通信情報保護學會誌
第7卷 第4號. 1997. 12

Key Recovery 시스템에 관한 고찰

A Study on the Key Recovery System

이 임 영*, 채 승 철*

요 약

본고에서는 현재 여러 국가와 기업에서 논의되고 있는 Key Recovery 시스템이 제안된 배경과 미국에서의 시행 정책과 현황 등을 살펴보고, Key Recovery 시스템을 구성하는 주요 요소와 실제 시스템의 구현시에 고려되어야 할 부분들을 보다 일반적인 관점에서 논의하고자 한다.

1. 서 론

사회가 산업사회에서 고도의 정보화 사회로 발전해가면서 많은 정보가 전자적 형태로 변환되어 유통되고 있으며 이러한 정보들은 아주 많은 영역에 관련되어 있다. 개인의 사적인 통화나 편지에서 기업의 유통정보, 국가간의 무역정보, 그리고 교통 제어나 자금 이체 등 거의 모든 분야의 정보가 전자적인 형태로 흘러다니고 있으며, 이러한 경향은 급격히 증가하는 추세에 있다. 이러한 흐름에 따라 각 국가는 정보화의 촉진을 위해 초고속 정보 통신망(Information Super Highway)과 같은 국가 정보 기반(National Information Infrastructure) 구축을 추진하고 있다. 앞으로는 정보화의 촉진이 국가 경쟁력과 직결되기 때문이다.

반면에 정보의 유통량이 많아지고, 정보에 대한 가치가 높아질수록 이러한 정보에 대한 보호 문제가 부각된다. 비록 전자적인 정보유통 기술이 편리하고, 고속화 되더라도 개인의 사생활이 침해받고 기업과 국가의 기밀이 누출된다면 정보망의 이용이 활성화되지 못할 것이기 때문이다. 다시 말하면, 정보 통신 시스템에 대한 안전성 확보가 정보화 촉진의 전제 조건이 되는 것이다.

이러한 문제점을 해결하기 위해 암호학(Cryptology)이 발전하게 되었고, 모든 정보 기술에 암호학적인 기술을 적용하여 정보를 안전하게 보호할 수 있게 되었다. 암호(Encryption)란 키와 알고리즘을 이용하여 평문을 알아보기 힘든 형태로 변환 시키는 방법이다. 만약 안전한 수학적인 알고리즘이 사용되고 안전하게 구현되었다면, 키를 알지 못하는 사람은 암호화된 데이터를 복호할 수 없을 것이다. 암호의 이러한 성질은 데이터의 노출 위험을 제거함으로써 정보 보호에 기여 했으나, 다른 한편으로

* 순천향대학교 컴퓨터학부

는 키 없이는 암호를 해독할 수 없다는 본래의 성질이 다시 문제점으로 제기되는 아이러니한 상황이 발생되었다. 암호화된 데이터의 소유자 자신이나 합법적으로 열람할 수 있는 권한을 가진 사람들 조차도 키의 분실이나 손상 위험에서 안전성을 보장받을 수 없다는 것이 그러한 문제의 요지이다. 이러한 위험에 대한 안전장치가 없다면 암호의 사용 자체가 심각한 사회적 문제 - 키를 훔쳐가거나, 중요한 데이터를 암호화 시켜 무용지물로 만들어 버리는 등의 - 로 제기될 수 있다. 또한 암호가 국가나 시민의 안전을 위협하는 범죄 집단 등에 대한 합법적인 도청이나 수사를 방해하는 수단으로 사용된다면, 이러한 암호는 국가의 법적인 집행력을 약화시키는 도구가 될 수도 있을 것이다. 이것은 개인, 기업, 국가 모두에게 암호 사용을 소극적으로 만드는 요인이 되며, 이러한 문제점을 해결하기 위해 다음과 같은 제안들이 나오게 되었다.

- 허가받지 않은 암호의 사용을 법률로 규제한다.
  암호 통신시 마다 국가의 허락을 얻는 것으로, 허가 받지 않은 암호의 사용을 불법화 함으로써 정부의 통제를 쉽게하고, 암호화의 확산을 억제하므로써 문제 자체를 축소하는 것이다.
- 발표되지 않은 Trapdoor가 있는 암호화 방식을 채택한다.
  국가가 계산할 수 있는 능력은 일반인보다 많기 때문에 이러한 계산량의 차이를 이용하거나, 알고리즘 안에 비밀리에 Trapdoor를 넣는 경우이다. 하지만 Trapdoor가 알려지거나 국가의 계산능력에 버금가는 외부인이 있을 경우에는 매우 심각한 위험을 초래한다.
- 안전한 Key escrow 방식과 관련된 기술의 자발적 채택안을 유도한다.
  Key escrow가 자발적이어야 하는 이유는, 만약 Key escrow를 시행하고자 하면, 법 집행을 하는 국가 입장에서는 모든 암호장비에 빠짐없이 적용하여야 하는데 - 만약 키를 위탁하지 않는 장비를 인정했을 경우, 범죄집단 등은 당연히 그러한 장비를 사용할 것이다 - 정부의 권한으로 실행하게 된다면 민간 부문의 강력한 반발에 부딪히기 때문이다.
- 정부의 개입 없이는 아무것도 할 수 없도록 한다.
  모든 암호화 장비의 등록제 등을 실시하여, 등록되지 않은 장비의 사용을 불법화 하는 것으로 어느 정도의 통제가 가능하다는 것이다. 실제로 프랑스에서는 이러한 정책을 취하고 있다.

본고에서는 .이들 가운데에서 세번째 방법인 Key Escrow(Key Recovery)와 관련된 사항들에 대하여 살펴보고자 한다.

2. Key Escrow의 흐름

Escrow의 사전적 정의는 「other written agreement deposited with a third person, by whom it is to be delivered to the grantee or promise on the fulfillment of some condition」(Webster's encyclopedic unabridged dictionary)으로 우리말로 하면 위탁(委託), 위임(委任)으로 번역할 수 있을 것이다. 그러므로 Key Escrow란 어떤 특정한 조건이 만족되었을 경우에 평문을 쉽게 얻을 수 있도록 제 3자(또는 기관)에게 키를 위임하는 것이다.

Key Escrow는 각각의 상황과 제안에 따라 Key recovery, Trusted-third party, Exceptional access, Lawful access, Data recovery등의 이름으로 사용되고 있다.

정당한 권한이 있을 때 키를 복구해서 암호

를 해독할 수 있는 안전장치에 대한 필요성은 국가에서 먼저 인식하게 되었다. 범죄 집단이나 외국으로 부터의 위협에 효과적으로 대처하고, 합법적인 도청을 보장하기 위하여 미국 정부는 1993년에 Key escrow 정책을 발표하였다. 정책의 요지는 암호화 장비의 비밀키를 정부에 위임해서 정부의 합법적인 법 집행 권한을 보장한다는 것이었다. Clipper Project로 알려진 이 정책은 1993년 4월 16일 클린턴 행정부에 의해서 발표되었으며 이후 계속적인 수정과 보완작업을 거쳐 현재는 Clipper IV까지 알려졌으며 그 내용은 다음과 같다.

Clipper I , 1993년 4월 16일 클린턴 행정부는 민간 부문의 암호 장비 사용을 가능케 함으로서 개인적인 커뮤니케이션을 보호하는 동시에 정부가 적법한 절차에 의거하면 복호화 키에 대한 접근권을 갖는다는 것으로 주요 내용은 다음과 같다.

- SKIPJACK 알고리즘의 사용(알고리즘 자체는 비공개(unclassified))
- 하드웨어적인 구현 (Clipper Chip 사용)
- 전화 통화에 대한 도청이 대상

이 계획은 발표 후 1년 정도의 평가 기간을 거쳐 1994년 2월 백악관은 이의 채택을 발표하였고, 상무성에서는 EES(Encryption Escrow Standard)를 FIPS-185로 승인하였다. 이후에 키 위임 기관(Key Escrow Agent)으로 재무성과 NIST(National Institute of Standards and Technology) 가 선정되었다. 또한 Clipper Chip의 차기 버전인 CAPSTONE Chip을 개발함으로써 도청 범위가 문서 및 일반 데이터에까지 확대되었다.

Clipper I 이라고 불리우는 이 계획은 암호알고리즘인 SKIPJACK 자체가 비밀로 분류되어 공개되지 않았으므로 안전도를 알 수 없고, trapdoor가 존재할 수도 있다는 것과 하드웨어로 구현된 Clipper Chip의 비용과 호환성 문제 등이 지적되었으며, NSA(National Security Agency)가 주도함으로써 민간 부문에서는 사생활 침해에 대한 우려와 함께 강력한 반발을 초래하였다.

Clipper II, 1995년 8월 Clipper I 의 발표 이후 나온 비판을 수렴하여 나온 것으로 그 내용은 다음과 같다.

- 상업적 키 위임(Commercial key escrow) 개념의 발전
- 키가 위임된 암호장비에 한하여 64비트 이하 키에 대한 암호장비의 수출 허용

상업적 키 위임이란 Key escrow가 정부의 법 집행 능력 확보가 목적이 아니라 개인의 키 손실에 따른 위협에 대비한다는 목적을 부각시킨 것인데, 키 위임 기관도 국가 기관이 아니라 민간기관을 허용하겠다는 것이다.

수출에 관한 항목은 기존의 미국의 정책은 암호장비를 무기로 간주하여 미국방성과 NSA의 허가를 얻어야 했으며, 40비트 이상의 키를 가지는 암호화 제품은 수출이 금지되어 있었다. 여기에서는 키 위임을 전제로 64비트의 키를 가지는 암호장비의 수출을 허용한다는 것인데, 커다란 반향을 일으키지는 못했다.

Clipper III, 1996년 5월 20일 Intelligence Working Group on Cryptographic Policy 보고서에서 발표된 것으로 그 내용은 다음과 같다.

- 공개키 방식(Public Key Cryptography)의 중요성 인식
- 키 관리 기반(Key Management Infrastructure) 방식 도입

- 키 관리 기반에 참여하기 위해서는 키를 위임해야 함

이 보고서에서는 키 관리 기반의 도입을 명시했는데 Key escrow를 개인이 키 관리 기반에 참여하는 전제 조건으로 둠으로써 보다 강력한 조건이 추가되었다.

Clipper IV. 1996년 10월 1일 미국의 정보화 부문을 주도하는 고어 부통령이 발표한 것으로 주요 내용은 다음과 같다.

- 향후 2년간 56비트의 키 수출을 허용하지만, 그 이후에는 key recovery를 지원할 수 있는 제품을 만들거나, 업계 자체가 나름대로의 위임 체계를 만들어야 함
- 상업적인 암호 장비는 더 이상 무기로 간주하지 않으며 관장 기관을 국무성(State Department)에서 상무성(Commercial Department)으로 이전
- 적절하지 못한 키 복구를 방지하고, 상업적인 키 복구를 용이하게 하는 법률을 제정
- 국내(미국)에서의 암호는 자유롭게 사용하며, Key recovery 시스템의 국내 사용은 자발적으로 이루어지도록 함

이것은 가장 최근에 발표된 내용으로 이때부터 미국 정부는 Key escrow가 아니라 Key recovery라는 용어를 사용하기 시작하였다. 또한 이 발표에서 관장 기관을 상무성으로 이전하였는데, 기존의 미국에서의 암호장비 수출 허가 과정은 수출업자가 국무성에 속한 Defense Trade Control Office에 요청서를 제출하면, 국무성에서 제고되든지 국방성으로 이관되었다. 전자의 경우는 간단하고 효율적인 절차를 거쳐 대부분 수출이 허가되지만, 후자의 경우는 대부분 긴 절차와 시간을 거치며, 이 과정에서 NSA의 결정이 매우 중요한 영향을 끼친다. 이러한 절차는 강력한 알고리즘을 가진 장비의 수출을 사실상 봉쇄한 것인데, 이러한 규제에 대해 민간기업은 이전부터 규제의 폐지 내지는 완화를 주장하고 있었다. 두번째 조항은 이러한 여론의 수렴이라고 할 수 있지만, 미국 정부의 키 위임 정책에 대한 의지는 변함이 없는 것 같다.

3. Key Recovery 시스템의 구성

Key recovery 시스템은 논리적으로 다음의 세가지 주요 구성 요소로 나뉘어 질 수 있다.

- 사용자 보안 요소(User Security Component, USC)
  데이터 암호화와 복호화 능력을 제공하는 하드웨어 장치나 소프트웨어 프로그램을 말한다. 여기에서 키를 복구할 수 있는 함수를 제공한다. 일반적으로 암호화된 데이터에 DRF(Data Recovery Field)라는 필드를 추가함으로써 복구 능력을 제공한다.
- 복구 기관 요소(Recovery Agent Component, RAC)
  키 복구 기관에 의해 운영되는 이 구성 요소는 키의 저장 장소, Recovery key의 허가와 사용 문제, 그 밖의 복호화를 용이하게 할 수 있는 기타 정보들을 관장한다. 이 구성 요소는 공개키 인증 관리 시스템의 일부가 되거나 KMI(키 관리 기반)의 일부가 되어야 할 것이다.
- 데이터 복구 요소(Data Recovery Component, DRC)
  암호문에 부가된 DRF에서 얻어지는 정보와 RAC에서 제공되는 정보로부터 평

문을 얻기 위한 알고리즘, 프로토콜, 장비 등으로 구성되는 요소이다. 이것은 반드시 허가된 데이터 복구시에만 시행되어야 한다.

이와 같은 논리적 구성요소들은 상당히 밀접한 상호관계를 가지며, 하나가 다른 것에 영향을 미치는 설계 요소가 된다.

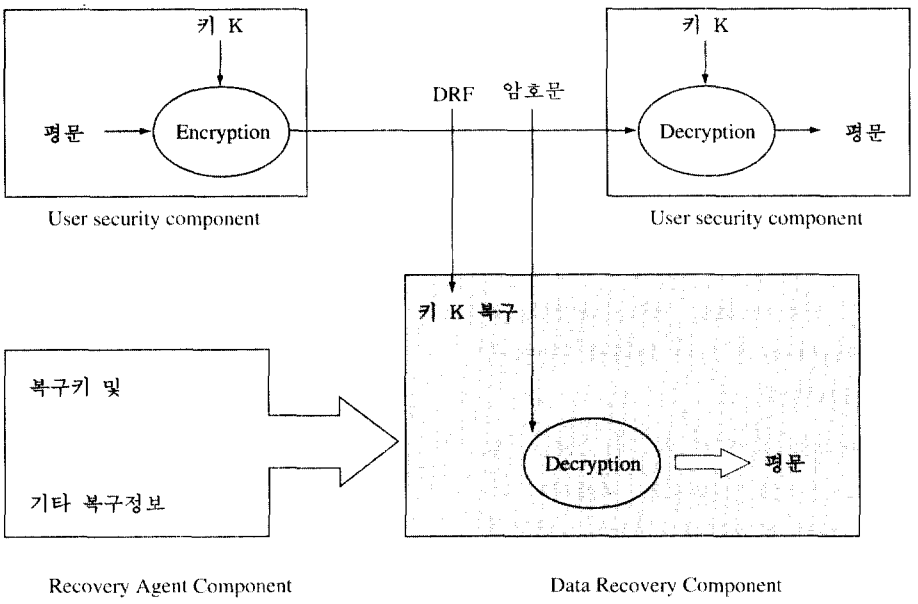


그림 1. Key Recovery 시스템의 구성 요소

그림 1은 이러한 요소들의 상호작용을 나타낸다. USC는 평문을 키 K로 암호화 하고, 암호문에 DRF를 덧붙인다. DRC는 DRF에 담겨진 정보와 RAC가 제공하는 정보를 종합해서 평문을 얻어낼 수 있다.

이러한 세가지 구성 요소는 여러가지 선택사항으로 구성되어 있다.

3.1 사용자 보안 요소(User Security Component)

USC는 암호화와 복호화를 하며, 데이터를 복구할 수 있도록 특정한 함수를 실행한다. 이것은 다음과 같은 특성들에 의해 성격이 좌우된다.

1) 적용 분야

어떤 영역의 키 복구가 가능하도록 만들 것인가를 선택한다. 일반적으로는 통신과 저장된 데이터의 영역으로 구분된다. 통신 영역은 전화 통화나 일반적인 네트워크 통신 같은 일회성 통신과 E-mail과 같이 일시적이지 않은 통신을 모두 포함한다. 저장된 데이터는 단순한 데이터 파일이나 저장된 E-mail과 같은 보다 일반적인 객체이다. 키 복구는 전자의 경우 법원에서 허가된 도청에 한해서, 후자의 경우는 키가 손상/분실 되었을 경우의 데이터의 소유자나 법원의 명령하에서 법 집행 관리에 의해 이루어져야 한다.

2) 데이터 암호화 알고리즘

어떤 암호 알고리즘이 사용할 것인가를 선택한다. 이것은 암호 알고리즘의 조작 방식과 명칭, 암호 키의 길이와 알고리즘 자체를 공개할 것인지, 기밀로 분류할 것인지를 결정한다. 만약 공개된 알고리즘이라면 알고리즘의 독점여부도 결정되어야 한다.

3) 식별자와 키

USC는 비상 상황의 복호화에 쓰이기 위한 식별자와 키를 저장해야 한다.

- 식별자 : 사용자 또는 USC 식별자, 키의 식별자, RAC나 복구 기관을 위한 식별자가 포함된다.
- 키 : USC마다 유일한 키, 사용자가 소유한 키, RAC에 사용되는 전체적인 시스템 키등을 포함한다. 이러한 키들은 공개이거나 비밀이다. 이러한 키들의 복사본이나 비밀키의 사본이 복구 기관에 의해 보관된다.

4) 복구 영역과 메커니즘

데이터가 키 K로 암호화 될 때 USC는 반드시 암호문과 키를 복구하기 위한 정보를 함께 묶어 주어야 한다. 일반적으로는 데이터 복구 필드(DRF)가 암호화된 데이터에 덧붙여진다. 이러한 바인딩은 다음과 같은 특성들에 의해 성격이 좌우된다.

- 어떤 기관이 복호할 것인가 : 비밀키 K는 수신자, 송신자 또는 양쪽 모두의 복구 기관이 가질 수 있다. 이것은 데이터 복구에 영향을 미친다.
- 키 분배의 역할 : DRF와 암호문의 바인딩은 의도적으로 어떤 사람에게 비밀키 K를 전송하는 프로토콜을 사용함으로써 통합될 수 있다. 이 방법에서 송신자는 의도한 사람이 키를 얻을 수 있도록 하기 위해서 반드시 유효한 DRF를 전송해야만 한다.
- DRF의 내용 : DRF는 복구키로 암호화된 비밀키 K 전체를 포함하거나 K의 일부분의 비트 정보를 포함한다. 일부 정보가 제공될 때 나머지 비트들은 Brute force를 통해 결정할 수 있다.
- 전송과 빈도 : 일반적으로 DRF는 메시지의 암호문이나 파일 헤더의 앞에서 전송된다. 만약 유실된다면 일정한 간격으로 재전송된다.
- 유효성 : DRF는 수신자가 DRF가 변경되지 않았는지 확인할 수 있도록 인증자를 포함한다.

5) 상호 운용

USC는 올바르게 동작하는 USC들 사이에서 상호 운용되도록 설계되어야 한다. 부당하게 변경된 USC나 키 복구를 지원하지 않는 USC를 가지고는 상호 운용될 수 없도록 한다.

6) 구현

USC는 하드웨어나 소프트웨어, 펌웨어(firmware), 또는 이들의 조합으로 구현될 수 있다. 하드웨어는 일반적으로 더 안전하며 공격에 대해 더 강하다. 만약 비밀로 분류되는 알고리즘이 사용된다면 그것은 temper-resistant 하드웨어로 구현되어야 할 것이다. 하드웨어로 구현하는 것은 특정한 목적의 암호 프로세서, 랜덤 넘버 생성기를 포함하며, 정밀한 시계를 포함하기도 한다. USC을 구현한 제품을 복구가능한 암호화 제품(또는 장치 recoverable encryption products)라고 부른다. 또는 escrow-

enhanced product나 escrow-enabled product라고 하기도 한다.

7) 보증

USC는 사용자가 키 복구 메커니즘이나 다른 기능을 쓰지 못하도록 만들 수 없다는 보증을 제공해야 한다. 오용될 수 있거나 수정될 수 있는 USC는 rogue USC이라고 하는데, 올바른 USC와 상호작용하는 rogue(single-rogue) USC를 식별할 수 있어야하며, 서로 다른 rogue와 상호작용하는 rogue(dual-rogue)를 구별해 낼 수 있어야한다. single-rogue는 수신자와 협력하지 않고서 속이려고 하기 때문에 유사시의 데이터 복구에 가장 큰 위협이 된다.

3.2 복구 기관 요소(Recovery Agent Component)

RAC는 복구 키와 키 복구에 필요한 다른 모든 정보를 저장해야 할 책임이 있으며, DRC(Data Recovery Component)에서 요구되는 데이터나 서비스를 제공함으로써 DRC를 도와주어야 할 책임이 있다. 이것은 다음의 요소를 가지고 있다:

1) 키 관리 기반 구조(KMI)의 역할

RAC는 KMI의 요소의 하나가 될 수 있다. 이것은 단일키 기반 구조(Single Key Infrastructure)나 공개키 기반 구조(Public Key Infrastructure)가 될 수 있다. PKI의 경우에 복구 기관은 공개키 인증서 발급과 같은 것을 수행할 수 있다. 또는 다른 독립체로 유지될 수도 있다.

2) 키 복구 기관

신뢰받는 기관(trusted parties)이라고 하는 복구 기관은 RAC를 관리해야 할 책임을 가진다. 복구 기관은 USC나 DRC와의 접점으로써 그들의 임무와 운영을 통합하는 키복구 센터(Key Recovery Center)에 등록되어야 한다.

- 복구 기관의 형태 : 복구 기관은 정부기관이나 사적인 부문의 내부 구성원일 수도 있다. 전자의 경우는 정부 기관이 서비스의 사용을 제한할 수 있을 것이며, 후자의 경우는 상업적인 서비스를 제공하는 어떤 독립적인 회사나 조직의 내부에서 상업적 혹은 개인적 키 복구 시스템으로 사용할 수 있을 것이다. 독립적인 복구 기관으로 구성할 수도 있다.
- 식별 능력 : 암호 사용자의 이름과 위치를 식별할 수 있는 능력을 지녀야한다.
- 접근 가능성 : 복구 기관의 위치 (e.g. 국내 또는 국외)와 운영시간에 의해 결정된다.
- 보안성 : RAC가 복구 정보를 합의된 조작이나 손실, 남용으로부터 얼마나 잘 보호하는 지를 나타내는 요소이다. 이것은 신뢰성과 회복성을 포함한다. 또한, 이것은 조작된 정보로부터 복구 정보를 보호하고 데이터 복구를 가능하게 하는 복구 기관에게 요구되는 신뢰성의 척도이다.
- 계정 확인 : 데이터 복구를 일부러 파괴하거나, 허가되지 않은 상황하에서 또는 허가되지 않은 곳에서 키를 공개하는 기관을 식별할 수 있도록 한다.
- 책무 : 양자간의 공모로 인해 키가 바뀌거나 사용할 수 없게 되는 경우에, 복구 기관의 의무를 나타낸다.
- 증명과 허가 : 복구 기관들이 어떤 정부기관으로부터 증명되고 허가되었는지를 나타낸다. 허가 자격을 갖기 위해서 복구 기관은 명시되는 조건을 가져야 할 수도 있다.

3) 복구 키

암호화된 모든 것은 암호화 키에 대한 접근을 용이하게 하는 복구 키와 함께 묶여진다. 복구 키는 다음과 같이 구성될 수 있다.

- 키의 형태 : 데이터 암호화 키, USC에 유일한 제품 키(product key), 사용자 키(암호화를 위해 사용된 public-private 키 쌍의 private 키), 여러 USC에 사용될 수 있는 마스터 키 등이 될 수 있다. 복구키가 사용자 키일 때는 RAC가 공개키 인증국의 역할을 하게 되며 Key escrow라는 용어는 이러한 종류의 시스템에 제한되어 쓰이기도 한다. Key recovery라는 용어는 복구키가 마스터 키일 경우에 주로 사용된다.
- 키의 분할 : 복구키는 여러개의 키로 나누어져서 각각은 분리된 기관에게 보관되어질 수 있다. 키는 쪼개어져서 n개의 복구 기관에 맡겨진 후 다시 키를 회복시킬 때 복구기관 전부가 필요할 수도 있고, "k out of n" 방식으로 n개 중에서 k개만 모이면 키를 복구할 수도 있다.
- 키의 생성/분배 기관 : 키는 RAC나 USC, 혹은 이들의 협조에 의해 생성될 수 있다. 만약 USC에 의해서 생성되었다면 키는 분할되어 VSS(Verifiable Secret Sharing scheme)에 의해 위임되며, 각 위임 기관은 원래의 키를 알지 않고서도 그들이 받은 각각의 조각이 유효성을 검증하게 된다. 키는 공동으로 생성될 수도 있다.
- 보관 시점 : 키는 제품 생산이나 시스템/제품의 초기화, 사용자 등록을 하는 동안 보관되거나 위임된다.
- Key 갱신 : 어떤 시스템에서는 복구키가 변경되는 것을 허용할 수도 있다. 이러한 변경은 사용자의 요청과 어떤 정규적인 기준 하에서 이루어 진다.
- 전체키 또는 부분 키 : 키 전부가 아니라 키의 일부분이 위임될 수 있다. 이러한 경우에 위임되지 않은 부분의 키는 데이터 복구가 필요한 시점에서 Brute force attack을 이용해서 찾아낸다.
- 키의 보관장소 : 이것은 Off-line(e.g. 플로피 디스크 또는 스마트 카드)이나 On-line이 될 수 있다.

4) 데이터 복구 서비스

DRC에게 정보를 공개하는 것과 같은 RAC가 제공하는 서비스이다.

- 인증 절차 : DRC을 운영하거나 사용하는 사람이 RAC의 서비스들을 사용할 수 있는 절차는 신분 증명과 복호된 데이터를 읽기 위한 법적 허가를 얻는 것을 포함해야 한다.
- 제공되는 서비스 : 다음중에서 선택할 수 있다.
  ① 복구키의 공개 : 이 방법은 복구키가 세션 키거나 사용자 키, 또는 제품일때 적용된다.(마스터키는 공개되지 않는다) 키는 후에 자동으로 파기되는 유효기간과 함께 공개되어야 한다.
  ② 파생된 키의 공개 : RAC는 특정한 시간 동안 암호화된 데이터를 복호화가 가능하도록 하는 time-bound key같은 복구키에서 파생된 키를 공개한다.
  ③ 암호화 데이터 복구 키 또는 다른 정보 : 이 방법은 DRF에서 마스터 공개키가 암호화 키로(또는 다른 정보로) 사용되었을 때 사용된다. RAC는 마스터 비밀

키를 DRC에게 주지 않고 복호화를 수행한다.

④ 분할 복호화 수행 : 각각의 복구 기관은 복호화된 조각을 DRC에게 제공한다. 이것들의 조합으로 평문이 얻어진다.

- DRC와의 데이터 전송 : 이 전송은 수동적으로 이루어지거나 전자적으로 이루어질 수 있다.

5) 위임된 키의 안전장치

RAC은 키를 조작이나 손실로부터 안전장치를 두어야한다. 이것은 기술적, 절차적, 법률적인 관점 모두에서 보호 받아야 한다. 예를 들면 지식의 분할, 여러 명의 통제, 물리적 보안, 암호학, 컴퓨터 보안, 시스템의 신뢰도, 검증과 확인의 독립성, 인증, 시스템 설정과 관리, 오용에 따른 제재 등이 있다.

3.3 데이터 복구 요소(Data Recovery Component)

DRC는 DRF에서 얻은 정보와 자신이 가지고 있는 정보를 사용해서 암호화된 데이터로부터 평문을 복구하는 것을 담당한다.

1) 수용능력

- 적절한 시점의 복호
- 통신 도청시의 실시간 복호
- 사후 처리 : DRC는 기록된 이전의 통신에 대해서 복호할 수 있다.
- 투명성 : 복호는 관계된 모임들에 대한 지식 없이 가능하다.
- 독립성 : 키가 한번 얻어지면 DRC는 독자적으로 복호화가 가능한데 이것은 RAC로부터 독립적이다.

2) 데이터 암호화 키 복구

데이터를 복구하려면 DRC는 암호화키 K를 반드시 얻어야 한다. 이때 송신자와 수신자중 어느쪽의 복구 정보를 가지고 있어야 하는 가의 문제와 RAC와의 상호작용 빈도를 결정해 주어야 한다. 일반적으로 실시간 복호를 하기 위해서는 송신자와 수신자 양쪽 모두의 복구 정보를 접근할 수 있어야 하며, 상호작용은 DRC는 하나의 데이터 복구키마다 또는 각각의 USC나 사용자 마다 RAC와 상호작용을 해야될 수도 있다. 세션키가 바뀔 때마다 실시간으로 복호를 하기 위해서는 DRC와 RAC간에 통신로가 구축되어 있어야 한다.

3) 복호화에 있어서의 안전장치

DRC는 복호하는 것을 통제하기 위해서 기술적, 절차적, 법률적 안전장치를 가져야한다.

예를 들면 데이터 복구는 일정한 기간 내에 법정의 허가를 받았을 때에 한해서 가능하다고 제한되어야 한다. 이러한 안전장치는 RAC에 의해 키가 공개될 때의 제한사항을 보충해 준다. 인증 매카니즘은 DRC가 키를 사용하여 조작된 메시지를 생성하는 것을 방지하는데 사용된다.

4. Key Recovery 시스템에 관한 고려사항

앞서 살펴본 Key Recovery System은 몇가지 관점에서의 고려되어야 할 사항을 지니고 있다. 여기에서는 키 복구 능력에 대한 요구사항과 위험요소, 그리고 복잡도와 비용의 네가지 관점에서 알아보고자 한다.

4.1 시스템이 어느 정도의 복구 능력을 가져야 할 것인가.

Key Recovery 시스템을 시행하고자 하는 민간과 정부가 키를 복구하는 목적이 본질적으로 다르므로 요구 사항에 있어 많은 차이점을 보이고 있다. 먼저 정부의 요구 사항을 살펴보자. 정부는 합법적인 방법이라면 개인이나 단체, 기업 등의 암호화된 정보에 접근할 수 있는 보증을 얻기를 바란다. 이것을 위한 정부의 요구사항으로는

- 정부기관이 정보에 접근하는 것은 사용자의 동의없이도 가능해야 한다.
- 정보의 소유자(사용자)는 정부기관의 접근 사실을 인지하지 못해야 한다.
- 어떠한 (시간적, 공간적)상황 속에서도 평문 정보에 가능한 신속하게 접근 가능해야 한다.
- 정보의 형태에 관계 없이 정보를 얻을 수 있어야 한다.

라는 것이 필수적이며, 모든 국가가 키 복구 시스템을 사용하기를 바란다.

그러나 민간의 요구 사항으로는

- 키가 유실/손상되었음을 신속하게 감지할 수 있어야 한다.
- 유실된 키를 신속하게 복구할 수 있어야 한다.
- 키의 손상위협에서부터 정보를 보호할 수 있어야 한다.
- 시행되는 동안의 사생활의 보호와 정보 누출의 방지가 있어야 한다.

등이 있다.

이러한 요구사항은 복구될 수 있는 데이터의 종류, 키의 종류, 복구 가능한 키가 관리되는 방법 그리고 키 인증과 키 복구 사이의 관계 등의 관점에서 크게 차이를 보인다. 실제로 Key Recovery를 어떤 분야에 적용시킬 것인가에 대한 것에서 상호 다른 의견차를 확인할 수 있다. 일반적인 경우의 암호화는 크게 통신분야(Communication)와 데이터(Stored data)의 경우로 나눌 수 있을 것이다.

민간의 입장에서는 거의 모든 것이 일회성에 그치는 통신분야의 경우에 키의 복구가 필요치 않다. 단지 키 유실을 사전에 감지할 수 있는 장치만 있으면 충분하다. 만약 키가 손상되었다면 그것을 감지한 후에 송/수신자간에 새로운 키를 협약해서 사용하면 그만이다. 이것은 제 3자가 필요치 않은 가장 바람직한 방법이다. 지속적인 가용성이 보장되어야 하는 저장된 암호화 데이터의 경우는 어느 정도 키 복구의 필요성이 있다. 하지만 이것 역시도 사용자 스스로가 사본을 주의깊게 관리한다던지, 자신이 신뢰할 수 있는 사람에게 위탁 관리할 수도 있다. Key Recovery는 이중에 선택할 수 있는 한가지 방법일 뿐이다. 하지만 정부의 입장에서는 오히려 일회성 통신에 대해 키 복구 능력을 갖기를 원하며 가능한 모든 암호화 영역과 제품에 Key Recovery를 적용시키기를 원한다.

그리고 암호의 또 다른 적용 분야인 인증에 있어서의 문제이다. 공개키 암호는 전통적인 용도 이외에 메세지의 무결성 확인과 부인봉쇄 등의 기능으로 전자 서명과 같은 분야에 응용되고 있고, 근래에 와서 암호가 상업적인 용도로 쓰이면서 중요하게 부각되는 부분이다. 전자 상거래의 많은 부분은 이러한 인증 기능에 의존하고 있는데, Key Recovery 시스템은 제 3자가 서명을 위조할 수 없다는 부인 봉쇄 기능을 깨트린다.

복구 기관의 신뢰도에 따라 다르겠지만, 근

본적인 전자서명(공개키 암호)의 기능 - 부인봉쇄, 무결성 보증, 사용자 인증 등 -이 약해지는 것이다. 지역적인 복구 기관의 신뢰도는 어느 정도 보장받는다고 해도 국제간의 신뢰도를 보증하는 것은 현실적으로 힘들기 때문이다.

그밖에 공개키 인증을 받기 위해서는 키 위임이 선행되어야 한다든지, 복구 기관의 선정 문제 등은 상기한 요구사항의 차이에서 비롯된 것이다.

4.2 새로운 위험요소

Key Recovery 시스템에는 이전에 겪어보지 않았던 새로운 취약 요소들이 있는데 이것은 앞서 언급된 Key recovery 시스템이 본래의 암호화 시스템의 개념과 상반되는 개념을 포함하고 있다는 본질적인 문제에서 발생한다.

1) 새로운 공격목표

복구 시스템은 복호 정보가 집중되어 있는 곳을 만듦으로써 범죄집단이나 다른 공격자들에게 새로운 공격 목표를 제공하게 된다. 정보의 가치가 재차 언급할 필요도 없이 중요한 것처럼, 이 새로운 공격 목표의 가치도 매우 높다. 하지만 이에 비해서 비교적 많은 숫자의 복구 기관에 대해서 충분히 안전도를 확보하는 것은 어려울 것으로 보인다. 공격자는 여러 개의 복구 기관중 취약한 한개의 복구 기관을 공격함으로써 전체 복구 시스템을 파괴하는 것이 가능하기 때문이다.

2) 내부자의 오용

암호가 잘못 사용되어 질 수 있는 것처럼 복구 정보 역시 고의적이던, 아니던 잘못 사용될 가능성이 높다. 허가된 사용권을 가진 사람이 개인의 욕심이나 이념 또는 타인의 협박이나 강요로 사용권을 오용할 수 있다. 이러한 예는 비슷한 권한을 가진 다른 사람들의 예에서 이미 많이 보아왔다.

또한 내부적인 오용의 문제를 국제적인 관점으로 확대한다면 국가의 이익을 위해 이러한 오용 자체가 정직하지 못한 국가에 의해서 제도화 될 수 있다. 자국의 이익을 위해서 국가의 법적인 장치들이 동의를 할 경우에는 이것이 가능한 것이다.

3) 평문을 얻는 새로운 방법

또 다른 위험 요소는 키 복구를 위한 접근이 사용자의 통제에서 완전히 벗어나 있다는 점이다. 복구를 위한 접근은 설계 당시 부터 사용자에게 숨겨지도록 되어 있으므로 사용자의 실수나 다른 요인에 의해서 키가 공개될 가능성을 배제할 수 없다.

4.3 Key Recovery 시스템의 복잡도

안전한 암호 시스템의 구현은 간단한 알고리즘과 프로토콜을 설계하여 구현할 때에도 매우 복잡하고 정밀한 과정을 거친다. 이때 아주 작은 변화가 주어졌을 때에도 심각한 보안 구멍(Security hole)이 생길 수 있다. 경험적으로 비교적 간단한 요구사항을 가진 암호화 시스템도 실제 구현과 응용에서 문제점이 발견되는 경우가 많다.

이러한 설계와 구현상의 경험을 바탕으로 보았을 때 Key Recovery 시스템이 안전하게 구현되어 의도한 대로 동작하는 것을 보장하기란 매우 어려운 일이다. 키 복구 시스템이 설계 단계에서 부터 하나 이상의 문제점이 잠복되어 있는지를 확인할 수 있는 학문적 도구가 마련되어 있지 않기 때문이다.

이것의 예는 실제로 최근에 시행된 미국의 Clipper chip에 기초한 EES에서 찾을 수 있다. 미국 정부는 NSA가 세계에서 가장 진보된 암

호 기술을 가지고 있다는 것을 믿었고, 국가와 군사적인 비밀 정보의 부분에 그들이 개발한 암호 시스템을 사용하였다. 하지만 클리퍼 칩은 초기 구현 후에 몇가지 문제점들이 발견되었다. 이것은 키 복구 시스템이 지금까지 전혀 검증되지 않았으며, 이전에 고려하지 못했던 많은 복잡도를 포함하고 있기 때문이다.

1) 규모의 복잡도

Key Recovery 시스템이 시행되는 범위와 관련된 것이다. 복구 시스템에서는 수많은 법 집행 기관과 수많은 사용자 그리고 사용자 각각이 소유하고 있는 수개의 비밀키-공개키 쌍을 관리해야하며 전화, 통신등의 각 세션마다, 저장된 각 파일과 E-mail 마다 키들을 복구할 수 있도록 관리해야 할 것이다. 또한 정보사회가 발전할수록 정보량은 증가할 것이고 그에 따라 관리해야 하는 키의 갯수와 관리 기관의 수도 급격하게 증가할 것이다.

2) 운용상의 복잡도

기본적으로 키를 복구하기 위해서는 키를 요구하는 사람/기관의 인증과 식별이 필요하며, 그가 복구할 수 있는 적법한 권한을 갖고 있는지에 대한 확인이 필요하며, 복구 기관은 요구되는 정보를 적당한 형태로(평문이나 복구된 키 등) 올바른 사람에게 적절한 시간내에, 안전하게 전송할 수 있어야 한다. 특히 법 집행을 위한 키의 복구는 빠른 시간내에 이루어져야하는 경우가 많은데, 이것을 위해서는 복구 기관과 복구 정보 요구기관 사이의 통신망이 완비 되어 있어야 한다. 또한 복구 기관에서 정보 요구 기관으로의 전송과정에서의 안전도도 고려되어야 한다.

4.4 Key Recovery 시스템의 비용

비용은 크게 설계비용, 운용비용, 사용자 비용의 증가를 들 수 있는데, 설계비용은 위에서 살펴본 거대한 규모와 안전도를 고려한 키 복구 제품을 설계해야 한다는 점에서, 운용비용의 증가는 복잡도와 운용상에 필요한 제반 통신 설비와 상호 인증을 위한 장치 등의 요구에 기인한다. 또한 사용자들은 키 복구를 보장받기 위해서 원래의 암호시스템의 비용보다 추가된 비용부담을 가지게 된다.

5. 결 론

정보사회가 발전함에 따라 암호 사용의 중요성과 수요는 점차 증가하는 추세이며 국내에서도 역시 마찬가지이다. 이러한 동향을 필연적이고 당연한 결과라고 할 수 있으나, 국내의 경우 사용자측이 국내 제품보다 외국 제품을 선호하는 경향을 보이고 있으며, 이는 외국 제품에 대한 수요로 이어지고 있는 실정이다. 반면에 선진국들의 정부는 이미 Key Recovery 시스템의 중요성을 인식하기 시작하여 미국과 OECD 등을 중심으로 표준안이 제안되고 있으며 민간의 요구에 의해서 점차 많은 상용 제품이 개발되고 있다. 이에 따라 외국의 키위임 제품의 국내 수입이 예상되며 이러한 것에 대한 대비책이 시급하다.

우리나라에서는 아직 암호 제품에 대한 인식이 충분하지 못하고, 보안 마인드의 확산이나 암호 제품의 사용이 미미한 실정이다. 따라서 현재의 상황은 민간 주도의 Key Recovery 시스템을 기대하기는 어렵다. 하지만 국내의 암호제품에 대한 잠재수요는 매우 크다고 판단되며, 현재와 같이 국내의 키 위임 체계가 없는 기반에서 잠재 수요가 실수요로 전환될 경우에는 많은 문제점들이 발생할 것이다. 따라서 국내에서는 정부 차원의 연구 개발이 진

행되어 Key Recovery System을 구축하는 것이 바람직하다고 본다.

장기적인 안목으로는 우리 현실에 적합한 키 관리 기반(Key Management Infrastructure)의 구축이 선행되어야 하고, 한국적인 Key Recovery 시스템을 구축할 수 있도록 키 위임 방식을 체계화 하고, 국제 간의 협약을 모색해야 할 것이다. 이를 위해서는 Key Recovery를 담당하는 기관 또는 부서를 신설하고, 이를 위한 전문가와 Recovery Service를 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 Key Recovery 시스템에 대한 비용과 안전성에 대한 연구가 이루어져야 한다.

이러한 검토 후에 시스템을 개발하여 시범적인 서비스를 통하여 유용성을 검증하고, 법제와 관리 방식의 체계를 세워야 할 것이다.

참고 문헌

[1] 한상근, 이영, "미국의 암호정책에 관한 연구-클리퍼칩을 중심으로", 한국통신정보보호학회지 제 4권 제 4호, 1994. 12

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

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

[4] Adi Shamir, "Prrtial Key Escrow: A New Approach to Software Key Escrow", Notes from the Key Escrow Conference, Washington, D. C., 1995. 9. 15

[5] Dorothy E. Denning, "Timestamps in Key Distribution Protocols.", Communications of the ACM, 1981. 8

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

[7] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.", IEEE Transacions on Information Theory, 1985. 7

[8] M. Hellman, "An Overview of public key Cryptography.", IEEE Communications Magazine, 1978.11

[9] Interagency Working Group on Cryptographic Policy, Enabling Privacy, Commerce, Security, and Public Safety in the Global Information Infrastructure, 1996. 5. 17

[10] SKIPJACK Review Interim Report, 1993. 7. 18.

[11] The White House, Office of the Press Secretary, Statement of the Press Secretary, 1993. 4. 16

[12] The White House, Office of the Press Secretary, Statement of the Press Secretary, 1994. 2. 4

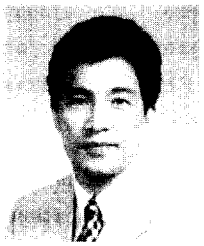
[13] The White House, Office of the Vice President, Statement of the Vice President, 1996. 10. 1

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

[15] D. Denning and D. Brandstad, "A Taxonomy for Key Escrow Encryption Systems", Communications of ACM, VOL 39, No. 3, 1996. 5

[16] Silvio Micali, "Fair Cryptosystems, in Building Big Brother", edited by L. Hoffman, 1995

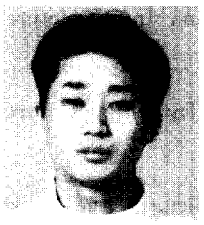
□ 著者紹介



이 임 영

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

※ 관심분야 : 암호이론, 정보이론



채 승 철

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

※ 관심분야 : 컴퓨터 보안