제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

이동통신 환경에서 키 복구 기능을 가진 키 분배 시스템에 관한 연구

주미리*, 서인석*, 원동호**
*국가보안기술연구소
**성균관대학교 정보통신공학부
e-mail:mrjoo@etri.re.kr

A Study on Key Exchange System with Key Recovery in Mobile Communications

Mi-Ri Joo*, In-Seog Seo*, Dong-Ho Won***
**National Security Research Institute
**Dept of Computer Engineering, Sungkyunkwan University

요 약

이동성과 편리성을 제공하는 이동 통신 환경은 다양한 장점을 가지고 있는 반면 무선이라는 특성상 보안에 대하여 취약하다. 따라서 기밀성과 인증 기능을 제공하는 다양한 암호 시스템 사용이 필요하게 되었으며, 암호의 역기능을 방지하기 위한 키 복구 기능이 포함된 다양한 키 분배 프로토콜이 제안되었다. 본 논문에서는 이동 통신 환경에 적합하게 설계된 키 복구 기능을 가진 키 분배 프로토콜에 대하여 분석하고, 이를 토대로 키 분배 프로토콜 설계 원칙을 제시하였다. 또한 제시한 설계 원칙을 기반으로 키 복구 기능을 가진 키 분배 프로토콜을 제안하였다.

1. 서론

최근 컴퓨터와 통신 기술의 급속한 발전으로 인하여 유·무선통신의 통합이 이루어지고 있으며, 사용자들은 시간과 장소에 구애받지 않고 유·무선 통합 환경을 이용하여 쉽고 빠르게 여러 가지 정보를 공유하고 유통할 수 있게 되었다. 특히, 이동 통신은 유선통신과 무선통신이 결합된 형태로 고정된 위치에 제약을 받지 않고 이동 중에 무선으로 통신하는 방식을 말한다.

이동성과 편리성을 제공해 주는 이동 통신 서비스의 수요는 국내·외에서 폭발적으로 증가하고 있다. 그러나, 무선 통신망을 이용하는 이동 통신은 불법적인 사용이나 도청 또는 추적을 통한 불법적인 행위나 각종 통신 범죄 행위 등에 매우 취약하여 유선을 이용하는 통신에 비해 정보의 유출, 불법 수정 등이 용이하고, 휴대 장치에 저장된 데이터는 휴대 장치 분실 시에 같이 분실될 수 있다.

이동 통신 환경에서 네트워크 요소들의 이동성을 높이기 위해서 단말기들은 상대적으로 적은 자원을 가지고 있고, 이로 인하여 암호 사용에 많은 제약을 받게 된다. 따라서, 보안 서비스 제공으로 인하여 시스템에 미치는 부하 증가와 단말기 소형화에 따른 계산 능력이 제한되어 있는 이동 통신 환경에서는 안전성과 효율성이라는 상반된 목적을 만족시키기 위해서 공개키 암호 방식을 사용하여 키를 분배하고 분배된 키를 이용하여 대칭키 암호 방식을 사용하는 다양한 암호 시스템이 제안되었다[1]. 그러나 키 분실 또는 손상 시 정당한 사용자조차 암호문을 복호할 수 없다는 암호의 역기능은 유사시 대책을 위한 키 복구 기능을 요구하게 되었다[2][3][4].

본 논문에서는 기존의 이동 통신 상의 키 분배 프로토콜에 대한 분석을 통해 설계 원칙을 제시하였다. 또한 이를 기반으로 키 복구 기능을 가진 키 분배 프로토콜을 제시하였다. 본 논문은 2장에서 이동 통신 환경의 키 분배 프로토콜 설계 시 고려되는 설계 원칙을 제시하고, 3장에서는 제시된 설계 원칙을 기반으로 이동 통신에 적합한 키 복구 기능을 가진 키 분배 프로토콜을 제안하였으며, 4장에서 결론을 맺었다.

2. 이동 통신 환경의 키 분배 프로토콜 설계 원칙

2.1 이동 통신환경의 특징

이동 통신은 단말기의 이동성을 가지는 통신을 지칭하는 용어로써, 초창기에는 음성 서비스 위주의 이동 전화(휴대 전화) 서비스에서 발전하여, 현재 무선 호출 서비스, 주파수 공용 통신 서비스, 위성 통신 서비스 등으로 확대 발전되어 왔다. 이동 통신 환경의 특징은 다음과 같다.

- 사용자의 이동성
  이동 통신 환경에서의 사용자들은 여러 도메인을 이동하며, 원격으로 여러 서비스와 자원을 사용하기를 원한다. 사용자의 위치, 움직임 등이 중요한 정보가 되므로 이를 보호해야할 필요가 있다.
- 이동 통신 기기의 이동성
  이동 통신의 사용자들은 휴대용 장치들을 가지고 다니며, 휴대성을 높이기 위하여 소형으로 제작되므로, 낮은 계산 능력과 적은 자원을 가진다.
- 무선 네트워킹
  무선 네트워킹은 사용자와 이동 통신 기기의 이동성을 높이기 위한 필수 조건으로 전송 매체가 대기 중의 공기이므로 물리적인 보안성이 없어 도청자에 의해 쉽게 도청되며, 사용자 및 이동 통신 기기가 여러 도메인을 이동함으로써 인증 정보의 핸드오프 등이 반드시 일어나야만 한다.

2.2 이동 통신환경의 키 분배 프로토콜 설계 원칙

이동 통신은 무선으로 통신을 하고, 공중파를 사용하기 때문에 기존의 유선 기반의 통신 시스템과는 몇 가지 다른 방법으로 보안을 한다. 이동 통신 장치는 데스크탑 컴퓨터보다 사고나 위협이 더 많이 존재하고, 이동 통신 기기의 손실은 데이터의 손실을 의미한다. 이를 방지하기 위해서 데이터를 보호하기 위한 하드디스크 암호화와 사용자 식별숫자(PIN : Personal Identification Number), 이동 단말 장치를 보호하기 위한 패스워드를 사용해야 한다. 본 장에서는 이동 통신 상에서 키 분배 프로토콜이 갖추어야할 설계 원칙을 제시하였다.

- 정당한 사용자 인증
  사용자는 상대방으로부터의 전송 정보의 유효성을 검사하기 위하여 통신 상대방이 자신이 프로토콜을 수행하고자 하는 사람인지 확인할 수 있도록 프로토콜을 설계해야 한다.
- 명시적 키 인증
  사용자는 자신이 통신하고자 하는 상대방만이 비밀 세션키를 계산할 수 있고 상대방이 그 키를 가지고 있음을 확인할 수 있어야 한다.
- 키 확인
  사용자는 자신이 통신하고자 하는 상대방이 실제로 비밀 세션키를 공유하고 있음을 확인할 수 있어야 한다.
- 기밀성 제공
  이동 통신에서 전달 매체는 대기이므로 보안에 취약하다. 따라서 이동 통신을 이용하여 전송되는 비밀 정보는 기밀성이 제공되는 형태로 전달되어야 한다.
- 무결성 제공
  이동 통신에서 전달 매체는 대기이므로 전송되는 정보에 오류가 발생하기 쉬우며 공격자가 전송 정보를 변경하기 용이하다. 따라서 전송 정보에 대한 무결성이 보장되어야 한다.
- 단말기 계산량 최소화
  이동 통신 기기는 사용자의 휴대성을 높이기 위하여 최소화하고 경량화되고 있다. 따라서, 이동 통신 기기는 낮은 계산량과 적은 자원을 가지고 있으므로 최소의 계산을 수행해야 한다.
- 전송 정보 최소화
  일반적으로 이동 통신 환경의 특징인 무선 통신은 유선 통신에 비하여 낮은 대역폭과 높은 에러율을 가지고 있다. 따라서, 이동 통신 환경에서 프로토콜은 메시지의 수와 전송되는 데이터가 최소화되어야 한다.
- 키 복구 기능 탑재
  비밀키 분실이나 손상 시 또는 암호를 이용한 범죄를 방지하기 위하여 키 복구 기능이 탑재되어야 한다.
- 키 복구 정보 유효성 검증
  사용자가 생성한 키 복구 정보에 대한 유효성은 제 3자가 검증할 수 있어 사용자가 키 복구 정보에 대한 부정행위를 할 수 없어야한다.
- 익명성 제공
  이동 통신 환경에서는 사용자의 위치 정보가 알려질 경우 개인의 프라이버시가 침해될 소지가 있으므로 의도된 사용자만이 상대방이 누구인지 알 수 있도록 익명성을 보장해야 한다.

3. 제안하는 키 분배 시스템

1996년 무선 통신 환경에서 세션키를 분배하고 사용자 인증을 수행하는 ASPeCT 프로토콜에 제시된 이후로 다양한 키 분배 프로토콜이 제시되었다 [5][6][7].

본 논문에서는 송수신자 양측에서 동일한 방법으로 키 복구 기능과 인증 기능을 가진 위탁 방식을 이용한 무선 통신상의 키 분배 및 키 복구 시스템을 제안하였다. 제안된 시스템은 2장에서 제시한 설계 원칙을 따르고 있으며 전송되는 정보량이 기존의 시스템에 비해 적해 효율적이다.

3.1 파라미터 생성과 검증

신뢰센터 *TTP*는 사용자의 암호용 공개키에 인증서를 발급해 주는 기관이며, 시스템을 이용하는 모든 사용자들은 위탁 정보 w를 생성하여 신뢰할 수 있는 키 복구 기관 *KRA*에게 이를 위탁한다. 이때 *KRA*는 사용자들이 임의로 선정할 수 있으며, *TTP*는 인증기관과 키 복구 기관의 역할을 하고 있다. 다음 [표 1]는 제안하는 시스템에서 사용되는 용어이다.

[표 1] 프로토콜의 약어 및 의미

약어	의미
A	사용자 A의 식별 정보
B	VASP B의 식별 정보
TTP_A (KRA_A)	A의 인증 기관 및 키 복구 기관
TTP_B (KRA_B)	B의 인증 기관 및 키 복구 기관
A_{Cert}	A의 공개키에 대한 인증서
B_{Cert}	B의 공개키에 대한 인증서
$E_{K_{AB}}$	K_{AB}로 관용 암호 방식으로 암호화
h_1, h_2, h_3	일방향 해쉬 함수

3.2 위탁 과정

본 논문에서 제안하는 키 복구 기능을 가진 키 분배 프로토콜에서 위탁 정보는 등록 과정에서 사용자가 선택한 키 복구 기관에 위탁된다.

① 사용자 A와 VASP B는 각각의 위탁 정보 w_A, w_B를 각각의 신뢰 기관 KRA_A, KRA_B 에게 위탁한다. 이때 신뢰 기관은 사용자 A 및 VASP B가 임의로 선정할 수 있다. 단, $1 \le w_A, w_B \le q-1$

② A와 B는 각각 $\phi_A = g^{w_A}$, $\phi_B = g^{w_B}$를 생성하여 이를 공개한다.

3.3 키 분배 및 인증 프로토콜

사용자 A와 VASP B는 위탁 과정에 따라 키 위탁 정보를 생성하여 자신이 선택한 신뢰기관에 이를 위탁하고 다음과 같이 세션키를 공유하고 키와 사용자를 인증한다.

[단계 1]

① 사용자 A는 임의의 난수 r_A를 선택한다.

$$r_A \in_R Z_{q-1},\ 1 \le r_A \le q-1$$

이때 p는 큰 소수이며 q 는 $q \mid (p-1)$인 소수이다.

② A는 g^{r_A}을 계산하여 g^a와 함께 전달한다. 이때 g는 Z_p^* 상에서 q의 order인 원시 원소이다.

③ A는 다음과 같이 s_A를 계산한다. 이때 f는 일방향 함수이며, w_A는 키복구 기관 KRA_A 에게 위탁한 정보이다.

$$s_A = (w_A h(g^{r_A}) + r_A) \bmod q$$

[단계 2]

① VASP B는 임의의 난수 r_B를 선택한다.

$$r_B \in_R Z_{q-1},\ 1 \le r_B \le q-1$$

이때 p는 큰 소수이며 q 는 $q \mid (p-1)$인 소수이다.

② B는 g^{r_B}를 계산한다. 이때 g는 Z_p^* 상에서 q의 위수인 원시 원소이다.

③ B는 다음과 같이 s_B를 계산한다. 이때 f는 일방향 함수이며, w_B는 키복구 기관 KRA_B 에게 위탁한 정보이다.

$$s_B = (w_B h(g^{r_B}) + r_B) \bmod q$$

④ B는 다음과 같이 세션키를 생성한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

⑤ B는 키 복구 필드를 생성한다.

$$s_B \oplus g^{ar_B} \oplus g^{br_A}$$

⑥ B는 키에 대한 무결성 검사를 위해 다음의 해쉬 값을 생성한다.

$$h_2(K_{AB}, g^{r_B}, B)$$

⑦ B는 자신의 인증서를 첨부하여 다음을 사용자 A에게 전송한다.

$$g^{r_B}, s_B \oplus g^{ar_B} \oplus g^{br_A}, h_2(K_{AB}, g^{r_B}, B), B_{Cert}$$

[단계 3]

① A는 [단계2]에서 전달받은 $h_2(K_{AB}, g^{r_B}, B)$값을 계산하여 무결성을 확인하고, 다음과 같이 세션키를 생성한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

② A는 $s_B \oplus g^{ar_B} \oplus g^{br_A}$로부터 s_B를 계산한다.

$$s_B = s_B \oplus g^{ar_B} \oplus g^{br_A} \oplus g^{ar_B} \oplus g^{br_A}$$

③ A는 다음과 같이 일방향 함수 값을 생성한다.

$$h_3(g^{r_A}, g^a, g^{r_B}, g^b, B)$$

④ 사용자 A는 ③에서 생성한 일방향 함수 값에 A의 인증서를 첨부하여 세션키로 암호화한다.

$$E_{K_{AB}}\{ h_3(g^{r_A}, g^a, g^{r_B}, g^b, B),\ A_{Cert}\}$$

⑤ 사용자 A는 ④에서 생성한 값 s_A, s_B에를 첨부하여 VASP B에게 전송한다.

$$E_{K_{AB}}\{ h_3(g^{r_A}, g^a, g^{r_B}, g^b, B),\ A_{Cert}\}, s_A, s_B$$

3.4 키 복구 과정

제안하는 프로토콜에서는 사용자 A의 도메인과 VASP B의 도메인에서 동일한 방법으로 키 복구를 할 수 있다.

① KRA_A는 다음과 같이 r_A를 계산한다.

$$r_A = s_A - w_A h(g^{r_A}) \bmod q$$

② KRA_A는 VASP B의 공개키 g^b와 r_A를 이용하여 다음을 계산한다.

$$g^{r_A b} = (g^b)^{r_A}$$

③ KRA_A 다음과 같이 g^{ar_B}를 계산한다.

$$g^{ar_B} = s_B \oplus g^{ar_B} \oplus g^{br_A} \oplus s_B \oplus g^{br_A}$$

④ KRA_A는 다음과 같이 세션키를 계산한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

4. 결론

이동성과 편리성을 가지고 있는 이동 통신 환경에서의 통신은 지속적으로 발전하고 있으며 향후 현재 유선 시스템의 많은 부분들이 무선 환경으로 변화할 것이다. 또한 전자상거래 등 다양한 응용 분야에서도 이동 통신이 사용되기 위해서는 정보보호가 필요하다. 그러나 이동 통신 환경에서 사용되고 있는 단말기는 제한된 계산 능력을 가지고 있어 안전성과 효율성이라는 상반된 목적을 만족시키는 암호 시스템이 요구되며, 암호의 역기능을 방지하기 위한 대비책이 요구된다.

본 논문에서는 이동 통신 환경에서 키 분배 프로토콜 설계 시 필요한 설계 원칙을 제시하고, 이를 기반으로 안전성과 효율성을 제공하고, 암호의 역기능을 방지할 수 있는 위탁 방식을 이용한 이동 통신상의 키 분배 및 키 복구 시스템을 제안하였다.

제안한 시스템은 전송되는 정보가 적어 기존의 프로토콜에 비하여 효율적이며, 키 복구 정보에 대한 유효성 검증이 가능하고, 송수신자 양측에서 동일한 키 복구 방식을 사용하고 있어 다양한 응용 분야에 적용될 수 있다. 따라서 클라이언트 대 서버 환경뿐만 아니라 클라이언트 대 클라이언트 환경 등에 적용할 수 있으므로 이에 대한 향후 연구가 필요하다.

참고문헌

[1] Advanced Security for Personal Communications Technologies
http://www.esat.kuleuven.ac.be/cosic/aspect/index.html

[2] NIST, "Escrowed Encryption Standard", Federal Information Processing Standards Publication 185, 1994

[3] Adam Young and Moti Yung, "Auto-Recoverablel Auto-Certifiable Cryptosystems", Advanced in Cryptology-Eurocrypto'98, Springer-Verlag, Lecture Notes in Computer Science, pp.17-31, 1998

[4] Pascal Paillier and Moti Yung, "Self-Escrowed Public Key Infrastructures", Proceedings of ICISC'99, The 2nd International Conference Information Security and Cryptology. Springer-Verlag, Lecture Note in Computer Science, 1999

[5] K. Rantos and C. MItchell, " Key Recovery in ASPeCT Authentication and Initialisation of Payment Protocol", presented at ACTS Mobile Summint, Sorrento, Italy, June 1999

[6] J.Nieto, D. Park, C. Boyd and E. Dawson, "Key Recovery in Third Generation Wireless Communication Systems", Public Key Cryptography - PKC 2000, LNCS 1751, pp.223 ~ 237, 2000

[7] C.H. Kim, P.J. Lee, "New Key Recovery in WAKE Protocol", Public Key Cryptography - PKC 2001, LNCS 1992, pp.325 ~ 338, 2001