시간기반 패스워드 암호화 시스템

민수홍*, 김명은, 조동섭
이화여자대학교 컴퓨터학과
e-mail:shmin@ewha.ac.kr

A New Login System using the Time Based Password (TBP)

Su-Hong Min*, Myoung-eun Kim, Dong-sub Cho
Dept of Computer Science and Engineering, Ewha Womans University

요 약

인터넷 서비스의 확대에 따라 사용자는 많은 웹사이트에 접근해 자원을 활용하게 되었고, 이와 함께 인터넷 보안에 대한 인식도 커지게 되었다. 본 논문에서는 보안 서비스 중 사용자 인증에 대해 연구하였다. 사용자는 시스템 자원을 활용하기 위해서 시스템으로부터 사용 권한을 획득해야 한다. 시스템 사용 권한을 획득하기 위해서 사용자는 ID, 패스워드 등의 사용자 정보를 시스템에 제공해야 한다. 사용자가 시스템 사용 권한을 획득하면, 사용자는 ID와 패스워드를 이용해서 시스템을 이용할 수 있다. 그러나 현재 숫자나 문자로 이루어진 패스워드 입력 값은 인증 받지 않은 사용자에게 도용될 가능성이 높다. 따라서 본 논문에서는 숫자, 문자로 이루어진 패스워드에 입력키의 시간 값을 적용해서 패스워드를 암호화하는 방법에 대해 제시한다.

1. 서론

인터넷 서비스의 보급과 기술이 확대되어감에 따라 이를 이용하는 사용자가 폭발적으로 증가하게 되었다. 인터넷 서비스를 사용하는 사용자들은 하루에도 수많은 웹사이트에 접근해서 시스템의 자원을 활용하고 있다. 이와 함께 보안에 대한 인식도 커지게 되었다. 본 논문에서는 보안 서비스 중 사용자 인증 서비스에 대해 연구하였다. 사용자 인증 서비스에는 기본적으로 가장 많이 쓰이는 ID-패스워드 기반 인증, 인증서 기반 인증, Kerberos 인증, 공개키 암호화 알고리즘 등 여러 가지 메커니즘이 있다. 이들 메커니즘들은 상황에 따라 달리 적용되는데, 본 논문에서는 가장 많이 쓰이고 있는 ID-패스워드 기반 인증에 대해 연구하였다.

이 논문은 과학기술부의 '여자대학교 연구기반 확충사업' 에 의하여 지원되었음.

사용자는 시스템의 자원을 이용하기 위해서 시스템으로부터 사용 권한을 획득하여야 한다. 사용자는 자신의 ID와 패스워드, 사용자 인적 사항 등을 시스템에 제공해 사용 권한을 얻는다. 사용자의 패스워드는 서비스 등급에 따라 암호화 (Encryption)되어 시스템에 보관된다. 그러나 사용자가 직접 입력하는 패스워드는 일반적으로 간단한 숫자나 문자의 조합으로 구성되어 있어 악의를 가진 사용자가 불법적인 방법으로 다른 사용자의 패스워드를 알아내는 일이 가능하다. 따라서 본 논문에서는 이 같은 문제점을 해결하기 위해서 사용자가 입력하는 입력 값과 입력 시간의 키 핸들링을 이용해서 패스워드를 암호화하는 방법을 제시하였다. 본 논문에서 제시한 시간기반 패스워드 암호화 방법은 사용자 자신이 입력한 패스워드의 키 값과 입력키를 누른 시간의 상대적인 장·단만 기억하면 되므로, 기존의 문자와 숫자만을

입력 값으로 받았던 로그인 시스템의 성능을 개선시킬 수 있다. 또한 간단한 알고리즘으로 이루어져 있어 프로그램의 이식성이 용이해 사용자 패스워드를 필요로 하는 다양한 분야에 적용이 가능하며, 높은 레벨의 보안을 제공하기 위해 쓰이는 암호화 기법과 함께 사용할 수 있다.

본 논문의 구성은 다음과 같다.

2장에서는 관련 연구로서 기존의 사용자 인증 서비스 중 ID-패스워드 기반의 보안 시스템에 관해서 살펴보고, 3장에서는 본 연구에서 제안하고 있는 시간기반 패스워드 암호화 알고리즘의 구현 및 수행 절차를 기술한다. 마지막으로 4장에서는 결론 및 향후 방향에 대해 기술한다.

2. 관련 연구

이 장에서는 기존의 사용자 인증 서비스 중 ID-패스워드 기반의 보안 시스템에 대해서 살펴본다.

▶ OTP (One-Time Password)

OTP (One-Time Password)는 사용자가 인증을 받고자할 때 매번 새로운 패스워드를 사용해야 하는 보안 시스템으로 전세계적으로 가장 많이 쓰이는 프로토콜이다. OTP는 매번 새로운 패스워드를 MD4 또는 MD5 해싱 알고리즘을 사용하여 만들어 낸다. OTP를 이용해 패스워드를 설정한 사용자는 매번 로그인을 시도할 때마다 새로운 패스워드를 이용한다. 이 방법은 침입자들이 이용하고 있는 스니핑 (Sniffing: 패킷 가로채기) 공격을 근본적으로 막아준다 [1,2].

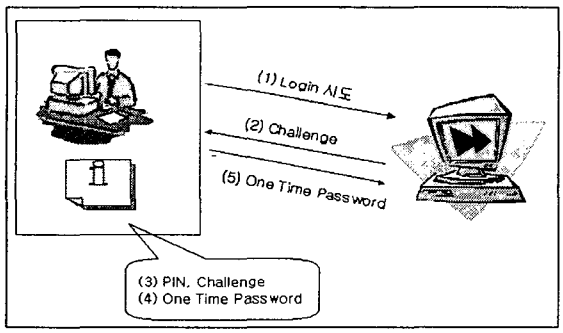

그림 1. One-Time Password

▶ 다이나티브의 웹스퀘어월

PC 보안 인증 장치로 패스워드 각 문자 사이의 입력 시간 차이를 이용해 인증 서비스를 제공한다. 이 방법은 본 논문에서 제시한 시간기반 패스워드 암호화 방법과 유사하다. 우리가 제시한 방법이 키의 입력 시간을 이용하는 것이라면 이 방법은 입력되는 키와 키 사이의 시간차을 이용하는 방법이다. 예를 들어 사용자가 패스워드를 '1234' 라고 입력할 경우, '1', '2' 사이의 시간간격, '2', '3' 사이의 시간간격, '3', '4'의 시간간격을 설정한다. 패스워드를 설정한 사용자는 다음번 로그인 시 입력키값과 키 사이의 입력 시간을 동시에 만족될 때 인증을 받을 수 있다. 그러나 웹스퀘어월은 사용자의 입장을 고려했을 때 여러 문제점을 가진다. 먼저 사용자가 자신이 설정한 키 값과 그에 해당하는 시간 간격을 기억해야하는 어려움이 따른다. 실제 패스워드로 사용되는 키의 길이는 8자 이상이므로 사용자는 8자 이상의 입력값과 각각의 키 사이의 입력 시간을 기억해야 한다. 둘째, 키와 키 사이의 시간 간격의 정확성이다. 처음 시스템에 접근하는 사용자는 키와 키 사이의 시간을 설정해서 패스워드를 지정한다. 사용자가 로그인 할 때, 처음 설정한 시간 간격으로 정확하게 키를 입력해야 시스템에 인증을 받을 수 있다. 그러나 사용자가 초단위로 설정한 시간간격의 차를 고려해서 입력값을 정확히 입력하는데에는 어려움이 따른다 [3].

3. 시간기반 패스워드 암호화 알고리즘

3.1 개요

시간기반 패스워드 암호화 알고리즘은 시스템이 사용자 인증을 요구할 경우, 기존의 패스워드 입력 값에 키의 입력 시간을 추가시키는 방법이다. 사용자는 기존의 패스워드 입력과 거의 동일한 방법으로 패스워드를 설정할 수 있으며, 부가적인 인터페이스 또한 요구되지 않는다.

본 방법은 사용자가 시스템에 사용자 인증을 획득하기 위해 사용자가 정한 패스워드를 입력한다. 사용자는 키 값과 키의 입력 시간 (키를 눌렀다가 떼었을 때의 시간차)을 고려해 패스워드를 설정한다. 키는 입력 값과 함께 키의 입력시간의 장·단을 설정할 수 있다. 예를 들어, '2437' 이라고 사용자가 키 값을 입력할 경우, '2'는 1초 이상으로 '4','3','7'은 1초 이하의 짧은 시간 동안 키를 입력하였다고 가정하면, 우리가 제시한 시간기반 패스워드 알고리즘에 의해 키의 입력 값과 키의 입력 시간이 핸들링된다. 더 이상 입력 키 값이 없으면, 입력 시간을 이용해

서 임계치를 구한다. 임계치는 입력 시간의 평균과 최악의 경우 (worst case) 의 평균값을 이용해서 두 평균값의 조합 평균으로 구한다. 정해진 임계치를 이용해 키의 입력 시간의 장·단을 결정한다.

표1. 입력키에 따른 입력 시간

password	2	4	3	7	평균	(worst) 평균	임계치
Elaspsed Time	1s 206ms	0s 372ms	0s 411ms	0s 114ms	0s 525.22ms	0s 545.45ms	0s 535.24ms

키의 입력시간이 임계치 이상이면 키를 오래 누른 것으로 설정해 원래의 키 값에 임의의 값을 더해 새로운 키 값을 구한다. 여기서는 '2'가 임계치 이상의 키 입력 시간을 가지므로 '2'에 임의의 값을 더해 새로운 키 값을 생성하게 된다. 나머지 입력 값인 '4','3','7'은 그대로 적용된다. 따라서 패스워드의 설정이 끝나면, 사용자는 다음 번에 로그인 할때, 2는 길게 누르고, '4','3','7'은 '2'에 비해 상대적으로 짧은 시간에 누름으로써 로그인 할 수 있다. 우리가 제시한 시간기반 패스워드 암호화 방법은 사용자의 입력 키 값과 사용자 자신이 생각하는 입력 시간의 상대적인 장·단만을 이용해 패스워드를 설정할 수 있다. 따라서 본 방법은 사용자의 입장을 고려해서 패스워드 설정의 복잡도를 줄일 수 있으며, 기존의 문자와 숫자만으로 구성된 패스워드 입력 값을 보완할 수 있다.

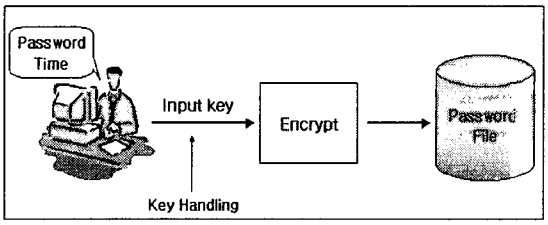

그림 2. 시간기반 패스워드 암호화 시스템 구조

3.2 개발 환경

◇ 운영체제: MS Window 2000 Advance Server
◇ 개발 툴: MS Visual Studio 6.0
◇ 코딩: MS Win32 API programming

3.3 구현 방법 및 수행 절차

1 단계: 키보드로 키 값을 입력받아 아스키코드 값으로 메시지 큐 (문자열 배열)에 저장한다.

1-1: 입력받을 수 있는 키 값은 아스키코드 0x20 ≦ key ≦ 0x7E 사이의 값이다. 키 값의 범위를 제한하는 이유는 문자이외의 키 값은 처리할 수 없도록 하기 위함이다.

1-2: 키보드로 키를 입력받을 때 키의 핸들링이 요구된다. 일반적으로 키보드에서 특정키를 오래 누르고 있을 경우, 문자가 연속해서 찍히게 되는 점을 감안해서 키의 입력 시간 동안 문자가 하나만 찍히도록 한다.

BOOL g_bKeyDown=FALSE; //키를 눌렀을 때의 상태, 로 초기값을 설정해, 키를 누르는 동안에는 g_bKeyDown=FALSE로 키 눌림이 해제될 때까지 키의 입력을 막는다. 키가 눌림이 해제되면, g_bKeyDown= TRUE가 되어 새로운 키를 입력 받을 수 있다.

2 단계: 입력받은 키 값의 입력 시간을 메시지 큐 (시간 배열)에 저장한다.

2-1: KEYDOWN 일 경우, win32 API 시간 함수인 GetTickCount()를 이용해서 키가 다운되는 시간을 구해 메시지 큐에 저장한다.

2-2: KEYUP 일 경우, 키눌림이 해제되는 시간을 GetTickCount()를 이용해서 구한 다음, 메시지 큐에 저장된 키 다운시간 값과의 차를 구한다. 키 다운과 업의 시간차를 메시지 큐에 저장한다.

3 단계: 입력 값이 더 이상 없으면 메시지 큐(시간 배열)에 저장된 각각의 키의 입력 시간의 평균을 이용해 임계치를 구한다.

3-1: 사용자가 키를 입력할 때, 키의 입력 시간에 일정한 편차를 줄 경우와 키의 입력 시간에 편차를 주지 않았을 경우로 나누어 생각해 볼 수 있다.
사용자가 키의 입력 시간의 장·단을 적절히 고려할 경우, 전체 키의 입력 시간의 평균을 이용해서 임계치를 결정할 수 있다. 그러나 사용자가 키의 입력 시간의 장·단을 구별하지 않아 입력 시간이 거의 일정한 경우 임계치를 결정하는 데 어려움이 따른다. 우리는 이 경우를 최악의 경우 (worst case)로

가정한다. 본 논문에서는 앞에서 말한 두 경우를 모두 고려해 임계치를 결정하였다. 임계치는 키의 입력시간의 평균값 ($T_a = \frac{\sum_{i=1}^{n} Ti}{N}$) 과 입력 시간의 최대 최소값의 차의 평균값 ($T_{aw} = \frac{Thw - Tlw}{2}$) 을 구해, 구해진 두 평균값의 조합 평균 (조합 평균은 시간적으로 변하는 변량을 구할 때 사용된다) 으로 정한다.

```
/* Ki = 입력키 값
   Ti = 입력 시간
   Tl = 입력 시간 중 최소값
   Th = 입력 시간 중 최대값
   Ta = 평균 입력 시간
   Taw = worst case 의 경우, 평균 입력 시간
   Tt = 임계치

(i≠h) Keystroke = {Ki, Ti}
 Keystroke Sequence Set =
{(K1,T1),(K2,T2),(K3,T3) · · · (Kn-1,Tn-1),(Kn,Tn)}
Ki ∈ { 입력키 값 (Keyboard Characters) }
   Tl-El ≦ Tl ≦ Tl+El
   Th-Eh ≦ Th ≦ Th+Eh

Ta= (Σ_{i=1}^{n} Ti)/N , Taw = (Thw - Tlw)/2

Tt = √(Ta * Taw) (Threshold: 임계치) */

1  switch EVENT of
2      case "AVERAGE" :
3        for (입력 키의 길이 k) do
4          Tsum ← Tsum + Ti ;
5          Ta ← Tsum / (입력 키의 길이) ;
         end for
6      case "Worst Average" :
7          Taw = (KeyElapsedMax
                 - KeyElapsedMin)/2.0 ;
8      case "Threshold" :
9          Tt = sqrt(KeyElapsedAverage *
               KeyWorstAverage) ;
10 end switch
```

그림 3. 시간 기반 패스워드 암호화 알고리즘

3-2: 각각의 키의 입력시간이 정해진 임계치 보다 큰 입력 값은 입력받은 키 값의 임의의 값을 더해서 새로운 키 값을 생성한다. 새롭게 생성된 키 값과 나머지 입력받은 키 값을 이용해서 패스워드로 설정한다.

4. 결론 및 향후 연구 방향

본 논문에서는 기존의 문자와 숫자로 이루어진 패스워드 입력키에 입력 시간을 적용한 시간기반 패스워드 암호화 방법을 제시하였다. 우리가 제시한 방법은 기존의 패스워드 입력 방법에 사용자의 상대적인 입력 시간 값만을 고려해서 기존의 로그인 시스템을 개선시켰다. 시간기반 패스워드 암호화 방법은 간단한 알고리즘으로 이루어져 있어 사용자의 패스워드를 필요로 하는 다양한 분야에 적용이 가능하다. 또한 높은 레벨의 보안을 요구하는 시스템에서 여러 가지 암호화 기법 (DES, Kerberos, SEED 등)과 함께 사용할 수 있다.

앞으로 본 논문에서 제시한 시간기반 패스워드 암호화 방법을 다양한 분야 (PDA, 도어락 (door rock) 등)에 적용해 성능을 평가할 예정이며, 기존의 여러 암호화 기법 알고리즘을 함께 사용하는 방법을 설계할 것이다. 또한 임계치를 이용해 시간의 장·단 외에 입력 시간의 길이를 상·중·하로 나누는 방법에 대해 연구할 예정이다.

5. 참고문헌

[1] D. McDonald and R. Atkinson, "One-Time Passwords In Everything (OPIE):Experience with Building and Using Stronger Authentication," Proceeding of the Fith USENIX UNIX Security Symposium, 1995

[2] N. Haller, "The S/KEY One-Time Password System," Proceeding of the Internet Society Symposium on Network and Distributed System Security, pp.151-158, 1994

[3] 다이나티브, http://www.dynative.com

[4] Kawase, T.; Watanabe, A.; Sasase, I, "Proposal of secure remote access using encryption", Global Telecommunications Conference, 1998. GLOBECOM 1998. The Bridge to Global Integration. IEEE , Volume: 2 , 1998