通信情報保護學會誌
第8卷 第4號. 1998. 12

키 복구 시스템에 관한 고찰 II

A Study on the Key Recovery System II

채 승 철*, 이 임 영*

요 약

암호가 법 질서에 위배되는 목적으로 사용되는 것을 막기 위해 선진 각국에서는 여러 가지 암호 정책을 수립하고 있다. 그 중에서 현재 가장 주목을 받고 있는 것이 키 복구(Key Recovery) 개념이다. 이 개념은 정부 수사기관에게 암호 통신에 대해 수사권을 행사할 수 있는 능력을 부여하는 것이다. 또한 수사권 행사 이외의 프라이버시 침해를 보호할 수 있어야 한다. 본 고에서는 현재까지 제안된 복구 방식과 동향 등을 살펴본다.

I. 서 론

암호는 이제 국내에서도 통신이나 정보 보호 등에 없어서는 안될 필수 도구로 자리잡고 있다. 가장 많이 사용되는 워드프로세서나 일반 웹 브라우저, 전자 메일 프로그램 등에서도 최신의 암호 기법을 이용한 암호화 기능이 추가되어 있고, 차세대 국가 전략 산업으로 육성되는 전자 상거래에 사용되는 암호를 위해 전자 서명법 등의 기본 법령이 제정중에 있다. 이처럼 군에서나 이용되던 암호가 일반인에게 사용됨으로써 이전에 가능하지 않았던 전자적인 인증과 서명 등과 같은 온라인 상의 신원 확인이 가능하게 되었다. 또한 개방 통신로 상에서도 정보를 안전하게 전송할 수 있는 정보 보호 기능이 제공됨으로써 실생활에서 일어나는 일들을 전자적으로 간편하게 처리할 수 있게 되었다.

그러나 암호 사용의 일반화가 이러한 긍정적 측면만 있는 것은 아니다. 키 없이는 복호가 불가능하다는 암호의 성질 때문에 암호화한 데이터를 관리하려면 키 관리에 상당한 주의를 기울여야 한다. 암호화라는 것은 커다란 비밀(문서)을 작은 비밀(복호용키)로 바꾸어 주는 역할을 하는 것이라고 할 수 있다. 크기가 작아진다는 것은 보관하기는 쉽지만 상대적으로 더 잃어버리거나 유실되기가 쉽다고 볼 수 있다.

이에 대한 대비책으로는 여러가지 방법이 있을 수 있다. 예를 들면, 자기 자신이 키를 주의깊게 관리하는 방법이 있을 수 있다. 키가 손상되거나 키를 담은 IC 카드를 잃어버릴 경우를 대비해서 복사본을 만들어 두는 것이다.

* 순천향 대학교 컴퓨터학부

하지만 이 방법은 키가 조금이라도 많아진다면 그다지 좋은 방법이 아니다. 키의 복사본이 늘어나면 그만큼 안전도가 떨어질 수 있기 때문이다.

또한 암호를 좋지 않은 목적에 이용하는 경우에 대한 대비책이 필요하다. 암호를 사용하면 범죄 공모라든가 범죄 사실의 은폐 등이 가능하며 비밀장부 등을 안전하게 보관할 수 있다. 차후에 이런 것들을 수사기관에서 조사하게 되면 용의자는 단순히 더미(dummy) 파일이라고 주장할 수 있을 것이다. 또한 국가간에서는 산업 스파이나 중요한 국가 정보 등의 유출 문제 등이 생길 수 있다. 만약 수사기관이 이런 것을 조사하려고 하면 매우 많은 암호 해독 비용이 필요하며 비도가 강한 암호를 사용한다면 조사 자체에 어려움을 겪을 것이다.

이러한 문제점들의 대안으로 현재 논의되고 있는 방법이 키 복구(Key Recovery)이다. 이 방법을 사용하면 사용자는 유사시에 키가 손실되어도 데이터를 복구할 수 있으며, 국가도 적법한 절차에 따르면 손쉽게 수사를 진행할 수 있다. 하지만 이 방법은 국민 개개인의 사생활을 침해할 소지가 있다는 이유로 반대하는 의견도 상당하다.

본 고에서는 이러한 키 복구 방식의 정의와 분류, 그리고 현재 나와있는 키 복구 방식들의 간단한 원리 등과 살펴보고 선진 각국의 관련된 진행 상황을 살펴볼 것이다.

II. 키 복구 시스템의 정의 및 배경

키 복구(Key Recovery) 시스템이란 "사전에 약속된 어떤 특정한 조건하에서 허가된 사람에게 복호화가 가능한 능력을 제공하는 암호 시스템"이라고 정의할 수 있다. 여기서 특정한 조건이라는 것은 여러 가지 상황이 될 수 있다. 예를 들면, 법 집행기관이 범죄 수사를 목적으로 암호문을 복호해야 한다거나, 암호문의 소유자가 키를 분실해서 복호를 할 수 없는 경우 등을 말한다. 허가된 사람은 사전에 미리 합의되어 복구 능력을 가질 수 있는 사람을 뜻한다. 이것은 정부기관, 개인, 기업 등이 될 수 있다.

즉, 키 복구란 암호 시스템에서 키를 가지고 암호문을 복호하는 정상적인 절차 외에 다른 방법으로 유사시에 암호문을 복호할 수 있는 방법이다.

복구 능력을 가진다는 것은 실제 데이터를 암호화한 키 자체를 얻어내거나 또는 복호된 평문을 얻는 것을 말한다. 암호문 생성시에 암호알고리즘 외에 어떤 특정한 메커니즘을 통해서 이러한 방식을 지원하는 것이 가능하다. Key escrow라는 용어는 복구키(recovery key)로 사용자의 비밀키를 위탁한 경우에 주로 사용되며 이것은 키 복구 또는 Key archive, Key backup, Data recovery라고도 한다.

암호의 사용은 근래까지 국가 정보기관이나 군사 기관을 중심으로 한 목적에 이용되어 왔었다. 그러나 최근에 들어서 암호가 더 이상 이러한 국가 기관들의 전유물이 아니라 전자상거래와 같은 상업적 목적이나 민간인들의 프라이버시 보호와 같은 부분에 사용되기 시작하였다. 이러한 암호 사용의 확산에도 불구하고 아직까지 대부분의 정부는 이러한 민간의 암호 이용에 대한 통제 정책을 강구하지 않고 있다. 정보가 아직 활성화되지 못한 대부분의 국가에서는 아직 암호의 국내 사용이 활성화되지 않았기 때문에 제한할 필요성을 느끼지 못하기 때문이다.

하지만 이미 미국이나 유럽 등의 국가에서는 민간에서 이용하는 암호를 통제하는 정책을 결정하고 있다. 이러한 규제 정책은 크게 암호의 수입/수출 규제와 사용에 관한 규제로 나누어지는데 이것의 목적은 각각 자국민과 국가의 안전에 관한 정보를 수집하기 위한 국가 보안상의 이유와 법 집행을 위해 특정한

범죄 활동의 증거 수집을 위한 이유로 대별될 수 있다. 강력한 암호 사용의 확산은 위의 두 가지 관점에 대한 위협을 증가시킬 수 있기 때문이다.

대부분의 경우 첩보기관은 통신의 도청과 분석에 의존해서 정보를 수집한다. 일반적으로 수출통제의 목적은 이러한 국가 보안적 관점에 그 목적이 있다. 미국에서는 국가 보안에 관계된 외국의 통신을 도청하고 분석하는 것을 용이하게 하기 위해서 수출 통제 정책을 취하고 있다.

또한 민간에서 이용되는 암호는 범죄자들에 의해 오용되거나 악용될 수 있다. 이러한 범죄 용의자의 행동을 감시하고, 관련된 정보를 수집하기 위해 자국 내부의 통신을 감시해야 할 필요성이 있다. 이러한 법 집행기관의 감시활동을 위해서는 자국내의 사용 제한이나 수입 제한이 필요하게 된다. 이러한 통제를 위해서 여러 가지 방법들이 제안되었지만, 그 중에서 가장 가능성 있는 대안이 키 복구 방식이라고 판단한 정부들이 키 복구 방식을 수출 및 암호 사용의 제한 정책으로 입안하기 시작하였다.

이와 같은 정책을 가장 먼저 추진하기 시작한 것은 미국이다. 미국은 가장 먼저 정보화 사회에 도달한 나라중의 하나이며, 때문에 위에서 언급된 문제들에 가장 먼저 직면하게 되었다. 미국 정부가 최초로 계획한 것은 암호 사용시에 복호용 키를 일정한 국가기관에 맡겨두고 이를 바탕으로 법 집행을 보장하겠다는 계획이었다. 이것이 클리퍼(Clipper) 정책라고 불리우는 키 위탁(Key Escrow) 정책이다.

그러나 이 계획은 초기 단계부터 사생활 침해를 우려한 시민들의 격렬한 반대에 부딪쳤다. 이후에 이 계획은 몇 번의 수정을 거쳐서 현재는 시행목적이 법 집행 보다는 시민들의 데이터를 안전하게 보호해 주는 것에 있다는 의미로 키 복구라는 용어를 사용하게 되었다.

III. 국가별 암호 정책 및 관련 동향

현재 각국에서는 키 복구에 관한 정부와 사용자의 논란이 진행 중이다. 키 복구 방식을 국가차원에서 도입하는 문제는 앞서 말한 정부의 필요성과 시민들의 사생활 보호에 대한 욕구가 서로 상충되는 부분이 있기 때문에 앞으로 많은 절충안이 필요할 것이다. 본 장에서는 각국의 현재 진행사항을 살펴본다.

1. OECD Guideline

1997년 3월, OECD는 암호 정책에 관한 8가지 기본 원칙을 채택하였다. 이 지침서의 본문 중 키 복구와 관련된 내용에서는 정부의 합법적인 수사권한과 민간의 프라이버시 보호에 대한 두 가지 요구를 모두 수용하였다고 볼 수 있다. 여기에서는 필수적인 키 복구 개념을 채택하지는 않았지만, 여섯번째 원칙에서는 정부에게 암호화된 정보의 평문을 억세스할 수 있는 능력을 주는 것을 허가하고 있다. 민간부분의 프라이버시 보호 요구에 대해서는 다섯번째 원칙에서 개인의 프라이버시에 대한 권리를 존중할 것을 명시했으며, 두번째 원칙에서는 사용자의 선택에 따라 사용하도록 언급하였다. 이러한 OECD 가이드라인을 넓은 시각에서 본다면 키 복구쪽을 지원한다는 것으로 해석할 수 있을 것이다. OECD 가이드라인은 결과적으로 정부가 암호를 제한하는 것을 지원하거나 키 복구 암호를 촉진시킬 것으로 예상된다.

2. 미국의 키 복구 정책

현재 미국 암호 정책은 1992년에 발표한 클리퍼 정책에 기반을 두고 있다. 클리퍼칩은 위탁된 키를 사용하여 정부가 적법한 도청을 수

행할 수 있는 장치로 미국 정부의 이러한 정책은 민간의 사생활 침해 가능성에 대한 이유로 많은 시민 자유 단체들의 반발을 야기시켰다. 키가 오직 법이 허가한 상황에서만 공개된다는 정부의 보증에도 불구하고 이 법안은 개인적인 사생활을 침해하는 것으로 받아 들여졌다. 광범위한 민간부문의 협의 과정을 거친 후에 클린턴 정부는 클리퍼 이후의 정책을 바꾸게 되었다. 결과는 정부가 접근할 수 있는 권한은 유지하지만 암호화 키를 가지고 있는 키 복구 기관은 사용자에게 선택하도록 양보한다는 것이다. 1996년 12월, 클린턴정부는 다음과 같은 행정 명령을 내렸다.

- 암호키의 길이나 알고리즘에 관계 없이 키 복구가 수용된 제품을 수출할 수 있다.
- 키 복구가 없는 56bit 암호 제품를 설계하고 수출할 수 있으며, 키 복구 제품을 1999년까지 계획해야 한다.

이 행정 명령은 또한 수출 통제의 관할권을 군수품 수출 제한을 관장하는 국무성에서 이중 용도 제품(dual-use goods) 제한을 관장하는 상무성으로 이전시켰다.

상무성은 1996년 12월 23일, 행정명령의 시행을 위해서 제한 정책을 발표하였다. 이 제한 정책은 표면상으로는 수출 통제 목적이지만 정부의 키 복구 요구를 만족하는 자국내 키 복구 기반구조의 설립을 의미한다. 키 복구 암호 제품을 수출하기 위해서는 반드시 제한 정책에 수립된 키 복구 요구사항의 기능을 만족해야 한다. 키 복구 암호용 수출 제품의 키나 수출 제품에 의해 암호화된 정보의 복호를 위한 정보 역시 제한 정책 내에 수립된 요구사항을 따르는 승인된 키 복구기관에 의해 관리되어야 한다.

상무성이 발표한 제한 정책의 명백한 의도는 상품 제조업자들이 수출뿐만 아니라 미국 내에서도 사용되는 하나의 키 복구 암호 시스템을 만들도록 유도하는 것이다.

미국의 수출 정책은 자국내의 암호 정책과 밀접한 관련이 있다. NIST는 키 복구 암호 제품을 위한 연방 표준을 설립하려고 하고 있으며, 다양한 기술적 가능성, 상호 운용성 등에 대한 검토를 수행하고 있다.

3. 유럽의 동향

미국 정부의 키 복구 정책과 관련된 일련의 움직임은 유럽 쪽에도 파급되고 있으며 이와 비슷한 정책이 제안되고 실행되려고 하는 움직임을 보이고 있다. 유럽 국가들 역시 전통적으로 국가가 암호 기술을 관리하여 왔기 때문에 인터넷의 보급에 따른 암호 기술의 일반화가 암호 정책에 커다란 영향을 미치고 있다. 하지만 유럽의 경우에는 키 복구(Key Recovery) 개념 보다는 암호 서비스와 키 관리 등을 수행하는 TTP(Trusted Third Party)의 허가제 개념을 이용한 규제 방식을 이용하려 하고 있으며, 앞으로도 비교적 엄격한 TTP를 이용한정책과 키 복구 개념을 이용한 정책이 공존하리라 예상된다.

1) 프랑스

1996년 7월 발표된 "Telecommunications Act of 1996"에서 제 17조에 암호 사용에 관한 규제를 명시하여 모든 TTP들은 필수적으로 면허를 획득해야 한다는 면허 제도를 요구하였다. 이러한 TTP들은 정부의 요구가 있을 때 사용자의 키를 제공해야 한다. 또한 이전에는 민간인들에게 40비트 이상의 암호 사용을 금지하고 있었지만, 이 법안에서는 정부에 의해 허가된 TTP에 키를 위탁한 사용자는 다른 제한 없이 암호 서비스를 사용할 수 있다는 내용을 담고 있다. 하지만, 키를 위탁하지 않은

사용자는 암호 사용시마다 정부기관에게 암호 사용 허가를 얻어야 한다. 또한 인증 및 정보의 무결성을 확보하기 위한 암호 사용은 자유롭지만, 정보의 비익을 목적으로 사용하는 암호 장치는 반드시 승인 과정을 거쳐야 한다.

2) 독일

독일은 본래 암호 사용의 자유를 보장하고 있었으나 1997년 4월에 내무부 장관의 연설에서 범죄 수사와 국가 보안을 위해 법적인 요구에 키를 제공하는 것을 제외한 자국내의 암호 사용 제한을 주장하면서부터 논란이 계속되고 있다.

독일에서는 1996년 12월에 「정보·통신 업무의 조건의 규제에 관계법률」이 작성되고 의회에서 심의되고 있지만, 그 제 3항 「전자 서명」의 제 12조항에서 「법률 집행기관은 필요에 따라 인증 기관이 관리하는 개인 정보를 입수하는 것이 가능하다」라는 것을 명시하고 있다. 또한 암호 장치의 선택의 자유와 범죄 목적의 이용을 막기위한 규제 사이의 밸런스를 조절하기 위해 암호 장치의 규제나 키 위탁 제도의 신설이 검토되고 있다

하지만 국제 상공회의소 독일 지부(The German chapter of the International Chamber of Commerce), 독일 산업연맹(Bundesverband der Deutschen Industrie e.V.) 및 독일 전기통신기업 조합(Teletrust e.V.) 등을 비롯한 산업계에서는 암호의 규제 도입에 대한 것을 다음과 같은 이유로 반대하고 있다.

- 암호의 이용을 법률로 제한하더라도 실제로는 이것을 피해갈 수 있으므로 실질적으로 암호 규제는 의미가 없다.
- 향후 기술 혁신을 예측할 수 없으므로 현재 기술에 기반한 통제 기술이 앞으로도 유효하다고 볼 수 없다.
- 현재 독일에서는 암호 통신에 이용되는 키를 신뢰 기관에 위탁하는 구조를 검토하고 있지만, 그러한 구조는 막대한 관리 비용이 들어간다.
- 암호 통신 사용자의 암호화 키 전부를 위탁하면 외국의 첩보 기관 등의 공격 목표가 될 소지가 있으며, 관리 조직의 부정행위가 생길 수도 있다.

3) 영국

1995년 노동당에서 'Communicating Britains Future'라는 성명을 발표하며 미국의 클리퍼 정책에 반대하며 영국은 법 집행기관에게 복호의 요구 권한만을 부여하겠다는 발표를 하였다. 그러나 노동당이 집권한 후인 1997년 3월 21일에 무역 산업부(DTI, Department of Trade and Industry)에서 발표한 'Licensing of Trusted Third Parties for the Provision of Encryption Services'에서는 암호화된 키 관리 서비스를 하기 위한 신뢰기관(TTP, Trusted Third Party)의 필수적인 등록을 요구하는 TTP의 면허제도를 시행한다고 발표하였다. 이 정책은 암호 제품에 대한 제한은 없지만, 서비스를 제공하는 TTP에 대한 정책으로 암호 사용자가 암호 서비스를 받기 위해서 등록된 TTP에서만 서비스를 받을 수 있도록 하였다. 영국에서는 다시 1998년 5월 암호 공개키 자유화에 관한 정책인 "Secure Electronic Commerce Statement"에서 영국 정부는 그 동안 암호제품 업체들이 정부에게 의무적으로 위탁해야했던 암호 공개키를 오는 하반기부터 자발적으로 위탁할 수 있도록 했다.

IV. 키 복구 관련 동향

현재 키 복구에 관한 논의는 선진국을 중심으로 계속되고 있다. 미국에서는 클리퍼 정책이 발표된 후 IBM을 비롯한 미국 내의 기업

들이 KRA(Key Recovery Alliance)를 결성해서 강력한 암호 제품 사용의 촉진을 위해 상업적인 용도의 키 복구의 상호 호환성, 키 복구(key recovery) 제품과 키복구를 지원하지 않는 제품(non-key recovery) 사이의 상호운용 등의 문제점 해결과 구현, 실행에 관한 해결책을 찾기 위한 활동을 펴고 있다. 현재 산하에 다섯 개의 위원회가 있으며 각국의 30여개 회사들이 참여하고 있다. KRA는 그동안 수출 제한 정책에 반대 입장을 취해왔던 산업계가 현실적인 수출 방안을 찾기 위해 마련한 대안이라고 할 수 있다.

또한 미국은 연방 키 관리기반 표준 개발을 위한 기술 자문 위원회(TACDFIPSFKMI, Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure)를 설립하고 미국내의 키 관리 기반 구조(KMI)를 제정하기 위해 논의를 진행했으며 이 가운데에 키 복구 표준안이 논의되고 있다. 이 위원회는 1996년 7월 24일 공식 승인되었으며 동년 12월 5~6일간 첫 미팅을 시작하여 Working Group으로 분류되어 각각 보안 요구사항, 상호운용 등의 사항을 토의하였고, 1998년 6월 17~19일에 마지막 회의를 가졌다. 이 표준위원회는 1998년 5월 29일 Advisory Committee에서 키 복구 모델과 각각의 기능과 보안 요구사항 등을 체계적으로 분류한 키 복구 표준안(Key Recovery Standard Draft)를 발표 하였다. 하지만 최종 미팅에서 키 복구를 위한 FIPS를 개발하는 위원회는 "기술적인 문제"와 "시민과 정부의 요구사항의 충돌" 때문에 표준 수립에 실패했다는 내용이 1998년 6월 26일 보도되었다.

1차 위원회는 표준화 작업이 여러 가지 요구사항들의 충돌, 기본적인 제품 평가 모델의 미완성 등으로 인해 표준화의 기준을 만족하지 못했기 때문에 표준안으로 상정하지 않고 위원회를 해산했다. 98년 8월에 재구성된 2차 위원회는 두차례의 회의에서 이전에 작업한 문서의 용어 검토, 요구사항 및 모델 검토 등을 거쳐 98년 11월 표준안(Draft Standard)을 제출하였다.

현재 키 복구에 대한 찬반 양론이 많은 논쟁을 벌이고 있다. 키 복구에 대한 반대 의견은주로 시민 자유단체들을 중심으로 키 복구와 미국을 비롯한 각국 정부에 대한 반대 운동이 벌어지고 있다. 이를 반대하는 단체로는 다음과 같은 단체들이 있다.

● **EPIC(Electronic Privacy Information Center) - www.privacy.com**

1994년에 설립된 영국에 있는 공공연구기관으로 시민의 자유와 사생활의 보호를 목적으로 설립되었다. 범세계적인 시민 권리와 인터넷의 자유에 관한 캠페인을 추진하고 있다.

● **IPC(Internet Privacy Coalition) - www.ipc.com**

인터넷상의 프라이버시 향상을 위한 도구(암호 제품) 사용의 자유를 얻기 위한 Golden key 캠페인 등을 벌이면서, 네트웍상에서의 시민 자유에 대한 정책과 현재 상정되는 법안이나 키 복구에 대한 반대 의견을 주로 보도하고 있다.

그 밖에도 영국의 IFEA(Internet Free Expression Alliance), 미국의 EFF(Electronic Frontier Foundation) 등이 반대 입장을 표명하고 있다.

또한 GILC(Global Internet Liberty Campaign)과 같은 단체는 영국의 내무 장관이 현재 영국의 EU의 장직을 이용하여 암호키에 대한 정부의 접근권을 보장하려 한다고 비난하였다. GILC은 프라이버시의 보호와 표현의 자유, 인터넷 전자상거래의 진흥 및 규제 정책의 실효성 등을 들어 영국의 입장에 반대하고 있다 . GILC는 1997년 OECD의 암호정책지침과 1997

년 EU의 "Towards A European Framework for Digital Signatures And Encryption" 상에 나타난 암호정책과 비교하면서 영국의 암호정책은 정보화 사회에서 영국의 지위를 2류 국가로 전락시키는 결과를 낳게 될 것이라 경고하고 있다. 이 성명서는 CDT(Center for Democracy and Technology) 와 ISOC(Internet Society) 등을 비롯하여 22개 단체들이 지지하고 있다.

GILC은 전세계 국가들의 암호정책을 조사하여 분석한 보고서인 "Cryptography and Liberty: An International Survey of Encryption Policy"를 발간하였다. EPIC(Electronic Privacy Information Center)은 GILC으로부터 보고서의 작성을 위촉받아 전세계 230여개 국의 암호정책을 조사하였는데, EPIC은 전세계적으로 온라인 프라이버시의 보호를 위한 기술을 제한하는 국가들은 극소수에 불과하다고 보고하고 있다. 이는 클린턴 행정부가 그 동안 주장한 바와는 전혀 상반되는 것으로 미국 행정부는 줄곧 전세계의 많은 국가들이 미국의 암호정책과 유사한 방향으로 정책을 수립하고 있다고 주장해왔다. 미국 정부에서는 이 보고서는 단지 행정부의 입장을 반대하기 위한 것이며, 대부분의 국가가 암호 제한을 하지 않는 이유는 아직 정보화가 진행되지 않아서 필요성을 느끼지 못하기 때문이라고 반박하였다.

V. 키 복구 방식의 분류

현재 제안된 키 복구 방식은 크게 위탁(Escrow) 방식과 캡슐화(Encapsulation) 방식으로 나눌 수 있다. 본 장에서는 각 방식의 특징에 대해서 논하기로 한다.

1. 위탁방식

위탁 방식은 사용자의 비밀키의 전부 또는 일부를 신뢰 받는 제 3자(Trusted Third Party)에게 위탁하는 방식으로 유사시에 키를 확실하게 얻을 수 있다는 장점이 있다. 이 방식은 유사시에 키를 확실하게 얻을 수 있다는 장점이 있는 반면에, 키를 위탁하는 제 3자의 신뢰도에 많은 영향을 받는다. 또한 이러한 키 위탁 방식에서 위탁되는 키는 대부분 한시적으로 사용되는 세션키(session key)가 아니라 사용자의 개인키(private key)와 같이 긴 주기 동안 사용되는 키(long-term key)가 되므로 신뢰도가 낮은 보관기관을 사용하는 경우에는 많은 문제점이 발생할 수 있다. 미국의 클리퍼 칩의 경우 초기에 정부 기관을 위탁기관으로 선정했으나 사용자들의 강력한 반발로 위탁기관을 민간 부문으로 이전하기도 했었다.

또한 위탁방식을 사용할 경우 제 3자의 신뢰도 뿐만 아니라 사용자들이 위탁한 키의 안전한 보관과 관리 문제, 키가 법률 기관에 의해 합법적인 도청 목적으로 공개되었을 경우에 키의 사용기간의 제한 등이 중점적인 문제로 등장한다. 부가적으로는 키를 사용자가 생성해서 위탁할 것인지, 위탁 기관이 생성한 후에 사용자에게 알려줄 것인지 등에 관한 문제가 있다.

위탁 방식에서는 키 위탁 기관의 신뢰도를 높이고 키 정보가 집중되어 공격목표가 되는 것을 막기 위해서 비밀 분산 방식(Secret Sharing Scheme)을 사용하여 위탁된 키를 여러 기관에 분산시키는 방식 등이 사용되고 있다.

이 방식을 사용하는 경우에는 복구 필드와 같은 부가 정보가 없으므로 현재 나와있는 기존의 모든 프로토콜에 별다른 수정없이 적용할 수 있다. 따라서 키 복구를 지원하지 않는 제품과의 상호 작용에도 별다른 문제점이 없어서 쉽게 적용이 가능하다는 장점이 있다.

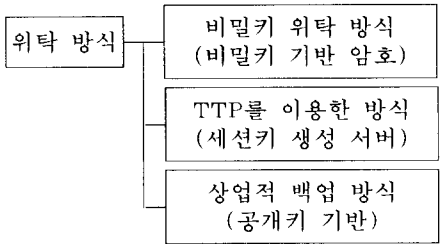


그림 1. 위탁 방식의 분류 및 방식

2. 캡슐화 방식

캡슐화 방식은 각각의 메시지 전송 또는 파일 저장시 마다 키 복구 필드를 생성해서 해당 메시지를 복구할 수 있는 정보를 데이터에 부가하는 방식으로 실제적인 키 위탁은 일어나지 않는다는 장점이 있다. 이처럼 키 복구에 필요한 정보를 담은 영역을 키 복구 필드(Key Recovery Field, KRF) 또는 데이터 복구 필드(Data Recovery Field, DRF)라고 하며, 유사시에 키의 복구가 필요한 경우 복구 기관이 가지고 있는 복구 키를 이용해서 키 복구 필드를 복호한 후 해당 키를 얻을 수 있다.

이 방식의 장점은 복구할 수 있는 정보가 사용자의 비밀키(private key)가 아니라 한시적으로 사용되는 세션키(session key)이기 때문에 합법적인 도청시에 도청 기간의 제한이 가능하다는 것과, 모든 복구 정보는 특정 기관에 위탁되지 않고 사용자의 데이터와 함께 존재하기 때문에 사용자 입장에서는 보다 안전하다는 확신을 가질 수 있다는 점이다. 또한 복구 필드에 들어가는 정보를 일정 수준으로 제한함으로써 복구 기관의 능력을 조절할 수 있다. 예를 들면, 복구 필드에 키의 부분 정보만을 넣어서 일정 능력이상의 복구 기관만이 해독할 수 있도록 한다거나, 몇 개의 복구 기관이 협력해야 키를 얻을 수 있도록 하는 것과 같은 방식을 취할 수 있다.

이 방식의 문제점은 복구 필드의 생성이 대부분 사용자 측(사용자의 암호화 제품 등)에서 일어나게 되므로 제품을 조작하거나 수신자와 공모한다면 복구 필드의 수정과 조작이 가능하다는 점이다. 키를 얻을 수 있는 확실성이 떨어질 수 있다

이 방식을 사용하면 기존의 프로토콜외에 복구 필드와 같은 부가 정보가 필요한데, 이것은 프로토콜 자체가 확장형식(extension format)을 지원하는 경우에는 이것을 이용하면 되지만, 그렇지 않은 경우에는 키 복구를 지원한지 않는 제품(Non-Key Recovery Product)와는 호환성에 문제가 생길 수 있다.

3. 기타

이 밖에도 키 복구와 관련된 여러 가지 대안들이 제안되었는데, 통신시 마다 세션키를 신뢰 서버가 생성해서 사용자에게 분배하는 방법, Ronald L. Rivest 등이 제안한 Translucent Cryptography 방식 등이 있다. 신뢰 서버를 사용하는 방식은 사용자가 암호 서비스를 사용하기 위해 항상 서버에 접속해서 작업을 수행하고, 서버는 사용자의 작업마다 세션키를 생성하고, 해당 세션키를 사후를 위해 저장하는 방식이다. Translucent Cryptography 방식에서는 OT(Oblivious Transfer) 방식을 이용해서 1/p의 확률로 메시지를 검사하여 암호문의 오용을 방지하는 기법을 사용한다. 여기서는 확률 p를 적절히 조절함으로써 사용자와 정부의 요구 사항을 적절히 만족시킬 수 있다고 제안하였다.

키 복구 방식은 일반적으로 위탁과 캡슐화의 두가지 방법을 적절히 조합하는 경우가 많다. 예를 들면, 위탁 방식에서도 알고리즘이나 사용자의 신원 확인을 위해 복구 필드를 부가하는 경우가 있을 수 있다. 두 방식의 장단점을 다음의 표에 정리 하였다.

표 1. 위탁 방식과 캡슐화 방식의 비교

	위탁 방식	캡슐화 방식
키 정보	사전에 특정 기관에 위탁	암호화된 데이터에 부가
복구 키	키 복구 키(Key Recovery Key) 또는 비밀키	세션키(Session Key)
장 점	- 유사시 확실한 키 복구 보장 기존 프로토콜과의 호환	- 사용자의 프라이버시 보호 - 복구 정보를 조절하면 복구기관의 능력 제어가 가능
단 점	- 사용자의 비밀키 노출에 대한 거부감 - 비밀 정보의 집중(위탁기관) - 위탁된 키의 관리 부담	- 복구 정보의 수정 또는 조작이 용이 - 기존 프로토콜과의 호환성(프로토콜에 확장 영역이 존재하면 호환됨) - 복구 키(일반적으로 복구기관의 비밀키)에 대한 관리
사용제품	- Clipper - Fair Cryptosystems - Yaksha Security System	- TIS RecoverKey - IBM SecureWay - AT&T CryptoBackup

VI. 키 복구 시스템

본 장에서는 현재 사용중인 시스템 중에서 몇 가지 방식의 구성 방법과 동작 과정을 살펴보기로 한다.

1. Fair Cryptosystem

1992년 Silvio Micali가 제안한 이 방법은 개인의 프라이버시와 정부의 법 집행 권한을 적절하게 보장해 주기 위해 기존의 암호 시스템을 공정(fair)하게 만들어 주는 방식이다. 즉, Fair Cryptosystem이란 불법적인 도청의 방지와 합법적인 도청의 용이성을 보장 해주는 암호 시스템이라고 할 수 있다.

이 암호 시스템을 사용하면 적당한 환경하의 제 3의 집단이 암호문을 복호 가능하거나, 두 사용자가 비밀통신에 키 복구 암호시스템(Fair Cryptosystem)을 사용하지 않고 있다는 증거를 얻을 수 있도록 설계되어 있다.

1) Fair Cryptosystem의 동작

Fair Cryptosystem은 키를 안전하게 위탁하고 위탁된 키가 오용되지 않도록 구성된 방법이다. 이 시스템은 사용자, 다수의 키 위탁기관, 그리고 인증 기관으로 구성된다. 이 암호 시스템에서 공개키 인증을 받기 위한 과정은 다음과 같다.

먼저 사용자는 주어진 공개키 시스템 내에서 자신의 공개키와 비밀키 쌍을 생성한다. 그런 다음 먼저 비밀키를 여러 개의 조각으로 분할하고, 각각이 원래 비밀키의 조각이라는 것을 확인할 수 있는 확인 정보를 생성해서 다수의 위탁기관에게 보낸다. 각 위탁기관은 수신된 키 정보를 확인하고, 인증기관에게 자신에게 비밀키의 일부가 올바르게 위탁되었다

는 것을 알려준다. 인증기관은 다수의 위탁기관에서 충분한 키가 위탁되었다는 것을 확인했을 때 사용자의 공개키를 인증해 준다. 이를 좀 더 자세하게 살펴보면 다음과 같다.

사용자 X의 공개키를 P_x, 비밀키를 D_x, 위탁기관을 $T_i(i=1, 2,..., n)$, 그리고 인증기관을 C라고 할 때 비밀키 D_x를 다음과 같은 속성을 만족하도록 여러 개의 비밀키 조각 정보 $D_{xi}(i=1, 2, ..., n)$로 분리한다.

- 속성 1. 비밀키 D_x는 n개의 비밀키 조각 D_{xi}를 모으면 다시 구성된다.
- 속성 2. n-1개 이하의 수열은 비밀키를 다시 만들 수 없다.
- 속성 3. 각각의 비밀 조각 정보 D_{xi}에 대해서 각각이 비밀키의 일부가 맞다는 증명을 할 수 있어야 한다.

사용자는 이렇게 분리된 비밀키 조각 D_{xi}을 위탁기관 T_i에게 각각의 D_{xi}가 올바르다는 것을 확인할 수 있는 증명정보 E_{xi}와 함께 전송한다.

각 위탁기관 T_i들은 사용자로부터 받은 비밀키 조각 D_{xi} 가 증명정보 E_{xi}로 올바르다는 것이 확인되면 두개의 쌍 (E_{xi}, D_x)를 안전하게 보관한 후에 승인 정보를 인증기관에게 보내준다. 인증기관 C는 모든 T_i가 승인한 공개키는 승인하고 이 키가 Fair PKC에서 사용자 X의 공개키가 된다.

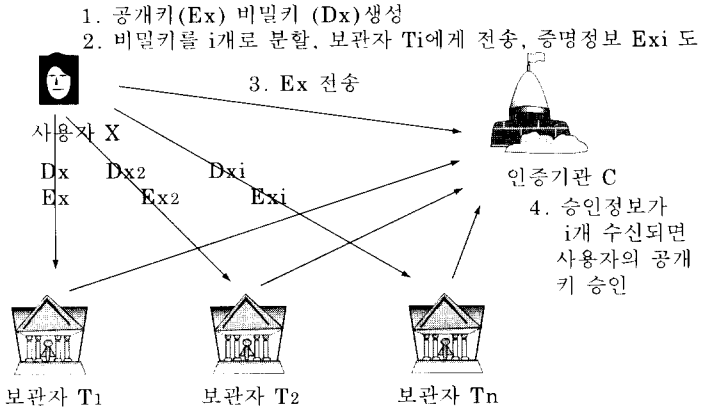


그림 2. Fair Cryptosystem의 키 위탁 및 승인 과정

2) 복구 과정 및 안전도

유사시에 키 복구가 필요하게 되면 인증기관 또는 제 3의 복구 기관이 각 위탁기관에 위탁되어 있는 키 정보들을 취합해서 비밀키를 복원하고, 이를 이용해서 메시지를 복구할 수 있다. 키의 위탁시에 각 보관자에게 전송되는 비밀키의 일부분과 증명 정보인 (D_{xi}, E_{xi})는 비밀키 D_x를 계산하는데 아무런 도움을 주지 못한다. 마찬가지로 인증기관 C도 공개키 P_x로부터 비밀키 D_x를 구할 수 없다. 따라서 이 과정은 비밀키의 노출을 막을 수 있고 본래의 Diffie-Hellman과 같은 비도를 갖는다. 또한 인증기관 C가 법원의 허가를 받은 경우에 정부는 각 보관자의 비밀키를 합해서 비밀키를 쉽게 복원할 수 있다. 이 방법은 RSA, Diffe-Hellman 방식 등에 쉽게 적용시킬 수 있다.

2. RecoverKey

RecoverKey는 미국의 TIS(Trusted Information Systems)사가 개발한 상업용 키 복구 제품으로 국내용과 수출용 버전이 있다. 국내용(미국) 버전의 경우 키 복구 필드를 선택적으로 붙일 수 있지만, 수출용 버전의 경우에는 항상 복구 필드를 생성해서 덧붙이도록 설계되어 있다. 이 기술은 데이터 저장과 통신에 이용할 수 있으며 복구기관의 공개키로 데이터 암호화 키(Data Encryption Key)를 암호화해서 복구 필드 내에 포함시킨다. 나중에는 이 복구 필드를 이용해서 키를 복구할 수 있다.

이 방식에서는 키 복구를 구현하기 위해 키 복구 센터(Key Recovery Center, KRC)라고 불리는 신뢰기관을 이용한다. 이 방식은 데이터의 암호화에 사용되는 키가 해당 메시지의 암호화할 때마다 데이터에 부가되므로 사전에 어떤 키 위탁도 할 필요가 없다. RecoverKey에 사용되는 알고리즘은 데이터 암호화에 RC2, RC4, DES 등이 사용되며, 공개키 방식의 암호는 RSA를 사용한다. 이 방식은 키 복구 센터를 사용자가 선택할 수 있다.

1) RecoverKey의 동작

이 방식은 사용자 등록과 데이터 저장, 통신의 세단계로 나눌 수 있다. 먼저 모든 사용자는 복구 시스템을 사용하기 전에 사용자 등록을 거쳐야 하는데 다음과 같은 과정을 거친다.

사용자는 먼저 키 복구기관(KRC)의 공개키를 요청해서 KRC의 공개키를 얻어온다. 사용자는 다시 이 키를 가지고 자신의 키에 대한 접근 권한 정보인 Access Rule을 암호화하여 자신의 공개키와 함께 복구 기관에게 제공한다.

복구기관은 이것을 자신의 안전한 데이터베이스에 저장한 후 사용자에게 저장된 데이터베이스의 인덱스인 ARI(Access Rule Index)를 암호화해서 전송한다. 이 인덱스는 32비트로 이루어져 있으며 이것은 사후에 사용자를 식별하고, 사용자의 접근이 유효한지 확인하는 데 사용된다.

등록된 사용자는 파일을 암호화할 때 세션키를 생성하여 파일을 암호화하고, 암호화된 파일에 자신이 해당되는 복구 기관의 공개키로 암호화된 세션키를 포함한 복구필드(KRF, Key Recovery Field)를 부가해서 저장한다.

통신 과정은 이와 유사하지만 복구 필드를 복구할 수 있는 복구기관의 수가 늘어날 수 있다. 이것은 수신자의 복구기관과 송신자의 복구기관이 모두 유사시에 해당 메시지를 복구할 수 있어야 하기 때문이다. 또한 통신과정에서는 KVF(Key Verification Field)가 추가되는데 이것은 세션키로 암호화되어서 수신자가 해당 세션키를 먼저 획득한 후 KVF를 스스로 만들어서 이것이 전송된 KVF와 일치하는 것을 확인하는 방법으로 전체 메시지의 복구 필드의 유효성을 확인한다.

2) 복구 과정

이렇게 저장된 파일은 다음의 과정을 거쳐서 복구된다.

- 사용자는 데이터를 암호화한 키가 유실되었을 때 복구필드와 대응되는 인증 정보와 함께 해당 복구 필드를복구기관에게 전송한다.
- 복구 기관은 복구 요청을 인증절차에 따라 검사한 후 올바르면 자신의 비밀키를 이용해서 해당 세션키를 복구한 후 상대방의 공개키로 암호화해서 전송한다.

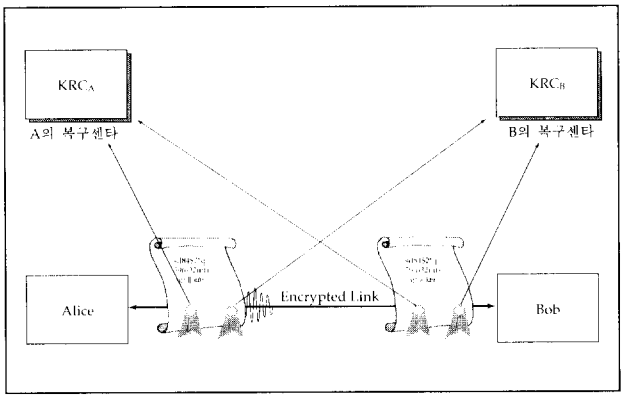


그림 3. RecoverKey의 통신과정

3. CryptoBackup

이 방식은 미국의 AT&T에서 개발된 방식으로 일반적인 데이터 백업과 같이 간편하게 암호학적 키들을 백업한다는 개념을 도입한 방식이다. 이 방식은 기존의 데이터 백업과 같은 정보 유실을 방지하는 역할을 한다고 할 수 있다. 또한 법 집행 목적으로 백업된 키를 사용하므로써 암호의 역기능 문제를 해결할 수 있다. 이 방식에서는 사용자가 몇 개의 백업 키들 중에서 선택할 수 있고, 각 키들은 몇 개의 기관에 공유될 수도 있다.

1) 구성 및 동작 과정

CryptoBackup은 신뢰할 수 있는 백업 기관(Trusted Backup Agent)과 백업용 소프트웨어로 구성되며 백업 기관은 백업용 키인 Public Master Key Vector(Public MKV)를 제공한다. 사용자는 이 시스템을 사용하기 위해서 먼저 백업 기관을 선택하고, 백업 기관에서 제공하는 Public MKV를 백업용 소프트웨어에 설치해서 세션키를 백업하면, 이후에 백업 기관만이 가지고 있는 Private Master Key Vector를 사용해서 복호할 수 있다.

공개키 기법을 이용한 CryptoBackup 시스템을 만들기 위한 방법은 다음과 같다.

함수 $f(x, r)$을 표 2에 나타난 두가지 속성을 갖는 함수일 때 (이와 같은 속성을 갖는 함수의 예를 들면, $x^r \bmod p$ (p는 큰 소수) 등이 있다.) 다음과 같은 방식으로 Crypto Backup이 구현된다.

먼저 백업 기관은 임의의 x와 랜덤수 r_M을 사용하여 자신의 Public Master Key를 정한다.

$$y = f(x, r_M)$$

사용자는 다음과 같은 방식으로 세션키를 생성한다.

$$k = f(y, r_U) \text{ (여기서, } r_U \text{는 랜덤수)}$$

다음과 같은 키 복구 필드 BRV(Backup Recovery Vector)를 암호화된 메시지나 파일에 부가한다.

$$BRV = f(x, r_U)$$

표 2. CryptoBackup에 사용되는 함수의 속성

- 속성 1. 함수 $f(x, r)$은 계산하기 쉽지만 함수의 결과로부터 r을 계산하기는 매우 어렵다. 즉, r은 x가 알려져도 $f(x, r)$의 값으로부터 계산하기가 어렵다.
- 속성 2. 임의의 r_1과 r_2에 대해서 $f(f(x, r_1), r_2) = f(f(x, r_2), r_1)$가 성립된다.

실제 사용될 때에는 사용자와 백업 기관을 식별하기 위한 식별자와 이를 증명할 수 있는 서명 등이 포함된다.

2) 복구과정 및 신뢰도의 향상

함수 f의 두번째 속성을 적용하면, 복구 기관은 BRV로부터 k를 복구할 수 있다는 것을 확인할 수 있다. 그러나 r_M을 알거나 첫번째 속성을 극복하지 못한다면 아무도 이것을 할 수 없다.

한가지 문제점은 이 방식에서 복구 기관이 BRV안에 들어있는 모든 키들을 억세스할 수 있다는 것인데, 이것을 방지하기 위해서 여러 개의 CryptoBackup 기관을 사용하거나 Private Master Key에 대해서 threshold scheme을 사용할 수 있다.

이 방식은 키 위탁 시스템에도 적용이 가능한데, BRV가 법 집행 필드가 되고, 이것을 바탕으로 법 집행을 할 수 있다.

4. Binding Cryptography

이 방식은 1997년 E.R. Verheul 등에 의해 발표된 논문에서 나온 방식으로 TIS와 유사한 공개키 기반의 키 복구 개념에 제 3자가 복구 필드가 올바른지 확인할 수 있는 부가 데이터(Binding data)를 추가한 개념이다. 여기에서는 사용자가 복구필드를 조작해서 키 복구가 불가능하도록 하는 것을 방지하기 위해서 제 3자가 복구 필드의 내용을 알 수 없으면서도 부정행위에 대한 검출이 가능하도록 하였다.

이 방식은 현재 ElGamal 타입의 공개키 암호 개념에 데이터를 바인딩하는 방법이 제시되어 있다.

1) 기존 방식의 문제점

일반적으로 복구 시스템에서 사용자의 암호화된 메시지는 다음과 같은 요소로 구성되어 있다.

$E_K(M) \| E_{\text{수신자의 공개키}}(K) \| E_{\text{복구기관의 공개키}}(K)$ (K : 세션키)

수신자와 복구기관은 각자 자신의 비밀키를 이용해서 세션키 K를 복구할 수 있다. 이 방식에서 사용자는 키를 위탁할 필요가 없다. 단지 통신에 사용되는 임시적인 세션키를 접근할 수 있도록만 해주면 된다. 이러한 개념은 AT&T CryptoBackup, RSA Secure, TIS commercial key escrow 등과 같은 많은 방식의 기본 개념을 이루고 있다. 하지만 이 개념의 중요한 약점은 수신자가 수신하는 세션키와 복구 기관이 수신하는 세션키가 같다는 것을 검사할 수 없다는 것이다. 때문에 이 방식에서는 암호화된 데이터에 두개의 세션키에 관계된 Binding Data를 추가하여 비밀정보의 누출없이 어떠한 제 3자라도 복구 영역의 세션키가 올바른지 검사할 수 있도록 하는 방식을 소개하고 있다.

2) 동작 방식

TRP(Trusted Recovery Party) A가 관장하는 영역에 있는 사용자 Alice가 TRP B가 관장하는 Bob에게 메시지를 보내려고 할 때 다음과 같은 방식으로 구성된다. 여기서 사용되는 방식은 ElGamal 방식의 공개키 개념으로 비밀키 x, 공개키 y ($y = g^x \bmod p$)가 사용된다.

각 TRP의 공개키, 비밀키를 x_A, y_A, x_B, y_B라고 표기할 때 Alice는 랜덤한 k와 세션키 S를 선택하고 다음 내용을 Bob에게 전송한다.

$E = E_S(M)$: 세션키 S로 암호화된 문서

$G = g^k$

$R_{B(B)} = (y)^k \cdot S$: Bob의 공개키로 암호화된 세션키 S

$R_A = (y_A)^k \cdot S$: TRPA의 공개키로 암호화된 세션키 S

$R_B = (y_B)^k \cdot S$: TRPB의 공개키로 암호화된 세션키 S

그리고 마지막으로 제 3자가 수신자와 TRP들이 받는 세션키가 일치하는지 검사할 수 있는 Binding Data를 여기에 덧붙인다.

Alice는 랜덤수 j를 선택하고 제 3자가 복구

필드가 올바른지 점검하기 위해 세션키 확인을 위한 바인딩 데이터(Binding Data)를 구성한다.

Binding Data = (C, D, E, z)

$C = g^j$, $D = (y/y_A)^j$, $E = (y/y_B)^j$, $z = w \cdot k + j \pmod q$

(단, j는 랜덤하게 선택된 임의의 수, w는 해쉬값 E, G, R_M, R_A, R_B, C, D, E와 시간, 신원 정보 등의 공개 정보를 입력으로 해쉬 함수를 취한 값)

3) 복구 과정

수신자인 Bob은 다음과 같은 수식에서 세션키 S를 얻을 수 있다.

$$R_{Bob} / G^y \pmod p$$

A와 B의 복구기관 TRP_A, TRP_B는 다음을 계산해서 S를 얻는다.

$$R_A / G^{xA} \pmod p, \quad R_B / G^{xB} \pmod p$$

제 3자는 다음 수식을 검증해서 2와 3에서의 세션키가 일치한다는 것을 확신할 수 있다.

$$g^z = G^w \times C$$

$$(y/y_A)^y = (R_{Bob}/R_A)^W \times D$$

$$(y/y_B)^y = (R_{Bob}/R_B)^W \times E$$

VII. 결 론

정보화 사회가 발전함에 따라 정보가치의 증가와 이를 안전하게 전송하기 위한 암호 사용에 대한 요구가 점차 많아질 것이다. 암호의 사용시에는 긍정적인 효과 뿐만 아니라 암호를 잘못사용함으로써 발생할 수 있는 부작용을 간과해서는 안될 것이다. 선진국들의 정부는 이미 국가 보안적인 관점과 사회 질서 유지의 관점에서 키 복구 시스템의 중요성을 인식하기 시작하여 이에 대한 표준 개발을 시도하거나 국가적 차원의 정책으로 복구 시스템의 사용을 의무화하고 있기도 하고, 민간 부문에서는 이에 대한 논란이 계속되고 있다.

국내에서는 키 복구 시스템에 대한 관심은 아직 미비한 실정이다. 하지만 가까운 미래에는 이들 선진국 암호 제품의 수입 등을 통해 외국의 복구 시스템이 국내에 유입될 수 있으며 국내의 여러 가지 특수성이나 암호 자체의 안전성 문제 등을 고려한다면 국내에서도 키 복구 시스템이 어떠한 형태로든 사용될 가능성도 있을 것이다. 현재는 이에 대한 인식이 민간이나 기업에서는 충분하지 못하다.

하지만 국내의 암호제품에 대한 잠재수요는 매우 크다고 판단되며, 현재와 같이 국내의 키 관리 체계가 없는 기반에서 키 복구를 수용한 외국 제품이 무분별하게 수입된다면 많은 문제점들이 발생할 것이다. 따라서 국내에서도 키 복구 시스템에 관한 연구 개발이 이루어지고, 이를 기반으로 외국의 키 복구 제품을 수용하는 것이 바람직하다.

장기적인 안목으로는 우리 현실에 적합한 키 관리 기반(Key Management Infrastructure)의 구축이 선행되어야 하고, 이에 따른 한국적인 키 복구 시스템 모델을 구축할 수 있도록 전문가와 복구 서비스를 위한 산업체 등을 육성하는 것이 바람직할 것이다.

또한, 키 복구 시스템은 앞서 말한 바와 같이 충분한 안전도에 대한 고려 없이 시행되어서는 곤란하며, 무작정 외국의 시스템을 도입할 수도 없으므로 민간과 정부 차원에서는 키 복구 시스템에 대한 비용과 안전성에 대한 연구가 이루어져야 한다. 이러한 검토 후에 시스템을 개발하여 시범적인 서비스를 통하여 유용성을 검증하고 법 제도와 관리 방식의 체계를 세워야 할 것이다

참 고 문 헌

[1] Hal Abelson, Ross Anderson, Steven M.Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G.Neumann, Ronald L.Rivest, Jeffrey I. Schiller and Bruce Schneier, "The Risks of Key Escrow and Trusted Third-Party Encryption", 1997. 5

[2] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison and Dvid M. Balenson. " Commercial Key Recovery" , Communications of the ACM, 1986. 3, volume. 39 pp 41-47

[3] David Paul Maher, "Crypto Backup and Key Escrow", Communications of the ACM, 1986. 3, volume. 39, pp 48-53

[4] Ravi Ganesan, "The Yaksha Seurity System", Communications of the ACM, 1986. 3, volume. 39, pp 55-60.

[5] Torben Pryds Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing", Advances in Cryptology-CRYPTO '91 Proceedings, pp 129-140, 1991

[6] Dorothy E.Denning, "A Taxonomy for Key Recovery Encryption System", Communications of the ACM, Vol. 39, pp 34-40, 1996

[7] Dorothy E. Denning and Miles Smid, " Key Escrowing Today" , IEEE Communications, Vol. 32, pp. 58-68, 1994

[8] "Securing electronic mail within HMG part I. Infrastructure and protocol", draft c. http://www.rdg.opengroup.org/public/tech/security/pki/casm/casm.htm, 1996.

[9] Silvio Micali, "Fair Cryptosystems", Advances in Cryptology-CRYPTO '92, 113-138, 1992

[10] Ross Anderson, "The GCHQ protocol and it's problems", EURO-CRYPTO '97, pp. 134-148, 1997

[11] Stephen T. Walker, Stephen B. Lipner, Carl M.Ellison and David M. Balenson, " Commercial Key Recovery" , Communications of the ACM, Vol. 39, pp. 41-47, 1996

[12] Rosario Gennaro, Don Johnson, Paul Karger, Mike Matyas, Mohammad Peyravian, Allen Roginsky, David Safford, Michael Willet, Moti Yung and Nev Zunic, "Secure Key Recovery", IBM Technical document, 1997

[13] Dorothy E. Denning and Miles Smid, " Key escrowing today" , IEEE Communications Magazine, 1994. 9

[14] Joe Kilian and Tom Leighton, "Fair Cryptosystems, Revisited" CRYPTO 95, 1995

[15] A. van Tilborg, "Binding Cryptography: A Fraud-Detectable Alternative to Key-Escrow Solutions," Computer Law and Security Report,January-February 1997, pp. 3-14.

[16] Dorothy E. Denning, "The U. S. Key Escrow Encryption Technology." , Computer Communications, to be published

[17] The White House, Office of the Vice President, "Statement of the Vice President", 1996. 10. 1

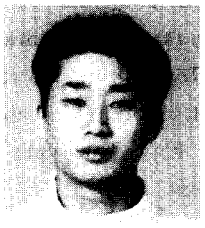
[18] " Trusted Information Systems, Commercial Key Escrow : Something for Everyone, Now and for the Future", TIS Report #541, 1995

[19] 최용락, 소우영, 이재광, 이임영, "통신망 정보보호", 도서출판 그린, 1996

[20] Mihir Bellare and Ronald L. Rivest, "Translucent Cryptography - An Alternative to Key Escrow, and it's Implementation via Fractional Oblivious Transfer, 1996

[21] 이임영, 채승철, Key recovery 시스템에 관한 고찰, 한국통신정보보호 학회지, 제 7권 4호, pp. 45-58, 1997

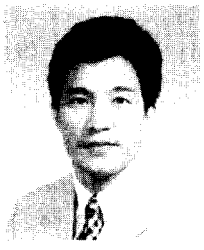
□ 著者紹介



채 승 철

1997년 순천향대학교 전산학과 졸업
1997년 ~ 현재 순천향대학교 전산학과 대학원

※ 주관심분야 : 컴퓨터 보안



이 임 영

1981년 홍익대학교 전자공학과 졸업
1986년 일본 오오사카대학 통신공학과(석사)
1989년 일본오오사카대학 통신공학과(박사)
1989 년 ~ 1994년 한국전자통신연구원 선임연구원
1994년 ~ 현재 순천향대학교 컴퓨터학부 교수

※ 주관심분야 : 암호이론, 정보이론