시간을 이용한 효율적인 일회용 패스워드 및 시간 교정 알고리즘

정회원 강 철 오*, 박 중 길**, 홍 순 좌***, 배 병 철****, 박 봉 주*****

A Study on the Algorithm of Improved One-Time Password using Time and Time Correction

Cheol-Oh Kang*, Joong-Gil Park**, Soon-Jwa Hong***, Byung-Cheol Bae****,
Bong-Joo Park***** *Regular Members*

요 약

시간을 이용한 일회용 패스워드 방식은 별도 동기가 필요 없기 때문에 클라이언트/서버 환경 등에서 특히 유용하게 사용될 수 있다 그러나 시간을 이용한 일회용 패스워드 방식에서는 시간편차에 의한 인증 실패가 발생할 수 있다. 이 논문에서는 시간편차에 의한 인증이 실패할 가능이 있는 기간을 표시하는 1비트 정보를 이용하여, 시간편차에 의한 인증 실패가 발생하지 않는 효율적인 일회용 패스워드 알고리즘을 제안하며, 아울러 제안된 일회용 패스워드 알고리즘에 부가정보 2 비트를 추가하여 시간교정을 겸할 수 있는 알고리즘 또한 제안한다.

ABSTRACT

In clients/server environments, the one-time password scheme using time is especially useful because it solves the synchronization problem. However, it has the problem that is time-slippage, and causes the authentication to fail. In this paper, we propose an effective one-time password algorithm, which solves the time-slippage problem through the use of 1-bit information, which denotes the duration in which the authentication could be failed because of time-slippage. This algorithm is added easily and quickly to current one-time password systems using time without requiring any change of protocols: the proposed algorithm can be implemented by adding only 1-bit information to the user authentication information, not by modifying the one-time password authentication system protocol. And we propose also the algorithm of time correction, which can be implemented by adding 2-bit information on the proposed one-time password.

I. 서 론

일회용 패스워드에 기반한 인증시스템들은 시간, 노이즈, 그리고 의사난수(pseudo-random sequence number) 같은 여러 non-repeating 값들을 생성하여 일회용 패스워드로 이용하며, 현재 주로 사용되는 non-repeating 값들과 관리되는 방법은 다음과 같다 [1].

- ◆ random 패스워드 목록 이용(패스워드 목록 내의 위치 동기화 필요)
- ◆ 의사난수 이용(sequence generator의 상태 동기화 필요)
- ◆ 시간 이용(시간의 동기화 필요)

많은 수의 클라이언트/서버 환경에서 위의 random 패스워드 목록과 의사난수 방법은 사용자별로 동기화 정보들을 별도로 유지 관리하여야 하는 요구사항이 있다. 따라서 이들 동기화 정보들을

* 국가보안기술연구소(cyberkan@etri.re.kr)
** 국가보안기술연구소(jgpark@etri.re.kr)
*** 국가보안기술연구소(sjhong@etri.re.kr)
**** 국가보안기술연구소(bcbae@etri.re.kr)
***** 호서대(bjpark63@hotmail.net)
※ 본 논문은 2002년 4월 JCCI 학술대회에서 우수논문으로 선정되어 게재 추천된 논문입니다.

유지 관리에 많은 문제점을 유발한다. 그러나 시간을 이용한 방법은 시간 정보 자체를 클라이언트/서버의 동기화된 정보로 이용할 수 있으므로, 별 다른 유지 관리 문제 없이 사용할 수 있다.

시간을 이용한 일회용 패스워드 인증 시스템은 시간의 단위기간 내에서 대표값을 취하여 단위기간 내에서는 이 대표값을 인증 시스템에 입력값으로 한다. 일반적으로 단위기간 내에서 대표값은 그 구간의 시작점으로 선택한다. 예를 들어, 1분마다 패스워드가 변경되는 인증 시스템은 그림 1과 같이 시각이 aa:bb:cc일 때는 그 대표값으로 aa:bb:00을 취한다.

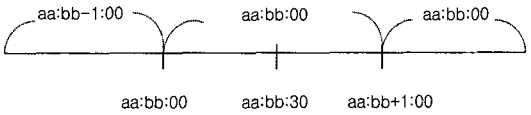


그림 1. 분 단위 패스워드 인증에서 대푯값

특히, 모든 단위기간이 일정할 때, 이 단위기간을 유효기간이라 부르며, 이 유효기간 동안은 동일한 대표값이 지속된다. 새로운 대표값이 시작되는 점을 변경점이라 하면 위 시스템의 유효기간은 1분이고 변경점은 매 0초가 되는 시점이다. 위의 시스템을 일반화하기 위하여 이후 모든 시간은 초로 환산한 시간을 사용하며, 시간을 이용한 일회용 패스워드의 일반적인 알고리즘은 다음과 같다.

<시간을 이용한 일반적인 알고리즘>
T_c: 클라이언트의 시간, T_s: 서버의 시간
R(x): 시간 x를 초로 환산한 후 해당되는 대표값을 계산하는 함수
ID_c: 클라이언트 고유번호, Password : 클라이언트 패스워드
H: 일반적인 일방향 함수
(클라이언트)
단계 C1 : T_c 읽음
단계 C2 : R(T_c) 계산
단계 C3 : H(ID_c, Password, R(T_c)) 계산
단계 C4 : ID_c, H(ID_c, Password, R(T_c)) 전송

(서버)
단계 S1 : ID_c, H(ID_c, Password, R(T_c)) 수신
단계 S2 : T_s 읽음
단계 S3 : R(T_s) 계산
단계 S4 : ID_c의 패스워드 Password 읽음
단계 S5 : H(ID_c, Password, R(T_s)) 계산
단계 S6: H(ID_c, Password, R(T_c)), H(ID_c, Password, R(T_s)) 비교

위의 시간을 이용한 알고리즘에서 다음과 같은 3가지의 문제점이 존재한다[1].

◆ 시간의 동기화(time synchronization) 문제
◆ 유효기간에서 동일 패스워드 재사용 문제
◆ 시간편차 문제

시간을 이용한 방식에서 인증 데이터를 일치시키기 위해서는 시간에 대한 동기가 보장되어야 하는데, 이 시간의 동기화 문제는 클라이언트와 서버가 지역적으로 멀리 떨어져 있는 경우에 발생한다. 그러나 이는 그리니치(Greenwich) 표준시간 프로그램을 클라이언트/서버 양쪽에 설치함으로써 별 무리 없이 해결이 될 수 있다.

유효기간(현재의 일회용 패스워드가 계속적으로 사용되는 기간)에서 동일 패스워드 재사용 문제는, 시간을 이용한 방식에서 유효기간 내에 클라이언트가 생성하는 일회용 패스워드가 항상 같게 되므로, 해커가 네트워크 상의 패스워드를 도청하여 유효기간 내에 재접속을 시도한다면, 해커가 사용자 인증에 성공하게 되어 인증 시스템에 문제를 야기한다. 이 문제는 사용자 별로 가장 최근의 인증 성공 시간을 유지함으로써 해결이 될 수 있다. 즉 한 번 인증 후에, 유효기간 내에 또 다시 접속 시도가 오면 서버는 가장 최근의 인증 성공 시간을 보고 유효기간이 끝나지 않았을 경우에 인증을 거부하도록 하면 된다.

그러나 시간을 이용한 방식에는 더욱 심각한 시간편차의 문제가 항상 존재한다[1]. 클라이언트들과 서버들 간에는 교정주기에 의한 시간편차와 클라이언트의 인증 데이터 계산시간, 그리고 전송시간 등에 의해 시간편차가 발생한다. 이 시간편차는 시간 동기를 보장하지 못하여, 인증이 제대로 수행되지 않는 기간을 발생시킨다. 인증 실패확률은 (1)과 같으며, 시간이 경과함에 따라 시간편차가 증가함으로, 점점 더 실패확률은 커져서 큰 문제가 된다(실패확률이 1보다 큰 경우에는 항상 인증 실패를 의미함).

인증 실패확률 = (시간편차+클라이언트 계산시간+전송시간) / 유효기간 (1)

일반적인 알고리즘에서 사용하는 일방향 함수는 계산 속도가 빠른 알고리즘을 사용하고 있으며, 전송시간이 시간편차에 비하며 적은 크기 일 때, 위의 인증 알고리즘에서 인증 실패확률을 줄이기 위해서는 시간편차가 적은 시계를 사용하고 유효기간을 확장하면 된다. 그러나 시간편차가 적은 시계를 사용하기 위해서는 많은 비용이 소요되며, 유효기간을 확장하는 것은 유효기간 내에 대표값을 반복 사용하는 것으로 인한 안전성에 위협을 받을 수 있다.
일반적으로, 시간편차에 의한 인증 실패 시에 해결하는 방법으로는 3 가지가 있다. 첫째는 별도의 조치를 취하지 않고, 시간편차에 의한 인증 실패 시에 다시 인증을 받도록 하는 것인데, 이는 인증 시스템의 성능 저하를 유발할 것이다. 둘째는 인증 실패 시에 서버에서 현재 인증값 전후의 여러 값과 비교하여 인증을 수행하는 것이다. 이 방법은 사용자의 패스워드가 서버에서 여러 패스워드로 간주되어 비교 사용되므로, 그만큼 비도가 떨어진다. 셋째는 인증 실패 시에 서버가 시간값을 클라이언트에 재전송하여 다시 인증을 수행하는 것이다. 이 방법 또한 3패스 인증이 되며 여전히 시간편차에 의한 인증 실패확률이 존재한다.

Ⅱ. 시간을 이용한 새로운 일회용 패스워드 알고리즘

이 논문에서는 시간을 이용한 일회용 패스워드 시스템 설계에서, 가장 큰 문제점으로 제시되고 있는 시간편차 문제를 해결할 수 있는 알고리즘을 제시한다. 각 클라이언트와 서버에 내장된 시계는 수정 진동자의 오차가 존재하며, 시계 교정주기에 의해 오차값은 변경 될 수 있다. 즉, 각 클라이언트와 서버 시계는 시계의 수정 진동자와 교정주기에 의한 오차를 갖게 된다 (일반적으로 클라이언트는 일회용 패스워드 생성기라 불리는 토큰을 이용한다). 이러한 오차로 인해, 내장 시계의 시간을 이용한 일회용 패스워드 인증 시스템을 사용하는 임의의 두 클라이언트/서버 간의 인증을 수행할 때, 다른 인증값이 발생되며 인증 실패의 한 요인이 된다. α 를 각 내장된 시계의 최대오차라고 하면, α 는 시계가 가진 수정 진동자의 최대오차와 컴퓨터의 시계 교정주기의 최대값에 의해 결정된다. 절대시각 N에 대해 클라이언트와 서버 시계의 최대오차가 $\pm\alpha$ 이므로, 클라이언트와 서버간의 시계 최대편차 T는 다음과 같이 구하진다.

$$T = 2\alpha \quad (2)$$

이제 기존의 시간을 이용한 인증 시스템에서 다음의 이론적인 배경을 도입하여 시간을 이용한 효율적인 인증 시스템을 구현하고자 한다.
$V \geq 2T$인 어떤 자연수 V, T에 대해서, 집합 Z, $N \rightarrow N$ 특성 함수(characteristic function) flagVT(x), $N \rightarrow N$ 단계 함수(step function) R(x)를 다음과 같이 정의한다

$$Z=\{x\in N \mid nV-T\leq x<nV+T \text{ for some } n\in N\}, \quad (3)$$

$$\text{flagVT}(x) = \begin{cases} 1 & \text{if } x \in Z \\ 0 & \text{otherwise,} \end{cases} \quad (4)$$

$$R(x) = \lfloor x/V \rfloor \times V, \quad (5)$$

여기서 $\lfloor y \rfloor$ 는 y 보다 크지 않는 최대정수를 의미한다.

보조정리 2.1 자연수 x, y, V, T에 대해서, $|x-y| < T$, $V \geq 2T$ 및 flagVT(x) = 0을 만족하면, R(x - T) = R(y)가 성립한다.

증명: $V \geq 2T$, flagVT(x) = 0이므로, $nV+T \leq x < (n+1)V-T$를 만족하는 자연수 n이 존재한다. 따라서 $nV \leq x-T < (n+1)V-2T$로 표기할 수 있으며 식 (16)의 정의에 의해 R(x-T) = n이다. $|x-y| < T$이므로, $x-T < y < x+T$이고, $nV < y < (n+1)V$이다. 즉 R(y) = n. 그러므로 R(x-T) = R(y)이다.

정리 2.1 자연수 x, y, V, T에 대해서, $|x-y| < T$, $V \geq 4T$ 및 flagVT(x) = 1을 만족하면, R(x - T) = R(y - 2T)이 성립한다.

증명: flagVT(x) = 1이므로, $x = nV + r$을 만족하는 적당한 $n \in N$과 $r(-T \leq r < T)$가 존재한다. 그러면, R(x-T) = (n-1)V이고 $|x-y| < T$이므로, $x-T < y < x+T$. $nV+r-T < y < nV+r+T$. $nV+r-3T < y-2T < nV+r-T$. 그러므로 $nV-V < y < 2T < nV$. R(y-2T) = (n-1)V.

이 논문에서는 시간편차에 의한 인증이 실패할 가능이 있는 기간을 표시하는 별도의 1 비트를 추가 전송하여, 시간을 이용한 기존의 인증 시스템에서 발생하는 시간편차에 의한 인증 실패확률을 제거하는 알고리즘을 제안한다.

<시간편차 보정 알고리즘>
T : 클라이언트와 서버 시계의 시간 최대편차
V : 유효기간
Ttflag : 시간편차에 의한 인증이 실패할 가능이 있는 기간을 표시하는 1 비트 플래그

(클라이언트)
단계 C1 : T_c 읽음
단계 C2 : R(T_c) 계산
단계 C3 : Ttflag = 0
단계 C4 : IF(T_c - R(T_c) < T) then Ttflag = 1
IF(V-(T_c-R(T_c))<=T) then Ttflag = 1
단계 C5 : IF(Ttflag = 1) then T_c = T_c - T
단계 C6 : H(ID_c, Password, R(T_c)) 계산
단계 C7 : ID_c,H(ID_c,Password,R(T_c)),Ttflag 전송

(서버)
단계 S1: ID_c, H(ID_c, Password, R(T_c)), Ttflag 수신
단계 S2: T_s 읽음
단계 S3: IF(Ttflag = 1) then T_s = T_s - 2T
단계 S4 : R(T_s) 계산
단계 S5: ID_c의 패스워드 Password 읽음
단계 S6 : H(ID_c, Password, R(T_s)) 계산.
단계 S7: H(ID_c, Password, R(T_c)), H(ID_c, Password, R(T_s)) 비교

위 알고리즘의 인증 성공확률은 유효기간과 시계의 시간편차에 영향을 받는다. 보조정리 2.1과 정리 2.1에 의하여 $V \geq 4T$ 이면, 위의 시간편차 보정 알고리즘은 정상적인 사용자와는 항상 인증 가능하다.

그러나 위의 시간편차 보정 알고리즘은 전송시간을 고려하지 않아 언제나 인증을 성공하는 것은 아니다. 클라이언트 계산, 전송, 지연 그리고 토큰 입력 시간 등을 간략히 지연시간이라 하면 지연시간은 위 알고리즘의 안정성에 많은 영향을 준다. 이 지연시간이 일정하다면 효과적인 인증 알고리즘을 도출할 수 있지만, 일정하지 않다면 인증 알고리즘 설계에 문제가 발생한다. 이 논문에서는 다음과 같은 변수 β 를 고려한 인증 알고리즘을 제시한다.

<전송시간을 고려한 시간편차 보정 알고리즘1>
β : 클라이언트 계산, 전송 및 지연에 따른 토큰 입력의 최소시간

(클라이언트)
<시간편차 보정 알고리즘>에서 단계 C1후에 T_c = T_c + β 만 추가

(서버)
<시간편차 보정 알고리즘>과 동일

위 알고리즘은 최소 지연시간을 클라이언트에서 미리 더하여 계산하므로, 클라이언트 시간 입력값과 서버의 인증시간 차이를 줄일 수 있다. 그러나 클라이언트 계산, 전송 및 지연에 따른 토큰 입력의 최대시간을 γ 라 할 때, 제안한 알고리즘은 지연시간의 변동폭의 차이($\gamma - \beta$)는 보정할 수 없다.

일반적으로 TCP/P 네트워크에서 전송시간의 지연은 매번 달리 발생하고, 이 달라지는 지연시간은 위 인증 알고리즘의 인증 실패의 중요한 요소가 될 수 있다. <129.254.163.146>에서 <168.188.129.155>에 연결할 경우(네트워크 hop: 7)에 최소지연은 25ms 이지만, 최대지연은 600ms까지 발생한다(연결이 되는 상태에서 실측한 값임). 이러한 네트워크 환경에서는 지연시간과 최소 지연시간만을 고려한 위의 알고리즘은 지연시간의 변동폭에 의해서 인증 실패가 발생한다. 특히 T보다 지연시간 변동폭이 훨씬 큰 경우에는 주로 이 지연시간 변동폭에 의해서 인증 실패가 발생한다.

이 논문에서는 시간편차와 지연시간의 변동폭을 고려하여 $\hat{T}$를 정의하고자 한다. 즉 $\hat{T}$를 시간편차와 지연시간 변동폭의 합으로 정의하고, $V \geq 4\hat{T}$ 라고 정의하여 위의 알고리즘을 다음과 같이 수정을 하면, 예상되는 네트워크의 최대 지연시간 내에서는 인증 실패가 발생하지 않는 효율적인 알고리즘이 된다. 따라서 위의 알고리즘은 시간을 이용한 일회용 인증 알고리즘으로써 매우 효과적이다.

<전송시간을 고려한 시간편차 보정 알고리즘2>
β : 클라이언트 계산, 전송 및 지연에서 토큰 입력 최소시간
γ : 클라이언트 계산, 전송 및 지연에서 토큰 입력 최대시간
$\hat{T}$: $T+(\gamma - \beta)$
V: $\geq 4\hat{T}$

(클라이언트)

<전송시간을 고려한 시간편차 보정 알고리즘1>>에서 T대신 $\dot{T}$ 적용

(서버)
<전송시간을 고려한 시간편차 보정 알고리즘1>>에서 T대신 $\dot{T}$ 적용

제안한 알고리즘과 기존의 알고리즘과의 성능 분석의 결과는 표 1에 정리하여 표시하였다. 이 표에서 나타낸 것처럼, 제안한 알고리즘은 시계의 시간편차에 따른 인증 실패확률이 없고, 또한 지연시간에 따른 실패확률도 예측된 최대 지연시간 이내에서는 인증 실패가 존재하지 않는 효율적인 인증 알고리즘이다.

표 1. 제안한 인증 알고리즘의 성능 분석

성능평가 요소 / 인증 알고리즘	시계의 시간편차에 따른 인증 실패 확률	기존 1패스 시스템에 적용 가능성	인증 시간	지연시간에 따른 인증 실패 확률
기존의 시간을 이용한 알고리즘	편차/유효기간	가능함	빠름 (1패스)	있음
Challenge-Response	없음	불가능	느림 (2패스)	없음
제안한 알고리즘	없음	가능함	조금 느림 (1패스 +△)	예상 최대지연시간 내에서는 없음

△:Ttflag 값 설정 시간

클라이언트마다 토큰 계산시간 및 전송시간 등 즉, 지연시간에 차이가 있는 경우에 기존의 인증 알고리즘들은 매우 불안정적이다. 그러나 사용자마다 정확한 최대 지연시간을 사전에 입력하여 이 논문에서 제안한 알고리즘을 사용한다면 이러한 문제점은 해결할 수 있으며, 사전에 시계의 시간편차의 정확한 한계치를 계산할 수 있다면, 매우 효율적인 인증 알고리즘을 구현할 수 있다.

클라이언트/서버 환경에서 시간을 이용한 일회용 패스워드 인증 시스템을 구현 시에 시간편차에 의한 인증을 실패할 경우가 존재한다. 이 논문에서는 이러한 기존의 인증 시스템에서 인증 실패기간에서 조차 인증 실패가 발생하지 않는 시간을 이용한 효율적인 인증 알고리즘을 제안하였다. 제안한 알고리즘은 일회용 패스워드 인증 시스템의 프로토콜 변화 없이, 단지 1 비트를 사용자 인증 정보에 추가함으로써 구현 가능하다. 그리고 이 알고리즘의 인증 실패확률은 클라이언트/서버의 최대 지연시간 범위 내에서는 없으며, 알고리즘이 간단하여 클라이언트/서버 양쪽에 빠른 수행시간을 제공한다. 그러므로 이 논문에서 제안한 알고리즘을 이용하여 일회용 패스워드 인증 시스템을 완전하고, 효율적으로 구현이 가능하다.

Ⅲ. 시간교정 기능을 갖는 새로운 일회용 패스워드 알고리즘

1 비트의 부가정보를 사용하는 시간을 이용한 인증 메커니즘은 시간의 최대편차 내에서 항상 인증이 성공하는 효율적인 인증 알고리즘이지만, 클라이언트와 서버의 시간의 최대편차가 T보다 큰 경우에는 인증 실패가 존재하게 되면, 클라이언트 시간의 오차를 수정해 줄 수가 없다. 하나의 클라이언트가 하나의 서버에만 접속하는 환경에서는 효율성을 보장할 수 있지만, 하나의 클라이언트가 여러 서버에 접속하여 시간을 이용한 인증 메커니즘을 적용할 경우에, 서버들의 시간이 다른 경우에 제안한 인증 메커니즘의 적용에 많은 문제점들을 내포할 수 있다. 즉 시간 차이가 T 이상인 A와 B 서버에서, A 서버에서 인증이 되었지만, B 서버에선 인증 실패가 항상 발생하여 클라이언트에게 시간교정을 요구할 수 있다. 이 같은 문제는 시간 전체를 전송하는 시스템에서도 발생할 수 있는 문제이며, 이러한 경우에도 항상 인증이 될 수 있는 알고리즘을 제안하고자 한다.

제안하는 방법은 기존 제안한 알고리즘의 1 비트 부가정보에 2 비트를 추가하여 총 3 비트의 부가정보로 시간교정 기능을 겸하도록 하는 것이다. 즉 유효기간인 V를 8개의 영역으로 나누어서, 클라이언트에서는 전송 시에 자신이 속한 영역값 3 비트를 서버로 전송하고, 서버는 이 값으로부터 시간편차에 의한 인증 실패할 가능이 있는 구간 여부를 판단하여 인증을 수행하고, 그리고 클라이언트와의 시간 영역에서 차이를 판단하여 다른 시간 영역에 있을 경우에 시간을 같은 영역에 위치의 수정한다.

이러한 방법을 적용하기 위해서 먼저 서버에는 최초의 클라이언트 등록 과정과 클라이언트마다 시간편차 정보를 유지 관리해야 한다. 최초의 클라이언트 등록에서 클라이언트 전체 시간 정보를 전달하여, 서버가 클라이언트와의 시간편차 정보를 계산

하여 유지 관리하게 한다. 시간교정 즉, 클라이언트의 재접속은 반드시 클라이언트와 서버의 시간편차가 T/2 이내인 경우에 이루어진다고 가정한다. 그리고, 제안하는 방법은 앞에서 제안한 시간을 이용한 인증 메커니즘의 개념을 그대로 이용하지만, 1 비트의 Ttflag 대신에 3 비트 Ttflag로 변경한다. 분 단위 인증 시스템에서 T를 15초 가정할 경우에 Ttflag의 값이 0, 1, 6, 7인 경우에 시간편차에 의한 인증 실패가 발생할 가능이 있는 것을 표시한다. 즉 1 비트에서 Ttflag가 1인 것에 해당한다.

제안하는 방법을 2 비트 부가정보로 표시하는 경우에는 시간교정의 기능을 제대로 수행하지 못한다. 2 비트 부가정보로 표현하는 경우에도 클라이언트와 서버가 다른 영역에 있을 경우에 시간교정할 수 있지만, 이 교정되는 시간은 T 미만의 편차를 갖는다. T 미만의 편차가 발생한 상태에서 클라이언트의 재접속이 T/2 편차가 발생한 상태에서 되는 경우에는 시간편차가 T 보다 큰 값을 갖게 되어 인증이 실패하게 된다.

3 비트의 부가정보로 표시하는 경우에는 시간교정의 기능까지도 제대로 수행할 수 있다. 3 비트 부가정보로 시간교정까지 가능한 이유는 클라이언트와 서버가 항상 T/2 이내의 시간편차를 가지면서 인증을 수행할 수 있기 때문이다. T/2 미만의 편차가 발생한 상태에서 클라이언트에서 서버에 접속할 때 시간편차가 T/2 이내 이므로 전체 시간편차는 T 이내가 되면 인증이 성공하고, 시간편차 교정 작업을 수행하게 된다. 이 알고리즘은 클라이언트에서 항상 T/2 시간편차이내에 재 접속을 할 경우에 인증이 성공하고, 시간교정을 수행할 수 있는 기능을 제공해 줄 수 있다.

Ⅳ. 결 론

클라이언트/서버 네트워크 환경에서 시간을 이용한 일회용 패스워드 인증 시스템을 구현 시에 시간편차에 의한 인증을 실패할 경우가 존재한다. 이 논문에서는 이러한 기존의 인증 시스템에서 인증 실패기간에서 조차 인증 실패가 발생하지 않는 시간을 이용한 효율적인 인증 알고리즘을 제안하였다. 제안한 알고리즘은 일회용 패스워드 인증 시스템의 프로토콜 변화 없이, 단지 1 비트를 사용자 인증 정보에 추가함으로써 구현 가능하다. 그리고 이 알고리즘의 인증 실패확률은 클라이언트/서버의 최대지연 시간 범위 내에서는 없으며, 알고리즘이 간단하여 클라이언트/서버 양쪽에 빠른 수행시간을 제공한다. 그러므로 이 논문에서 제안한 알고리즘을 이용하여 일회용 패스워드 인증 시스템을 완전하고, 효율적으로 구현이 가능하다.

또한, 이 논문에서는 2 비트의 부가정보를 이용한 새로운 시간교정 기능을 포함하는 인증 메커니즘을 제안하였다. 제안한 메커니즘은 많은 필요성이 대두되고 있는 무선환경 등의 여러 분야에서 효율적이며 안전한 인증 시스템으로 적용이 가능하다

참 고 문 헌

[1] Warwick Ford, Computer Communication Security, Prentice Hall, pp.109-148, 1994.

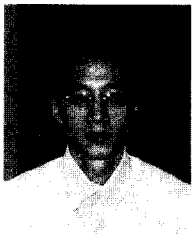
[2] Neil M. Haller, "The S/Key(TM) one-time password system," Proc. Internet Society Symposium on Network and Distributed System Security, pp.151-158, 1994.

[3] A. Simizu, T. Horioka, and H.Inagaki, "A password authentication method for contents communication on the internet," IEICE Trans. Commun., vol.E81-B, no.8, pp.1666-1673, Aug. 1998.

[4] Joonggil Park, Yongjin Kim, Younggil Kim, Gyutae Baek, Kiyoung Baek, and Jaecheol Ryou, "The Development of a One-time Password Mechanism Improving on S/KEY," Korea Institute of Information Security & Cryptology, vol 9, no, pp.25-35, 1999.

[5] Manjula Sandirigama, Akihiro Shimizu, Matu-Tarow Noda, "Simple and Secure Password Authentication Protocol," IEICE Trans. Commun., vol.E83-B, no.6, pp.1363-1365, June 2000.

강 철 오(Cheol-Oh Kang) 정회원



1993년 2월 : 인하대학교 전산과 졸업

1995년 2월 : 인하대학교 전산과 석사

1995.1~1998.12 : 국방정보체계 연구소 연구원

1999.1~2000.1 : 국방과학연구소 연구원

2000. 2~현재 : 국가보안기술연구소 선임연구원
<주관심 분야> 네트워크/시스템 보안, 채널 은닉

박 중 길(Joong-Gil Park) 정회원

1986년 : 동국대학교 전자계산학과 졸업
1988년 : 서강대학교 전자계산학과 석사
2002 : 충남대학교 컴퓨터 과학과 박사
1988년~2000년 : 국방과학연구소 선임연구원
2000년~현 재 : 국가보안기술연구소 선임연구원/팀장
<주관심 분야> 정보보호(컴퓨터보안, 네트워크보안)

홍 순 좌(Soon-Jwa Hong) 정회원

1989년 : 숭실대학교 전산학과 졸업
1991년 : 숭실대학교 전산학과 석사
1991년~2000년 : 국방과학연구소 선임연구원
2000년~현재 : 국가보안기술연구소 선임연구원
<주관심 분야> 암호이론, 네트워크 및 인터넷 보안

배 병 철(Byung-Cheol Bae) 정회원

1994년 2월 : 홍익대학교 전산과 졸업
1996년 2월 : 홍익대학교 전산과 석사
1996.~1998.12 : 국방정보체계 연구소 연구원
1999.1~2000.1 : 국방과학연구소 연구원
2000. 2~현재 : 국가보안기술연구소 선임연구원
<주관심 분야> 네트워크/시스템 보안

박 봉 주(Bong-Joo Park) 정회원

1986년 : 서강대학교수학과 졸업
1988년 : 서강대학교 대학원 수학과 졸업(이학석사)
2000년 : 서강대학교 대학원 수학과 졸업(이학박사)
1988년~2000년 : 국방과학연구소 선임연구원
2000년~2000년 : 국가보안기술연구소 선임연구원
2001년~현재 : (주)시큐진 책임연구원
2002년~현재 : 호서대학교 컴퓨터과학과 겸임교수
<주관심 분야> 정보보호, 컴퓨터통신, S/W 및 H/W 고속 프로토콜