2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

프라이버시 보호를 위한 키 복구 시스템 모델에 대한 연구

국상진*, 임양규*, 원동호*
*성균관대학교 전기전자 및 컴퓨터 공학과
e-mail:skook@dosan.skku.ac.kr

A Study on Key Recovery System model for Privacy

Sang-Jin Kook*, Yang-Kyu Lim*, Dong-Ho Won*
*School of Electrical & Computer Eng., Sungkyunkwan University

요약

사생활 침해라는 문제와 법 집행 능력의 보장이라는 문제점 사이에서 논쟁 중인 키 복구 기술은 다양한 관점에서 연구되고 있다. 본 논문에서는 여러 가지 방식의 키 복구 시스템에 대하여 고찰함과 동시에 키 캡슐화 방식을 사용하는 키 복구 시스템 모델을 제안한다. 또한 이 모델은 사생활 침해 문제에 좀더 효과적으로 대처하도록 이루어진 키 복구 시스템 모델이다.

1. 서론

현대 사회가 고도화된 정보화 사회로 바뀌어 가면서 사람들은 다양한 정보에 대하여 보다 쉽게 접근할 수 있게 되었다. 이는 사람들에게 편리성을 제공하였지만, 반대로 정보의 유출 또한 쉽게 발생 할 수 있게 되었다.

정보 유출을 막는 좋은 해답으로서 주로 군사적인 목적에서만 주로 사용하던 암호가 제시되어 왔으며, 또한 민간부분에까지도 급속하게 확산 되어가고 있다.

암호의 사용은 정보의 누출을 방지하고, 상대방의 신원을 확인 할 수 있도록 할 뿐 아니라 전자상거래를 할 수 있도록 하는 등 많은 장점을 가지고 있다. 그러나 이에 반하여 범죄자들에 의한 암호의 악용과 키의 분실 및 손상 등에 따른 암호문의 복호 불가 등 그 역기능도 발생하고 있다.

역기능에 대한 대책으로 현재 키 복구에 대한 연구가 세계적으로 활발히 진행되고 있으며, 그 결과물 또한 관심의 대상이 되고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 키 복구의 정의에 대하여 기술하고, 3장에서는 키 복구 방식에 대하여 기술 허였고, 4장에서는 키 복구 시스템에 대한 가정에 대한 기술하였으며, 5장에서는 프라이버시 보호의 관점에서 새로운 키 복구 시스템 모델에 제안하였고, 마지막으로 6장에서는 결론에 이르도록 구성되었다.

2. 키 복구의 정의

일반적으로 키 복구란 암호문의 소유자만이 평문으로 복호 할 수 있는 암호화된 데이터에 대해 특정한 조건이 만족될 경우에 한해서 허가된 사람 또는 기관에게 복호가 가능한 능력을 제공하는 기술 및 체계를 말한다.

그러나 키 복구 방식과 관련하여 개인의 사생활 보호와 정부의 법 집행 능력 보장이라는 두 가지 상반된 목적에 대하여 끊임없는 논쟁이 진행되고 있으며, 키 복구 시스템을 채택하려는 국가들 역시 전자상거래 진흥과 개인의 프라이버시 보호라는 상반된 기능 사이에서 적정한 균형을 찾으려고 연구하고 있다.

3. 키 복구 방식

키 복구 방식은 크게 키 위탁 방식, 키 캡슐화 방식, TTP방식의 세 가지 방식으로 나누어진다.

키 위탁 방식은 복구될 사용자의 비밀키, 비밀키의 부분 또는 키 관련 정보를 하나 이상의 신뢰 기관에 위탁하는 방식이다. 이 방식은 사용자의 비밀키가 위탁 기관에 직접 맡겨져야 하므로 개인의 프라이버시가 모두 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.

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 목적키를 얻을 수 있다. 그러므로 복구되는 키가 사용자의 long term 키가 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.

TTP 방식은 신뢰할 수 있는 제 3자 즉, TTP를 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.

4. 키 복구 시스템에 대한 가정

키 복구 시스템을 사용하는데 있어서 사용자의 자발적 참여와 강제적 참여라는 두 가지 관점으로 나누어 보아야 한다.

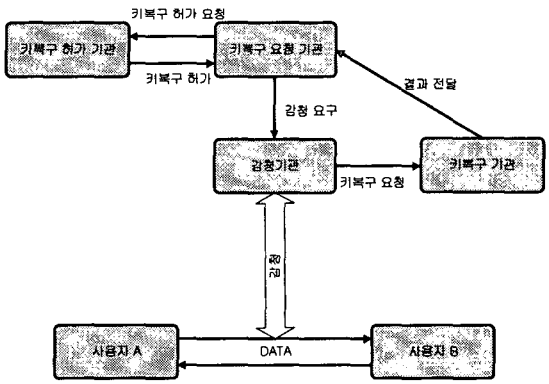
사용자가 키의 분실이나 손상으로부터 자신의 소유하고 있는 정보에 접근 할 수 없을 경우에, 일어나는 손실에 대비하기 위하여 키 복구 시스템을 사용하는 경우 개인적 측면 또는 사용자의 자발적 참여 관점으로 볼 수 있다. 이에 반하여 키 복구 요청 기관이 범죄 수사 등의 합법적인 필요로 인하여 다른 사용자들의 암호화된 정보에 접근하려 할 때에는 모든 사람들이 키 복구 시스템을 사용하고 있어야만 가능한 가정이다. 이때에는 키 복구 시스템의 강제적 참여 관점이 된다.

키 복구 시스템에의 자발적 참여와 강제적 참여의 사이에는 개인의 프라이버시 보호와 법 집행 보장이라는 두 가지 측면을 고려해야 한다.

5. 제안하는 시스템

5.1 일반적인 키 복구 모델

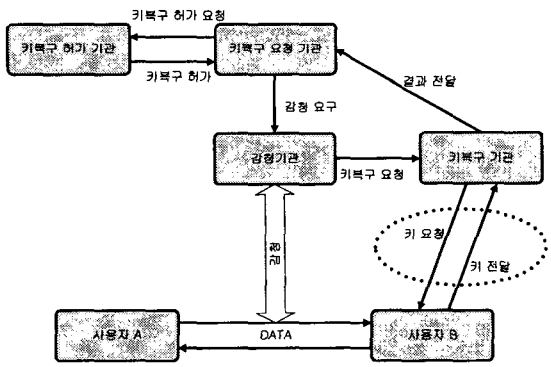
일반적인 키 복구 시스템의 모델은 [그림 1]과 같다.



[그림 1] 일반적인 키 복구 모델

키 복구 요청 기관의 요구에 의하여 키 복구 허가 기관은 적법성 평가 후에 키 복구 허가를 하며, 키 복구 기관은 감청된 데이터에 대하여 키 복구를 행한다.

5.2 제안하는 키 복구 모델



[그림 2] 제안하는 키 복구 모델

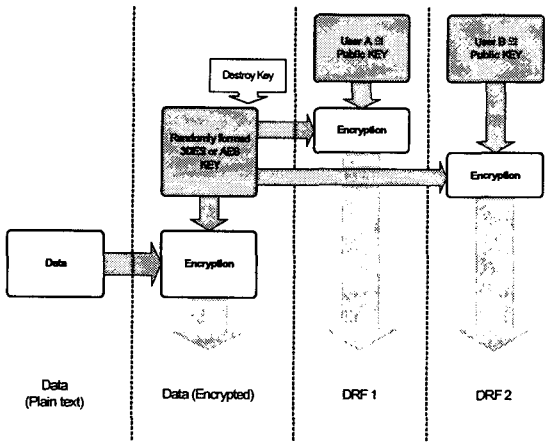
제안하고 있는 키 복구 모델은 키 캡슐화 방식을

사용하고 있으며, 또한 일반적 키 복구 모델과 비교하여 키 복구 기관이 키 복구 시에 항상 사용자에게 직접 키 정보를 요구해야만 한다. 즉 사용자들은 키 복구가 될 때마다 키 정보를 키 복구 기관에 전달함으로서 자신의 데이터에 대한 키 복구 빈도, 횟수 등의 정보를 알 수 있다.

[그림 2]는 제안하고 있는 키 복구 시스템의 모델을 도식화한 그림이다. 키 복구 요청은 송수신하는 어떠한 사용자에게도 가능하다.

5.2.1 키 복구 필드의 생성

키 복구 필드의 생성은 [그림 3]과 같다.



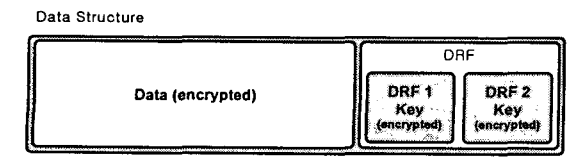
[그림 3] Data Recovery Field의 생성과정

· Step 1 : User A는 전송하려는 데이터를 Random하게 생성된 3DES Key로 암호화하여 DF를 생성한다.

· Step 2 : 사용된 3DES Key는 자신의 공개키로 암호화하여 DRF1을 생성한다.

· Step 3 : 사용된 3DES Key를 수신자의 공개키로 암호화하여 DRF2를 생성한다.

· Step 4 : 사용된 3DES Key는 폐기한다.



[그림 4] Data 구조

위 Step을 거친후 만들어진 데이터 구조는 [그림 4]와 같다.

Data Field :

$$DF = En_{3DES\ Key}(Data)$$

Data Recovery Field :

$$DRF = DRF1 \mid DRF2$$

$$DRF1 = En_{Pub\ A}(3DES\ Key)$$

$$DRF2 = En_{Pub\ B}(3DES\ Key)$$

5.2.2 키 복구 요청

키 복구 요청 기관은 키 복구 허가 기관으로부터 키 복구의 허가를 받은 후, 키 복구 허가서, 사용자 정보를 감청 기관에 전달한다.

5.2.3 감청

감청 기관은 User A와 User B 사이에 전송되고 있는 Data를 감청 후에, 감청된 데이터, 사용자 정보를 키 복구 기관에 전달한다.

5.2.4 키 복구 기관의 키 복구

· Step 1 : 키 복구 기관은 사용자에게 Data를 전달하고 3DES Key를 요청한다.

· Step 2 : 사용자는 DRF1 또는 DRF2를 이용하여 3DES Key를 복구한다.

· Step 3 : 복구된 3DES Key를 키 복구 기관에 전달한다.

· Step 4 : 키 복구 기관은 Data를 복호하여 키 복구 요청 기관에 전달한다.

5.2.5 키 복구가 불가능한 경우

키 정보를 신뢰할 수 있는 위탁 기관에 위탁하는 키 위탁 방식 경우는 대부분 키 복구가 가능하다. 그러나 캡슐화 방식을 사용하는 본 시스템에서는 다음과 같은 경우가 발생하기도 한다.

· 사용자가 의도적으로 잘못된 DRF를 생성할 경우

· 사용자가 의도적으로 잘못된 키를 전달하여 키 복구 기관이 올바른 암호문을 복호 할 수 없게 되는 경우

· 키 복구 기관의 정당한 요구에도 불구하고 키 복구를 의도적으로 거부하는 경우

6. 결론

키 복구 시스템은 개인, 기업, 국가적 차원에서도 그 활용 가치를 인정받고 있고, 그 연구도 활발히 진행되고 있다. 그러나 제도적인 문제, 프라이버시 침해의 문제 등으로 논란이 되고 있다.

본 논문에서는 사용자의 프라이버시 보호 측면이 강조된 키 복구 시스템 모델을 제안하였다.

본 시스템에서는 키 복구 가능의 유무를 실제로 사용자가 선택하기 때문에, 합법적으로 요구되는 키 복구에 대해서는 사용자의 3DES Key 제공 의무를 규정하는 등의 법·제도적 보완이 필요하다.

참고문헌

[1] National Institute of Standards and Technology, FIPS Publication 185 : "Escrowed Encryption Standard", Feb. 1994.

[2] D. E Denning and D. K. Branstad. "A taxonomy for key escrow encryption system", Communications of the ACM, vol.39, no.3, pp.34-40, 1996.

[3] Stephen T. Walker, Steven B.Lipner, Carl M.Ellison, David M. Balenson "Commercial Key Recovery", 3. 1996. Vol.39. NO.3, Communications of the ACM

[4] VeriSign, "Key Management Service Administrator's Guide", http://www. verisign.com/rsc/doc/onsite/4.5.1/KeyMgt/KMS.pdf

[5] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, pp.612-613, 1979.

[6] National Institute of Standards and Technology, "Requirement for Key Recovery Products", Dec. 1998.

[7] Yair Frankel, Moti Yung, "Escrow Encryption Systems Visited : Attacks, Analysis and Designs", Crypto'95, Springer-Verlag, Lecture Notes in Computer Science, LNCS 963, pp.223-235, 1995.

[8] A. Young, Moti Yung, "Auto-Recoverable and Auto-Certifiable Cryptosystems", Advanced in Cryptography-Eurocrypt '98, Springer-Verlag, Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 17-31, 1998.

[9] Pascal Paillier and Moti Yung, "Self-Escrowed Public-Key Infrastructures", ISISC'99, pp. 249-261.

[10] 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 Recovery, Key Escrow, and Trusted Third-Party Encryption" ftp://research.att.com/dist/mab/key_study.txt Final Report, 27 May 1997.