사용자 질의어를 이용한 개인 인증 보안 알고리즘★

이창조*

요 약

개인 인증 보안은 온라인 시스템에서 사용자 인증 서비스를 사용하기 위한 중요한 수단이다. 본 논문에서는 사이버테러 대응 목적으로 온라인 인증서를 효율적으로 활용하는 방법의 일환으로 이 논문에서 설계한 SOL이라 불리는 알고리즘을 온라인 전자거래 인증에 적용하기 위한 방법을 설계하고 구현해 보았다. 이 결과는 각종 인증서의 효율적인 관리와 활용을 통해서 정보화 시대의 근간을 이루고 있는 온라인 인증에 대한 서비스를 보다 효율적으로 이용할 수 있을 것이다. 특히 SOL은 특정 목적을 지니고 운영하는 소규모 단위의 온라인 시스템에 호환성을 가지도록 효율적으로 접목시켜 상호 호환하여 사용할 수 있음을 본 논문을 통해서 알 수 있게 된다.

Algorithm of certificate security based-on using query language

LEE Chang-Jo*

ABSTRACT

Certificate security oriented cyber certificate is important tool for the purpose of offering user-authentication service based on on-line system. In the paper, we analyzed management implement which could make the efficient use of certificate security oriented cyber terror response. This algorithm called SOL(Security Oriented Language) will make efficient use of the service about authentication consisting of the basis in the age of information through efficient management and partial use of each certificates. Especially, SOL could be used efficiently by grafting a small group of on-line system which is operated with particular purposes.

Key words : Certificate security, Certificate Algorithm.

접수일(2011년 11월 16일), 수정일(1차:2011년 12월 09일), 게재확정일(2011년 12월 14일)

★ 본 논문은 영산대학교 교내연구비 지원에 의하여 연구되었음.

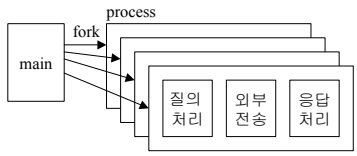
* 영산대학교 자유전공학부

1. 서 론

온라인 공간에서 해당사이트에 접속을 시작하기 전에는 항상 인증과정을 거쳐야 하며 개인정보 보안의 위험을 감수하면서 접속이 시작된다. 흔히 ID나 패스워드를 입력함으로써 저장되어 있던 데이터베이스와 매칭되어 접근이 가능하게 된다. 이에 본 논문에서는 온라인 공간에서 개인 인증을 통한 접속시에 철저하고 개인 정보에 관한 질의어의 비밀번호를 보다 쉽고 질의어를 매우 까다롭게 설정하여 타인에게 유출되지 않도록 하는 유저인터페이스를 설계하는 것이 그 목적이다. 현재 많이 사용되고 있는 인증 형태는 One-Time password의 형식으로 사용되고 있으며[1] 이는 한가지의 암호로 계속해서 사용함으로써 그 허점이 노출되기가 쉽다. 한번 접속한 비밀번호는 처음 접속 이후부터는 인증 데이터, 보통 비밀번호의 입력 없이 서비스를 사용할 수 있도록 해주는 서비스가 SSO[3] 인데 이것이 가능하기 위해서는 획득한 티켓과 함께 세션키 또는 세션키를 복호화 할 수 있는 사용자의 키가 평문 형태로 시스템에 저장되어 있어야 한다[2]. 그러나 이 경우 공격자가 합법적인 사용자의 시스템을 제어할 수 있게 되면 아무런 노력 없이 해당 사용자로 위장하여 서비스를 사용할 수 있는 보안 허점을 지니게 된다. 이런 이유 때문에 본 논문에서 제안하고 구현한 시스템인 SOL(Security Oriented Language) 알고리즘은 편리성을 갖추고 보안성과 안전성을 높이기 위해 SSO서비스는 제공하지 않으며 접속 때 마다 비밀번호를 입력해야 하는 번거로움은 존재하지만 매번 질의어에 따라 입력하도록 설계되어져 있다.

본 논문에서 설계하고 구현한 SOL의 알고리즘은 일반적인 인증형태가 동일 응용 서버 뿐 만 아니라 응용 서버에 대해서도 SSO 서비스를 제공하기 위한 수단으로 사용되고 있으므로 본 시스템은 이러한 비밀번호의 단점을 해소하기 위한 방안으로서 한 화면에서 상속되는 윈도우 형태의 실행결과를 볼 수 있도록 그 도구를 개발하였고 이것을 이용하여 실행해 봄으로써 실제 네트워크 또는 온라인, 오프라인 상에서도 적용할 수 있도록 설계 되었으며 특히 매번 접속 시에는 무조건 변하는 개인 인증 보안을 사용하여 보다 강화되고 보안이유지되는 알고리즘 기법을 구현한 것이다.

본 논문에서 사용된 온라인 개인 인증 보안 SOL 알고리즘의 처리과정은 다음 (그림 1)과 같이 질의처리부분, 외부전송부분 그리고 응답처리부분으로 크게 나뉘어 진다.

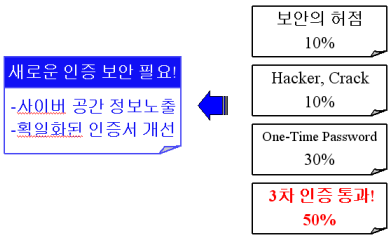


(그림 1) SOL 알고리즘의 처리 과정

여기에서 외부 전송부분은 주 화면으로 다시 돌아가도록 구성되었다. 왜냐하면 각 서버의 접속허용과 개인 정보의 공개 보호[4][5]로 인한 접근이 불가함으로 단지 원래의 화면으로 돌아가는 것으로 외부 전송이 완료 되었다고 가정을 하고 있기 때문이다. 그 처리 과정은 질의처리, 외부전송, 응답처리[6]의 순으로 진행된다.

2. 사이버 인증 인터페이스 설계

본 논문에서 제안하고 설계한 온라인 유저 인터페이스는 온라인 상이나 사이버 공간 및 인터넷 뱅킹과 스마트폰 뱅킹, 텔레뱅킹등의 사용자들을 위한 설계로서 보다 쉽게 접근하면서 타인이 도용할 수 없도록 개인의 보안[7]이 철저히 될 수 있는 보안도구를 구현해 보고자 알고리즘을 설계하여 구현해 보았다. 이러한 아이디어는 온라인 공간에서 매일 접속되는 ID와 비밀번호입력, 그리고 인터넷 PC 뱅킹을 자주 사용하던 중에 보안의 허점이 노출되면서 고찰하게 되었고 가능한 기존의 데이터베이스[8]를 활용하여 사용할 수 있게 하는 메커니즘을 설계하게 되었으며 한번으로 통과되는 비밀번호 형태[9]를 벗어나 새로운 질의어의 응답으로 인증을 하고자 설계하였다. 다음 (그림 2)는 새로운 인증 보안의 필요성에 대해 고찰한 그림이다.



(그림 2) 새로운 인증 보안의 필요성

2.1 SOL 알고리즘의 설계

본 논문에서는 온라인 사이버 인증 보안 알고리즘을 적용하기 위해 독립적으로 구현되었다. 여기에서 설명되는 툴과 방법은 사용자의 전체 인증 보안 프로그램에 추가될 수 도 있고 응용하여 합해질 수도 있다. 매번 질의어가 바뀌어 2단계로 통과되는 SOL 알고리즘은 다음과 같다. 개인정보의 데이터베이스를 입력하고 삽입되는 정보를 위하여 질의어에 맞게 통과시키는지를 검사한 후 사용자와 질의어의 구간을,

L = {1단계의 질의어}
M = {2단계의 질의어}
H = {통과 질의어} 와 같이 정의하고,

s1, s2 그리고 s3은 사용자 데이터베이스의 개인정보 키이고 p는 질의어에 매칭되는 비밀번호이며 AH는 질의어의 헤더로 정의하여 통과되어 필터링 하는 알고리즘의 코드이다.

```
input PIN
save PIN DB
while (process SOL query)
{     scan (1'st query of SOL)
      if a query is 1'st query
        answer password(kind of number 4 digit)
        {  passing : check (s1, s2, s3, p, AH)
                     save s1 ,s2, s3
                     pass a query
           information : calculate (security level)
            switch (security level)
             { L : pass random 1 st query
                   extract (password of query)
                   check (s1, p, AH)
                     if not validate
                       try again 3 times
                     else system exit
               M : pass random 2'nd query
                   extract (password of query)
                   check (s2, p, AH)
                     if not validate
                       try again 3 times
                     else system exit
               H :  pass random last query
                   extract (password of query)
                   check (s3, p, AH)
                     if not validate
                       try again 3 times
                     else system exit
                   notify SOL DB manager
      else drop the last query
} } }
```

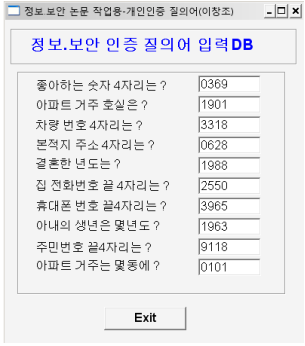
2.2 SOL 알고리즘의 구현 방법

본 논문에서 사용한 툴은 파워빌더 버전으로서 보다 강력한 개인 인증에 관한 데이터베이스가 요구되므로 본 논문에서도 클라이언트/서버용 도구[10]를 개발하여 새로운 인증 보안 알고리즘에 적용하고자 하였다. 작업이 원활히 작동되도록 작업을 하여야 한다. 본 시스템 툴의 구현 환경은 다음 (그림 3)과 같다.

(그림 3) SOL 알고리즘의 구현 환경

본 논문에서 작성하는 메뉴나 윈도우는 독립적으로 구성되는 모듈로 오브젝트 단위로 구성하였으며 이 오브젝트는 각각의 특성과 프로퍼티, 이벤트, 함수를

가지고 구성하였다. 가령 이메일의 ID나 비밀번호[11]와 같은 입력 형태이지만 첫 번째 질의에 대한 응답을 한다는 점이 그 초점이다. 특히 두 번째 질의어도 같은 방식으로 수시로 바뀌게 되어 있어 다음과 같은 10가지의 질문들이 무작위로 추출됨으로 키보드해킹[12]이나 타인으로부터 도용되는 것을 방지하고자 방화벽[13]이 설계되고 구현되어져 있다. 본 논문에서는 다음 (그림 4)와 같이 10가지의 개인 데이터베이스를 가지고 SOL의 질의어가 설계 되었다. 물론 이 질의어는 사용자가 임의로 바꿀 수 있도록 하였다.



(그림 4) 개인 신상에 관한 입력항목

이 질의어에서는 일부항목을 제외하고는 대부분의 항목이 공격자 입장에서 쉽게 알아낼 수도 있겠지만 이 질의어에 관한 데이터베이스는 개인이 직접 작성하여 입력하도록 설계 하였다. 이 논문에서는 이해를 돕기 위해 가급적 쉬운 질의어를 작성해 놓았으므로 사용자는 타인이 전혀 알 수 없는 어려운 질의어를 수시로 변경, 수정 가능하도록 설계되어져 있다. 가령 주민번호 끝 4자리는? 같은 질의어는 주민등록등본만 노출되면 4자리의 비밀번호를 쉽게 도용할 수 있겠지만 사용자는 위의 질의어를 바꾸어 “아버님의 제사 날짜 4자리는?” 이라고 수정한다면 본인 외에는 알 수 없는 정보일 것이다. 이와 같이 10개의 질의어를 본인만 알 수 있는 정보들로 작성하여 그 중에서 무작위로 질의어가 바뀌도록 하여 타인의 도용이 불가능 하도록 구현하였다. 또한 본 논문에서는 숫자 4자리를 입력하도록 한 것은 현재 은행권에서는 일반적으로 4자리의 숫자를 비밀번호로 사용하고 있어 이와 데이터베이스의 호환성을 갖기 위해 4자리로 설계하였다. 앞의 자리수가 4자리 보다 작으면 0으로 처리하도록 설계 되었고 가능한 개인 데이터베이스를 작성할 때에는 4자리의 형태로 입력하도록 이 시스템에서는 권장하고 있다.

위의 10개 질의어 중 무작위로 두 번째까지의 질의어가 모두 통과되어야만 다음의 진행과정에 진입할 수가 있다. 즉, 여기에서 온라인 공간이나 사이버, 텔레뱅킹, 이메일 등과 연결하여 진입 가능하게 스크립트를 작성해 주면 여러 형태에서도 응용이 가능하다고 하겠다[14].

이런 질의어들이 구성되고 개인 데이터베이스에 저장되면 유동적이고 무작위로 질의어가 제시되며 3회 이상 입력오류가 생길 시에는 시스템을 빠져 나오도록 설계 되었다.

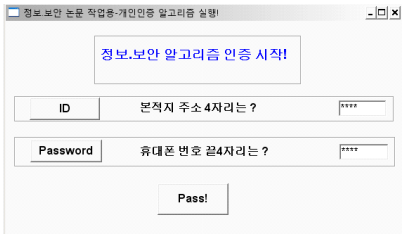
3. SOL 알고리즘의 구현 결과

다음은 본 논문에서 설계하고 구현한 SOL알고리즘을 적용하여 개인 데이터베이스의 질의어에 대한 구현 결과를 살펴본다. 이 시스템을 응용하면 온라인 사이트에서 ID와 비밀번호를 대체하여 개인 인증서로 형태로 사용할 수 있도록 설계되었다. 다음 (그림 5)는 현재 온라인 상에서 일반적으로 사용되고 있는 개인 인증의 입력형태이다. 이것은 한번 사용하면 번거롭다는 이유로 계속해서 똑 같은 ID나 비밀번호를 그대로 사용하고 있는 것이 일반적인 실정이다.

(그림 5) 온라인 상에서 일반적인 로그인 형태

본 논문에서 구현한 알고리즘은 위의 (그림 5)에서의 입력방법을 다음 (그림 6)에서와 같이 개인 인증에

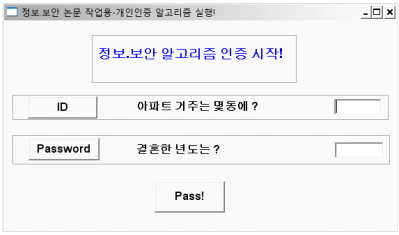
관한 데이터베이스를 미리 10개 정도 입력해 놓고 이 질의어 중에서 무작위로 ID나 비밀번호를 대체하게 되어 도출하게 되는 알고리즘으로 다시 로그인시에는 또 다른 질의어가 도출되어 타인이 도용하지 못하도록 하는 것이 이 시스템의 핵심이라 할 수 있다.



(그림 6) SOL의 첫 번째 구현 결과

이 시스템은 유선, 무선, 모바일 네트워크[15]에서 모두 사용 가능하도록 설계되어 졌으며 현재 로그인하고 있는 모든 형태에 적용 가능하도록 하였다.

다음 (그림 7)은 또 다른 질의어가 생성되는 두 번째 실행결과를 보여주고 있다. 질의어가 매번 접속때마다 다른 질의어가 도출됨으로서 타인이 최근 ID와 비밀번호를 도용했다 하더라도 그 다음 로그인에서는 질의어에 맞는 비밀번호를 맞게 입력하는 것은 거의 불가능 하다고 할 수 있다. 또한 이 질의어가 노출된다는 가능성이 존재하면 곧바로 개인 질의어를 다시 데이터베이스에 입력하여 타인이 알 수 없는 정보들을 이용하여 작성해 놓으면 보다 안전한 로그인을 할 수 있다.



(그림 7) SOL의 두 번째 구현 결과

본 논문에서 온라인 사용자들의 질의어를 사용하여 사이버테러에 대응하거나 사이버범죄에 대응하고자 좀 더 개선된 개인 인증의 보안 알고리즘을 적용하여 실제로 사용할 수 있도록 설계하였으며 각 질의어는 순차적인 것이 아니라 랜덤(무작위) 함수를 이용하여 10개의 질의어 중에서 무작위로 선택된 첫 번째 질의어와 두 번째 질의어가 현재 사용하고 있는 ID와 비밀번호 입력창을 대신하여 입력하도록 하고 있다.

4. 결론 및 향후과제

본 논문에서 설계한 온라인 유저인터페이스는 고정되고 획일된 계정이나 사용자암호의 입력형태를 벗어나 새로운 알고리즘을 적용하여 온라인 상에서 사용하도록 개선된 인증 보안 알고리즘을 설계하고 구현해 보았다. 본 논문의 시스템인 SOL 알고리즘을 적용하여 얻어지는 기대효과로는 다음과 같다.

① 온라인 사용자를 위한 개인 인증 보안의 연계로 인한 인증 강화 효과
② One-Time Password대신 2단계의 유동 질의어로 개인 인증 보안의 강화 효과
③ 사이버상의 온라인 인증서의 ID와 비밀번호 둘 다 적용 가능 효과
④ 사이버 공간에서의 모든 개인 인증 사용, 인터넷, 보안이메일 로그인시 보안 효과
⑤ 인터넷뱅킹 및 사이버테러 범죄에 대한 사전 차단 효과
⑥ 인터넷뱅킹 보안카드의 분실 및 타인의 정보 도용에 대비한 해킹 차단 효과
⑦ 은행 데이터베이스를 그대로 사용(4자리)함으로 호환성을 가진 비용 절감 효과

본 논문에서 설계하고 구현한 SOL 알고리즘의 향후 연구 과제는 예외적인 경우에 대한 대비로서 건망증 보유자 및 비밀번호의 연속된 입력 오류등으로 인한 문제도 고려하여 사이버 인증의 처리방안에 대해서도 새로운 알고리즘이 적용되는 연구도 병행하여 진행되어야 할 것이다.

온라인 상에서의 개인 인증에 대한 사이버 테러에 대응하고 인증서의 보안적인 측면에서 타인이 도용할 수 없도록 하는 것이 본 논문의 핵심이라 할 수 있으며 온라인 상에서와 무선 모바일, 스마트폰 등 인증

시스템이 필요한 곳에는 호환가능하도록 하여 모두 적용이 가능하도록 하는데 필요충분조건을 제기하게 한다.

본 논문에서 설계하고 구현한 SOL알고리즘의 실제 활용이 가능한 부분은 현재 사이버 공간상에서 로그인 하는 형태의 암호방식이나 은행뱅킹에서 사용되는 4자리의 비밀번호 입력방식 및 스마트폰이나 무선 인터넷 로그인 방식에서 호환하여 사용가능 할 수 있도록 하였으나 사용자의 편의성도 최대한 고려하여 기억할 수 있는 범위 내에서 가장 어려운 질의어를 구성하는 방법도 강구되어야 할 과제이다.

참고문헌

[1] 이창조,김상복 “차세대 사이버 인증 보안을 위한 알고리즘의 설계 및 구현에 관한 연구”, 한국사이버테러정보전학회, 정보.보안 논문지, 제6권 제3호 pp.69~78, 2006.

[2] Naomaru Itoi, Tomoko Fukuzawa, Peter Honeyman, "Secure Internet Smartcards", 2000.

[3] Imprimerie Nationale : Projet de Loi de Finances pour 1995, Etat de la Recherche et du Developpeonent Technologique, Paris, 1994.

[4] Qinzheng Kong, Graham Chen, Rubina Y. Hussain, “A Management Framework for Internet Services", Citr Technical Journal Vol.3. pp 47-55.

[5] James D. Allen, Patrick T. Gaughan, David E. Schimmel, and S. Yalamanchili, "Ariadne -an adaptive router for fault- tolerant mulicomputers," Proceedings 23st Int'l Symp. on Computer Architecture, pp. 278-288, April. 1994.

[6] J. Duato, P. Lopez, F. Silla and S. Yalamanchili, "A high performance router Architecture for interconnection networks," 1996 International Conference on Parallel Processing, pp. 61-68, 1996.

[7] Marcus J.Ranum, "Thinking About Firewalls", Proceedings of Second International Conference on Systems and Network Security and Management, April, 1993.

[8] M. Chatel, "Classicial versus Transparent IP Proxies", RFC:1919, Mar. 1996.

[9] N.haller and C.Metz, "A One-Time Password System", IETF RFC 1938, 1996.

[10] Phil Karn, Neil M.Haller, and John S.Walden, Bellcore, S/Key software kit, available via anonymous FTP from thumper.bellcore.com: /pub/nmh/skey/*.

[11] Stephen T. Kent, "Internet Privacy Enhanced Mail(PEM)", Communications of the ACM, August, 1993.

[12] ANSI X9.62, The Elliptic Curve Digital Signature Algorithm(ECDSA), Draft Standard, 1997.

[13] Winfield Treese and Alec Wolman, "X Through the Firewall, and Other Application Relays, "Cambridge Research Lab. Technical Report 93/10, Digital Equipment Corporation, May 3, 1993.

[14] Akyildiz I. F, J. Mcnair, J. Ho, H. Uzunalioglu, W. Wang, "Mobility Management in Current and Future Communications Networks," IEEE Network, July/August 1998.

[15] Elnahas A, N. Adly, "Location Management Techniques for Mobile Systems," Information Sciences, 130, 1-22, 2000.

[저 자 소 개]

이 창 조 (LEE Chang-Jo)

1989년 중앙대학교 대학원
전자계산학과
S/E전공(이학석사)
1993년 프랑스 파리 소르본느 VI대학
인공지능학전공(박사수료)
1998년 경상대학교 대학원
전자계산학과
NCS전공(공학박사)
2009년~2010년:영산대학교
학부대학 학부장
2011년~현재 :영산대학교
자유전공학부 교수

email : Lcj7311@ysu.ac.kr