情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

RSA-EPAKE의 사전공격에 대한 안전성 분석*

윤 택 영[1†], 박 영 호[2‡], 류 희 수[3]
[1]고려대학교, [2]세종사이버대학교, [3]경인교육대학교

Cryptanalysis of an Efficient RSA-Based Password-Authenticate Key Exchange Protocol against Dictionary Attack*

Taek-Young Youn[1†], Young-Ho Park[2‡], Heuisu Ryu[3]
[1]Korea University, [2]Sejong Cyber University, [3]Gyeongin National University of Education

요 약

최근, Park 등은 RSA의 기반 인증된 키 교환 프로토콜을 제안하고, 제안한 프로토콜의 안전성을 증명했다. 본 논문에서는 Park 등에 의해 제안된 프로토콜을 분석하고, 사전공격에 취약함을 보인다. 또한 제안하는 공격의 성능을 분석함으로써 공격 방법이 Park 등이 제안한 프로토콜에 매우 효율적임을 보인다.

ABSTRACT

Recently, an efficient password-authenticated key exchange protocol based on RSA has been proposed by Park et al. with formal security proof. In this letter, we analyze their protocol, and show that it is not secure against an active adversary who performs a dictionary attack. Moreover, we analyze the performance of the proposed attack and show that the attack is a threatening attack against the protocol.

Keywords : Cryptanalysis, Key Exchange, Password, RSA

Ⅰ. 서 론

패스워드 기반 키 교환 프로토콜 (PAKE)은 두 통신 주체가 사전 공유된 패스워드를 사용하여 안전한 통신을 수행할 수 있게 해주는 암호학적 도구로 Bellovin와 Merritt이 최초로 제안하였다[2]. 이후 많은 PAKE 프로토콜들이 제안되었다[1,3-11].

기존에 제안된 PAKE 프로토콜들은 기반하는 난제에 따라 Diffie-Hellman 키 교환 프로토콜 기반의 프로토콜과 RSA 암호시스템 기반의 프로토콜로 분류할 수 있다. RSA 암호시스템을 기반으로 안전한 PAKE 프로토콜을 설계하는 것이 쉽지 않기 때문에 대부분의 PAKE 프로토콜들은 Diffie-Hellman 키 교환 프로토콜을 기반으로 설계되었으나 RSA 기반의 PAKE 프로토콜(RSA-PAKE)을 안전하게 설계하기 위한 연구가 많이 이루어지고 있다[1,4-11].

일반적으로, RSA-PAKE 프로토콜은 RSA 파라미터를 생성하고 검증하는 단계와 이를 기반으로 키를 교환하는 단계로 구성된다. 첫 번째 단계에서 서버 A는 RSA 공개키 (n,e)와 비밀키 d를 생성하고 공개키를 클라이언트 B에게 전송한다. 그러면 B는 받은 공개키

접수일 : 2008년 9월 22일; 채택일 : 2008년 12월 1일
* "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))
† 주저자, taekyoung@cist.korea.ac.kr
‡ 교신저자, youngho@sjcu.ac.kr

[표 1] RSA-EPAKE 프로토콜의 수행 과정

A		B
1. $n=p\cdot q\in[2^{l-1},2^{l}]$ 2. $r_A\in\{0,1\}^{k_2}$ 3. $e=2H(n,s)+1$: 다음 만족하는 값으로 선택 3.1 e는 s에 대해 k_1비트 소수 3.2 $\gcd(e,\phi(n))=1$ 4. $d=e^{-1}\bmod(\phi(n))$	(id_A,n,s,r_A) ---------->	
		1. $e=2H(n,s)+1$ 2. $r_B\in\{0,1\}^{k_2}$, $r\in Z_n^*$ 3. $\alpha=T(pw,r_A,r_B,id_A,id_B,s,n)$ 4. 다음중 한 개라도 틀리면 프로토콜 종료 4.1 $n\in[2^{l-1},2^{l}]$은 홀수 4.2 $e=2H(n,s)+1$는 k_1 비트의 소수 4.3 $\gcd(\alpha,n)=1$ 5. $\beta=r^{e}\cdot\alpha\bmod(n)$
	(id_B,r_B,β) <----------	
1. $\alpha=T(pw,r_A,r_B,id_A,id_B,s,n)$ 2. $\gcd(\alpha,n)\neq 1$ 이면 프로토콜 중단 3. $r'=(\beta\cdot\alpha^{-1})^{d}\bmod(n)$ 4. $\gamma=H_1(r',r_A,r_B,id_A,id_B,s,n)$	(id_A,γ) ---------->	
		1. $\gamma\neq H_1(r,r_1,r_2,id_A,id_B,s,n)$면 프로토콜 종료 2. $\delta=H_2(r,r_A,r_B,id_A,id_B,s,n)$ 3. $sk=H_3(r,r_A,r_B,id_A,id_B,s,n)$
	(id_B,δ) <----------	
1. $\delta\neq H_2(r',r_A,r_B,id_A,id_B,s,n)$면 프로토콜 중단 2. $sk=H_3(r',r_A,r_B,id_A,id_B,s,n)$		

가 신뢰할 수 있는 것인지 검증한다. B가 받은 공개키를 신뢰할 수 있는 RSA 파라미터라고 판단하면 A와 B는 교환한 RSA 파라미터에 대한 신뢰성과 사전 공유된 패스워드를 기반으로 키 교환을 수행한다.

RSA-PAKE 프로토콜은 PKI (Public-Key Infrastructure)의 존재를 가정하지 않기 때문에 프로토콜에서 사용되는 RSA 파라미터는 인증서 없이 사용된다. 따라서 어떤 공격자는 통신에 사용되는 RSA 파라미터를 자신의 선택에 따라 변경함으로써 RSA-PAKE를 공격하기 위해 사용할 수 있다. 위에 설명된 두 단계 중에서 첫 번째 단계의 목적은 이와 같은 공격 환경에서 신뢰할 수 있는 RSA 파라미터를 공유하는 것이다. RSA-PAKE 프로토콜은 기본적으로 이와 같은 RSA 파라미터 변경 공격에 안전하도록 설계되어야 한다. RSA-PAKE 프로토콜의 설계에서는 RSA 파라미터의 신뢰성을 효율적으로 증명하기 위한 방법을 개발하는 것이 중요한 연구 주제이다.

최근, Park 등은 매 세션에 사용되는 RSA 파라미터의 신뢰성을 효율적으로 검증할 수 있는 RSA 기반의 키 교환 프로토콜(RSA-EPAKE)을 제안하고 키 교환 프로토콜에 대한 안전성 기준에 준하여 제안하는 프로토콜의 안전성을 증명하였다[7]. 본 논문에서는 RSA-EPAKE의 안전성을 분석하여 능동적인 공격자가 수행하는 오프라인 사전공격에 취약함을 보이고 제안하는 공격의 성능을 분석하여 매우 효율적으로 패스워드를 찾을 수 있음을 보인다.

Ⅱ. Park 등의 RSA-EPAKE

본 장에서는 RSA-EPAKE의 구성을 살펴본다. 두 통신주체 A와 B는 패스워드 pw를 사전에 공유한 것으로 가정하고 논의를 진행한다. id_A와 id_B는 각각A와 B의 아이디어라도 하자. RSA-EPAKE가 사용하는 함수는 다음과 같다. 보안 변수 k_1, k_2에 대하여 다음의 해쉬 함수를 정의 한다: $H:\{0,1\}^{*}\rightarrow\{0,1\}^{k_1-1}$, $T:\{0,1\}^{*}\rightarrow Z_n$, $H_1,H_2,H_3:0,1^{*}\rightarrow 0,1^{k_2}$. $l=|n|$ 이다. 1024 비트 RSA를 사용하는 경우 $k_1=96$, $k_2=160$, $l=1024$를 사용한다. ([7]를 참고하라.) RSA-EPAKE 프로토콜은 다음과 같이 수행된다.

Step 1. A는 $r_A \in \{0,1\}^{k_2}$, l비트 RSA 모듈로 n를 선택하고 관계식 $\gcd(e,\phi(n))=1$ 를 만족하는 k_1비트 $e=2H(n,s)+1$가 소수가 되기 위한 난수 s를 선택하여 공개지수 e와 $d=e^{-1}\bmod(\phi(n))$를 계산한다. A는 B에게 (id_A,n,s,r_A) 를 전송한다.

Step 2. B는 난수 r_B를 $\{0,1\}^{k_2}$에서 선택하고 $\alpha=T(pw,r_A,r_B,id_A,id_B,s,n)$를 계산한다. B는 다음을 확인 한다: $n\in[2^{l-1},2^l]$은 홀수; $e=2H(n,s)+1$는 k_1 비트의 소수; $\gcd(\alpha,n)=1$. 만약 한 개의 조건이라도 만족하지 않는 것이 있으면 B은 프로토콜을 중단한다. 그렇지 않으면 B는 $r\in Z_n^*$로 $\beta=r^e\cdot\alpha\bmod(n)$를 계산하고 (id_B,r_B,β)를 A에게 전송한다.

Step 3. A는 $\alpha=T(pw,r_A,r_B,id_A,id_B,s,n)$를 계산한다. 계산된 α가 $\gcd(\alpha,n)\neq1$를 만족하면 A는 프로토콜을 중단한다. 반대로 $\gcd(\alpha,n)=1$를 만족하면 A는 $r'=(\beta\cdot\alpha^{-1})^d\bmod(n)$와 $\gamma=H_1(r',r_A,r_B,id_A,id_B,s,n)$를 계산하고 (id_A,γ)를 B에게 전송한다.

Step 4. B는 $\gamma=H_1(r,r_1,r_2,id_A,id_B,s,n)$를 확인하고 만족하지 않으면 프로토콜을 중단한다. 위 조건이 만족하면 B는 $\delta=H_2(r,r_A,r_B,id_A,id_B,s,n)$를 계산하고 세션키를 $sk=H_3(r,r_A,r_B,id_A,id_B,s,n)$로 계산한다. B는 (id_B,δ)를 A에게 전송한다..

Step 5. A는 $\delta=H_2(r',r_A,r_B,id_A,id_B,s,n)$를 확인하고 만족하지 않으면 프로토콜을 중단한다. 위 조건이 만족하면 A는 세션키를 $sk=H_3(r',r_A,r_B,id_A,id_B,s,n)$로 계산한다.

Ⅲ. RSA-EPAKE에 대한 분석

본 장에서는 RSA-EPAKE의 안전성을 분석 한다.공격 방법을 설명함에 있어 공격자는 RSA 서버(A)를 가장하여 정당한 사용자 B의 패스워드를 찾아내는 경우로 기술한다.

1. 공격 시나리오

Step 1. 공격자 E는 $r_E\in0,1^{k_2}$와 l비트의 RSA 모듈 n을 선택한다. n은 큰 소수 p, q에 대해 $n=3pq$로 표현되는 값으로 선택된다. E는 $e=2H(n,s)+1$이 k_1비트의 소수이고 $\gcd(e,\phi(n))=1$를 만족하는 s를 찾는다. E는 (id_A,n,s,r_E)를 정당한 사용자 B에게 전송한다.

Step 2. B는 정상적인 키 교환 과정에서의 Step 2와 동일하게 프로토콜을 진행한다. B는 난수 r_B를 $\{0,1\}^{k_2}$에서 선택하고 $\alpha=T(pw,r_A,r_B,id_A,id_B,s,n)$를 계산한다. B는 다음 조건들을 확인 한다:

1. $n\in[2^{l-1},2^l]$은 홀수,
2. $e=2H(n,s)+1$는 k_1 비트의 소수,
3. $\gcd(\alpha,n)=1$.

만약 한 개의 조건이라도 만족하지 않는 것이 있으면 B은 프로토콜을 중단한다. 그렇지 않으면 B는 $r\in Z_n^*$를 선택하여 $\beta=r^e\cdot\alpha\bmod(n)$를 계산하고 (id_B,r_B,β)를 A에게 전송한다.

E는 n을 홀수로 선택하고 e를 k_1 비트의 소수로 계산되게 하는 s를 선택하였기 때문에 B가 프로토콜을 중단하는 경우 $\gcd(\alpha,n)\neq1$임을 알 수 있다. B가 프로토콜을 중단하지 않는 경우 이후 공격이 진행될 수 있다.

Step 3. B가 프로토콜을 중단하지 않으면 E는 B가 A에게 전송한 통신 데이터 (id_B,r_B,β)를 가로채고 수집된 정보를 기반으로 오프라인 패스워드 사전공격을 수행한다. 공격방법을 설명하기에 앞서 다음의 사실을 확인하자. B는 $\gcd(\alpha,n)\neq1$인 경우에만 프로토콜을 중단하기 때문에 프로토콜이 중단되지 않았다는 사실을 통해서 E는 올바른 패스워드로 생성한 α가 $\gcd(\alpha,n)=1$를 만족한다는 것을 알 수 있다. E는 이와 같은 사실에 기반 하여 오프라인 패스워드 사전공격을 수행할 수 있다. 우선, $r_E, r_B, id_A, id_B, s,\ n$ 는 E가 획득할 수 있는 정보이다. E는 추측한 패스워드 pw'에 대해 $\alpha'=T(pw',r_A,r_B,id_A,id_B,s,n)$를 계산한다. 올바른 패스워드는 $\gcd(\alpha,n)=1$를 만족하기 때문에 $\gcd(\alpha',n)\neq1$인 α'가 생성되는 패스워드 pw'는 올바르지 않은 것임을 확인할 수 있다. 이와 같은 과정을 반복함으로써 전체 패스워드 중에서 확실하게 사용자의 패스워드가 아닌 것을 걸러낼 수 있다.

n은 3을 인수로 갖고 있기 때문에 $\gcd(\alpha',n)\neq1$인 α'는 1/3의 확률로 발생하고 1/3의 패스워드가 해당 조건을 만족하는 α'를 생성한다. 결과적으로 한 번의 공격 시도를 통해 올바른 패스워드일 가능성이 있는 패스워

드의 집합은 2/3로 줄어든다. 공격시도는 1/3의 확률로 검출되므로 E는 2/3의 확률로 공격을 성공할 수 있으며, 각 공격의 성공으로 인해 올바른 패스워드일 가능성이 있는 패스워드의 집합을 2/3로 줄일 수 있다.

2. 제안하는 공격의 효율성 분석

D를 패스워드의 집합이라고 하고 trial을 어떤 공격 알고리즘 E이 공격을 시도하는 사건으로 정의하자. successful trial을 위 알고리즘 E가 수행한 공격이 성공하고 올바른 통신 참여자 B가 공격을 위해 삽입된 RSA 모듈 n이 3을 인수로 갖는 것을 인지하지 못하는 사건으로 정의한다. n이 3을 인수로 갖지 않는 다는 것은 $\gcd(\alpha, n) \neq 1$임을 의미한다. 각 successful trial의 수행으로 패스워드의 후보군은 전체 후보군의 2/3 크기로 감소한다. 즉, 1/3 패스워드들은 올바른 패스워드가 아닌 것으로 판단되어 제거된다. 따라서 m회의 successful trial을 수행하면 패스워드 후보군의 크기가 $(2/3)^m \|D\|$로 줄어들게 된다. $\|D\| = 2^{80}$라고 가정하자. $m \approx 136.76$에 대해 $(2/3)^m \|D\| = 1$가 만족하므로 올바른 패스워드를 유일하게 결정하기 위해 대략 137회의 successful trial이 수행되어야 한다. t회의 trial에서 $2/3t$회의 successful trial이 발생하므로 137회의 successful trial을 획득하기 위해 대략 $205.5 \approx 137 \times 3/2$회의 trial이 필요하다. 결과적으로 대략 206회의 trial을 통해 올바른 패스워드를 결정할 수 있다.

n을 구성하는 작은 소수를 3으로 한정하는 경우 주어진 n이 3의 배수인지 확인함으로써 상기 공격을 쉽게 막을 수 있다. 하지만, 적당히 큰 임의의 소수 x를 사용하여 $n = xpq$을 구성하면 보다 현실적인 공격을 수행할 수 있다.

Ⅳ. 결 론

본 논문에서는 Park 등에 의해 제안된 패스워드 기반 인증된 키 교환 프로토콜을 분석하여 오프라인 사전공격을 수행하는 능동적 공격자에게 안전하지 않음을 보였다. 제안한 공격방법으로 RSA-EPAKE를 분석하면 206회의 온라인 공격을 시도함으로써 올바른 패스워드를 결정할 수 있다. 온라인 공격은 실패 회수를 제한함으로써 쉽게 막을 수 있으나 본 논문에서 제안한 공격방법은 일회의 온라인 공격을 통해 다수의 패스워드 후보를 제거할 수 있기 때문에 공격자가 많은 정보를 획득할 수 있고 이에 따라 RSA-EPAKE 프로토콜은 Park 등이 주장한 안전성을 제공하지 못한다.

참고문헌

[1] F. Bao, “Security Analysis of a Password Authenticated Key Exchange Protocol”, in Proc. of ISC 2003, LNCS 2851, pp. 208-217, Springer-Verlag, 2003.

[2] S. M. Bellovin, M. Merritt, “Encrypted key exchange: password-based protocols secure against dictinary attacks”, In Proc. of 1992 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society, pp. 72-84, 1992.

[3] M. Bellare, D. Pointcheval, and P. Rogaway, “Authenticated key exchange secure against dictionary attack”, in Proc. of Eurocrypt 2000, LNCS 1807, pp. 139-155. Springer-Verlag, 2000.

[4] D. Catalano, D. Pointcheval, and T. Pornin, “Trapdoor Hard-to-Invert Group Isomorphisms and Their Application to Password-based Authentication”, Journal of Cryptology, Vol.20, Number 1, pp. 115.149, Springer-Verlag, 2007.

[5] P. MacKenzie, S. Patel, and R. Swaminathan, “Password-Authenticated Key Exchange Based on RSA”, in Proc. of ASIACRYPT 2000, LNCS 1976, pp. 599-613, Springer-Verlag, 2000.

[6] S. Patel, “Number Theoretic Attacks on Secure Password Schemes”, in Proc. of IEEE Symposium on Security and Privacy, pp. 236-247, IEEE Computer Society, 1997.

[7] S. Park, J. Nam, S. Kim, D. Won, “Efficient Password-Authenticated Key Exchange Based on RSA”, in Proc. of CT-RSA 2007, Springer-Verlag, LNCS 4377, pp. 309-323, Springer-Verlag, 2007.

[8] D. S. Wong, A. H. Chan, and F. Zhu, “More

Efficient Password Authenticated Key Exchange Based on RSA", in Proc. of INDOCRYPT 2003, LNCS 2904, pp. 375-387. Springer-Verlag, 2003.

[9] M. Zhang, "Further Analysis of Password Authenticated Key Exchange Protocol based on RSA for Imbalanced Wireless Networks", in Proc. of ISC 2004, LNCS 3225, pp. 13-24. Springer-Verlag, 2004.

[10] M. Zhang, "New Approaches to Password Authenticated Key Exchange based on RSA", in Proc. of ASIACRYPT 2004, LNCS 3329, pp. 230-244. Springer-Verlag, 2004.

[11] F. Zhu, D. S. Wong, A. H. Chan, and R. Ye, "Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks", in Proc. of ISC 2002, LNCS 2433, pp. 150-161. Springer-Verlag, 2002.

<著 者 紹 介>

윤 택 영 (Taek-Young Youn) 학생회원
2003년 2월 : 고려대학교 수학과 이학학사
2005년 2월 : 고려대학교 정보보호대학원 정보보호학과 공학석사
2005년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정
<관심분야> 암호 이론, 정보보호 이론, 암호 프로토콜, 부채널 공격

박 영 호 (Young-Ho Park) 정회원
1990년 2월 : 고려대학교 수학과 이학사
1993년 2월 : 고려대학교 수학과 이학석사
1997년 2월 : 고려대학교 수학과 이학박사
2002년 3월~현재 : 세종 사이버 대학교 부교수
<관심분야> 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격

류 희 수 (Heuisu Ryu) 정회원
1989년 2월 : 고려대학교 수학과 이학사
1992년 2월 : 고려대학교 수학과 이학석사
1999년 5월 : 미국 Johns Hopkins 수학과 Ph.D
2002년 9월~현재 : 경인교육대학교 수학교육과 조교수
<관심분야> 암호이론 및 알고리즘, 정보보호교육, 정수론, 수학교육