스마트 카드를 이용한 익명성을 제공하는 방송 콘텐츠 암호화 키 교환 프로토콜

*황병희 **김범한 ***이동훈
고려대학교 정보경영공학전문대학원
*lovesstar@korea.ac.kr

A Key Agreement Protocol with User Anonymity for Content Transmission Using Smart Card

*Byung-Hee Hwang **Bum-Han Kim ***Dong-Hoon Lee
Graduate School of Information Management and Security, Korea University

요약

인터넷과 같이 안전하지 않은 네트워크 환경에서 도청은 손쉽게 일어난다. 또한 수신자가 누구인지 알아내기가 쉽다. 이러한 환경에서 정당한 수신자에게 방송 콘텐츠를 안전하게 제공하면서 익명성을 제공하기 위해서는 서버와 수신자 사이에 익명성을 제공하는 키 교환이 필요하다. 스마트 카드를 이용한 익명성을 제공하는 키 교환 프로토콜은 이러한 요건을 충족시킨다. 스마트 카드를 이용한 방법은 여러 가지가 존재하나 이 논문에서는 Kumar Mangipudi 가 제안한 sika프로토콜을 향상시킨 Ren-Chiun Wang의 프로토콜을 알아보고, 취약점을 분석한다. 마지막으로 취약한 점을 보완한 프로토콜을 제안하고 제안한 프로토콜의 안전성을 분석한다. 제안하는 프로토콜은 Ren-Chiun Wang의 프로토콜보다 안전성 측면에서 향상되었다.

1. 서론

요즘은 인터넷이나 핸드폰을 사용하여 방송 콘텐츠를 많이 이용한다. 서버들은 이러한 방송 콘텐츠들이 등록된 정당한 사용자에게만 전달되고 정당하지 못한 사용자들 에게는 전달되지 않기를 원한다. 이렇게 특정한 조건을 만족하는 사용자들에게만 정보를 전달하기 위해서는 세션 키 교환이 필요하다. 세션 키를 교환하게 되면 세션 키를 알고있는 가용자만이 방송 콘텐츠를 전달받아 이용할 수 있다. 또한 키를 사용함으로서 정보의 무결성이나 기밀성을 보장 할 수 있다.

또한 방송 콘텐츠라는 특성상 사용자가 누구인지 알려지지 않기를 원하는 사용자도 존재한다. 이러한 사용자들의 요구를 만족시키기 위해서는 사용자의 익명성 보장이 필요하다.

위의 두 가지 조건, 세션 키 교환과 사용자의 익명성 보장을 위해서는 스마트 카드를 사용한 익명성을 제공하는 프로토콜을 사용하면 충분하다. 여러 가지 프로토콜이 존재한다. 이러한 프로토콜은 Yang의 프로토콜을 분석하여 Kumar Mangipudi 가 향상 시켰고 이것을 다시 Ren-Chiun Wang이 분석하여 향상시켰다.

여기서는 Ren-Chiun Wang의 프로토콜을 알아보고, 취약점을 분석한다. 그리고 그것을 더욱 향상 시킨 프로토콜을 제안한다.

2. Ren-Chiun Wang의 프로토콜

이번 장에서는 Ren-Chiun Wang의 프로토콜을 살펴보고, Ren-Chiun Wang의 프로톡콜의 취약성을 분석한다.

가. Ren-Chiun Wang의 프로토콜

Ren-Chiun Wang의 프로토콜은 타원곡선 이산대수 문제의 어려움에 안전성을 두고 있다.

키 생성 단계

1 단계 스마트 카드 생성 센터(SCPC)는 큰 소수 p와, Z_p에서 $4a^3+27b^2 \bmod p \neq 0$를 만족하는 원소 a,b에 대하여 타원곡선 방정식 $E_p : y^2 = x^3 + ax + b$을 선택한다. 위수가 큰 생성자 G를 선택한다.

2 단계 SCPC는 각각의 사용자 및 서버에 대하여 Z_p^*에서 난수 X_i를 선택하여 각 사용자 및 서버의 비밀키로 하고, 그에 대응하는 $PK_i = X_i \times G$를 계산하여 각 사용자 및 서버의 공개키로 한다. 마지막으로 SCPC는 등록한 사용자와 서버의 아이디와 공개키로 이루어진 공개키 테이블 만들어서 발표한다. 테이블 1처럼 구성되어 있다.

익명의 유저 확인 및 키 동의 단계

1 단계 사용자는 Z_p^*에서 난수 t_1을 선택하고 공개키 테이블을 이용해 서버의 PK_s를 얻는다. 그 후 사용자는 $Key_1 = t_1 \times PK_S$,

"본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

$T_1 = t_1 \times G$ 를 계산하고, 계산된 Key_1을 이용해서 $M_1 = E_{Key_1}(ID_i, Nonce_1)$을 계산한다. 마지막으로 사용자는 서버에게 (T_1, M_1)으로 이루어진 서비스 요청 신호를 보낸다.

2 단계 서비스 요청 신호를 받은 후에 서버는 $Key_1 = T_1 \times X_S$를 계산하고 그 것을 사용하여 $D_{Key_1}(M_1)$을 계산해서 $(ID_i, Nonce_1)$를 얻는다. 마지막으로 서버는 ID_i가 공개키 테이블에 존재하는지 확인한다. 만약 공개키 테이블에 없다면 서비스를 거부하고, 그렇지 않다면 서버는 Z_p^*에서 난수 t_2를 선택하고, 사용자의 공개키 PK_i를 공개키 테이블에서 얻는다. 그 후 그것들을 이용하여 $Key_2 = t_2 \times PK_i$, $Key_3 = T_1 \times t_2$, $T_2 = t_2 \times G$를 계산한다. 서버는 $M_2 = E_{Key_2}(H(Key_3 \| Nonce_1), Nonce_2)$를 계산하고 마지막으로 M_2와 T_2를 사용자에게 전송한다.

3 단계 사용자는 $Key_2 = T_2 \times X_i$, $Key_3 = T_2 \times t_1$를 계산한다. 사용자는 Key_2를 사용하여 $D_{Key_2}(M_2)$를 계산한다. 만약 $(Key_3 \| Nonce_1)$의 해쉬값이 복화된 암호문에 존재한다면 사용자는 $H(Key_3 \| Nonce_2)$를 서버에게 전송한다.

4 단계 서버는 Key_3와 $Nonce_2$를 이용하여 받은 메시지가 정확한지 아닌지 검증 한다. 만약 정확하다면 서버는 사용자와 세션키를 $SK = H(Key_3)$를 설정했다고 생각한다.

나. Ren-Chiun Wang의 프로토콜 취약성 분석

Ren-Chiun Wang의 프로토콜의 취약점을 살펴보면 공개키가 생성자에 난수 X_i가 곱해진 형태로 되어 있고 공개키 테이블에 아이디가 공개되어 있다. 이러한 특징은 선형적인 성격을 가지게 된다. 이것은 위조 공격에 대하여 취약성이 존재하는 것을 알 수 있다.

공격 1 정상적인 사용자 C, D에 대하여 $2 \times PK_C = PK_D$인 관계가 성립하면 $2 \times X_C \times G = 2 \times PK_C = PK_D = X_D \times G$ 인 관계가 성립하고 $2 \times X_C = X_D$ 인 관계가 성립하여 C는 D의 비밀 키를 알 수 있다. 비밀 키가 알려진다면, C는 D의 비밀 키와 공개키 테이블에 있는 아이디를 이용하여 D처럼 위장할 수 있다.

공격 2 정상적인 사용자 C,D,E에 대하여 $PK_C + PK_D = PK_E$인 관계가 성립하면 $PK_C + PK_D = X_C \times G + X_D \times G = (X_C + X_D) \times G = PK_E = X_E \times G$인 관계가 성립하고 $X_C + X_D = X_E$ 인 관계가 성립하여 C와 D가 공모하면 E의 비밀 키를 알 수 있다. 비밀 키가 알려진다면, C와 D는 E의 비밀 키와 공개키 테이블에 있는 아이디를 이용하여 E처럼 위장할 수 있다.

3. 제안하는 프로토콜

이번 장에서는 프로토콜을 제안한다. 제안하는 프로토콜은 Ren-Chiun Wang의 프로토콜을 개량하여 안전성을 향상한 것으로 타원 곡선의 이산대수 문제의 어려움에 안전성을 두고 있다..

가. 키 생성 단계

1 단계 스마트 카드 생성 센터(SCPC)는 큰 소수 p와, Z_p에서 $4a^3 + 27b^2 \bmod p \neq 0$를 만족하는 원소 a,b에 대하여 타원 곡선 방정식 $E_p : y^2 = x^3 + ax + b$ 을 선택한다. E_p위에서 위수가 큰 생성자 G를 선택한다.

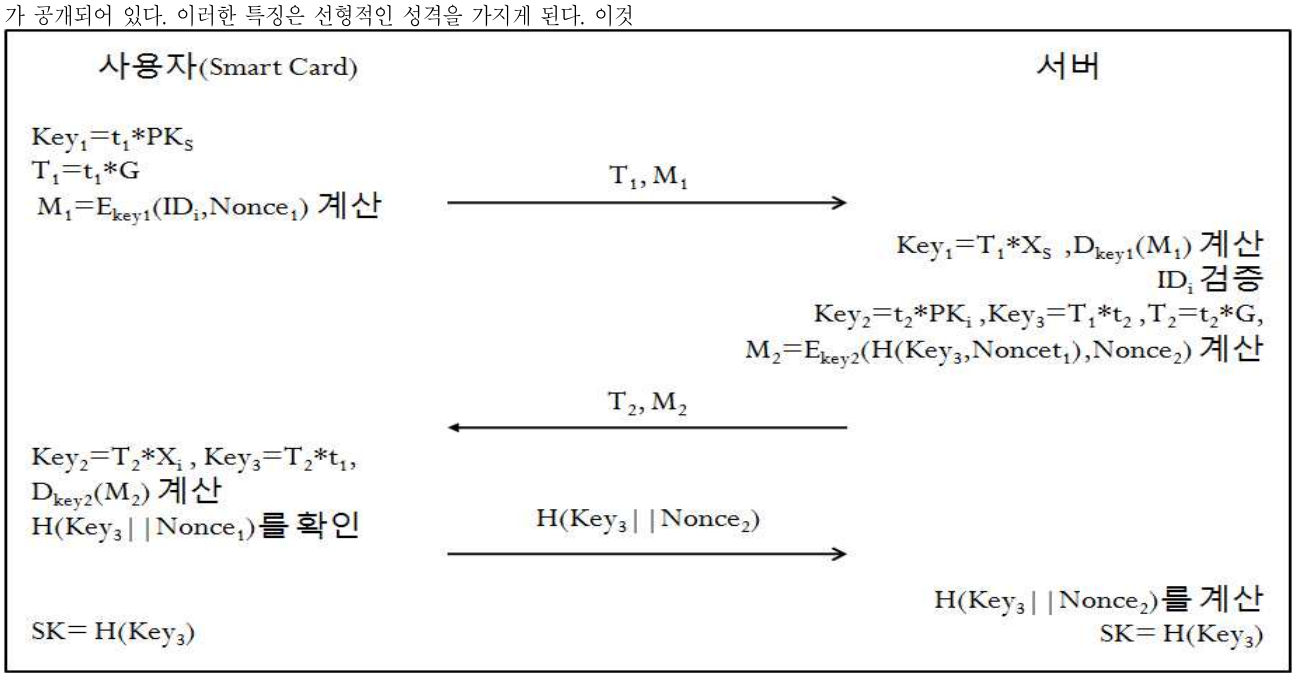

그림 1 Ren-Chiun Wang의 프로토콜의 익명의 유저 확인 및 키 동의 단계

2 단계 SCPC는 각각의 사용자 및 서버에 대하여 Z_p^*에서 난수 X_i를 선택하여 각 사용자 및 서버의 비밀키로 하고, 그에 대응하는 $PK_i = X_i \times G$를 계산하여 각 사용자 및 서버의 공개키로 한다. SCPC는 각 사용자 및 서버의 아이디의 해쉬값 $H(ID_i)$를 계산한다. 마지막으로 SCPC는 등록한 사용자와 서버의 아이디의 해쉬값과 공개키로 이루어진 공개키 테이블 만들어서 발표한다. 공개키 테이블의 모습은 아래와 같다.

아이디의 해쉬값	공개키
$H(ID_1)$	$PK_1(=X_1 \times G)$
$H(ID_2)$	$PK_2(=X_2 \times G)$
...	...
$H(ID_S)$	$PK_S(=X_S \times G)$

표 1 공개키 테이블

나, 익명의 유저 확인 및 키 동의 단계

1 단계 사용자는 Z_p^*에서 난수 t_1을 선택하고, 서버의 아이디를 해쉬한 값 $H(ID_S)$를 계산한다. 계산된 $H(ID_S)$과 공개키 테이블을 이용해 서버의 PK_s를 얻는다. 그 후 사용자는 $Key_1 = t_1 \times PK_S$, $T_1 = t_1 \times G$ 를 계산하고, 계산된 Key_1을 이용해서 $M_1 = E_{Key_1}(ID_i, Nonce_1)$을 계산한다. 마지막으로 사용자는 서버에게 (T_1, M_1)으로 이루어진 서비스 요청 신호를 보낸다.

2 단계 서비스 요청 신호를 받은 후에 서버는 $Key_1 = T_1 \times X_S$를 계산하고 그 것을 사용하여 $D_{Key_1}(M_1)$을 계산해서 $(ID_i, Nonce_1)$를 얻는다. 서버는 $H(ID_i)$를 계산한다. 마지막으로 서버는 $H(ID_i)$가 공개키 테이블에 존재하는지 확인한다. 만약 공개키 테이블에 없다면 서비스를 거부하고, 그렇지 않다면 서버는 Z_p^*에서 난수 t_2를 선택하고, 공개키 테이블과 $H(ID_i)$를 사용하여 사용자의 공개키 PK_i를 얻는다. 그 후 그것들을 이용하여 $Key_2 = t_2 \times PK_i$, $Key_3 = T_1 \times t_2$, $T_2 = t_2 \times G$를 계산한다. 서버는 Key_2, Key_3를 이용하여 $M_2 = E_{Key_2}(H(Key_3 \| Nonce_1), Nonce_2)$를 계산하고 마지막으로 M_2와 T_2를 사용자에게 전송한다.

3 단계 사용자는 $Key_2 = T_2 \times X_i$, $Key_3 = T_2 \times t_1$를 계산한다. 사용자는 Key_2를 사용하여 $D_{Key_2}(M_2)$를 계산한다. 만약 $(Key_3 \| Nonce_1)$의 해쉬값이 복화된 암호문에 존재한다면 사용자는 $H(Key_3 \| Nonce_2)$를 서버에게 전송한다.

4 단계 서버는 Key_3와 $Nonce_2$를 이용하여 받은 메시지가 정확한지 아닌지 검증 한다. 만약 정확하다면 서버는 사용자와 세션키를 $SK = H(Key_3)$를 설정했다고 생각한다.

4. 안전성 분석

가. 스푸핑 공격에 대한 저항

익명의 유저 확인 및 키 동의 단계의 1 단계에서 모든 사람은 서비스 요청을 도청 할 수 있다. 그러나 아무도 서버의 비밀 키 X_S없이 M_1을 복원하거나 $Nonce_1$을 얻을 수 없다. 2 단계에서 서버를 제외한 공격자는 정확한 응답 H(Key3||Nonce1)을 보낼 수 없다.

나. 알려진 키 공격에 대한 저항

한 번 사용된 세션 키 $H(Key_3)$가 공격자에게 들어나더라도, 공격자는 과거의 세션 키들을 추측하거나 미래의 통신을 위협할 수 없다.

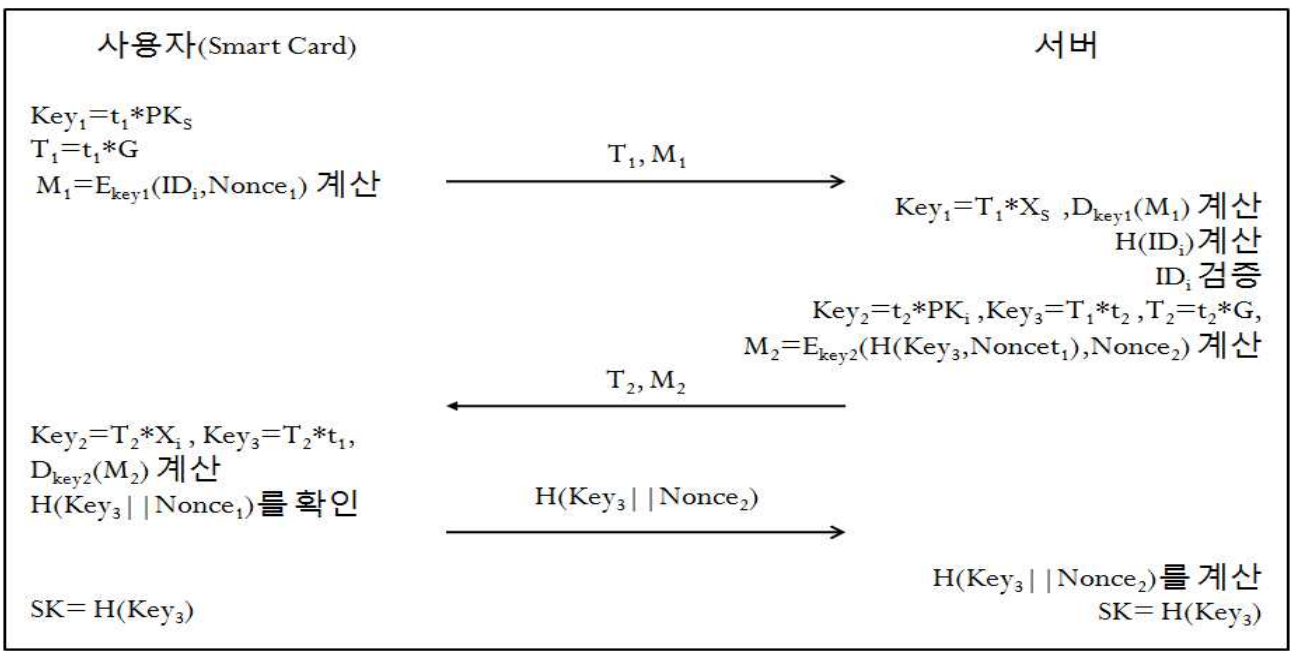

그림 2 제안하는 프로토콜의 익명의 유저 확인 및 키 동의 단계

공격자가 세션 키 $H(Key_3)$를 얻고 통신 메시지를 도청했더라도, 공격자는 도청으로부터 비밀 값 T_1, T_1 에 포함된 사용자와 서버의 개인키 X_i, X_S를 추론할 수 없고 메시지를 복원할 수 없다. 이 처럼 하기 위해서 공격자는 타원곡선 이산대수문제를 풀어야 한다.

다. 재생 공격에 대한 저항

익명의 유저 확인 및 키 동의 단계의 1 단계에서 모든 사람은 도청한 서비스 요청을 서버에게 서비스 재생 할 수 있다. 서버는 응답 신호를 되돌려 보내야 한다. 첫째로 공격자는 사용자의 ID_i를 알아야 한다. 이 처럼 하기 위해서는 서버의 비밀 키가 드러나야 한다. 공격자가 3 단계에서 정확한 검증을 보내기 위해서는 공격자는 2 단계에서 사용자의 비밀 키 X_i 를 획득해야 하고, 그 것을 이용하여 메시지를 복원해야 한다. 위의 문제는 매우 어렵다. 그러므로 우리 프로토콜은 재생 공격에 안전하다.

라. 위조 공격에 대한 저항

한 명 또는 두 명의 사용자가 선형적인 특징과 자신들의 비밀 키를 이용하여 새로운 제3자의 비밀 키를 얻었다 할지라도 그들이 공개키 테이블에서 얻을 수 있는 것은 제 3자의 ID_i가 아니라 $H(ID_i)$를 얻을 수 있다. 그러나 $H(ID_i)$에서 ID_i를 알아내는 안전한 해쉬 함수를 사용한다면 불가능 하다. 따라서 공격자는 다른 사용자로 위장할 수 없다.

마. DOS 공격에 대한 저항

만약 누군가가 위조된 메시지를 보내서 사용자나 서버를 속이려 한다면 그들은 비밀 키를 얻기 위해 어려운 타원곡선 이산대수 문제를 풀어야 하고 그것을 사용해 거짓 메시지를 보내야 한다. 우리는 타원곡선 이산대수 문제를 푸는 것이 매우 어렵다는 것을 알고 있다.

바. 완전한 전방향 안전성

만약 사용자나 서버의 비밀 키가 공격자에 의해 들어 났다면, 공격자는 서비스 요청이나 M_2를 복원 할 수 있다. 공격자는 여전히 비밀 값 T_1, T_2없이 도청과 복원 된 메시지로부터 과거의 공통 세션 키 $H(Key_3)$를 추론할 수 없다. 공격자는 타원 곡선 이산대수 문제를 풀어야 한다.

아. 익명성

익명의 유저 확인 및 키 동의 단계 1 단계에서 사용자의 ID_i는 암호화되어서 전송된다. 또한 테이블에도 ID_i대신 $H(ID_i)$만이 나타나 있다. 따라서 우리가 ID_i를 알아내기 위해서는 M_1을 Key_1을 사용해서 복원해야한다. 아무도 서버의 비밀 키 없이는 복원 할 수는 없다.

5. 결론

제안하는 프로토콜은 Ren-Chiun Wang의 프로토콜을 개량한 것이다. 제안하는 프로토콜은 Ren-Chiun Wang의 프로토콜이 제공하는 안전성을 제공하면서도 취약점을 효과적으로 보완했다. 따라서 제안하는 프로토콜은 방송 콘텐츠 암호화에 필요한 세션 키를 동의하는데 알맞은 프로토콜이다.

6. 참고문헌

[1] W.B. Lee and C.C. Chang, “"User Identification and Key Distribution Maintaining Anonymity for Distributed Computer Network"", Computer Systems Science and Engineering, Vol. 15, No. 4, pp. 113-116, 2000.

[2] W. Diffie and M. Hellman, “"New Directions in Cryptography"", IEEE Trans Inf Theory, Vol. 22, No. 6, pp. 644-654, 1976.

[3] T.S. Wu and C.L. Hsu, “"Efficient User Identification Scheme with Key Distribution Preserving Anonymity for Distributed Computer Networks"", Computer & Security, Vol. 23, No. 2, pp. 120-125, 2004.

[4] Y.J. Yang, S.H. Wang, F. Bao, J. Wang, and R.H. Deng, “"New Efficient User Identification and Key Distribution Scheme Providing Enhanced Security"", Computer & Security, Vol. 23, No. 8, pp. 697-704. 2004,

[5] C.L. Lin and T. Hwang, “"A Password Authentication Scheme with Secure Password Updating"", Computers & Security, Vol. 22, No. 1, pp. 68-72. 2003,

[6] C.-C. Yang and R.-C.Wang. "Cryptanalysis of a user friendly remote authentication scheme with smart cards". Computers & Security, Vol. 23, pp. 425-427, 2004.

[7] C.-C. Yang, R.-C.Wang, and T.-Y. Chang. "An improvement of the yang-shieh password authentication schemes." Applied Mathematics and Computation, Vol. 162, pp. 1391-1396, 2005.

[8] C.-C. Yang, R.-C. Wang, and W.-T. Liu. "Secure authentication protocol for session initiation protocol." Computers & Security, Vol. 24, pp. 381-386, 2005.

[9] Y. Yang, S. Wang, F. Bao, J. Wang, and D. H. Deng. "New efficient user identification and key distribution protocol providing enhanced security." Computers & Security, Vol. 23, No. 8, pp. 697-704, 2004.

[10] W.-B. Lee and C.-C. Chang. "User identification and key distribution maintaining anonymity for distributed computer network." Computer System Science Engineering, Vol. 15, No. 4, pp. 113-116, 2000.

[11] K. Mangipudi and R. Katti. "A secure identification and key agreement protocol with user anonymity(sika)". Computers & Security, Vol. 25, pp. 420-425, 2006.

[12] R. Wang, W. Juang, C, Wu, C. Lei "A Lightweight Key Agreement Protocol with User Anonymity in Ubiquitous Computing Environments" 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp. 313-318 2007.