M-Commerce 상에서 키 복구를 지원하는 무선 인증 및 키 설립 프로토콜

(A New Key Recovery Protocol of Wireless Authentication Key Establishment for the M-Commerce)

이 용 호 † 이 임 영 ††
(Yong-Ho Lee) (Im-Yeong Lee)

요 약 무선 인터넷이 활성화되면서 E-Commerce에서 M-Commerce로의 전환이 빨라지고 있으며, 많은 서비스 제공자들은 무선 기술을 이용해 다양한 M-Commerce 서비스를 사용자들에게 제공하고 있다. M-Commerce가 활성화되면서 보안 프로토콜에 대한 중요성이 인식되고 있다. 특히, 무선상에서 이루어지는 WAKE(Wireless Authentication and Key Establishment) 프로토콜은 M-Commerce를 수행하고자 하는 사용자와 서비스 제공자가 필수적으로 거쳐야 하는 것으로 그 중요성은 매우 크다고 할 수 있다. 키 복구 기술은 사용자가 키를 유실하거나 또는 암호를 불법적으로 사용하였을 경우 키 복구를 통해서 키에 대한 접근을 할 수 있게 해주는 키 관리의 한 부분이다. WAKE 프로토콜에 키 복구 기능을 지원하고자 하는 노력은 ASPeCT 프로젝트에 의해서 처음으로 시도되었다. 이후 다양한 WAKE 키 복구 프로토콜이 제안되었다. 본 논문에서는 기존에 제안되었던 WAKE 키 복구 프로토콜의 문제점을 알아보고 이들을 해결하는 새로운 WAKE 키 복구 프로토콜을 제안한다.

키워드 : 무선, 인증, 키 설립, 키 복구, 무선 전자상거래

Abstract As Mobile Internet gets more popular, the switchover of E-Commerce to M-Commerce gets faster and many service providers offer diverse M-Commerce service by using mobile technology. Also, as M-Commerce makes rapid progress, the security protocol gets more widely recognized for its significance. In particular, WAKE(Wireless Authentication and Key Establishment) protocol carried out wirelessly is of great importance, since the user and service provider must get through to carry out the M-Commerce. Key recovery method is a part of the key management in order to provide an emergency recovery of key whenever necessary, like when the user lost the key or the cryptosystem was illegally used. The ASPeCT project first tried to support the key recovery function in WAKE protocol Since then, a variety of WAKE Key Recovery protocols have been proposed. In this thesis, problems of WAKE Key Recovery protocols proposed so far are analyzed and new WAKE Key Recovery protocol is suggested to solve those problems.

Key words : Wireless, Authentication, Key Establishment, Key Recovery, M-Commerce

1. 서 론

정보통신 기술의 발전으로 인하여 M-Commerce 사용자가 기하급수적으로 증가하고 있으며, 이에 따라 관련 서비스 또한 증가하고 있다. 이와 더불어 사용 환경이 유선에서 무선으로 넘어오면서 보안에 대한 사용자들의 인식이 한층 높아졌다. 그러나 무선 환경은 유선 환경에 비해 계산능력이 적다는 문제점을 가지고 있다. 따라서 이러한 단점을 고려하여 보안 기술을 적용하여야 한다. 보안 기술은 유선 환경에서와 마찬가지로 안전한 전자상거래 서비스를 제공하기 위해서 통신정보에 대한 기밀성, 개체 인증 그리고 무결성 등의 기능을 제공해야 한다[1].

M-Commerce를 수행하기 위해서는 참여하는 개체간 즉, 사용자와 사용자 혹은 사용자와 서비스 제공자 사이

† 정 회 원 : 한국정보통신기술협회 S/W시험인증센터 연구원
abysskey@tta.or.kr
†† 종신회원 : 순천향대학교 정보기술공학부 부교수
imylee@sch.ac.kr
논문접수 : 2002년 8월 13일
심사완료 : 2003년 2월 4일

에 WAKE(Wireless Authentication and Key Establishment) 프로토콜을 수행해야 한다. 이 프로토콜은 두 개체 사이에 인증과 암호화에 사용되는 비밀키를 설립하는 것으로써 M-Commerce에서 반드시 필요한 프로토콜이라 할 수 있다. 무선 환경이 고려되기 시작하면서부터 WAKE 프로토콜에 키 복구 기능을 추가하고자 하는 노력이 있었다. 최초의 WAKE 키 복구 프로토콜은 ASPeCT(European Commision ACTS Project) 프로젝트에 의해 개발되었다. 키 복구는 사용자가 키를 분실 혹은 도난 당해서 중요 데이타에 대해 접근을 할 수 없게 되거나, 암호를 불법적인 목적으로 사용하여 국가의 정당한 법 집행 권한을 방해할 경우에 일정한 조건을 갖추면 키 복구 과정을 수행하여 암호화된 데이타에 대해 접근할 수 있도록 하는 키 관리 기술중의 하나이다[2]. 본 논문에서는 기존 연구들이 소개하고 있는 방식들에 대해 분석하고 이를 토대로 WAKE 키 복구 프로토콜의 요구사항을 도출하며, 이를 해결할 수 있는 새로운 WAKE 키 복구 프로토콜을 제안한다.

본 논문은 총 6장으로 구성되고 각각의 내용은 다음과 같다. 2장에서는 WAKE 키 복구 프로토콜의 요구사항에 대하여 알아보고, 3장에서는 기존에 제안되었던 방식들에 대해서 살펴본다. 4장에서는 제안 방식을 소개하며, 5장에서는 제안 방식을 고찰하고 기존 방식과 비교 분석을 수행한다. 마지막으로 6장에서 결론을 맺는다.

2. WAKE 키 복구 프로토콜의 요구사항

2.1 기본적인 보안 요구사항

WAKE 키 복구 프로토콜이 가져야 하는 필수적인 5가지 요구사항에 대하여 알아본다[2,3].

- 인증 : 인증이란 전송된 메시지가 자기라고 주장하는 실제의 출처로부터 전송되었음을 수신자에게 확인시키는 것이다.
- 기밀성 : 기밀성이란 전송 정보에 대한 도청이나 감시와 같은 소극적 공격으로부터 전송 정보를 보호하는 요구사항이다.
- 무결성 : 무결성이란 전송 정보가 전송되는 과정에서 제 3자에 의해 불법적으로 수정 또는 위조되지 않고 수신됐음을 보장하는 요구사항이다.
- 무선 환경을 고려한 멱승 연산량 : 무선 환경에서 사용되는 무선 단말기는 연산량이 작다. 따라서 WAKE 키 복구 프로토콜을 수행할 때 보안성을 유지하면서 연산량을 최소화하여야 한다.
- 위장 공격 방지 : 위장 공격 방지란 제 3자가 사용자 또는 서비스 제공자로 위장하여 통신 상대방에게 피해를 주는 행위를 방지하기 위한 요구사항이다.

2.2 키 복구 기능을 고려한 보안 요구사항

여기서는 WAKE 프로토콜에 키 복구 기능을 추가하면서 고려되어야 하는 4가지 요구사항에 대하여 알아본다[2,6].

- 복구 공개 검증성 : WAKE 키 복구 프로토콜을 수행하게 되면 통신을 수행하는 두 개체 사이에 비밀키가 설립된다. 이러한 비밀키에 대하여 유사시 키 복구가 가능하다는 것을 공개적으로 검증 가능해야 한다.
- 적은 계산량 : WAKE 프로토콜에 키 복구 기능을 추가하기 위해서 사용되는 자원은 최소화되어야 한다.
- 도메인 확장성 : WAKE 키 복구 프로토콜에서 키 복구 기관이 두 개로 분리되는 경우 두 개의 키 복구 기관 모두에게 해당하는 사용자의 키 복구 기능을 제공해야 한다는 것이다.
- 불법적인 키 복구 방지 : WAKE 프로토콜에 키 복구 기능을 추가하기 위해서는 통신 당사자를 제외한 다른 개체가 필요하게 된다. 그리고 이 개체에게 통신 당사자간에 설립되는 키에 대한 관련 정보를 위탁하게 되므로, 불법적인 키 복구에 대한 위험이 존재한다.

3. 기존 방식 분석

3장에서는 기존에 제시된 3가지 WAKE 키 복구 프로토콜에 대해 설명한다.

3.1 R-M WAKE 키 복구 프로토콜

여기서는 1999년 Rantos와 Mitchell이 제안한 WAKE 키 복구 프로토콜을 소개한다[2,4].

(1) 사전 준비 단계

1) 사용자는 TTP에게 초기값 ku를 위탁한다.

2) 사용자는 랜덤값 s를 선택하여 u를 계산한 후, u를 이용하여 L을 계산한다.

- $u = f(k_u, s)$, (f는 임의의 일방향 함수)
- $L = (g^{u_0})^u$

(2) WAKE 단계

WAKE 단계는 그림 1과 같다.

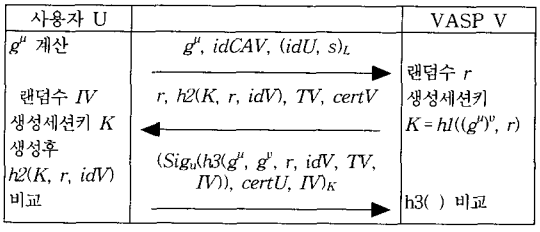

그림 1 R-M WAKE 키 복구 프로토콜

(3) 키 복구 단계

1) 키 복구 기관은 통신 데이타 감청시, 전송 정보들 중에서 g^{μ}, $(idU, s)_L$을 획득한다. 그리고 L과 s를 차례대로 계산한다.

$$L=(g^{\mu})^{w}$$

$$s=((idU, s)_L)_L$$

2) 사용자가 위탁한 k_u와 s를 이용하여 u를 계산한다.

$$u=f(k_u, s)$$

3) u를 이용하여 세션키를 복구한다.

$$K=h1((g^{v})^{u}, r)$$

3.2 N-P-B-E WAKE 키 복구 프로토콜

이 방식은 Nieto 등이 R-M WAKE 키 복구 프로토콜에서 VASP 위장 공격이 가능하다는 문제점을 제기하고 이를 해결하고자 제안한 프로토콜이다[5].

(1) 키 복구 정보 생성 단계

1) 키 복구 기관은 사용자와 공유된 w_u를 이용하여 ψ를 계산하고, 이를 공개한다.

$$\psi=g^{wu} \bmod q$$

2) 사용자는 랜덤수 u를 선택하고 U를 계산하여 공개한다.

$$U=g^{u} \bmod q$$

3) 사용자는 c를 계산한다.

$$c=h(U) \bmod q$$

4) 사용자는 s를 계산하여 공개한다.

$$s=w_u*c+u \bmod q$$

(2) 키 복구 정보 공개 검증 단계

이 단계에서 제 3자는 누구나 키 복구 정보가 올바르게 생성되었다는 것을 공개적으로 검증 가능하다.

1) 키 복구 정보를 공개적으로 검증하고자 하는 사용자는 c'를 계산한다.

$$c'=h(U) \bmod q$$

2) 공개된 값들을 이용하여 g^{s}와 $\psi^{c'}*U$를 계산하고 이것이 같은지 비교한다. 만약 같다면 키 복구 정보가 올바르게 생성되었다는 것이 증명된다.

$$g^{s} \stackrel{?}{=} \psi^{c'}*U$$

(3) WAKE 단계

상기 모든 과정이 완료되면 WAKE 단계가 진행된다. WAKE 단계는 그림 2와 같다.

(4) 키 복구 단계

이 과정은 키 복구 기관에 의해 이루어지게 되며, 전송되는 정보 중 $r\oplus g^{uv}$를 획득하고, 다음과 같은 과정을 진행하여 키를 복구한다.

1) 공개되어 있는 U를 이용하여 c를 계산한다.

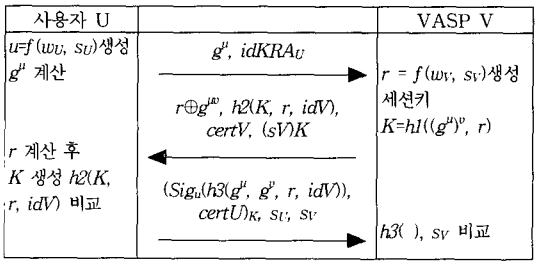

그림 2 N-P-B-E WAKE 키 복구 프로토콜

$$c=h(U) \bmod q$$

2) 계산된 c와 공유된 s를 이용하여 u를 계산한다.

$$u=s-w_u*c \bmod q$$

3) 계산된 u와 공개 정보 g^{v}를 이용하여 $g^{uv} \bmod p$를 계산하고, $r\oplus g^{uv}$에서 r을 획득한다.

$$r=r\oplus g^{uv}\oplus g^{uv}$$

4) 계산된 g^{uv}와 r을 이용하여 세션키 K를 복구한다.

$$K=h1((g^{v})^{u}, r)$$

3.3 K-L WAKE 키 복구 프로토콜

이 방식은 N-P-B-E WAKE 키 복구 프로토콜에서 VASP가 속한 도메인에서는 키 복구 정보 생성과 공개 검증 그리고 키 복구가 수행되지 않는다는 문제점을 제시하고 이를 해결하고자 제안한 프로토콜이다[2,6]. 이 방식은 대부분 상기 N-P-B-E WAKE 키 복구 프로토콜과 동일하다. 그림 3은 K-L WAKE 단계를 나타낸다.

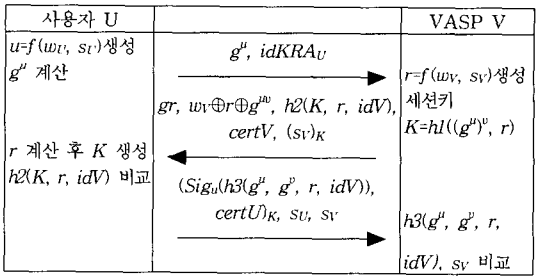

그림 3 K-L WAKE 키 복구 프로토콜

다음은 N-P-B-E WAKE 키 복구 프로토콜에서 추가된 부분이다.

- VASP가 속한 도메인에 사용자측과 동일하게 키 복구 정보 생성 과정과 키 복구 정보 공개 검증 과정을 그대로 추가하였다.
- VASP가 속한 도메인에서도 키 복구를 가능하게 하기 위해서 WAKE-KR 프로토콜 과정에서 $w_v\oplus r$

$\oplus g^{w_U}$를 추가하였다. VASP가 속한 도메인의 키 복구 기관은 w_v와 r를 알 수 있으므로 g^{w_U}를 계산할 수 있고, 이를 이용하여 세션키를 복구할 수 있다.

4. 제안 방식

4.1 시스템 계수

다음은 제안하는 프로토콜에 사용되는 시스템 계수들을 나타낸다.

- p : 큰 소수
- g : Z_p상의 원시원소
- $*$: 사용자 A, 사용자 B
- X_*, Y_* : $*$의 개인키와 공개키($Y_*=g^{X_*} \bmod p$)
- w_* : $*$와 신뢰기관간에 공유된 비밀값
- j_* : $*$와 키 복구 기관간에 공유된 비밀값
- $Cert(*)$: $*$의 공개키 인증서
- h : 안전한 일방향 해쉬함수
- R_A, R_B : 사용자 A와 사용자 B가 각각 생성하는 랜덤수

4.2 프로토콜

4.2.1 초기화 단계

초기화 단계를 수행하기 전에 사용자는 공개키 기반 구조하에서 공개키 쌍을 생성하여 인증서를 발행 받는 선수 과정을 거친다. 이 과정을 마친 후 초기화 단계를 수행한다. 유사시 키 복구를 위한 비밀정보 위탁 및 키 복구 정보 생성 과정에서 사용자와 키 복구 기관 그리고 사용자와 신뢰 기관 사이에 이루어지는 통신은 안전한 채널을 통하여 이루어진다고 가정한다.

(1) 유사시 키 복구를 위한 비밀정보 위탁 및 키 복구 정보 생성 과정

여기서는 사용자 A가 수행하는 과정만을 나타낸다. 사용자 B는 사용자 A와 동일한 과정을 수행한다.

1) 사용자 A는 키 복구 기관과 비밀값 j_A를 안전하게 공유한다.
2) 키 복구 기관은 공유된 비밀값의 공개 검증값 J_A를 계산하여 공개한다.

$$J_A=g^{j_A} \bmod p \quad (1)$$

3) 사용자 A는 신뢰 기관과 비밀값 wA를 안전하게 공유한다.
4) 신뢰 기관은 공유된 비밀값의 공개 검증값 WA를 계산하여 공개한다.

$$W_A=g^{w_A} \bmod p \quad (2)$$

(2) 키 복구 정당성 공개 검증을 위한 공개 파라미터 생성 과정

여기서는 사용자 A가 수행하는 과정만을 나타낸다. 사용자 B는 사용자 A와 동일한 과정을 수행한다. 또한 사용자가 w_A와 j_A를 분실하지 않았다고 가정한다.

1) 사용자 A는 키 복구 기관과 신뢰 기관이 공개한 값을 이용하여 c_A와 s_A를 계산하고, s_A를 공개한다.

$$c_A=J_A \oplus W_A \bmod p$$
$$sA=w_A+j_A*c_A \bmod p \quad (3)$$

(3) 키 복구 정당성 공개 검증 과정

1) 키 복구 정당성을 공개 검증하고자 하는 개체는 사용자가 공개한 s^A를 이용하여 식 (4)의 좌변과 같이 계산하고, 키 복구 기관과 신뢰 기관이 각각 공개한 J_A와 W_A를 이용하여 식 (4)와 같이 우변을 계산한다. 계산된 결과를 비교하여 같으면 키 복구 정당성을 만족하게 된다.

$$g^{sA} \bmod p \stackrel{?}{=} J_A^{cA}*W_A \bmod p \quad (4)$$

위 식은 다음과 같이 유도된다.

$$J_A^{cA}*W_A \bmod p$$
$$=g^{jA*cA}*g^{wA} \bmod p$$
$$=g^{sA} \bmod p$$

4.2.2 무선 인증 및 키 설립 단계

이 단계는 초기화 단계를 수행한 후에 이루어지는 단계로써 사용자 A와 사용자 B간에 이루어진다.

1) 사용자 A는 비밀값 j_A와 w_A를 이용하여 키 복구 정보 KRI_A와 K_A 그리고 인증 정보 RK_A를 다음과 같이 계산한다.

$$KRI_A = j_A \oplus w_A$$
$$K_A = KRI_A \oplus R_A$$
$$RK_A = g^{K_A} \bmod p \quad (5)$$

2) 사용자 A는 인증 정보 RK_A와 랜덤수 R_A에 서명을 수행하여 사용자 B에게 전송한다.

$$Sig_{XA}(RK_A||R_A) \quad (6)$$

3) 사용자 B는 수신된 서명문을 검증한 후 RK_A와 자신의 개인키 X_B를 이용하여 SK_B를 계산한다.

$$SK_B = RK_A^{XB} \bmod p$$
$$= g^{KA*XB} \bmod p \quad (7)$$

4) 사용자 B는 전송된 R_A와 자신이 생성한 SK_B 그리고 R_B를 생성하여 다음과 같이 세션키 K_{AB}를 계산한다.

$$K_{AB} = h(SK_B||R_A||R_B) \quad (8)$$

5) 사용자 B는 자신이 가지고 있는 정보와 전송된 정보를 이용하여 무결성을 위한 검증값 hm을 계산하고 이와 함께 다음 정보들을 구성하여 사용자 A에게 전송한다.

$$hm=h(R_A||R_B||K_{AB})$$
$$hm||Cert(B)||R_B\oplus SK_B \quad (9)$$

6) 사용자 A는 전송된 B의 공개키 Y_B와 자신이 생성한 K_A를 이용하여 SK_A를 계산한다.

$$SK_A=Y_B^{K_A} \bmod p$$
$$=g^{X_B*K_A} \bmod p \quad (10)$$

7) 사용자 A는 계산한 SK_A와 전송된 $R_B\oplus SK_B$를 이용하여 R_B를 계산하고, SK_A와 R_A를 이용하여 세션키 K_{AB}를 계산한다.

$$R_B=R_B\oplus SK_B\oplus SK_A$$
$$K_{AB}=h(SK_A||R_A||R_B) \quad (11)$$

8) 사용자 A는 hm'를 구성하여 전송된 hm과 비교한다. 만약 같다면 사용자 B를 인증하고 키 K_{AB}를 설립하게 된다.

$$hm'=h(R_A||R_B||K_{AB})$$
$$hm' \stackrel{?}{=} hm \quad (12)$$

4.2.3 유사시 키 복구 단계

1) 키 복구 기관은 적법한 과정을 통하여 무선 인증 및 키 설립 프로토콜에서 전송되는 R_A, $Cert(B)$, $R_B\oplus SK_B$를 획득한다.

2) 키 복구 기관은 적법한 과정을 통하여 신뢰 기관이 사용자 A와 비밀리에 공유하고 있는 w_A를 획득하고 자신이 사용자 A와 공유하고 있는 비밀값 j_A를 이용하여 키 복구 정보 KRI_A를 계산한다.

$$KRI_A=w_A\oplus j_A \quad (13)$$

3) 키 복구 기관은 획득한 값들을 이용하여 K_A와 SK_A를 차례로 계산한다.

$$K_A=KRI_A\oplus R_A$$
$$SK_A=Y_B^{K_A} \bmod p$$
$$=g^{X_B*K_A} \bmod p \quad (14)$$

4) 키 복구 기관은 R_B를 계산하고 세션키 K_{AB}를 복구한다.

$$R_B=R_B\oplus SK_B\oplus SK_A$$
$$K_{AB}=h(SK_A||R_A||R_B) \quad (15)$$

4.3 도메인 확장에 따른 프로토콜 확장

제안된 방식은 동일한 도메인에 속해있는 두 사용자를 가정하고 있다. 따라서 키 복구 기관과 신뢰 기관은 두 사용자가 동시에 신뢰한다는 가정을 가지고 있다. 만약 하나의 도메인에서 멀티 도메인으로 도메인이 확장된다면 사용자 A와 사용자 B가 서로 다른 도메인에 속하게 되기 때문에 신뢰하는 신뢰 기관과 키 복구 기관이 서로 다르게 된다. 본 장에서는 도메인 확장에 따라 발생하는 문제점을 해결하는 방법에 대해 소개한다.

사용자 B가 신뢰하는 키 복구 기관에 키 복구 기능을 제공하기 위해서는 4장에서 제안한 프로토콜 중 식 (9) 부분에 $c_B*j_B\oplus w_B\oplus SK_B$를 추가하여야 한다.

$$hm||Cert(B)||R_B\oplus SK_B||c_B*j_B\oplus w_B\oplus SK_B \quad (16)$$

다음은 식 (9)를 식 (16)과 같이 변경하였을 때 사용자 B가 신뢰하는 키 복구 기관에서 키 복구를 하는 과정이다.

1) 키 복구 기관은 적법한 과정을 통하여 무선 인증 및 키 설립 전송되는 R_A, $R_B\oplus SK_B$, $c_B*j_B\oplus w_B\oplus SK_B$를 획득한다.

2) 키 복구 기관은 c_B를 계산하고, 적법한 과정을 통하여 신뢰 기관이 사용자 B와 공유하고 있는 비밀값 w_B를 획득한다. 그리고 자신이 사용자 B와 공유하고 있는 비밀값 j_B를 이용하여 SK_B를 계산한다.

$$c_B=J_B\oplus W_B \bmod p$$
$$SK_B=c_B*j_B\oplus w_B\oplus SK_B\oplus c_B*j_B\oplus w_B \quad (17)$$

3) 키 복구 기관은 SK_B를 이용하여 R_B를 계산하고, R_B를 이용하여 세션키 K_{AB}를 복구한다.

$$R_B=R_B\oplus SK_B\oplus SK_B$$
$$K_{AB}=h(SK_B||R_A||R_B) \quad (18)$$

5. 제안 방식 고찰 및 비교 분석

표 1은 상기 요구사항들을 기준으로 기존 방식과 제안 방식을 비교 분석한 것이다.

표 1 기존 방식과 제안 방식 비교 분석표

요구사항 \ 프로토콜	R-M 프로토콜	N-P-B-E 프로토콜	K-L 프로토콜	제안 프로토콜
인증	O	O	O	O
기밀성	O	O	O	O
무결성	O	O	O	O
복구 공개 검증성	X	O	O	O
위장 공격 방지	X	O	O	O
도메인 확장성	X	X	O	O
불법적인 키 복구 방지	X	X	X	O
멱승 연산량(A, B)	(3, 1)	(2, 1)	(2, 2)	(2, 1)
통신 오버헤드 (통신회수, 상대수치)	- (3, 0)	$r\oplus g^{uv}$, $(sv)_K$, s_U, s_V (3, 4)	g^{rv}, $(sv)_K$, s_U, s_V, $w_V\oplus rv\oplus g^{uv}$ (3, 5)	$c_B*j_B\oplus w_B\oplus SK_B$ (2, 1)

O : 제공, X : 제공하지 않음

6. 결 론

무선의 가장 큰 장점은 이동성과 편재성이라 할 수

있다. 무선 단말기의 보급 확산으로 인하여 사용자들은 언제 어디서나 그리고 위치를 이동하면서 다른 사용자와 무선 통신을 수행할 수 있게 되었다. 그러나 이러한 장점을 가지고 있는 반면 보안에 취약하다는 단점 또한 가지고 있다. 무선상에서 이루어지는 통신의 보안 취약점을 해결하기 위해서는 통신 당사자간에 인증이 수행되어야 하고 통신 데이타에 대해 기밀성과 무결성을 제공받아야 한다. 또한 설립된 키의 분실이나 오용 등에 의해 발생하는 여러 가지 문제점을 해결할 수 있는 키 복구 기능이 제공되어야 한다. 이러한 보안 서비스를 제공받기 위해서는 WAKE 키 복구 프로토콜이 절대적으로 필요하다.

본 논문에서는 기존에 제시되었던 WAKE 키 복구 프로토콜을 분석하여 이들의 문제점을 분석하였고, 이와 관련된 새로운 요구사항을 제시하였다. 그리고 기존에 제안된 요구사항과 새로운 요구사항을 모두 만족할 수 있는 새로운 WAKE 키 복구 프로토콜을 제안하였다. 제안한 프로토콜은 기존에 제시된 프로토콜들에 비해 안전성 및 효율성이 매우 뛰어남을 알 수 있다. 향후 신뢰기관과 키 복구 기관의 비중을 줄이고 WAKE 프로토콜의 계산량과 통신량을 감소시키는 방법들이 연구되어야 할 것이다.

참 고 문 헌

[1] 최용락, 소우영, 이재광, 이임영, 컴퓨터 통신 보안, 도서출판 그린, 2001.

[2] 이용호, 이임영, 김주한, 문기영, WAKE 키 복구 프로토콜에 관한 연구, 한국멀티미디어학회 춘계학술발표논문집, pp. 912-915, 2002.

[3] DongGook Park, Colin Boyd and SangJae Moon, Forward Secrecy and Its Application to Future Mobile Communications Security, PKC2000, Springer-Verlag, pp. 433-445, 2000.

[4] K. Rantos and C. Mitchell, Key Recovery in ASPeCT Authentication and Initialization of Payment protocol, ACTS Mobile Summit, 1999.

[5] J. Nieto, D. Park, C. Boyd, and E. Dawson, Key Recovery in Third Generation Wireless Communication System, PKC2000, Springer-Verlag, pp. 223-237, 2000.

[6] ChongHee Kim and PilJoong Lee, New Key Recovery in WAKE Protocol, PKC2001, Springer-Verlag, pp. 325-338, 2001.

이 용 호

2001년 2월 순천향대학교 컴퓨터공학과 졸업. 2003년 2월 순천향대학교 전산학 전공 석사. 2003년 3월~현재 한국정보통신기술협회 S/W시험인증센터 전임연구원. 관심분야는 암호토콜, 키관리, 정보보호, S/W시험인증

이 임 영

정보과학회논문지 : 정보통신 제 30 권 제 2 호 참조