情報保護學會論文誌
第19卷 第1號, 2009. 2

공개키 인증서를 사용하지 않는 전방향 안전성을 보장하는 E-mail 프로토콜*

권 정 옥,† 구 영 주, 정 익 래, 이 동 훈‡
고려대학교 정보경영공학전문대학원

An E-Mail Protocol Providing Forward Secrecy without Using Certificated Public Keys*

Jeong Ok Kwon,† Young Ju Koo, Ik Rae Jeong, Dong Hoon Lee‡
Graduate School of Information Management and Security CIST, Korea University

요 약

이메일 시스템에서 전방향 안전성(forward secrecy)이란, 메일 사용자와 메일 서버가 장기간 사용하는 비밀키(long-term key)가 노출되더라도 이전 세션들에서 전송된 이메일 메시지의 기밀성(confidentiality)이 보장되는 것을 말한다. 기존 전방향 안전성을 지원하는 이메일 프로토콜들에서는 사용자의 공개키를 사용하기 때문에 공개키에 대한 인증을 위해서는 공개키 기반구조(PKI, Public Key Infrastructure)의 구축이 반드시 필요하다. 본 논문에서는 PKI의 구축이 필요 없이, 사용자의 메일 계정의 패스워드만을 이용하는 전방향 안전성을 보장하는 패스워드 기반의 이메일 프로토콜을 제안한다. 본 논문에서 제안하는 패스워드 기반의 이메일 프로토콜은 인증된 공개키가 필요 없으므로 제한된 자원의 모바일 환경 등에 적합하다.

ABSTRACT

Forward secrecy in an e-mail system means that the compromising of the long-term secret keys of the mail users and mail servers does not affect the confidentiality of the previous e-mail messages. Previous forward-secure e-mail protocols used the certified public keys of the users and thus needed PKI(Public Key Infrastructure). In this paper, we propose a password-based authenticated e-mail protocol providing forward secrecy. The proposed protocol does not require certified public keys and is sufficiently efficient to be executed on resource-restricted mobile devices.

Keywords: E-mail protocol, Forward secrecy, PKI, Authenticated key exchange

접수일 (2008년 6월 11일), 수정일 (2008년 10월 1일), 게재확정일 (2008년 12월 8일)
* 이 논문은 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-2008-314-D00412). 이 연구에 참여한 연구자 중 일부는 '2단계 BK21사업'의 지원비를 받았음.
† 주저자, pitapat@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

Ⅰ. 서 론

이메일의 사용은 그 편리함과 네트워크의 발전에 따른 빠른 지원 속도로 사무실 일처리와 커뮤니케이션에 있어서 없어서는 안 될 생활의 일부가 되었다. 그러나 인터넷 범죄가 늘어나고 있고 그 위험성이 증가함에 따라 악의적인 공격자에 의해 전송하는 과정에서 이메일

의 콘텐츠가 쉽게 드러나거나 수정될 가능성을 무시할 수 없다. 1995년 Bacard등은 이메일의 메시지에 대한 기밀성과 인증을 제공하기 위한 PGP(Pretty Good Privacy)[1,2]를 제안하였다. PGP는 현재 NIST 표준이다. 그러나 PGP는 이메일의 기밀성과 인증을 제공하지만 이메일 메시지에 대한 전방향 안전성을 보장하지 않는다. 만약 공격자가 장기간 사용되는 사용자의 비밀키(long-term secret key)를 얻게 되면 공격자는 그 이전에 전송된 암호화된 이메일 메시지도 모두 복호화 해볼 수 있다. 일반적으로 키 교환 프로토콜에서는 전방향 안전성을 보장하기 위해서 Diffie-Hellman 키 교환을 사용한다. 그러나 이메일과 같은 store-and-forward 시스템에서는 수신자가 송신자와 지속적으로 통신을 유지할 수 없기 때문에 Diffie-Hellman 키 교환 기법을 적용하기 어렵다.

전방향 안전성을 보장하기 위한 시도로 2005년 Sun 등과 2006년 Kim 등이 이메일 프로토콜을 제시하였다[3,4]. Sun 등[3]은 두 가지 타입의 이메일 프로토콜을 제시 하였으나, 두 번째 프로토콜은 전방향 안전성을 보장하지 않는다. 2005년 Dent 등은 Sun 등이 제시한 두 번째 프로토콜에서 수신자의 롱텀 비밀키가 드러나게 되면, 그 이전의 암호화된 이메일 메시지도 모두 들어난다는 것을 보였다[5]. Kim 등[4]도 전방향 안전성을 보장하는 두 가지 이메일 프로토콜을 제안하였지만, 두 번째 프로토콜은 클라이언트와 서버 위장 공격(impersonation attack)에 취약함을 2007년 Yoon등이 보였다[6]. 이창용 등[7]은 타원곡선 기반의 signcryption 기법을 사용한 단일 수신자와 그룹 수신자를 위한 이메일 프로토콜을 제안하였다. Sun 등과 Kim 등과 이창용 등의 이메일 프로토콜[3,4,7]에서는 PKI를 사용하기 때문에 사용자의 공개키에 대한 인증서를 발행하고, 폐기하는 CA(Certificate Authority)와 같은 제 3 신뢰기관이 필요하다.

나날이 커뮤니케이션 기술이 급속히 발전함에 따라 모바일 커뮤니케이션 환경이 생활에 빠르게 스며들고 있다. 이메일 서비스를 제공하는 AOL, Gmail, MSN, Yahoo와 같은 주된 사업자들도 모바일 이메일 서비스를 제공하고 있다. 모바일 환경에서는 모바일의 이동성과 무선과 같은 특징으로 인해 보안에 대한 잠재적인 위험이 더욱 크다. 모바일 서비스는 이미 넓게 상용화되어 있지만, 아직까지 모바일 커뮤니케이션 환경에서는 PKI를 지원하지 않는다. 더군다나 모바일 장치는 제한된 자원을 가지고 있기 때문에 PKI를 사용하기 위해 요구되는 계산을 수행할 만한 능력이 충분치 못하다. 따라서 이러한 모바일 어플리케이션에 적용 가능한 안전한 이메일 시스템이 필요하다.

본 논문에서는 전방향 안전성을 보장하는 효율적인 패스워드 기반의 이메일 프로토콜을 제안한다. 즉, 장기 사용되는 사용자와 서버의 비밀키가 노출되더라도, 그 이전에 전송된 이메일 메시지에 대한 기밀성을 보장한다. 또한 이전의 이메일 프로토콜과는 달리 PKI를 필요로 하지 않으므로 인증서 발급과 검증, 폐기와 같은 인증서 관리의 문제가 없다. 제안하는 이메일 프로토콜은 현재 널리 확산되고 있는 모바일 메일에 실질적으로 적용할 수 있는 안전한 이메일 프로토콜이다.

Ⅱ. 이메일 프로토콜의 보안 요구사항

이메일 프로토콜에서 요구되는 안전성은 인증과 메시지 기밀성과 전방향 안전성이다. 인증이란 메시지 위조 및 변조 등과 같은 공격을 통해서 프로토콜 개체를 위장할 수 없어야 함을 의미한다. 예를 들어, 만약 이메일 프로토콜이 인증을 제공하지 않는다면, 송신자를 위장하여 메시지를 수신자에게 보내는 것과 같은 공격을 수행할 수 있다. 메시지 기밀성이란 전송되는 이메일 메시지에 대한 정보를 정당한 수신자 이외에 얻을 수 없어야 함을 의미한다. 전방향 안전성이란 사용자와 서버들의 롱텀 비밀키(long-term secret key)가 노출되더라도 그 이전에 전송된 암호화된 이메일 메시지에 대한 정보를 얻을 수 없어야 함을 의미한다.

Ⅲ. 패스워드 기반의 인증된 이메일 프로토콜

본 장에서는 인증서 사용이 없이 메일 계정의 패스워드만을 이용하는 전방향 안전성을 제공하는 패스워드 기반의 인증된 이메일 프로토콜인 PAE(Password-Based Authenticated E-mail)를 제안한다.

인증된 키 교환에서는(AKE, Authenticated Key Exchange) 통신에 참여하는 개체 간 인증을 통해 그들 사이에 숏텀키(short-term key) 또는 세션키를 공유한다. 패스워드 기반의 AKE(PAKE, Password Authenticated Key Exchange)의 경우, 오직 사람이 기억하는 패스워드를 사용하여 인증하며, 세션키를 공유

한다. PAE 프로토콜은 PAKE를 기본 요소로 사용한다.

프로토콜에는 메일 서버 S_A와 S_A에 등록된 송신자 A, 메일 서버 S_B와 S_B에 등록된 수신자 B, 이렇게 네 참여자가 존재한다. 여기서 서버 S_A와 S_B가 같을 경우 PAE는 쉽게 수정 가능하므로, 본 논문에서는 S_A와 S_B가 서로 다른 메일 서버라고 가정한다. 사용자 $A(B)$는 패스워드 $pw_A\,(pw_B)$를 사용하고, 서버 $S_A(S_B)$는 사전에 $PW_A = H(pw_A)(PW_B = (pw_B))$를 저장한다.

PAE는 로그인 단계, 메일 송신 단계, 메일 수신 단계의 세 단계로 구성된다. 로그인 단계에서 사용자와 사용자의 메일 서버는 세션키를 공유하기 위해 PAKE 프로토콜을 실행한다. PAKE 프로토콜로 PAE는 Kobara[8] 등에 의해 제안된 두 개체간의 PAKE 스킴을 수정하여 사용한다. Kobara 등에 의해 제안된 PAKE 프로토콜을 적용하는 이유는 기존 제안된 PAKE 프로토콜 중에 이상적인 함수와 같은 랜덤 오라클(random oracle)을 필요치 않는 구조이면서 가장 효율적이라고 알려진 프로토콜이기 때문이다. 송신 단계에서 메일 송신자는 수신자에게 이메일을 전송한다. 이 단계에서 수신자는 온라인일 필요는 없다. 수신 단계에서 수신자는 이메일 서버로부터 이메일을 받는다. 이 단계에서 송신자는 온라인일 필요는 없다.

3.1 공개 정보

다음은 프로토콜의 모든 개체에게 공개되는 공개 정보이다.

[표 1] 기 호

l	안전성 파라미터(security parameter)
G	소수인 q를 위수(order)로 갖는 디피-헬만 결정(DDH, Decisional Diffie-Hellman) 문제가 어려운 순환 군(cyclic group)
g_1, g_2	G의 생성자로, 서로의 이산대수 관계를 알 수 없도록 생성
M	강력한 위조 불가능성(strongly unforgeability)을 갖는 MAC(메시지 인증 코드, Message Authentication Code) 알고리즘. Key는 l을 입력으로 하여 MAC 키 k_{mac}을 생성. k_{mac}이 주어지면 Mac은 메시지 m에 대한 태그, $\tau = Mac_{k_{mac}}(m)$를 계산. Vfy는 k_{mac}을 이용해 메시지와 태그 쌍을 검증하여 유효하면 1을, 그렇지 않다면 0을 출력
SE	대칭키 암호 스킴. K는 키 생성 알고리즘으로 l을 입력으로 하여 비밀키 k를 출력. $E_k(m)$는 암호 알고리즘으로 k를 사용하여 평문 m에 대한 암호문 c를 출력. $D_k(c)$는 복호화 알고리즘으로 k를 사용하여 암호문에 대한 평문을 출력
PE	공개키 암호 스킴. PK는 키 생성 알고리즘으로 l을 입력으로 하여 개인키와 공개키 쌍인 (x,y)를 출력. $PE_y(m)$는 암호화 알고리즘으로 y를 사용하여 평문 m에 대한 암호문 c를 출력. $PD_x(c)$는 복호화 알고리즘으로 x를 사용하여 암호문에 대한 평문을 출력
H	$\{0,1\}^* \rightarrow \{0,1\}^l$인 해쉬 함수
F	의사 랜덤 함수 집합(pseudorandom function family)

3.2 PAE 프로토콜

프로토콜 설명에서 개체 아이디는 개체의 이름과 동일하게 사용한다. 송신자 A는 모바일 장치에 일회용(one-time) 개인키와 공개키 쌍인 (α_A, β_A)를 가지고 있다고 가정한다. 사용자는 일회용 개인키와 공개키 쌍을 프로토콜에서 사용하는 공개키 암호 스킴 PE의 키 생성알고리즘 K를 사용하여 공개키로부터 개인키를 유도해 낼 수 없도록 생성한다. A의 메일 서버 S_A는 A와 이전 프로토콜을 수행하여 얻은 (A, β_A)을 저장한다고 가정한다. 유사하게 수신자 B도 (α_B, β_B)를 가지며, B의 메일 서버 S_B는 (B, β_B)를 저장한다. (α_A, β_A)와 (B, β_B)는 한번만 쓰이는 값이며, 프로토콜에서 수신자의 일회용 공개키 β_B는 프로토콜에서 생성되는 세션키인 k_{SS}, K_A, K_B로 암호화되기 때문에 세션키(k_{SS}, K_A, K_B)를 알 수 있는 사람만이 암호화 및 복호화를 할 수 있다. β_B를 변조하기 위해서는 세션키(k_{SS}, K_A, K_B)를 알아야 하므로 β_B에 대한 인증은 세션키(k_{SS}, K_A, K_B)를 통해 이뤄진다. 따라서 프로토콜에서 β_B에 대한 공개키 인증서는 전혀 필요하지 않는다. [그림 1]은 PAE 프로토콜을 나타내며, 각 단계는 다음과 같다.

A의 로그인 단계: A가 서버 S_A에 로그인하고자 할 때, A와 S_A는 다음과 같이 프로토콜을 시행한다.

(1) A는 $PW_A = H(pw_A)$를 계산하고, 랜덤 값 $x_A \in Z_q^*$를 선택한다.
그리고$(A, X_A = g_1^{x_A} \cdot g_2^{H(A \,\|\, S_A \,\|\, PW_A)} \bmod p)$를 S_A에게 전송한다.

(2) S_A도 랜덤값 $y_A \in Z_q^*$를 선택하고,

<A의 로그인단계> $A(pw_A)$		$S_A(PW_A = H(pw_A))$
$x_A \in Z_q^*$		$y_A \in Z_q^*$
$A, X_A = g_1^{x_A} \cdot g_2^{H(A \parallel S_A \parallel PW_A)} \bmod p$	$\rightarrow \quad \leftarrow$	$S_A, X_{S_A} = g_1^{y_A} \cdot g_2^{H(A \parallel S_A \parallel PW_A)} \bmod p$
$k_A = g_1^{x_A y_A} \bmod p$		$k_A = g_1^{x_A y_A} \bmod p$
$\tau_A = Mac_{k_A}(A \parallel S_A \parallel X_A \parallel X_{S_A})$	$\rightarrow \quad \leftarrow$	$\tau_{S_A} = Mac_{k_A}(S_A \parallel A \parallel X_A \parallel X_{S_A})$
$Vfy_{k_A}(\tau_{S_A}) = 1$인지 확인		$Vfy_{k_A}(\tau_A) = 1$인지 확인
$K_A = F_{H(A \parallel S_A \parallel k_A)}(A \parallel S_A \parallel X_A \parallel X_{S_A})$		$K_A = F_{H(A \parallel S_A \parallel k_A)}(A \parallel S_A \parallel X_A \parallel X_{S_A})$

<A의 송신단계> $A(K_A)$	$S_A(K_A)$	S_B
$E_{K_A}(A \parallel S_A \parallel B) \rightarrow$		
	S_A와 S_B는 AKE 프로토콜을 수행하여 k_{SS}를 교환	
		(B, β_B) 검색
		$\leftarrow \quad Y_B = E_{k_{ss}}(S_B \parallel S_A \parallel B \| \beta_B)$
	$\leftarrow Y_A = E_{K_A}(S_A \parallel S_A \parallel B \| \beta_B)$	
$Z = PE_{\beta_B}(A \parallel B \parallel m)$		
$Z_1 = E_{K_A}(A \parallel B \parallel Z) \rightarrow$		
	$Z_2 = E_{k_{ss}}(S_A \parallel S_B \parallel Z) \rightarrow$	$Z_3 = E_{K_B}(Z)$를 계산 (A, B, Z_3)를 보관

<B의 수신단계>	$S_B(K_B)$	$B\ (K_B, \alpha_B)$
	$Z_3 \rightarrow$	
		$m \leftarrow PD_{\alpha_B}(Z)$
		모바일 기기의 (α_B, β_B)를 (α'_B, β'_B)로 대체

[그림 1] PAE 프로토콜

$(S_A,\ X_{S_A} = g_1^{y_A} \cdot g_2^{H(A \parallel S_A \parallel PW_A)} \bmod p)$를 A에게 전송한다.

(3) A는 $k_A = (X_{S_A} / g_2^{H(A \parallel S_A \parallel pw_A)})^{x_A} \bmod p$ 와 $\tau_A = Mac_{k_A}(A \parallel S_A \parallel X_A \parallel X_{S_A})$를 계산하고, τ_A를 S_A에게 전송한다.

(4) S_A도 $k_A = (X_A / g_2^{H(A \parallel S_A \parallel pw_A)})^{y_A} \bmod p$ 와 $\tau_{S_A} = Mac_{k_A}(S_A \parallel A \parallel X_A \parallel X_{S_A})$를 계산한 후, τ_{S_A}를 A에게 전송한다.

(5) $A(S_A)$는 $\tau_{S_A}(\tau_A)$를 검증한다. 만약 MAC 태그가 유효하지 않다면 프로토콜을 중단하고, 그렇지 않다면 A와 S_A는 세션키 $K_A = F_{H(A \parallel S_A \parallel k_A)}(A \parallel S_A \parallel X_A \parallel X_{S_A})$를 계산한다.

A의 메일 송신 단계: A가 B에게 메시지 m을 전송하고자 할 때, A와 S_A 그리고 S_B는 다음과 같이 프로토콜을 시행한다.

(1) A는 S_A에게 $E_{K_A}(A \parallel S_A \parallel B)$를 전송한다.

(2) S_A와 S_B는 안전한 AKE(Authenticated Key Exchange) 프로토콜을 사용하여 세션키 k_{ss}를 공유한다. (예를 들어, 서버 간에는 공개키 기반의 AKE 프로토콜을 수행하여 세션키를 공유할 수 있다.)

(3) S_B는 현재 저장되어 있는 (B,β_B)를 이용하여 $Y_B = E_{k_{SS}}(S_B \| S_A \| B \| \beta_B)$를 만들어 S_A에게 전송한다.
(4) Y_B를 수신 후에 S_A는 $Y_A = E_{K_A}(S_A \| A \| B \| \beta_B)$를 A에게 전송한다.
(5) A는 K_A를 사용하여 Y_A를 복호하여 β_B를 얻는다. $Z = PE_{\beta_B}(A \| B \| m)$를 계산하고, $Z_1 = E_{K_A}(A \| B \| Z)$을 S_A에게 전송한다.
(6) S_A는 K_A를 사용하여 Z_1을 복호한 후 Z를 얻고, $Z_2 = E_{k_{SS}}(S_A \| S_B \| Z)$를 S_B에게 전송한다.
(7) Z_2를 전송 받은 후, S_B는 k_{SS}로 Z_2를 복호하여 Z를 얻고, $(A, B, Z_3 = E_{K_B}(Z))$를 저장한다.

B의 로그인 단계: A의 로그인 단계와 동일하다. B가 성공적으로 S_B에 로그인한 후에 B와 S_B는 세션키 K_B를 교환한다.

B의 메일 수신 단계:
(1) S_B은 Z_3을 B에게 전송한다.
(2) B는 K_B를 이용하여 Z_3을 복호하여 Z를 얻고, 모바일 장치에 저장된 개인키 β_B를 이용하여 Z로부터 메시지 m을 얻는다. B는 새로운 일회용 개인키/공개키 쌍 (α'_B, β'_B)를 PK를 사용하여 생성하고, 모바일 장치에 (α_B, β_B)를 (α'_B, β'_B)로 대체한다. 그리고 나서 $E_{K_B}(B \| S_B \| \beta'_B)$를 S_B에게 전송한다.
(3) S_B는 현재 저장되어 있는 (B, β_B)를 (B, β'_B)로 대체한다.

Ⅳ. 안전성 및 효율성 분석

4.1 안전성 분석

다음에서 PAE가 인증 및 메시지 기밀성과 전방향 안전성을 제공함을 보인다.

인증 및 메시지 기밀성: PAE에서 만약 인증을 제공하지 않는다면 다음과 같은 위장 공격과 메시지 기밀성에 대한 공격이 가능하다.

(1) 만약 공격자가 메일 서버 S_A에게 메일 송신자 A를 위장할 수 있다면 공격자는 송신자의 메일 서버와 동일한 세션키 K_A를 성공적으로 공유할 수 있고, 공유한 세션키를 이용하여 자신이 보내고자 하는 이메일을 A가 보낸 것처럼 수신자에게 전송할 수 있다.; 공격자가 수신자 메일 서버 S_B에게 송신자 메일 서버 S_A로 위장할 수 있다면 공격자는 S_B와 동일한 세션키 k_{SS}를 성공적으로 공유할 수 있고, 공유한 세션키를 이용하여 자신이 보내고자 하는 이메일을 A가 보낸 것처럼 수신자에게 전송할 수 있다.; 만약 공격자가 메일 수신자 B에게 메일 서버 S_B를 위장할 수 있다면 공격자는 수신자와 동일한 세션키 K_B를 성공적으로 공유할 수 있고, 공유한 세션키를 이용하여 B의 일회용 공개키를 알 수 있다. 따라서 공격자는 자신이 보내고자 하는 이메일을 A가 보낸 것처럼 수신자에게 전송할 수 있다.
(2) PAE에서 이메일 메시지는 수신자 B의 일회용 공개키 β_B로 암호화된다. 만약 공격자가 송신자 A에게 메일 서버 S_A로 위장할 수 있다면 공격자는 송신자와 동일한 세션키 K_A를 성공적으로 공유할 수 있고, 공유한 세션키를 이용하여 자신이 선택한 일회용 공개키를 송신자에게 전송할 수 있다. 송신자는 공격자의 일회용 공개키로 메시지를 암호화하게 되기 때문에 공격자는 자신의 일회용 비밀키를 이용하여 송신자의 메일 메시지를 복호할 수 있게 된다.; 만약 공격자가 송신자 메일 서버 S_A에게 수신자 메일 서버 S_B로 위장할 수 있다면 공격자는 S_A와 동일한 세션키 k_{SS}를 성공적으로 공유할 수 있고, 공유한 세션키를 이용하여 자신이 선택한 일회용 공개키를 송신자에게 전송할 수 있다. 앞의 경우와 마찬가지로 공격자는 자신의 일회용 비밀키를 이용하여 송신자의 메일 메시지를 복호할 수 있게 된다.

이처럼 PAE의 인증 및 메시지 기밀성은 사용자와 메일 서버 간에 설립된 세션키와 메일 서버 간에 설립된 세션키의 기밀성에 기반한다. 따라서 SE와 PE가 모두 안전한 암호 스킴이라는 가정 하에 PAE의 인증 및 메시지 기밀성에 대한 안전성은 세션키의 키 기밀성(key secrecy)을 통해 보인다. 키 기밀성이란 계산적으로 제한된 능력을 가진 공격자가 프로토콜의 정직한 참가자

에게 자신이 선택한 메시지를 보내거나 도청을 통해서 공유된 세션키에 대한 정보를 얻을 수 없어야 함을 의미한다. 이러한 키 기밀성은 공격자 Eve가 임의의 난수로부터 세션 키를 구분하는 확률로 측정된다. Eve가 주어진 챌린지(challenge) 값이 실제 세션키 인지 랜덤 값인지를 올바르게 구분할 확률을 $\Pr[CG]$라고 할 때, l이 안전성 파라미터(security parameter)일 때, Eve의 이득(advantage)은 $Adv_{Eve}(l) = 2 \cdot \Pr[CG] - 1$ 이다. 만약 t가 공격자에게 허용되는 시간이라고 할 때, 모든 다항 시간(polynomial time) 공격자들에 대해서 $Adv(l,t) = \max_{Eve}\{Adv_{Eve}(l)\}$가 무시할만한(negligible)[1] 값이라면, 프로토콜은 키 기밀성을 제공한다고 한다.

PAE의 키 기밀성은 결정적 디피-헬만 가정(DDH assumption)에 기반한다. DDH 문제는 $G = \langle g \rangle$가 소수인 q를 위수로 갖는 순환군이고, (g, U, V, W)가 주어졌을 때, 주어진 값이 실제 DDH 값인지 랜덤한 값인지를 구분하는 문제이다. 만약 다음의 부등식을 만족한다면, 알고리즘 D는 ϵ의 이득(advantage) $Adv^{ddh}_{G,D}$로 DDH 문제를 푼다고 한다:

$$|\Pr[u,v \leftarrow Z_q : D(g,g^u,g^v,g^{uv}) = 1] - \Pr[u,v,w \leftarrow Z_q : D(g,g^u,g^v,g^w) = 1]| \geq \epsilon.$$

만약 t가 공격자에게 허용되는 시간이라고 할 때, 모든 다항 시간 공격자들에 대해서 $Adv^{ddh}_{G}(t) = \max_{D}\{Adv^{ddh}_{G,D}\}$가 무시할만한(negligible) 값이라면, 그룹 G에서 DDH 가정을 만족한다고 한다.

만약 PAE의 공격자 Eve가 K_A로부터 유용한 정보를 얻어낼 수 있다면, Eve는 랜덤 값과 세션키 K_A를 무시할 수 없는(non-negligible) 확률로 구분해 낼 수 있다는 것은 명백하다. 따라서 K_A에 대한 키 기밀성을 증명하기 위해서 DDH 문제가 어렵다는 가정이 성립할 때, 공격자 Eve가 K_A와 랜덤 값을 다항 시간 내에 구별할 수 없음을 보인다.

Eve의 이득(advantage), $Adv_{Eve}(l)$을 계산하기 위해 우선 두 게임 $Game_0$과 $Game_1$을 정의한다. $Game_0$에서 프로토콜 메시지는 PAE 프로토콜에 따라 구성된다. $Game_1$에서는 프로토콜에서 사용되는 MAC 키인 k_A를 랜덤 값으로 대체하여 사용한다. 만약 두 게임에서 Eve의 이득이 무시할 수 없는 확률로 다르다면 Eve를 사용하여 DDH 문제를 무시할 수 없는 확률로 푸는 알고리즘 D를 다음과 같이 만들 수 있다. 이것은 DDH 문제가 어렵다는 사실에 모순되므로 무시할 수 없는 확률로 다항 시간 안에 세션키에 대한 기밀성을 깨는 공격자가 존재 할 수 없음을 의미한다.

D에는 DDH 문제 사례의 입력 값 $(g_1, U = g_1^u, V = g_1^v, W)$이 주어진다. D는 $W = g_1^{uv}$이면, 1을 출력하고, W가 랜덤한 값이라면 0을 출력한다. D는 입력 값을 프로토콜의 메시지에 다음과 같이 심는다. D는 $X_A = U \cdot g_2^{H(A \| S_A \| pw_A)} \bmod p$, $X_{S_A} = V \cdot g_2^{H(A \| S_A \| pw_A)} \bmod p$, $k_A = W$를 계산한다. 그리고 Eve에게 챌린지 값으로 동전 던지기(coin fliping)를 하여 앞면이 나오면 k_A를 이용하여 프로토콜에 따라 계산한 K_A를 주고, 뒷면이 나오면 랜덤 값을 준다. Eve는 챌린지 값이 실제 세션키라면 1을 출력하고, 랜덤한 값이라면 0을 출력한다. D는 Eve의 답을 DDH 문제의 답으로 그대로 출력하며 종료한다.

DDH 문제의 해답과 키를 구분하는 문제의 해답은 동일하다. D는 (g_1, U, V, W)가 DDH 값이 맞느냐 아니냐에 따라 $Game_0$ 또는 $Game_1$을 Eve에게 완벽히 시뮬레이션해 줄 수 있다. 즉, 만약 (g_1, U, V, W)이 DDH 값이 맞으면 D은 $Game_0$을 시뮬레이션하고, 그렇지 않으면 $Game_1$을 시뮬레이션한다. 따라서 D가 성공할 확률 $Adv^{ddh}_{G,D}$가 다음과 같다고 할 때, $|Game_0$에서 Eve의 $\Pr[CG] - Game_1$에서 Eve의 $\Pr[CG]| = Adv^{ddh}_{G,D}$가 된다.

$$Adv^{ddh}_{D} = |\Pr[u,v \leftarrow Z_q^*, (g_1, U, V, W) \leftarrow (g_1, g_1^u, g_1^v, g_1^{uv}) : D(g_1, U, V, W)] = 1| - |\Pr[u,v,w \leftarrow Z_q^*, (g_1, U, V, W) \leftarrow (g_1, g_1^u, g_1^v, g_1^w) : D(g_1, U, V, W)] = 1|.$$

$Game_1$에서 k_A는 랜덤 값이므로 프로토콜 메시지와는 독립적이다. 이로부터 K_A 또한 프로토콜 메시지와 독립적이라는 것을 알 수 있으므로, $Game_1$에서 Eve의 $\Pr[CG]$는 1/2보다 클 수 없다. 따라서 $Adv_{\mathbf{PAE}}(l,t) \leq \leq 2Adv^{ddh}_{G}$이다. K_B에 대한 키 기밀성 역시 이와 마찬가

1) 어떤 함수 f가 무시할만한 하면, f는 충분히 큰 값들에 대해, 모든 다항함수(polynomial)의 역수보다 더 빨리 감소한다. 즉, 모든 상수 c에 대해서, 다음을 만족하는 자연수 N이 존재한다. N보다 큰 모든 n에 대해서, $f(n) < \frac{1}{n^c}$.

[표 2] 전방향 안전성을 제공하는 안전한 이메일 프로토콜의 효율성 및 인증서 검증 여부 비교

스킴	지수승 연산량		사용자 측의 인증서 검증여부
	송신자	수신자	
Sun 등의 첫 번째 스킴[3]	$Cert\,Vfy+Sig+Ver+1$	$Cert\,Vfy+1$	O
Kim 등의 첫 번째 스킴[4]	$PEnc+Cert\,Vfy+Sig+1$	$PDec+Cert\,Vfy+Vfy+2$	O
제안 스킴	$PEnc+1$	$PDec+1$	X

*$Cert\,Vfy$: 인증서 검증 시 필요한 지수승 연산, Sig: 서명 생성 시 필요한 지수승 연산, Vfy: 서명 검증 시 필요한 지 수승 연산, $PEnc$: 공개키 암호 알고리즘에 필요한 지수승 연산, $PDec$: 공개키 복호 알고리즘에 필요한 지수승 연산

지로 증명된다.

두 메일 서버간의 세션키 k_{SS} 또한 안전한 AKE 프로토콜을 이용하여 설립되기 때문에 랜덤 값과 구별 가능하지 않다.

전방향 안전성: 두 서버가 전방향 안전성을 제공하지 않는 AKE 프로토콜을 이용하여 세션키 k_{SS}를 공유했다고 가정해보자. AKE가 전방향 안전성을 제공하지 않으므로 공격자는 서버의 롱텀키를 이용하여 두 서버간의 세션키 k_{SS}를 계산할 수 있다. 공격자는 k_{SS}를 이용하여 Y_B를 복호화 함으로써 B의 일회용 공개키 β_B를 얻을 수 있다. 그러나 공격자는 일회용 공개키 β_B에 대응하는 일회용 개인키 α_B값을 계산할 수 없으므로 전송된 이메일 메시지를 복호화 할 수 없다. 따라서 롱텀키가 노출되기 이전에 전송된 이메일 메시지에 대해서 어떠한 정보도 얻을 수 없다. 공격자가 pw_A와 pw_B를 획득했을 경우, 사용자와 서버간의 임시키 k_A와 k_B는 Diffie-Hellman 키 교환 기법으로 생성되기 때문에 공격자는 pw_A와 pw_B로부터 세션키 K_A또는 K_B를 알아낼 수 없으며 β_B에 대한 정보도 알아낼 수 없다.

주의: PAE는 정직하게 행동하는 서버들 간에 이메일 메시지의 기밀성을 제공한다. 즉, 서버들은 도청을 통해서 사용자의 이메일 메시지에 대한 어떠한 정보도 얻을 수 없다. 그러나 만약 서버들이 정직하지 않게 프로토콜을 수행한다면, 서버는 모든 사용자의 패스워드를 알고 있기 때문에 사용자의 메시지에 대한 정보를 알아낼 수 있는 단점이 있다. 이러한 단점은 공개키 기반의 이메일 프로토콜에 비하여 패스워드만을 비밀키로 사용하는 모든 패스워드 기반의 이메일 프로토콜이 가지는 부득이한 사항이다.

4.2 효율성 분석

[표 2]에서 전방향 안전성을 제공하며 안전하다고 알려진 이메일 프로토콜과 제안 프로토콜의 계산량을 비교한다. 프로토콜들에서 수행하는 연산 중 가장 많은 비용이 드는 연산은 지수승 연산이기 때문에 표에서는 지수승 연산만을 비교한다. [표 3]에서는 [3]에서와 같이 송신자 측에서 메일을 전송하기 위해 사전에 계산 가능한 부분은 제외하고 온라인으로 수행해야하는 지수승 연산과 수신자 측에서 메일을 복호화하기 위해서 수행해야하는 지수승 연산을 비교한다. 그리고 사용자 측의 공개키 인증서 검증의 필요성 대해 비교한다.

Ⅴ. 결 론

본 논문에서는 전방향 안전성을 제공하는 효율적인 패스워드 기반의 인증된 이메일 프로토콜인 PAE를 제안한다. PAE는 사용자가 공개키 인증서 없이 메일 계정의 패스워드만을 이용하여 암호화된 이메일을 주고받는 것을 가능하게 한다. 따라서 PAE는 공개키 기반구조(PKI)를 적용하기 어려운 여러 환경에서 사용될 수 있는 실용적인 이메일 프로토콜이라 할 수 있다.

참고문헌

[1] A. Bacard, The Computer Privacy Handbook: A Practical Guide to EMail Encryption, Data Protection, and PGP Privacy Software, Peachpit Press, Jan. 1995.

[2] B. Schneier, E-Mail Security with PGP and PEM: How to Keep Your Electronic Mail

Private, John Wiley Press, Jan. 1995.

[3] H.M. Sun, B.T. Hsieh, and H.J. Hwang, “Secure E-mail Protocols Providing Perfect Forward Secrecy,” IEEE Communications Letters, vol. 9, no. 1, pp. 58-60, Jan. 2005.

[4] B.H. Kim, J.H. Koo, and D.H. Lee, “Robust E-Mail Protocols with Perfect Forward Secrecy,” IEEE Communications Letters, vol. 10, no. 6, pp. 510-512, June 2006.

[5] A.W. Dent, “Flaws in an E-Mail Protocol of Sun, Hsieh, and Hwang,” IEEE Communications Letters, vol. 9, no. 8, pp. 718-719, Aug. 2005.

[6] E.J. Yoon and K.Y. Yoo, “Cryptanalysis of Robust E-Mail Protocols with Perfect Forward Secrecy,” IEEE Communications Letters, vol. 11, no. 5, pp. 372-374, May 2007.

[7] 이창용, 김대영, 심동호, 김상진, 오희국, “완전한 전방향 안전성을 제공하는 실용적인 저자우편 프로토콜,” 정보보호학회논문지, 17(5), pp. 27-38, 2007년 10월.

[8] K. Kobara and H. Imai, “Pretty-simple password-authenticated key exchange under standard assumption,” IEICE Transactions on Fundamentals, vol. E85-A, no. 10, pp. 2229-2237, Oct. 2002.

[9] 김범한, 구재형, 이동훈, “완전한 전방향 안전성을 보장하는 이메일 프로토콜,” 한국정보보호학회 충청지부 학술대회, pp. 37-48, 2005년 10월.

[10] 이창용, 김대영, 김상진, 오희국, “Signcryption 기반의 완전한 전방향 안전성을 제공하는 이메일 프로토콜,” 한국정보보호학회 2006년도 하계학술대회, pp. 344-348, 2006년 6월.

<著 者 紹 介>

권 정 옥 (Jeong Ok Kwon) 정회원
2000년 8월: 동덕여자대학교 전자계산학과 학사 졸업
2003년 2월: 고려대학교 정보보호기술협동과정 석사 졸업
2007년 2월: 고려대학교 정보보호대학원 박사 졸업
2007년 3월~2007년 8월: 고려대학교 정보보호기술연구원 박사후연구원
2007년 9월~현재: 고려대학교 BK21 유비쿼터스 정보보호 사업단 연구교수
<관심분야> 암호프로토콜, 암호이론

구 영 주 (Young Ju Koo) 학생회원
2007년 2월: 숭실대학교 수학과 학사 졸업
2007년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 암호프로토콜, 암호이론

정 익 래 (Ik Rae Jeong) 정회원
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
<관심분야> 암호프로토콜, 암호이론, 계산이론, 프라이버시 보호기술

이 동 훈 (Dong Hoon Lee) 종신회원
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
<관심분야> 암호프로토콜, RFID/USN 보안, 프라이버시 보호기술