유비쿼터스 환경에서 제한적인 능력을 갖는 이동장치를 위한 경량의 인증 프로토콜 구현

임규상* · 유일선*

*한국성서대학교

Implementing a Light-Weight Authentication Protocol for Resource-Constraint Mobile Device in Ubiquitous Environment

Kyu-Sang Lim* · Ilsun You*

*Korean Bible University

E-mail : karismalimks@hanmail.net

요 약

유비쿼터스 환경에서 사용자가 휴대하는 이동장치는 제한적인 능력을 갖기 때문에 강력한 보안성과 경량의 연산량을 지원하는 인증 프로토콜이 요구된다. 최근에 제안된 S/Key 기반의 인증기법들은 경량의 암호화 연산과 함께 강력한 사용자 인증, 세션키 교환을 제공함으로써 이러한 요구사항을 만족한다. 특히, You와 Jung이 제안했던 프로토콜은 효율성과 보안성을 함께 고려할 때 가장 우수하다. 본 논문에서는 You-Jung 기법을 다른 기법들과 비교 분석하고 실제 유비쿼터스 환경에서의 적용을 위해 이동장치 상태변화를 설계하고 프로토콜을 구현한다.

ABSTRACT

In ubiquitous environment, mobile devices, which users carry, tend to be resource-constraint, thus resulting in the need for an authentication protocol, which provides light-weight computations as well as strong security. Recently S/Key based protocols, which satisfy such a requirement by achieving light-weight computations, strong authentication and session key exchange, have been proposed. In particular, You and Jung's protocol is more efficient and secure than others. In this paper, we compare and analyze You-Jung with other protocols. Also, we design an authentication scenario and status of mobile devices while implementing the protocol.

키워드

S/Key, 일회용 비밀번호, 사용자 인증, 유비쿼터스 보안

Ⅰ. 서 론

유비쿼터스란 사용자가 시간과 장소에 구애받지 않고 컴퓨터나 네트워크를 의식하지 않는 상태에서 자유롭게 컴퓨팅 서비스를 제공 받을 수 있는 환경을 의미 한다[1]. 유비쿼터스 기술이 확산된다면, 가정, 직장 또는 이동 공간 등에서의 편리성과 안전성, 그리고 효율성이 크게 증대되며, 그 결과 우리의 삶의 질이 향상될 것이다. 하지만 유비쿼터스 기술의 긍정적 측면에도 불구하고 이 기술로 인해 초래될 역기능 또한 무시할 수 없다[2][3]. 예를 들어, 홈 네트워크 환경은 TV, 전등, 세탁기, 냉장고 등의 가전제품을 원격으로 제어할 수 있는 편리함을 제공하지만 사용자 사칭 공격, 도청, 서비스 거부 공격 등과 같은 다양한 보안 위협을 유발한다. 이처럼 유비쿼터스 환경에서 보안서비스를 제공하는 것은 필수적이며, 특히 사용자 인증은 매우 중요한 서비스 중의 하나이다. 본 논문은 유비쿼터스 환경에서의 사용자 인증에 중점을 두고자 한다. 유비쿼터스 환경

에서 사용자가 휴대하는 이동장치는 제한적인 능력을 갖기 때문에 강력한 보안성과 경량의 연산량을 지원하는 사용자 인증이 요구된다. 최근에 제안된 S/Key 기반의 인증기법들은 경량의 암호화 연산과 함께 강력한 사용자 인증, 세션키 교환을 제공함으로써 이와 같은 유비쿼터스 환경에서의 요구사항을 만족한다[2-7]. 특히 You-Jung기법은[2] Yeh-Shen-Hwang[6], Lee-Chen[7], PKAS[3] 기법등과 비교했을 때 효율성과 보안성에서 가장 우수하다. 본 논문에서는 You-Jung 기법을 다른 기법들과 비교 분석하고 실제 유비쿼터스 환경에서의 적용을 위해 이동장치 상태변화를 설계하고 프로토콜을 구현한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 S/Key 기법과 그의 개선안들을 기술하고, Ⅲ장에서는 You-Jung 기법을 분석한다. Ⅳ장에서는 You-Jung기법에서 이동장치 상태변화를 설계하고 프로토콜을 구현한 후 다른 프로토콜들과의 성능 비교를 하고 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 S/Key 기법과 그의 개선기법들에 대해 기술한다.

S/Key 기법은 재전송 공격 또는 도청공격으로부터 컴퓨터 시스템을 보호하기 위해 고안되었다[4]. S/Key 기법은 인증과정에서 사용자의 패스워드가 네트워크에서 전송되지 않으며 사용자의 비밀정보가 서버를 포함한 그 어떠한 시스템에도 저장될 필요가 없다는 장점을 가지고 있다. 하지만 오프라인 사전공격이나 서버위장공격, Preplay 공격에 취약하다는 문제점을 갖는다[5].

최근에 제안된 스마트 카드기반의 개선된 S/Key 기법인 Yeh-Shen-Hwang 인증방식[6]은 SEED를 공유 비밀키로 사용함으로써 서버 위장공격과 Preplay 공격 그리고 오프라인 사전공격에 대비하였고 로그인 과정을 단순화하였다. 또한 세션키 분배를 통해 인증 후 다양한 보안서비스를 가능하게 하였다. Yeh-Shen-Hwang 기법이 제안될 당시에 SEED와 사용자 비밀키의 저장을 위해 스마트 카드에 의존적인 것이 문제가 되었으나 유비쿼터스 환경에서는 일반적으로 사용자들이 이동장치를 휴대하기 때문에 경량의 연산에도 불구하고 강력한 보안서비스를 제공하는 Yeh-Shen-Hwang 기법은 유비쿼터스 환경을 위한 적합한 인증기법으로 인식되었다[2][3]. 그러나 Yeh-Shen-Hwang 기법은 Stolen-Verifier 공격, Denning-Sacco 공격에 취약점을 가지며 SEED의 안전한 분배가 어렵다는 문제점이 있다[3][4]. Yeh-Shen-Hwang 기법의 취약점 중 Stolen-Verifier 공격을 개선하기 위해 Lee-Chen 기법[7]이 제안되었다. Lee-Chen 기법은 강화된 보안성과 Yeh-Shen-Hwang 기법과 비슷한 수준의 효율성을 제공함에도 불구하고 서비스 거부 공격과 하나의 비밀번호가 유출되면 그 이전에 사용되었던 세션키가 모두 붕괴되는 문제점을 갖는다. You-Jung 기법은 이 두 가지 문제점을 개선하였다[2].

한편, PKAS 기법[3]은 Lee-Chen 및 You-Jung 기법과 다르게 공개키 암호화 기술을 사용하여 Yeh-Shen-Hwang 기법을 개선하였다. 그러나 이 기법은 공개키 연산으로 인한 성능저하와 에너지 소모량 증가의 문제를 갖는다.

Ⅲ. You-Jung 기법

본 장에서는 보안성과 효율성을 모두 고려할 때 가장 우수한 You-Jung 방식을 분석하고자 한다. You-Jung 기법은 등록, 로그인, 인증의 3단계로 구성되며 초기에 클라이언트(사용자의 이동장치에 해당함)가 서버로부터 분배된 $SEED(=id \oplus SK)$ 값을 받았다고 가정한다. You-Jung 기법의 등록 및 로그인 과정은 각각 그림 1과 2와 같다.

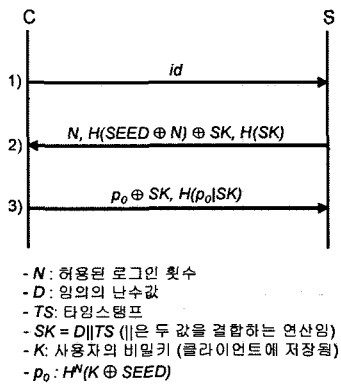

그림 1. You-Jung방식의 등록 단계

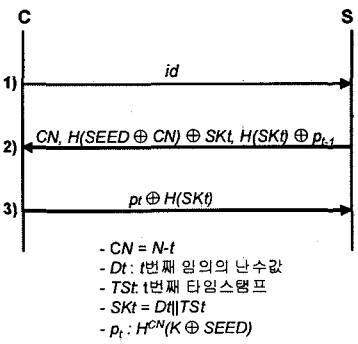

그림 2. You-Jung방식의 로그인 단계

You-Jung 기법의 등록단계를 분석해 보면 클라이언트는 3)에서 $p_0 \oplus D$ 와 함께 $H(p_0 | D)$를 서버에게 함께 보냄으로써 서버가 갖는 p_0가 서비스

거부 공격으로부터 안전함을 얻게 해준다. 여기서 로그인정보 p_0와 N은 서버에 저장되고 클라이언트에도 p_0가 저장 된다.

로그인 단계이후에 인증단계가 되면 서버는 클라이언트로부터 받은 $p_t \oplus H(SKt)$와 $H(SKt)$로 새로운 일회용 비밀번호인 p_t를 얻는다. 여기서 얻은 p_t의 해쉬 값과 서버에 저장된 p_{t-1}이 같다면 클라이언트의 인증은 성공한다. 그 이후에 서버는 마지막 비밀번호인 p_t와 로그인 횟수 값인 CN을 사용자 데이터베이스에 저장한다. 서버에 의해 임의로 생성된 SKt는 서버와 클라이언트 사이에 안전한 메시지 교환을 위해 세션키로 사용될 수 있다. 또한, 이러한 세션키들은 로그인 단계의 3)에 있는 $p_t \oplus H(SKt)$에 의해 p_t가 유출될지라도 붕괴되지 않는다.

IV. You-Jung 기법의 구현 및 분석

4.1 이동장치의 상태변화

본 논문에서는 그림 3과 같이 You-Jung 기법에서의 이동장치의 상태변화를 설계하였다.

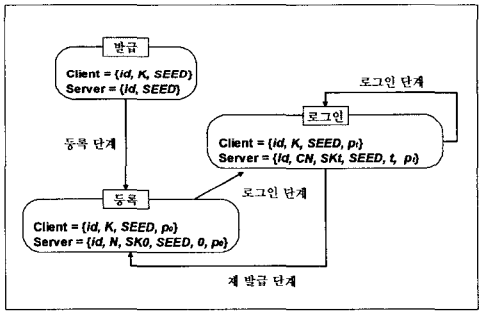

그림 3. You-Jung방식 상태변화

You-Jung 기법은 크게 발급 및 등록, 로그인 상태로 나눠지는데 처음 이동장치의 발급상태에서는 Server와 Client가 사용자에 대한 $SEED$값을 가지고 있다. 등록상태에서 Client는 서버로부터 받은 N값을 통해 p_0값을 만들어 저장하며 Server는 사용자에 대한 N값과 $SK0$값 그리고 로그인 횟수에 대한 $t(=0)$값과 Client로부터 받은 p_0값을 저장한다. 마지막으로 로그인상태에서 Client는 CN값에 의해 p_t값을 만들어 저장하고 서버는 CN과 SKt값 그리고 로그인 횟수t와 Client로 받은 p_t값을 갱신해 저장한다.

4.2 You-Jung 기법의 구현

본 논문에서는 C#언어와 비쥬얼 스튜디오 닷넷을 사용하여 You-Jung 기법을 구현하였고 Windows XP Professional 환경에서 테스트를 하였다. 사용자가 유비쿼터스 서비스에 인증을 하기 위해서는 그림 4와 같이 PIN(Personal Identification Number)을 입력하고 서비스 인증을 요청한다. PIN 검증이 끝나면 사용자는 id와 비밀키 K 등이 이동장치에 저장되어 있기 때문에 더 이상의 추가적인 입력을 요구 받지 않고 인증과정을 진행할 수 있다.

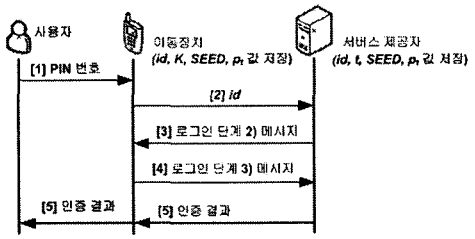

그림 4. 사용자 인증 흐름

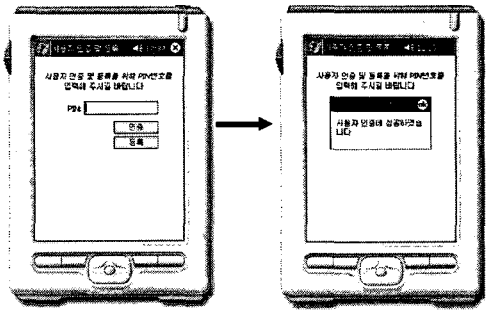

그림 5. 사용자 인증 결과 화면

그림 5는 사용자 인증모듈을 구현한 결과화면을 나타내며 그림 6과 7은 등록단계의 소스코드 중 일부를 보여준다.

```
/* 랜덤값 SK 생성 */
Random rnd = new Random();
int rand = Convert.ToInt32(rnd.Next(10000));
string SK = HashFunc(Convert.ToString(rand));

/* H(SEED^N)^SK 계산 */
string SN = Xor(SEED,N);
string HSN = HashFunc(SN);
string HSND = Xor(HSN,SK);

/* H(SK) 계산 */
string HSK = HashFunc(SK);
```

그림 6. 등록단계 2) 소스

```
/* p0값 계산*/
string p0 = Xor(K,SEED);

/*K^SEED를 N횟수만큼 해쉬계산*/
for (int i=1; i<=NSave; i++){ p0 = HashFunc(p0); }

/* p0^SK 계산 */
string pXor0 = Xor(p0,SK);

/* H(p0|SK) */
string pCon0 = String.Concat(p0,SK);
string HpCon0 = HashFunc(pCon0);
```

그림 7. 등록단계 3) 소스

4.3 성능 분석

본 절에서는 You-Jung기법과 기존의 기법들의 프로그램 성능을 비교분석 한다. 분석 방법은 실제 각각의 기법들의 N값을 10000으로 가정하고 등록 후에 로그인 단계를 1회에서 10회 반복 했을 때에 그 속도를 비교해 보았다. X축은 반복횟수를 의미하고, Y축은 소요시간(초)을 의미한다.

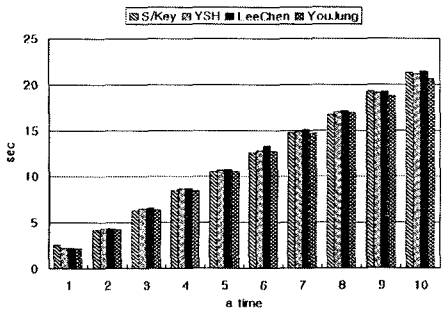

그림 8. 프로그램 속도비교

그림 8을 확인해보면 다른 기술들에 비해 You-Jung 기법이 보안성을 강화 하였음에도 불구하고 다른 기술들과 성능의 차이를 보이지 않는 것을 확인할 수 있다.

V. 결 론

본 논문에서는 유비쿼터스 환경에서 제한적인 능력을 갖는 이동장치에 적합한 사용자 인증 기법을 연구하였다. 이를 위해 S/Key의 개선기법들을 분석하였고 특히 보안성과 효율성을 모두 고려할 때 가장 우수한 You-Jung의 기법을 구현하였다. 또한, 다른 기법들과 성능비교를 통해 You-Jung의 기법이 우수한 보안성에도 불구하고 성능의 차이가 거의 없음을 보였다.

참고문헌

[1] H. Sun, "Home Networking," Mitsubishi Electric Research Laboratories, 2004, http://www.merl.com/projects/hmnt/

[2] I. You and E. Jung, "A Light Weight Authentication Protocol for Digital Home Networks," ICCSA 2006, Springer-Verlag LNCS 3938, pp. 416-423, May 2006

[3] I. You, "A One-Time Password Authentication Scheme for Secure Remote Access in Intelligent Home Networks," KES 2006, Springer-Verlag LNAI 4252, pp. 785-792, Oct. 2006

[4] N. Haller, "The S/KEY One-time Password," RFC 1760, Feb. 1995.

[5] C. J. Mitchell and L. Chen, "Comments on the S/KEY User Authentication Scheme," ACM Operating Systems Review, vol.30, no.4, pp.12-16, Oct. 1996.

[6] T. C. Yeh, H. Y. Shen and J. J. Hwang, "A Secure One-Time Password Authentication Scheme Using Smart Cards," IEICE Transaction on Communication, vol.E85-B, no.11, pp.2515-2518, Nov. 2002.

[7] N. Y. Lee and J. C. Chen, "Improvement of One-Time Password Authentication Scheme Using Smart Cards," IEICE Transaction on Communication, vol. E88-B no.9, pp.3765-3767, Sept. 2005.