슈도피아 함수를 이용한 다중 패스워드 관리 방안

장 화 식[†] · 신 원[††] · 이 경 현[†††]

요 약

본 논문에서는 가상공간에서 다중 패스워드 관리와 변경을 수행하는 슈도피아 함수를 이용하여 효율적인 다중 패스워드 관리 방안을 제안한다. 사용자와 웹사이트가 주어지면 슈도피아는 웹사이트에서 익명의 계정을 설정하는데 필요한 사용자 이름과 패스워드를 자동적으로 생성한다. 제안 방안에서 사용자는 자신의 경험과 연관된 "개인 엔트로피"를 사용하여 패스워드를 보호할 수 있다. 또한 본 방안은 전자상거래, 인터넷 뱅킹 시스템과 같은 인터넷 관련 응용에서 폭넓은 도구로 적용될 수 있다.

A Multi-password Management Scheme using Pseudopia Function

Hwa-Sik Jang[†] · Weon Shin[††] · Kyung-Hyune Rhee[†††]

ABSTRACT

In this paper, we propose an efficient password management scheme using the Pseudopia function which performs a multi-password management and change scheme in the cyberspace. For a given user and a web-site, the Pseudopia automatically generates a user name and a password that can be used to establish an anonymous account at the web-site. In the proposed scheme, a user can protect his password using "the personal entropy" which relates to his own life experiences, that identified only by himself. The proposed scheme can be applied to the broad tools for the Internet related applications such as electronic commerce and Internet banking system.

1. 서 론

최근 인터넷 인구가 폭발적으로 성장함과 함께 빠르고 편리한 사용자 환경의 요구로 인하여 현실세계의 많은 서비스들이 인터넷의 가상세계에 등장하고 있다. 현실세계의 상거래나 서비스의 제공은 면대면(Face-to-Face)으로 이루어지지만, 네트워크 상에서는 컴퓨터를 통한 가상의 서비스 및 상거래가 이루어지도록 구현된다. 따라서 실명을 대신하는 가상의 신분을 갖게 되는데 주로 자신의 별칭인 ID 개념을 사용한다. 인터넷 상에서의 전자우편, 파일전송, 뉴스그룹 등의 일반 서비스뿐만 아니라 쇼핑몰 또는 인터넷 뱅킹 등의 가상 거래에서도 이러한 ID를 이용한 가상의 신분을 사용하고 있다. 특히 가치이전이 수반되는 전자상거래에서는 이러한 가상의 신분인 ID와 그에 해당하는 패스워드에 대한 지식으로 실제 개인을 연결시켜 다양한 정보 및 서비스 제공으로까지 이어지고 있다. 이러한 이유 때문에 오늘날 다양한 방법들을 동원하여 각 사용자에 대한 ID 관리를 여러 절차에 거쳐서 수행하고 있으며 여러 가지의 신분확인 과정을 도입하고 있다. 즉, 정당한 정보와 서비스를 제공받기 위해서는 신분확인이 선행되어야 하는 가장 중요한 작업이며 이를 기반으로 공유자원에 대한 접근제어 등이 수행된다.

† 정 회 원 : 부경대학교 전자계산학과 박사수료
†† 준 회 원 : 부경대학교 전자계산학과 박사수료
††† 종신회원 : 부경대학교 전자컴퓨터정보통신공학부 교수

논문접수 : 2000년 9월 6일, 심사완료 : 2000년 11월 6일

특히, UNIX 기반의 시스템에서는 전통적으로 ID와 패스워드 기법을 사용하였고 이를 기반으로 구축되기 시작한 현재의 많은 인터넷 및 WWW 서비스들도 간결하고 효율적이지만 안전하지는 못한 ID에 기반을 둔 신분확인 기법을 사용하고 있다[1]. 웹사이트 상에서 서비스를 받기 위해서는 사용자 ID와 패스워드를 요구하는 경우가 대부분이며, 여러 웹사이트를 접속하는 사용자의 경우 편의를 위해서 다른 웹사이트에도 같은 ID와 패스워드로 등록하여 사용하는 경향이 있는데, 이 경우 불순한 동기를 가진 웹사이트의 관리자에게 다른 웹사이트의 사용자 ID와 패스워드를 유추할 수 있게 하여 범죄에 이용당하거나 의도하지 않은 개인 프라이버시 노출 문제를 일으키기도 한다[3].

본 논문에서는 인터넷과 같은 기상 공간에서 본인의 신분확인에 이용되는 패스워드 분실과 변경을 위한 효율적인 방안을 제안하고, 웹사이트에서 사용되는 주요 ID에 대한 익명성을 제공함으로써 개인 프라이버시를 보호할 수 있는 방안을 제안한다. 제안 방안은 주 사용자 ID와 패스워드를 이용하는 환경 하에서 일방향 해쉬 함수를 적용하여 사용자 ID와 패스워드를 웹사이트마다 다르게 생성·제공함으로써 익명성을 보장하고, 주 패스워드 분실시 본인확인 절차를 개인의 독특한 성향이나 생활 정험인 개인 엔트로피에 관련된 문제를 이용하여 Challenge-Response 형태로 본인임을 확인하는 시스템 구현을 목적으로 한다

본 논문의 구성은 2장에서는 기존 방안에 대해서 기술하고, 3장에서는 제안시스템인 패스워드 관리 방안 및 사용자 신분확인 방안에 대하여 설명한다. 4장에서는 제안 방안의 안전성 평가 및 확장성에 대하여 기술하고, 마지막 5장에서 결론을 맺는다.

2. 기존 방안

인터넷을 이용한 다양한 서비스가 등장하고 고객 유치를 위한 많은 상업적인 방법들이 동원되고 있다. 이 과정에서 정당한 서비스를 사용하기 위하여 각 사용자는 한 쌍의 ID와 패스워드를 소유하고, 이를 통하여 신분확인에 적용하게 된다. 그러나 많은 웹사이트에 접속함에 따라 해당하는 ID와 패스워드의 수는 비례해서 증가하게 되고 이의 관리를 용이하도록 하기 위하여 서로 다른 웹사이트에서 동일한 ID와 패스워드를 사용하는 경우가 발생하고 있다. 특히, 인터넷의 개인 프라이버시 침해라는 새로운 사회적 문제가 부각되고 있는 이 시점에서 여러 상업 업체들이 개개인의 정보를 이용하여 사용자의 인터넷 사이트 방문 기록, 로그 파일을 통한 개인의 인터넷 접속 성향 등을 서로 공유하는 현상까지 벌어지고 있다.

Anonymizer에서는 WWW상에서의 사용자의 URL (Uniform Resource Locator)을 일종의 프락시를 통하여 익명화하여 서버에 사용자의 정보가 누출되지 않도록 하고 있다[6]. 특히, URL 암호화를 통하여 각 웹페이지 링크에 대한 프라이버시를 제공하도록 암호화 알고리즘을 도입하고 있다. Anonymizer에서는 프락시 서버를 사용함으로써 웹 서버에 대해 사용자의 IP 주소나 도메인 이름 정보를 숨김으로써 익명성을 제공해 주지만 적어도 두 가지 고려해야 할 사항이 있다. 첫 번째로, 프락시 서비에는 사용자들의 모든 요청에 대한 기록(log)이 남으므로, 사용자는 프락시 서비스 제공자가 자신의 정보를 누출하지 않도록 신뢰되어야 한다. 또한 프락시는 웹 서비에 대해 사용자의 실체를 숨기기에는 적합하지만, 사용자에게 웹 서버의 실체를 감추기에는 적합하지 않다.

E. Gabber 등이 제안한 Janus Function은 개인의 프라이버시를 보호하기 위하여 해쉬 함수를 이용하여 서로 다른 웹사이트의 ID와 패스워드의 연관성을 유추하지 못하도록 구성하였다[5]. Janus는 브라우저의 익명성을 제공해주기 위해 Anonymizer와 유사한 proxy 서버로 동작하고 웹 서버의 익명성을 제공하기 위해 URL의 웹 서버에 대한 참조 부분을 공개키 암호방식을 사용해서 암호화하고 복호화 한다. Janus 시스템을 사용함으로써 서버의 IP 주소나 호스트 이름을 숨길 수 있는 이점을 제공하지만 단지 URL만이 암호화되므로 실제 데이터 스트림에 대한 보안성은 제공하지 않는다.

Lucent Technology사의 LPWA(Lucent Personalized Web Assistant)는 스팸메일을 방지하고 각각의 웹사이트에 대해 유일한 사용자 ID, 패스워드, 전자우편 주소를 생성함으로써 사용자의 프라이버시를 보호한다[7] LPWA는 사용자들이 각 사이트에 대한 자신의 계정을 기억해야 하는 부담을 덜어주고, 가명을 사용함으로 인해 사용자의 실제 신원이 노출되지 않도록 함으로써 개인화된 웹 브라우징과 익명성을 동시에 제공해 준다.

Chaum은 익명의 웹 통신에 관한 제안을 하고 있는

데, 전용 라우터를 이용하여 메시지 암호화, 전자메일, 리턴 주소 등을 외부 도청 공격으로부터 보호하고, 주소를 추적 불가능하게 함으로써 익명성을 보장한다[4].

컴퓨터 및 자원에 대한 상당한 허가권을 얻기 위하여 사용자 신분확인 메커니즘이 필수적으로 요구되는데, 최근에 보다 정확한 신분확인 기법을 위해 생체확인 기법이 도입되고 있으나 비용이 비싸고 실제 네트워크 시스템에 적용하기 어려운 단점이 있다. 현재 네트워크에 적용 가능한 저렴하고 안전한 방안으로 동적인 패스워드 기법, Challenge-Response 기법 등이 도입되고 있으며 다양한 응용분야가 존재한다. 본 논문에서는 C.Ellison 등[2]이 제안한 개인 엔트로피(personal entropy)라는 개념과 기존의 인터넷 및 WWW에서 가장 많이 사용되고 있는 ID와 패스워드 기법을 근간으로 이를 향상시킨 새로운 방법을 제안하고자 한다.

3. 제안방안

3.1 패스워드 관리 방안

본 논문에서는 사용자 ID와 패스워드를 기반으로 하는 효율적이고 안전한 패스워드 관리 방안을 제안한다. 본 제안 방안에서 사용되는 용어는 <표 1>과 같다.

〈표 1〉 패스워드 관리 방안에 사용되는 용어들

U	사용자
W_i	: i번째 웹사이트의 URL 주소
ID_U	: 사용자의 주 ID
PW_U	: 사용자의 주 패스워드
ID_{W_i}	W_i에 대한 사용자 ID
PW_{W_i}	: W_i에 대한 사용자 패스워드
Pseudopia(슈도피아)	패스워드 관리 함수
T	사용자 U가 슈도피아에 로그인한 시각
H	일방향 해쉬함수

사용자는 인터넷을 통하여 WWW에 접속할 수 있는 환경을 갖추고 있다. 슈도피아는 사용자와 임의의 웹사이트 중간에 위치하며 사용자의 ID 및 패스워드와 관련된 동작을 담당하여 처리한다. 사용자와 슈도피아 사이는 안전한 네트워크로 연결되어 있으며 슈도피아와 웹사이트 W_i 사이는 공개된 인터넷 환경이다. (그림 1)은 제안된 슈도피아의 동작 방식을 보여준다.

① 사용자 등록 요청

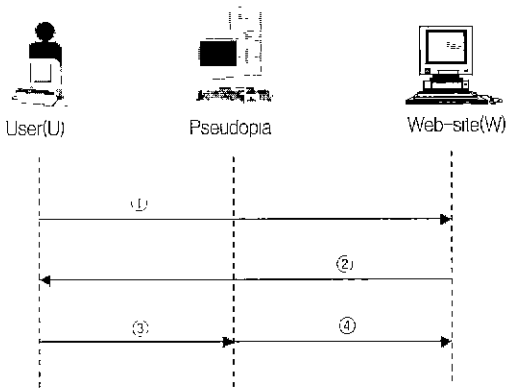
사용자 U는 서비스를 제공받기 위하여 웹사이트 W_i에 접속하여 사용자 등록 페이지를 요청한다.

② 사용자 등록 페이지 전송

웹사이트는 사용자의 요구에 의해 사용자 등록 페이지를 전송한다. 서비스 사용을 위해 사용자 등록에 필요한 각종 기입 사항을 요구한다.

③ 사용자 등록 완료

사용자는 각종 필수적인 기재사항을 작성하고 등록을 완료한다. 이 시점에서 사용자의 ID와 패스워드도 입력하게 되는데, 여기서 ID_U와 PW_U가 생성된다.



(그림 1) 패스워드 관리를 위한 슈도피아의 동작방식

④ 슈도피아의 동작

사용자가 전송한 등록 메시지를 슈도피아가 관여하여 다른 부분은 그대로 전송하지만 사용자가 입력한 ID_U와 PW_U 대신에 ID_{W_i}와 PW_{W_i}를 전송한다. 즉, 사용자의 로그인 시간을 적용한 타임스탬프 T를 생성한 후 일방향 해쉬함수 H를 이용하여 $ID_W = H(ID_U, W_i, T)$, $PW_W = H(PW_U, W_i, T)$를 각각 생성하고 사용자에 대한 타임스탬프 T를 안전하게 저장한다.

⑤ 반복

사용자가 다른 웹사이트 W_j에 등록할 때도 같은 방식으로 동작하는데, 사용자는 역시 자신의 ID_U와 PW_U를 입력하면 중간에서 슈도피아가 처리하여 $ID_{W_j} = H(ID_U, W_j, T)$, $PW_{W_j} = H(PW_U, W_j, T)$를 생성하여 웹사이트 W_j에게 전송한다.

따라서, 사용자는 단 한 쌍의 ID_U와 PW_U만을 가지고 여러 웹사이트에 서로 다른 ID와 패스워드 쌍으로써 접속할 수 있게 된다. 이를 통하여 사용자는 패스워드 관리를 효율적으로 수행할 수 있으며, 각 웹사이트간의 ID와 패스워드 쌍을 전혀 다르게 둠으로써 웹사이트끼리 연관된 정보 유출의 가능성을 줄일 수 있다. 따라서, 제안방안은 웹사이트 상에서 ID와 패스워드 공유를 통한 연결자체에서 사용자에 대한 신분을 알 수 없게 하고, 웹사이트와의 연결 동안 데이터 흐름에 있어 익명성을 제공하는 두 가지 기능을 제공한다.

3.2 신분확인 방안

전자상거래 및 인터넷 뱅킹에서 네트워크 상에서 본인임을 확인해야 하는 경우가 종종 발생하는데, 네트워크를 통하여 본인임을 확인하는 방법은 부가적인 장비가 필요하거나 비효율적이어서 실제에 적용하기가 상당히 힘들다. 본 논문에서는 개인의 특성, 경험 등을 기반으로 하는 개인 엔트로피 개념을 도입하여 네트워크 상에서 효율적이고 안전하게 신분을 확인하는 방안을 제안한다. 본 제안 방안에서 사용되는 용어는 <표 2>와 같다.

〈표 2〉 사용자 신분확인 방안에 사용된 용어들

U	: 사용자
q_i	: i번째 질문
a_i	: i번째 질문에 대한 정답
r_U	: 사용자 U에 해당하는 난수
E_k	: 대칭키 k를 이용하여 암호화
H	: 일방향 해쉬함수

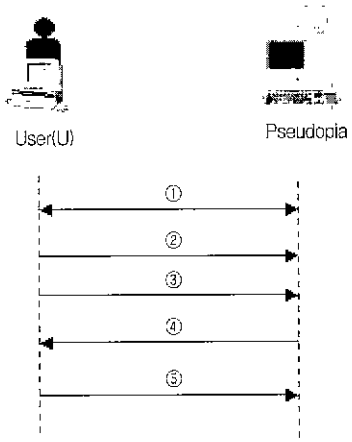
사용자와 슈도피아 사이는 안전한 네트워크로 연결되어 있거나 콘솔에서 직접 수행된다고 가정한다. (그림 2)는 제안된 슈도피아의 동작 방식을 보여준다.

① 사용자 등록

사용자 등록 절차를 수행하고, 개인 엔트로피에 기반하는 n개의 질문 $(q_1, \cdots, q_n)$을 생성하거나 합의하여 선택한다.

② 사용자 대답 저장

사용자는 n개의 질문 $(q_1, \cdots, q_n)$에 해당하는 n개의 대답 $(a_1, \cdots, a_n)$을 작성한 후 슈도피아로 보낸다. 이 때 슈도피아는 임의의 난수 r_U를 생성하고 각



(그림 2) 사용자 신분확인 절차

질문과 대답, 난수를 일방향 해쉬함수 H에 적용하여 대칭키 k로 암호화한 $(s_1, \cdots, s_n)$을 생성한다. 여기서, $s_i = E_k(H(q_i, a_i, r_U))(1 \le i \le n)$ 이다. 슈도피아는 $((q_1, \cdots, q_n), (s_1, \cdots, s_n), r_U, k)$를 안전하게 보관함으로써 사용자 등록 과정을 종료한다.

③ 신분확인 요청

서비스를 사용하다 패스워드를 분실했다든지 패스워드 변경이 필요한 경우 사용자의 신분확인 절차를 거친 후 필요한 조치를 취하게 되는데, 일반적인 시스템에서는 직접 서비스 해당 기관을 찾아가서 수행하게 된다. 그러나 본 제안 방안에서는 네트워크를 통하여 신분확인을 요청하고 신분확인 절차를 수행한다.

④ 질문 전송

슈도피아는 사용자 등록시 사용했던 질문 $(q_1, \cdots, q_n)$을 사용자 U에게 전송한다.

⑤ 대답 전송

사용자 U는 대답 $(a_1', \cdots, a_n')$을 작성하여 전송한다. 슈도피아는 질문 $(q_1, \cdots, q_n)$, 사용자의 대답 $(a_1', \cdots, a_n')$, 난수 r_U를 일방향 해쉬함수 H에 적용시켜 $H(q_i, a_i', r_U)(1 \le i \le n)$를 계산하고 s_i를 k로 복호화한 $H(q_i, a_i, r_U)(1 \le i \le n)$와 각각 같은지 비교한 후 일정 수준에 도달하면 본인임을 확인하고 원하는 서비스를 제공한다.

정보의 중요도에 따라 신분확인 절차 ①, ⑤ 과정을

서비스 사용 때마다 수행하도록 설정할 수 있으나 사용의 편의성을 위하여 패스워드 변경이나 본인 확인이 꼭 필요한 서비스인 경우에만 선택적으로 동작시킬 수 있다.

4. 안전성 평가 및 시스템 확장

4.1 안전성 평가

패스워드 관리 방안에서 가능한 공격 시도 또는 취약성 요인을 살펴보면 다음과 같다. 먼저 웹사이트 W_i에서 ID_{W_i}와 PW_{W_i}를 이용하여 사용자의 ID_U와 PW_U를 추측하려는 시도이다. 이것은 슈도피아의 일방향 해쉬함수 출력값을 통하여 입력값을 추측하려는 시도와 동일한데, 사용하는 해쉬함수의 안전성이 증명된다면 계산량적으로 해쉬함수의 역을 구하는 것과 같고 이것은 사실상 매우 어렵다. 두 번째는 여러 사용자가 슈도피아를 사용하는 경우 같은 웹사이트 W_i에 대하여 사용자 ID와 패스워드의 충돌 가능성이 존재한다. 우연히 서로 다른 사용자가 ID_U, PW_U를 동일하게 지정하더라도 사용자의 로그인 시각 T가 다르다면 역시 서로 다른 ID_{W_i}, PW_{W_i}을 생성하므로 중복의 가능성이 확률적으로 상당히 줄어들게 된다. 세 번째는 비밀값 저장에 따른 비밀 누출의 위험인데, 이는 슈도피아가 사용자의 최초 로그인 시각 또는 패스워드 변경 시각을 기반으로 하는 T만을 저장하므로 사용자의 ID_U, PW_U에 대한 어떠한 정보도 저장하지 않는다. 따라서 슈도피아의 안전성은 일방향 해쉬함수의 안전성과 T의 랜덤성에 전적으로 의존한다.

신분확인 방안에서 안전성 평가 요소를 살펴보면 다음과 같다. 먼저 개인 엔트로피에 기반하는 질문의 개수를 n이라 하고, 한 질문에 대한 대답의 경우의 수는 256가지를 넘는다고 가정한다. 또한 사용자 본인이 하나의 질문에 대해 정답을 맞출 확률을 P_0(예를 들어, 0.95), 사용자가 n개의 질문에 대해 k개를 맞출 확률을 $P_1(k, n, P_0)$, t개의 정답을 맞추어 슈도피아를 통과할 확률을 $P_2(t, n, P_0)$(예를 들어, 0.99998)이라 두자. 정당한 사용자가 k개의 정답을 맞추었다면,

$$P_1(k, n, P_0) = \binom{n}{k} P_0^k (1-P_0)^{n-k}$$

이 된다. 한편, 일반적으로 공격시스템이 128 비트 대칭키 시스템의 키를 알기 위한 무작위 공격에 필요한 경우의 수는 2^{128}이다. 이와 같은 정도의 안전성을 가지도록 신분확인 시스템을 구성하기 위해서는 가능한 응답의 개수가 256가지 이상을 가지는 질문에 대해 $t=16$개를 맞추어야만 이것을 만족한다고 볼 수 있다. 따라서

$$P_2(t, n, P_0) = \sum_{i=t}^{n} P_1(i, n, P_0) = 0.99998$$

이 되는 질문의 개수 n은 24가 된다. 이 사실을 이용하여 신분확인이 필요한 경우 응답의 가능성이 256가지 이상의 경우의 수를 가지는 질문 24개를 구성하여 사용자에게 보내어 16개 이상의 정답을 대답할 수 있다면 본인으로 간주하는 것이다. 이러한 예에서 보안 강도 t를 설정하고 n을 찾은 후 이를 표로 구성하면 <표 3>과 같다.

한편 보다 안전한 신분확인 기법을 적용하고자 할 경우, 더 큰 P_2값이 요구되어지고 이에 따른 (n, t)표가 새로이 구성되어 적용될 수 있다.

<표 3> $P_2 = 0.99998$인 경우 (n, t) 표

n	t	n	t	n	t
5	1	6	1	7	2
8	3	9	3	10	4
11	5	12	6	13	7
14	7	15	8	16	9
17	10	18	11	19	11
20	12	21	13	22	14
23	15	24	16	25	17
26	17	27	18	28	19
29	20	30	21		

4.2 구현 방안 및 개선

제안 패스워드 관리 방안에서 ID 및 패스워드를 효율적으로 관리하기 위해서 단지 T만을 안전하게 저장한 후 사용하는데 웹사이트 $W_i(1 \le i \le n)$의 패스워드가 변경되는 경우 모든 $PW_{W_1}, \cdots, PW_{W_n}$이 다시 계산되어야 한다. 따라서, 실제 시스템 구현시에는 각각의 웹사이트 $W_1, \cdots, W_n$에 따라 서로 다른 $T_1, \cdots, T_n$를 저장해 둔다면 패스워드 변경시 해당하는 웹사이트에 대한 T_i만을 반영하면 다른 웹사이트의 패스워드 변경없이 개별적으로 패스워드 갱신이 가능하다. 또한 시스템의 안전성이 해쉬함수의 강도에 의존하므로 현재 안전하

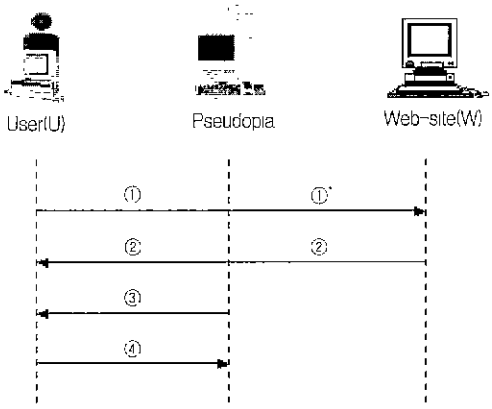
다고 알려진 $SHA-1$, $MD5$, HAS 등을 시스템에 적용한다면 익명성을 가지는 개별화된 웹브라우징이 가능하다. 실제 시스템 구현시 슈도피아는 사용자 개인 시스템 내부에 위치하여 브라우저와 같이 사용될 수 있으며, 또한 프락시와 같은 형태로 시스템 외부에 서버를 두어 사용할 수도 있다. 특히, 외부에 위치하는 경우에는 다양한 환경의 사용자에 대한 배려가 있어야 하고, 개별 사용자에 대한 비밀 데이터도 안전하게 보존되어야 한다.

제안 신분확인 방안에서 사용자 신분확인을 위한 목적을 제대로 달성하기 위해서는 질문이 얼마나 개인적인가 하는 것이 매우 중요한 부분이 된다. 예를 들어, "자신의 생일", "최초의 TOEIC 시험 성적"과 같은 질문은 256가지 경우의 수를 넘으므로 충분히 질문의 대상이 될 수 있다. 또한 "최초의 이성친구 이름"과 같은 훨씬 더 경우의 수가 많은 개인적인 질문을 구성함으로써 안전성에는 큰 영향을 미치지 않으면서 앞의 (n, t)를 감소시켜 사용자의 편의성을 증가시킬 수 있다. 실제 시스템 구현시에는 슈도피아에서 매우 많은 질문을 미리 준비해놓고 사용자가 모두 응답한 다음, 신분확인시 부작위로 (n, t)에 해당하는 일부분만을 질문하거나 또는 질문 구성을 시스템과 사용자의 동의하에 함께 구성하여 개인 엔트로피를 높일 수 있다. 슈도피아는 네트워크 상에서 반드시 본인임을 확인해야 하는 인터넷 뱅킹 등의 응용분야에 적용할 수 있으며, 궁극적으로 시스템의 안전성은 본인인 경우에는 상당히 쉬운 질문이지만 다른 사람인 경우에는 대답하기 어려운 질문을 어떻게 찾아내는가 하는 것에 달려 있다.

4.3 결합 방안

본 절에서는 이전에 제안했던 패스워드 관리 방안과 신분확인 방안을 결합하여 새로운 방안을 설명한다. (그림 3)의 슈도피아는 편소에는 효율적인 패스워드 관리 기능을 제공하면서 패스워드 분실 및 갱신과 같은 본인임을 반드시 확인해야 하는 경우 신분확인 기능을 수행하는 시스템이다.

①과 ①'은 웹사이트 W_i에 접속하기 위해 슈도피아를 통한 ID와 패스워드 전송 과정이다. 사용자는 ①과정에서 자신의 ID_U와 PW_U를 입력하면 슈도피아가 받아서 처리하여 이미 저장된 T를 이용하여 $ID_{W_i}=H(ID_U, W_i, T)$, $PW_{W_i}=H(PW_U, W_i, T)$를 계산한 후 ①' 과정에서 웹사이트 W_i에 전송한다. ②와 ②'은 수신과정이다. 슈도피아는 별다른 동작을 하지 않고 받은 메시지를 그대로 사용자에게 전송하지만 패스워드 갱신 등의 요구 등을 관찰하여 다음의 동작을 대비한다. ③은 사용자가 주 사용자 패스워드를 분실했거나 갱신 요청으로 인하여 사용자에게 신분확인을 위한 개인 엔트로피에 기반한 질문을 전송한다. ④에서 사용자는 질문에 대한 대답을 전송하면 슈도피아는 본인인지 아닌지를 판단하여 다음 동작을 수행한다.



(그림 3) 결합된 방안에서의 슈도피아 동작 절차

5. 결 론

본 논문에서는 기존의 패스워드 관리 방안과 본인 신분확인 방안을 살펴보고, 인터넷 가상공간에서 효율적인 ID 및 패스워드 관리 방안, 안전한 신분확인 방안을 제안하였다. 각각의 제안 방안에 대한 안전성 평가를 수행하고 시스템 확장 및 개선 방안을 논의하였다.

인터넷에서 개인 프라이버시의 침해는 심각한 수준이며, 심지어 상업적인 목적을 위하여 웹사이트끼리 사용자 정보를 공유하여 사용하는 실정이다. 제안 방안의 슈도피아는 이를 보호하기 위한 한 방법을 제시하며 개별화된 웹 브라우징을 제공함으로써 웹사이트 입장에 있어 익명성을 제공하고 하나의 ID, 패스워드 쌍으로써 여러 웹사이트의 ID와 패스워드를 관리할 수 있는 효율적인 방법을 제공한다. 또한 확률적인 방법과 개인 엔트로피 개념을 도입하여 네트워크 상에서 본인임을 확인하는 방법을 제공하여 기존의 방안보다

경제적이고 안전한 방법을 통하여 신분확인이 가능하도록 한다. 이러한 가상 공간에서의 패스워드 관리 방안과 신분확인 방안은 결합하여 하나의 통합 방안으로 동작할 수 있으며, 정보 전달이 주요한 가치이신 요소로써 사용되는 인터넷 뱅킹이나 전자상거래 환경 등에서 본 제안 방안은 광범위하게 활용될 수 있을 것으로 판단된다

참 고 문 헌

[1] A. Frisch, Essential system administration. 2ed., O'Reilly & Associates, Inc., 1995.

[2] Carl Ellison, Chris Hall, Randy Milbert and Bruce Schneier, "Protecting Secret Keys with Personal Entropy," Elsevier Science, 1999.

[3] CERTCC-KR. http : //www.certcc or.kr/

[4] D Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, Vol.24, No.2, 1981.

[5] E. Gabber, Gibbons P, Matias Y and Mayer A., "How to make personalized web browsing simple, secure, and anonymous," Internet Proceedings of Financial Cryptography97, 1997.

[6] The Anonymizer. http : //www.anonymizer.com

[7] The Lucent Personalized Web Assistant. http : // www bell-labs com/project/lpwa/

장 화 식

e-mail : hsjang@unicom.pknu.ac.kr

1993년 계명대학교 통계학과 졸업(학사)

1995년 부경대학교 대학원 전자계산학과 졸업(석사)

2000년 부경대학교 대학원 전자계산학과(박사수료)

1996년~1999년 제주관광대학 사무자동화과 전임강사

2000년~현재 부경대학교 BK21 기계공학부 계약교수

관심분야 : 컴퓨터보안, 정보보호, 암호학 등

신 원

e-mail redcomet@unicom.pknu.ac.kr

1996년 부경대학교 전자계산학과 졸업(학사)

1998년 부경대학교 대학원 전자계산학과 졸업(석사)

2000년 부경대학교 대학원 전자계산학과(박사수료)

1998년~현재 부경대학교 강사

관심분야 정보보호, 컴퓨터 보안, 네크워크 보안, 암호학 응용

이 경 현

e-mail khrhee@pknu.ac.kr

1978년~1982년 경북대학교 사범대학 수학교육과(이학사)

1983년~1985년 한국과학기술원(KAIST) 응용수학과(이학석사)

1988년~1992년 한국과학기술원(KAIST) 수학과(이학박사)

1985년~1991년 한국전자통신 연구소(ETRI) 연구원

1991년~1993년 한국전자통신 연구소(ETRI) 선임연구원

1995년~1996년 호주 Adelaide대학 응용수학과 교환교수

1993년~1995년 부산수산대학교 전자계산학과 전임강사

1995년~1999년 부경대학교 전자계산학과 조교수

1999년 일본 동경대학 생산기술연구소 객원연구원

1999년~2000년 부경대학교 전자컴퓨터정보통신공학부 부교수

1997년~현재 한국멀티미디어학회 논문편집위원

1997년~현재 한국멀티미디어학회 학술이사, 운영위원

1999년~현재 (주)인트넷 기술고문

1999년~현재 (주)아시아 디자인 기술고문

2000년~현재 한국통신정보보호학회 영남지부 감사

2000년~현재 부경대학교 전자컴퓨터정보통신공학부 부교수

관심분야 : 컴퓨터보안, 정보보호, 네트워크성능 평가, 광대역 통신망 암호학, 대기체계