캡슐화 방식의 키 복구 시스템 구현

o
고정호, 김경태, 이강수
한남대학교 컴퓨터공학과

Implementation of Key Encapsulation based Key Recovery System

Jeong-Ho Ko, Kyung-Tae Kim, Gang-Soo Lee
Department of Computer Engineering, Hannam University

요 약

현재 국내에서는 암호이용에 대한 법 제정을 가지고 많은 문제들이 제기되고 있다. 일반인에게 암호의 사용은 피상적이지만, 일부 선진국에서는 전자상거래 및 인터넷에서의 암호사용에 대하여 구체화 시켜 실행하는 단계에 이르고 있다. 그러나, 이러한 암호 선진국에 있어서도 암호의 양면성, 즉 암호의 기밀성을 통한 개인정보와 기업정보 등을 포함하는 데이터의 보호와 범죄의 은닉에 사용될 수 있다는 문제를 가지고 있으며, 이에 대한 해결책으로 키 복구 방법을 사용하고 있다. 그러나, 키 복구 방법은 개인의 인권 침해라는 새로운 문제를 대두 시켰으며, 암호선진국들은 인권보호단체와 민간단체 그리고 기업의 반발에 의하여 키 복구 방법에 대한 새로운 서비스를 제공하고 있다. 국내에서도 연구 및 개발은 미비하지만 키 복구로 인하여 암호이용에 대한 법 제정이 지연될 정도로 전자상거래에 있어서, 그 비중이 크다고 할 수 있다. 본 논문에서는 키 복구 서비스를 사용하면서, 개인의 인권을 보호할 수 있는 키 복구 시스템을 소개한다.

1. 서론

현대사회는 21세기를 맞이하여, 정보기술의 발달이 극대화되어 비즈니스와 일상생활에 있어서 경쟁력과 효율성을 향상시켰다. 특히, 인터넷을 통하여 송·수신되는 데이터는 전자문서의 형태로 전송되며, 이러한 전자문서는 비인가자가 접근하는 것이 가능하다. 이러한 문제를 해결하기 위한 방법으로 암호기술이 사용되고 있으며, 전자상거래에 있어서 암호기술은 기밀성과 무결성, 인증 서비스를 제공함으로써 중요성이 더욱더 증가하고 있다[1,2].

기밀성 서비스는 특정 보안체계를 통해서 데이터의 비밀성을 유지하는 것을 의미한다. 즉 전달내용을 제3자가 획득하지 못하도록 하는 것이다. 전자결제를 위하여 은행계좌번호와 비밀번호를 인터넷을 통하여 상인에게 전달할 때 암호화하여 전송함으로써 도청자가 스니핑에 의하여 그 내용을 얻어내더라도 풀지 못하도록 할 필요가 있다. 비밀키 암호 방식 또는 공개키 암호화 방식 모두에 의해 해결할 수 있다.

무결성 서비스는 정보 전달 도중의 정보훼손 여부를 확인하는 것이다. 즉, 전달받은 내용이 중간에 권한이 없는 방식으로 변경된 것이 아닌지를 확인할 필요가 있다. 무결성은 메시지 다이제스트를 암호화하여 보냄으로써 해결 할 수 있다.

인증 서비스는 정보를 보내는 사람의 신원을 확인하는 것이다. 다시 말하면 통신 시스템에서 인증은 서명이나 편지의 내용이 실제로 정확한 곳에서부터 오는지 확인하는 것이다. 가령 판매자가 어떤 고객으로부터 상품대금으로 신용카드 번호를 받았을 때 고객이 신용카드의 실제 소유자인지를 확인할 필요가 있다. 인증은 공개키 암호화 방식에 의하여 해결 할 수 있다.

암호화 방법을 사용함으로써 전자문서를 보호할 수 있지만, 전자문서의 암·복호를 위해 사용되는 암호키의 관리문제가 제기되었다. 즉, 키의 분실 및 파손, 기관에서의 감사, 그리고 정부기관 등이 합법적인 절차를 통해 전자문서에 접근할 수 있도록 하는 신뢰서비스가 필요하게 되었다.

일반적으로, 이러한 서비스는 키 복구 시스템을 통하여 제공하고 있으며, 키 복구 시스템의 사용은 개인의 인권 침해라는 새로운 문제를 제기하게 되었다.

국내에서도 암호이용법에 대한 법 제정에 있어서, 키 복구서비스에 대한 문제가 논란이 되고 있다. 키 복구 서비스는 신뢰성 향상이라는 측면에 있어서 반드시 필요한 서비스이지만, 개인의 인권을 침해할 수 있기 때문에 국내에서 시행되려고 하다가 개인의 인권침해라는 반발로 그 시행이 중지되었던 전자주민카드와 같은 미묘한 문제라 할 수 있다.

본 논문에서는 신뢰성을 향상시키며, 또한 개인의 인권을 보호할 수 있는 키 복구 시스템에 대하여 기술하였다. 2장에서는 일반적인 키 복구 시스템에 대하여 알아보겠고, 3장에서는 본 논문에서 소개하는 키 복구 시스템에 대한 환경과 구성 그리고 키 복구 프로토콜에 대하여 기술하며, 4장에서는 실제적인 시뮬레이션을 통한 수행 시험결과와 일부 다른 키 복구 시스템과 본 논문에서 소개한 키 복구 시스템을 비교하였고, 끝으로 5장에서는 결론과 향후 연구방향에 대하여 기술하였다.

2. 관련연구

키 복구 기술은 개인이 자신의 공개키를 잃어버렸을 경우, 그리고 회사나 기관에서 사원의 정보를 공유해야 하는 경우, 정부에서 법적인 권한을 가지고 조사해야 하는 경우에 필요한 것이다.

국외에서 이러한 키 복구와 암호화 정책에 대한 정책결정을 주도하는 주요 선진국의 표준화 단체 및 기관으로는 미국 IETF(Internet Engineering Task Force), NIST(National Institute of Standards and Technology), 유럽의 ECMA(European Computer Manufactures Association, 유럽컴퓨터제조자협회) 그리고 국제 표준화기구인 ISO와 ITU 등을 통하여 활발히 추진되고 있다. 국내에서는 한국정보통신기술협회(TTA)에 의하여 표준화가 추진되고 있다[2].

키 복구 방식은 크게, 키 위탁 방식과 캡슐화 방식으로 나누어진다. 키 위탁 방식은 다시 위탁 방식, 상업적 키 백업 방식과 TTP(Trusted-Third Party)방식으로 분류된다. 키 위탁 방식은 키 자체를 공인된 기관에 위탁하는 것이며, 키 캡슐화 방식은 키 복구 시에 복구 필드를 이용하는 것이다. 캡슐화 방식은 어떤 키도 사전에 저장할 필요가 없으며, 복구 정보를 제한하여 복구기관의 능력을 제한할 수 있으므로 사용자의 거부감이 적으며, 도청 기간을 제한할 수 있다는 장점이 있다. 단점으로는 복구 정보의 수정과 조작이 가능하며 키를 얻을 수 없는 가능성도 있다. 그러나 본 시스템에서는 이러한 단점을 보완하여 개발하였다[4~10].

3. 키 복구 시스템 구현

3.1 개발환경

본 시스템은 Unix환경에서 C++로 작성되었으며, 암호 알고리즘으로는 공개키 알고리즘으로 RSA와 대칭키 알고리즘으로 DES, 전자서명 알고리즘으로 국내에서 개발된 KCDSA, 해쉬 알고리즘으로 SHA-1을 사용했으며, 암호 통신을 위해 BSD Socket을 이용하였다.

3.2 키 복구 시스템의 구성

시스템의 구성은 사용자가 키 복구 요청시 사용하는 UA(User Agent)와 전체 세션키를 복구해주는 키 복구 서버(Key Recovery Center : KRC), 부분세션키를 복구해주는 복구 대행자(Key Recovery Agent : KRA)의 엔티티로 구성된다.

3.3 키 복구 수행과정

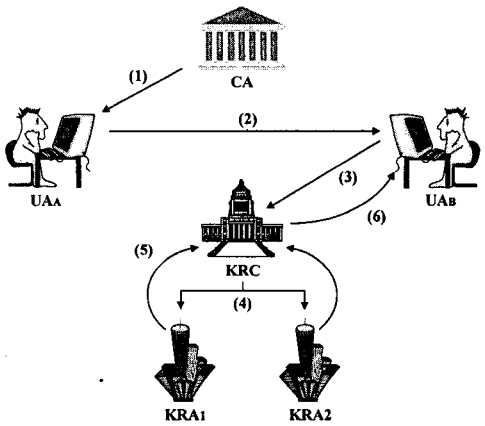

그림 1. 키 복구 수행과정

본 논문에서 구현한 키 복구 시스템은 그림 1과 같은 수행과정을 거쳐 키를 복구한다. 각 개체들 사이의 통신은 모두 암호화되어 전송된다.

(1) 송신자 A가 수신자 B에게 메시지의 암호문을 송신하기 위하여 인증기관(Certificate Authority : CA)으로부터 B의 공개키를 받아온다.

(2) 송신자 A는 CA에서 가져온 수신자 B의 공개키로 암호문을 작성하고, KRI(Key Recovery Information)를 생성하여 공개키 인증서와 함께 B에게 송신한다. 메지시의 전송 프로토콜은 다음 그림 2와 같다.

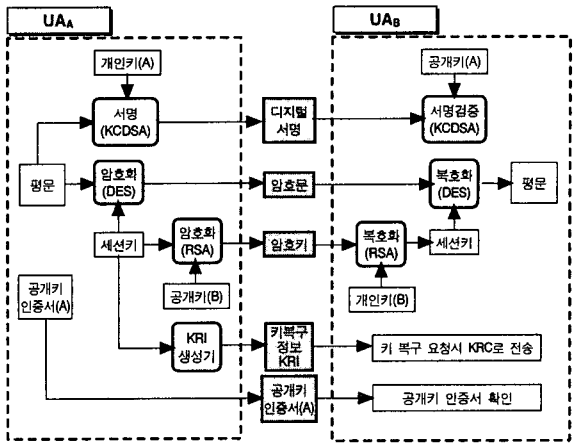

그림 2. 메시지 전송 프로토콜

위의 그림과 같이 공개키 기반의 통신을 위해, 암호문을 생성하는데 사용된 세션키를 수신자의 공개키로 암호화하여 전송하는 방식을 채택하였으며, 이 암호화된 세션키를 복호화할 수 없을 때와 사용자가 속한 기관의 감사나 정부 또는 법 집행 기관의 감사가 요구될 때 KRI를 이용하여 세션키를 복구할 수 있도록 구현하였다.

(3) 수신자 B가 키의 손상이나 유실로 인하여 수신된 암호문을 복호할 수 없을 때, 키 복구를 요청하기 위해 복구 요청서를 작성하여 수신 메시지 내에 포함된 KRI와 함께 KRC에게 송신

(4) 키 복구 요청을 받은 KRC는 사용자 식별 및 인증을 수행하고, KRI로부터 암호화된 부분세션키를 추출하여 복구요청서와 함께 각각의 KRA에게 송신

(5) KRA는 KRC의 요청 확인 후 암호화된 부분세션키를 복호하여 KRC에게 송신

(6) KRC는 부분세션키를 조합한 전체 세션키를 복구하여 키 복구 요청자에게 송신하면, 요청자는 세션키를 이용하여 수신된 메시지를 복호할 수 있다.

3.5 키 복구 정보 KRI

KRI는 세션키 복구를 위한 정보로서 메시지 전송시 암호문과 함께 전송되며, 내용은 다음과 같다.

$$KRI = RSA_{KRC}(RSA_{KRA1}(tk_1), RSA_{KRA2}(tk_2), \ldots, RSA_{KRAn}(tk_n), time, ID)$$

KRI는 세션키를 KRA의 개수로 분할하여 부분세션키를 생성한다. 그리고 부분세션키를 각각의 KRA 공개키로 암호화한 다음, 암호화된 부분세션키들과 KRI 생성시간과 메시지를 수신할 수신자의 ID 값을 포함하여 KRC의 공개키로 암호화하여 KRI를 생성한다. 여기에서 수신자의 ID 값은 메시지의 소유자와 키 복구 요청자가 동일한지를 확인하기 위한 값이다.

KRC는 개인키로 KRI를 복호화하여 암호화된 부분세션키를 추출해 각각의 KRA에게 송신한다. 그리고 각각의 KRA는 암호화된 부분세션키를 KRA의 개인키로 복호화하여 부분세션키를 추출한 다음, KRC의 공개키로 암호화하여 KRC에게 송신한다. KRC는 수신된 부분세션키들을 개인키로 복호하여, 모두 조합하므로 세션키를 복구한 후, 복구된 세션키를 키 복구 요청자의 공개키로 암호화해서 송신하게 된다. 그러므로 키 복구 요청자는 복구된 세션키로 암호문을 복호할 수 있다.

표 1. 알고리즘 처리속도 측정결과 비교

암호알고리즘	처리속도	키 크기 (byte)	CPU 속도	참조
DES (enc.)	2.3 Mbps	-	80486 66 MHz	http://www.kisa.or.kr
	2.16 Mbps	-	Pentinum 90 MHz	http://basslet.rsa.com/rsalabs/faq/html/3-1-2.html
	5.20 Mbps	16	SUN Ultra 10 (333MHz)	본 연구
RSA (enc.)	23 Kbps	128	Pentinum 200 MHz	http://www.kisa.or.kr
	21.6 Kbps	64	Pentinum 90 MHz	http://basslet.rsa.com/rsalabs/faq/html/3-1-2.html
	7.4 Kbps	128	Pentinum 90 MHz	http://basslet.rsa.com/rsalabs/faq/html/3-1-2.html
	150 Kbps	344	SUN Ultra 10 (333MHz)	본 연구
SHA-1	6.25 Mbps	-	Pentium 90 MHz	http://ncadl.nca.or.kr/HTML/1996/96095/96095.htm
	21.49 Mpbs	-	Sun-Sparc-20	http://ncadl.nca.or.kr/HTML/1996/96095/96095.htm
	11.82 Mbps	-	SUN Ultra 10 (333MHz)	Our result
KCDSA (signature)	40 Kbps	135	SUN Ultra 10 (333MHz)	본 연구

4. 시스템 성능분석

본 실험은 SUN Ultra 10(CPU 333MHz)과 256MB의 메인 메모리를 갖는 워크스테이션에서 수행되었고, 통신속도는 56Kbps로 가정하였다. 표 1은 본 시스템에서 사용된 알고리즘의 처리속도를 직접 측정한 결과이며, 키를 복구하는 걸리는 소요시간(실행시간과 통신시간)을 그림 3에서 간트 챠트로 보인다.

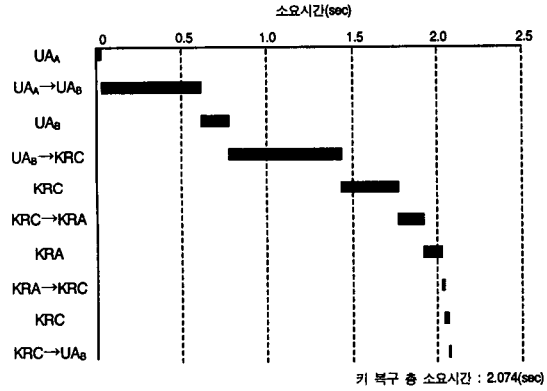

그림 3. 키 복구 소요시간 간트차트(KRA 2개)

그리고, 표 2에서는 기존의 다른 키 복구 시스템과 비교한 결과를 보인다.

표 2. 키 복구 시스템들과의 비교[3]

	Fair Cryptosystem	Clipper Chip	Fail Safe Key Escrow	Blind Decoding	Recovery Key	개발 시스템
소프트웨어 구현	○	×	○	△	○	○
사용자의 키 생성	○	×	○	○	○	○
도청기한 제한	×	×	×	○	○	○
키 복구 기관들의 공모	가능	가능	가능	불가능	가능	불가능
개인의 인권 보장	○	×	×	×	○	○

5. 결론 및 향후 연구방향

본 논문에서는 캡슐화 방식의 키 복구 시스템을 구현하였다. 이 방식은 모든 복구정보를 특정기관에 위탁하지 않고 사용자의 데이터에 포함하므로 개인의 인권을 보호할 수 있으며, 복구정보를 제한하여 복구기관의 능력을 조절할 수 있다는 장점을 가지고 있다. 향후 연구방향으로는 키 복구 서비스를 위한 향상된 보안기능의 개발과 데이터에 대한 기밀성과 대응되는 키 복구 서비스를 위한 효율성의 적절한 조화에 대한 연구가 필요하다.

참고문헌

[1] 이임영, 채승철, "Key Recovery 시스템에 관한 고찰", 한국통신정보보호학회, Vol. 7, No. 4, pp. 45~58, 1997. 12.

[2] 채승철, 이임영, "키 복구 시스템에 관한 고찰 II", 한국통신정보보호학회, Vol. 8, No. 4, pp. 97-111, 1998. 12.

[3] 채승철, 이임영, "안전한 키 위탁 시스템에 관한 연구", 한국통신정보보호학회, Vol. 9, No. 2, pp. 83-91, 1999. 6.

[4] Hal. Abelson, *et al.*, "The Risks of Key Escrow and Trusted Third-Party Encryption," *http://www.cdt.org/crypto /risks98/risks98.pdf*, 1997.5.

[5] NIST, "REQUIREMENTS FOR KEY RECOVERY PRODUCTS," FINAL REPORT, *http://csrc.nist.gov/key- recovery/*, Nov. 1998.

[6] Dorothy E. Denning and Miles Smid, "Key Escrowing Today," *IEEE Communications Magazine*, Sep. 1994.

[7] Dorothy E. Denning, Dennis K. Branstad, "A Taxonomy for Key Escrow Encryption Systems," *Communications of ACM*, vol 39, no. 3, pp.34-40, May. 1996.

[8] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, David M. Balenson, "Commercial Key Recovery," *Communications of ACM*, vol 39, no 3, pp.41-47, May. 1996.

[9] David Paul Maher, "Crypto Backup and Key Escrow," *Communications of ACM*, vol 39, no 3, pp.48-53, May. 1996.

[10] Ravi Ganesan, "The Yaksha Security System," *Communications of ACM*, vol 39, no 3, pp.55-60, May. 1996.