최종 승인시간을 이용하는 개선된 패스워드 기법

(The Improved-Scheme of Password using Final Approval Time)

지 선 수*, 이 희 춘**
(Seon-Su Ji and Hee-Choon Lee)

요 약 인터넷의 개방성과 정보공유 및 교환의 용이성으로 인해 해킹사건은 발생 빈도수가 높아지고 있으며, 해킹유형 또한 고도화·복잡화되고 있다. 그리고 그 피해규모와 심각성은 측정이 불가능하다. 패스워드 보안은 인터넷에서 자신과 정보를 보호하기 위한 필수적인 도구이며, 이것은 아무리 강조해도 지나치지 않는다. 패스워드는 암호화할 경우 7글자 이상으로 구성하면 충분하다. 본 논문에서는 가상키보드들 통해 패스워드를 입력하며, 아이디의 일부정보와 최종 접근 승인시간을 기반으로 하는 개선된 1회용 패스워드 변경기법을 적용하는 확장 알고리즘을 제안한다.

핵심주제어 : MD5, 암호화, 일방향 함수, 일회용 패스워드, 정보엔트로피, 최종 승인시간

Abstract The internet is currently becoming popularized and generalized in our daily life. Recently, a lot of hacking tools have appeared on the internet. And damage size and seriousness the measurement is impossible. The password security protects oneself and information is the tool which is essential for from the internet, if this emphasizes no matter how, does not go to extremes. If applies a encryption, a 7 character password is sufficient, so long as attackers don't pick easily guessed values. In this paper, entering password using the virtual keyboard, I propose a new and improved one time password algorithm using information a part of ID and final approval time.

Key Words : Encryption, Final Approval Time, Information Entropy, MD5, One Time Password, One way Function

1. 서 론

현재 그리고 미래의 정보와 지식이 중심이 되는 정보사회에서 인터넷 정보의 신뢰성에 대한 저평가에도 불구하고 인터넷 정보의 파급효과는 예측하기 어려울 정도로 매우 크다. 생활수준을 한 차원 끌어올린 인터넷이 우리의 생활을 지배하기 시작하면서 정보의 유통방식을 획기적으로 바꾸었다. 그러나 컴퓨터에 기록된 다른 사람의 개인 정보를 불법적으로 탈취하여 부정하게 이용하려는 시도가 끊임없이 진행되고 있다. 예를 들어 해킹, 컴퓨터 바이러스 유포, 사생활 침해, 집중력쇠퇴, 사실(fact)의 실종 등의 심각한 사회적 문제가 나타난다. 즉 인터넷은 사회적, 문화적, 윤리적 역기능과 순기능이 동시에 존재함에도 불구하고, 현대인의 생활 중심에 자리매김하면서 무조건적인 인터넷 의존 형으로 변화하고 있다[1][2]. 인터넷의 개방성과 정보공유 및 교환의 용이성으로 인해 인터넷에서의 해킹사건은 발생 빈도수가 기하급수적으로 높아진다.

* 강릉원주대학교 정보기술공학과, 제1저자
** 상지대학교 컴퓨터데이터정보학과, 교신저자

해킹유형 또한 고도화하고 그로 인한 피해의 심각성은 하루가 다르게 변화하며, 진화하고 있다. 개인정보의 침해사건 중 96% 이상이 해킹에 의해 발생되는 오늘날에 보안기법은 강화되지만, 사용하는 사람의 보안의식은 매우 낮고 소극적이다.

정보에 접근하고 이를 활용할 수 있는 능력이 중요시 되는 현시점에서 인터넷 서비스의 확대에 따라 사용자는 특정 사이트의 사용 권한을 획득하기 위해서 아이디(ID)와 패스워드 등의 사용자 정보를 해당 사이트에 제공한다. 사용자들이 선택하여 이용하는 패스워드는 '랜덤성(randomness)'이 매우 낮다. 따라서 인터넷에 접근할 때 보안을 생활화하기 위해 ①정기적인 패스워드 변경, ②각 사이트마다 다른 아이디와 패스워드의 사용, ③웹브라우저의 방문기록 및 캐시파일 삭제 등을 권장하고 있다. 그럼에도 불구하고 매일 수만 개의 악성코드가 생성되고 있으며, 공격자들이 만들어내는 신종 악성코드 수와 보안 전문가들이 처리하는 '해킹 시그니처(hacking signature)' 수의 격차는 기하급수적으로 커지고 있다는 것이 오늘날의 현실이다[3][4]. 일반적으로 아무리 잘 갖추어진 보안대책이라도 허점이 있기 때문에 무작위 강제 공격, 중간자 공격, 사전 공격 등을 이용하는 집요한 공격자에 의해 결국 뚫리기 마련이다. 공격이 시작되거나 종료된 후 뚫린 허점을 막기 위한 해결책을 찾아가는 사후약방문식의 보안기법을 개발하는 것이 현재 보안정책의 악순환 과정이다. 현재와 같이 정보보호에 대한 준비와 대응책을 소홀히 한다면 가까운 미래의 재앙이 될 수도 있다.

1960년대 패스워드 기법이 도입된 이후에 공격자로부터 비밀을 유지하고, 이용자에게 기억하기 용이하며, 강력하고, 효율적인 패스워드에 대한 개선책이 필요하게 되었다. 개인정보보호를 위한 보안기법을 강화하기 위해 사용된 '1회용 패스워드(OTP : one time password)'가 그 중의 하나이다. 초기에는 은행이나 게임업체 등에서 제한적으로 도입하여 사용하였지만 최근에는 아이디와 패스워드 유출을 방지하기 위한 강력한 정보보호 차원에서 활성화되고 있다[4].

현실적으로 인터넷을 사용하면서 패스워드를 정기적으로 바꾸는 것은 매우 번거로운 일이다. 또한 패스워드의 분실과 탈취에 대한 책임과 의무를 개별 사용자에게만 모두 지울 수 없다. 기존의 공격 형태를 수집하고, 분석하여 대응기법을 만들고, 엔진에 포함시키는 일련의 작업들만으로는 모든 사이버 공격에 대응할 수 없게 되었다. 따라서 사용자의 편리성이 보장되면서 공격자에게 혼돈과 확산을 증가시키며, 해독의 어려움과 시간을 가중시킬 수 있는 개선되고 확장되는 패스워드 기법은 끊임없이 요구된다. 즉 최종 접근 승인시간과 salt 시스템을 기반으로 하는 안전하고, 강력한 패스워드를 구현하는 개선된 방법과 공격에 적극적으로 대응하고, 예방하는 기술이 필요하다.

본 논문에서는 효율적이고 강력한 패스워드를 구현하며, 공격이 진행되기 전에 적극적으로 예방과 방어하는 기법을 이용하는 개선된 방법을 제시한다. 논문의 구성은 다음과 같다. 2장에서 암호화되고 개선된 패스워드 관련 연구에 대해 조사한다. 3장에서는 최종 승인시간을 기반으로 하는 강력하고, 정보엔트로피(information entropy)를 증가시키며, 가변적인 1회용 패스워드를 구현하며, 예방적 · 방어적 차원에서 적극적인 보안을 구현하는 개선된 방법을 제안한다. 적용결과를 가지고, 4장에서 결론을 제시한다.

2. 관련연구

인터넷 이용자와 운용자의 대부분은 개인정보와 관련되거나 기억하기 쉬운 7글자 내외의 단어를 조합하여 구성하며, 보안을 위해 해시 알고리즘을 적용한다. 사용자의 개인정보가 타인에게 유출 및 도용될 수 있다는 것을 인지하면서도 안전성보다는 편리성이 우선시되는 것이 현재 개인정보보호 환경의 현실이다.

전체 기업의 63.6%가 정보보호에 대한 비용 지출이 전혀 없으며, 인터넷 이용자의 절반가량은 사이버 보안에 무방비 상태이며, 이용자 중 46%가 한 달에 한 번도 보안패치를 업데이트하지 않고 있는 것으로 지적되었다. 또한 인터넷 사용자의 20%는 패스워드를 공유하여 사용하며, 사용자의 60%는 문자의 제한된 범위, 예를 들어 소문자 혹은 숫자만으로 구성된 패스워드를 사용하였다. 사용자의 65.3%는 6~8 글자를 바탕으로 패스워드를 구성하여 사용한다. 특히 키보드 입력정보 중 인증정보 등을 훔칠 수 있는 키 로깅

(key logging) 관련 위협이 기밀정보에 대한 위협 중 76%를 차지한다[3][5].

일반적으로 인터넷에서 웹사이트에 접근하기 위해 알파벳, 숫자, 특수문자 등 67개 내외의 문자를 가지고 패스워드를 조합하여 사용할 수 있다. 패스워드에 대한 제약이 강하고 많을수록 사용자는 기억의 한계 때문에 ①패스워드를 어디엔가 기록하여 보관하려하며, ②과거의 패스워드를 재사용하려하며, ③패스워드 변경주기나 위험성을 망각하며, ④기억하기 쉬운 단순한 패스워드를 사용한다. 효과적인 패스워드 관리는 사용자의 행위와 기술을 모두 포함시키는 범위에서 비밀스럽고, 편리하게 이용할 수 있도록 운영되어야 함을 제시하였다. 문자조합에 따른 패스워드의 가능한 수는 <표 1>과 같이 표시할 수 있다[6][7].

<표 1> 패스워드 길이에 따른 문자와 숫자 조합 수

문자집합	5	6	7	8	9	10
0-9	$1.00e^5$	$1.00e^6$	$1.00e^7$	$1.00e^8$	$1.00e^9$	$1.00e^{10}$
a-z	$1.19e^7$	$3.09e^8$	$8.03e^9$	$2.09e^{11}$	$5.43e^{12}$	$1.41e^{14}$
a-z, 0-9	$6.05e^7$	$2.18e^9$	$7.84e^{10}$	$2.82e^{12}$	$1.02e^{14}$	$3.66e^{15}$
a-z, A-Z	$3.80e^8$	$1.98e^{10}$	$1.03e^{12}$	$5.35e^{13}$	$2.78e^{15}$	$1.45e^{17}$
a-z, 0-9, spec(6)	$1.31e^8$	$5.49e^9$	$2.31e^{11}$	$9.68e^{12}$	$4.07e^{14}$	$1.71e^{16}$
a-z, 0-9, punct(3)	$9.02e^7$	$3.52e^9$	$1.37e^{11}$	$5.35e^{12}$	$2.09e^{14}$	$8.14e^{15}$
a-z, 0-9, A-Z	$9.16e^8$	$5.68e^{10}$	$3.52e^{12}$	$2.18e^{14}$	$1.35e^{16}$	$8.39e^{17}$

경험적과 심리적으로 볼 때 일반 웹사이트 접근자는 최대 100회의 패스워드를 추측·시도하여 실패한다면 스스로 포기하는 경향이 있지만, 컴퓨터를 이용한 자동화된 프로그램은 초당 백만 개 이상의 패스워드를 추측할 수 있다[7].

예를 들어 <표 1>에서와 같이 공격자가 평문으로 된 패스워드를 단순하게 추측하는데 90일을 기준으로 할 경우 $90\times24\times60\times60\times100\times1{,}000{,}000=7.776e^{14}$으로 계산되므로 음영으로 된 곳의 사선으로 표시된 부분은 패스워드 구성요소로 충분하다고 판단되는 부분이다. 이때 공격자의 성공확률이 1%라고 가정한다. 또한 공격자가 암호화된 패스워드를 추측하는데 같은 방법으로 90일을 기준으로 할 때 $90\times24\times60\times60\times100\times100=7.776e^{10}$으로 계산되므로 음영으로 된 부분은 패스워드 구성요소로 충분하다고 판단되는 부분이다. 그러므로 논리적으로 패스워드를 암호화할 경우 7글자 이상의 알파벳, 숫자, 특수문자(6) 조합으로 패스워드를 구성하여도 충분하다. 이것은 <표 1>에서 5번째 행에 표시되어 있다. 패스워드는 저장매체를 이용하는 것 보다 오직 이용자의 두뇌에 기억되어 활용되어야한다는 기억한계측면에서 볼 때 이것은 적절한 수이다.

패스워드는 어떤 프로그램이나 암호를 사용하여도 메모리에 흔적이 남기 때문에 결국에는 전부 혹은 일부분의 정보가 복원될 가능성이 매우 높다. 최근에 로그인을 안전하게 하기위해 강력한 패스워드를 가지고 salt 시스템과 해시함수를 활용하는 패스워드에이전트가 제안되었다. 이것은 패스워드 탈취에 대한 강력한 보호를 제공하며, 어깨너머 훔쳐보기(shoulder surfing)의 위험을 감소시킬 수 있음을 보였다[8]. 이러한 취약점을 보완하기 위해 패스워드는 입력하는 실시간에 따라 변하는 가상키보드(VK : virtual keyboard)를 이용하여 입력하는 것이 효과적일 수 있다는 것을 보였다[5][9].

많은 대안적인 연구에도 불구하고, 패스워드의 약한 및 강한정책, 사용자의 편의성 및 불편성, 관리의 양면성 문제로 개인정보보호의 중요성에 비해 보안 관리의 허점이 크게 개선되지 못하였다. 예를 들어 약한 패스워드 구성은 전사적 및 사전공격에 매우 취약하다. 강한 패스워드는 공격자로부터는 강하게 보호될 수 있지만, 키 로깅 및 어깨너머 훔쳐보기 등으로부터 보호조치를 해야 한다. 그러므로 입력된 패스워드는 salt 시스템과 암호화 과정을 거쳐 개선되고, 공격자에게만 부담을 가중시킬 수 있는 효율적인 기법의 연구가 필요하다.

3. 변경, 확장되는 패스워드 설계

Salt 시스템, 해시 알고리즘을 기본으로 하는 개선된 1회용 패스워드 기법을 적용한다. 이때 Chang-Yang-Hwang의 알고리즘을 참조한다[8][10].

3.1 제안된 방법

실시간으로 변하는 가상키보드를 통해 패스워드를 입력한다. 아이디의 일부정보와 최종 접근 승인시간을 기반으로 하는 개선된 1회용 패스워드 변경기법을 적용하는 확장 알고리즘을 제안한다.

1단계 : Alice가 웹 사이트에 회원으로 가입할 때 가입 시점의 최초시간 혹은 최종 접근 승인시간(st_A)과 p를 이용하여 확률수(R_A)를 구한다. Alice가 입력한 최초 아이디(id_A)와 패스워드(pw_A)를 바탕으로 st_A에 따라 Alice의 id_A중 일부분(m)을 임의로 선택하여 salt 시스템 등을 응용한 변형된 1회용 패스워드(pw_A')를 계산한다. pw_A', id_A, st_A를 서버에 저장한다. 이때 id_A의 수가 k(given)개 미만일 경우 임시로 지정한 문자를 채워준다. 합법적인 사용자의 최종 접근 승인시간을 참고한다.

$$R_A = (st_A \bmod p(given), random)$$
$$st_A | R_A \rightarrow st_A'$$
$$\text{if}(id_A > k) | R_A \rightarrow id_A'$$
$$else\ (\{id_A + char(given)\} | R_A) \rightarrow id_A'$$
$$h(\{id_A' + pw_A + st_A'\} | st_A) \rightarrow pw_A'$$
$$Save\{pw_A' \mid id_A \leftarrow id_A', st_A \leftarrow st_A'\}$$
$$\text{and } display\ time(st_A)$$

여기에서 k와 p는 사전에 주어지는 임의의 상수이다.

2단계 : Bob은 웹사이트에 접근하기 위해 아이디(id_B)와 가상키보드를 이용하여 패스워드 pw_B를 각각 입력한다.

3단계 : Bob의 $id_{B(\rightarrow A)}$에 대응되는 $st_{B(\rightarrow A)}$를 참조하여 다음을 계산한다.

$$R_B = (st_B \bmod p(given), random)$$
$$st_B | R_B \rightarrow st_B'$$
$$\text{if}(id_B > k) | R_B \rightarrow id_B'$$
$$else\ (\{id_B + char(given)\} | R_B) \rightarrow id_B'$$
$$h(\{id_B' + pw_B + st_B'\} | st_{B(\rightarrow A)}) \rightarrow pw_B'$$

4단계 : 3단계에서 계산한 pw_B'와 서버에 저장된 pw_A'가 일치하는지를 검증한다.

$$Verify\ \ pw_B' \oplus pw_A'$$
$$exchange\ \ st_{(Now)} \rightarrow st_A$$
$$go\ to\ [first\ step]$$

pw_B'와 pw_A'가 일치할 경우 Alice와 Bob은 동일인으로 판단한다. 이때 합법적인 사용자의 검증이 완료된 접근 승인시간($st_{(Now)}$)을 바로 전 접근 승인시간(st_A)으로 변경한다. 1단계로 이동한다. 여기에서 $\oplus$는 XOR 함수이다.

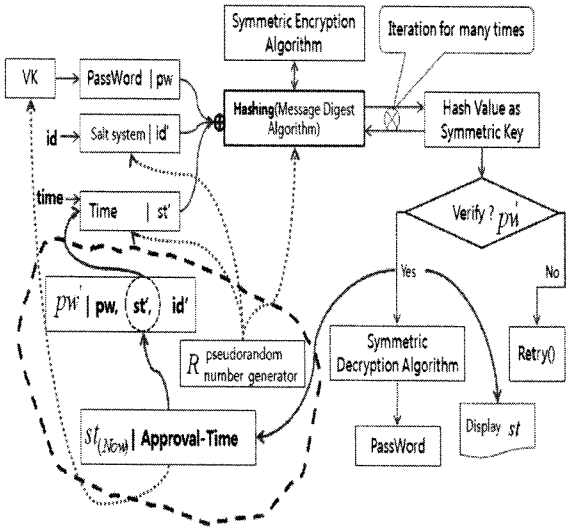
$h()$는 일방향 해시함수이며, 적용되는 패스워드 확장 알고리즘은 다음과 같다.

$$X_o = f(pw_{(org)} + salt_{(value)})$$
$$For\ i = 1\ \ to\ \ 2^t(iteration)$$
$$X_i = f(X_{i-1})$$
$$pw' = h_{MD5}(X_{2^t} + PRF(t_{(Approval-Time)}))$$

여기에서 pw'은 변형된 패스워드, $pw_{(org)}$는 사용자가 입력한 최초의 패스워드, $salt_{(value)}$는 id_A로부터 얻은 정보의 일부분이다. $f()$는 일방향 수학함수이며, $t_{(Approval-Time)}$는 최초가입 혹은 접근승인이 될 때의 시간을 나타내는 변수이다. 또한 $PRF()$는 의사난수함수(pseudo random function)를 의미한다.

<그림 1>에서 제안된 알고리즘의 구현과정을 표현하였다. 그림에서 점선으로 표시된 영역은 논문에서 제안한 부분으로서 합법적인 사용자의 최종 접근 승인시간에 따라 패스워드가 변경되고, 확장된다. 즉 최종 접근 승인시간(st_A)에 따른 가변적인 1회용 패스워드가 만들어 진다. {입력된 아이디 일부 정보(salt), 패스워드, 합법적인 사용자가 마지막으로 접근승인이

된 시간} 등이 조합된 정보를 기반으로 해시 함수 등을 이용하여 확장된 알고리즘을 적용하는 것을 보여준다. 사용자가 비록 긴 패스워드를 이용하지 않더라도 혼돈과 확산을 증가시킬 수 있으며, 이것은 공격자로 하여금 효과적인 방법을 찾기가 더욱 어렵게 할 것이다.



<그림 1> VK, st, salt, 해시 함수 등을 적용한 개선된 1회용 패스워드 구현도

3.2 적용

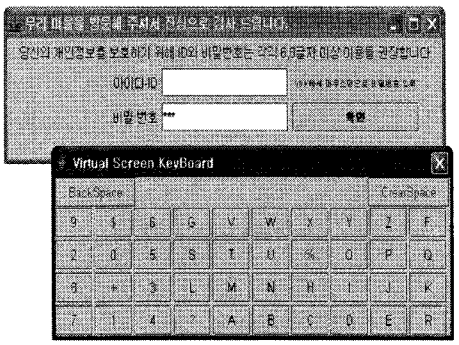
현재의 시간($st_{(Now)}$) 정보를 9자리로 구성하였으며, m은 2, p는 99로, k는 7로 설정하였다. 최종 접근 승인 시간에서 두 자리, 입력된 아이디에서 두 자리, 패스워드 정보를 기반으로 한다. 즉 $Permutation\{id'+pw+st'\}$을 가지고 승인시간을 기반으로 하는 난수에 따라 그 위치 조합을 다르게 한 후 해시 알고리즘을 적용하였다. 그리고 알고리즘을 구현하는 과정은 J2SE를 이용하였다.

일반적으로 아이디를 입력한 후 패스워드를 입력하기 위해 가상키보드로 입력포인터가 이동되는 순간 아이디 입력창을 비워두도록 한다. 또한 패스워드가 들어갈 텍스트 창은 키보드 입력이 되지 않도록 비활성화 시킨다. <표 2>에서와 같이 동일한 패스워드를 입력하더라도 최종 승인시간과 조합방식에 따라 결과가 다른 1회용 패스워드가 구성된다. 즉 입력된 패스워드(□)에 합법적인 마지막 사용자가 접근승인이 되었을 때의 최종시간의 일부정보(▥)와 아이디의 부분정보(目)의 순서조합이 다르게 추가되어 확장된 패스워드를 이용한다. 따라서 공격자로 하여금 패스워드 추측의 부담을 가중시킬 수 있다.

<표 2> 정보의 순서조합에 따라 변형되고, 확장된 패스워드 형태

입력된 패스워드	표현된 패스워드(pw')	
hong123	目+□+▥	S땝ðPv<? 숂?? 늧
	目+▥+□	D즐?><M_T? 돜/
	□+目+▥	?#O,_┼ *a쥜
	□+▥+目	┘&cJ慴e?[朴稙x†
	▥+□+目	?햡く じ?P?? 즐
	▥+目+□	L田<??¶漢>?┘K

<그림 2>는 구현된 프로그램 결과화면이다.



<그림 2> 프로그램 구현 결과화면

<표 3>은 <표 1>의 5번째 항을 적용할 경우 패스워드 길이에 따라 기존방법[10]과 제안된 방법을 적용할 때의 정보엔트로피를 보여준다.

<표 3> 패스워드 길이에 따른 정보엔트로피

문자집합	5	6	7	8	9
기존방법	0.64	0.77	0.90	1.03	1.16
제안방법	0.90	1.04	1.17	1.28	1.41

제안된 방법을 이용할 경우 $0.13m$배 만큼의 정보 엔트로피가 증가하므로 공격자에게 불확실성의 부담을 증가시킬 수 있다.

3.3 개선효과

입력되는 모든 정보가 암호화되며, 특히 실시간으로 키 배치가 변하는 가상키보드, salt 시스템을 적용함으로서 공격자에게 해독의 어려움과 시간을 가중시킬 수 있다. 또한 합법적인 사용자의 접근 승인시간에 따라 확장되는 1회용 패스워드를 관리함으로서 우연적 요인(chance cause)과 이상적요인(assignable cause)에 의한 정보유출 가능성을 최대한 억제할 수 있다.

[심리적 효과] 아이디의 일부정보와 최종 접근 승인시간을 기반으로 확장된 1회용 패스워드 암호화 기법을 이용함으로서 사용자에게 패스워드 관리의 신뢰와 심리적 안정감을 줄 수 있다.

[사전공격에 대비] salt 개념과 최종 접근 승인시간을 이용하여 변경되고, 확장된 1회용 패스워드를 적용한다. <표 1>의 5행을 참고로 하고, $(m=2)$, x개의 문자를 사용하여 암호화하며, 아이디와 최종 접근 승인시간 일부정보가 각각 추가되는 제안된 기법을 적용할 경우 $(m+0.66)+x$개의 패스워드를 사용할 때와 동일한 효과가 있다. 즉 패스워드에 m글자로 이루어진 2쌍의 정보가 마지막 승인시간에 따라 다르게 추가되어 순서·조합되므로 사용자에게는 기억의 부담을 주지 않으면서, 공격자에게는 무거운 부담을 줄 수 있다.

[키 로깅 위협대비] 실시간에 따라 키보드 배치가 변화되며, 입력창을 비워둠으로서 훔쳐보기를 통하여 타인에게 쉽게 노출될 수 있는 기회를 최소로 축소할 수 있다. 또한 네트워크 위변조에 대한 대응에 효과적일 수 있다.

4. 결 론

보안은 누가 지켜주기보다 사용자 스스로 지키기 위해 최선의 노력을 할 때 자신의 정보를 지킬 수 있다. 즉 정당한 사용자가 웹사이트를 합법적으로 접근하여 승인된 시간을 사후 관리함으로서 패스워드 관리의 보안성을 높일 수 있다.

본 논문에서 제안된 방법 즉, 마지막 합법적인 사용자의 접근 승인이 이루어진 시간과 아이디 일부정보를 기반으로 하여 변경되고, 확장된 1회용 패스워드를 유지함으로서 사전공격에 대한 차단효과를 극대화 할 수 있다. 또한 사용자에게 심리적 안정감을 부여함으로서 패스워드 관리의 신뢰성을 부여할 수 있다. 사용자에게 기억의 부담을 주지 않으면서 $0.13m$배 만큼의 정보엔트로피가 증가하므로 공격자에게 불확실성의 부담을 줄 수 있다. 그리고 입력된 패스워드가 특정 길이보다 작을 때 임의의 문자를 채워줌으로서 관리의 효율성을 증대시킨다.

일반적으로 사용하는 패스워드의 정보엔트로피는 낮을 수밖에 없기 때문에 1회용 인증키, 마코브 체인과 정보엔트로피를 고려한 효율적이고 가변적인 패스워드 관련 연구는 향후 진행되어야 할 영역이다.

참 고 문 헌

[1] 중앙일보, *인터넷 발전으로 '사실(fact)'이 사라진다.*, 2010. 12. 11.

[2] 지선수, "SPRT를 기반으로 하는 누적합 스테간 분석을 이용한 은닉메시지 감지기법", 한국산업정보학회논문지, 제 15권, 제 3호, pp. 37-43, 2010.

[3] 방송통신위원회와 한국인터넷진흥원, *2009년 정보보호 실태 조사결과*, 2010.

[4] N. Provos and D. Mazières, "A Future-Adaptable Password Scheme", Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference Monterey, California, USA, June 1999.

[5] The Imperva ADC, "Consumer Password Worst Practices", ADC White Paper, pp. 1-5, Dec. 2009.

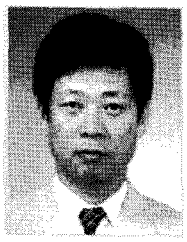
[6] Benjamin Strahs, Chuan Yue and Haining Wang, "Secure Passwords Through Enhanced Hashing", Bachelor Thesis of College of William and Mary, 2009.

[7] Hitachi ID Systems, Inc, *Password*

Management Best Practices, [Online] Available http://hitachi-id.com/.
[8] S. J. Aboud, "Efficient Password-Typed Key Agreement Scheme", International Journal of Computer Science Issues, Vol. 7, No. 2, pp. 26-31, 2010.
[9] Fraud Newsletter, *Virtual Keyboard and Password Creation*, 27 September 2010.
[10] Chih-I Wang, Chun-I Fan, and D. J. Guan, "Cryptanalysis on Chang-Yang-Hwang Protected Password Change Protocol", [Online] Available http://eprint.iacr.org/.

지 선 수(Seon-Su Ji)

- 정회원
- 1984년 충남대학교 계산통계학과(학사)
- 1986년 중앙대학교 응용통계학과(석사)
- 1993년 중앙대학교 응용통계학과(박사)
- 2006년 명지대학교 컴퓨터공학과(박사수료)
- (현)강릉원주대학교 정보기술공학과 교수
- 관심분야 : 혼잡제어, 정보보안(암호키, 정보은닉), 이미지 프로세싱



이 희 춘(Hee-Choon Lee)

- 정회원
- 1974년 강원대학교 수학교육과(학사)
- 1981년 경희대학교 교육대학원수학교육 전공(석사)
- 1983년 경희대학교 수학과(석사)
- 1987년 경희대학교 수학과(통계학)(박사)
- 2009년 강원대학교 컴퓨터과학과(박사)
- (현)상지대학교 컴퓨터데이터정보학과 교수
- 관심분야 : 전산통계, 정보보호, 전자상거래 추천시스템

논 문 접 수 일 : 2011년 03월 29일
1차수정완료일 : 2011년 06월 07일
2차수정완료일 : 2011년 08월 08일
게 재 확 정 일 : 2011년 08월 31일