공개키 기반 구조에서의 인캡슐레이션 방식 키복구 절차

윤혁중°, 임진수, 이상하, 김동규

아주대학교 컴퓨터공학과

Encapsulation Key Recovery Procedure in Public Key Infrastructure

Hyuk-Joong Yoon, Jin-Soo Lim, Sang-Ha Yi, Dong-Kyoo Kim

Department of Computer Engineering, Ajou University

요 약

키복구는 암호화 제품의 사용자가 암호화키를 분실하여 데이터를 복호화할 수 없을 때 데이터를 복구하거나 수사기관등이 합법적인 절차로 암호화된 데이터를 복호화하기 위한 수단이다. 정보보호의 중요성에 대한 인식이 확대되어 앞으로 많은 종류의 암호화 제품이 개발될 것으로 예상되기 때문에 다양한 키복구 기술의 개발과 키복구 기술간의 호환성의 해결이 시급한 실정이다. 본고에서는 공개키 방식에 기반을 둔 전자상거래와 전자정부등에서 채택할 수 있는 인캡슐레이션 키복구 기술과 이를 위한 절차에 관하여 논한다. 공개키기반구조에서 키복구는 사용자와 법집행기관 모두의 요구를 충족시켜야 한다. 키복구기관을 인증관리센터의 관리하에 두고 인증관리센터가 인증하는 키복구기관의 공개키를 이용하여 키복구필드를 생성하는 인캡슐레이션 기술을 사용함으로써 사용자는 자신이 직접 세션키를 제어할 수 있는 장점이 있고 법집행기관도 필요한 경우에 언제나 사용자의 세션키를 복호화할 수 있다.

1. 서 론

컴퓨터의 대량보급과 정보통신 기술의 발달은 정보의 신속한 제공, 다양한 정보의 접근이라는 장점을 가져왔지만, 정보의 누출로 인한 개인 사생활의 침해와 더 나아가 국가중요 정보등의 누출도 함께 발생했다. 이러한 부작용을 해결하기 위해 암호화가 사용되어졌다. 암호화란 평문을 암호화키를 사용하여 암호화 알고리즘에 적용시켜 암호문을 생성하는 방법으로써 암호화키를 알고 있는 사람만이 암호문을 다시 평문으로 변환시킬 수 있다. 암호화의 사용으로 기밀 정보 누출의 문제점은 해결되었지만 암호화 키의 분실시 암호화된 데이터를 복구할 수 없는 문제점과 암호가 국가와 시민의 안전을 위협하는 반사회적 집단에 의해 사용됨으로써 합법적인 수사를 방해할 수 있는 수단으로 전락한다는 문제점이 발생했다.

미국에서는 이러한 점을 인식하고 암호화 제품에 대해 규제 정책을 실시해왔지만 개인의 사생활 침해가 생길 수 있어서 민간의 반대에 부딪쳐왔다. 현재는 부당한 암호기술의 악용을 방지하기 위해 암호문에 대한 합법적 접근권을 보장하는 기술로써 키복구(Key Recovery) 방식을 채택하고 있다.

우리나라에서도 암호화사용촉진을 위해 공개키기반구조와 키관리 기반기술의 중요성이 증대하고 있다. 본 논문에서는 인캡슐레이션 키복구 방식에 기반하여, 현재 우리나라에서 추진하고 있는 공개키기반구조에서 사용될 수 있는 키복구 절차를 제안한다.

2. 키복구방식의 종류[1]

2.1 키위탁 방식

키위탁방식이란 키전체나 키의 일부분을 하나 이상의 위탁 에이전트가 저장하는 방식을 말한다. 키의 분실시나 법집행시에 위탁 에이전트가 키전체나 키일부를 제공함으로써 정보의 복구가 가능하고 또는 위탁된 키를 사용하여 직접 정보를 복구할 수도 있다. 키위탁방식의 장점은 위탁 에이전트를 사용자가 선택할 수가 있고, 키의 일부분을 분산시킴으로써 공격 목표를 분산시킬 수도 있다는 것이다. 단점으로는 암호화 키 생성시에 제 3 자와의 통신 오버헤드와 위탁 에이전트의 저장장소 요구사항이다.

2.2 키분배센터로써 신뢰받는 제 3 자 방식

신뢰받는 제 3 자(TTP:Trusted Third Party)를 사용하는 방식으로써 암호화 세션키를 안전한 통신을 원하는 주체들이 아닌 신뢰받는 제 3 자가 생성하고 분배하는 방식이다. 여기서 신뢰받는 제 3 자는 키분배센터(KDC : Key Distribution Center)로 불린다. 키분배센터가 유사시의 키복구를 위해 세션키의 사본을 저장하고 있다면 위탁 에이전트의 역할을 하는 것이다. 장점은 키분배센터의 중앙집중화된 키관리이고 단점으로는 각 세션키에 대해 키분배센터와 사용자간에 온라인 통신이 필요하고, 세션키의 저장에 드는 장소와 비용, 키분배센터에서의 키노출(key compromise)에 대한 잠재성을 들 수 있

다.

2.3 키 인캡슐레이션 방식

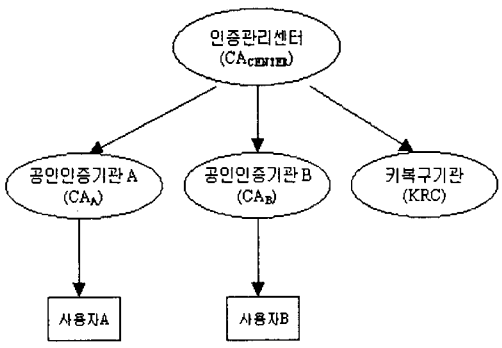
세션키가 외부의 제 3 자에게 위탁되거나 저장되지 않고 대신에 키복구에 필요한 정보가 전송되는 메시지나 파일에 부가되는 방식이다. 여기에서 키복구 에이전트는 키복구를 요청한 주체에게 키복구 정보를 풀어서 세션키를 제공하는 기능을 한다. 그러나 키복구 에이전트의 책임에 키복구 에이전트가 직접적으로 세션키를 복구할 수 없도록 키복구 요청자가 추가적인 정보를 가지고 있을 수도 있다. 장점으로는 정상적인 오퍼레이션 동안은 오버헤드가 작고, 두개 이상의 키복구 에이전트들이 사용되면 공격대상이 분산된다는 것이다. 단점으로는 키복구 정보가 어떻게 암호화된 메시지나 파일에 부가되는지 표준화할 필요성이 존재하고, 키복구 정보가 전송동안이나 저장되어 있을 때 분실되어져서는 안된다는 것이다.

3. X.509 인증서

인증서는 공개키에 대한 신뢰성을 확보하기 위한 일종의 증명서로써 믿을 수 있는 제 3 자에 의해 발급되며 공개키의 무결성을 제공한다. 이러한 역할을 하는 제 3 자를 인증기관(CA:Certificate Authority)이라 한다. 인증서를 발급한 기관은 발급뿐만 아니라 인증서 정지 및 폐지, 인증서 갱신, 인증서 공고등 계속적인 관리를 하여야 한다[2].

대표적인 인증서로는 ITU-T 의 X.509 가 있다. X.509 인증서는 인증서 버전, 인증서의 일련번호, 전자서명 알고리즘 식별자, 인증서를 발급한 인증기관의 이름, 공개키정보, 위의 정보들에 대한 전자서명이 포함된다. 현재 X.509v3 까지 나와있으며 이전 버전에 비해 확장필드에 다양한 정보를 포함할 수 있다. 확장필드에 포함되는 내용은 공개키와 정책 정보, 인증서의 대상과 발행자의 속성, 인증경로 제한등이다[3].

4. 인캡슐레이션 방식 키복구 절차



<그림 1> 인증기관과 키복구기관 모델

<그림 1>은 인증기관과 키복구기관(KRC:Key Recovery Center)모델에 대한 간략한 그림이다. 공인인증기관과 인증관리센터(CA_{CENTER})는 계층적인 구조를 가지고 있다. 모든 공인인증기관을 관리하는 최상위인증기관으로써 인증관리센터가 존재하고 각 분야별로 전자상거래, 행정, 금융등을 관리하는 공인인증기관이 존재한다[4]. 법집행기관이나 사용자가 유사시 키복구를 요청하기 위한 키복구기관은 인증관리센터가 임명하고 계층적인 관계를 유지한다. 따라서 인증관리센터가 공인인증기관 뿐만 아니라 키복구기관의 인증서 발급, 정지 및 폐지, 갱신 등의 관리를 하게된다. 필요한 경우에는 각 공인인증기관마다 키복구기관을 임명하여 관리할 수도 있을 것이다.

키복구필드는 키복구기관이 공개한 정보를 이용하여 생성하고 키복구기관은 유사시에 자신만이 알 수 있는 유일한 정보를 이용하여 키복구필드를 복호화하여 암호화 세션키를 얻는다. 따라서 키복구필드를 생성하고 복호화하는 정보로써 키복구기관의 공개키 쌍을 이용할 수 있다. 사용자가 암호화에 사용한 세션키에 대한 키복구필드를 생성하기 위해서는 키복구기관의 공개키를 사용하고 키복구기관은 키복구필드를 복호화하기 위해 키복구필드를 생성할 때 사용하였던 공개키의 쌍이 되는 비밀키를 사용한다. 키복구기관의 비밀키는 유일하게 키복구기관만이 알고 있는 정보이므로 자신만이 키복구필드를 복호화할 수 있는 조건이 만족한다. 사용자는 키복구필드 생성을 위한 키복구기관의 공개키가 인증된것인지 확인하는 절차가 필요하다. 키복구기관은 공개키 쌍(공개키와 비밀키)을 생성해서 사용자들이 이용할 수 있도록 공개키를 공개한다. 키복구기관의 공개키 정보는 사용자들이 믿고 사용할 수 있도록 키복구기관의 인증서에 포함되어 있고 인증서는 상위기관인 인증관리센터에 의해 전자서명되어진다. <그림 2>는 키복구기관의 공개키 정보가 들어있는 X.509 인증서 형식이다.

인증서 버전
인증서 일련번호
전자서명 알고리즘 식별자
인증관리센터의 X.500 이름
유효기간
키복구기관의 X.500 이름
키복구기관의 공개키 정보
인증관리센터의 유일한 식별자
키복구기관의 유일한 식별자
확장필드
인증관리센터의 전자서명

<그림 2> 키복구기관의 X.509 인증서

암호화되는 데이터는 통신 데이터와 저장 데이터의 두가지 영역으로 나눌 수 있다. 키복구를 위한 절차는 영역에 따라 다르다.

4.1 통신 데이터

통신 데이터는 기밀성과 무결성이 보장되어져야 한다.

공인인증기관 A에 속해있는 사용자 A가 공인인증기관 B에 속해있는 사용자 B에게 데이터를 전송하려면 다음과 같은 절차를 거쳐야 한다.

가. 인증서 발급 및 검증

사용자 A는 인증관리센터로부터 자가전자서명된 인증관리센터의 인증서를 수신한 후, 공개된 인증관리센터의 공개키를 이용하여 인증서를 검증한다. 이 후 사용자 A는 자신의 인증서를 발급해주는 공인인증기관의 공인 지정 여부를 확인하기 위해 공인인증기관 A로부터 인증서를 수신하고, 검증된 인증관리센터의 공개키를 이용하여 인증서를 검증한다. 마찬가지로 공인인증기관 B의 공인 지정 여부를 검증한다. 이 후 사용자 A는 자신의 인증서와 B의 인증서를 공인인증기관 A, B로부터 수신받는다. 다음으로 사용자 A는 키복구필드 생성을 위한 키복구기관의 공개키를 확보하기 위하여 키복구기관의 인증서를 수신한 후 인증관리센터의 공개키를 이용하여 인증서를 검증한다.

나. 메시지 암호화 및 키복구필드 생성

사용자 A가 사용자 B에게 전송하려는 메시지 M은 A가 생성한 세션키로 암호화된다. 세션키는 B의 공개키로 암호화하여 오직 B만이 복호화할 수 있도록 한다. 키복구필드에는 세션키를 키복구기관의 공개키로 암호화한 내용이 들어간다. 마지막으로 위의 내용들에 대한 전자서명을 생성한다.

$E_{K_s}[M] \| E_{KU_{KA}}[K_s] \| E_{KU_{KB}}[K_s] \| E_{KR_S}[H\{E_{K_s}[M] \| E_{KU_S}[K_s] \| E_{KU_{KA}}[K_s]\}]$

다. 키복구 절차

법집행기관이 A에서 B로 전송되는 메시지에 대한 도청을 원하는 경우, 법집행기관은 적법한 절차를 거쳐 전송되는 메시지를 가로챈다. 키복구기관에서 키복구필드를 키복구기관의 비밀키로 복호화하여 세션키를 얻는다. 그리고 세션키로 암호화된 메시지를 복호화할 수 있다. 사용자 B가 메시지를 전송받은 후에 메시지를 복구할 수 없는 경우에는 사용자 B가 키복구필드를 키복구센터에 전송한다. 이 때 전송중 키복구필드의 무결성을 확보하기 위해 사용자 B는 전자서명을 해야 한다. 만약 전송도중 키복구필드의 내용을 임의의 도청자가 변경을 한다면 키복구센터가 복호화한 세션키는 사용자 A가 생성한 실질적인 세션키가 아니기 때문에 사용자 B가 메시지를 복호화하는데 사용할 수가 없게 된다. 키복구기관이 세션키를 사용자에게 전송하는 과정에서는 기밀성과 무결성이 보장되도록 세션키를 사용자의 공개키로 암호화하고 키복구센터의 전자서명을 덧붙여 사용자에게 전송한다.

4.2 저장 데이터의 경우

사용자 A가 중요한 데이터를 암호화하여 자신의 로컬 컴퓨터에 저장한다고 가정한다.

가. 인증서 발급

사용자 A는 인증관리센터로부터 자가전자서명된 인증관리센터의 인증서를 수신한 후, 공개된 인증관리센터의 공개키를 이용하여 인증서를 검증한다. 검증이 되면 다음으로 키복구필드 생성을 위한 키복구기관의 공개키를 확보하기 위하여 키복구기관의 인증서를 수신한 후 인증관리센터의 공개키를 이용하여 인증서를 검증한다.

나. 데이터 암호화 및 키복구필드 생성

데이터 M을 암호화하기 위해 세션키를 생성하고 생성한 세션키를 이용하여 데이터를 암호화하고 세션키는 키복구기관의 공개키로 암호화하여 저장한다.

$E_K[M] \| E_{KU}[K_s]$

다. 키복구 절차

법집행기관이 키복구를 원하는 경우에는 적법한 절차를 거쳐 사용자의 로컬 컴퓨터에 있는 키복구필드를 획득하여 키복구기관에서 세션키를 얻고 데이터를 복호화한다. 사용자가 데이터를 암호화한 세션키를 분실한 경우, 키복구필드를 키복구기관에서 키복구기관의 비밀키로 복호화하여 세션키를 얻고 메시지를 복호화한다. 이때 키복구필드가 전송도중 변경되는 것을 방지하기 위하여 사용자가 전자서명을 하여 전송한다. 키복구기관이 세션키를 사용자에게 전송하는 경우에는 기밀성과 무결성이 보장되도록 세션키를 사용자의 공개키로 암호화하고 키복구기관의 전자서명을 덧붙여 사용자에게 전송한다.

5. 결론 및 향후 연구

본 논문에서는 인캡슐레이션 키복구 방식을 채택한 공개키기반구조에서 유사시 암호화키를 복구하기 위한 키복구정보를 생성하고 사용자나 법집행기관이 키복구를 행하는 절차에 관해 논하였다. 본 논문에서 제안된 절차는 현재 우리나라 암호화서비스기반구조에 키복구기술이 적용될 경우, 키복구를 위한 절차로써 사용될 수 있을 것이다. 인캡슐레이션 방식을 채택함으로써 세션키가 제 3자에 노출되지 않고 사용자만이 세션키를 제어할 수 있게 되어 사용자에 대한 프라이버시가 보호될 수 있고, 법집행기관은 필요한 경우 적법한 절차를 거치면 키복구를 통해 암호화된 데이터를 복호화할 수 있다. 따라서 암호화제품의 사용자, 법집행기관 모두가 만족할 수 있는 키복구가 이루어진다.

암호화의 역기능을 해소하기 위해 키복구의 중요성이 날로 부각되고 있다. 키복구는 키관리기반구조의 일부분으로써 공개키기반구조와의 연계방안을 고려하여 개발되어야 할 것이다. 앞으로 다양한 기술의 키복구를 채택한 암호화 제품이 생산되리라 예상된다. 따라서 인캡슐레이션 방식이 아닌 다른 키복구 기술을 채택한 제품이라도 호환성을 가지고 작동할 수 있도록 다양한 키복구 기술간의 호환성에 관한 연구가 이루어져야 할 것이다. 키복구는 개인의 프라이버시와 밀접한 관련이 있으므로 오용되어 사생활 침해가 일어나지 않도록 키복구제도 도입과 키복구 절차가 적법하게 이루어질 수 있는 법률의 제정도 필요하리라 본다.

[참고 문헌]

[1] Key Recovery Alliance, "CRYPTOGRAPHIC INFORMATION RECOVEYRY USING KEY RECOVERY", http://www.kra.org, Aug. 1997.

[2] William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY: Principles and Practice, Prentice-Hall, 1999.

[3] R.Housley, W. Ford, W. Polk, D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, Jan. 1999.

[4] 홍기융, 인증관리센터 구축 및 운영계획, 제 4회 정보보호 심포지움, 1999. 4.