通信情報保護學會誌
第 10 券 第 1 號, 2000. 3

키 복구 시스템의 요구사항에 관한 고찰

유 희 종*, 주 미 리*, 원 동 호*, 김 지 연**, 박 성 준**

요 약

암호가 빠르게 민간에 보급됨에 따라 여러 가지 역기능이 대두되고 있다. 이에 대한 대책중의 하나로 키 복구 정책이 여러 나라에서 고려되고 있으며 다양한 키 복구 제품들도 출시되고 있는 추세이다. 특히 미국에서 키 복구 정책이 활발히 논의되고 있으며 이에 따른 키 복구 제품의 요구사항에 관한 표준안을 NIST에서 제정하였다. 본 고에서는 키 복구 시스템이 갖추어야 할 요구사항을 NIST에서 제안한 조건에 맞추어 분석하였다. 본 고의 내용은 크게 두 가지로 요약할 수 있다. 먼저 미국의 NIST에서 제시한 키 복구 제품의 요구사항에 대하여 살펴본 후 이 요구사항들을 현재까지 제시된 키 복구 시스템에 적용시켜 만족 여부를 분석하였다. 따라서 본 고는 새로운 키 복구 방식의 개발이나 키 복구 제품의 설계에 도움을 줄 수 있으리라 기대된다.

Ⅰ. 서 론

암호화된 통신은 사용자의 프라이버시를 보호하며 비밀 문서의 보관에 좋은 수단이다. 그러나, 암호가 민간에 보급됨에 따라 암호의 긍정적인 기능 뿐 아니라 암호의 역기능도 부각되었다. 다시 말해 범죄자들의 암호 이용과 키의 분실, 손상 등에 따른 암호문의 복호 불가 등이 그것이다. 이에 대한 대책으로 현재 키 복구에 대한 연구가 세계적으로 활발히 진행 중이며, 다양한 정책이 제시되고 있다. 또한 현재 여러 가지 키 복구 제품들이 출시되었거나 개발중에 있다.

1998년 미국의 NIST(national institute of standards and technology)에서는 연방 정부에서 사용될 키 복구 제품에 대한 요구사항을 명세한 요구사항[11]을 제시하였다.

NIST에 의해 제시된 요구사항에서는 키 복구 기술의 향후 발전을 도모하기 위해 그 적용 범위를 특정 키 복구 기술로 한정하지 않았으며, 모든 키 복구 시스템에 적용이 가능한 일반적인 모델을 제시하였다. NIST의 키 복구 모델은 키 복구 시스템을 크게 다음과 같이 나누고 있다.

- 키 복구 정보 생성(key recovery information generation)
- 키 복구 정보 관리(key recovery information management)
  - 키 복구 정보 전달 기능
  - 키 복구 정보 검증 기능
- 키 복구(key recovery)
  - 키 복구 요청 기능
  - 키 복구 대행 기능

NIST의 키 복구 제품에 대한 요구사항은 키 복구 시스템을 구현한 제품에 대해 기능, 보안, 보안 확신, 상호운용 요구사항을 적용하고 있다.

본 고에서는 NIST의 요구사항을 살펴보고 이를 현재까지 제시된 여러 가지 키 복구 시스템들에 적용하여 만족여부를 분석하였다. 본 고의 2장에서는 NIST가 제시한 키 복구 시스템에 대한 요구사항에 관해 알아보고, 3장에서는 일반화된 키 복구 시스템 모델을 간단히 살펴보며, 여러 가지 키 복구 기술들을 NIST에서 제시한 키 복구 모델에 적용시켜 설명한다. 마지막으로 4장에서는 2장에서 언급된 요구사항들에 대한 각 키 복구 기술의 만족여부에 대해 알아본다.

* 성균관대학교 전기 전자 및 컴퓨터 공학부
** 한국 정보 보호 센터
※ 이 원고는 1999년 한국정보보호센터의 과제(98-260-07)에 의하여 연구되었음

II. NIST의 키 복구 제품 요구사항

암호는 전송 또는 저장 데이터의 기밀성을 유지하는 중요한 수단이다. 적당히 강력한 암호 알고리즘이 어느 정도의 안전성을 가지고 사용되고 구현되었을 때, 암호는 권한이 없는 사용자들에게 전송 또는 저장된 데이터가 노출되는 것을 막을 수 있다. 그러나 암호화된 데이터를 복호하는데 필요한 키의 손상이나 분실 등은 정당한 사용자들이 복호하는 것을 막을 수 있다. 그러한 상황에서 정당한 사용자들이 암호화된 데이터에 접근할 수 있도록 돕기 위해 이 표준은 키 복구 제품에 대한 요구사항을 제정한다.

NIST의 요구 사항은 연방 정부 기관에 의해 사용되는 키 복구 제품이 만족해야 할 요구사항에 대한 명시이다. 평가 제품은 하나 이상의 키 복구 시스템 기능을 구현해야 하나 한 제품이 KRS(키 복구 시스템 : key recovery system)의 모든 기능을 구현할 필요는 없다. 그러한 제품들은 데이터에 대한 접근이 적당하게 인가되었을 경우에 한해서 암호화되어 저장되었거나 통신중인 데이터의 복호를 위해 사용되는 키의 복구 기능을 제공한다.

1 사용된 용어와 범위

- Key Recovery System(KRS, 키 복구 시스템) : 복호화 키를 얻을 수 없을 때 정당한 사용자가 암호화된 데이터에서 평문을 복호할 수 있도록 하는 시스템
- Key Recovery(KR, 키 복구) : 수많은 키 복구 기술에 적용하는 광범위한 용어
- Target key : 각 키 복구 기술이 복구하고자 하는 키는 다음과 같다.
  - 데이터 복호에 사용될 수 있는 데이터 암호화 키(DEK, data encryption key) 혹은
  - 암호화된 DEK를 (직/간접적으로) 복호하는데 사용될 수 있는 키
- Key Recovery Information(KRI, 키 복구 정보) : Target key를 복구하기 위해 키 복구 기술이 필요로 하는 정보의 집합
- KRI Management
  - KRI의 존속 기간 : brief time during transmission, long time in storage
  - KRI의 저장 장소 : KRA(≥1), 메시지에 첨부, 단말 사용자 시스템, CA 등

이 요구사항에 언급된 두 가지 키 복구 기술은 KRA가 DEK를 복구하도록 암호화된 데이터에 KRI를 첨가시키는 기술인 캡슐화 방식과 KRA가 단말 암호 장치의 키(일반적으로 공개키/비밀키 쌍과 같은 long term key)에 직접 접근할 수 있도록 하는 기술인 키 위탁 방식이며 TTP(trusted third party)-기반의 방식은 언급되지 않았다. 그러나 본 고에서는 이 방식에 대한 NIST 키 복구 제품 요구사항 분석도 적용하였다.

2. NIST의 키 복구 제품 요구사항

NIST의 키복구 제품 요구사항은 모두 208가지의 항목으로 구성되며 다음으로 분류될 수 있다.

- 기능 요구사항(요구사항 5~24)
  : 키 복구 시스템의 동작에 필수적인 기능적 요구사항 제시
- 보안 요구사항(요구사항 25~174)
  : 각 키 복구 시스템 기능에 대해 적용
  : 암호 알고리즘의 강도, 감사 사항 등에 대한 요구사항
  : 세 개의 레벨로 분류(level 0, level 1, level 2)
- 보안 확신 요구사항(요구사항 175~208)
  : 키 복구 시스템 기능을 구현하는 데 적용되는 요구사항(level A, level B, level C)
  : 제품의 구성, 배달, 작동법, 안내문서 등에 관한 사항으로 구성
- 기타 요구사항(요구사항 1~4)
  : 다른 키 복구 기술간의 상호 운용에 대한 요구사항 및 키 복구 시스템에 대한 일반적 요구사항 제시

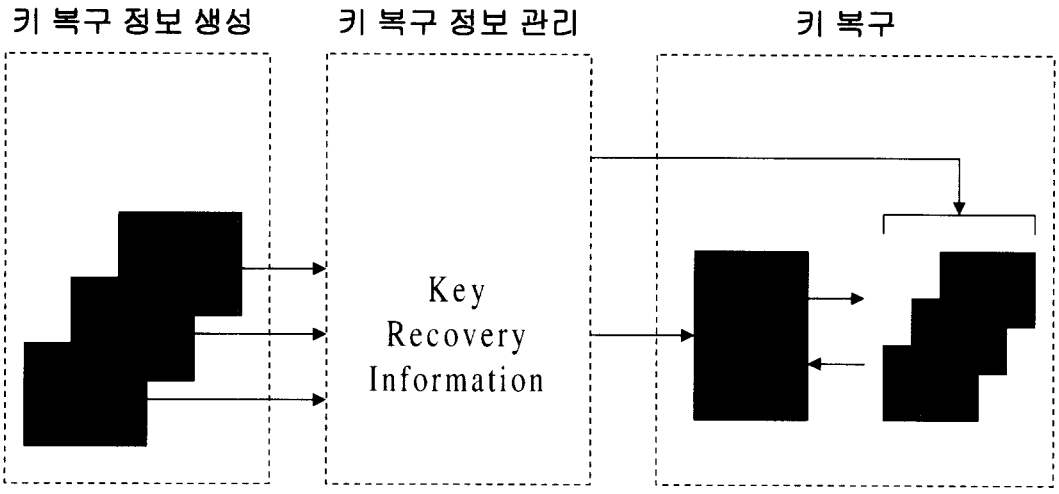

그림 3.1. 키 복구 시스템의 일반적 모델

Ⅲ. 기존의 키 복구 제품 기능 분석

본 고에서는 키 복구 방식을 세 가지로 분류하며 현재까지 제안된 각 방식의 대표적인 제품이나 프로토콜을 다음과 같이 분류하였다.

- 키 위탁 방식
  - EES(escrowed encryption standard)
  - TIS Software Key Escrow
  - Active Investigator
- 캡슐화 방식
  - Commercial Key Escrow
  - Traceable Ciphertext
  - Binding Cryptography
- TTP 기반의 키 복구 방식
  - GCHQ 키 복구 방식
  - 수정된 GCHQ 키 복구 방식

키 복구 시스템(KRS)은 복호화 키를 사용할 수 없는 경우에 정당한 권한이 있는 사람으로 하여금 암호화 데이터에서 평문을 복호해 낼 수 있도록 하는 시스템으로 키 복구라는 용어는 다양한 키 복구 기술(예 : 키 위탁, 캡슐화 등)에 광범위하게 적용될 수 있다. 각 키 복구 기술은 target key라 불리는 키의 복구를 목적으로 하며, target key는 다음과 같다.

- 데이터를 복호하는데 사용되는 데이터 암호화 키(DEK) 혹은
- 암호화된 DEK를 복호하는데 사용되는 키

Target key를 복구하기 위해서 필요한 정보는 각 기술마다 다르며, 그 정보들을 키 복구 정보(KRI)라고 한다. Target key 복구를 위해 필요한 정보인 키 복구 정보들은 키 복구 기술에 따라서 암호문이 전송되는 짧은 기간 동안만 존재할 수도 있고, 암호문이 저장되어 있는 비교적 긴 기간 동안 존재할 수도 있다. 또한 하나 이상의 KRA에 분산되어 존재하거나 사용자 단말 시스템, 제 3의 기관 시스템, 또는 신뢰기관내의 메시지에 덧붙여진 형태로 존재할 수 있다.

그림 3.1은 키 복구 정보 생성, 키 복구 정보 관리, 키 복구의 세 부분으로 이루어지는 키 복구 시스템의 일반적 모델을 나타내고 있다. 키 복구 정보 생성은 하나 이상의 키 복구 정보 생성 기능에 의해 수행되며 키 복구 정보 관리는 키 복구 정보 전달 기능과 키 복구 정보 검증 기능에 의해 수행된다. 마지막으로 키 복구는 키 복구 요청 기능과 하나 이상의 키 복구 대행 기능에 의해 수행된다.

일반화된 키 복구 시스템(KRS)의 구성은 다음과 같다.

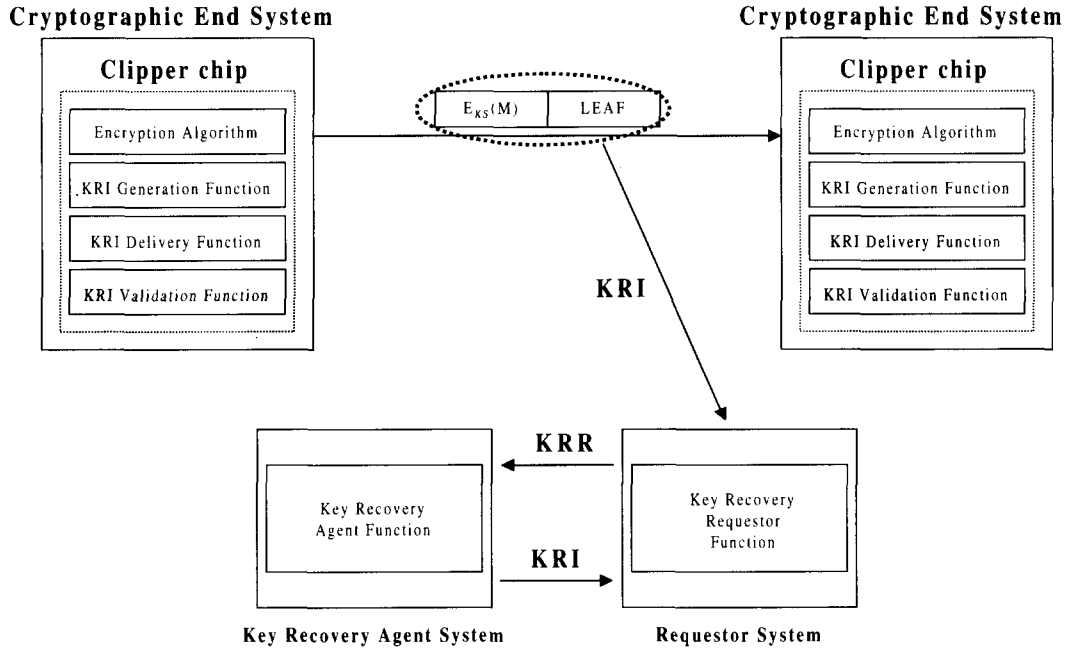

그림 3.2. EES 기능 블록도

- KRS = KRI Generation + KRI Management + Key Recovery
  - KRI Generation(KRI 생성) : 하나 이상의 KRI Generation Function에 의해 수행
  - KRI Mgmt.(KRI 관리): KRI Delivery Function과 KRI Validation Function (선택적)에 의해 수행
  - Key Recovery : Key Recovery Requestor Function과 하나 이상의 KRA Function에 의해 수행

키 복구 시스템은 여러 장소(예 : 암호 단말 시스템, KRA 시스템, KRR 시스템, 저장 또는 전송 매체)에 걸쳐서 존재할 수 있다. 또한 키 교환 메커니즘이 키 복구 메커니즘에 의존할 필요는 없으며,키 교환 메커니즘은 KRI를 생성하거나 분배하는 데 사용될 수 있다.

1. 키 위탁 방식

키 위탁 방식은 복구될 사용자의 비밀키, 비밀키의 부분 또는 키 관련 정보를 하나 이상의 신뢰기관에 위탁하는 방식으로 위탁되는 키는 사용자가 오랫동안 사용하게 되는 키(long term key)이다. 이 방식에서는 사용자의 비밀키가 위탁 기관에 직접 맡겨져야 하므로 개인의 프라이버시가 전적으로 위탁 기관에 의존한다는 문제점을 안고 있다. 그러므로 위탁 기관의 신뢰성이 매우 중요한 문제이며 이를 보장하기 위한 방법으로 두 개 이상의 위탁기관을 이용하는 비밀 분산 개념이 주로 사용되고 있다. 또한 법 집행기관에 의해 복구되는 키가 사용자의 long term 키가 아닌 일정 기간동안만 사용하는 세션키가 되게 한다면 사용자들의 프라이버시 침해에 대한 거부감 문제도 어느 정도 해결이 가능하다. 그러나 위탁되는 키의 유효성에 대한 문제도 해결이 되어야 한다는 문제도 있다.

반면에 이러한 키 위탁 방식은 유사시에 키 복구를 확실하게 할 수 있다는 장점이 있으며 위탁 기관의 신뢰성만 보장된다면 편리하고 안전한 키 복구 방식이다.

1.1 EES[1]

EES는 NIST에서 제시한 키 복구 시스템 모델에 그림 3.2처럼 대응될 수 있다. EES에서는 각 사용자의 암호 단말 장치에 내장되어 있는 tamper-proofness 칩(예 : clipper, capstone)에서 암·복호화 및 KRI 생성, 전달, 검증 기능이 수행된다. 법 집행 기관은 송수신자들 사이에 전송되는 암호문과 그 암호문에 덧붙여져 전송되는 KRI, 즉 LEAF를 감청하여 LEAF내에 포함되어 있는 정보를 이용하여 각 KRA에 키 복구 요청을 하는 KRR 기능을 수행하게 된다. 법 집행 기관으로부터 키 복구 요청을 받은 KRA, 즉 각 Escrow Agent는 그 요청에 알맞은 키 복구 정보를 법 집행 기관에 제공한다.

1.2 TIS Software Key Escrow[3]

TIS사에서 제안한 Software Key Escrow 방식은 기본적으로는 EES 방식을 따르고 있으나 EES에서 하드웨어로 구현되었던 키 복구 기능들을 소프트웨어로 구현하였으며, LEAF의 생성 및 검증에 공개키 방식을 이용하고 있다. LEAF의 생성 및 검증에 공개키 방식을 이용함으로써 M. Blaze의 공격을 부분적으로 해결한 이 방식은 그림 3.3에서처럼 NIST의 키 복구 시스템 모델에 적용시킬 수 있다.

그림에서 보는 것처럼 TIS Software Key Escrow 시스템은 사용자 단말에 위치한 키 복구 기능이 하드웨어가 아닌 소프트웨어로 존재하며, 키 복구 정보의 구성이 다르다는 점을 제외하면 EES의 모델과 흡사하다.

1.3 Active Investigator[4]

P. Horster, Markus Michels, Holger Petersen이 제안한 이 방식은 EES등의 방식에서 키가 한 번 복

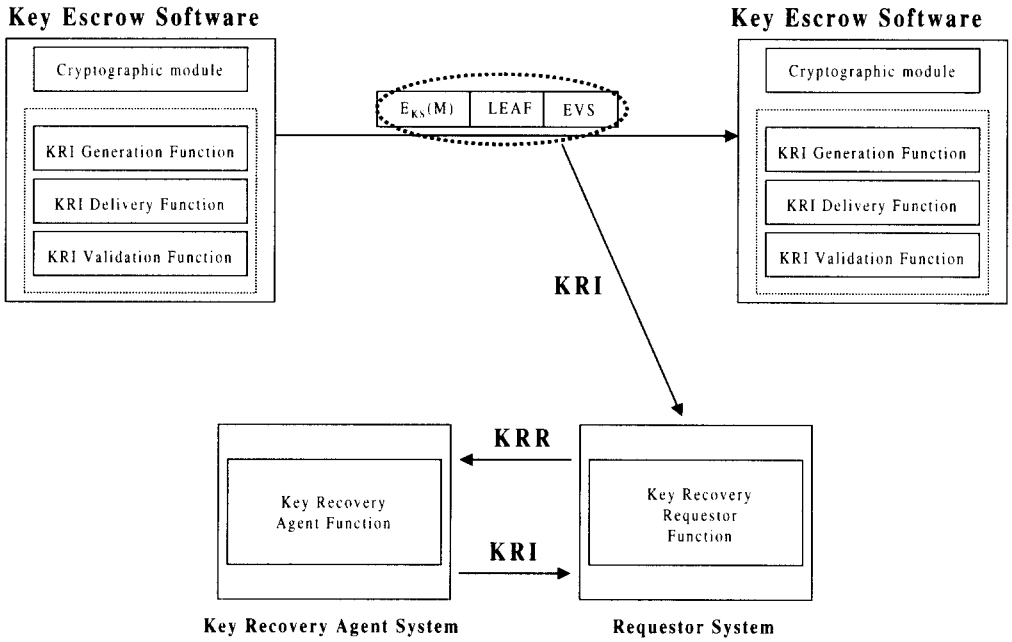

그림 3.3. TIS Software Key Escrow 기능 블럭도

구되었을 때 법원의 허가 없이도 암호문이 Investigator에 의해 불법적으로 복호될 수 있다는 문제점에 대한 해결책을 제시하고 있다. 이 방식에서는 키 복구 정보를 키 분배 프로토콜을 통하여 전달하고 있으며, 그림 3.4와 같이 NIST의 키 복구 시스템 모델에 적용할 수 있다.

이 시스템에서는 각 사용자 단말 장치에 탑재된 키 교환 프로그램이 KRI를 생성하여 네트워크를 통해 상대 단말 장치로 전송을 하고, 네트워크는 KRI를 전송하기 전에 KRI의 유효성을 검사하는 KRI 검증 기능을 수행한다.

2. 캡슐화 방식

캡슐화 방식은 키 위탁 방식과는 달리 암호문을 생성하는 각 세션마다 키를 복구해 낼 수 있는 정보를 포함하는 필드를 생성해서 해당 암호 메시지에 부가시키는 방식으로 실제적인 키 위탁이 일어나지는 않는다. 법 집행 기관의 키 복구는 복구 기관이 가진 복구키를 이용하여 암호화된 데이터에 부가된 복구 필드를 복구 한 후 target 키를 얻을 수 있다. 그러므로 복구되는 키가 사용자의 long-term key가 아니라 세션키가 되도록 할 수 있기 때문에 도청 기관의 복구 능력을 제한할 수 있게 되어 사용자의 입장에서는 키 위탁 방식보다는 안전에 대한 확신을 가질 수 있다. 또한 기존의 프로토콜에서 확장 필드가 존재한다면 이를 이용하여 복구 필드를 부가시킴으로써 구현 비용의 절감과 높은 호환성이 가능하다는 장점이 있다.

그러나 복구 필드의 생성이 사용자측에서 일어나므로 이 필드에 대한 사용자의 부정이 충분히 가능하게 되어 복구 필드의 유효성 확인 과정이 반드시 필요하며 복구 기관의 신뢰성도 키 위탁 방식에서와 마찬가지로 보장되어야 한다.

2.1 Commercial Key Escrow[5]

기존의 키 복구 시스템들이 국가적 측면의 요구, 즉 합법적인 암호문에 대한 접근권을 만족시키는데 초점을 맞춘 것에 비해 TIS사의 Commercial Key Escrow는 일반 사용자들의 키가 분실 또는 손상되었을 경우에 키를 복구할 수 있도록 하는 사용자의 요구에 초점을 맞춘 시스템이며, 이 시스템은 그림 3.5처럼 NIST의 키 복구 시스템 모델에 적용시킬 수 있다.

각 사용자의 프로그램에서 KRI의 생성, 전달 및

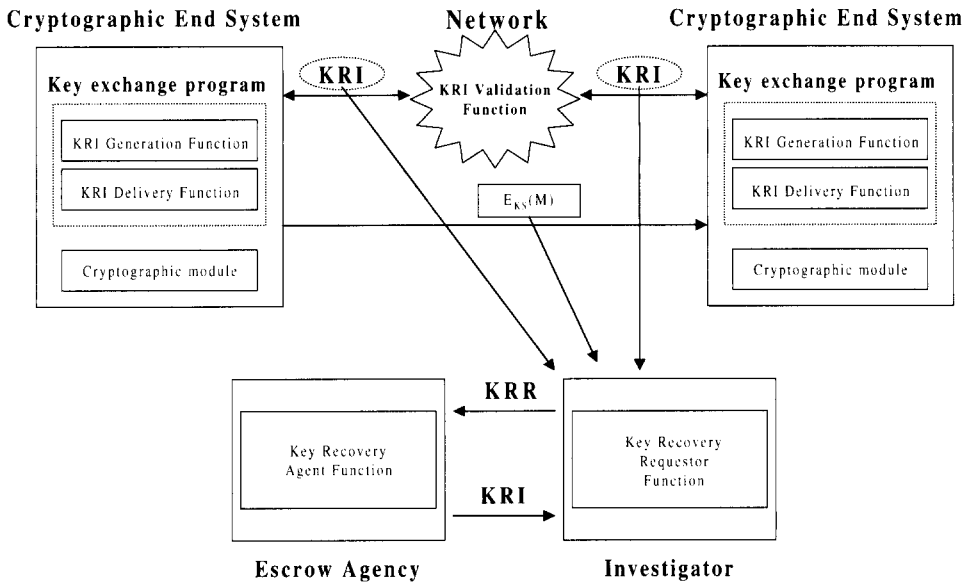

그림 3.4. Active Investigator 기능 블럭도

요청 기능을 수행하게 되고 DRC는 각 사용자 프로그램의 키 복구 요청을 받아 키를 복구해 주는 KRA 기능을 수행한다.

앞에서 언급했다시피 Commercial Key Escrow 시스템은 사용자의 키 분실 시 키 복구에 초점을 맞춘 것으로 KRI 검증 기능은 존재하지 않으며, 다만 키 복구 시에 DRC에 의해 DRF를 제출하는 사용자에 대한 확인 과정이 있다.

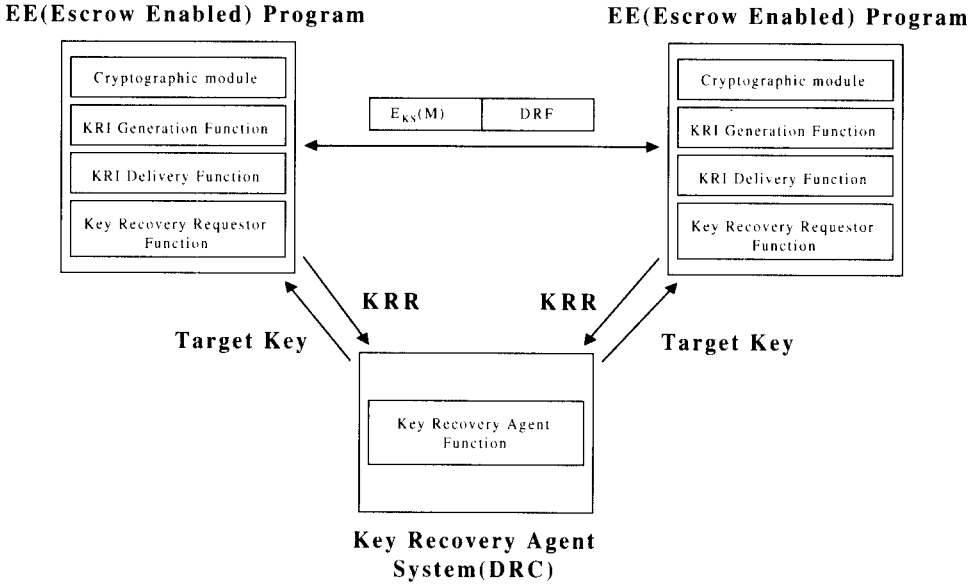

그림 3.5. Commercial Key Escrow 기능 블럭도

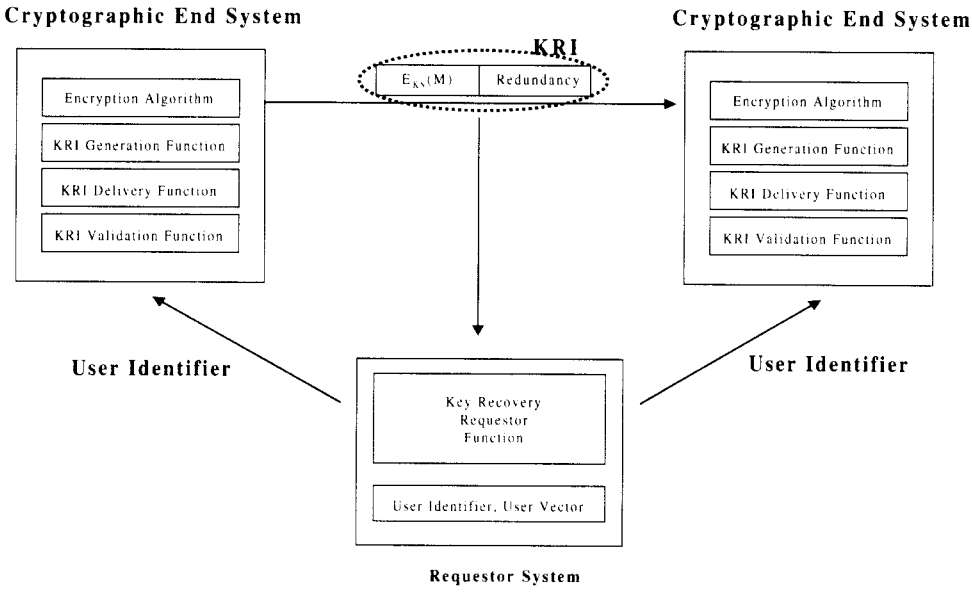

그림 3.6. Traceable ciphertexts 기능 블럭도

2.2 Traceable ciphertexts[6]

Clipper에서는 암호문에 부가되는 LEAF(law enforcement agency field)를 통해서만 LEA(law enforcement agency)가 송신자와 수신자를 추적할 수 있었다. 이를 소프트웨어 기반의 키 복구 시스템으로 구현하기 위해서 1995년 Y. Desmedt는 traceable ciphertexts 방식을 제안하였다.

이 방식은 암호문에 수신자를 추적(식별)할 수 있는 redundancy(키 분배 정보)를 부가하는 방법으로 그림 3.6처럼 NIST의 키 복구 시스템 모델에 적용시킬 수 있다.

그림처럼 traceable ciphertexts 방식에서는 KRA가 존재하지 않으며, LEA는 등록된 사용자들에게 각각에 해당하는 개인 식별 정보(사용자 벡터)를 나누어주고 이를 비밀리에 보관한다. 사용자들은 LEA로부터 받은 개인 식별 정보를 이용하여 redundancy를 생성하여 암호문에 부가하여 통신을 한다.

LEA는 도청 후 암호문에 부가된 redundancy를 통하여 사용자들을 추적할 수 있다.

2.3 Binding cryptography[7]

1997년 E. R. Verheul 등에 의해서 제시된 binding cryptography는 EES와 TIS-CKE의 중간 개념으로 KRA(TRP)에게 실제 메시지를 전달하지는 않지만, KRA의 공개키로 세션키를 암호화함으로써 키복구 정보를 제공한다.

이 방식은 부정 행위를 방지할 수는 없지만, 사용자의 비밀 정보에 대한 지식없이 제 삼자조차도 부정 행위를 발견할 수 있다. 암호문은 세션키로 암호화된 메시지와 수신자의 공개키로 암호화된 세션키 KRA(TRP)의 공개키로 암호화된 세션키 그리고 binding data로 구성된다. Binding data를 통해서 제 삼자까지도 암호문의 정당성을 검증할 수 있다. 그림 3.7처럼 사용자들은 암호문을 구성하고 KRR은 암호문을 도청하여 만일 binding data에서 부정 행위가 감지되면 KRA에게 KRI를 요청한다. KRA는 KRR의 정당성을 확인한 후 자신의 비밀키로 세션키를 복호하여 KRR에게 KRI를 전달한다. KRR은 KRA로부터 받은 KRI를 이용하여 암호문을 복호한다.

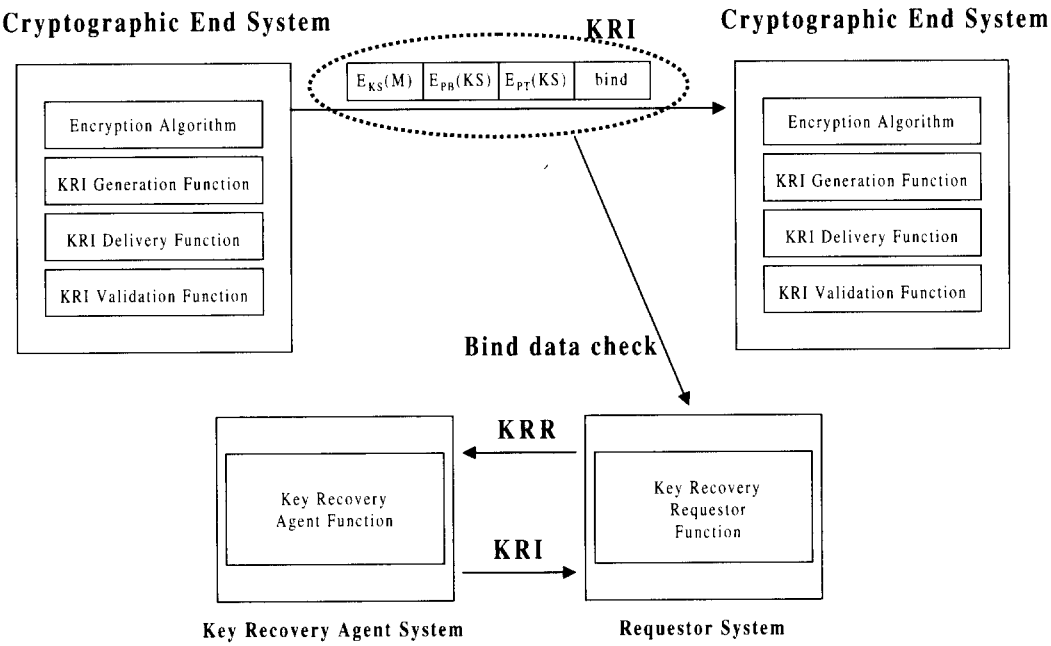

그림 3.7. Binding cryptography 기능 블럭도

3. TTP(trusted third party) 기반의 키 복구 방식

TTP 키 복구 방식은 신뢰할 수 있는 제 삼자 즉, TTP(trusted third party)를 가정하여 복구될 사용자의 비밀키를 그 사용자의 TTP로 지정된 기관에서 모두 생성하고 사용자에게 분배하는 방식으로 실제적인 키의 위탁은 일어나지 않으나 사용자의 long term 키를 TTP가 직접 가지고 있으므로 위탁된다고 말할 수도 있다. 사용자들의 비밀키를 TTP로 지정된 기관에서 생성·분배하므로 각 기관들의 신뢰성 보장이 절대적이어야 한다.

키 생성시 각 사용자들의 TTP들은 비밀키를 사용하여 사용자들의 long term 키를 생성한다. 사용자들은 이 키를 받아 세션키를 생성하여 비밀 통신을 하게된다.

TTP들이 사용자들의 비밀키를 모두 가지고 있으므로 유사시에 TTP에 의한 키 복구가 확실히 보장되며 TTP 사이의 키 생성 방식이 통일된다면 국가간 호환성이 뛰어나다는 장점이 있다. 그러나 개인의 프라이버시가 전적으로 TTP에게 의존하며 TTP의 수가 너무 많이 요구되고 이에 따르는 TTP와 사용자 사이의 병목현상과 TTP 자체 사이의 병목현상이 심하다는 것이 단점이다.

3.1 GCHQ 키 복구 방식[8][10]

TTP에 기반한 키 복구 방식은 영국 정부에서 키 복구 시스템을 구현하기 위해 제안한 방식으로 NIST에서 제시한 키 복구 시스템 모델에 [그림 3.8]처럼 대응될 수 있다. 이 방식에서는 신뢰할 수 있는 제 삼자, 즉 각 사용자의 TTP를 키 복구 기능의 KRA로 설정하고 이 KRA가 다른 영역의 KRA와 공유된 비밀 정보를 이용하여 암호화된 데이터 통신에 필요한 모든 키 혹은 키 요소를 사용자에게 전송한다. 암호 단말 시스템은 이 비밀 정보를 이용하여 다른 암호 단말 시스템과의 세션키를 공유할 수 있고 이를 사용하여 암호화된 데이터를 주고받을 수 있다.

키 복구 요구 시스템은 송수신자들 사이에 전송되는 암호문과 그 암호문에 덧붙여져 전송되는 KRI를 감청하여 KRA에 키 복구 요청을 하는 KRR 기능을 수행하게 된다. 키 복구 요구 시스템으로부터 키 복구 요청을 받은 KRA, 즉 각 암호 단말 시스템의 TTP는 그 요청에 알맞은 키 복구 정보(KRI)를 키 복구 요구 시스템에 제공하여 키 복구 요구 시스템이 키 복구를 수행할 수 있게 한다.

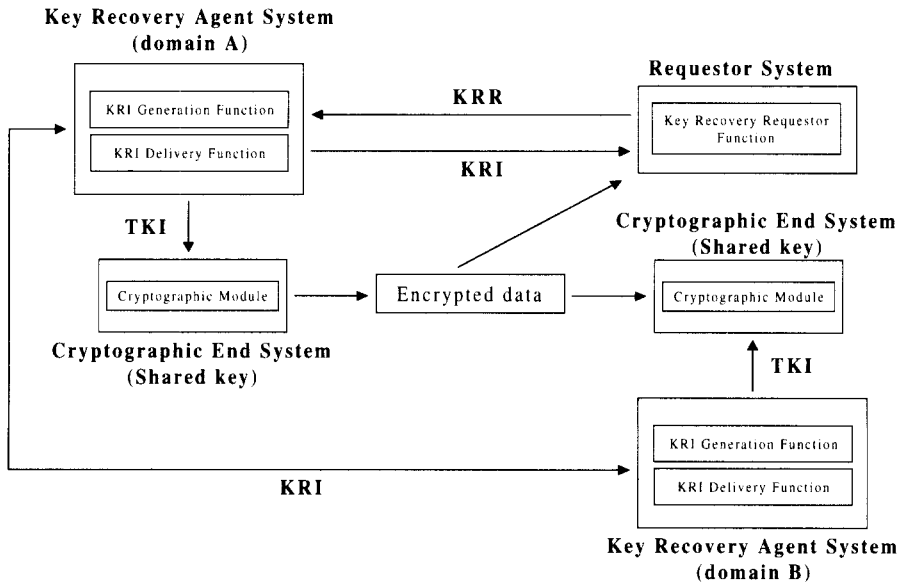

그림 3.8. TTP 기능 블럭도

Ⅳ. 기존 시스템의 요구사항 만족도 분석

본 장에서는 3장에서 언급한 대표적인 기존 키 복구 시스템에 대해서 2장의 NIST 키 복구 제품 요구사항[11]을 실제로 적용시켜 분석해 보았다. 그러나 기능 요구사항을 제외한 나머지 요구사항들은 실제 구현된 제품에 대한 요구사항들에 대해 나열하고 있으므로 키 복구 기술별 만족여부를 가려낼 수 없다. 이러한 항목에 대해서는 만족여부에 대한 설명을 생략하였다.

3장의 키 복구 시스템을 NIST 요구사항에 적용시 다음과 같이 각각을 표시하였다

- 키 위탁 방식
  - EES : [EES]-93[1]
  - EES에 대한 공격 : [M. Blaze의 공격]-94[2]
  - TIS Software Key Escrow : [TIS Software Escrow]-95[3]
  - Active Investigator : [Active Investigator]-95[4]
- 캡슐화 방식
  - Commercial Key Escrow : [Commercial Key Escrow]-95[5]
  - Traceable Ciphertext : [Traceability]-95[6]
  - Binding Cryptography : [Binding Cryptography]-97[7]
- TTP 기반의 키 복구 방식
  - GCHQ 키 복구 방식 : [GCHQ]-96[8]
  - 수정된 GCHQ 키 복구 방식 : [GCHQ 수정 프로토콜]-97[9][10]

◦ 요구사항 8

> 키 복구 정보 생성 기능의 각 객체는 KRI의 부분 또는 모두를 생성해야 하고 모든 KRI 생성 기능은 키 복구를 위한 충분한 KRI를 생성해야 한다.

[EES]-93

EES에서는 두 개의 Escrow Agent(NIST, 재무성의 자동화 시스템부)가 KRR 기능이 제공하는 UID와 법원 영장을 받아 그에 해당하는 KU를 복구하는 데 필요한 정보인 K#와 EKC(encrypted key component)를 LED(law enforcement decryptor)에게 제공하게 되고 LED는 EA들로부터 받은 정보들로부터 KU를 얻어낼 수 있다.

[TIS Software Escrow]-95

두 EA에게 UIP가 제공되었을 때 각 EA들은 UIP에 해당하는 KU를 복구하기 위한 정보(KU_{priv1}, KU_{priv2})를 LED에게 제공함으로써 KU를 얻어낼 수 있다.

[Commercial Key Escrow]-95

EEP(escrow enabled program)는 키 복구시 사용되는 정보인 DRF를 데이터 데이터를 암호화할 때마다 생성하게 되는 데 DRC(data recovery center)의 비밀키로 암호화되어 있는 DRF(data recovery field)가 DRC로 전송되면 DRC는 자신의 비밀키로 DRF를 복호함으로써 KS를 얻어낼 수 있다.

[Active Investigator]-95

KRR(investigator) 기능이 각 EA에게 법원의 명령과 복구하려는 키의 사용자 ID를 제공하면 EA는 KRR 기능에 그 사용자의 비밀키를 제공한다. Investigator는 EA로부터 제공받은 비밀키와 두 사용자가 세션키 KS를 설정하기 위해 교환하는 정보(r_A, s_A)를 통해 세션키 KS를 복구할 수 있다.

[Traceability]-95

송신자는 사전에 자신의 비밀키를 KRA에게 위탁하지 않으며, KRR은 trapdoor(redundancy)를 통해서 단지 수신자를 추적할 뿐이며, 암호문을 복호할 수 있는 키를 복호할 수 없다.

[Binding Cryptography]-97

송신자는 사전에 자신의 비밀키를 KRA에게 위탁하지 않고, 암호문에 사용되는 세션키를 KRA(TRP : trusted recovery party)의 공개키로 암호화하여 키 복구 정보를 생성한다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97

KRA, 즉 각 사용자의 TTP는 KRA 기능을 수행하며 날짜, 인증 정보, 알고리즘 식별자, 암호화된

키 등의 데이터 복구에 충분한 KRI 정보를 생성한다.

◦ 요구사항 9

> KRI 생성 기능의 한 객체는 다른 키 복구 기능이 사용할 KRI의 일부 또는 전부를 암호문과 연관시킬 수 있도록 조립, 구성해야 한다.

[EES]-93

EES 장치는 Clipper나 Capstone 같은 칩을 내장하고 있는 암호 단말 장치에서는 LED(law enforcement decryptor)에서 키 복구를 위해 사용할 수 있도록 E_{KF}(UID || E_{KU}(KS) || CS)의 형태로 LEAF를 구성하여 암호문에 덧붙인다.

[TIS Software Escrow]-95

암호 단말 장치에 내장되어있는 EEP(enabled escrow program)에서는 LED(law enforcement decryptor)에서 키 복구를 위해 사용할 수 있도록 LEAF와 EVS를 구성하여 암호문에 덧붙인다.

[Commercial Key Escrow]-95

EEP는 암호화를 실행할 때마다 DRC의 공개키로 암호화된 세션키와 사용자 ID, 그리고 DRC의 공개 식별정보를 포함하고 있는 DRF를 구성하여 암호문 내에 포함시키거나 덧붙인다.

[Active Investigator]-95

각 사용자 단말 장치는 네트워크에서 전송 받은 정보(m_A)를 기반으로 상대방에게 세션키를 설정하는 데 필요한 정보인 r, s를 생성하여 전송하며, 이 정보는 investigator가 세션키 KS를 복구하기 위해 사용한다.

[Traceability]-95

암호문에는 수신자를 추적하기 위한 redundancy가 있으며, 이 redundancy를 통하여 다른 키 복구 기능에 적용할 수 있다.

[Binding Cryptography]-97

송신자가 수신자에게 전송하는 암호문은 세션키를 이용하여 암호화된 메시지에 수신자의 공개키를 이용하여 암호화된 세션키와 KRA의 공개키를 이용하여 암호화된 세션키 및 bind 데이터가 연접되어 있다. 이 정보들을 통하여 다른 키 복구 기능에 적용할 수 있다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97

다른 사용자나 정부와 같은 합법적 감청 기관이 사용할 데이터 복구에 충분한 KRI를 생성한다. 이 KRI는 사용자의 메시지 복호에 필요한 TKI 획득 정보를 충분히 담고 있으며 이는 KRA에게 합법 기관이 요청시 복구 가능하다.

◦ 요구사항 10

> KRI 생성 기능은 출력의 유효성을 보장해야 한다.

[EES]-93

EES에서는 LEAF를 생성시키기 위해 필요한 정보(UID, KU, KF, KS, IV)들은 temper proofness 칩인 clipper나 capstone 칩에 내장되어 있거나 칩내에서 생성하게 된다. 그러므로 LEAF를 생성하는 데 사용되는 정보들은 정당하게 되고 그러므로 KRI 생성 기능에서 생성되는 LEAF는 정당함이 보장된다.

[M. Blaze의 공격]-94

정당해 보이지만 전송되는 암호문에 대응되지 않는 LEAF를 생성해 내는 공격(brute-force LEAF search)이 존재한다.

[TIS Software Escorw]-95

공개 정보들로부터 LEAF를 생성하여 수신된 LEAF와 비교함으로써 그 정당성을 검사한다.

[Active Investigator]-95

사용자 단말 장치에서 생성된 KRI, 즉 r과 s는 상대에게 전달되기 전에 네트워크에 의해서 그 정당성이 검사된 후 전달된다.

[Traceability]-95

암호문에 있는 redundancy를 통해서 수신자의 신분을 확인할 수 있고, 만일 redundancy가 제거되면, 수신자는 암호문을 복호할 수 없다.

[Binding Cryptography]-97
Binding 데이터를 통해 제 삼자에 의해서도 유효성을 검사할 수 있으며, 또한 수신자의 신분 정보와 송신자가 서명한 time-stamp에 의해서 시간 제한을 둘 수도 있다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97
KRI를 생성한 후 생성 기관의 그 결과에 대한 validity 검사는 없다.

◦ 요구사항 11

> KRI 생성 기능은 생성된 KRI를 KRI 전달 기능에 제공해야 한다.

[EES]-93
Clipper나 capstone 칩 내에서 생성된 LEAF는 수신 단말 장치로 전송되기 전에 KRI 전달 기능에 의해 대응되는 암호문에 덧붙여진다.

[M. Blaze의 공격]-94
송신 단말 장치에서 생성된 LEAF를 대응되는 암호문에 덧붙이지 않고 암호문만 전송함으로써 가능한 공격(LEAF feedback)이 존재한다.

[TIS Software Escorw]-95
송신 단말 장치에서 생성된 LEAF와 EVS는 수신 단말 장치로 전송되기 전에 KRI 전달 기능에 의해 LEAF에 대응하는 암호문에 덧붙여진다.

[Commercial Key Escrow]-95
데이터가 암호화될 때마다 생성되는 DRF는 KRI 전달 기능에 의해 대응하는 암호문에 덧붙여지거나 암호문 내에 포함되게 된다.

[Active Investigator]-95
사용자 단말 장치에서 생성된 r과 s는 상대방과 세션키 KS를 설정하기 위하여 KRI 전달 기능에 의해 전송 매체를 통해 네트워크로 전송된다.

[Traceability]-95
생성된 KRI(redundancy)는 ElGamal 암호 시스템을 사용하여 전달한다.

[Binding Cryptography]-97
생성된 KRI는 ElGamal 암호 시스템을 사용하여 전달한다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97
생성된 KRI를 US의 MSP에서 개발한 보안 프로토콜로 전달하여 전송한다.

◦ 요구사항 12

> KRI 생성 기능의 수준 2 제품은 KRI 생성을 비활성화하기 위한 설비를 제공하지 않아야 한다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97
KRI는 영국의 메일 시스템에 적합한 형태로 구성되었으나 메일 시스템에 독립적인 US MSP의 보안 표준 프로토콜에 따라서 전송된다.

◦ 요구사항 14

> KRI 전달 기능은 저장된 암호문에 대응하는 KRI를 지속적으로 사용할 수 있도록 저장해야 한다.

[EES]-93
EES를 설명하는 FIPS PUB-185[1]에서는 EES의 적용 범위를 전화 시스템을 통한 음성, 데이터 통신으로 한정하고 있으며, 저장 데이터에 대해서는 다루지 않고 있다.

[TIS Software Escorw]-95
TIS사에서 제안한 software key escrow는 EES를 기준으로 만들어졌으므로 EES와 같은 전화 시스템을 통한 전송 데이터에 대해서만 적용 범위가 한정된다.

[Commercial Key Escrow]-95
메시지가 암호화될 때 생성되며 키를 복구하기 위한 정보를 담고 있는 DRF는 암호문에 덧붙여지거나 암호문 내에 포함되어 암호문과 함께 저장된다

[Active Investigator]-95
네트워크는 과거에 사용되었던 특정 사용자의 (ID, (m, r, s), c)를 기록하며, 이 정보들로부터 과거의 암호문을 복호할 수 있다.

[Traceability]-95
KRR은 각 사용자에 해당하는 고유의 신분 정보를 비밀리에 보관한다.

[Binding Cryptography]-97
암호문에 사용되는 세션키와 동일한 세션키가 수신자 및 KRA의 공개키로 암호화되어 있으므로, 해당 암호문에 대한 세션키를 지속적으로 사용할 수 있다.

◦ 요구사항 15

> KRI 전달 기능은 KRI가 KRR 기능이나 KRA, 또는 양쪽 모두에서 이용될 수 있도록 (KRI를 KRR이나 KRA에게 전송하거나 그들이 접근할 수 있는 곳에 둠) 해야 한다.

[EES]-93
송신측 단말 장치에서 생성된 LEAF를 대응되는 암호문에 붙여서 통신 채널을 통해 수신측에 전송함으로써 LED가 LEAF를 이용할 수 있게 한다.

[M. Blaze의 공격]-94
송신측 단말 장치에서 생성된 LEAF를 그에 대응하는 암호문에 붙여서 보내지 않고 암호문만 보냄으로써 KRR기능이 KRI를 이용할 수 없도록 하는 공격(LEAF feedback)이 존재한다.

[TIS Software Escorw]-95
송신측 단말 장치에서 생성된 LEAF와 EVS를 대응하는 암호문과 함께 통신 채널을 통해 수신측에 전송함으로써 LED가 LEAF를 이용할 수 있게 한다.

[Commercial Key Escrow]-95
데이터 암호시 생성되는 DRF를 대응되는 암호문에 덧붙여 놓음으로써 후에 KRR 기능이 DRF에 접근할 수 있게 한다.

[Active Investigator]-95
각 사용자는 상대방과 세션키 KS를 공유하기 위한 정보를 네트워크를 통해 전송함으로써 KRR이 그 정보에 접근할 수 있게 한다.

[Traceability]-95
KRI 정보는 KRR 기능에 의해서 이용할 수 있다.

[Binding Cryptography]-97
KRI는 암호문에 포함되어 전달되므로, KRR 기능이나 KRA 기능에서 모두 이용할 수 있다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97
KRI는 키복구를 위한 KRR 기능이나 KRA기능에서 모두 이용 가능하다.

◦ 요구사항 16

> KRI 전달 기능은 KRI가 KRI 검증 기능에서 이용될 수 있도록(통신 채널이나 저장 장치를 통해) 해야 한다.

[EES]-93
송신측 단말 장치에서 LEAF가 생성되면 전달 기능은 LEAF와 IV를 함께 대응되는 암호문에 붙여서 수신측 단말 장치로 통신 채널을 통해 전송함으로써 수신 측에서 validity 검사가 일어난다.

[M. Blaze의 공격]-94
송신측 단말 장치에서 생성된 LEAF를 대응하는 암호문에 붙여서 보내지 않고 수신측에서 임의로 생성한 IV에 대해 정당한 LEAF를 자신에게 feedback함으로써 가능한 공격(LEAF feedback)이 존재한다.

[TIS Software Escrow]-95
수신측에서 LEAF를 재생성하기 위해 필요한 정보들을 공개해 놓음으로써 KRI 검증 기능이 수행될 수 있게 한다.

[Active Investigator]-95
각 사용자가 상대방과 세션키 KS를 공유하기 위해 나누어 가지는 정보 r, s는 반드시 그 정보들의 정당성을 검증하는 네트워크를 통해 전송된다

[Traceability]-95
암호문에 있는 redundancy를 통해서 유효성 검사를 실시하고, 유효하지 않으면 암호문은 복호되지 않는다.

[Binding Cryptography]-97
암호문에 KRI 및 유효성 확인을 위한 Binding 데이터가 있으므로, Binding 데이터를 이용하여 유효성 검사를 할 수 있다.

[GCHQ]-96 [GCHQ 수정 프로토콜]-97
KRI Validation 기능이 가지고 있는 간단한 메시지 출처 인증 확장 기능에서 이용 가능하다. 이 확장은 미국의 US와 영국의 UK 두가지 기능 중 하나를 선택하여 사용할 수 있다.

[R. Anderson]-97
영국의 UK 기능은 US보다 안전하지 않고 계산 속도도 느리기 때문에 특별한 응용을 제외하고는 보통 US를 사용한다.

◦ 요구사항 17

> KRI 검증 기능은 활성화(turn on) 또는 비활성화(turn off) 될 수 있어야 한다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97
이 기능은 간단한 메시지 출처 인증 기능이 있으며 중요하지 않은 확장 기능의 경우 활성화나 비활성화가 가능하다.

◦ 요구사항 18

> KRI 검증 기능은 검증 기능이 활성화 되어있는 상태에서 유효성 검사가 실패하면 암호 단말 장치에서 평문으로의 접근은 거부되어야 한다.

[EES]-93
수신측 암호 단말 장치에서 수신된 LEAF가 정당하지 않다고 판정되면, 수신측 암호 단말 장치에서는 암호문을 복호하지 않는다.

[M. Blaze의 공격]-94
정당해 보이지만 실제로는 부당한 LEAF를 사용하여 정당성 검사를 통과하는 공격(LEAF feedback, brute-force LEAF search)이 존재한다.

[TIS Software Escorw]-95
수신측에서 공개 정보들로부터 재 생성한 LEAF와 전송된 LEAF를 비교하여 두 LEAF가 다를 경우, 즉 유효하지 않은 LEAF로 판정되면 수신측은 암호문을 복호 하지 않는다.

[Active Investigator]-95
KS 설정을 위해 전송되는 정보, 즉 r과 s는 상대측으로 전송되기 전에 네트워크에 의해 항상 그 정당성을 검증받게 된다. 만약 정당성 검사가 실패하면 그 정보들은 상대측으로 전송되지 않으며, 결국 암호통신을 위한 KS 조차 설정할 수가 없게된다.

[Traceability]-95
Redundancy로 유효성을 검사하여, 만일 redundancy가 유효하지 않으면, 수신자는 암호문을 복호할 수 없다.

[Binding Cryptography]-97
Binding 데이터로 유효성을 검사하여 단지 부정행위를 발견할 뿐이고, 평문에 대한 접근 거부 기능은 없다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97
활성화된 경우 검증이 실패하면 실행은 종료된다.

◦ 요구사항 19

> KRR 기능은 주어진 KRI에 대해 하나 이상의 KRA 기능들과 상호 작용함으로써 target key를 복구할 수 있어야 한다.

〔EES〕-93
법 집행기관은 취득한 LEAF로부터 얻어진 UID를 법원 영장과 함께 각 EA들에게 보내고 EA들이 그 UID에 해당하는 K#와 EKC를 LED에게 전송하면 LED는 그 정보들로부터 KU를 복구해내게 된다.

〔TIS Software Escorw〕-95
법 집행기관은 취득한 LEAF에서 얻어진 UIP를 법원 영장과 함께 각 EA들에게 전송하면 EA들은 그 UIP에 해당하는 KU의 비밀키 조각을 법 집행기관에게 제공한다. 법 집행기관은 EA에게서 제공받은 정보들로부터 KU를 복구할 수 있다.

〔Commercial Key Escrow〕-95
키를 분실한 사용자는 복호를 원하는 암호문에 부가되어 있는 DRF와 개인 인증정보를 DRC에 제공하면 DRC는 그에 해당하는 KS를 구해서 사용자에게 제공한다.

〔Active Investigator〕-95
r과 s가 주어졌을 때 법 집행기관이 EA에게 해당 사용자의 ID와 법원 영장을 제공하여 해당 사용자의 비밀키를 얻어냄으로써 KS를 구해 낼 수 있다.

〔Binding Cryptography〕-97
법 집행 기관이 취득한 암호문에는 KRA의 공개키를 이용하여 target key(세션키)를 암호화한 정보가 있으므로, 이를 이용하여 세션키를 복구할 수 있다.

〔GCHQ〕-96 〔R. Anderson〕-97 〔GCHQ 수정 프로토콜〕-97
이 프로토콜은 신뢰할 수 있는 제 삼자를 가정하고 있기 때문에 KRA로부터 얻은 KRI로부터 사용자 비밀 데이터를 복호할 수 있는 target key를 얻을 수 있다.

◦ 요구사항 20

KRR 기능이 전송하는 암호화 데이터는 복구 가능해야 한다.

〔Binding Cryptography〕-97
Binding 데이터를 이용하여 유효성을 검사한 뒤, TRP의 공개키로 세션키가 암호화되어 있으므로, TRP는 자신의 비밀키로 세션키를 복구 한 후, KRR에게 세션키를 전송하여 KRR이 암호문을 복구할 수 있도록 한다.

◦ 요구사항 21

KRA 기능은 target key 복구 시 필요한 키, 키 요소 또는 다른 정보를 저장한다.

〔EES〕-93
각 EA는 각 UID에 해당하는 KU를 구하기 위해 필요한 정보인 K#와 EKC를 안전하게 저장한다.

〔TIS Software Escrow〕-95
명확한 언급은 없지만 기본적으로 모델 자체가 EES를 따르고 있으므로, 각 EA들은 키 복구에 필요한 정보를 안전하게 저장하고 있다고 가정한다.

〔Commercial Key Escrow〕-95
DRC는 KS를 복구하는데 필요한 정보인 DRC의 비밀키를 안전하게 저장한다.

〔Active Investigator〕-95
각 EA는 사용자의 ID와 그 사용자들의 시간대별 비밀키 등 키 복구에 필요한 정보들을 저장하고 있다.

〔Binding Cryptography〕-97
KRA는 자신의 비밀키로 세션키를 복구한다.

〔GCHQ〕-96 〔R. Anderson〕-97 〔GCHQ 수정 프로토콜〕-97
KRA 기능은 각 사용자의 target key 복구에 필요한 키를 생성하고 저장한다.

◦ 요구사항 22

KRA 기능을 작동시키기 위해 필요한 모든 정보와 KRA 기능을 사용하는 모든 암호 모듈은 가용성을 위해 안전하게 복사되어야 한다.

[EES]-93

각 EA는 각 UID에 해당하는 K#와 EKC의 복사본을 별도의 장소에 안전하게 보관하고 있다.

◦ 요구사항 23

> KRR 기능이 제공하는 KRI를 처리하여 요청자가 얻은 데이터를 복호하는 데 필요한 부분 또는 모든 정보를 보내야 한다.

[EES]-93

KRA는 LED가 제공하는 UID를 받아 KU를 생성하는데 필요한 정보인 K#와 EKC를 LED에 전송하고, LED는 그 정보들로부터 KU를 복구해 낼 수 있다.

[TIS Software Escorw]-95

KRA는 LED(law enforcement decrypor)가 제공하는 UIP를 받아 KU를 생성하는데 필요한 정보인 KU_{priv1}, KU_{priv2}를 LED에 전송하면 LED는 그 정보들로부터 KU를 복구해 낸다.

[Commercial Key Escrow]-95

사용자가 복호하고자 하는 암호문에 대응하는 DRF와 사용자 인증정보를 DRC에 제공하면 DRC는 DRC의 비밀키로 KS를 구해서 사용자에게 제공한다.

[Active Investigator]-95

각 EA들은 법 집행기관이 제공하는 법원 영장과 키 복구 대상자의 ID를 받아서 그에 해당하는 사용자의 비밀키를 제공하고, 법 집행기관은 그 비밀키와 네트워크에서 얻은 다른 정보들로부터 사용자의 KS를 구해낼 수 있다.

[Binding Cryptography]-97

KRI가 취득한 암호문을 TRP에게 보내면, TRP는 KRI의 warrant가 정당할 때 TRP의 비밀키로 세션키를 복구하여 KRI에게 전송한다.

◦ 요구사항 24

> KRA 기능이 전송하는 암호화 데이터는 복구 가능해야 한다.

각 키 복구 스킴에서 이 요구사항에 대한 명확한 언급은 하고 있지 않지만 KRR과 KRA 사이에 전송되는 정보는 KRI나 TKI와 같이 키 복구에 있어서 중요한 정보이므로 전자적 또는 물리적으로 보호되어 전송되며, 수신측에서 복구될 수 있어야만 한다.

[EES]-93

각 KRA가 KRR에게 암호화된 정보 EKC1, EKC2를 전송하면, KRR은 EKC와 함께 전송된 K#1, K#2를 통하여 EKC를 복호할 수 있는 키(KCK)를 얻어내며, 그 키를 통하여 암호화되어 전송된 EKC를 복호(KC를 얻어냄)해 낼 수 있다.

[Commercial Key Escrow]-95

DRC는 사용자의 요청을 받아 해당 사용자의 세션키 KS를 암호화하여 사용자에게 전송하며, 사용자는 암호화된 KS를 복호하여 KS를 얻어낸다.

◦ 요구사항 25~32

> 모든 암호 모듈의 FIPS 수준에 관한 요구사항이다.

[R. Anderson]-97

GCHQ 프로토콜에는 암호 알고리즘 제한은 없으나 실제 영국에서는 Red Pike라는 암호 알고리즘의 사용을 강요하고 있다. 영국 정부와의 통신이 필요한 응용들에서 이 암호 알고리즘이 사용되고 있기 때문이다. 영국 정부는 이를 강요한 적이 없다고 부인하고 있지만 이 알고리즘을 사용해야만 정부와의 통신이 가능하다.

◦ 요구사항 39

> KRI 생성 기능은 둘 이상의 KRA로 TKI를 나눈다.

[GCHQ]-96 [R. Anderson]-97 [GCHQ 수정 프로토콜]-97

각 사용자마다 그 사용자를 담당하는 KRA는 하나이므로 둘 이상의 KRA로 TKI를 나누지 않고 하나의 KRI만이 사용자의 TKI를 소유한다.

V. 결 론

본 고에서는 NIST의 키 복구 제품 요구 사항을 분석하고 분석된 요구사항을 여러 가지 키 복구 제품이나 키 복구 방식에 적용시켜 기능 블럭도를 도시하였으며 요구 사항에 대한 만족 여부를 분석하였다. 현재까지 제시된 키 복구 시스템의 요구사항 만족도는 다음과 같다.

- 기능 요구사항 : 키 복구 시스템의 필수적 기능에 대한 사항들로 대부분 만족
- 보안 요구사항 : 일부분 만족
- 보안 확신 요구사항 및 기타 요구사항 : 만족 여부 판단 불가능(실 제품에 적용 가능)

현재 세계 각 국에서 암호 사용이나 키 복구와 관련된 여러 가지 정책 및 기반 기술에 대한 연구가 활발히 진행되어 왔던 것에 반해 국내에서는 최근까지도 키 복구를 포함한 암호 사용 전반에 관한 법제나 기술에 대한 연구가 미흡하다고 생각된다. 따라서 본 연구는 우리 나라의 실정에 적합한 키 복구 기술이나 제품 개발에 많은 도움을 줄 수 있을 것으로 기대된다.

참 고 문 헌

[1] NIST, "Escrowed Encryption Standard", *Federal Information Processing Standards Publication (FIPS PUB) 185*, 1994.

[2] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard", *Proceedings of Second ACM Conference on Computer and Communications Security*, Fairfax, VA, PostScript, pp. 59-67, November 1994.

[3] David M. Balenson, Carl M. Ellison, Steven B. Lipner, Stephen T. Walker, "A New Approach to Software Key Escrow Encryption", *manuscript*, 1994

[4] Patrick Horster, Markus Michels, Holger Petersen, "A New Key Escrow System with Active Investigator", *Proc. Securicom, Paris, La Defence*, 8.-9. June, (1995), S.15-28. ; also see *Theoretical Computer Science and Information Security Technical Report TR-95-4-f*, Department of Computer Science, University of Techno- logy Chemnitz- Zwixkau.

[5] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, Dennis K. Branstad, David M. Balenson, "Commercial Key Escrow : something for everyone now and for the future", *TIS Report* no. 541, 1995

[6] Yvo Desmedt, "Securing Traceability of Ciphertexts - Towards a Secure Software Key Escrow System", *Eurocrypt '95*, LNCS 921, Springer-Verlag, Berlin 147-157, 1995.

[7] E. R. Verheul, H. C. van Tilborg, "Binding ElGamal : A Fraud - Detectable Alternative to Key Escrow Proposals", *Eurocrypt '97*, LNCS 1233, Springer- Verlag, Berlin 119-133, 1997.

[8] CESG, "Securing Electronic Mail Within HMG - Part1 Infrastructure And Protocol Draft C", 21 March 1996, document T/3113TL/2776/11: available at URL http://www.rdg.opengroup.org/public/tech/security/pki /casm/casm.htm.

[9] Ross Anderson, Michael Roe, "The GCHQ Protocol and its Problems", Advanced in Cryptology - *Eurocrypt '97*, Springer-Verlag, Lecture Notes in Computer Science, LNCS 1233, pp134-148, 1997.

[10] Mark P Hoyle, Chris J. Michell, "On Solutions to the key escrow problem", *Springer-Verlag (LNCS 1528)*, Berlin pp.277-306, (1998).

[11] NIST, "Report of the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure", Available at http://csrc.nist.gov/keyrecovery/, 1998.11

〈著者紹介〉

유 희 종 (Hui-Jong Yu)
1999년 : 성균관대학교 정보공학과 졸업
1999년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 석사과정
〈관심분야〉 암호이론, 정보이론

주 미 리 (Mi-Ri Joo)
1996년 2월: 성균관대학교 정보공학과(공학사)
1998년 2월: 성균관대학교 대학원 정보공학과(공학석사)
1999년~현재: 성균관대학교 전기전자 및 컴퓨터 공학부 박사과정
〈관심분야〉 암호이론, 정보이론

원 동 호 (Dong-Ho Won)
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 전자공학과 석사
1988년 : 성균관대학교 전자공학과 박사
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국가정보화 추진위원회 자문위원
1990년~1999년 : 한국통신정보보호학회 이사
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1982년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
1999년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부장
(겸)정보통신대학원장, 한국통신정보보호학회 부회장
〈관심분야〉 암호이론, 부호이론

김 지 연 (Jee-Yeon KIM)
1995년 2월 성균관대학교 정보공학과(공학사)
1997년 2월 성균관대학교 대학원 정보공학과(공학석사)
1996년 12월 ~ 현재 한국정보보호센터 연구원
〈관심분야〉 암호이론, 암호 프로토콜

박 성 준 (Sung-Jun Park)
1983년 : 한양대학교 수학과 졸업
1985년 : 한양대학교 수학과 석사
1996년 : 성균관대학교 정보공학과 박사
1985년~1994년 : 한국전자통신연구소 선임연구원
1996년~현재 : 한국정보보호센터 기반기술팀장
〈관심분야〉 암호이론, 계산이론, 정보이론