# 인증서를 이용한 보안성이 강화된 일회용 패스워드 검증 시스템의 설계

정회원 김 현 철*, 이 창 수**, 이 경 석*, 전 문 석*

# A Design of One-time Password Verification System with Enhanced Security Using Certificate

Hyun-chul Kim*, Chang-soo, Lee**, Kyung-seok Lee*, Moon-seog Jun* ***Regular Members***

요 약

일회용 패스워드 메커니즘은 동일한 비밀번호를 반복적으로 사용함으로써 발생할 수 있는 패스워드 재사용 문제를 해결한다. 그러나 패스워드 생성 시점에 주기적 대표성으로 인해 여전히 패스워드 재사용 문제가 존재하며, 시간 편차 및 인증 횟수 비동기화 등으로 인한 인증 실패가 발생할 수 있다. 본 논문에서는 비동기적으로 패스워드를 생성하여 사용자와 교환하고 교환한 패스워드에 대해 사용자의 개인키로 전자서명한 후 인증서와 함께 유효성 검증을 요청함으로써 부인방지를 보장한다. 위와 더불어 유효성 검증을 인증서 검증과 패스워드 검증으로 세분화하여 수행함으로써 보안성을 한층 더 강화할 수 있는 일회용 패스워드 검증 시스템을 제안하고 설계한다. 또한, 기존 메커니즘과의 비교 분석을 통해 제안하는 메커니즘이 재생공격, 부인방지, 동기화로 인한 실패 확률 등에서 우수함을 확인 할 수 있었다.

**Key Words** : One-time password, Certificate, Verification, Digital Signature, Non-repudiation

ABSTRACT

The one-time password system solves the problem concerning password reuse caused by the repeated utilization of an identical password. The password reuse problem occurs due to the cyclic repetition at the time of password creation, and authentication failure can occur due to time deviation or non-synchronization of the number of authentication. In this study, the password is created asynchronously and exchanged with the user, who then signs using a digital signature in exchange for the password and a valid verification is requested along with the certificate to ensure non-repudiation. Besides this, a verification system for one-time password is proposed and designed to improve security by utilizing the validity verification that is divided into certificate verification and password verification. Comparative analysis shows that the mechanism proposed in this study is better than the existing methods in terms of replay attack, non-repudiation and synchronization failure.

## Ⅰ. 서 론

최근 일부 거대 기업의 고객 정보 유출 사고를 계기로 내부 정보에 대한 유출 우려 및 이로 인한 개인 정보 도용에 따른 피해의 심각성이 대두되고 있다. 위와 같은 불법적인 접근으로부터 내부 정보를 안전하게 보호하고 유지하기 위해서는 접근을 요청하는 접근 요청자가 정당한 권한을 부여받은

* 숭실대학교 컴퓨터학과(dmzpolice@ssu.ac.kr, 2008kslee@ssu.ac.kr, mjun@ssu.ac.kr)
** (주)리테일테크 기술연구소 (micropow@nate.com)
논문번호 : KICS2008-10-442, 접수일자 : 2008년 10월 9일, 최종논문접수일자 : 2009년 2월 23일

사용자임을 증명하기 위한 절차가 필요하다. 이러한 증명 절차는 사용자가 인증 서버에 자신이 누구임을 밝히는 식별, 인증 서버가 접근을 요청하는 사용자를 증명하는 인증, 접근이 허용된 사용자에 대해 시스템 자원 사용을 허가하는 권한부여 단계로 이루어진다. 특히, 인증 과정은 접근 요청자가 서비스 제공자로부터 제공되는 서비스를 제공받기 위해서는 필수적인 요구 조건이다[1][2].

현재 사용하기 쉽고 가격이 다른 메커니즘에 비해 저렴하다는 이유로 패스워드 기반의 인증 메커니즘이 가장 널리 이용된다. 하지만 다수의 사용자들이 이름, 생일, 취미 등과 같은 자신과 직간접적으로 연관된 정보들을 패스워드로 이용한다는 점에서 추측하기 쉽고, PWDUMP[18], NT Crack[21][22], John the Ripper[19][20]와 같은 Software Crack 도구에 의해 쉽게 깨질 수 있다는 문제점이 존재한다. 또한, 원격 접속 시 패스워드가 평문으로 전송될 경우 스니핑 공격에 대상이 될 수 있으며, 마지막으로 무차별 공격에 의해 결국에는 패스워드가 깨진다는 단점이 존재한다[1][14]. 이러한 패스워드 방법의 문제점을 해결하기 위하여 패스워드 생성 강화 정책 및 실패한 로그인 시도 횟수 제한 설정 등과 같은 여러 대안이 제기 되었으나 정적 패스워드를 사용함으로써 발생하는 근본적인 문제 즉 패스워드 재사용으로 인한 패스워드 도청 및 위조 문제는 해결할 수 없다는 한계를 가지고 있다.

일회용 패스워드(OTP : One-time Password) 메커니즘은 생성한 패스워드를 한번만 사용하고 폐기하는 것으로 동일한 패스워드가 다시 생성되지 않기 때문에 패스워드 재사용으로 인해 발생되는 보안 문제를 해결함과 동시에 개인정보 유출에 따른 사용자 인증 강화 및 전자 금융거래 보안 강화 등의 부가적인 기능을 제공한다. 이러한 OTP 메커니즘은 패스워드 생성매체와 인증 서버간의 동기화 유무에 따라 비동기식 방법과 동기식 방법으로 구분된다. 비동기식 방법은 높은 보안성을 보장한다. 하지만 사용의 불편함과 서버 집중화 현상, 그리고 부인방지를 제공하지 못하는 문제가 발생한다. 동기화 방법은 비동기화 방법의 문제를 해결한다. 그러나 패스워드 생성매체와 인증서버 사이의 동기화를 위한 동기화 값이 해당 주기 또는 해당 시간에 대해서는 동일하기 때문에 스니핑 공격에 노출될 수 있으며, 동기화를 위한 별도의 동기화 과정이 필요하다는 문제점이 존재한다[3][4][9][11][17].

본 논문에서는 위와 같은 기존 OTP 방법의 문제점을 개선하고 보안성을 더욱 강화할 수 있는 인증서를 이용한 보안성이 강화된 일회용 패스워드 검증 시스템을 설계하고 제안한다. 제안하는 시스템은 전자 금융 거래를 기반으로 하고 있으며 인증을 요청하는 사용자, OTP를 생성하고 검증하는 서비스 제공자, 인증서에 대한 발급 및 검증을 수행하는 인증기관으로 구성된다.

서비스 제공자는 접근 요청자의 ID, 세션 값, 그리고 자신이 임의적으로 생성한 랜덤 값을 조합하여 일회용 패스워드를 생성하고 생성한 패스워드에 대하여 해쉬를 수행한 후 암호화하여 사용자에게 전송한다. 사용자는 서비스 제공자로부터 전송받은 해쉬값에 대하여 자신의 개인키로 전자서명한 후 전자서명메시지와 인증서를 서비스제공자에게 전송하고 인증을 요청한다. 이를 통해 전송 부인방지를 보장할 수 있다. 서비스 제공자는 전송받은 인증서에 대한 유효성 검증을 위해 인증기관에게 해당 인증서에 대한 유효성 검증을 요청하고 인증기관은 요청받은 인증서에 대한 유효성 검증을 수행한 후 검증 결과를 서비스 제공자에게 전송한다. 이를 통해 사용자 인증을 제공할 수 있다. 서비스 제공자는 인증기관으로부터 전송받은 해당 인증서에 대한 상태 결과를 확인 한 후 사용자의 공개키로 전자서명메시지를 복호화하여 해쉬값을 획득한다. 획득한 해쉬값과 자신이 보유하고 있는 해쉬값을 비교 검증함으로써 생성한 패스워드에 대한 무결성 및 인증을 보장한다.

본 논문은 다음과 같은 순서로 구성되어 있다. 1장의 서론에 이어서 2장에서는 일회용 패스워드에 관련된 기존 연구에 대하여 기술하고, 3장에서는 본 연구를 통해 제안하는 일회용 패스워드 기법에 대하여 기술한다. 4장에서는 실험환경 및 다른 메커니즘들과의 비교 분석 결과를 기술하고, 마지막으로 5장에서는 본 연구의 결론과 향후 연구 방향에 대하여 기술한다.

## Ⅱ. 관련연구

### 2.1 비동기식 일회용 패스워드 메커니즘

비동기식 일회용 패스워드 방식은 (그림 1)과 같이 서비스제공자와 패스워드 인증서버 사이의 동기화 되는 기준 값 없이 서버가 제시한 질의 값을 수학적 알고리즘을 이용하여 응답 값을 생성하고 해당 응답 값을 서버에 전송하여 자신을 인증하는 방식으로 높은 보안성을 제공한다[6][9][11][12].

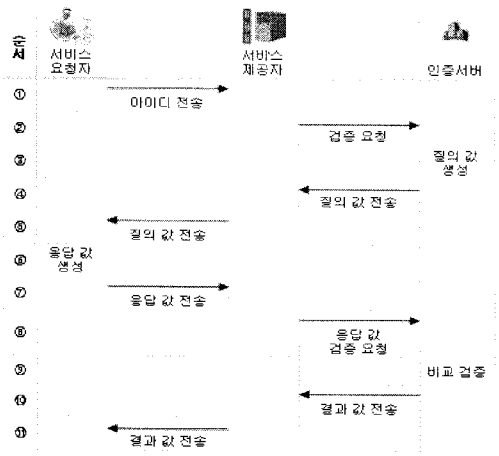



그림 1. 비동기식 방법의 검증 절차

### 2.2 동기식 일회용 패스워드 메커니즘

동기식 방법은 패스워드 생성 매체와 패스워드 인증 서버 사이에 동기화된 값을 통해 OTP를 생성하는 방법으로 시간동기화 방법과 이벤트동기화 방법으로 구분된다. 다음의 (그림 2)는 동기식 방법의 절차를 보여주고 있다.

#### 2.2.1 시간 기반의 동기식 일회용 패스워드 기법

시간 동기화 방법은 사용자가 별도의 질의 값을 입력하지 않고 자동으로 일정주기 또는 일정시간 간격으로 대표 값을 생성하여 패스워드 입력 값으로 사용함으로써 비동기화 방법의 문제점을 해결한다. 하지만 이러한 대표 값은 해당 주기 또는 해당 시간에 대해서는 동일한 값을 갖기 때문에 패스워드 재사용 문제가 발생할 수 있으며 패스워드 생성 매체와 인증 서버간의 동기화된 시간을 사용하기 위한 별도의 동기화 과정이 필요하다는 단점이 존재한다[4][9][11].

#### 2.2.2 이벤트 기반의 동기식 일회용 패스워드 기법

이벤트 동기화 메커니즘은 패스워드 생성 매체에서 생성된 비밀번호 횟수와 인증 서버가 생성한 비밀번호가 자동으로 동기화되기 때문에 시간 동기화 방식의 문제점을 해결한다. 하지만 사용자 실수나 호기심 등으로 OTP가 생성되어 생성매체와 인증서버 사이에 동기화 횟수가 상이할 수 있다는 문제점이 존재한다[9][10][11][13].

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변화하고 있다.

## Ⅲ. 제안하는 시스템

도메인은 이미 엄청난 수가 존재하며, 그 사용량 역시 매우 빈번하다. 또한, 기존의 도메인을 그대로 사용함으로써 추가적인 시스템 도입에 따른 비용이 소요되지 않으며 구조적인 특성상 네트워크 부하를 효과적으로 분산시킬 수 있다. 본 논문에서는 검증 서버를 각각의 도메인 내에 분산시킴으로써 비동기식 기법의 구조적 문제로 발생할 수 있는 중앙 집중화 문제를 해결한다. 제안하는 시스템의 처리과정은 인증서 발급 및 등록, 사용자 등록, 사용자 인증, 패스워드 인증 네 단계로 구분된다.

### 3.1 인증서 발급 및 등록

공인 인증체계에서는 대면 확인을 거쳐 높은 수준의 보안을 유지한다. 사용자는 (그림 3)과 같이 인증서 등록과정에서 개인은 주민번호, 서비스를 제공하는 사용자의 경우는 법인번호를 인증기관(CA : Certificate Authority)에게 제공해야 한다. 이를 통해

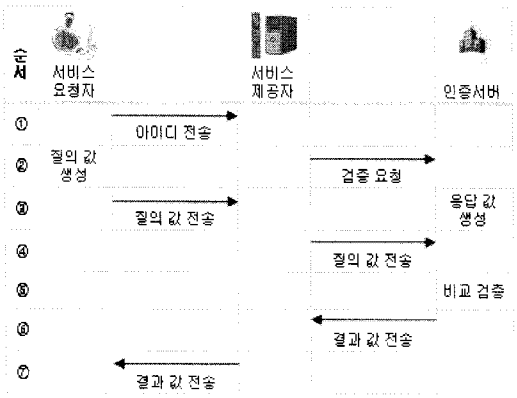



그림 2. 동기식 방법의 검증 절차

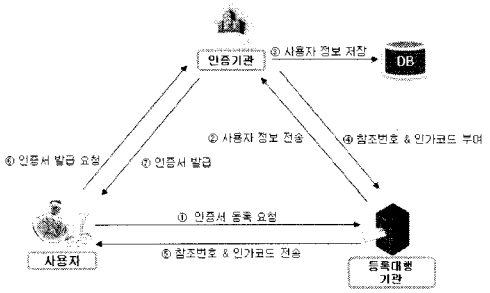



그림 3. 인증서 등록 및 발급

인증기관은 사용자에 대한 신원 정보를 확보하게 되고 인증서를 발행하게 된다. 특히 사용자 신원 정보는 인증서를 식별할 수 있는 정보로 사용된다.

### 3.2 사용자 등록

사용자는 자신이 서비스를 받고자 하는 서비스제공자에게 자신이 등록하고자 하는 ID와 인증서를 (그림 4)와 같이 전송하고 사용자 등록을 요청한다. 서비스제공자는 인증 서버에 해당 사용자에 대한 인증서 상태를 요청하고 해당 사용자가 정당한 사용자 일 경우 자신의 데이터베이스에 사용자 ID와 인증서 정보를 저장한다.

### 3.3 사용자 인증 및 패스워드 인증

본 논문에서 제안하는 OTP 시스템은 인증서를 이용한 사용자 인증 과정과 패스워드 인증 두 단계로 구분하여 처리하고 제안하는 시스템의 상세 프로세스는 (그림 5)와 같다.

① 사용자는 자신의 ID를 서비스 제공자에게 전송하고 일회용 패스워드를 요청한다.

② 서비스 제공자는 세션식별자 S와 랜덤 값 R을 생성한다. S는 해당 통신을 식별하는데 사용함과 동시에 사용자에게 전송할 일회용 패스워드 OTP를 생성하기 위한 정보로 사용된다. R은 OTP를 생성하기 위한 정보로만 이용된다.

③ 서비스 제공자는 ID, S, R을 이진정보로 변환하고 논리연산을 수행하여 OTP를 생성한다.

④ 서비스 제공자는 생성한 OTP를 해쉬하여 해쉬값 $Q_Value = h(OTP)$를 생성한다. Q_Value는 차후에 무결성 검증 및 패스워드 검증에 사용된다.

⑤ 서비스 제공자는 Q_Value에 대하여 사전에 사용자와 교환하여 확보하고 있는 대칭키 sk를 이용해 암호화를 수행하여 암호화된 질의값 $EQ_Value = E_{sk}(Q_Value)$를 생성한다.

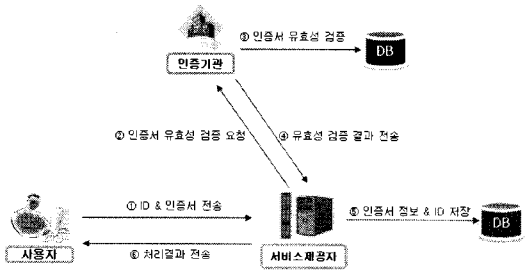



그림 4. 사용자 등록 절차

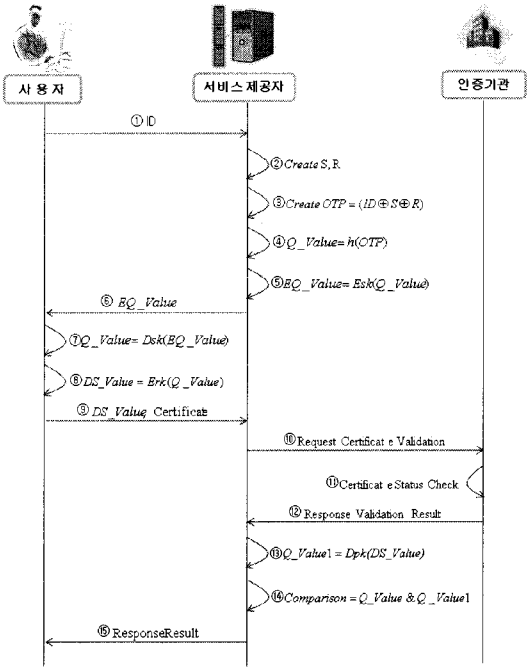



그림 5. 제안하는 시스템의 상세 프로세스

⑥ 서비스 제공자는 EQ_Value를 사용자에게 전송한다.

⑦ 사용자는 전송받은 EQ_Value에 대하여 대칭키 sk를 이용하여 복호화를 수행하고 질의 값 $Q_Value = D_{sk}(Q_Value)$를 획득한다.

⑧ 사용자는 획득한 Q_Value에 대하여 자신의 개인키 rk로 전자서명을 수행하여 전자서명 값 $DS_Value = E_{rk}(Q_Value)$를 생성한다.
이를 통해 송신자 부인방지를 제공할 수 있다. 특히, 부인방지는 전자 금융 거래에서 송신자가 거래한 사실을 부인하지 못하게 하는 근거로서 선택이 아닌 필수요소이다.

⑨ 사용자는 DS_Value와 인증서를 서비스 제공자에게 전송하고 인증을 요청한다.

⑩ 서비스 제공자는 전송받은 사용자 인증서에 대한 유효성 검증을 인증기관에게 요청한다.

⑪ 인증기관은 전송받은 인증서에 대한 유효성 검증을 수행한다.

⑫ 인증기관은 유효성 검증 결과를 서비스 제공자에게 전송한다.

⑬ 서비스 제공자는 검증 결과를 확인하고 유효한 인증서 일 경우 사용자로부터 전송받은 DS_Value를 사용자의 공개키 pk를 이용하여 복호화를 수행하고 응답 값을 획득한다. 응답 값은 $Q\_Value1$

$= D_{pk}(DS_Value)$값을 가진다.

⑭ 서비스 제공자는 자신이 '④'에서 확보하고 있는 질의 값 Q_Value와 사용자로부터 전송받은 응답값 Q_Value1을 비교한다. 이를 통해 OTP값의 무결성을 보장함으로서 패스워드의 위변조가 없음을 확인 할 수 있다.

⑮ 검증 결과를 사용자에게 전송한다.

## Ⅳ. 실험 및 비교분석

### 4.1 실험 환경

제안하는 시스템의 실험을 위한 환경 구성은 다음과 같다. 먼저 서버의 하드웨어적 구성은 CPU : Intel® Xeon® 5140 듀얼코어 프로세서 2.33GHz, 내장 캐시 : 4MB L2 캐시, 메모리 2048M, 네트워크 인터페이스 : 듀얼 NC373i 다기능 기가비트이며, 클라이언트의 하드웨어적 구성은 CPU : Intel® Pentium 듀얼코어 E2180, 내장 캐시 : 1MB L2 캐시, 메모리 DDR2 1024M, 네트워크 인터페이스는 Intel® Pro/1000 MT Network Connection을 사용하였다.

시스템 소프트웨어는 서버의 운영체제로 리눅스 페도라 8.0, 클라이언트의 운영체제는 Windows XP Professional을 사용하였으며 인증 서버를 구축하기 위해 CryptoSys PKI Linux Version과 Mysql을 이용하였고, 클라이언트의 사용자 인터페이스 개발을 위해 Visual_C++ 2005를 이용하였다.

해쉬 알고리즘으로는 160비트 출력 크기의 SHA1을 이용하였고, 해쉬 정보에 대한 암복호화를 위해서는 3DES 알고리즘을 이용하였다. 또한, 공개키 알고리즘으로 RSA 알고리즘을 이용하였다.

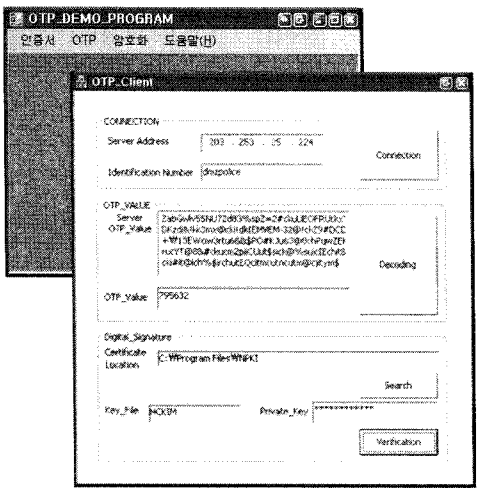



그림 6. 실행 화면

(그림 6)은 실행화면으로써 서버에서 생성된 OTP가 암호화되어 사용자에게 정확하게 전달되는지, 그리고 전송받은 OTP에 대하여 사용자의 개인키를 이용하여 전자서명 한 후 검증을 요청했을 때 검증이 정확하게 이루어지는지에 대하여 중점을 두고 실험을 진행하였다.

### 4.2 비교 분석

제안한 메커니즘과 기존 메커니즘과의 성능 분석을 위하여 재생공격, 기밀성, 무결성, 부인방지, 동기화, 인증시간, 동기화로 인한 실패확률, 인증형태 등 총 8가지 성능 평가 요소에 대하여 비교 분석을 수행하였다.

Ⅰ. 재생공격 : 시간 기반 동기화 메커니즘은 일정 주기 동안의 동일한 대표값을 이용하여 패스워드를 생성함으로써 재생공격 위협에 노출되어 있으나 제안 메커니즘을 포함한 다른 메커니즘들은 패스워드 생성 값에 대하여 주기성을 가지지 않기 때문에 재생공격으로부터 안전하다.

Ⅱ. 기밀성 및 무결성 : 제안 메커니즘과 기존 메커니즘 모두 암호화와 해쉬를 적용하여 해당 정보를 전송함으로써 기밀성과 무결성을 보장할 수 있다.

Ⅲ. 부인방지 : 기존 메커니즘과 달리 제안한 메커니즘은 사용자의 개인키를 이용하여 OTP에 대해 전자서명을 수행하기 때문에 부인방지를 보장하며, 위와 더불어 전자서명값과 인증서를 함께 전송하고 이를 통해 인증서 인증 및 패스워드 인증을 수행하기 때문에 보안성을 더욱 강화한다.

Ⅳ. 동기화 : 비동기화 메커니즘과 제안하는 메커니즘은 인증 요청이 발생할 때마다 새로운 패스워드를 임의적으로 생성하기 때문에 별도의 동기화를 필요로 하지 않는다.

Ⅴ. 인증 시간 : 제안하는 메커니즘에서 향후 지속적으로 해결해야 되는 부분으로 시간동기화 방법, 이벤트 동기화 방법은 1패스 인증을 이용함으로써 빠른 인증 시간을 보장하지만 제안하는 메커니즘과 비동기 메커니즘은 2패스 인증을 이용하기 때문에 기존 동기화 방법에 비해 인증 시간이 다소 오래 걸린다는 단점이 존재한다.

Ⅵ. 동기화로 인한 실패 확률(가용성) : 시간 동기화 방법은 인증을 요청하고 일정시간 이상 인증을 받지 못하면 해당 패스워드는 폐기되고 새로운

표 1. 성능 분석

| 평가요소 / 인증 메커니즘 | | 재생 공격 | 기밀성 | 무결성 | 부인 방지 | 동기화 | 인증 시간 | 동기화로 인한 실패확률 | 인증형태 |
|---|---|---|---|---|---|---|---|---|---|
| 비동기화 메커니즘[6][12] | | 불가능 | 제공 | 제공 | 미제공 | 없음 | 느림 (2패스) | 없음 | Type Ⅰ |
| 동기화 방식 | 시간기반[4][10] | 가능 | 제공 | 제공 | 미제공 | 있음 | 빠름 (1패스) | 있음 | Type Ⅰ |
| | 이벤트기반[10][11] | 불가능 | 제공 | 제공 | 미제공 | 있음 | 빠름 (1패스) | 있음 | Type Ⅰ |
| 제안하는 메커니즘 | | 불가능 | 제공 | 제공 | 제공 | 없음 | 느림 (2패스) | 없음 | Type Ⅰ+Ⅱ |

비밀번호가 생성될 때까지 기다려야한다. 또한, 이벤트 동기화 방법은 OTP 생성매체와 인증 서버간의 인증 횟수가 동기화 되어 있지 않으면 해당 패스워드 값은 폐기되며 이로 인해 가용성을 보장할 수 없다는 문제가 발생한다. 그러나 제안하는 알고리즘과 비동기식 알고리즘은 동기화 과정 없이 인증 요청시점에서 패스워드를 생성하고 이를 통해 상호 인증을 수행하기 때문에 동기화로 인한 실패 확률이 없으며 이를 통해 가용성을 보장할 수 있다.

Ⅶ. 인증형태 : 인증을 위해 기존의 기법들은 사용자 기억 정보에 의존하는 인증 형태인 Type Ⅰ만을 제공한다. 그러나 제안하는 기법은 사용자 기억 정보와 소유 정보가 결합된 인증 형태인 Type Ⅱ를 제공함으로서 보안성을 강화 할 수 있으며 이러한 비교 분석 결과를 정리하면 (표 1)과 같다.

## V. 결 론

본 논문에서는 기존의 비동기식 일회용 패스워드 인증 메커니즘, 시간을 이용한 동기식 인증 메커니즘 그리고 이벤트 기반의 동기식 인증 메커니즘의 구조 및 절차 그리고 보안적 취약점을 분석하고 이를 해결하기 위한 인증서를 이용한 보안성이 강화된 일회용 패스워드 메커니즘을 제안하였으며 다른 메커니즘과의 비교 분석을 통해 제안 메커니즘의 우수성을 증명하였다. 제안하는 메커니즘을 위한 기본 프레임은 공개키 기반 구조를 사용하였으며, 패스워드 생성 형태는 비동기식 방법을 사용하였다. 또한 생성한 패스워드에 대해서는 사용자의 개인키로 전자서명을 수행함으로서 부인방지를 보장하였으며 인증과정을 인증서 검증과 패스워드 검증으로 세분화하여 기존 일회용 패스워드 메커니즘에 비해 한층 강화된 보안성을 제공할 수 있었다. 그러나 기존 동기식 방법과 달리 2패스 인증을 사용한다는 점에서 인증 시간이 다소 오래 걸린다는 단점이 있으며, 인증서 생성 시 인증서 저장 폴더를 변경할 경우 해당 인증서를 찾지 못하는 경우가 간혹 발생하였다. 따라서 제안하는 시스템은 시간적 특성보다는 인터넷뱅킹, 전자결제, 의료시스템과 같은 보안성이 강조되는 분야에 적합할 것으로 판단되며, 향후에 본 논문에서 단점으로 지적된 인증 시간을 감소시킬 수 있는 방법에 대한 연구를 지속적으로 진행해 나갈 것이다.

## 참 고 문 헌


[1] 이성운, 김현성, 유기영, "패스워드 기반의 효율적인 키 교환 프로토콜", 한국정보과학회논문지, 정보통신 제31권 제4호, pp.347-352, 2004.

[2] 최은정, 김찬오, 송주석, "공개키 암호 기법을 이용한 패스워드 기반의 원거지 사용자 인증 프로토콜", 한국정보과학회논문지, 정보통신 제30권 제1호, pp.75-80, 2003.

[3] Cheng Xiao-rong, Feng Qi-yuan, Dong Chao, Zhang Ming-quan, "Research and Realization of Authentication Technique Based on OTP and Kerberos", HPCASIA'05, pp.412-416, 2005.

[4] 박중길, 장태주, 박봉주, 류재철, "시간을 이용한 효율적인 일회용 패스워드 알고리즘", 한국정보처리학회논문지, 제8-C권 제4호, pp.373-378, 2001.

[5] SHIMIZU Akihiro, HORIOKA Tsutomu, INAGAKI Hirohito, "A password authentication method for contents communication on the internet", IEICE transactions on communications, Vol.E81-B, No.8, pp.1666-1673, 1999.

[6] Chris J. Mitchell, Liqun Chen, "Comments on the S/KEY user authentication scheme", ACM Operating Systems Review, Vol.30, No.4, pp.12-16, 1996.

[7] 유일선, 조경산, "공개키를 적용한 S/KEY 기반

의 안전한 사용자 인증 프로토콜", 한국정보처리학회논문지, 제10-C권 제6호, pp.763-768, 2003.
[8] Chun-Li Lin, Ching-Po Hung, "Masquerade on One-Time Password Authentication Scheme", FGCN2007, pp.279-283, 2007.
[9] 김영국, "One Time Password", GIS, 2006. URL source: http://www.gsion.com
[10] 김기영, "일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰", 한국정보보호학회지, 제17권 제3호, pp.26-31, 2007.
[11] 최동현, 김승주, 원동호, "일회용 패스워드(OTP : One-Time Password) 기술 분석 및 표준화 동향", 한국정보보호학회지, 제17권 제3호, pp.12-17, 2007.
[12] Nail M. Haller, "The S/KEY ONE-TIME PASSWORD SYSTEM", Internet Society Symposium on Network and Distributed System Security, pp.151-158, 1994.
[13] Nail M. Haller, C. Metz, P. Nesser and M. Straw, "A one-time password system", RFC2289, 1998.
[14] 박왕석, 정종필, 박창섭, 이동훈, "패스워드를 이용한 인증 프로토콜들에 대한 고찰", 한국정보보호학회학술지, 제9권 제4호, pp.51-63, 1999.
[15] Men Long, Uri Blumenthal, "Manageable One-Time Password for Consumer Applications", ICCE 2007, pp.10-14, 2007.
[16] 박중길, 김영진, 백규태, 백기영, 류재철, "S/KEY를 개선한 일회용 패스워드 메커니즘 개발", 한국정보보호학회논문지, 제9권 제2호, pp.25-35, 1999.
[17] J. Archer Harris, "OPA : A One-Time Password System", ICPPW02, 2002.
[18] PWDUMP6 Version1.7.2, 2008. URL source: http://www.foofus.net/fizzgig/pwdump/downloads.htm
[19] Solar Designer. John the ripper, 2003. URL source: http://www.openwall.com/john/
[20] Lim, R. "Parallelization of John the Ripper using MPI". Nebraska: University of Nebraska. January 22, 2004.
[21] Alec D.E. Muffett, "Crack v4.1 - A Sensible Password Checker for Unix". Unix Software Engineer Aberystwyth, Wales, UK.
[22] Bugtraq: ANNOUNCE : NTCrack v2.0. URL source: http://seclists.org/bugtraq/1997/Mar/0103.html

**김 현 철** (Hyun-chul Kim) 정회원

2003년 인제대학교 컴퓨터학부 (학사)
2005년 경원대학교 전자계산학과 (석사)
2006년 3월~현재 숭실대학교 컴퓨터학과 박사과정
<관심분야> PKI, 공인전자문서, 디지털 ID관리, 정보호호, 암호학

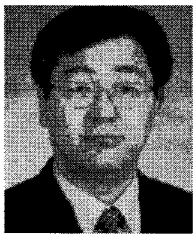
**이 창 수** (Chang-soo, Lee) 정회원

1999년 한서대학교 컴퓨터과학과 (학사)
2002년 숭실대학교 컴퓨터공학과 (석사)
2005년 숭실대학교 컴퓨터공학과 (박사)
2006년~현재 (주)리테일테크 기술연구소 수석연구원
<관심분야> 영상처리, 멀티미디어보안, RFID 보안, 네트워크 보안

**이 경 석** (Kyung-seok Lee) 정회원

1978년 숭실대학교 (학사)
1981년 성균관대학교 (석사)
1986년 University Paris 7 (박사)
1987년~2008년 산업연구원 연구위원
2008년~현재 숭실대학교 겸임교수
<관심분야> 데이터베이스, 네트워크보안, 정보보안 표준, 정보보안 알고리즘

**전 문 석** (Moon-seog Jun) 정회원



1981년 숭실대학교 전산학과 (학사)
1986년 University of Maryland 전산학과 (석사)
1989년 University of Maryland 전산학과 (박사)
1989년~1991년 New Mexico State University Physical Science Lab. 책임연구원
1991년~현재 숭실대학교 컴퓨터학과 정교수
<관심분야> Network Security, 암호학, PKI, 디지털 ID관리, 전자여권, 정보보호