스트림 알고리즘을 이용한 OTP 생성 및 동기화 인증 프로토콜

이장춘* · 이훈재**· 김태용**

*동서대학교 유비쿼터스 IT

**동서대학교 컴퓨터정보공학부

Authentication Protocol with OTP Generation and Synchronization using Stream algorithm

Jang-chun Lee* · Hoon-jae Lee** · Tae-yong Kim**

*Ubiquitous IT, Dongseo University

**Computer engineering, Dongseo University

E-mail : kpoto@paran.com, {hilee, tykimw2k}@gdsu.dongseo.ac.kr

요 약

현재 네트워크상에서 사용자를 인증하는 부분은 시스템 보안상으로 아주 중요한 역할을 하고 있다. 공개된 네트워크에서는 개인의 중요한 프라이버시 정보를 보호하기 위해 인증 절차를 거치게 된다. 이러한 인증 방법에는 간단한 Identity/Password 인증부터 복잡한 생채 공학 인증까지 다양한 기술들이 존재 한다. 최근 금융보안업계가 주축이 되어 일회용패스워드(OTP : One Time Password) 인증 시스템을 활용하기 위한 기술적 시도 및 개발이 활발히 이루어지고 있다. 일회용 패스워드는 사용자가 인증 받고자 할 때 새로운 패스워드를 생성하고 사용 후 버린다는 구조를 가지고 있다. 이는 매번 같은 패스워드를 사용했을 때 발생하는 보안 문제점을 해결할 수 있다. 그러나 OTP 인증 방법에도 여러 가지 공격 방법에 취약한 문제점들이 노출되어 있다. 본 논문은 기존의 인증 프로토콜 문제점을 개선하고 크기가 작은 스트림 알고리즘을 이용하여 스마트카드에서 사용 가능한 새로운 인증 프로토콜을 제안한다.

키워드

OTP, 인증 프로토콜, Smart card

Ⅰ. 서 론

최근 인터넷과 같은 통신 기술이 급속하게 발달하여 많은 부분의 업무들이 인터넷을 통해서 이루어지고 있다. 인터넷은 개방형 네트워크이기 때문에 어떠한 사용자라도 접속가능하게 된다. 이는 악의적인 사용자가 공격을 목적으로 접근하게 되었을 때 도청, 침입, 도난 등의 피해를 당할 수 있다. 이러한 피해를 막기 위해 최근 인터넷 보안에 대한 관심이 높아지고 있다. 특히 전자금융거래의 급속한 발전으로 인해 인터넷 뱅킹 서비스의 이용이 증가되고 있으며 이에 따른 전자금융 해킹 및 보안 사고가 발생되고 있다.

이러한 보안 사고의 발생을 줄일 수 있는 방법 중 사용자 인증 방법이 가장 보편적으로 사용된다.[1] 인증(Authentication) 이란 특정 사용자가 접속을 요구할 때 사용자의 신원에 대한 보증 기능으로 현재 Identity/Password를 기반으로 한 인증 기법이 가장 많이 사용되고 있다. 간단한 패스워드 인증 방법 이외에 사용자가 소유하고 있는 매체나 사용자 고유의 생체정보를 이용한 강력한 인증 방법도 사용되고 있다. 이러한 인증 방법들은 보안의 중요성에 따라 구분되어서 사용된다.

현재 전자금융거래에서 사용되는 인증 방법은 보안 카드와 공인 인증서를 이용하여 사용자를 인증하고 있다. 그러나 최근에는 일회용 패스워드(OTP)[1,2] 기법을 새롭게 도입하여 사용되고 있다. 일회용 패스워드(OTP)[1,2]는 사용자가 인증을 요구할 때 패스워드를 생성하여 사용하는 방법으로 매번 생성된 패스워드는 서로 다른 값을 가지고 있어 한번 사용된 패스워드는 재사용하지 않게 된다. 이는 공격자가 네트워크상에서 패스워드를 도청하거나 사용자가 패스워드를 분실하더라도 안전을 보장할 수 있게 된다. 또한 일회용 패

스워드는 익명성, 휴대성, 확장성의 특징을 가지고 있으며 사용자의 개인 정보를 저장하여 이용하지 않기 때문에 개인 정보유출을 사전에 방지할 수 있다.

본 논문의 2장에서는 OTP(One Time Password)에 대한 기술을 알아보고 3장에서는 스마트카드[4,5,6]에 사용되는 인증 프로토콜 중 기존에 연구되었던 Das et al.[4]와 chien et al.[5]의 프로토콜을 분석 후 개선하여 새로운 동기화 인증 프로토콜을 제안한다. 그리고 마지막으로 4장에서 결론과 향후 과제에 대해 서술하겠다.

Ⅱ. OTP(One Time Password) 기술

OTP[1,2]는 One Time Password 의 약자로써, 사용자가 인증을 요구할 때마다 새로운 패스워드를 생성하여 사용하는 방식이다. OTP 생성 방식에는 OTP 기기와 인증 서버간의 동기화 여부에 따라 비동기화 방식과 동기화 방식으로 나뉘게 된다.

2.1 비동기화 방식

비동기화 방식은 OTP 기기를 초기화 할 때 인증서버에 미리 약속해 놓은 동기화 정보를 사용하지 않고 사용자가 직접 인증 서버로부터 받은 질의 값을 OTP 기기에 입력하여 OTP 값을 생성하는 방법이다. 이러한 방법을 이용한 대표적인 기법이 질의-응답(Challenge-Response) 방식이며 현재 전자금융거래에서 도입하여 사용되고 있다.

질의-응답 방식은 사용자가 인증을 요청할 때 인증 서버로부터 받은 임의의 값을 OTP 기기에 직접 입력한 후 OTP 값을 생성하는 방식으로 생성된 OTP 값을 인증 서버에 재전송하여 인증 절차를 완료하게 된다. 이는 OTP 기기와 인증 서버간의 동기화 정보가 필요 없는 장점을 가지고 있지만 사용자가 직접 OTP 기기에 질의 값을 입력해야 되고 생성된 OTP 값을 인증 서버에 전송하기 위해 다시 OTP 값을 입력해야 되는 불편함을 가지고 있다. 또한 인증 서버는 사용자의 질의 값을 따로 관리해야 되는 부담을 가지게 된다.

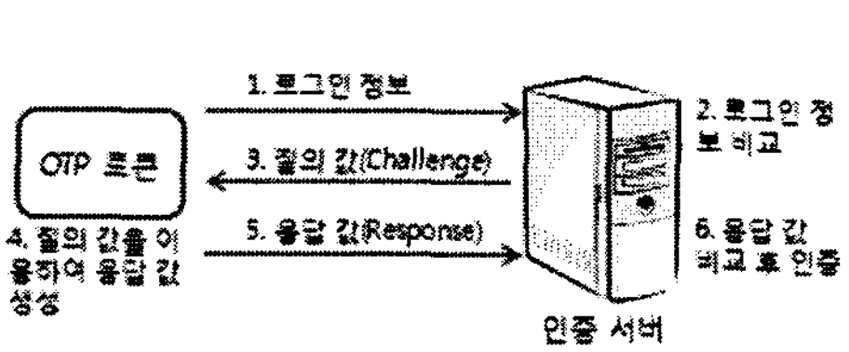

그림 1. OTP 비동기화 방식

2.2 동기화 방식

동기화 방식은 OTP 기기를 초기화 혹은 생산될 때 인증 서버와 미리 약속된 동기화 정보를 이용하여 OTP 값을 생성하는 방식이다. OTP 기기와 인증 서버 간에 반드시 동기화가 이루어져야 정확한 인증 절차를 이룰 수 있는 단점이 있지만, 질의-응답 방식에서 사용자가 직접 질의 값, 응답 값을 입력해야 되는 불편함을 개선한 방식이다.

동기화 방식에는 동기화를 위한 정보를 무엇으로 사용하느냐에 따라 시간 동기화(Time Synchronous) 방식, 이벤트(Event Synchronous) 동기화 방식, 조합(Time-Event Synchronous) 방식으로 구분 된다.

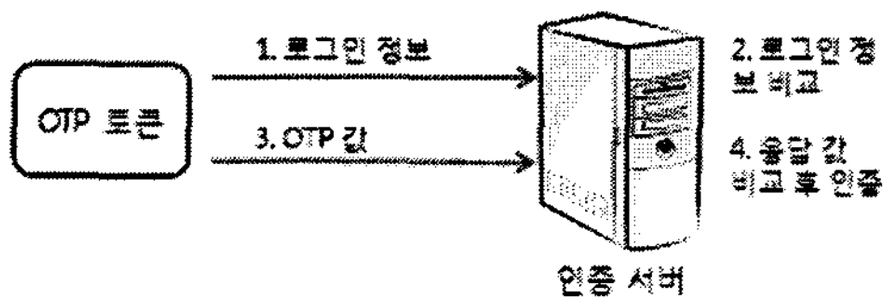

그림 2. OTP 동기화 방식

1) 시간 동기화 방식(Time Synchronous)

시간 동기화 방식은 OTP 기기에서 약속된 특정한 시간마다 패스워드를 자동으로 생성하는 형태이다. 이는 사용자가 별도의 질의 값을 입력할 필요가 없어 사용하기 편하지만 OTP 기기와 인증 서버간의 시간이 동기화 되어 있어야 되고 만일 사용자가 일정시간 안에 OTP 값을 인증 서버에게 전송하지 못하게 되면 다음 패스워드가 생성될 때 까지 대기 후 사용해야 되는 단점을 가지고 있다. 또한 공격자가 사용자와 인증 서버 중간에서 MITM(Main-IN-The-Middle) 공격으로 OTP 값을 획득하게 되었을 때 일정 시간동안 사용할 수 있는 위험성을 가지고 있다.

2) 이벤트 동기화 방식(Event Synchronous)

이벤트 동기화 방식은 OTP 기기와 인증 서버간에 동일한 카운터 값을 이용하여 OTP 값을 생성 하는 방식이다. 카운터 값은 공개된 시간 값과는 달리 OTP 기기와 인증 서버만이 알 수 있는 값으로 공격자가 추측 할 수 없는 장점을 가지고 있다. 이 방식은 사용자가 일회용 비밀번호를 생성할 경우 카운터 값을 입력 값으로 사용하여 비밀번호를 생성 한다. 비밀번호 생성 후에는 카운터 값을 증가시켜 저장하게 되며 증가된 카운터 값은 다음 비밀번호 생성 시 입력 값으로 사용된다. 이 방식은 여러 번의 인증 요구 시 OTP 기기와 인증 서버간의 인증 실패 혹은 통신 장애등으로 카운트 값이 달라질 수 있다. 이 같은 경우 OTP 기기와 인증 서버는 다시 카운터 값을 동기화해야 되는 불편함을 가지고 있다.

3) 조합 방식(Time-Event Synchronous)

시간-이벤트 조합 방식은 시간 동기화 방식과

이벤트 동기화 방식의 장점을 조합하여 구성한 방식으로, OTP 기기와 인증 서버 간에 동기화된 시간 값과 동일한 카운터 값을 이용하여 OTP 값을 생성하게 된다.

Ⅲ. 스마트카드 인증 프로토콜

이번 장에서는 기존에 연구되었던 인증 프로토콜의 분석과 제안 프로토콜을 서술한다. 다음 수식은 사용될 용어에 대한 정의이다.

U_i : 사용자의 스마트카드.
S : 인증 서버.
PW_i : 사용자의 비밀번호.
$\oplus$: XOR 연산.
h( ) : 일방향 해쉬 함수.
x, y : 인증 서버의 비밀키.
R : 암/복호 키
E_k( ) : 암호 알고리즘
KS_c( ) : 스트림 알고리즘의 c번째 키스트림 값

3.1 Das et al. 프로토콜[4]

Das et al. 프로토콜에서는 스마트카드를 이용한 사용자의 익명성을 보장하여 위치 노출을 막을 수 있는 방법을 제시하고 있다.[4] 이 프로토콜은 등록 단계, 로그인 단계, 검증 단계 의 3가지의 단계로 구분되어 동작하게 된다.

[등록 단계]
1. 사용자가 입력한 PW_i를 안전한 채널을 통해 인증서버 S에 전송한다.
2. 인증서버 S는 N_i를 계산 하고 등록 중인 스마트카드 U_i에 h(), N_i, y를 저장한다.
   $N_i = h(PW_i) \oplus h(x_s)$

[로그인 단계]
1. 사용자는 스마트카드 U_i를 리더기에 삽입한 후 패스워드 PW_i를 입력한다.
2. 다음 과정은 스마트카드에서 수행한다.
   1). $C_{ID_i} = h(PW_i) \oplus h(N_i \oplus y \oplus T)$
   2). $B_i = h(C_{ID_i} \oplus h(PW_i))$
   3). $C_i = h(N_i \oplus B_i \oplus y \oplus T)$
3. 스마트카드는$[C_{ID_i}, N_i, C_i, T]$를 인증서버 S에게 전송한다.

[검증 단계]
1. S는 U_i로부터 받은 $[C_{ID_i}, N_i, C_i, T]$와 받은 시간 T'를 이용하여 다음 과정을 수행한다.
2. T와 T' 사이의 시간 간격을 확인한다.
3. $h(PW_i) = C_{ID_i} \oplus h(N_i \oplus y \oplus T)$
4. $B_i = h(C_{ID_i} \oplus h(PW_i))$
5. $C_i = h(N_i \oplus B_i \oplus y \oplus T)$ 계산 후 식이 일치 여부를 확인한다.

3.2 chien et al. 프로토콜[5]

[등록 단계]
1. 사용자는 새로운 스마트카드 U_i를 등록하여 사용한다. 사용자 고유의 ID_i과 입력한 PW_i를 안전한 채널을 통해 인증서버 S에 전송한다.
2. 인증서버 S는 다음 계산을 수행한다.
   1) $m = h(ID_i \oplus x) \oplus h(x) \oplus PW_i$
   2) $I = h(ID_i \oplus x)$
3. S는 U_i에 [I, m, h(), p] 값을 저장하여 초기화 한다.

[로그인 단계]
1. 사용자는 스마트카드 U_i를 리더기에 삽입하고 자신의 ID_i 와 PW_i를 입력한다.
2. 다음은 스마트카드에서 수행되는 과정이다.
   1) $r_u = g^x \bmod p$
   2) $M = m \oplus PW_i$
   3) $C = M \oplus r_u$
   4) $R = I \oplus r_u = h(ID_i \oplus x) \oplus r_u$
3. 인증을 위해 S에게 메시지 [C, T, $E_R(r_u, ID_i, T)$]를 전송한다.

[검증 단계]
1. S는 비밀키 x를 이용하여 R 값을 계산한 후 전송받은 $E_R(r_u, ID_i, T)$을 복호화 한다.
2. T와 T'사이의 시간 간격(time interval)을 확인한다.
3. 다음 식을 계산하여 일치 여부를 확인한다. $R = h(ID_i \oplus x) \oplus r_u$ 만일 값이 일치하지 않으면 S는 인증 요청을 거절한다.
4. S는 $E_R(r_s, r_u+1)$를 계산 후 U_i에게 전송한다. $r_s = g^y \bmod p$
5. U_i는 전송받은 $E_R(r_s, r_u+1)$을 복호화한 후 r_u+1 값을 비교 하고 세션키 K_{US}를 생성한다. $K_{US} = r_s^x = g^{xy}$

3.3 Das et al , chien et al 프로토콜 분석

Das et al 프로토콜은 동적 아이디를 사용함으로써 스마트카드를 사용하는 사용자의 익명성을 제공해 준다. 그러나 로그인 단계에서 전송되는 $[C_{ID_i}, N_i, C_i, T]$ 값 중 고정된 값 N_i 문제점을 chien et al 프로토콜에서 지적하여 익명성을 보장 받지 못한다. 개선된 chien et al 프로토콜은 익명성은 보장하지만 복잡한 지수 계산과 무거운 암/복호화 과정을 가지고 있다.

3.4 제안 프로토콜

[등록 단계]
1. 사용자는 스마트카드 U_i를 등록하여 사용한

다. 사용자 고유의 ID_i과 입력한 PW_i 그리고 이벤트 동기화에 필요한 카운터 c 값을 안전한 채널을 통해 인증서버 S에 전송한다.

2. 전송 받은 ID_i, PW_i, c 값을 이용하여 S는 OTP값을 계산한 후 데이터베이스에 저장한다. $OTP = KS_c(ID_i)$
3. 스마트카드 U_i는 KS(), h(), c, y를 저장한다.

[로그인 단계]

1. 사용자는 스마트카드 U_i를 리더기에 삽입한 후 패스워드 PW_i를 입력한다.
2. 다음 과정은 스마트카드에서 수행한다.
   $M = KS_c(ID_i) \oplus y$
   $L = h(y \oplus T)$
   $P = KS_{c+1}(PW_i)$
3. 스마트카드는[M, L, T]를 인증서버 S에게 전송한다.

[검증 단계]

1. S는 T와 [M, L, T]를 받은 시간 T'를 이용하여 시간 간격을 확인. $L' = h(x \oplus T)$를 계산하여 L 비교해 T값 변경 유무를 확인한다.
2. $M \oplus y = KS_c(ID_i)$
3. $KS_c(ID_i)$를 검색하여 c, PW_i 값을 확인 후 다음 식을 계산한다. $P' = KS_{c+1}(PW_i)$
4. S는 P' 값을 스마트카드 U_i 에게 전송한다.
5. U_i는 생성된 P와 전송받은 P'값을 비교한다.
6. 정상적인 인증이 확인 되면 S는 다음 수식을 계산한다.
   1) 데이터베이스의 N 값을 $N' = KS_{c+1}(ID_i)$ 변경 한다.
   2) c 값을 증가 시킨다.
7. 스마트카드 U_i는 c 값을 증가 시킨다.

3.5 제안 프로토콜 분석

본 논문은 인증 단계에서 사용되는 타임스탬프(time stamp) T와 매 인증마다 변경되는 OTP 값을 이용하기 때문에 Repaly attack(재사용공격)에 안전하고, 사용자가 입력한 비밀번호 값이 사용자와 서버간의 통신 중에 직접 보내지 않기 때문에 Offline Guessing attack(오프라인 추측 공격)에도 안전하다. 또한 매 인증마다 OTP 값이 변경되기 때문에 Main in the middle attack(중간자 공격)에 안전하며 사용자의 익명성 또한 보장된다.

표 1. 사용 함수 개수

	로그인 단계	인증 단계
Das et al.[4]	5H	4H
chien et al.[5]	1C+1H+1S	2H+3C+3E
our scheme	2KS+1H	2KS+1H

C : 암/복호화 E : 지수 계산 H : 해쉬 함수
KS : 스트림 알고리즘

Ⅳ. 결 론

본 논문에서는 Das, Saxena, Gulati[4] 가 제안한 프로토콜이 익명성을 보장 하지 못하는 문제점을 알아보았고, 익명성 문제를 개선한 chien, Chen[5]의 프로토콜을 분석해 보았다.

제안된 프로토콜은 스트림 알고리즘의 키 스트림 값을 이용하여 OTP와 같은 일회성 데이터를 생성하게 된다. 스트림 알고리즘은 초기화 부분을 생략한 변형된 형태로 입력 값을 스마트카드의 ID 값 혹은 사용자의 비밀번호로 이용된다. 암/복호화 과정이 아닌 결과로 나오는 키스트림 값들의 조합을 이용하기 때문에 보안의 강도에 따라 OTP의 길이를 유동적으로 변경할 수 있다. 그리고 다른 암호화 알고리즘의 암/복호화 과정보다 훨씬 가볍다.

OTP는 인터넷 서비스에 사용자를 인증하는 수단으로 발전하고 있다. 이러한 OTP 기술을 다양한 시점에서 접근하여 여러 인증 시스템과 환경에 적용할 수 있는 연구가 요구되어진다.

감사의 글 : 본 연구는 정보통신부의 대학 IT연구센터 지원 사업 및 산업자원부의 지역혁신 인력양성사업의 연구 결과로 수행되었음.

참고문헌

[1] 백미연, "전자금융거래의 보안 강화 방안 및 OTP(One time Password) 이용현황", 지급결제와 정보기술, pp. 71-100, April 2006.

[2] T.Tsuji, T.Kamioka, and A. Shimizu, "Simple and secure password authentication protocol" ver.2(SAS-2), IEICE Technical Report, OIS2003-30, vol.102, no.314, September 2002.

[3] 서승현, 김우진, "OTP 기술현황 및 국내 금융권 OTP 도입사례", 정보보호 학회지, 제17권 제3호,pp. 18-25, 6 2007

[4] M.L. Das, A. Saxena, V.P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transctions on Consumer Electronics, Vol. 50, No.2, pp.629-631, 2004.

[5] H.Y. Chien, C.H. Chen, "A Remote Authentication Scheme Preserving User Anonymity", IEEE AINA'05, Vol. 2, pp. 245-248, 2005

[6] J.J Shen, C.W. Lin, M.S. Hwang,"A modified remote user authentication scheme using smart cards, IEEE Trens. Consumer Electronic, Vol. 49, No.2, pp. 414-416, 2003