One-Time Password를 이용한 상호인증

강민정* · 강민수* · 신현식** · 김현덕*** · 박연식****

*경상대학교 정보통신공학과 · **여수대학교 전자통신공학과

· ***진주산업대학교 전자공학과 · ****경상대학교 정보통신공학과 / 해양산업연구소

Inter-Authentication which utilize One-Time Password

Min-jung Kang* · Min-su Kang* · Hyun-sik Shin*** · Hyun-deok Kim*** · Yeoun-sik Park****

*Dept. of Information & Communication Engineering, Gyeong-sang National University

**Dept. of Electronic Communication Engineering, Yosu National University

***Dept. of Electronic Engineering Chinju National University

****The Institute Of Industry College of Marine Science, Gyeong-sang National University

요 약

OTP(One-time Password)는 지금까지 사용자 인증을 하기 위한 방법으로 많이 이용되어져 왔다. OTP를 이용한 사용자 인증은 상당히 효율적이고 경제적인 측면이 많아서 쉽게 이용할 수 있는 방법 중 하나이다. 본 논문에서는 OTP를 메시지 인증에까지 적용하여 보고 OTP를 이용한 상호인증이 가능함을 제시하고자 한다.

먼저 서론에서는 OTP의 특징 및 개요에 대하여 살펴보고, 본론에서 OTP를 이용한 사용자 인증 방법 및 메시지 인증의 방법에 대하여 설명한다. 그리고 마지막으로 OTP가 어떻게 상호인증 기능을 제공하는지 살펴보고자 한다.

ABSTRACT

OTP (One-time Password) had been used much by method to do user certification so far. Because aspect that user certification that use OTP is efficient and economical fairly is much, it is one of method that can use easily. This treatise would apply OTP in message authentication and wishes to show that OTP is available for inter-authentication.

First, examine about OTP's characteristic and overview in introduction, and explain about user certification method to use OTP in main discourse and method of message certification. And finally, wish to examine how OTP offers inter-authentication function.

Ⅰ. 서 론

지금까지 등한시 되었던 보안 문제가 최근 급속한 네트워크 기술의 발전으로 관심이 집중되고 있다. 특히 시간적 · 공간적 제약을 극복하고 새로운 시장으로 부상한 전자상거래에서는 회원 관리 문제 및 지불수단의 안전성 문제 등으로 인하여 더욱 보안의 중요성이 부각되고 있는 실정이다. 이러한 전자상거래 서비스를 제공하는 서버들의 상당수는 사용자 계정과 패스워드를 인증 기반으로 하는 유닉스 시스템을 사용하고 있는데, 동일한 패스워드 사용으로 인하여 갈수록 패스워드 누출 위험성이 커지고 있다. 이러한 문제를 해결하기 위한 방안 중 하나가 일회용패스워드를 사용하는 것으로 일회용패스워드는 특정 서버에 접속하고자 할 때, 로그인 과정에서 발생할 수 있는 문제를 해결하기 위해 암호화와 해쉬 함수를 사용한다.

본 논문에서도 암호화 및 해쉬 함수와 더불어 공개키를 이용하여 사용자 인증 및 메시지 인증 방법을 소개하고자 한다.

공개키를 이용한 기존의 인증방식은 개인식별 정보에 기반한 identity-based, 인증서에 기반한 certification-based, 두가지 방식의 중간 개념인

self-certified public key의 세가지 방법이 있다[1]. 이 세가지 방법은 검증가능성(verifiability)을 제공하기 위해서 인증기관(certification agendy)을 이용하는데, 본 논문에서는 OTP(One-Time Password) 알고리즘을 이용하여 인증기관 없이 사용자 인증 및 메시지 인증을 제공하여 궁극적으로 상호인증이 가능함을 제시하고자 한다.

II. OTP를 이용한 사용자 인증

OTP(One-Time Password)는 사용자가 특정 서버에 접속하고자 할 때마다 항상 다른 비밀번호를 제공함으로써 로그인과 관련하여 한층 더 강화된 안전성을 제공한다. 즉, 공개키 암호화 기법과 해쉬 함수(MD5)를 이용하여 사용자가 서버에 접속하고자 할 때마다 항상 다른 비밀번호를 제공하고 있다.

여기서 공개키 암호화 기법을 이용하는 이유는 비밀키 방식을 이용했을 때보다 속도는 느리지만, 관리대상 키 수가 적고 키 전송 과정이 필요 없어서 인증 서비스 구현시에는 주로 공개키 방식을 이용한다. 그리고 해쉬 함수는 일방향 해쉬 함수로 주어진 정보로부터 해쉬값을 만들어 낼수는 있어도, 이 해쉬값으로부터 원래의 정보를 복구할 수는 없다.

OTP 구현방법은 크게 S/KEY 시스템, Challenge-Response 방식, Time-Synchronous 방식 등 세가지가 있는데 본 논문에서는 Challenge-Response 방식을 변형하여 사용한다[2]. 즉, 클라이언트가 로그인을 요구하면 서버가 사용자 확인을 하고 클라이언트가 발생시킨 난수를 해쉬 함수 처리하여 패스워드로 사용한다. 이때 정당한 사용자임을 확인 받기 위하여 주로 사용하는 개인정보인 ID는 추측에 의한 접근이 가능하므로 ID 이외의 특별한 개인 정보가 더 필요로 하게 된다. 이러한 점을 감안하여 제시하는 사용자 인증을 위한 OTP 시스템 구성은 그림 1과 같다.

첫 번째 단계에서 사용자 확인을 위해 사용되는 세션키는 추측에 의한 접근을 차단하기 위하여 앞단계에서 사용한 난수를 두 번째 접속부터 입력하도록 한다. 그래서 사용자는 난수가 생성될 때마다 이를 기억해야 하는 번거러움이 있는데, 이를 해결하기 위하여 생성된 난수를 디스켓에 저장해두고 이용하도록 한다.

세 번째 단계에서 생성되는 난수는 반드시 클라이언트에서 생성할 필요는 없다. 하지만 서버에서 난수를 생성한다면 서버의 부담이 더 가중될 뿐만 아니라 해커들의 주공격 대상이 될 수도 있다.

이때 "난수"는 메시지 인증과 상호인증을 하기 위한 가장 중요한 세션키이므로 사용자 password와 주민등록번호, 접속시간, 서버의 비밀키를 이용하여 생성한다. 그래서 추측이나 해킹에 의한

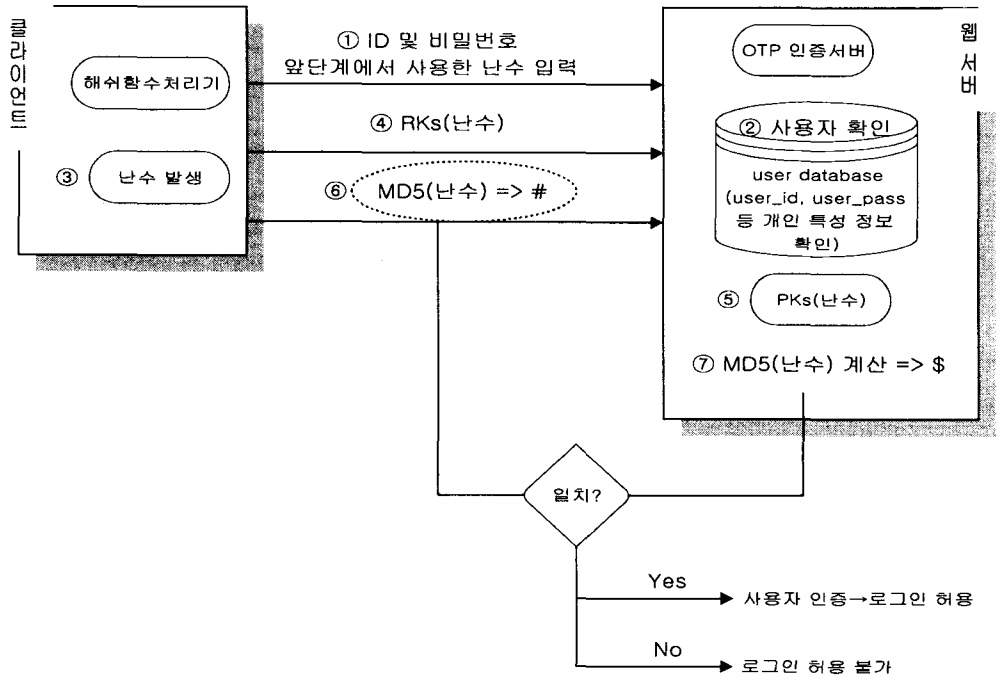

그림 1. OTP를 이용한 사용자 인증
(RKs : 서버의 공개키, PKs : 서버의 비밀키)

접근을 최대한 차단시킴으로써 신뢰성 있는 사용자 인증을 제공한다.

III. OTP를 이용한 메시지 인증

네트워크 보안 분야에서 가장 논란의 소지가 많은 부분 중 하나가 메시지 인증 관련 분야이다. 상상을 초월하는 복잡한 공격기술과 이에 대한 방어책들로 한동안 메시지 인증 기술은 굉장히 어려운 분야로 인식되어져 왔으나, 오늘날 메시지 인증 기술은 암호화 방식과 해쉬 함수를 이용한 여러 알고리즘들의 등장으로 한결 쉽게 이용할 수 있게 되었다[3].

메시지 인증 기술은 한마디로 수신된 메시지가 특정 송신자로부터 변경되지 않고 전송되어져 왔다는 것을 확인시켜주는 기술로써, 데이터 완전성과 부인방지 기능을 만족해야 한다. 이러한 메시지 인증 기술을 구현하는 방법은 message encryption, 메시지 인증 코드(MAC), Hash 함수 등 세가지 방법이 있다[4].

본 논문에서는 사용자 인증에서 사용했던 난수를 해쉬 함수 처리하여 메시지 인증기능을 구현하도록 하겠다.

그림 2에서 제시하고 있는 메시지 인증 방법은 사용자 인증에 이용되어진 난수를 전송하고자 하는 메시지와 함께 일방향 해쉬 함수로 처리하여 그 결과를 비교함으로써, 메시지 변조의 유무를 결정하는 방법이다. 이 때 보통 해쉬 함수 처리된 결과는 암호화하여 전송하는데, 본 논문에서는 통신 당사자들만 알고 있는 난수를 이용함으로써 메시지 다이제스트 암호화 과정을 생략할 수 있다. 그러나 새로 로그인을 할 때만 난수값이 변경되므로 이미 로그인된 상태에서 두 번 이상 메시지 전송을 하고자 하는 경우엔 필히 처음부터 메시지 다이제스트를 암호 처리하여야 할 것이다.

전송되는 메시지의 완전한 기밀성을 추가하기 위해서는 메시지 자체를 비밀키로 암호화해서 전송해야 한다. 그림 3은 메시지 자체를 암호화했을 경우와 하지 않았을 경우를 비교한 것이다.

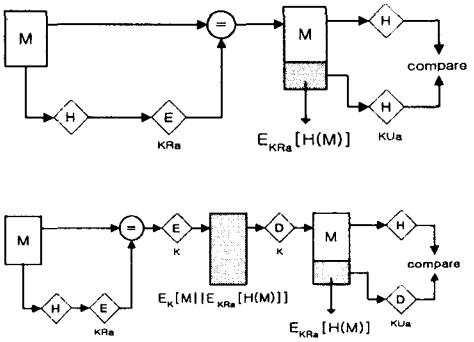

그림 3. 메시지 암호화 한 경우와 아닌 경우
(KRa, KUa : 공개키
K : 비밀키
H(M) : 메시지 다이제스트)

여기서 사용한 해쉬 함수는 MD5로 128bit 메

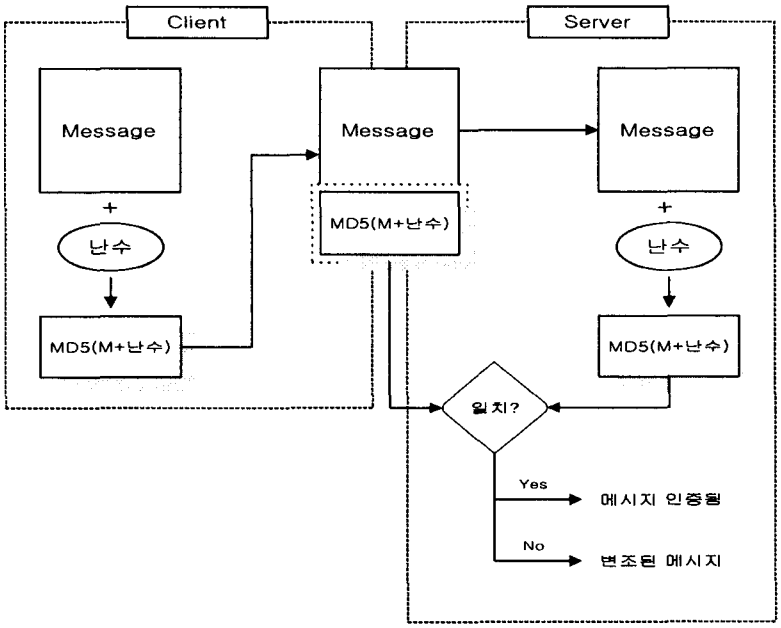

그림 2. OTP를 이용한 메시지 인증

시지 다이제스트를 출력한다. 그러나 최근 다양해진 MD5 공격들로 인하여 좀더 안전한 해쉬 함수에 대한 요구가 증대되었는데, 그 결과 등장한 것이 SHA-1과 RIPEMP-160으로 MD5보다 해쉬 길이가 늘어나므로 그만큼 처리속도가 느리다는 단점이 생긴다[6].

표 1. 해쉬 함수 비교

종류	해쉬 길이	속도	안전성	표준화 상황
MD5	128	104.3	공격법 증가 추세	IETF
RIPEMD-160	160	36.0	1995년 개정후 깨지지 않음	ISO
SHA-1	160	41.2		

IV. OTP를 이용한 상호인증

통신하고 있는 상대방들은 서로의 신분확인에 대해 상호 만족하며 세션키로 교환할 수 있도록 비밀성(신원증명과 세션키 정보가 암호화된 형태로 통신)과 적시성(메시지 재전송의 위협에 대비)을 갖추고 있어야 한다[6]. 이러한 조건을 갖춘 여러 가지 상호인증 방법으로는 관용암호방식에 의존하는 kerberos와 공개키 인증서와 디지털서명에 기반을 둔 X.509가 대표적이다.

X.509는 사용자 인증서의 신뢰성을 위해 인증기관(Certification Authority)이 반드시 필요한데, 현실적으로 통신을 하고자 하는 모든 개인이 신뢰할만한 인증기관에서 발행한 공개키 인증서를 갖는다는 것은 아직까지 많은 어려움이 있다.

kerberos는 모든 사용자의 패스워드를 알고 이것을 중앙 데이터베이스에서 저장·관리하는 인증서버(Authentication Server)를 이용하는데, 사용자 인증이 패스워드에만 의존하고 있음으로써 패스워드 공격에 상당한 취약점을 가지고 있다[6].

하지만 본 논문에서는 로그온시 이용했던 난수가 비밀성과 적시성을 제공함으로써 인증기관 없이 패스워드 공격에도 대응가능한 상호인증 기능을 갖추고 있다 하겠다.

V. 결론 및 향후 연구 방향

본 논문에서는 클라이언트가 발생시킨 난수를 세션키로 이용하여 공개키 암호방식과 해쉬 함수로 처리함으로써 사용자 인증과 메시지 인증이 가능함을 제시했다.

완전한 비밀성과 적시성을 가진 신뢰할만한 사용자 인증과 메시지 인증 기능을 제공하기 위해서는 "난수"를 얼마나 효율적으로 생성·관리하는가에 달려 있다. 그러므로 본 논문에서 제시한 방법으로 사용자 인증과 메시지 인증을 구현하고자 한다면 소프트웨어적으로 난수를 발생시키기 보다는 클라이언트에 난수 발생기를 별도로 설치하여야 한다. 그런 결과로 오류 및 해킹으로부터의 위험을 줄임과 동시에 속도도 더 향상시킬 수 있다. 하지만 각 클라이언트마다 설치해야 하는 나수발생기 비용문제를 고려해야 할 것이다.

한번 접속된 후 두 번 이상 메시지 전송을 하고자 할 때는, 해쉬 함수 처리된 메시지와 난수를 암호화하여 전송해야 하는 번거러움이 있다. 이러한 절차를 줄이기 위해서는 난수 사용시간을 설정하거나 메시지 전송을 하고자 할 때마다 자동으로 새로운 난수를 생성시키는 방법을 적용시키는 것에 대해 향후 연구할 가치가 있다고 본다.

참고문헌

[1] 주미리,이보영,양형규,원동호, "전자상거래 인증 서비스를 위한 검증 가능한 자체 인증 방식", 한국정보처리학회지 2000, Vol.7, No.9

[2] 김영수, "그룹웨어 보안을 위한 일회용 패스워드 알고리즘의 설계 및 구현", 박사학위논문, 한국해양대학교, P61~68, 2000.

[3] William Stallings, "컴퓨터 통신 보안", 그린, P329

[4] "정보보호이론 강좌", http://www.dongguk.ac.kr/~shkim2/chapter3/chapter3_7

[5]"해쉬알고리즘", http://www.softforum.com/korean/learningcenter_12.html

[6] William Stallings, "컴퓨터 통신 보안", 그린, P417