제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

임시 정보를 이용한 안전한 키 분배 기법에 관한 연구

서대희*, 이임영*
*순천향대학교 정보기술공학부
e-mail:1636711@hitel.net

A Study on key distribution protocol using temporary information

Dae-Hee Seo*, Im-Yeong Lee*
*Division of Information Technology Engineering
SoonChunHyang University

요약

최근 인터넷의 급성장에 따라 유·무선 네트워크를 기반으로 하여 사용자 정보를 이용한 안전한 보안 서비스가 요구되고 있다. 그러나 서비스 사용자의 증가에 따른 개인 정보의 안전성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 사용자의 임시 정보를 이용한 안전한 키 분배 기법을 제안한다. 제안된 방식은 기존의 사용자 정보를 기반으로 이루어지는 키 분배 프로토콜의 취약성을 보완하면서 확장이 가능한 새로운 방식을 제안함으로써 안전성과 확장성을 보장하고 있다. 제안 방식은 기존에 제시된 사용자 정보 기반의 키 분배 프로토콜과 비교 분석함으로서 안전성과 효율성을 검증한다.

1. 서 론

인터넷 활용 영역이 다양한 분야로 확대되면서 사용자들에게 여러 가지 보안 서비스를 제공해 주기 연구가 활발히 진행중에 있다.

특히, 안전한 통신을 위한 안전한 키 분배 프로토콜중 개인 식별 정보에 기반한(ID-based) 암호 방식은 1984년 Shamir에 의해 최초로 소개되었다. 개인 식별 정보에 기반한 암호 방식의 경우 개인 ID 자체가 공개키의 역할을 하는 방식이다.

ID 기반의 방식의 경우 스마트 카드를 이용한 방식에도 적용이 가능할 뿐만 아니라 공개키 암호 방식을 사용하면서 공개키 디렉토리를 필요로 하지 않는 방식으로 많이 응용되고 있다.

본 논문에서는 사용자의 임시 정보를 이용한 안전한 키 분배 프로토콜을 제안하였다. 본 논문의 2장에서는 사용자 정보를 기반으로한 키 분배 프로토콜이 가져야 하는 보안 요구사항을 제시하고 3장에서는 기존의 사용자 식별 정보를 기반으로한 키 분배 방식에 대한 안전성을 분석한다. 4장에서는 2장에서의 보안 요구사항을 만족할 수 있는 키 분배 프로토콜을 제안한다. 5장에서는 제안된 방식을 기존 방식과 비교 분석한 뒤 6장에서 결론을 맺고자 한다.

2. 개인 식별 정보에 기반한 프로토콜 고려사항

본 장에서는 개인 식별 정보에 기반한 프로토콜의 보안 고려사항을 제시하고자 한다. 기본적으로 요구되는 기밀성, 무결성에 대한 보안 서비스를 제외하고 추가적인 사항에 대해서만 논하고자 한다.[4-6]

- 익명 사용자 : 송신자와 수신자 사이에 전송되는 데이터에서 각각의 비밀스러운 개인 정보를 공개하지 않으면서 안전한 세션키 설정이 가능해야 한다.
- 인증 : 키 분배 프로토콜이 진행되는 동안 각 개체는 자신이 통신하고자 하는 개체의 인증과 자신이 통신하는 수신자만이 비밀 세션키를 계산할 수 있고 상대방이 실제로 그 키를 가지고 있음을 확인할 수 있어야 한다.
- 알려진 키에 대한 안전성 : 키 분배 프로토콜을 수행한 사용자들은 자신이 의도하지 않은 다른 사용

자와 세션키를 공유하지 않았음을 확인할 수 있어야 한다.

- 키 갱신 : 고정적인 세션키의 설정은 세션키가 노출될 경우 사용자간의 비밀스러운 세션에 보안적 취약점을 노출 시킬 수 있다.

- PFS(Perfect Forward Secrecy): 각 사용자의 비밀키가 노출되더라도 두 사용자간에 과거에 설정했던 세션키는 노출되지 않아야 한다.

3. 개인 식별 정보를 기반의 키 분배 프로토콜 관련 연구

개인 식별 정보를 기반의 프로토콜의 경우 1984년에 최초로 소개된 이후 Fundamental ID-based 방식, 확장 프로토콜 방식, 자체 인증에 기반한 프로토콜 방식등 여러 프로토콜이 연구되고 있다.

그러나 각각의 방식의 경우 다음과 같은 문제점이 발생하고 있다.[1-4]

① Fundamental ID-based 방식

- 인증 : 본 방식의 경우 묵시적인 키를 인증하고 ID에 기반하여 개체를 인증한다. 따라서 ID가 변조될 경우 사용자 위장이 가능하다.

- 키 위장 : 공개된 계수(ID or 공개키)를 변조하여 개체간에 이루어지는 키에 대한 위장 공격이 가능하다.

② 확장된 ID-based 방식

- 인증 : 확장된 방식의 경우 개체인증과 키에 대한 확인 기능을 제공하지 않는다.

- 키 갱신 : 본 방식의 경우 송신자가 생성한 랜덤수를 기반으로 하여 키 갱신이 이루어지는 일방향성을 갖게 된다.

- 알려진 키에 대한 안전성 : 일방향성 키 갱신을 통해 수신자측에서 분신된 키에 대한 안전성을 보장할 수 없다.

③ 자체인증에 기반한 방식

- 인증 : 자체 인증 방식의 경우 개체 인증과 키 확인 기능을 제공하지 못한다.

- 알려진 키에 대한 안전성 : 자체 인증에 기반한 방식은 고정된 비밀키를 사용하여 이전 비밀키가 노출될 경우 안전성에 심각한 취약점을 내포하고 있다.

- 키 갱신 : 고정된 비밀키의 사용으로 인한 묵시적 키 인증은 비밀키가 노출될 경우 공격자에 의한 위장 공격에 노출되어 있다.

4. 익명정보를 이용한 안전하고 효율적인 키 분배 프로토콜 제안

본 장에서는 사용자의 개인 비밀 정보를 안전하게 유지하면서 사용자의 임시정보를 이용한 안전하고 효율적인 키 분배 방식을 제안한다.

4.1 각 개체 및 시스템 계수

다음은 사용자의 익명정보를 이용한 안전한 키 분배 프로토콜을 제안하기 위한 시스템 계수를 기술한다.

- 시스템 계수(a : Alice, b: Bob)

p, q : 공개된 소수 ($512bit \le Length \le 1024bit$, $2^{L-1} < p_* < 2^L$을 만족하는 소수, $q_* \mid (p_* - 1)$)

r : 의사난수

R_a, R_b : 사용자 A, B의 개인키 ($R_a \in Z_n$)

X_a, X_b : 사용자 A, B의 공개키 ($X_a = g^{R_a} \bmod p$ $X_b = g^{R_b} \bmod p$

g : Z_n상에서의 최대 위수를 갖는 원소

KH : Keyed 해쉬 함수

PI : 사용자 신원정보(PI : Personal Information)

T : 타임 스탬프

4.2 프로토콜 진행

Step 1 신원정보 등록 및 익명 ID발급 단계

① Alice는 자신이 생성한 의사난수 r_a를 이용하여 K_a를 다음과 같이 생성한다.

$$K_a = g^{r_a} \bmod p$$

생성된 K_a를 keyed 해쉬 함수의 키로 사용하여 Alice의 신원정보 PI_a와 X_a를 연접한 뒤 e_a를 생성한 후 Z_a와 A_a를 생성한다.

$$e_a = KH_{K_a}(PI_a \| X_a)$$

$$Z_a = (e_a \| T_a)$$

$$A_a = g^{(R_a - r_a)} \bmod p$$

생성된 K_a, A_a를 TTP의 공개키로 암호화하여 다음을 전송한다.

$$E_{X_{ttp}}(K_a \| A_a \| Z_a),\ e_a,\ T_a$$

② TTP는 전송된 $E_{X_{ttp}}(K_a \| A_a)$를 자신의 공개키로 복호화한 뒤 $Z_a' = Z_a$이면 TTP는 Alice의 익명 ID인 AID를 생성한 뒤 공개키 서명하여 공개된 환경에 $Sig_{R_{ttp}}(AID)$, T_{ttp}를 공개한다.

$$AID = (A_a)^{r_{ttp}} \bmod p$$

Step 2 익명 ID를 기반으로 Alice와 Bob의 인증 및 키 분배 프로토콜 진행 단계-1

Alice는 Step 1에서 생성된 e_a, Z_a를 이용하여 Bob의 인증 및 키 분배 설정을 위한 D_a, S_a를 다음과 같이 생성한다.

$$D_a = r_a + R_a A_a \bmod p$$

$$S_a = \frac{K_a}{R_a * Z_a} \bmod q$$

이상의 내용을 생성한 Alice는 Bob에게 다음을 전송한다.

$$AID,\ A_a,\ D_a,\ S_a,\ T_a$$

Step 3 익명 ID를 기반으로 Alice와 Bob의 인증 및 키 분배 프로토콜 진행 단계-2

Step 1에서 Alice로부터 전송받은 K_a를 기반으로 의사난수 r_{ttp}를 생성하여 K_{ttp}을 계산한다.

$$K_{ttp} = g^{(K_a \cdot r_{ttp})}$$

TTP는 K_a와 r_{ttp}, Z_a를 Bob의 공개키로 암호화하고, K_{ttp}를 해쉬한후 다음을 Bob에게 전송한다.

$$E_{X_b}(Z_a \| r_{ttp} \| K_a),\ h(K_{ttp}),\ T_{ttp}$$

Step 4 검증과정을 통한 Alice와 Bob의 인증 및 분배 단계

Bob의 경우 TTP와 사용자 A에게서 전송된 정보에 대한 검증을 수행하기 위해 TTP에서 전송된 $E_{X_B}(Z_a \| K_{ttp} \| r_{ttp})$ 를 자신의 개인키로 복호화하여 Z_a과 r_{ttp}, K_a를 획득하고 다음의 검증 과정을 거쳐 그 정당성을 확인한다.

① Bob은 TTP와 Alice에게서 전송된 정보의 검증을 수행한다.

$$K_{ttp} = (g^{r_{ttp}} \cdot X_a \cdot g^{Z_a})^{S_a}$$

$$= (g^{r_{ttp}} \cdot g^{R_a} \cdot g^{Z_a})^{\frac{K_a}{R_a * Z_a}}$$

$$= g^{(K_a \cdot r_{ttp})}$$

전송 정보의 검증이 올바르다면 다음과 같이 임시정보의 검증을 수행한다.

$$AID = (g^{D_a} \cdot X_a^{-A_a} \cdot A_a \cdot K_a^{-1})^{r_{ttp}} \bmod p$$

$$= (g^{r_a + R_a A_a} \cdot g^{-R_a A_a} \cdot g^{R_a - r_a} \cdot g^{-r_a})^{r_{ttp}} \bmod p$$

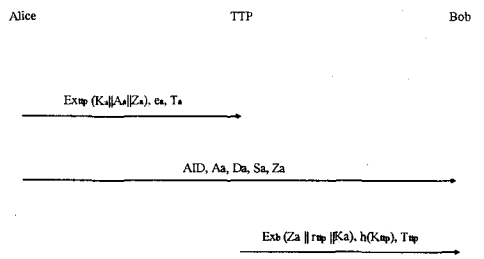
$$= (g^{R_a - r_a})^{r_{ttp}} \bmod p$$

$$= (A_a)^{r_{ttp}} \bmod p$$

임시정보 검증과 전송 정보의 검증을 수행한 후 모두가 올바르다면 Bob은 Alice를 묵시적인 인증을 수행하고 다음과 같은 세션키 C를 생성한다.

$$C = H(AID \oplus K_a) \bmod p$$

제안된 프로토콜의 전체 프로토콜의 흐름은 그림 1과 같이 표현할 수 있다.



(그림 1) 제안된 안전한 키 분배 프로토콜

5. 제안방식 비교 분석

본 제안 방식은 2장에서 제시한 보안 요구사항을 다음과 같이 만족한다.

- 익명 사용자 : 제안 방식의 경우 송신자와 수신자가 세션키 설정을 위해 개인의 비밀 정보가 아닌

TTP에 의해 생성된 임시 정보를 이용하게 된다.

- 인증 : 제안방식은 키 분배 프로토콜이 진행되는 동안 묵시적인 개체인증을 통해 송/수신자의 인증이 가능하며 인증된 수신자만이 비밀 세션키를 계산할 수 있다.
- 알려진 키에 대한 안전성 : 제안방식의 프로토콜을 수행한 사용자의 경우 의도되지 않은 사용자와 세션키를 공유하지 않았음을 확인하기 위해 공개키 암호화 알고리즘과 의사난수를 적용하였다.
- 키 갱신 : 송신자에 의해 생성된 의사난수를 이용해 계산된 K를 세션키 생성에 계수로 사용함으로써 새로운 세션이 설립될 경우 고정된 키의 사용으로 인한 키 갱신의 취약점을 보완하였다.
- PFS(Perfect Forward Secrecy): 제안된 프로토콜은 세션이 새롭게 생성될 때 마다 생성되는 새로운 의사난수를 이용하여 과거에 설정했던 세션키와는 다른 세션키가 생성되도록 하였다.

5. 결론

정보통신의 급속도로 발전하고 있는 가운데 안전한 네트워크 서비스에 대한 연구가 빠르게 진행되어 가고 있으며, 이를 기반으로 컴퓨터 분야 뿐만 아니라 많은 유·무선 환경에서 적용할 수 있는 보안 기술이 필요하게 되었다. 이러한 보안 기술중에서 공개 환경에서 사용자들의 개인 정보를 보호하면서 기존의 인터넷 환경을 유지할 수 있는 기술에 대한 연구는 미흡한 실정이다. 따라서 본 논문에서는 기존의 인터넷 환경을 이용하면서 안전성을 유지할 수 있는 키 분배 프로토콜을 제안하였다.

본 논문에서 제안된 방식은 기존의 ID/패스워드 기술을 그대로 이용하면서 개인의 신원정보를 노출시키지 않으면서 상호 안전한 통신이 가능한 방법을 제시하였다. 제안된 방식은 기존의 ID기반의 키 분배 프로토콜의 확장으로 구분될 수 있으며, 프로토콜의 안전성이 TTP의 안전성에 귀착된다 볼 수 있다.

향후 연구 방향을 좀 더 실용적이면서 갱신 및 탈퇴가 자유로운 환경에서의 키 관리 구조에 대한 연구가 지속될 것이다.

6. 참고문헌

[1]. ANSI X9.42, "Agreement of sysmmetric Key on Using Diffie-Hellman Cryptography", 2001

[2]. ANSI X9.63, "Public Key Cryptography for the finanacial service industry : key agreement and key transport using elliptic curve cryptography", 2001

[3]. C.J. Mitchell, M.Ward, P. Wilson, "Key control in key agreement protocols", Electronics Letters 14th, Vol.34, No.10, May, 1998

[4]. Y. Dodis, S.Micali, "Parallel Reducibility for Information Theoretically Secure Computation", CRYPTO '00, 2000

[5]. S.J. Kim, M. Mambo et al, "On the security of the Okamoto-Tanaka ID-Based Key Exchange scheme against Active attacks", IEICE Trans, pp231-238, Jan. 2001

[6]. Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996

[7]. 이임영 "전자상거래 보안입문", 생능출판사, 2001