멀티 에이전트 기반 전자문서 복구

강상승° 임신영 함호상
한국전자통신연구원 전자상거래연구부
kss@etri.re.kr

A Study on the Multiple Agent-based Recovery for Electronic Documents

Sang-Seung Kang° Shin-Young Lim Ho-Sang Ham
EC/CALS Dept., ETRI

요 약

인터넷상에서 전송되는 암호화된 전자문서의 수신자가 자신의 암호키를 손상 혹은 분실하여 전자문서를 복구할 수 없을 때, 암호화된 전자문서를 복구할 수 있는 기술이 요구된다. 본 논문에서는 암호화된 통신 및 저장된 전자문서의 안전하고 신뢰성있는 복구를 지원하기 위해 멀티 에이전트 기반의 전자문서 복구 기술을 제안하였다. 제안한 방식은 기존 캡슐화 방식의 키복구 기술을 개선한 것으로, 멀티 에이전트 기반 복구, 해당 에이전트의 비밀 지정 기술, 동적인 공개키 분배 등의 특성을 지니는 새로운 방식이다. 공개키 기반 구조에서 실행되는 제안한 전자문서 복구 방식을 이용함으로써 정보보호 기능을 갖는 정보시스템들의 가용성이 향상될 수 있다.

1. 서론

통신망 상에서 운용되는 정보시스템에서의 전자문서에 대한 보안성은 매우 중요하며, 이를 위한 정보보호 시스템들이 개발되어 정보시스템 내에서 운영되고 있다. 정보보호 시스템들은 많은 수와 양(키당 16~344바이트 이상)의 암호키들을 이용하여 중요한 전자문서들을 암호화하여 통신 및 저장하고 있다. 따라서 정보시스템에서는 많은 수의 암호키들을 관리해야한다. 그러나, 암호키(특히, 개인키 또는 세션키)가 분실 및 손상되거나, 암호키를 소유한 사람을 일정한 시간 내에 찾을 수 없을 때, 암호화된 전자문서를 복구할 수 없으므로 이를 복구하기 위한 기술이 요구된다. 또한, 정보시스템의 소속 기업 또는 기관에서도 기관의 보안정책 및 법 집행에 따라서 암호화된 전자문서를 복호화 할 수 있어야 한다[1,2].

본 논문에서는 암호화된 통신 및 저장된 전자문서의 안전하고 신뢰성있는 복구를 지원하기 위해 멀티 에이전트 기반의 전자문서 복구 기술을 제안하였다. 제안한 방식은 기존 캡슐화 방식의 키복구 기술을 개선한 것으로, 멀티 에이전트 기반 복구, 해당 에이전트들의 비밀 지정 기술, 동적인 공개키 분배, 수신자에 의한 새로운 키쌍 생성 등의 특성을 지니는 새로운 방식이다. 또한 전자상거래 인프라내의 전자문서 복구를 위한 방식으로 개발된 것이지만 암호 통신을 이용하는 모든 정보 시스템에서 응용될 수 있다. 공개키 기반 구조에서 실행되는 제안한 전자문서 복구 방식을 이용함으로써 정보보호 기능을 갖는 정보시스템들의 가용성이 향상될 수 있다. 본 논문의 구성은 다음과 같다. 2장에서는 기존 방식의 특성과 문제점을 논하고, 3장에서는 기술적 요구사항에 대해 기술한다. 4장에서는 멀티 에이전트 기반의 전자문서 복구를 위한 시스템을 설계하고 분석하며, 마지막으로 5장에서는 결론을 맺는다.

2. 기존 연구

암호화된 전자문서의 복구를 위한 방식으로는 크게 키 위탁 방식, 신뢰된 제삼자(TTP) 방식, 상업적 키 백업 방식 및 키 캡슐화 방식으로 나눌 수 있다[3-6]. 이들 중에서 키 위탁 방식과 TTP 방식은 트랜잭션 오버헤드와 대량의 메모리를 요구하므로, 정보시스템상의 병목이 될 수 있다. 상업적 키 백업 방식은 이러한 오버헤드를 줄이지만, 암호화된 전자문서에 직접 접근이 가능하므로, 사용자들은 그들의 개인키를 백업하는 것에 불안감을 느낄 수 있다. 특히, 키 위탁 방식은 개인의 프라이버시 문제와 바인딩 문제가 발생할 수 있다. 그러나, 키 캡슐화 방식에서는 키의 소유자가 키복구의 권한을 가지므로, 개인 비밀의 침해로부터 비교적 자유롭고 다른 방식에 비해 많은 장점을 가진다. 그러나 기존의 키 캡슐

화 방식에는 다음과 같은 몇 가지 문제점들이 있다. 첫째, n개의 키복구 에이전트를 활용하는 시스템에서의 세션기 처리 방법이 알려져 있지 않다. 둘째, 송신자가 지정한 에이전트의 신원을 수신자가 알게 되므로 투명성이 저하된다. 셋째, 키복구 에이전트들이 정해져 있으므로 에이전트간의 결탁 공격 가능성이 있다. 넷째, 수신자는 다수의 키복구 에이전트와 직접 통신을 해야하므로 수신자마다 키복구 기능들이 설치되어야 한다.

기존 기술 중에서 대표적인 방식으로 IBM의 2단계 CSKR(Cryptographic Secure Key Recovery)[7]이 있다. CSKR에서는 1개의 복구 제공자와 2개 이상의 키복구 에이전트에 의해 키복구 서비스를 제공한다. CSKR에서는 서비스 시간을 줄이기 위해 공개키 암호 연산을 최소화하고 있다. 즉, 시간이 많이 걸리는 공개키 암호 연산은 KG에 대해서만 실행하며, KG는 KK로부터 유도할 수 없으므로, 세션그룹 내의 단위 세션마다 여러번 사용될 수 있다. CSKR에서는 단위 세션(예; 단위 트랜잭션)들을 그룹세션으로 쉽게 그룹화 할 수 있을 때만 장점을 가지며 키복구 에이전트가 미리 정해져 있으므로, 수신자(키복구 요청자)는 키복구 에이전트의 식별자를 알 수 있다. 따라서, 키복구 서비스의 투명성이 저하되고 결탁 공격의 가능성이 존재한다. 또한, 키복구 시스템당 1개의 난수를 이용하고 있다.

3. 기술적 요구사항

정보시스템을 운영하는 도중에 암호화된 정보를 복호화할 수 없을 때, 정보시스템은 더 이상의 작업을 진행할 수 없다. 따라서, 키복구의 시간을 줄이고 보안성을 높이는 것이 중요하다. 이러한 기술적인 요구사항들을 살펴보면 다음과 같다[8,9].

- 효율성 확보 : 손망실된 키의 복구를 통한 암호화된 정보를 최소한의 시간과 자원(컴퓨터 및 통신자원)으로 해결해야한다.
- 보안성 확보 : 전자문서 복구 기술은 정보시스템상의 악의를 가진 주체(일반 사용자, 키복구 센터 및 키복구 기관 등)에게 보안공격의 대상이 될 수 있다. 예컨대, 암호화된 정보의 범적인 소유자 모르게 그 암호화된 정보를 복호화 하는 것을 차단해야만 한다.
- 상호운용성 확보 : 전자상거래 시스템과 같은 정보시스템은 하나의 기관 내에서뿐만 아니라 국제적으로 가동될 수 있다. 따라서, 인터넷을 통해 형성된 다양한 플랫폼 및 서로 다른 정보시스템들간에서 연동이 가능해야 한다.
- 국제표준의 준수성 : 전자문서 복구와 관련된 시스템의 주요 기능요구사항 및 기존 구조들은 이미 국제적으로 표준화되었다. 예컨대, 키복구 시스템 벤더들은 키복구 연맹(KRA)[1]을 결성하여 시스템의 요구사항들을 공동 개발하고 있으며, 미국 NIST의 RKRP[9]는 키복구 시스템의 사실상의 국제 표준이라 할 수 있다.

4. 멀티 에이전트 기반 전자문서 복구 방식

멀티 에이전트 기반의 전자문서 복구 방식은 2보다 큰 n개의 키복구 에이전트를 지정하여 시스템을 구성하는 방식으로 제안사항은 다음과 같다.

- fork와 join 함수에 의한 멀티 에이전트 기반 복구 : 멀티 에이전트 기반 복구 시스템에서, 세션키(128비트)는 128/n비트로 분할하지 않고, n-1개의 난수키와 세션키를 이용하여 n개의 중간키(128비트)들을 생성하므로, 세션키에 대한 보안성이 증대된다. 그림 1의 프로토콜에서 fork 함수는 세션키(ssk)와 난수키(rk)들을 이용하여 세션키를 키복구 에이전트의 갯수만큼 분할하여 중간키(ik)들을 생성하는 것이며, join 함수는 부분키들을 결합하는 것이다.

· fork(ssk, n) = ik_1, ... ik_i, ... ik_n, (where, $ik_1 = ssk \oplus rk_1$, $ik_2 = rk_1 \oplus rk_2$, ..., $ik_i = rk_{i-1} \oplus rk_i$, ..., $ik_n = rk_{n-1}$)

· join(ik_1, ... ik_i, ... ik_n) = $ik_1 \oplus ik_2 \oplus$ ..., $\oplus ik_i \oplus$ ... $\oplus ik_n$

그림 2는 선택한 에이전트가 2개일 경우와 3개일 경우의 중간키들의 생성과정을 예로 보인다. 송신자는 각 ik_i들을 해당하는 키복구 에이전트들의 공개키로 암호화하며, 각 키복구 에이전트들은 자신의 개인키로 복호화하여 키복구 센터로 보낸다. 키복구 센터에서는 join 연산을 통해 세션키를 복구하게 된다. 한편, n개의 키복구 에이전트를 가질 때, $(ssk \oplus rk_1) \oplus (rk_1 \oplus rk_2) \oplus$ ..., $(rk_{i-1} \oplus rk_i)$,

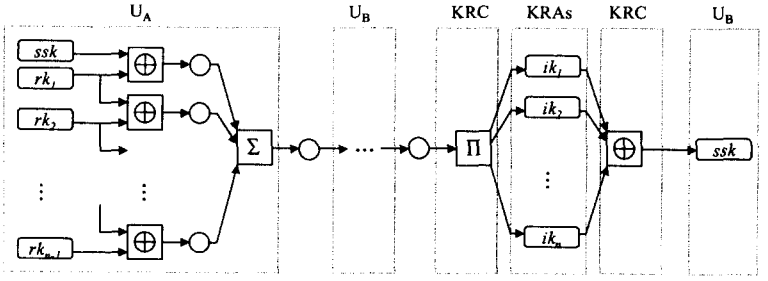

그림 1. 멀티 에이전트 기반 전자문서 복구 프로토콜

.... $\oplus(rk_{n-2}\oplus rk_{n-1})\oplus rk_{n-1} = ssk$ 이므로 세션키는 보존된다.

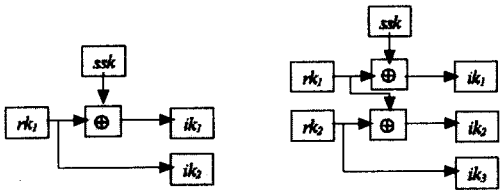

그림 2. 선택한 에이전트 수에 따른 중간키 생성과정

- KRA 집단으로부터 2개 이상의 KRA들의 비밀 지정 : 송신자는 다수의 KRA들을 비밀리에 지정하며 키복구 정보 내에 이에 대한 정보를 삽입한다. 이로써, 수신자는 키복구 에이전트를 알 수 없도록(또는 알 필요가 없도록) 한다. 수신자는 오직 키복구 센터의 공개키만을 알면 된다. 이를 통해 수신자에게 키복구의 투명성을 제공하고 파트들간의 공모공격 가능성을 줄인다.

- 인증시 첨부 방법에 의한 동적인 공개키 분배 : 공개키가 포함된 인증서는 필요한 곳에 필요한 시기에 분배한다. 다음의 인증서들은 공개키 기반구조를 통해 획득한다.(인증서의 정적 분배)
· 송신자(키복구 정보의 생성자) : 수신자, 키복구 센터 및 지정한 키복구 에이전트의 인증시(공개키가 포함)
· 수신자(키복구 서비스의 요청자) : 키복구 센터
· 키복구 센터 : 키복구 에이전트
나머지 인증서들은 필요한 시기와 곳에만 키복구 정보와 함께 보낸다.(인증시의 동적 분배)
· 키복구 센터 : 수신자가 키복구를 요청할 때 수신자의 인증서를 키복구 요청 메시지로부터 획득한다.(키복구 요청 메시지에 수신자의 인증서가 첨부됨)
· 키복구 에이전트 : 키복구 센터가 키복구를 요청할 때 키복구 센터의 인증서를 키복구 요청 메시지로부터 획득한다.(키복구 요청 메시지에 키복구 센터의 인증서가 첨부됨) 일반적으로 키복구 시스템에서 잠재적인 수신자는 수만명 이상이 될 수 있으므로, 키복구 센터가 사전에 모든 수신자의 인증서를 획득할 필요가 없으므로, 이러한 방법을 통해 인증서의 획득시간을 줄일 수 있다.

- 수신자에 의한 새로운 키쌍 생성 : 수신자는 자신의 개인키를 분실했으므로, 새로운 키쌍(공개키 및 개인키)을 생성하여 인증기관에 등록하고 이를 이용한다. 따라서, 수신자의 개인키를 불법적으로 획득했거나 사용기간이 만료된 수신자의 공개키를 이용할 수 없도록 한다.

- 키복구 서비스의 선택성 : 키복구 서비스는 정보시스템의 일반 사용자에게는 매우 민감한 사항이므로, 정보의 소유자인 송신자와 수신자가 선택할 수 있게 한다. 이를 통해 활용성이 증대될 수 있다.

멀티 에이전트 기반 전자문서 복구 시스템에서 추가적으로 고려해야 할 사항은 신뢰도의 trade-off 문제이다. 즉, 에이전트 수가 많아질수록 보안성은 증가하나 트래픽의 증가에 따른 성능이 저하되는 문제가 발생한다. 따라서 적용하려는 시스템의 환경에 따라 적절한 에이전트 수의 선택이 필요하다.

5. 결론

정보시스템 내에는 많은 수의 암호키들이 존재하며 안전하고 효율적으로 관리되어야 한다. 또한, 분실한 암호키에 대한 복구 기능도 포함되어야 한다. 본 논문에서는 이러한 필요성을 충족하면서 보다 신뢰성있는 서비스를 제공할 수 있는 멀티 에이전트 기반의 전자문서 복구 방식을 제안하였다. 제안한 방식은 정보보호 기술을 활용하는 모든 정보시스템들의 가용성 향상에 기여하며 보안성을 증대시킬 것이다. 부가적인 연구로는 정보보호 시스템에 대한 국제평가 및 인증기준에 따른 제안한 방식의 검증이 필요하다고 하겠다.

6. 참고 문헌

[1] Key Recovery Alliance, Cryptographic Information Recovery using Key Recovery, A Working Paper, Version 1.2, http://www.kra.org, Aug. 1997.

[2] Lance J. Hoffman, et. al., "Cryptography Policy," *Communications of the ACM*, pp. 109-117, Sep. 1994.

[3] Dorothy E. Denning and Dennis K. Branstad, "A Taxonomy for Key Escrow Encryption Systems," *Communications of the ACM*, pp.34-40, Mar. 1996.

[4] Jingmin He and Ed Dawson, "A New Key Escrow Cryptosystem," *Lecture Notes in Computer Science*, Vol.1029, pp.105-113, 1995.

[5] D. P. Maher, "Crypto Backup and Key Escrow," *Communications of the ACM*, pp. 48-53, Mar. 1996.

[6] Stephen T. Walker, et. al, "Commercial Key Recovery," *Communications of the ACM*, pp.41-47, 1996.

[7] R. Gennaro, et. al., Secure Key Recovery, IBM Thomas J. Watson Research Center, 1999.

[8] Sang-Seung Kang, et. al., "Realization of a New Encapsulation-based Key Recovery Protocol," *JCCI 2000*, May. 2000.

[9] Requirements for Key Recovery Products, Final Report, FIPS(Federal Information Processing Standard), http://csrc.nist.gov/keyrecovery/, Nov. 1998.