허가된 범위 외의 도청을 방지하는 암호 통신 복호화 키 제공 방식

한규석, 윤찬엽, 김광조*

*한국정보통신대학교 공학부

Design of Lawful Interception Architecture Using ID-Based Cryptosystem

Kyusuk Han, Chan Yeob Yeun, Kwangjo Kim*

*Engineering School, Information and Communications University.

요 약

국가의 안보 및 범죄 수사를 위해 법원의 허가를 받은 감청 기관의 요청에 따라 통신 사업자가 통신 내용을 전달하는 경우, 통신 사업자가 제공한 암호 통신에 대한 복호화 방법 역시 제공해야 할 경우가 있다. 가입자 간의 암호 통신에 사용되는 키 교환에 대해 ID 기반 암호 기법은 가입자 간의 공개키 인증에 대한 절차를 생략할 수 있으며, 키 공탁이 가능하여 공개키 발급 기관의 공개키 쌍의 생성이 용이하다는 특징을 갖고 있다. 그러나 역으로 감청 기관에게 전달된 마스터키를 통해 도메인 전체에 대한 도청 역시 가능하다는 문제점이 있다. 따라서 본 논문은 ID 기반 암호 시스템의 키 공탁 특성을 이용하면서, 마스터키를 획득한 감청 기관의 도청을 방지할 수 있는 기술적 방안을 제시한다.

I. 서론

국가 안보나 범죄 수사를 위해 통신 감청의 필요성이 있으며, 법률에 의해 우편물의 검열, 전기 통신의 감청 또는 통신 사실 확인 자료 제공, 공개되지 않은 타인 간의 대화를 녹음 또는 청취할 수 있도록 하고 있다. 암호 통신의 경우 통신 사업자는 암호 통신에 사용된 통신 사업자가 제공한 암호 기법의 복호화 방안을 제공할 필요가 있다는 것에 대해 여러 국가의 감청 관련법이나 3GPP 등의 기술 요구 사항에서 명시하고 있다[5].

통신 사업자는 감청 요청에 대응하여 가입자가 사용하는 대칭키나 가입자의 공개키 쌍을 감청 기관에 제공할 수 있으며, 대칭키를 제공하는 것은 세션의 변경 시마다 공유되는 키를 생성하여 제공해야 하므로 복잡한 키 관리가 요구되며, PKI 기반의 공개키 쌍을 제공하는 것은 감청 이후 공개키 쌍을 갱신하지 않는 경우 감청 기관에 의한 도청 가능성이 존재하는 문제점이 있다.

ID 기반 공개키 쌍을 제공하는 경우, ID 기반 암호 기법의 키 공탁 특성을 바탕으로 감청 기관에 마스터키를 제공함으로써, 용이한 감청이 가능하지만, 감청 허용 범위 이상의 도청이 가능하며, 감청 권한이 말소된 경우, 도청 방지를 위해 마스터키와 전체 공개키 쌍을 갱신해야 하는 문제점이 있다.

따라서 본 논문은 ID 기반 암호 기법을 기반으로 하고 있으며, 허용 범위 외의 도청을 방지하고, 감청 종료 후 마스터키의 갱신이 불필요한 ID 기반 공개키 쌍 제공 방안을 기술하고 있다.

본 논문의 구성은 다음과 같다. 2장에서 감청 기술에 대한 동향을 기술하며, 3장에서 본 논문에서 제안된 방식을 설명하고 있다. 4장에서 기존 방식과의 비교를 하며, 5장에서는 본 논문의 결론을 기술한다.

II. 관련 연구

2.1 감청 기술 동향

ETSI는 ETSI TR 101 331 [1], ES 201 158 [2], ETSI ETR 330 [3], TS 101 671 [4]등에서 감청 요구 사항 및 구조에 대해 규정하고 있다. 대부분의 국가는 ETSI에 의해 개발된 감청 표준을 도입하고 있다.

미국의 경우는 Communications Assistance for Law Enforcement Act (CALEA) 에 의해 감청 요구 사항 및 방법을 관리하고 있다. 3GPP는 TS 33.106 [5], TS 33.107 [6], TS 33.108 [7]에서 감청 구조 및 방법에 대해 명세하고 있다. 3GPP는 ETSI와 ANSI의 표준을 반영하고 있다.

2.1 키 공탁 기술 동향

공탁 기관의 능력을 제한하는 접근 방식으로, Micali [8]는 Secret sharing을 이용한 기법을 제안하였고, Shamir [9]는 부분적인 키 공탁 (Partial Key Escrow)을 통해 키 재구성을 위한 어느 정도의 시간 소모를 요구함으로써, 부정한 기관이 저장된 키에 대한 갑작스럽거나 대규모 악용을 방지하는 기법을 제안하였다.

감청 기관의 부정행위를 방지하는 접근 방식으로, 영장 제한 (Warrant bound)이 있는 공탁 기법 [10]이 있으며, Fraud Detectability [11]와 Compliance Certification [12]은 감청 기관이 자신과 암호 통신 수신자가 같은 복호화 값을 갖는 것을 확신시키는 방식이다. Abe와 Kanda [13]는 키 공탁 기술에 대한 요구 사항을 정리하였으며, 감청 시간을 제한할 수 있는 단방향 통신에 대한 PKI 기반의 키 공탁 기법을 제안하였다.

III. 제안 방식

3.1 참여 개체 및 구조

제안하는 ID 기반 암호 통신 감청 구조는 다음의 그림 1와 같다.

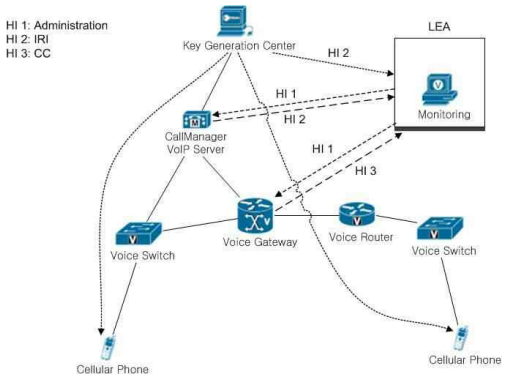

그림 1 암호 통신 감청을 위한 제안 구조

감청에 대해서 다음의 참여자가 있다고 가정한다.

- 감청 기관 (Law Enforcement Agency, LEA)

감청 기관은 법률에 근거하여 통신 내용의 수집을 요청하여 통신 내용을 전달받는 인가된 기관이다.

- 통신 서비스 제공자 (Mobile Operator, MO)

통신 서비스 제공자는 가입자에게 암호 통신을 포함하는 이동 통신 서비스를 제공하며, 감청 기관의 요청에 의해 암호 기법 및 암호 통신 내용을 제공하는 개체를 말한다.

- 신뢰된 키 관리 기관 (Key Generation Center, KGC)

통신 서비스 제공자 및 가입자, 감청 기관 등에게 암호화에 사용되는 키를 발급하는 기관이며, 감청 기관의 요청에 의해 가입자의 키를 제공하는 기관이다.

- 가입자 (Subscriber)

통신 서비스를 제공받으며, KGC로부터 암호화에 사용되는 키를 발급 받은 개체를 말한다.

3.2 가정

LEA는 합법적인 감청 절차를 통해 암호 통신의 해독을 할 수 있는 개체이다. 그러나 LEA가 합법적인 절차 없이 통신 내용을 도청을 시도하고, 혹은 KGC의 마스터키를 획득하려는 시도를 하는 경우를 가정한다.

이와 같은 경우 다음의 요구 사항을 정의할 수 있다.

- LEA는 가입자의 암호 통신 내용을 해독할

수 없다.

- LEA는 KGC의 암호 통신 해독 정보를 획득할 수 없다.

3.3 감청 사전 절차

감청을 위해 가입자 A, B가 통신하는 경우를 가정한다. 사전 절차는 가입자가 키 생성 기관(KGC)로부터 ID 기반 암호 시스템의 공개키 쌍을 얻는 절차이며, [14] 등과 같다.

3.3 감청 절차

본 논문에서는 LEA의 양방향 통신의 경우(통화) 암호 통신 감청 절차에 대해서만 기술한다.

- LEA는 KGC와 통신 서비스 제공자 (MO)에게 가입자 A에 대한 감청 요청 전달
- 가입자 A가 난수 r_A과 r_A에 대한 서명을 생성 후 MO의 공개키로 암호화하여 서버에 전달

  $Enc_{ser}(r_A \| sign_A(r_A))$

  Enc는 공개키 암호화 함수이고, $sign$은 서명 생성 함수이다. 각 함수에 인자는 암호화나 서명에 사용된 키의 소유를 의미하며 Enc_{ser}는 서버의 공개키로 암호화, $sign_A$는 A의 개인키로 서명했음을 의미한다. ||는 접합(concatenation)을 의미한다.
- MO가 가입자 A로부터 전달 받은 난수 r_A와 서명 확인 후 난수 r_A와 A의 서명을 확인 후, 가입자 B의 공개키로 암호화하여 가입자 B에 전달.

  $Enc_B(r_A \| sign_A(r_A))$

  만약 MO가 가입자 B에게 전달할 때, MO의 서명을 첨부 요구가 있다면, 다음과 같이 변형될 수 있다.

  $Enc_B(r_A \| sign_A(r_A) \| sign_{Ser}(r_A \| sign_A(r_A)))$
- B는 전달 받은 정보를 복호화하여 서명 검사를 통한 난수 확인 후 난수 r_B 생성하고, 서명 생성 후 서버 공개키 암호화하여 MO에 전달

  $Ver_A(r_A \| sign_A(r_A))$ -> Yes/No

  if the signature is valid,

  $Enc_{ser}(r_B \| sign_B(r_B))$
- MO는 B로부터 전달된 r_B와 서명을 확인 후 A의 공개키로 암호화하여 A에게 전달

  $Enc_A(r_B \| sign_B(r_B))$

  $Ver_B(r_B \| sign_B(r_B))$ -> Yes/No
- A와 B는 각각 $devf(r_A,r_B)$를 계산. 여기서 $devf$는 r_A와 r_B를 통해 새로운 값을 도출하는 함수이며, +나 ×도 포함하는 일반적인 연산을 의미한다.
- MO는 KGC에 LEA로부터 전달된 감청 요청과 가입자 A의 ID와 함께 $devf(r_A,r_B)$ 전달
- KGC는 감청 기관 (LEA)에게 HI2을 통해 $devf(r_A,r_B)sH(ID_A)$ 전달
- MO는 HI2를 통해 암호 통신 관련 정보를 전달하고 HI3을 통해 서버 패킷 전달

본 방식은 가입자와 LEA의 공모가 있는 경우에도 s에 대해 알기 어려운 방식이다.

LEA가 $devf(r_A,r_B)$ s $H(ID_A)$를 갖고 있는 채로 가입자에게 $sH(ID_A)$ 혹은 $devf(r_A,r_B)$을 얻는 경우, s에 대해서 계산하는 것은 ECDLP의 계산 난이도와 같다.

IV. 기존 방식과 비교

먼저, 대칭키 기반의 방식은 감청을 위해 가입자 간의 암호 통신에 사용되는 공유 키 획득하거나 암호 기법에 대한 백도어 장치를 마련하는 것을 예상할 수 있다.

그러나 현재 대칭키 암호 기법으로 널리 사용되고 있는 AES 등은 알려져 있는 백도어가 존재하지 않으며, 대칭키 기반 방식으로 가입자 간 공유키를 획득하는 것은 세션 키의 경우 세션 변경 시마다 KGC가 키를 생성하여 지속적으로 LEA에게 전달해야 하는 부하가 발생한다.

한편, 인증서 기반의 공개키 기반의 방식은 KGC가 가입자의 개인키를 통해 가입자 간의 키 합의 기법을 통해 생성된 공유키와 동일한 키를 복제함으로써 공유키를 획득하는 방식이 가능하며, 가입자의 개인키를 제공하는 방안을 생각할 수 있다. 그러나 개인키를 제공하는 경우 감청 후 가입자가 개인키를 갱신하지 않는 이상 도청에 취약한 문제점이 있다.

마지막으로, ID 기반 암호 기법을 사용하는 경우는, 다음과 같다.

- 가입자 간에 키 합의 기법을 통해 생성된 공유 키 획득
- KGC가 저장한 마스터 키 LEA에 제공

그러나 KGC가 저장한 마스터키를 제공하는 것은 ID 기반 암호 시스템의 키 공탁 특성을 기반으로 하는 것이나, 마스터키를 변경하지 않으면 도청을 방지할 수 없는 문제점이 있다. ID 기반 암호 시스템에서 마스터 키는 전체의 개인키와 연관되어 있으며, 마스터키를 변경하는 경우 전체의 개인키 역시 변경해야 한다.

제안된 방식은 ID 기반 암호 시스템의 키 공탁 특성을 바탕으로, 마스터키를 변경하지 않고 도청을 방지할 수 있는 장점이 있다. 표 2는 기존의 방식과의 비교이며, 비교 항목은 [13]을 기반으로 한다.

표 2 기존 방식과 비교

Property	대칭키 방식	Abe-Kanda [13]	제안 방식
감청범위제한	o	o	o
Admissibility	x	o	o
통신방해탐지	x	o	o
복수감청기관	x	o	-
Target hiding	x	o	x
Off-line EA	x	o	o
송신자인증	?	o	o
EA/KGC 키등록	Initially registered	t^2 log P	Initially registered
개인키 수	1	t+1	1
Key exchange	D-H	키 교환 방식 제안	기존방식 사용

V. 결론

본 논문에서는 ID 기반 암호 시스템을 기반으로 암호 통신에 대해 합법적인 감청을 허용하고, 불법 도청을 방지하는 방식을 제안하고 있다. 3 가지 프로토콜이 마련되어 있으며, 본 논문에는 그 중 KGC의 마스터키를 보호하며 암호 통화에 대한 감청에 대해 기술하고 있다.

제안된 방식은 기존 방식과 키 관리의 효율성과 도청 방지의 용이함에서 장점을 보이고 있다.

[참고문헌]

[1] ETSI TR 101 331: "Telecommunications security; Lawful Interception (LI); requirements of Law Enforcement Agencies".

[2] ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[3] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

[4] ETSI TS 101 671: "Handover Interface for the lawful interception of telecommunications traffic".

[5] 3GPP TS 33.106: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements".

[6] 3GPP TS 33.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions".

[7] 3GPP TS 33.108: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover interface for Lawful Interception (LI)

[8] Micali, S. "Fair Public Key Cryptosystems.", In Proc. Advances in Cryptology-CRYPTO '92, Santa Babara, CA, August 16-20, LNCS, 740, 113-138, Springer, Berlin, 1992

[9] Shamir, A., "Partial Key Escrow: A New Approach to Software Key Escrow.", In Key Escrow Conf., Washington, DC, September 15, 1995

[10] Jefferies, N., Mitchell, C., and Walker, M., "A Proposed Architecture for Trusted Third Party Services.", In Proc. Cryptography: Policy and Algorithms, Brisbane, Australia, July 3-5, LNCS, 1029, 98-104., Springer, Berlin, 1995

[11] Verheul, R. and van Tilborg, Henk C. A., "Binding ElGamal: A Fraud-detectable Alternative to Key Escrow Proposals.", In Proc. Advances in Cryptology-EUROCRYPT '97, Konstanz, Germany, May 11-15, LNCS 1233, 119-133, Springer, Berlin.

[12] Frankel, Y. and Yungm, M., "Escrow Encryption Systems Visited: Attacks, Analysis and Designs", In Proc. Advances in Cryptology-CRYPTO '95, Santa Babara, CA, August 27-31, LNCS 963, 222-235, Springer, Berlin

[13] Abe, M. and Kanda, M., "A Key Escrow Scheme with Time-Limited Monitoring for One-way Communication", British Computer Society 2002, The Computer Journal, Vol. 45, No. 6, 2002

[14] D. L. Vo, F. Zhang, K. Kim, "A New Threshold Blind Signature Scheme from Pairings,", Proceeding vol. 1/2, pp. 233-238. 2003 Symposium on Cryptography and Information Security (SCIS2003), Itaya, Japan, Jan. 26-29, 2003