKE의 $Auth_C$ 및 $Auth_S$와 같이 생성된 세션키에 대한 키확신을 쌍방간에 제시하며 둘 다 인증된 DH 키교환 방식을 사용하므로 중간자공격(man-in-the-middle attack)에 강인하다.

(3) 계산량을 비교하기 위하여 대부분의 실행 시간을 소비하는 지수승 횟수를 고려한다. $g_1^{e_1}g_2^{e_2}$의 계산은 $g_1^{e_1}$ 및 $g_2^{e_2}$을 분리하여 계산할 필요가 없다. 앞서 설명한 바와 같이 다중 병렬 멱승법[23]을 사용하는 경우 평균적으로 $g_1^{e_1}g_2^{e_2}$은 $g_1^{e_1}$보다 곱셈이 약 20%이 증가한다[8]. 표 2의 지수승 계산량은 이 집계를 이용한 것이다. 제안된 방식은 EAP-SRP과 비교하여 볼 때 상대적인 최소값을 갖는다.

(4) 오프라인 사전공격 : 3.2절에 설명된 바와 같이 SPAKE는 서버의 검증자 파일을 암호화하여 보관하기 때문에 이 공격에 가장 강인하다. 반면 EAP-MD5는 단순한 오프라인 사전공격에도 취약하며, EAP-SRP은 서버 파일 타협에 의한 추가적 사전공격에 취약하다.

(5) 전방향 안전성(forward secrecy) : 롱텀(long-term) 비밀값(패스워드, 아이디, AS의 검증자 파일)의 타협이 이전 세션값의 타협을 의미하지 않는다면, 프로토콜은 전방향 안전성를 만족한다라고 정의된다[19]. EAP-SRP과 EAP-SPAKE에서의 개체들은 일회성 랜덤한 난수에 기인한 세션키를 생성하기 때문에, $q=|\mathbb{Z}_p^*|$가 상당히 큰 경우 비밀값들로부터 세션값을 유도하는 것은 확률적으로 불가능하다.

(6) 기존 EAP 인증방식과 특성 비교 : EAP [RFC 2284] 인증방식으로 EAP-TLS[RFC2716], EAP-TTLS[2], EAP-MD5[RFC2284], PEAP, EAP-SRP[1] 등이 있다[3,4,24]. EAP-TLS는 사용자와 인증서버가 인증서를 이용하여 상호인증하고 랜덤한 키를 생성 분배하는 방식이다. 이 방식은 신원보호가 제공되지 않으며 공개키기반구조(PKI) 관리 시스템을 필요로 한다. EAP-TTLS는 EAP-TLS의 확장 형태로 가입자 인증은 패스워드로, 서버인증은 인증서를 이용하여 인증하는 방식이다. PEAP는 EAP-TTLS(Tunneled TLS)와 유사한 형태로 가입자 인증정보를 TLS 프로토콜을 통해 안전하게 터널링한 후 가입자 인증을 처리하는 방식이다. EAP-TTLS 및 PEAP는 TLS 설정시 가입자에 대한 인증 미비로 중간자공격에 취약하다.

5. 결론 및 향후 연구 방향

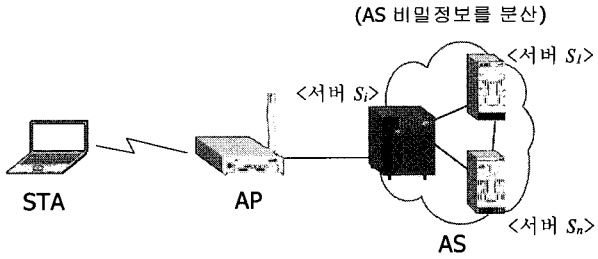
본 논문에서는 SPAKE 및 EAP-SPAKE을 제안하였다.

3장에서는 기존 방식과 비교하여 연산량 및 메시지 교환 측면에서 상대적으로 효율적이고, 기존 시스템과 융화가 좋은 패스워드-기반 인증된 키교환 방식 SPAKE을 제안하였다. 제안된 방식은 패스워드 검증자-파일의 추측가능성 및 랜덤성(randomness)을 증가시키기 위해 패스워드를 분할하였으며, 패스워드의 분할 수에 관계없이 항상 일정하게 일대일 클라이언트와 서버관계로 유지된다는 점에서 기존 유사한 방식 [15,16]과 차이점을 지니도록 하였다. 또한 AMP[6] 및 EPA[8]와 같이 서버의 검증자-파일을 서버 비밀키 s로 암호화함으로서 서버가장 공격 및 추가적 사전 공격에 대해 강한 저항성을 지니도록 하였다. AMP와 EAP는 지수승 횟수 및 교환 메시지 크기 측면에서 기존 제안된 방식 보다 우수하기는 하나, AMP는 4-메시지교환(4-pass)란 점이 EPA는 두 개의 생성원을 사용해야 한다는 점이 응용에 있어서 제한을 갖게 된다. 이와 같은 점을 통해 SPAKE가 상대적으로 약간 효율적임을 알 수 있다.

본 논문의 4장에서는 SPAKE에 바탕 둔 새로운 무선 근거리 통신망 EAP-SPAKE 방식을 제안하였다. 제안된 방식은 기존 방식 EAP-MD5 및 EAP-SRP 보다 양방향 인증 제공 여부, 세션키 생성 및 키확신, EAP Request/Response 메시지 통신량, 멱승 계산량, 난수생성 계산량, 사전공격에 대한 저항성 등과 같은 측면에서 상대적으로 약간 효율적이며 기존 알려진 공격에 대한 강한 저항성을 지닌다.

본 연구에 대한 향후 연구 방향은 다음과 내용을 다루고자 한다.

1장에서 앞서 언급했던 바와 같이 패스워드-기반 인증시스템에서 서버의 파일 타협의 가장 좋은 해결책으로 [13,14]에서와 같이 검증자-파일을 임계치 기법을 통해 분산하는 것이다[6]. 즉



〈그림 5〉 분산된 서버환경에서의 EAP-SPAKE 구조

EAP-SPAKE에 비밀분산 기법을 적용함으로써 AS(인증서버이며 <서버 S_i>로 표기, 단 $1 \leq i \leq n$ 중의 특정서버라 가정)의 비밀정보(검증자-파일 (e, τ) 및 서버의 암호화 키 s)를 다수 서버들 {<서버 S_1>,…,<서버 S_n>}에게 분배시킨 분산서버 환경에서의 EAP-SPAKE을 제시하는 것이 가능하다. 물론 패스워드-기반 인증시스템 자체의 보안성이 완벽하지 못하다면 분산서버 환경으로의 확장은 아무런 의미를 갖지 못한다.

[25]에서는 강한 비밀분산(robust secret sharing) [26] 방식과 영지식 비대화형 증명(ZKNIP: Zero-Knowledge Non-Interactive Proof) 방식을 이용하여 분산서버 환경에서의 패스워드-기반 인증된 키교환을 제시하였다. ZKNIP는 ZKIP(Zero-Knowledge Interactive Proof)보다 효율적이기는 하나 역시 연산량을 많이 줄이지는 못한다. [27]은 이와 같은 문제점을 해결하기 위하여 ZKP 제거를 제안하였다. 이와 별도로 [28]는 Weil pairing 및 Tate pairing을 이용한 Bilinear pairing 기반 분산서버 환경에서의 패스워드-기반 인증을 제안하였다.

현재 알려지기 시작한 공격(해킹 및 바이러스의 지능적 통합) 유형 및 네트워크/컴퓨터의 발전 속도(광통신 및 All-in-One 칩의 일반화 따른 AP/AS 성능의 향상)를 감안하여 볼 때 단독 인증서버를 다수의 서버환경으로 확장하는 것은 당연한 진화라 여길 수 있다. 이에 따라 향후 연구 방향은 이와 전제 사항을 토대로 ZKP가 없는 분산서버 환경에서의 EAP-SPAKE 및 낮은 연산량을 갖는 Bilinear pairing 기반의 EAP-SPAKE에 있다.

참 고 문 헌

[1] J. Carlson, B. Aboba, and H. Haverinen, "EAP SRP-SHA1 Authentication Protocol", *IETF Network Working Group* <draft-ietf-pppext-eap-srp-03.txt>, (July. 2001)

[2] Paul Funk and Simon Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", *IETF PPPEXT Working Group*, Available at http://securitytechnet.com /resource/ietf/wg-draft/ draft-ietf-pppext-eap-ttls-02.txt (2002)

[3] 정병호, 강유성, 김신효, 정교일, "공중 무선랜 망에서 인증 및 키관리 기술 동향", 전자통신동향분석 제17권 제4호, (2002.8)

[4] 이광수, "무선네트워크 보안의 허와실 그리고 미래", *Wireless Network Security Forum* 2003, 사이트 http://wsf.cnetkorea.co.kr/report8.html (2003)

[5] V. Boyko, P. MacKenzie, and S. Patel, "Provably Secure Password Authenticated Key Exchange Using Diffie-Hellman," *Advances in Cryptology-EUROCRYPT' 2000*, LNCS 1807, pp. 156-171 (2000)

[6] T. Kwon, "Ultimate Solution to Authentication via Memorable Password," *IEEE P1363.2 Working Group*, Available at http://grouper.ieee.org/groups/1363/passwdPK/submissions.html#amp (2000)

[7] T. Kwon, "Authentication and key agreement via memorable passwords," *In Proceedings of the ISOC Network and Distributed System Security (NDSS) Symposium* (2001)

[8] Y. Hwang, D. Yum, and P. Lee, "EPA: An efficient password-based protocol for authenticated key exchange," *Information Security and Privacy, 8th Australasian Conference, ACISP'2003*, LNCS 2727, pp. 324-335 (2003)

[9] T. Kwon, "Addendum to Summary of AMP," *IEEE P1363.2 Working Group*, Available at http://grouper.ieee.org/gro ups/1363/passwdPK/contributions/am psummary2.pdf (2003)

[10] S. Bellovin and M. Merritt, "Encryted key exchange: password-based protocols secure against dictionary attacks," *Proceedings of IEEE Comp. Society Symp. on Research in Security and Privacy*, pp. 72-84 (1992)

[11] T. Wu, "Secure remote password protocol," *Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium*, pp. 97-111 (1998)

[12] M. Bellare and P. Rogaway, "The AuthA protocol for password-based authenticated key exchange," *IEEE P1363.2 Working Group*, Available at http://grouper.ieee.org/groups/1363/ passwdPK/conributions.html#autha (2000)

[13] P. MacKenzie, T. Shrimpton, and M. Jakobsson, "Threshold Password-Authenticated Key Exchange," *Advances in Cryptology-CRYPTO'2002*, LNCS 2442, pp. 369-384 (2002)

[14] Xunhua Wang, "Intrusion Tolerant Password-Enabled PKI," *Proceedings of 2nd annual PKI Research Workshop*, Available at http://middleware.internet2.edu/pki03/PKI03-proceedings.html (2002)

[15] T. Kwon, "Refinement and Improvement of Virtual Software Token Protocols," *IEEE Communications Letters*, Vol. 8, No. 1, pp. 75-77 (2004)

[16] W. Ford and B. Kaliski, "Server-Assisted Generation of a Strong Secret from a Password," *IEEE P1363.2 Working Group*, Available at http://grouper.ieee.org/groups/1363/passwdPK/contributions.html#FK00 (2000)

[17] 이정현, 김현정, 이동훈, "다중서버를 이용한 인증된 키교환 프로토콜," 정보보호학회논문지 13권 1호, pp. 87-98 (2003)

[18] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attack," *Advances in Cryptology-EUROCRYPT '2000*, LNCS 1807, pp. 139-155 (2000)

[19] S. Blake-Wilson, A. Menezes, "Authenticated Diffie-Hellman Key Agreement Protocols," *Selected Areas in Cryptography'98-SAC'98*, LNCS 1556, pp, 339-361 (1998)

[20] Ueli Maurer and Stefan Wolf, "Diffie-Hellman, Decision Diffie-Hellman, and Discrete Logarithms," *Proceedings of IEEE International Symposium on Information Theory Society-ISIT' 1998*, pp. 327 (1998)

[21] D. Boneh, "The decision Diffie-Hellman problem," *Algorithmic Number Theory, Third International Symposium-ANTS-III*, LNCS 1423, pp. 48-63 (1998)

[22] D. Denning and G. Sacco, "Timestamps

in key distribution protocols", *Communications of the ACM*, vol 24, no 8, pages 533-536 (1981)

[23] A. Menezes, P. van Oorschot, S. Vanston "Handbook of applied cryptography," *CRC Press, Inc.*, pp 618 (1997)

[24] 박영만, 박상류, "공중 무선랜에서의 이중요소 인증된 키교환 프로토콜", 한국정보보호학회 논문지 제13권 제5호, (2003.8)

[25] 류종호, 염흥열, "분할된 패스워드 기반 인증된 키교환 프로토콜", 한국정보보호학회논문지 제17권 제5호, (2004.10)

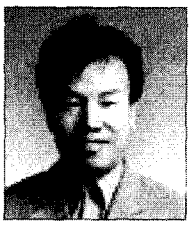
[26] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust Threshold DSS Signatures," *Advances in Cryptology - EUROCRYPT'96*, LNCS 1070, pp. 354-371 (1996)

[27] Masayuki Abe, "Robust Distributed Multiplication without Interaction", *Advances in Cryptology - CRYPTO'99*, LNCS 1666, pp. 130-147 (1999)

[28] Songwon Lee, Kyusuk Han, Seok-kyu Kang, Kwangjo Kim, and So Ran Ine "Threshold Password-Based Authentication Using Bilinear Pairings", *European PKI*, LNCS 3093, pp. 350-363 (2004)

◐ 저 자 소 개 ◑

유 종 호 (Ryu Jong Ho)
1998년 순천향대학교 전자공학과 졸업(학사)
2000년 순천향대학교 대학원 전기 · 전자공학과 졸업(석사)
2004년 순천향대학교 대학원 전기 · 전자공학과 졸업(박사)
2004년 ~ 현재 한국전자통신연구원 정보보호연구단 연구원
관심분야 : 네트워크보안, 인터넷정보보호
E-mail : ryubell@etri.re.kr



서 동 일 (Seo Dong Il)
1989년 경북대학교 전자공학과 졸업(학사)
1994년 포항공과대학교 정보통신공학과 졸업(석사)
2004년 충북대학교 전자계산학과 졸업(박사)
1994년 ~ 현재 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀장
2001년 ~ 현재 ASTAP Forum Information Security 의장
관심분야 : 네트워크보안, 해킹, 인터넷정보보호
E-mail : bluesea@etri.re.kr

염 흥 열 (Youm Heung Youl)
1981년 한양대학교 전자공학과 졸업(학사)
1983년 한양대학교 대학원 전자공학과 졸업(석사)
1990년 한양대학교 대학원 전자공학과 졸업(박사)
1982년 ~ 1990년 한국전자통신연구소 선임연구원
1990년 ~ 현재 순천향대학교 공과대학 정보보호학과 교수
1997년 ~ 2000년 순천향대학교 산업기술연구소 소장
1997년 ~ 현재 한국통신정보보호학회 총무이사(현재), 학술이사, 교육이사
2000년 ~ 현재 순천향대학교 산학연컨소시엄센터 소장
2003년 ~ 현재 ITU-T SG17 Q.L Rapportuer
관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안
E-mail : hyyoum@sch.ac.kr