타인의 관찰에서 안전한 패스워드 시스템

박종민* · 김용훈* · 조범준*

Password System Enhancing the Security agains

Jong-Min Park* · Yong-Hun Kim* · Beom-Joon Cho*

요 약

본 논문에서는 다중 사용자가 컴퓨터 시스템을 이용하려는 사용자의 적법성을 확인하는 방법을 개선하기 위하여 타인의 관찰로부터 노출되기 쉬운 패스워드의 약점들을 보안하고, 시스템의 안전성을 높이기 위한 SPS(Secure Password System)라는 패스워드 시스템을 제안하였다. SPS는 쉬운 구현과 낮은 비용을 포함한 전통적 패스워드 시스템의 대부분의 이점들을 받아들였고, 또한 전통적 패스워드 시스템에 쉽게 이식될 수 있다. 제안한 SPS는 실험 결과 침입자의 온라인 사전적 공격과, 클라이언트에서의 패스워드 노출에 대해 높은 안전성을 보였다

ABSTRACT

In this paper, the new password system called SPS(Secure Password System) in order to enhance the security of the system as well as to improve the weakness of the password which is very easy to be disclosed by other people, improving the methods which is identifying the users' legality using the computer system in the multi-users computer. SPS is adopting several strong points such as Easy Embodiment, Low Cost, and most of the good points of the traditional password system. In addition, it makes an easy introduction from the traditional password system. Above SPS has the high stable security in the practical experiments about both the literal attack of the online intruders and the exposure of Clients' password.

Key words

sps, password, security, online, clients

Ⅰ. 서 론

안전한 통신채널 형성을 위한 인증방법에는 여러 가지가 있지만, 사람의 기억을 이용하는 방법이 가장 효율적이며, 그 방법에는 패스워드 시스템이 대표적이다. 패스워드 시스템은 잘 알려져 있고, 구현이 쉬우며, 비용이 저렴하고 유용성을 포함한 자체의 장점들 때문에 널리 사용되어 왔다.[1,2] 그러나 패스워드 시스템은 사용자가 디바이스 상에서 패스워드를 입력할 때, 디바이스에서 타인에게 패스워드를 노출시키는 치명적인 단점을 갖고 있다. 따라서 타인의 관찰과 침입에 대하여 안전한 패스워드 시스템을 개발하는 것은 대단히 중요하다. 하지만 이러한 패스워드 시스템은 아직 출현하지 않았고, 계속 연구되어지고 있다.

본 논문에서는 SPS라는 패스워드 시스템을 제안하고자 한다. SPS는 타인의 관찰과 침입자에 대한 안전성을 향상시킨 패스워드 시스템을 목표로 한다. 이러한 이유로 SPS의 안정성에 관해 우리는 온

*조선대학교 컴퓨터공학과

접수일자 : 2004. 8. 24

라인 사전적 공격[3-7]을 시도하는 침입자를 고려해보았다. SPS에서, 침입자는 패스워드의 입력과정을 관찰하여 왔었고, |P|는 패스워드 P의 길이이고, |S|는 알파벳 집합 S에서 알파벳의 개수라고 했을 때, P에서는 어느 알파벳이 S의 요소가 되는 $1 \le i \le |S|$에 대해 $i \times |P|$ 알파벳을 기억하여 왔다. 인지 심리학에서 말하는 인간의 기억의 종류인 장기기억과 단기기억 중 단기기억은 정보를 밀러의 매직 넘버인 7±2(평균 7개)의 덩어리로 나눠서 기억하게 된다는 것은 아주 잘 알려진 사실이다. 따라서 증명 $i/|S|$는 P가 4자리 숫자로 구성된다는 조건하에서 실용적인 방법으로 $2/|S|$보다는 적다는 것이다. 따라서 SPS는 온라인 사전적 공격[3-7]에 대한 전통적 패스워드 시스템과 같은 안전성을 지니고 있다.

전통적 패스워드 시스템에서, 사용자는 문자화된 타이핑에 의해 패스워드를 입력하고, SPS의 사용자는 GUI(Graphical User Interface)상에서 패스워드를 입력한다. SPS는 쉬운 구현과 저렴한 비용 등과 같은 전통적인 패스워드 시스템의 장점 대부분을 답습하고 있기 때문에 전통적 패스워드 시스템은 SPS에 이식이 가능하다.

II. 관련 연구

패스워드 시스템 보안의 위협이란 사용자의 패스워드가 불법적으로 노출되는 것을 말한다. 시스템에 불법 침입하려는 자는 아래의 네 가지 방법으로 사용자의 패스워드를 알아낼 수 있다.

첫째, 시스템의 패스워드 파일을 읽어내는 방법이 있다. 패스워드 파일은 사용자들의 패스워드와 식별자를 저장한 파일로서 만약 노출되면 시스템과 모든 사용자들의 자료는 위험에 빠지게 된다. 따라서 패스워드파일은 일반 사용자에게 접근을 제한하며 오직 보안 관리자만이 권리를 갖게 한다. 그러나 시스템의 고장이 생겨 일반 사용자들도 패스워드 파일에 접근 가능하다거나 보안 관리자가 불순한 마음을 품었을 때에는 이와 같은 패스워드 시스템은 전혀 안전하지 못하다. 보다 확실한 방법은 패스워드를 일방함수를 사용하여 그 결과를 식별자와 함께 파일에 저장하여 패스워드 파일이 노출되어도 안전을 유지하게 하는 것이다. 이 방법은 입력된 패스워드에 일방함수를 적용하여 그 결과를 저장된 것과 비교함으로써 사용자의 인증을 한다.

둘째, 사용자와 시스템 간에 패스워드를 주고받는 통신을 도청할 수 있다. 통신회선의 도청은 엿듣기만 하는 수동적 라인 태핑(passive line tapping)과 적극적 라인 태핑(active line tapping)이 있다. 만약 보안 관리자가 패스워드 시스템의 도청의 위험이 크다고 판정하면 통신되는 패스워드는 입력 장소에서 암호화되어 비교 장소까지 전달되는 방법을 취해야 한다.

셋째, 패스워드가 부주의하게 만들어져 쉽게 추측할 수 있는 경우이다. 실제로 사용자들은 자신들과 연관되거나 흔히 사용하는 단어를 패스워드로 선택하는 경우가 많으므로 패스워드의 추측이 용이한 경우가 많다. 패스워드의 추측을 어렵게 하려면 사용자가 보다 무작위로 선택하거나 자동으로 시스템에서 패스워드를 무작위로 골라주는 방법이 있다[8,9].

넷째, 사용자가 입력하는 것을 직접 보고 확인하는 방법이 있다. 이 방법은 가장 확실하게 패스워드를 알아낼 수 있는 방법이다. 하지만 이 방법은 사용자가 긴 패스워드를 사용하고, 빠르게 입력한다면 충분히 예방이 가능한 방법이다. 하지만 일반 사용자들은 7자 내외의 패스워드를 사용하고, 또한 패스워드가 가장 많이 이용되는 수많은 인터넷 사이트에서는 일반적으로 8자 내외의 패스워드를 권장하고 있다.

8자 내외의 패스워드의 경우 사용자의 입력 과정을 침입자가 옆에서 눈으로 확인한다면 충분히 암기할 수 있는 정도의 길이이다. 이는 밀러의 매직넘버에 해당되는 길이로 일반인이 충분히 한번의 관찰로 암기할 수 있다. 본 논문에서는 이러한 네 번째의 문제를 해결하기 위한 방법으로 SPS를 제안한다.

III. Secure Password System (SPS)

3.1 시스템 개관

SPS의 목적은 전통적인 패스워드 시스템에서 침입자에 대한 보안을 증진시키는 데에 있다. 이런 이유 때문에, SPS의 안전성에 관련되어서, 사용자에게 알려지지 않는 공격들을 숙고하여야 한다. 즉 우리는 온라인상의 사전적 공격과 침입자의 유형을 숙고하여야 한다.

온라인상의 사전적 공격에서, 침입자는 반복적으로 사전으로부터 패스워드를 가져오고 사용자로서 위장하기 위해 패스워드 입력을 시도한다. 만약 위장이 실패하게 되면, 침입자는 사전으로부터 이 패스워드를 지워버리고 다른 패스워드를 사용하여 재시도 한다. 실질적으로 온라인 사전적 공격 같은

형태를 보호하는 표준 방법은 패스워드가 만기되어 소멸되기 전에 사용자에게 허용되는 실패 횟수를 제한하거나, 또는 사용자가 로그인 시도를 할 수 있도록 허용되는 비율을 줄이는 것이다. 이런 이유로, 전통적인 패스워드 시스템은 온라인 사전적 공격에 대해 안전한 것으로 간주되고 있다. 정리 1은 온라인 사전적 공격에 대한 SPS의 안정성이 전통적 패스워드 시스템과 같다는 것을 보여준다.

정리 1: S가 알파벳의 집합이고, 이 집합 S를 x1, x2,…, xn로 표현하고 이 중에서 랜덤하게 선택된 알파벳 xi($1 \le i \le n$)를 패스워드라고 할 때, 침입자는 매번 1/ | S | n의 확률로 패스워드를 입력하게 된다.

보드에서 전개된 알파벳의 개수는 패스워드가 침입자에게 노출되었다는 가능성과 관계가 있다.

정리 2: S가 보드에서 전개된 알파벳들의 집합이 되게 하자. SPS에서 침입자는 i×n개의 알파벳을 기억할 수 있다는 조건하에 i/ | S | 의 가능성을 갖는 패스워드를 배울 수 있다. 이 때 i는 $1 \le i \le$ | S | 이고, n은 패스워드의 길이이다.

정리 1과 정리 2는 모두는 이론적인 증거를 요구하지 않을 정도로 명확하지만, 전통적인 패스워드 시스템이 온라인 사전적 공격에 대해 안전하다고 해도 침입자에 대한 안정성을 높이기 위해서는 이 법칙들이 중요하다.

SPS의 실제 적용에서, 사용자가 패스워드에 알파벳을 입력할 때마다, 침입자가 보드 상에 전개되는 모든 | S | 의 알파벳을 기억한다는 것은 비실용적이다. 예를 들자면, 십진 숫자들로 구성된 패스워드를 요구하는 자동 금전출납기에서, 사용자가 십진 숫자를 입력할 때마다 침입자가 열자리 숫자를 기억한다는 것은 불가능한 일일 것이다. 인지심리학에서, 인간은 밀러의 매직 넘버인 7±2의 덩어리로 나눠서 기억을 재생시켜야 한다는 것은 아주 잘 알려진 사실이다. 이런 이유 때문에, 실제 적용에서 i/ | S | 가 선택될 확률은 패스워드가 네 자리 숫자로 구성된 조건 하에서 2/ | S | 보다 적은 것이다. SPS가 정의되지 못한다면, 그때 침입자는 정리 2의 확률보다 높은 확률을 갖고 있는 패스워드를 알게 될 수 있다.

3.2 시스템 제안

SPS는 S가 알파벳의 집합인 | S | 셀들로 구성된 GUI 상에 보드를 전개하고, 보드는 중복 없이 랜덤하게 선택된 S의 모든 알파벳을 전개한다. SPS가 처음으로 보드 상에 | S | 의 알파벳들을 전개 시킬 때, 사용자는 보드 상에서 패스워드를 입력시킬 셀을 결정한다. 다음에서 S가 십진법 숫자 집합일 경우에 사용자가 SPS에 패스워드를 입력하는 방법을 정의하고자 한다.

정의: S가 십진수의 집합이고, 패스워드 xi가 이 집합 x1, x2,…., xn들에서 $xi \in S(1 \le i \le n)$가 되도록 하고, 사용자는 패스워드를 입력할 셀의 위치 j를 결정한다. SPS는 (1)과 (2)를 n번 실행하고 다음으로 (3)과 (4)를 한번 실행하는 패스워드 시스템이다.

(1) SPS는 중복 없이 무작위로 선택된 순서인 보드에서 $k(1 \le k \le n)$번째 십진수 집합 | S | 를 전개한다.

(2) y가 보드의 j번째 숫자가 되도록 한다. 만약 $y<xk$가 된다면, 사용자는 상측 화살 키를 xk-y번 누르게 될 것이고, 만약 $y \ge xk$이면 사용자는 상측 화살 키를 10+xk-y mod 10번 누르게 될 것이다. 그런 후에 사용자는 엔터 키를 누르게 된다. 보드 상에서 나타내지는 모든 값들은 사용자가 상측 화살 키를 한 번 누를 때마다 동시에 1씩 증가된다. 그리고 값이 9인 셀은 사용자가 상측 화살 키를 한 번 누를 때 0으로 바뀔 것이다.

(3) SPS는 중복 없이 무작위로 선택된 순서인 | S | 셀들에서 (n+1)번째 | S | 인 십진수들을 전개한다.

(4) 사용자는 j번째 셀이 특별한 기호를 포함할 때까지 상측 화살 키를 누른다. 그 다음 사용자는 입력의 종료를 알리기 위해 엔터 키를 누른다. 이 과정에서 사용자가 상측 화살 키를 한 번 누르게 될 때, 값이 9인 셀은 0으로 바뀌고, 값이 0인 셀은 특별한 기호(문자)로 바뀐다.

예 : S를 십진수의 집합이 되게 하고, x1x2=69가 패스워드가 되고, @를 특별한 기호로 사용한다. 그리고 사용자는 패스워드를 입력할 셀의 위치를 6번째로 결정한다. 그런 후에, 사용자와 SPS는 (1)과 (2)를 두 번 실행하고, (3)과 (4)을 다음과 같이 한 번 실행한다.

(1) SPS가 3,6,1,7,0,5,9,8,2,4(그림1) 순서로 십진 숫자들을 전개

3	6	1	7	0	5	9	8	2	4

그림 1. 첫 번째 십진 숫자들의 전개

(2) 6번째 셀에서 보여준 숫자는 5이고 6-5=1이다. 그러므로 사용자가 보드 상에서(그림2)

모든 값을 1 올리기 위해 상측 화살 키를 누른다. 그런 다음 사용자가 엔터 키를 누르면 각 셀의 모든 값이 1씩 증가되고, 그 중 값이 0인 셀은 1이 증가되면 특별한 기호 '@'로 바뀌고, 6번째 셀에 패스워드 중 첫 번째인 '6' 이 삽입된다.

4	7	2	8	@	6	0	9	3	5

그림 2. 6번째 셀에 6이 삽입된 후

(1) SPS가6,4,5,0,2,7,9,8,1,3(그림3)의 순서로 십진 숫자를 전개

6	4	5	0	2	7	9	8	1	3

그림 3. 두 번째 십진 숫자들의 전개

(2) 6번째 셀에서 보여준 숫자는 이제 7이고, 9-7=2이 된다. 따라서 사용자는 상측 화살 키를 두 번 누른다. 그런 후에 사용자는 엔터 키를 누른다(그림4).

8	6	7	2	4	9	1	0	3	5

그림 4. 6번째 셀에 9가 삽입된 후

(3) SPS가7,1,3,0,2,6,5,9,4,8(그림5) 순으로 십진 숫자들을 전개

7	1	3	0	2	6	5	9	4	8

그림 5. 세 번째 십진 숫자들의 전개

(4) 6번째 셀에서 보여준 숫자는 6이 됩니다. 따라서 사용자는 6번째 셀에 @을 입력하기 위해 상측 화살 키를 다섯 번을 누른다. 그런 후에 사용자는 입력의 끝을 알리기 위해 엔터 키를 누른다.

1	6	8	4	7	@	0	3	9	2

그림 6. @가 삽입된 후

위에서 정의된 SPS에서, 보드 상에 전개된 숫자는 쉽게 조정될 수 있다. 따라서 우리는 S를 위와 같이 십진 숫자들의 집합으로 제한하지 않는다.

IV. 실험 및 고찰

SPS는384Mb RAM, 700MHz Pentium III급 컴퓨터상에 OS로 윈도우 2000 서버를 운영하면서 C++언어로 구현되었다. 패스워드의 입력시간을 얻기 위해 30명의 테스터들이 50회씩 패스워드를 입력하여 평균 5.10초 걸렸다. 반면에 전통적인 패스워드 시스템은 2.54초 걸렸다. 표 1의 데이터는 각 테스터들이 50회씩 패스워드를 입력하는데 걸린 시간의 평균값을 내림차순으로 정렬한 결과이다. 이 데이터에 대한 연속 확률 분포를 구한 결과 그림 7과 같이 정규 분포에 유사한 결과를 볼 수 있었다.

표 1. 30명 각 개인의 평균 입력시간

4.13	4.22	4.41	4.47	4.51	4.52	4.59	4.62	4.87	4.92
4.99	5	5.01	5.06	5.06	5.13	5.14	5.16	5.17	5.2
5.21	5.24	5.27	5.28	5.61	5.68	5.72	6.1	6.21	6.52

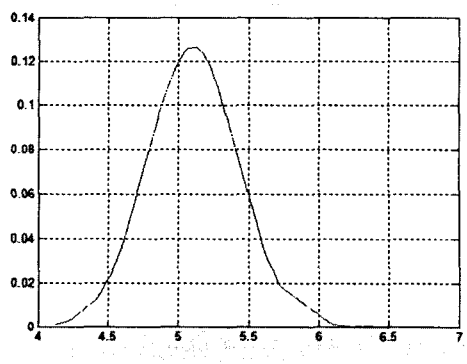

그림 7. 실험결과의 연속 확률 분포 곡선

입력 시간을 개선하기 위해 SPS가 정의 (2)에서 자동으로 셀 안에서 모든 값들을 증가시키는 방법을 고려하였고, 사용자는 엔터 키를 쳐서 알파벳이 셀에서 전개되도록 한다. 이 방법은 시간 간격이 0.25초로 설정 될 때, 평균 5.83초에서 0.73초를 줄일 수가 있다. 실험 결과는 SPS가 패스워드 입력 시간이 증가되지만 침입자에 대한 안전성을 높일 수 있다는 것을 보여준다.

SPS가 clear-text 내에 패스워드를 저장하는 시스템에 설치된다면, SPS가 알파벳을 생성해서 패스워드의 입력 시간은 현저하게 짧아지게 된다. 왜

냐하면 SPS가 $1 \leq \delta \leq |S|$ 와 $2 \leq k \leq n+1$ 동안 정의 (2)에서 $x_k - y \leq \delta$인 알파벳을 선택할 수 있기 때문이다. 그러나 정의 (1)에서 확률은 $1/\delta^n$로 증가될 것이다. 따라서 시스템 사자는 안정성 수위의 고려하여서 δ을 설정해야만 한다.

V. 결 론

패스워드의 사용은 컴퓨터 보안에 있어서 일부에 지나지 않는다. 하지만 대부분의 컴퓨터시스템이 패스워드를 이용해서 사용자를 인증하고 자료에 대한 접근을 제어하고 있으므로 그에 따른 패스워드의 사용에 대한 보안은 아주 중요한 문제라 할 수 있다. 패스워드는 컴퓨터 네트워크나 시분할 원격접근 컴퓨터 시스템에서 주로 사용하므로 시스템에 침투하고자 하는 자는 컴퓨터와 멀리 떨어진 곳에서 직접적인 위협을 느끼지 않고도 침투 시도가 가능하다는 특징이 있다. 실제로 해커에 의한 시스템 침투 사례는 여러 가지가 알려져 있다.

정보화 시대로 가고 있는 현 시점에서 그와 같은 시스템의 보안위협은 커다란 자산의 손실 또는 사회적 혼란을 초래할 수 있다. 본 논문에서는 현재 가장 널리 사용되는 패스워드 시스템을 기반으로 하는 SPS를 제안하였다. SPS는 온라인 사전적 공격에 대한 전통적 패스워드 시스템의 안전성을 보전하면서 i/S의 확률로 클라이언트에서 패스워드의 노출을 막는다.

SPS는 쉬운 구현과 저렴한 가격을 포함하는 전통적인 패스워드 시스템의 대부분의 장점들을 이어 받았다. 그리고 SPS는 전통적인 패스워드 시스템에 쉽게 이전이 가능하다. 패스워드가 네 자리 숫자로 구성된 경우, 패스워드의 입력시간은 전통적인 패스워드 시스템의 두 배이지만 안정성은 증가되는 것을 알 수 있었다. 향후 패스워드 입력시간 단축에 관한 연구가 필요할 것이다.

참고문헌

[1] D. C. Feldmeier and P. R. Karn, "UNIX Password Security-ten years later," Advances in Cryptology-CRYPTO '89,LNCS 435, pp.44-63, 1990.

[2] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," Proceedings of the 2nd USENIX UNIX Security Workshop, pp. 5-14, 1990.

[3] G. Denker and J. Millen, "CAPSL Integrated Protocol Environment", In DARPA Information Survivability Conference (DISCEX 2000), pp207-221, IEEE Computer Society, 2000.

[4] L. Gong, "A Security Risk of Depending on Synchronized Clocks", ACM Operating Systems Review, Vol.26, No.1, January, pp.49-53, 1992.

[5] Li Gong. Variations on the Themes of Message Freshness and Replay or, the Difficulty of Devising Formal Methods to Analyze Cryptographic Protocols. In Proceedings of the Computer Security Foundations Workshop VI, pages 131--136. IEEE Computer Society Press, LosAlamitos, California, 1993.

[6] V. Boyko, P. MacKenzie, and S.Patel. Provably Secure Password Authenticated Key Exchange Using Diffie Hellman. Eurocrypt 2000.

[7] D. Jablon. Strong password-only authenticated key exchange. Computer Communication Review, 26(5):5--26, October 1996

[8] Neil Haller. The s/key(tm) one-time password system. In Proceedings of the 1994 Symposium on Network and Distributed System Security, pages 151--157, February 1994

[9] Neil Haller. The s/key(tm) one-time password system. Symposium on Network and Distributed System Security, pages 151--157, February 1994.

저자소개

박종민(Jong-Min Park)

1988년 조선대학교 졸업(공학석사)
2004년 조선대학교 박사과정 수료
※관심분야 : 생체인식, 패턴인식, 인공지능, 정보보호 및 보안

김용훈(Yong-Hun Kim)

2000년 전남대학교 물리교육과 석사
2001년 조선대학교 컴퓨터공학과 박사과정
※관심분야 : 패턴인식, 정보보안 등

조범준(Beom-Joon Cho)

1980년 조선대학교 전기공학과 (공학사)
1988년 한양대학교 전기공학과 (공학박사)
2004년 한국과학기술원 전자전산학과 전산학전공(공학박사)
1980년~현재 조선대학교 전자정보공과대학 컴퓨터공학부교수
1993년~1997년 조선대학교 전자계산소장
2002년~현재 한국멀티미디어학회 부회장
2000년~2002년 조선대학교 전자정보공과대학 학장
※관심분야 : 인공지능, 패턴인식, 뉴로컴퓨터