Pseudopia 함수를 이용한 다중 패스워드 관리방안

김영인†, 윤희영†, 이경현‡
† 부경대학교 전산정보학과
‡ 부경대학교 컴퓨터멀티미디어전공

A Multi-password Management Scheme using Pseudopia Function

Yung-In Kim†, Hee-Young Yoon†, Kyung-Hyune Rhee‡
† Department of Computer & Information Science, PKNU
‡ Department of Computer and Multimedia Engineering, PKNU

요 약

본 논문에서는 실생활에서 개인이 관리해야 하는 다수의 패스워드를 효율적으로 관리하고 가상 공간에서 패스워드 분실 및 변경을 효과적으로 수행하기 위한 Pseudopia라는 패스워드 전용관리 함수를 제안한다. 제안 방안은 인터넷 접속에 사용되는 사용자 id나 패스워드를 일 방향 함수를 이용하여 웹사이트마다 다르게 제공함으로써, 사용자id를 통한 패스워드 유추 또는 신분 노출의 문제점을 방지해 주고, 주요 패스워드의 분실 시 기존 방식인 사용자와 관리자의 면대면 신분확인 방식을 개선함으로써, 인터넷 사용자에게 보다 편리하고 안전한 환경을 제공할 수 있다.

1. 서론

최근 인터넷 인구가 폭발적으로 성장함으로써 빠르고 편리한 사용자 환경의 요구로 현실세계의 수많은 서비스들이 인터넷의 가상세계에 등장하고 있다. 현실세계에서 상거래나 서비스의 제공은 인간을 중심으로 이루어지지만, 가상 세계에서는 인간이 만든 컴퓨터와 네트워크라는 도구로 모든 서비스가 제공되고 이를 이용한 상거래도 이루어지고 있다. 이러한 거래의 중심에는 가치이전이 있고, 반드시 신뢰가 수반되어야 한다. 그러나, 가상 세계에서 가치이전을 위한 상호 신뢰는 여러 가지 문제점이 존재하며, 이에 대한 문제점들이 해결되지 않으면 현실세계에서 가상 세계로의 이전도 힘들다. 문제 해결 방안으로 인터넷에서 제공되는 서비스가 중요할수록 각 사용자에 대한 계정 관리를 여러 보안 절차에 따라 수행하고 있으며, 다양한 방법을 동원하여 본인에 대한 신원확인을 하고 있다. 계정을 관리하는 방법에는 사용자 ID와 패스워드를 요구하는 경우가 대부분이며, 여러 웹사이트를 접속하는 사용자의 경우 같은 id와 패스워드로 다른 웹사이트에 접속하는 경향이 있는데, 이 경우 불순한 동기를 가진 웹사이트의 관리자가 다른 웹사이트의 사용자 id와 패스워드를 유추할 수 있게 하여 범죄에 이용당하거나 의도하지 않은 개인 신분 노출 문제에 직면하기도 한다.

본 논문에서는 인터넷과 같은 가상 공간에서 본인의 신분확인에 이용되는 주요 패스워드의 분실이나 변경을 위한 효율적인 방안을 제안하고, 웹에서의 익명성을 제공함으로써 개인 프라이버시 보호방안을 제안한다. 제안 방안은 주 사용자 id와 패스워드를 이용하여, 충돌회피 일 방향 해쉬 함수로 새로운 사용자의

id와 패스워드를 웹사이트마다 다르게 생성하여 제공함으로써, 익명성을 보장하고, 주 패스워드 분실 시 본인확인 절차를 사용자 스스로의 생활경험 혹은 개인의 독특한 성향과 관련된 문제를 미리 등록해 두고 패스워드 관리를 담당하는 시스템에서 본인확인을 원하는 사용자에게 여러 가지 문제를 시도(Challenge) 형태로 물어보고 응답(Response)에 대해 엔트로피 관점에서 분석 한 후 본인을 확인하는 시스템 구현을 목적으로 한다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 기 제안 방안에 대해서 기술하고, 제 3 장에서는 제안시스템에 대한 설명을, 제 4 장에서는 제안 방안의 평가 및 확장성 및 대해서 기술하고, 마지막 5장에서 결론을 맺는다.

2. 기 제안 방안

2.1 익명성 보장 방안

인터넷에서 신분 노출은 새로운 문제를 야기하는데, 원치 않는 메일을 받는 일, 본인을 가장한 상거래의 성립 등 자신의 의도와는 상관없이 범죄에 이용될 소지가 있으며, 개인의 인터넷 방문현황, 상거래 현황, 심지어는 로그 파일을 분석하여 개인의 금융거래 정보까지 노출시킴으로써 범죄에 악용하는 경우도 있다.

Anonymizer 사이트[3]에서 익명성 제공 방안으로는 접속사이트의 URL을 Encryption하여 프락시 사이트에서만 쿠키정보를 Decryption 할 수 있으며, E. Gabber, P. Gibbon이 제안한 야누스(Janus) Function[3]도 개인 프라이버시를 보호하기 위하여 일방향 해쉬 함수를 이용하여 접속자의 익명성을 제공하며, Lucent Technology 사의 LPWA(Lucent Personalized Web Assistant) 프로젝트는 스팸메일을 방지하는 방안을 제안하고, Chaum의 Mix Network 프로젝트는 익명의 웹 통신에 관한 제안을 하고 있는데, 전용 라우터를 이용하여 메시지 Encryption은 물론, 전자메일, 리턴 주소 등을 외부 도청 공격을 방지하고, 주소를 추적 불가능하게 함으로써 익명성을 보장한다.

2.2 신분 확인 방안

컴퓨터 사용자의 정당성을 확인하거나, 요구하는 서비스에 대한 정당성을 확인하는 사용자 신분확인 메커니즘은 컴퓨터 시스템에 대한 접근제어 및 중요 서비스 제공 여부에 대한 판단기법으로 현재 패스워드를 가장 많이 사용하고 있다. 그 외 신분확인 기법으로 생체적인 방법, 동적인 패스워드 기법 등이 있는데, 이들 중 네트웍 환경에서는 주로 일반 패스워드와 동적인 패스워드 기법이 사용되고 있다.

3. 제안 방안

3.1 익명성 보장 방안

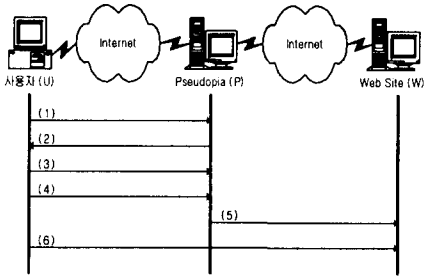
< 사용 용어 설명 >

U : 사용자, P : 제안 시스템(Pseudopia), W_i : 웹사이트, T : time stamp, ID_u : 주 사용자 id,

PW_u : 주 패스워드, ID_{wi} : i 사이트 접속용 id

PW_{wi} : i 사이트 접속용 패스워드

3.1.2.1 사용자 등록 및 로그온 절차



<동작 설명>

(1) 사용자 U는 Pseudopia에 회원으로 가입.

(2) 사용자 U는 Pseudopia에 ID_u 를 등록

(3) U는 Pseudopia를 경유 W_i 에 계정등록을 요청.

(4) 새로운 사용자 id ID_{wi}와 패스워드 PW_{wi} 등록

1) P(ID_u,W,T) --> ID_{wi}생성.

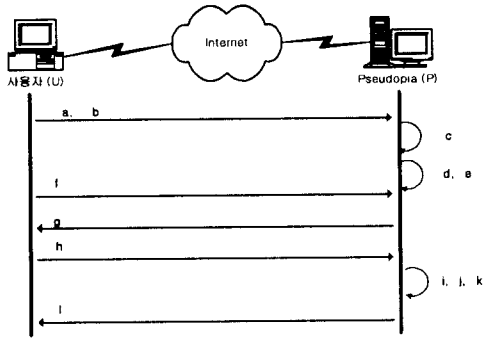
2) P(PW_u ,W,T) --> PW_{wi} 생성

* 이때 반드시 DB에 T를 안전하게 보관

(5) U는 P(ID_{wi} , ID_{wi}) send to W

3.2 개인 엔트로피 기반 신분확인 방안

<질문의 입력>



a. n개의 질문 $(q_1,\cdots,q_n)$을 생성하여 n개의 대답 $(a_1,\cdots,a_n)$을 서버에 보낸다.

b. 이 때 salt 값으로 r_s 를 생성한다

c. 각 질문과 대답 그리고 랜덤 수를 연결하여 해쉬

$$h_1=H(q_1+a_1+r_s),\cdots,h_n=H(q_n+a_n+r_s)$$

를 하여 $s_1,\cdots,s_n$을 생성한다.

d.암호화 $(E_{h_1}(s_1)=c_1,\cdots,E_{h_n}(s_n)=c_n)$

e. $(q_1,\cdots,q_n,r_s,c_1,\cdots,c_n)$을 안전하게 보관

<비밀번호 변경 시>

a. n개의 질문$(q_1,\cdots,q_n)$을 사용자에게 묻는다.

b. 사용자는 대답 $a_1',\cdots,a_n'$을 대답한다.

c. 각 질문과 대답 그리고 랜덤 수를 조합하여 해쉬

$(h_1'=H(q_1+a_1'+r_s),\cdots,h_n'=H(q_n+a_n'+r_s)$

d. $(D_{h_1'}(c_1)=s_1',\cdots,D_{h_n'}(c_n)=s_n')$를 복호화

$$h_1=H(q_1+a_1+r_s),\cdots,h_n=H(q_n+a_n+r_s)$$

를 얻는다.

e. 이 때 질문에서의 "c "의 결과와 비교한다

f. 복호된 결과에 대한 정답이 원하는 엔트로피에 도달하면 비밀번호 변경을 허락한다.

3.3 2 가지 방안을 결합 새로운 방안

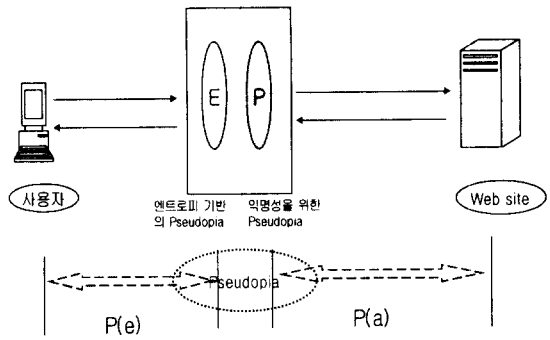
본 절에서는 위에서 설명된 두 가지 방안을 결합한 새로운 방안을 제안한다. 인터넷 가상세계에서 개인의 계정은 신분이며, 계정의 익명성은 신분의 익명성으로 직결되므로, 이를 통한 개인 프라이버시의 보호가 가능하다.

제안방안에서는 주 패스워드인 PW_u를 이용하여 다중의 패스워드를 생성한다.

<사용 용어 설명>

P(e) : 엔트로피를 위한 Pseudopia

P(a) : 익명성 보장을 위한 Pseudopia



<그림 8> 두 방식을 결합한 시스템 구성도

<Figure 8> Configuration for Combined Pseudopia

(동작 방식)

(1) 익명성 보장을 위한 Pseudopia

1) P(ID_u, W, T) = ID_{ui} 웹사이트에 제공.

2) P(PW_u, W, T) = PW_{ui} 웹 사이트에 제공

3) 1), 2)를 통한 Anonymous web browsing

(2) 개인 엔트로피 기반의 신원확인

1) 질문과 대답의 SET을 DB에 안전하게 저장

2) 엔트로피 기반 본인 확인

4. 시스템 확장성 및 평가

4.1 익명성 보장 방안의 안전성 평가

-사용자 ID_u 와 PW_u 추측

사용자 ID_u와 패스워드 PW_u 는 사용자가 모든 제안시스템을 통하여 웹사이트에 접속하는 모든 계정정보를 알 수 있기 때문에 추측이 불가능해야 하며, 본 논문에서는 일 방향 해쉬 함수를 사용하여 이 문제를 해결하였다.

- 사용자 id 및 패스워드 충돌

Pseudopia를 통하여 동일한 웹사이트에 중복되는 id와 패스워드가 생성되어서는 안되며, 이를 위하여 본 논문에서는 서로 다른 사용자가 우연히 동일한 ID_u 와 PW_u를 지정하더라도 salt (time stamp)

T에 의해서 중복을 피할 수 있도록 설계되었다.

- Pseudopia의 역할에 따른 안전성 고려사항

Pseudopia에서는 사용자가 패스워드를 변경하여 접속한 최근의 시스템 타임 스템프만 사용자 데이터로 보관하고 있으며, 이 정보도 암호화하여 안전하게 저장되어 있다.

4.2 질문의 개수와 엔트로피와의 상관관계

질문의 개수를 n이라 하고 정답의 개수를 t라고 할 때, 한 질문에 대한 경우의 수는 256가지를 넘는다. 그리고 128bit의 키 길이를 가지는 암호문을 해독하기 위해 키를 알아내기 위한 무작위 공격법에 필요한 경우의 수는 2^{128}이다. 따라서, 256가지 경우의 수를 가지는 질문을 t개 맞추면 2^{128}을 만족한다고 할 수 있다. 이 때의 $t=16$이다. 한편, 한 질문을 이용자 본인이 맞출 확률을 P_0라 하고, P_0를 0.95라고 가정하자. 그리고 이용자가 전체 질문에 대한 엔트로피를 통과할 확률을 P_2라 하고, P_2를 0.99998이라고 둔다. 정당한 사용자가 k개의 정답을 했다면

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

위에서 $t=16$ 이므로

$$P_2(t,n,P_0)=\sum_{i=t}^{n}P_1(1-P_0) \quad (2)$$

(1)과 (2)에서 $P=0.99998$을 만족하는 n을 찾으려면 (n,t) 표에서 $n=24$가 된다.

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

5. 결론

본 논문에서는 가상공간에서 사용자 인증의 필요성과 계정 관리의 문제점 그리고 인터넷상에서 프라이버시 보호를 위하여 익명성이 필요함을 주장하였다. 제 2장에서는 기존의 프라이버시 보호대책과 본인 인증기법에 대한 조사를 하였으며, 제 3장에서는 개선된 사용자 계정관리 방안과 프라이버시 보호대책 그리고 개인 엔트로피를 이용한 사이버 공간에서의 본인확인 방안에 대한 제안 시스템의 설명을 하였고, 제 4장에서는 익명성 보장방안의 안정성과 개인엔트로피에 기반한 사이버 공간에서의 신분확인 기법에 대한 평가를 하였다.

인터넷에서 개인 프라이버시의 침해는 심각한 수준이며, 시스템 관리자의 의도에 의해 무차별적으로 이루어지고 있는 실정이다. 바람직한 사용자 계정관리 정책과 패스워드 관리방안, 사이버 공간에서의 신분확인 기법 등은 인터넷에서 가치이전을 수반하는 주요 정보 전달에서는 매우 중요한 요소이며, 제안 시스템이 많은 도움을 줄 수 있을 것이다.

개선되어야 할 사항으로 엔트로피 기반에서 보다 쉽고 효율적으로 질문을 생성하고 질문의 개수를 줄여 사용자의 편의를 제고하는 방안이 필요하며, 개인 프라이버시 보호 시스템에서 주 패스워드가 변경되었을 경우 자동으로 모든 가입된 사이트의 패스워드를 변경할 수 있는 메카니즘이 필요하다.

본 논문은 익명성이 보장되는 계정관리 기법을 제안하였고, 이로 인하여 개인 프라이버시가 보호되었으며, 궁극적으로 가상공간에서 개인 엔트로피에 기반한 새로운 형태의 신분 확인 방안을 제시하였다.

[참고문헌]

[1] S. Garfinkel, G. Spafford. Web Security and Commers. O'Reilly & Associates, 1997, p.92~98, 1997

[2] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM.

[3] E. gabber, P. Gibbons, Y.Matias, and A. Mayer. how to make personalized web browsing simple, secure, and anonymous. Internet proceedings of Financial Cryptography '97. 1997.

[4] Warwick Ford, "Computer Communication Security", Prentice-Hall, 1994

[5] J. Reagle and L. Cranor. The platform for privacy preferences Communications of the ACM

[6] P. F. Syverson, D. M. Goldschlag, and M. G.

Reed. Anonymous connections and onion routing. In Proceedings of the 1997 IEEE Symposium on Security and Privacy

[7] Proceedings of the IEEE International Conference on Image Processing 1997, 1998

[8] N. Memon, P.W.Wong, "Protecting Digital Media Content," Comm. of the ACM, Vol.41, No.7, pp.35-43, 1998

[9] M.D.Swánson, M. Kobayashi and A. H. Tewfik, "Multimedia Data-Embedding and Watermarking Technologies," Proc. of the IEEE, Vol. 86, No.6, pp.1064-1087, 1998

[10] R. Anderson Ed., "Information Hiding," in Lecture Notes in Computer Science, Vol.1147, Springer, 1996

[11] R.Anderson and F.A.P.Petitcolas, "On the Limits of Stegangoraphy," IEEE JSAC, Vol. 41, No.7, pp.474-481, 1998

[12]松井甲子雄, "電子透かしの基礎", 森北出版株式會社, 1998(in Japanese)

[13]W. Bender, D. Gruhl, N.Morimoto and A Lu, "Techniques for Data Hiding," IBM Syst. J., Vol. 35, pp.313-336, 1996

[14]N. Nikolaidis, I. Pitas, "Copyright Protection of Images Using Robust Image Signature," In proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, pp.2168-2171, 1996

[15] Carl Ellison, Chris Hall, Randy Milbert, Bruce Schneier, Protecting Secret Keys with Personal Entropy

[16] www.anonymizer.com

[17] 今井秀樹(Hideki Imai) 著 암호이야기