情報保護學會論文誌
第13券 第4號, 2003. 8

패스워드 인증 키교환 프로토콜의 안전성에 관한 고찰*

이 희 정**

Remark on the Security of Password Schemes

Hee Jung Lee**

요 약

본 논문에서는 패스워드기반 키 교환 인증 프로토콜들, EKE2(Encrypted Key Exchange)와 PAK(Password Authenticated Key exchange)의 안전성에 대해서 살펴본다. 위의 프로토콜들은 이상적 모델을 이용하여 안전성이 증명되었다. 그럼에도 불구하고 공격자의 공격 능력에 따라 프로토콜이 위험할 수 있음을 지적한다. 좀 더 자세히 설명하면 합법적인 사용자가 다른 사용자의 패스워드를 알아내려고 할 때 즉, '내부자' 가 공격을 할 경우 내부자는 서버와 합법적인 통신을 원하는 만큼 진행하여 서버의 일회성 비밀키, 즉 난수에 대한 정보를 얻는다. 내부자는 이를 이용하여 서버와 다른 클라이언트간의 통신을 도청하여 오프라인을 통하여 다른 클라이언트의 패스워드를 알아낼 수 있다. 물론 이러한 공격이 가능하기 위해서는 몇 가지 전제 조건이 있다. 본 논문에서는 이러한 공격 형태를 구체적으로 살펴보고 이상적 모델을 이용하여 안전성을 증명할 때에는 공격자의 능력을 정의하는 데에 좀 더 신중해야함을 지적하고자 한다.

ABSTRACT

We discuss the security of two famous password authenticated key exchange protocols, EKE2 and PAK. We introduce 'insider assisted attack'. Based on this assumption, we point out weakness of the security of EKE2 and PAK protocols. More precisely, when the legitimate user wants to find other user's password, called "insider-assisted attacker", the attacker can find out many ephemeral secrets of the server and then after monitoring on line other legitimate user and snatching some messages, he can guess a valid password of the user using the previous information. Of course for this kind of attack there are some constraints. Here we present a full description of the attack and point out that on the formal model, one should be very careful in describing the adversary's behavior.

keyword : *subgroup confinement, password, authenticated key exchange, LCG*

Ⅰ. 서 론

최근에 패스워드가 갖고 있는 특성 때문에 패스워드를 기반으로 하는 키 교환 인증 프로토콜(PAKE, password authenticated key exchange protocol)이 많이 연구되어지고 있다. 이러한 프로토콜의 예로, 불안전한 네트워크 상에서 클라이언트와 서버간에 패스워드만을 비밀로 하면서 안전한 통신을 할 수 있도록 제공하는 프로토콜들(PAKE)을 들을 수 있다. 이 프로토콜의 안전성은 공격자가 얼마나 온라인을 통하여 프로토콜 참여자와 통신을 하느냐에 전적으로 의존한다. 즉, 이는 공격자가 패스워드에 관한 정보를 얻

* 본 연구는 2002년 강남대학교 교내연구비에 의해서 수행되었습니다.
** 강남대학교 응용수학 전공(hjlee@kangnam.ac.kr)

을 수 있는 유일한 방법이 online guessing밖에는 없다는 것을 의미한다. 많은 키 교환 인증 프로토콜들이 소개되었고 또 이들의 취약점이 발견되고는 했다.[1,2,3] 키 교환 인증 프로토콜들의 안전성을 최초로 Bellare[2]와 Shoup[3]이 이상적인 모델(formal model)로 증명하였다. 이것을 바탕으로 Bellare,[4] Boyko[5] 등도 패스워드기반 프로토콜들을 이상적 모델을 통하여 안전성을 증명하였는데 예를 들어 키 확인을 하는 EKE2(Encrypted Key Exchange protocol)[4]나 PAK(Password Authenticated Key Exchange protocol)[5] 등을 들 수 있다. 현재까지는 이러한 이상적 모델을 이용하여 증명된 프로토콜들은 완벽한 안전성을 제공한다고 간주되어지고 있다.

본 논문에서는 EKE2나 PAK 프로토콜을 이용하여 서버가 사용자를 인증하는 서버 클라이언트시스템을 살펴보려고 한다. 먼저 '내부자 공격'에 대해서 설명하려고 하는데 이는 이미 Halevi,Krawczyk[6]에서 소개된 것이다. 실세계에서 내부자의 도움을 받은 공격자가 있으리라는 가정은 얼마든지 있을 수 있다. 또한, Halevi,Krawczyk[6]에서 지적했듯이 시스템의 내부자 자신이 공격자가 될 경우도 얼마든지 있을 수 있다. 따라서 우리는 공격자가 시스템 내에서 자신의 아이디(ID)를 가질 수 있고 거기에 따른 공인된 패스워드를 가지고 공격을 할 확률을 고려해야만 한다. 따라서 공격자가 자신의 아이디를 이용하여 다른 사용자를 공격하지 못하도록 하는 프로토콜이 필요하다. 그러나 이러한 내부자 공격에 대해서 EKE2나 PAK 프로토콜이 이상적 모델을 통하여 안전성이 증명되었음에도 불구하고 취약한 점이 있음을 알 수 있다. 구체적으로 살펴보면 일종의 서브그룹(subgroup) 공격을 통하여 서버의 일회성 비밀정보 일부를 원하는 만큼 여러 차례에 걸쳐서 알아낸 후 온라인상의 합법적인 사용자가 송수신하는 것을 보고 그러한 정보와 이미 알아낸 정보를 이용하여 합법적인 사용자의 패스워드를 추측할 수 있다. 물론 공격이 가능하기 위해서는 위에서도 언급했듯이 사용상의 몇몇 가정이 필요하다.

2장은 패스워드 인증의 역사와 패스워드 키 교환 인증 프로토콜, EKE2나 PAK에 관한 설명을 하고 3장에서는 EKE2나 PAK에 행해지는 내부자 공격을 하기위한 사전 작업에 대해서 알아보고 4장에서는 구체적인 공격방법을 소개한다. 마지막으로 이러한 공격에 대한 보안 방법과 이상적 모델에서 공격자의 행동 능력을 정의할 때는 매우 조심해야함을 지적한다.

II. 패스워드 인증

2.1 패스워드 키 교환 인증 프로토콜들

패스워드 기반 인증법은 패스워드가 갖는 적은 정보량에도 불구하고 너무나 쉬운 사용상의 이점 때문에 사용자 인증에 매우 많은 관심을 받는 방법이다. 주어진 환경에 따라 목적을 달성하기 위해서 여러 프로토콜들이 개발되었는데 이중에서 EKE가 패스워드 키교환 인증 프로토콜들 중에 중요한 역할을 했다. EKE에 이어서 많은 패스워드 키교환 인증 프로토콜들이 안전성의 요구에 따라 개발되었다. 그러나 많은 패스워드 프로토콜은 패스워드를 보호하기 위해서 특별한 방법들을 사용하여서 공식적인 안전성을 증명하지 못하였고 동시에 그러한 프로토콜에 대한 안전성 주장을 그대로 믿을 수도 없다. OKE[7]가 증명이 가능하게 되었고 그를 이어 SNAPI, EKE2, PAK등도 가능하게 되었다. 최근에 SRP, SPEKE, PAK, AMP등이 IEEE P1363 공개키 표준 그룹에서 패스워드 기반 인증된 키교환 프로토콜의 표준화 후보들로 선택되어졌다. 이 분야의 증명가능한 접근을 위해서 EKE, PAK등에 관한 공식적인 모델을 통한 안전성 증명을 다시 살펴보는 것이 필요하다고 생각된다.

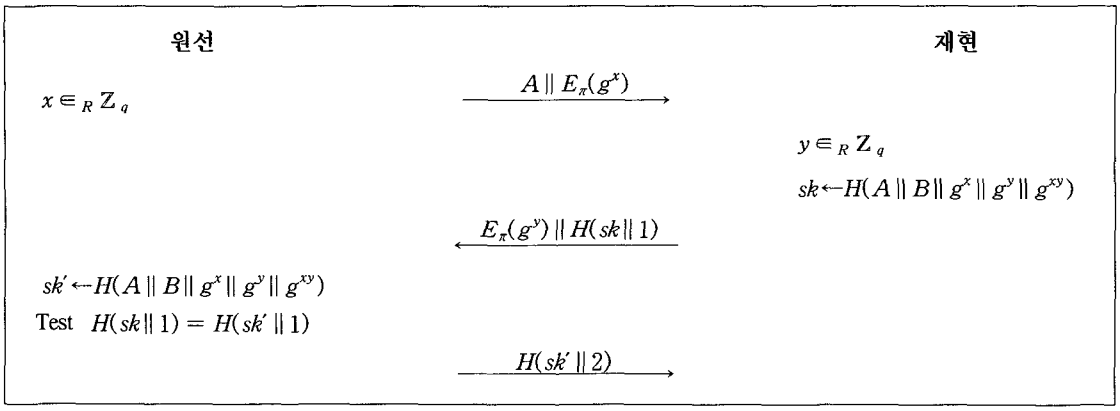
2.2 EKE2와 PAK 프로토콜

간단히 EKE2와 PAK 프로토콜을 살펴보도록 한다.

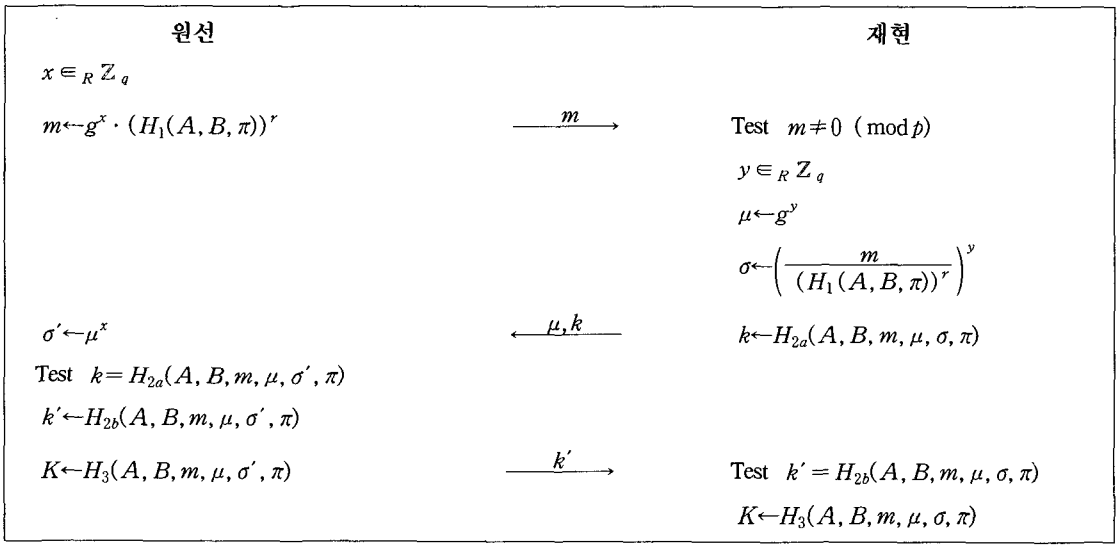
x(160비트)는 해쉬 함수와 비밀키의 안전성 파라미터라고 하고 ι(1024 비트)는 군의 비트 크기라고 생각하자. 이때 $\iota > x$이다. $\{0,1\}^*$는 임의의 길이의 유한 비트 열이라고 하고 $\{0,1\}^n$은 길이가 n인 비트 열이라고 하자. 그리고 q를 크기가 x이고 p는 크기가 ι인 소수들로 $p = qr + 1$이라고 하자. 이때 r과 q는 서로 소이다. g를 위수가 q인 Z_p^*의 부분군의 생성자라고 하자.

H, H_{2a}, H_{2b}, H_3를 $\{0,1\}^*$에서 $\{0,1\}^x$로 가는 해쉬 함수들이라고 하고 H_1은 $\{0,1\}^*$에서 $\{0,1\}^n$, $(n \geq \iota + x)$로 가는 해쉬 함수라 하자. 여기서 H, H_{2a}, H_{2b}, H_3, H_1들은 서로 독립인 암호학적 해쉬 함수로 간주할 수 있다. 지금부터는 특별한 언급이 없는 한 이러한 기호를 위의 정의대로 따를 것이다.

여기서 π는 사용자 원선과 서버 재현간의 패스워드이고(A와 B는 원선과 서버의 아이디를 뜻한다) 공유한 세션키는 $H(sk \| 0)$이고 암호화 함수, E는 이



〔그림 1〕 EKE2 프로토콜 흐름



〔그림 2〕 PAK 프로토콜 흐름

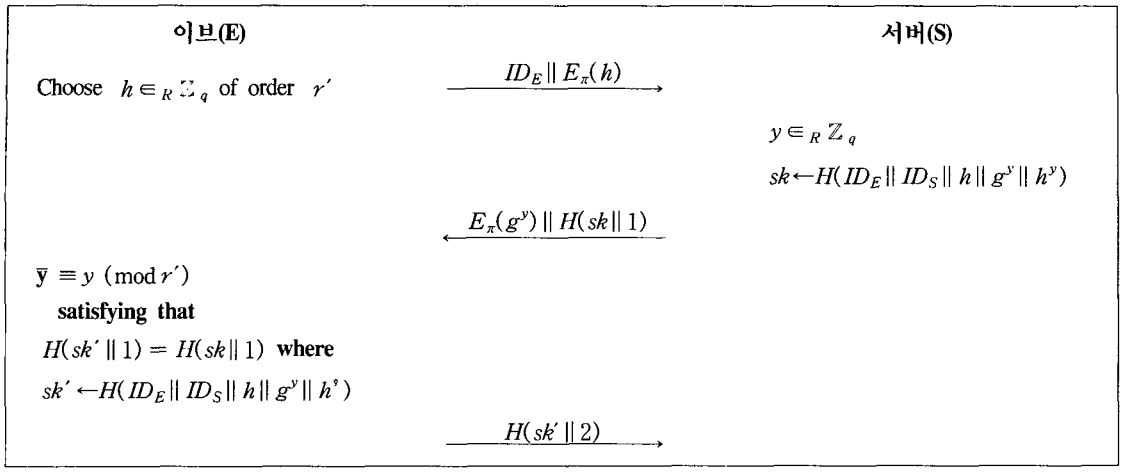
상적인 오라클로 간주한다. 지금까지 이러한 함수가 구체적으로 어떤 것인지는 아직 알려져 있지 않다.

여기서 공유된 세션키는 K이다. m과 μ는 Z_p^*에 있는 위수가 q인 원소들이다. 만약 테스트가 실패하면 재현에 의해서 프로토콜은 중지될 것이다.

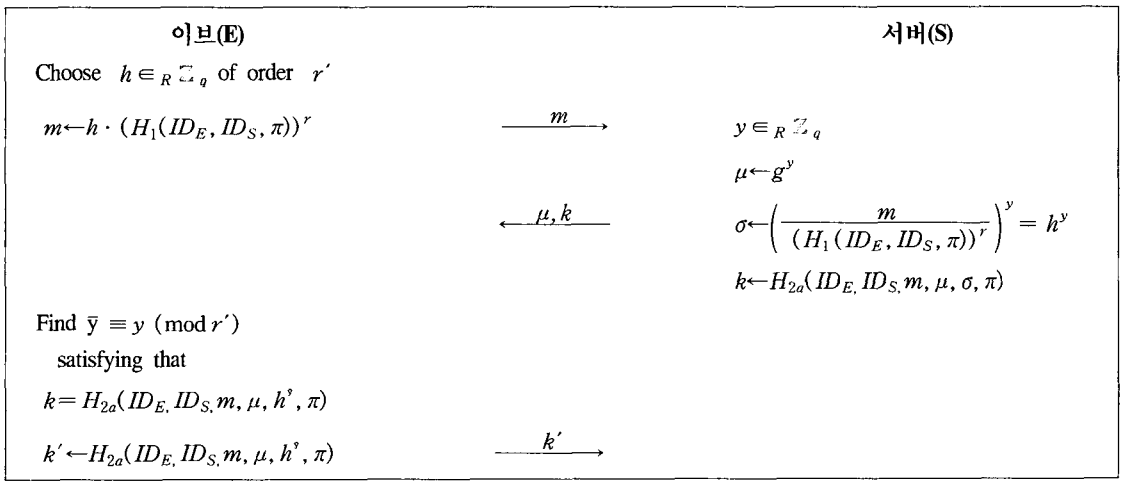
Ⅲ. EKE2와 PAK에 대한 내부자 공격의 사전 작업(공격)

S를 클라이언트-서버 시스템이라고 하자. 이 시스템은 서버가 사용자를 단지 패스워드만으로 인증해 주는 시스템을 뜻한다. 이 시스템 S에서 이브는 합법적으로 자신의 아이디, ID_E와 이에 대한 패스워드 π를 가지고 있다. 서버의 아이디는 ID_S라 하자. 이러한 이브가 시스템 S를 공격할 때 이브를 내부 공격자라고 한다.

EKE2와 PAK에 대한 공격을 하기 위해서 이브는 먼저 서버의 일회성 비밀키의 정보를 알아낼 필요가 있다. 그 이유는 다음 장에서 구체적으로 설명하겠지만 간단히 설명하면 서버가 다른 클라이언트와 통신을 하고 있을 때 그 클라이언트의 패스워드를 알아내기 위해서는 서버의 난수를 알아야 하고 서버가 LCG를 이용하여 난수를 생성한다고 하면 그때의 난수를 찾아내기 위해서 초기 값이 필요하므로 그에 대한 준비 작업을 뜻한다. 이를 위해서 시스템 파라미터에 약간의 제한이 필요한데 $p-1$을 나누는 약수 r이 $\sqrt{q}$보다 훨씬 작은 약수 r'을 갖는다고 해야 한다. r'이 $\sqrt{q}$보다 훨씬 작다는 이야기는 다소 불분명해 보인



〔그림 3〕 EKE2 공격



〔그림 4〕 PAK 공격

다. 여기서는 r'보다 작은 임의의 알려지지 않은 x에 대하여 $H'(h^x)$가 주어졌을 때 무작정 x를 찾는 것이(exhausted search) 계산상으로 가능한 정도의 크기를 의미한다. $H'(h^x)$가 주어졌을 때 x를 찾는 방법이 exhausted search이외에 어떤 것이 있는지 아직 잘 모르겠으나 만약 그러한 것이 발견된다면 우리의 공격은 더욱 강력해 질 것이다.

[그림 3]과 [그림 4]는 EKE2와 PAK에 대한 내부자 공격의 사전단계를 보여준다.

이브는 위수가 r'인 Z_p^*에 있는 원소 h를 선택해서 g^x대신 h를 서버에 보낸다. 여기서 이브는 서버와 아무런 의심도 받지 않은 채 프로토콜을 완전히 실행할 수 있다. 이때 h의 위수가 r'로 작기 때문에 서버의 비밀키에 대한 정보를 일부 찾을 수 있다. 자세히 언급하면 이브는 서버에게 $m = h * H_1^r(ID_E, ID_S, \pi)$(또는 EKE2 경우는 $m = ID_E \| E_\pi(h)$)을 보낸다. m은 위수가 q가 아니지만 서버는 전혀 그것을 눈치 채지 못한다. 이브는 서버로부터 두 개의 값을 얻게 되는데 g^y와 h^y에 대한 해쉬 값이다. y를 서버의 일회성 비밀키라 하자. 이브는 y에 대한 일부 값, 즉, $\bar{y} \equiv y \bmod r'$를 얻게 된다. 이브가 원하는 만큼의 프로토콜을 시행하여 y들에 대한 일부 값들을 알아낸다. 이러한 사전 작업을 통하여 서버가 사용하는 일회성 비밀키의 값을 알아내려는 것이 목적이다.

이러한 공격형태는 프로토콜이 가지고 있는 이산대수문제를 해결하는데 다소 쉽게 하고 있다. 다시 말하면, $\bar{y}$를 얻은 이브는 $y = ar' + \bar{y}$라고 할 때 $g^y / g^{\bar{y}} = (g^{r'})^a$의 이산대수문제(DLP)를 해결하므로 써 일

회성 비밀키 y를 찾을 수 있다. 이는 원래의 EKE2와 PAK가 $|q|$정도의 이산대수문제를 푸는 것에서 $|q|-|r'|$정도 크기의 이산대수문제를 푸는 것으로 줄어들었다.($|n|$은 n정도의 비트 크기를 뜻한다.) EKE2나 PAK 프로토콜에 대한 공격은 보통 생성자 g에 대한 이산대수문제를 풀거나 온라인 상의 추측을 통하여 이루어지는데 우리의 공격 방법은 이러한 어려움을 다소 쉽게 해주는 효과가 있다.

이제 지금까지 언급한 내용을 정리로 요약하려고 한다.

정의 1

합리적인 시간 안에 t크기만큼의 공간에서 일일이 찾아보는(exhausted search) 것이 가능할 때 이러한 양의 정수 t를 탐색 범위(exhausted bound)라고 하자.

정리 1

r의 약수 r'이 탐색 범위(exhausted bound)라고 가정하자. EKE2와 PAK의 y에 관한 일부정보를 r'크기의 후보들에 대한 이산대수문제를 풀어내므로 알아낼 수 있다.

증명: 위에서 이미 언급되었다.

위에 언급된 공격 법은 작은 부분 군 공격(small subgroup confinement) 방법과 같음을 알 수 있을 것이다. 작은 부분 군 공격의 예로 단순화시킨 Diffie-Hellman 실행에 대한 man-in-the-middle 작은 부분 군 공격이 있다. 우리의 공격 법은 단지 작은 부분 군 공격 방법만을 이용한 것이 아니고 '사전 작업(공격)'이란 어휘에서 알 수 있듯이 우리의 공격 중 한 과정에서 사용하는 기법임을 밝혀두고자 한다. 구태여 우리가 사용한 작은 부분 군 공격 방법과 man-in-the middle 공격에서 사용한 작은 부분 군 공격 방법의 차이점을 언급한다면 우리는 완전히 비밀키를 찾아내는 것이 아니고 단지 일회성 비밀키의 일부를 찾아낸다는 것이다.

Ⅳ. EKE2와 PAK 프로토콜 공격

이 절에서는 EKE2와 PAK 프로토콜에 대한 내부자 공격을 자세하게 설명하려고 한다.

먼저 다음과 같은 실질적인 가정을 하자.

1) 탐색 범위인 r의 약수 r'이 존재한다.
2) 클라이언트-서버 시스템 S는 일차 합동 유사 난수 생성자(linear congruential pseudo-random number generator(*LCG*)[8]를 난수 생성자로 사용한다.
3) 이브는 시스템의 사용자로 자신의 아이디, $ID_{이브}$, 와 유효한 자신의 패스워드, π,를 갖고 있다.

실제에 있어서 LCG, 또는 Truncated LCG와 같은 난수 발생기를 쓰는데 이는 다음 번 난수에 대한 예측이 가능한 단점이 있음에도 불구하고 빨라서 효율성이 높기 때문이다. 여기서 예측이 가능하다는 것은 유사 난수 발생기가 주어진 초기값에 따라 수열을 생성했을 때 단지 추측하는 것보다는 훨씬 높은 확률로 다음 난수를 예측할 수 있음을 뜻한다. Bellare[9] 등은 암호 기법에 LCG등을 사용할 때는 매우 조심해야 한다는 것을 경고했다. 그러나 여기서 우리가 지적하고 싶은 것은 그들은 LCG에 의한 수열에 대해서 전체 혹은 일부의 정보를 안 것이 아니다. 예를 들어, LCG를 사용하는 DSS[10]에서 그들은 공격자가 유사 난수 발생기에 의해서 생성된 수열에 관한 어떠한 정보도 없이 공격하는 것이다. 따라서 이러한 LCG 사용상의 주의는 우리가 하려는 공격과는 관계가 없음을 지적하려 한다.

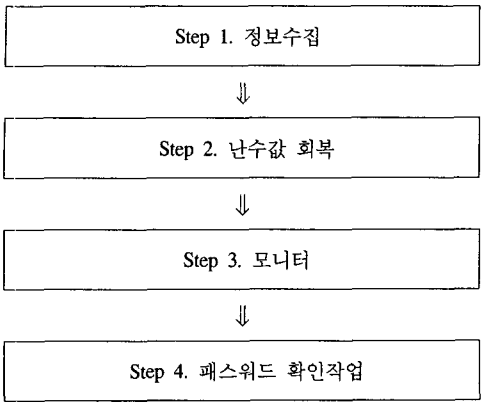
4.1 공격법

공격의 방법을 대략적으로 설명하면 다음과 같다.

- 첫단계 : 온라인 상에서 서버와 합법적인 절차를 통해 *LCG*에 의해서 생성된 y들에 관한 부분정보를 원하는 만큼 얻는다.
- 둘째 단계: 첫 단계로부터 이브는 y들 중의 하나의 값, y_0, 을 찾는다.
- 셋째 단계 : 이브는 서버와 다른 사용자간의 통신을 온라인 상에서 모니터한다.
- 넷째 단계 : 서버로부터의 마지막 메시지를 가로챈 후에 이브는 패스워드 공간과 초기값, y_0에 따른 LCG의 결과 값을 이용하여 오프라인을 통하여 사용자의 유효한 패스워드를 찾아낸다.

각 단계를 좀더 구체적으로 살펴보면 다음과 같다.

단계 1 : 합법적으로 이브는 r'이 탐색 범위(exhausted bound)이기 때문에 상식적인 시간 안에 $\bar{y}$를 계산해 낼 수 있다. 이때 이러한 과정을 반복함으로



〔그림 5〕 The strategy of the presented attack

써 그녀가 원하는 만큼의 $\overline{y}$들을 얻을 수 있다. 특히 이러한 y들에 관한 일부 정보들은 LCG에 의해서 연속적으로 생성된 것들일 수가 있다.

단계 2: LCG는 다음과 같이 난수를 생성한다.

$z_{i+1} \equiv az_i + b \bmod M$ 이때, a, b, 그리고 M은 고정된 값이다. 이브는 임의의 난수 y에 관한 부분정보를 얻을 수 있다. 여기서 M은 q로 간주하고 {여러번의 공격을 통하여 얻은 y들의 값} = $\{y_i\}$라 하자. 각 y_i에 관한 값들은 다음 과정에 의해서 찾을 수 있다.

I. 부분정보 $\overline{y_1}, \cdots, \overline{y_k}$를 사용하여 a, b와 M을 찾아낸다.[11]

II. 부분정보 $\overline{y_1}, \cdots, \overline{y_k}$와 a, b와 M으로부터 모든 y_i들을 찾을 수 있다.[12]

I과 II에서 LLL알고리즘을 사용하는 데 이는 다항식 시간 안에 구할 수 있다. I에서는 두 단계로 나누어 a와 b그리고 M을 구하는데 첫 번째 단계는 a를 법M에 대해서 해를 갖는 다항식을 생성한다. 두 번째 단계로는 이러한 다항식들의 수열을 가지고 M의 배수를 찾아내는 알고리즘을 이용한다. 이것은 heuristic하지만 수열의 다항식의 숫자가 늘어날수록 m에 빨리 접근되어 진다. 이렇게 M을 찾은 후에는 a를 찾는다. I에서는 $(n+1)\times(n+1)$크기의 행렬에 LLL 알고리즘을 적용하는데 이때 $n \approx \sqrt{2\log M}$이고 구성성분의 크기는 $B(\log B \approx \sqrt{\frac{\log M}{2}})$보다 크지 않다. II에서는 $k \times k$ 크기의 행렬에 LLL 알고리즘을 적용하는데 이때 $k \approx \frac{\log M}{\log r}$ 이고 $B = (k-1)\log M$이다.

단계 3: 합법적인 사용자 원선이가 서버와 PAK 등과 같은 프로토콜을 이용하여 키를 교환하고 있고 같은 시간에 이브가 이들의 통신을 보고 있다. 이때 이브는 m, μ, k를 얻게 된다.

단계 4: $\{\pi_i\}_{i\in I}$를 패스워드 집합이라고 하자. 이브는 패스워드 π_i를 추측하고 y_0를 초기값으로 한 LCG에 의해서 생성된 난수, y_i를 구한다. $(\frac{m}{H_1^r(A, ID_S, \pi_i)})^{y_i}$를 계산한 후 k가 $H_{2a}(A, ID_S, m, \mu, (\frac{m}{H_1^r(A, ID_S, \pi_i)})^{y_i})$과 같은 지를 비교한다. 이브는 이러한 과정을 가능한 공간 $\{\pi_i\}\times\{y_i\}_{j\in J}$에서 참이 나올 때까지 반복한다. 주어진 공간은 사전적 공격이 가능하다. 이러한 과정은 EKE2에서도 똑같이 확인할 수 있다.

참조. 시스템 S는 EKE2나 PAK 프로토콜에 대해서 위와 같은 공격이 이루어졌는지도 알지 못한다. 왜냐하면 공격자가 유효한 패스워드를 가지고 합법적인 사용자간의 공개된 정보만을 가지고 공격하기 때문이다.

V. 결 론

본 논문에서는 EKE2와 PAK 프로토콜이 위와 같은 공격에 취약할 수 있음을 보였다. 이러한 취약점을 보완하기 위해서 몇 가지 방법들을 제안한다. 첫 번째 방법은 프로토콜을 보완하는 것으로 프로토콜에 전달되어 온 메시지로부터 군에 속하는지를 확인하는 과정을 삽입한다. 예를 들어 PAK의 경우 m으로부터 $H_1(A, B, \pi)$을 이용하여 h를 얻은 후 이것이 생성자 g에 의해서 만들어진 군에 속하는지 여부를 확인한다. 이것이 너무 작은 부분 군에 속한다면 공격이 행해지고 있음을 감지할 수 있다. 두 번째 방법으로는 키 생성 과정에서 $\frac{r}{2} = (\frac{p-1}{2q})$의 가장 작은 인수가 q와 크기가 거의 같은 그러한 소수 p를 선택한다. 또는 안전 소수(safe prime, p=2q+1)를 선택한다. 이러한 경우에는 작은 부분 군 공격(small subgroup confinement)을 막을 수 있다. EKE2와 PAK 프로토콜에 관해서 이러한 키 생성과정에서 소수에 관하여 제한을 두는 것은 이번이 처음인 것으로 알고 있다. 또 다른 방법으로는 난수 발생자로 LCG가 아닌 다른 것을 사용하는 것이다. 그러므로 써 난수를 예측하기 어렵게 한다면 안전할 수 있을 것이다.

최근에 키 교환 또는 분배 프로토콜에서 주요 관

심은 증명이 가능한 안전성을 보여주는 것이다. 증명이 가능한 프로토콜이 아니면 사람들은 그러한 프로토콜을 사용하는 데에 주저하는 듯하다. 위의 두 프로토콜은 이러한 흐름에 부합하여 이상적인 모델을 통하여 안전성을 증명하였다(Bellare,[2] Boyko[5]). 그들은 그들의 가정들 하에서 안전하다고 주장하였으나 새로운 공격자의 능력에 따라 취약함을 보였다. 따라서 이상적인 모델을 통해서 증명함에 있어서도 공격자의 행동을 정의하는 데에 좀더 주의해야 할 것이다.

참 고 문 헌

[1] M. Bellare, R. Canetti, and H. Krawczyk, A Modular approach to the design and analysis of authentication and key exchange protocols, In STOC, pp. 419~428, 1998

[2] M. Bellare, P. Rogaway, Entity authentication and key distribution, In CRYPTO'93, Lecture Notes in Computer Science vol.773, Springer-Verlag, pp.232~249, 1993.

[3] V. Shoup, On formal models for secure key exchange, IBM Research Report RZ3120, 1999, Available at http://epint.iacr.org/1999/012.

[4] M. Bellare, D. Pointcheaval, and P. Rogaway, Authenticated key exchange secure against dictionary attacks, In EUROCRYPT'2000, Lecture Notes in Computer Science vol.1807, Springer-Verlag, pp.139~155, 2000.

[5] V. Boyko, P. MacKenzie and S. Patal, Provably secure password-authenticated key exchange, In EUROCRYPT'2000, Lecture Notes in Computer Science vol. 1807, Spinger-Verlag, pp.156~171, 2000.

[6] S. Halevi and H. Krawczyk, Public-key cryptography and password protocols, No.3, pp.230~268.

[7] S. Lucks, Open key exchange: How to defeat dictionary attacks without encrypting public keys, The Workshop on Security Protocols, April 7~9, 1997.

[8] D. E. Knuth, the art of computer programming Volumn 2, Seminumerical Algorithms, second edition, Addison-Wesley, 1980.

[9] M. Bellare, S. Goldwasser and D. Micciancio, Pseudo-Random Number Generation within Cryptographic Algorithms: the DSS Case., Advances Vol.1294, B. Kaliski ed, Springer-Verlag, 1997.

[10] FIPS 186-2 revised version 2002.

[11] A, Joux and J. Stern, Lattice Reduction: A Toolbox for the Cryptanalyst, Journal of Cryptology, vol.11, no.3, pp.161~185, 1998.

[12] Alan M. Frieze, Johan Hastad, Ravi Kannan, Jeffrey C. Lagarias, and Adi Shamir, Reconstructing truncated integer variables satisfying linear congruences, SIAM Journal on Computing, 17(2), April pp.262~280, 1988.

[13] S. Bellovin and M. Merritt, Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-file compromise, In ACM Conference on Computer and Communications Security, pp.244~250, 1993.

[14] S. Bellovin and M. Merritt, Encrypted key exchange: Password based protocol secure against dictionary attacks, In Proceedings of IEEE Security and Privacy, pp.72~84, 1992.

[15] L. Gong, M. Lomas, R. Needham, and J. Saltzer, Protecting poorly chosen cations, vol.11, no.5, pp. 648~656, June 1993.

[16] IEEE P1363.2, Standard Specifications for Public Key Cryptography: Password-based Techniques, August 2002.

[17] D. Jablon, Strong Password-only authenticated key exchange, ACM Computer Communications Review, vol.26, no.5, pp.5~26, 1996.

[18] T. Kwon, Authentication and key agreement via memorable passwords, In Network and Distributed System Security Symposium, 2001.

[19] A.K. Lenstra, H.W. Lenstra and L.Lovasz, Factoring polynomial with integer coefficients, Mathn. Ann., 261, pp.513~534, 1998.

[20] P. MacKenzie, More Efficient Password-Authenticated Key Exchange, In RSA Conference, Cryptographer's Track, 2001, pp.361~377.

[21] P. MacKenzie, The PAK suites: Protocols for Password-Authenticated Key Exchange, 2002.

[22] P. MacKenzie, S. Patel, and R. Swaminathan, Password-authenticated key exchange based on RSA, Asiacrypt, Springer-Verlag, 2000.

[23] T. Wu, Secure remote password protocol, In Net work and Distributed System Security Symposium, 1998.

〈著者紹介〉

이 희 정 (Hee-Jung Lee) 정회원
1980년 2월 : 이화여자대학교 문리대학 수학과 졸업
1989년 8월 : 펜실베니아 주립대학교(Penn. State Univ.) 이학박사
1994년 3월~현재 : 강남대학교 응용수학 전공 부교수
<관심분야> 정수론, 암호학