신원 기반 암호화 방식의 개선된 안전한 키 발급 기법

권세란° 이상호
이화여자대학교 컴퓨터학과
sranie@ewhain.net° shlee@ewha.ac.kr

Improved Secure Key Issuing in ID-based Cryptography

Saeran Kwon° Sang-Ho Lee
Department of Computer Science and Engineering , Ewha Womans University

요 약

신원(ID) 기반 암호시스템은 인증서 관리의 복잡함이 없는 좋은 장점이 있는 반면, KGC(Key Generator Center)가 사용자의 비밀 키를 발행해 주기 때문에 안전하게 개인키를 사용자에게 전송해야 하는 문제와 KGC가 모든 사용자의 비밀 키 값을 얻을 수 있는 키 복구(key escrow) 문제가 나타난다. 이 성질을 제한하기 위해 제안된 여러 기법 중 가장 널리 사용되는 것으로는 다수의 KGC들이 threshold 기법을 이용하여 사용자의 개인키를 발행해 주는 방법이 있으나, 이것은 모든 KGC들이 개인의 신원을 각각 확인해야 되는 비효율성이 있다. AISW'04에서 Lee등은, 하나의 KGC에서 요청자의 신원을 확인하며 다른 신뢰기관들은 개인키 보안을 협조해 주는 방식으로 개인키를 발행하고 발행한 개인키는 은닉방법에 의해 안전하게 전송할 수 있는 장점을 가진 키 발급 기법을 제안하였다. 그러나 그들의 방법은 키 복구 권한 제한 부분이 취약하며 또한 서비스 거부 공격에 안전하지 못한 단점을 갖고 있는데 본 논문에서는 이러한 취약성을 분석하며 이를 보완하여 키 복구 권한을 제한하면서 동시에 서비스 거부 공격에도 안전한 개선된 키 발행 기법을 제안한다.

1. 서 론

기존의 공개키 기반 암호 시스템에서 나타나는 인증서 발행 및 관리 문제를 단순화시킬 수 있는 ID기반 암호 시스템에 대한 개념은 Shamir[7]에 의해 처음으로 소개되었고, 이 개념을 실용적인 ID-기반의 암호 스킴으로 보여준 것은 Boneh와 Franklin[2]이었다. 그들이 제안한 스킴은 사용자의 공개키는 이름이나 E-mail 주소 혹은 IP 주소 등 공개된 정보에서 직접 얻으며, 개인키는 신뢰 기관 KGC가 발행하도록 하는 공개키 시스템이다. 그것은 인증서나 그에 따라 발생하는 인증서 관리의 어려움이 제거된 효율적 시스템이지만 KGC가 모든 사용자의 개인키를 알 수 있어 Key escrow 문제가 발생하게 되므로, 구조적으로 KGC에 대해 절대적인 신뢰를 부여해야 하는 단점이 있다. 또한 구체적으로 명시하지는 않았지만 개인키를 발급 할 경우 요청자에 대한 인증 방법 및 안전하게 개인키를 전달하는 방법 등 구현에서 고려되어져야 하는 많은 사항들도 해결되어야 된다.

이런 Key escrow 문제를 해결하기 위해 다양한 기법들이 제안되었는데, 일반적으로 가장 널리 사용되는 방법은 한 KGC가 갖고 있는 마스터키(master key)의 역할을 다수의 KGC들에게 분산하는 방법이다(Boneh와 Franklin[2], Chen et al.[3], Hess[4]). 하지만 그와 같은 기법은 한 사용자의 개인키를 발행하기 위해서는 분산된 마스터키의 share를 갖고 있는 모든 KGC들이 독립적으로 각각 요청자의 신원을 확인해서 개인키를 발행하는 부담이 있다. Lee 등[5]은 이런 부담을 줄이기 위해, 사용자의 개인키는 한군데의 KGC에서 발행하며 그것의 비밀성은 다수의 KPA(Key Privacy Authority)들에게서 보호받도록 하는 프로토콜을 제안하였다. 이 기법의 장점은 KGC만이 요청자의 신원을 확인하여 개인키를 발행하므로 신원확인 부담이 적으며 또 발행된 개인키를 blind 기법을 써서 안전하게 전송할 수 있다. 하지만 그들이 키 보호를 위해 제안한 기법 즉 KPA들이 사용자들의 blind된 비밀키에 그들의 마스터키를 스칼라 곱하여 blind 시킨 후 사용자에게 반환해 주는 방식으로는 의도를 가진 KGC의 키복구 권한을 제한하지 못하는 약점이 노출되며 또한 적극적인 공격자들의 서비스 거부(denial-of-service) 공격에도 취약한 단점이 보여 진다.

본 논문에서는 이 기법의 이러한 취약성을 구체적인 공격의 예를 보이면서 분석하며 또한 취약적인 부분을 제거하여 KGC의 key escrow에 대한 제한성을 가지면서 서비스 거부공격에 견딜 수 있는 개선된 키 발급 기법을 제안한다.

논문의 구성은 2장에서 Lee 등의 기법[5] 소개 및 그것에 대한 공격을 구체적으로 기술한다. 3장에서 취약성이 보완된 개선된 방법을 제안한다. 4장에서 결론을 기술한다.

2. 기존 키 발급 방법(Lee[5])소개와 공격법 분석

2.1 기존 키 발급 방법 소개

1단계. 시스템 설정

KGC는 두개의 군 G_1, G_2와 그들 사이의 bilinear map $e: G_1 \times G_1 \rightarrow G_2$ 및 G_1 상의 위수가 소수 q인 임의의 점 P를 명시한다. 또한 세 개의 해쉬함수 $H_1 : \{0,1\}^* \rightarrow G_1$ 와 $H_2 : G_2 \rightarrow \{0,1\}^l$ (l은 평문 블록 길이) 그리고 $H_3 : G_2 \rightarrow Z_q^*$ 를 선택 명시하며 마지막으로 마스터키 $s_0 \in Z_q^*$를 선택한 후 KGC의 공개키 $P_0 = s_0 P$를 명시한다.

2단계. KPA들에 의한 시스템 공개키 설정

n개의 KPA들은 분산된 방식으로 각자 그들의 마스터 키 s_i를 택하여 비밀로 간직하고 공개키 $P_i = s_i P$ $(i = 1, \cdots, n)$를 공개한다. KPA들은 연속적으로 협동하는 방식으로 $Y = s_0 s_1 \cdots s_n P$를 계산하여 사용자 그룹에게 시스템 공개키로 Y 를 공개한다.

3단계. KGC가 주도하는 사용자 키 발행

사용자는 은닉값 x를 선택하여 은닉요소값(blinding factor) $X = xP$를 계산한 후 KGC에게 그의 신원 값 ID와 은닉요소 X를 함께 보내면서 개인키를 발행해 주기를 요청한다. KGC는 먼저 사용자의 신원이 ID인지를 확인하고 공개키 $Q_{ID} = H_1(ID, KGC, KPA_1, \cdots, KPA_n)$를 계산한다. 다음에, 자신의 마스터키로 만든 사용자의 부분 비밀키를 blind시켜 $Q_0' = H_3(e(s_0 X, P_0))s_0 Q_{ID}$ 를 계산한다. 동시에 Q_0'에 대한 자신의 서명 $Sig_0(Q_0') = s_0 Q_0'$을 계산하여 함께 사용자에게 보낸다.

4단계. KPA들이 주도하는 사용자 키 발행

사용자는 $i = 1$ 부터 n 까지 해당되는 KPA_i들에게 연속적인 방법으로 ID, X, Q_{i-1}'과 Q_{i-1}'에 대한 전단계 신뢰기관의 서명 $Sig_{i-1}(Q_{i-1}')$을 함께 보낸다. 각 KPA_i들은 $e(Sig_{i-1}(Q_{i-1}'), P) = e(Q_{i-1}', P_{i-1})$을 확인하여 서명의 올바름을 검증하고, 검증된 경우엔 자신의 마스터키로 $Q_i' = H_3(e(s_i X, P_i))s_i Q_{i-1}'$와 이것에 대한 서명 $Sig_i(Q_i') = s_i Q_i'$ 을 계산하여 함께 사용자에게 보낸다. 사용자가 마지막 신뢰기관 KPA_n을 거치면 $Q_n' = H_3(e(s_n X, P_n))s_n Q_{n-1}'$을 얻게 된다.

5단계. 키 회수

사용자는 아래 방법으로 Q_n'에서 은닉 값을 제거한 후 그의 개인키 D_{ID}를 회수한다.

$$D_{ID} = \frac{Q_n'}{H_3(e(P_0, P_0)^x) \cdots H_3(e(P_n, P_n)^x)} = s_0 s_1 \cdots s_n Q_{ID}$$

2.2 공격법 분석

위의 키 발급 방법은 공격자가 사용자의 은닉값 x 나 신뢰기관들의 마스터키 s_i를 모르기 때문에 BDHP(Bilinear Diffie-Hellman Problem)문제의 어려움을 가정한다면, 통신채널을 통해 전송메시지를 가로채거나 중간에 사용자를 위장하여 절차과정에 개입한다 할지라고 의도한 사용자의 개인키를 복구할 수 없다. 하지만 KGC가 사용자의 개인키를 얻고자 할 경우엔 KGC의 key escrow 성질을 제한할 장치가 없다.

공격을 구체적으로 기술하면 위 과정의 4번째 단계에서, KGC가 자신이 선택한 은닉값 z을 가지고 은닉요소값 $Z = zP$를 새로 만들어 이전에 사용자 ID에게 보내준 $Q_0' = H_3(e(s_0 X, P_0))s_0 Q_{ID}$와 서명 $Sig_0(Q_0')$을 함께 KPA_1에게 보내면 KPA_1은 사용자의 신원 확인이나 은닉요소 값에 대한 확인 없이 서명 검증 계산 $e(Sig_0(Q_0'), P) = e(Q_0', P_0)$만을 확인하기 때문에 이것을 사용자의 제대로 된 요청으로 받아들여, key 발행을 해주게 된다. 이와 같은 방법으로 KGC가 마지막 신뢰기관 KPA_n까지 키보안 제공 요청을 수행하면 KGC는 $Q_n' = H_3(e(s_0 X, P_0))H_3(e(s_1 Z, P_1) \cdots H_3(e(s_n Z, P_n)) \cdot s_0 s_1 \cdots s_n Q_{ID}$ 를 얻을수있다. 키회수단계에서 KGC는 은닉값 z 와 자신의 마스터키 s_0 를 가지고 아래와 같은 방법으로 사용자의 개인키를 복구할 수 있다.

$$D_{ID} = \frac{Q_n'}{H_3(e(s_0 X, P_0))H_3(e(P_1, P_1)^z) \cdots H_3(e(P_n, P_n)^z)} = s_0 s_1 \cdots s_n Q_{ID}$$

다음으로 위의 프로토콜은 DoS(denial-of-service) 공격에 취약함을 볼 수 있다. 4단계에서 KPA_i들에 의해 행해지는 키 보안 서비스과정을 살펴보면 사실 KPA_i에 의해 작성되는 서명은 전송 채널에 접근할 수 있는 어떤 공격자라도 위조 할 수 있다. 그러므로 KPA_i에 의한 서비스를 방해하고자 하는 악의의 공격자는 의미없는 키 발행 요구를 무수히 요청하여 정당한 사용자에 대한 키 발행을 무기력화시킬 수 있다. 유추 가능한 위협(threat)을 살펴보면 공격자가 임의의 위조값 a을 선택하여 위조 키발행 요구값 $Q'' = aP$을 계산한다. 이때 공격자는 a값을 알고 있으므로 아래처럼 Q''에 대한 KPA_{i-1}의 서명 $Sig_{i-1}(Q'')$을 위조할 수 있다. 즉 $Sig_{i-1}(Q'') = s_{i-1} Q'' = s_{i-1} aP = aP_{i-1}$을 계산할 수

있다. 위 프로토콜의 4단계 과정에서는 전단계 KPA_{i-1}이 요구 메시지 에 행한 서명만 검증하므로 $e(Sig_{i-1}(Q''), P) = e(Q'', P_{i-1})$이 성립하면 요청을 받은 KPA_i는 불필요한 키발행을 수행해 주게 되어 정당한 요청자에 대한 서비스를 저해하게 된다.

3. 개선된 안전한 키 발급 기법

제안되는 키 발급기법은 기존 키 발급기법의 취약성을 보완하기 위해 KPSI-List(Key Privacy Service Issue List)를 스킴에 첨가하며 또한 gap Diffie-Hellman(GDH) 군[6]을 사용한 Boneh, Lynn, Shacham[1]에 의해 제안된 short signature scheme을 서명 스킴으로 사용한다. 시스템 변수 및 구성은 기존과 마찬가지로 사용한다. 아래에서 단계별로 제안된 절차를 살펴본다.

KGC가 주도하는 사용자 키 발행단계
사용자의 공개키에 키의 유효기간을 표시하는 T를 첨가하여 기존키가 손상되거나 KGC가 더 이상 사용자를 인증하지 않을 경우 키 폐기(key revocation)를 용이하도록 한다. 또한 사용자가 제출한 은닉요소값(blinding factor) $X = xP$를 $Q_0' = H_3(e(s_0X, P_0))s_0Q_{ID}$에 대한 KGC의 서명단계에 포함시켜 공격자가 임의로 blinding factor를 변경할 수 없도록 하며, 또한 기존의 방식에서 나타난 신뢰기관에 대한 용이한 서명 위조를 어렵게 하기 위해 Q_0'에 직접 마스터키를 스칼라곱 하지 않고 해쉬를 시켜 나온 함수값에 스칼라곱을 한다. 이 방법은 이미 안전성이 증명된 short signature 기법[1]을 적용한 것으로 식으로 표현하면 KGC의 Q_0'에 대한 서명은 $Sig_0(Q_0') = s_0H_1(ID, X, T, Q_0')$로 계산해 준다. KGC는 요청한 사용자 ID에게 T, Q_0' 와 $Sig_0(Q_0')$를 발급해 준다.

KPA들이 주도하는 사용자 키 발행단계
KPA들은 사용자의 키 보안 요청이 오면 우선 사용자 ID와 은닉요소 $X = xP$ 그리고 유효기간 T를 KPSI-List에 기록한다. 이것의 이점은 만약 KGC가 사용자 ID의 개인키를 복구하려는 의도로 자신이 선택한 blinding factor Z와 그것을 포함시켜 만든 서명을 KPA에게 제출하면 비록 서명 검증을 위한 연산식 $e(Sig_0(Q_0'), P) = e(H_1(ID, Z, T, Q_0'), P_0)$이 만족된다 하더라도 다른 blinding factor를 가진2개의 유효한 요구 기록이 KPSI-List에 기록되게 되므로 이와 같은 시도는 확인될 수 있어 KGC에 의한 key-escrow를 제한하는 효과가 된다. 더 약한 공격으로 KGC가 blinding factor만 바꾸어 서비스를 요청할 경우는 서명검증 연산식이 성립하지 않으므로 KPA는 당연히 서비스를 거부하게 된다.

이 단계에서도 KPA_i의 사용자에게 전송될 메시지 Q_i'에 대한 서명기법은 개선된 방식을 적용한다. 즉, Q_i'의 서명은 $Sig_i(Q_i') = s_iH_1(ID, X, T, Q_i')$로 계산한다.
이런 서명 기법을 적용하면 기존의 방식에서 가능했던 공격자들의 KPA_i들에 대한 서명 위조가 어려워지므로 공격자들이 DoS 공격을 하기 어려워진다.

4. 결론

본 논문에서는 Lee등[5]이 제안한 'ID 기반 암호 시스템에서 안전한 키 발행 프로토콜'이 KGC의 키 복구 권한 제한 부분이 취약하며 서비스 거부 공격을 받을 수 단점을 갖고 있음을 분석하여, 이를 보완하기 위해 KPSI-list 등을 스킴에 첨가하고 안전한 서명 기법을 적용한 개선된 방식의 키 발행 프로토콜을 제안하였다.

참고문헌

[1] Boneh, D., Lynn, A. and Shacham, H., "Short signatures from the Weil pairing", Advances in Cryptology-Asiacrypt'01, LNCS 2248, pp514-532 (2001)
[2] Boneh, D. and Franklin, M., "Identity Based Encryption from the Weil Pairing", Advances in Cryptology-Crypto'01, LNCS 2139, pp213-229 (2001)
[3] Chen, L., Harrison, K., Smart, N.P. and Soldera, D.,"Applications of Multiple trust authorities in Pairing based Cryptosystems", Proc. of InfraSec'02, LNCS 2437, pp260-275 (2002)
[4] Hess, F., "Efficient Identity based Signature Schemes based on Pairings", Proc. of SAC'02, LNCS 2595, pp310-324 (2003)
[5] Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J. and Yoo, S., "Secure Key Issuing in ID-based Cryptography", Proc. of AISW'04, vol. 32, pp69-74 (2004)
[6] Okamoto, T. and Pointcheval, D., " The gap-problems: a new class of problems for the security of cryptographic schemes", Proc. of PKC'01, LNCS 1992, pp104-118 (2001)
[7] Shamir, A., "Identity Based Cryptosystems and Signature Schemes", Advances in Cryptology-Crypto '84, LNCS 0196, pp47-53 (1984)