임베디드 시스템과 전자상거래에서 함수형 패스워드방식의 사용자 인증 및 보안 방법에 대한 연구

이 은 서[†] · 문 호 영[††] · 이 상 호[†††]

요 약

100여 년 동안 사용자 확인의 한 축을 담당해오던 비밀번호가 비대면 거래가 활성화 되면서 점차 제 기능을 다하지 못하여 이제 바뀔 때가 되었으며, 그 한 방편으로써 간접패스워드인 브레인키를 패스워드시스템에 적용하면 사용자의 패스워드의 해킹 등 다양한 유출 경로가 없으므로, 보다 안전한 전자 상거래를 활성화시킬 수 있다. 비밀번호는 현대인에게 있어서 생활필수품이므로 이에 대한 독점적 지위와 시장선점은 중요한 의미를 갖는다. 또한 비밀번호에 대한 문제는 국내에 국한 되지 않으므로 국내의 상업성은 일개 기업에 국한 되지 않고 국제표준화를 선도할 수 있으므로 국가적 이익에도 부합된다. 본 연구에서는 전자상거래에서 발생하는 보안 솔루션을 제시하고자 한다.

키워드 : 전자상거래, 보안 방법, 함수형 패스워드

A Study for Method of the User Authentication and Security apply to the Type of Function password in the Embedded System and Electronic Commerce

Lee Eun Ser[†] · Moon Ho Young[††] · Lee Sang Ho[†††]

ABSTRACT

Password, a traditional user confirmation method that is used for more than 100 years, has become useless as a lot of transactions are dealt by indirect contacts. As a result, an alternative for password is required now. In this paper, we propose a novel confirmation method, which is called Brain-Key. It uses an indirect password input method. It reduces the risks due to hacking, and prevents a big credit accident because it prevents passwords to be reused. Our proposed model has general applicability so that it can be applied in domestic market as well as international markets. This research may provide solutions for the security problems in the electronic commerce.

Key Words : Electronic commerce, Security method, Function password

1. 연구배경

새로운 정보산업의 방향은 정보통신연구의 발전과 함께 정보의 생산, 유통, 소비에 이르는 사이버경제 구축에 열을 올리고 있으며, e-business라는 새로운 패러다임을 창출하기에 이르렀다. 그러나 현실 세계에서도 그러하듯이 사이버 경제의 안전과 신용에 대한 믿음이 없이는 사상누각에 불과한 일이 될 것이며, 다른 사이버 영역에 있어서도 공통적인 문제임에 틀림없을 것이다. 단순히 보안연구를 도입하고 보안솔루션을 설치하는 것도 중요하겠지만, 우선 그것이 왜 필요한지를 생각하고 이해하는 보안 마인드를 가지는 것이 급선무일 것이다[1].

※ 본 연구는 서울시 산학연 협력사업(10581 cooperate Org 93112)의 지원에 의하여 수행되었음.
† 종신회원 : 숭실대학교 정보미디어기술 연구소 연구 교수
†† 정 회 원 : ㈜패스허브 대표
††† 종신회원 : 숭실대학교 컴퓨터학부 교수
논문접수 : 2007년 3월 15일, 심사완료 : 2007년 5월 15일

전자금융거래가 활성화되면서, 신용카드 분실 및 위조, 비밀번호 노출로 인한 금융사고가 빈번하게 발생되고 있다. 본인을 확인할 수 있는 방법으로 비밀번호가 가장 적당하고 유일하다. 이렇듯 본인확인의 최종수단인 비밀번호가 노출이 된다면 이로 인해 대형금융사고가 발생할 수 있는 위험성이 항상 내포되어 있다. 때문에 비밀번호 관리의 중요성은 더욱 커져가고 있다.

일반적으로 비밀번호 외우는 모든 통장이나 신용카드 비밀 번호를 하나로 만드는 경우가 많다. 만약 이렇게 하다가 비밀번호가 누출된다면, 그 책임은 전적으로 소비자 (사용자) 져야 한다[2].

사용자는 ATM과 같이 공개된 장소에서 비밀번호를 사용하거나 모바일 기기나 인터넷 등 통신상에서 비밀번호를 사용한다.

공개된 장소에서의 비밀번호 사용은 훔쳐보기의 대상이 될 수 있고 통신상에서의 비밀번호 사용은 스파이 프로그램 등 해킹의 대상이 되어 소비자는 항상 정보 유출 위험에 노

출되어 있다고 볼 수 있다[6][7].

금융기관에서는 인터넷뱅킹, 폰뱅킹, 펌뱅킹, 사이버 트레이딩, 자동화 기기 전자 지갑 등 첨단 금융서비스를 통한 고객과의 비대면 거래 시 고객의 과실이나 정보누출로 인한 금융 사고를 방지하기 위해 키보드보안, 보안카드 및 공인인증서를 도입하는 등 2중 또는 3중의 안전장치를 마련하고 있다. 더 나아가 사용이 번거롭고, 사용할 수 있는 장소도 제한이 있는 보안카드(Security Card)를 대체하기 위해서 1회용 비밀번호 방식인 OTP의 도입이 진행 중이다.

그러나 기존 OTP는 휴대형 기기방식으로 도입을 위한 비용도 만만치 않거나 분실 시 여전히 비밀번호의 노출에서 자유로울 수 없다.

함수형 패스워드 브레인키는 이러한 단점을 개선한 간접 패스워드 방식 비밀번호 인증 솔루션으로 기존 OTP의 휴대 불편을 해소하고 저렴한 솔루션이다.

최종적으로 브레인키는 1회용 비밀번호 방식을 좀 더 쉽고 편리하게 활용하도록 한 방식이라고 할 수 있다.

따라서 본 연구에서는 전자상거래에서 활용할 수 있는 암호화 알고리즘과 구현물을 소개하고자 한다.

2. 관련연구

2.1 인증

인증은 크게 두 가지의 의미로 해석할 수 있는데, 먼저 사용자 또는 메시지에 대한 인증(Authentication)과 공개키의 무결성에 대한 인증(Certification)이 있다. 전자의 경우는 일반적으로 경험할 수 있는 신분증이나 비밀번호를 이용하여 신분을 확인하는 방식으로 많은 메커니즘과 응용을 볼 수 있다. 후자의 경우는 일반적으로 경험할 수 없지만 현재 전자상거래 등에 필요한 공개키에 대해 공인된 인증기관의 서명을 통하여 무결성을 보장하는 것으로 안전하게 공개키를 사용할 수 있는 기반을 마련해 준다[3, 4, 5, 11, 12, 13].

2.2 전자거래 실태 및 정부 대책

우리나라가 세계최고수준의 인터넷 이용환경을 바탕으로 인터넷에 기반한 금융거래 및 상거래 규모가 급증하였다. 그러나 지난 2005년 5월에 발생한 인터넷뱅킹 해킹사건은 전자금융, 전자상거래를 포함한 전자거래 전반에 대한 불신 초래 및 거래의 위축을 우려하여 정보통신부에서는 2005년 9월 20일 전자거래 안정성 강화 종합대책을 발표하였다[1].

2.2.1 전자거래 보안 실태 및 문제점

(1) 해킹방지프로그램 실태 및 문제점

전자거래 해킹에 악용될 수 있는 해킹프로그램에 대한 수집, 분석이 보안업체별로 진행되어 효과적인 대응이 어렵고, 저작권문제로 해킹·보안업체의 키보드입력탐지 기능을 회피하며, 보안프로그램의 어플리케이션 영역에서의 해킹방어에 한계를 노출하고 있다.

(2) 전자금융 운영·관리방식 실태 및 문제점

인터넷뱅킹에 사용하는 보안카드의 안전성을 담보할 수 없고 금융거래 비밀번호, 계좌정보의 악용가능성이 상존하며 사이버 증권 / 보험거래는 해킹에 대비가 미흡하다.

(3)전자상거래 운영·관리방식의 실태 및 문제점

대다수 쇼핑몰사이트의 키보드 해킹프로그램 제공이 미흡하고 카드사 제공 결재프로그램의 재설치 과정에서 본인 확인절차가 취약하다.

(4) 공인인증서 관리체계의 실태 및 문제점

위·변조 신분증에 의한 인증서 발급 및 해킹을 통해 입수한 신상정보로 공인인증서 재발급이 가능하다. 또한 원격제어 프로그램을 통한 공인인증서의 절취가 가능하며, 피싱 및 해킹프로그램을 통해 금융정보 및 비밀번호를 확보하기 쉽기 때문에 현재의 관리체계로는 안정성 보장하기가 어렵다.

2.2.2 분야별 세부 추진대책

(1) 해킹방지프로그램

다양한 해킹프로그램 등 인터넷 저해 프로그램을 수집·분석할 수 있는 시스템을 마련하고 관련기관 간 정보를 공유하며 해킹 프로그램의 대상이 되는 키보드 입력 정보를 보호할 수 있는 대책을 마련한다. 이를 위해 전자거래 시 상용 키로거 프로그램을 탐지 하도록 하며 인터넷 뱅킹의 전 과정에 걸쳐 암호화를 추진한다[8][9].

(2) 전자금융 운영·관리부문

(가) 인터넷뱅킹/텔레뱅킹

보안카드의 비밀번호 입력방법을 개선(35개에서 1190개로)하고, 장기적으로 일회 성 비밀번호 생성기의 도입을 추진하여 보안카드를 OTP로 전환한다. 또한 보안등급, 수준별 거래한도를 차등 적용하여 거래의 안정성을 높인다. 텔레뱅킹 시 도청방지시스템 적용을 적극 유도하며 소유주가 불분명한 전화에 의한 텔레뱅킹을 제한한다[10].

(나) 사이버 증권·보험

사이버 증권·보험 거래 시 인증서사용을 의무화 하여 개인·금융정보를 보호하고 해킹 방지프로그램을 의무적으로 제공하여 인터넷뱅킹 수준의 전자거래 안정성을 강화한다. 또한 증권·보험사의 창구에서도 비밀번호 기재를 금지하고 PIN PAD를 사용한다.

(3) 전자상거래 운영·관리부문

전자지불업체, VAN사는 고객 비밀번호 보관을 금지하고 업무상 필요한 금융정보는 암호화하여 보관한다. 카드사 제공 인증시스템은 재발급 시 SMS, 공인인증서, OTP중 하나를 사용하여 확인 후 발급하도록 절차를 강화하며 30만원이상 결제 시 공인인증서 사용을 의무화 한다.

(4) 공인인증서 부문

타인에 의한 공인인증서 재발급을 방지하기 위해 인터넷뱅킹에서 사용하는 보안카드 입력방식을 적용한다. 공인인증서 보관 시 이동식 저장장치를 이용하도록 유도하고 이동식 저장장치는 암호화 기능이 있는 제품을 사용하도록 권고한다.

3. 함수형 패스워드 브레인 키

3.1 브레인 키 인증 알고리즘의 개념

함수형 패스워드인 브레인키는 사용자와 패스워드 제어시스템 간에 사전에 약속한 함수 및 패스워드 제어시스템으로부터 제공되는 변수 값으로 계산된 값을 입력하는 것에 의해 사용자 확인을 받을 수 있도록 하는 간접적인 패스워드 입력을 통한 사용자 확인방법 및 그 장치에 관한 것으로, 종래에는 패스워드를 통해 사용자를 확인 받고자 할 때 무엇을 알고 있는지 알고 있는 것을 직접적으로 입력하는 것이 일반적이기 때문에 시행착오 법이나 추측 법을 통해 알아내거나 사용자가 사용하는 것을 지켜보면 도용할 수 있는 문제점이 있었던 바, 사용자가 패스워드 입력방법을 소정의 패스워드 제어시스템과 약속되거나 주어지는 변수로 된 함수로 등록하고, 이후 사용자 확인을 받는 시점에서 입력되는 값이 패스워드 제어시스템과 약속되거나 주어져서 정해지는 변수 값을 대입하여 사용자가 등록한 함수로 계산한 값인지 비교해서 사용자를 확인하는 것을 특징으로 하는 것으로 사용자가 입력하는 것이 본인이 알고 있는 패스워드 입력 방법에 의해 나온 결과치만 입력하며, 입력하는 내용에 식별자에 대해 사용하고자 하는 권리 행사 방법을 구분해둔 채널번호와 함께 입력하고, 응답시간 범위 내에 입력하면 도용자가 패스워드를 입력한 것을 비디오카메라를 몰래 설치하여 훔쳐본다 하더라도 도용할 수 없을 뿐 아니라 사용자의 확인이나 인증이 필요한 각종 현금자동 지급기, 신용카드 조회기, 디지털 서명, 휴대형 단말기, 전자상거래 등에서 필수적인 요소 기술로 사용할 수 있으며, 신용카드 등의 카드 류나 은행계좌, 사용자의 ID, 신분증 등에서 사용자의 권한을 효과적으로 보호할 수 있게 된다.

함수형 패스워드인 브레인키는 머리 속의 한 개의 패스워드를 간접적인 방법으로 매번 바꾸어서 입력하므로 더 자세하게는 사용자가 정상적으로 입력하는 패스워드를 지켜보아도 입력된 패스워드를 통해서는 도용할 수 없도록 패스워드를 제어하는 패스워드 제어시스템을 구성하고 이를 통해 사용자를 확인할 수 있도록 한 것에 관한 것이다.

함수형 패스워드는 변동 패스워드 방식으로 종래의 고정형 패스워드방식의 문제점을 해결하기 위해서 안출한 것이며, 그 목적이 사용자가 자신의 권리를 스스로 원하는 만큼 패스워드를 입력하는 방법을 사용자가 스스로 정하도록 하고 입력하는 단계에서부터 사용자가 식별자에 대한 권리의 표현을 할 수 있도록 하여 단지 패스워드를 입력하는 것만을 지켜보아서는 패스워드를 알 수 없도록 하며, 본인이 아니면 패스워드를 다시 사용하기 어렵도록 패스워드를 입력할 때 사용자가 등록되어 있는 계산방식을 통해 계산된 결과를 입력하는 방법, 다시 말해 사용자가 정한 변수로 이루어진 계산식이나 함수를 알고 있느냐를 직접적인 계산식이나 함수를 입력하는 것이 아니고 이를 통해 처리된 결과만을 입력하는 간접적으로 알고 있는 것을 확인하는 방법을 사용하는 패스워드 제어시스템을 구성하고 입력 결과를 해석하여 사용자를 확인하는 간접적인 패스워드 입력을 통한 사용자 확인방법을 제공하는 데에 있는 것이다. 함수는 이론적으로 논리함수를 포함하여 수학적으로 가능한 모든 함수들이 적용 가능하며 비밀번호를 상수나 단어를 입력하지 않고 변수에 의해 값이 결정되는 함수인 F(X)를 패스워드로 등록하고 입력할 때에는 입력시점에 결정되는 연산 조건 변수인 X를 대입하여 연산 조건에 의한 F(X)를 계산한 결과값Y값을 입력하므로, 관측자의 입장에서는 Y값을 보아서는 사용자가 알고 있는 F(X)를 직접적으로 알 수 없게 하는 방법이다. 즉, Y값이 나올 수 있는 F(X)는 이론적으로는 무한대이기 때문에 패스워드의 유출 위험성이 줄어든다.

3.2 용어 정의

함수형 패스워드인 브레인키는 상기의 목적을 달성하기 위하여 사용자가 본인이 알고 있는 패스워드 입력방법에 의해 나온 결과치만 입력하도록 하고, 입력하는 내용에 식별자에 대해 사용하고자 하는 권리 행사 방법을 구분해둔 채널번호와 함께 입력할 수 있도록 하며, 응답시간 범위 내에 입력하도록 하는 것을 특징으로 하는 패스워드 제어시스템을 구성하여 사용자를 확인하는 것을 특징으로 하며, 이하 그 구체적인 연구내용을 좀더 자세히 설명하면 다음과 같다.

* 식별자 : 다른 것과 변별력을 갖는 것. 즉 주민등록증, 카드, 통장, USER ID, 신분증, 차량, 디지털인감, 문서, 목소리, 홍채, 지문 등에 다른 것과 구별이 되도록 디지털화 한 것으로 카드의 경우 카드번호가 되고, 지문의 경우는 지문인식기를 통해 생성된 지문데이터나 지문관리번호가 된다.
* 사용자 : 식별자에 대해 정당한 사용권리를 가진 자
* 채널 : 사용자가 식별자의 권리 수행방법을 여러 개로 구분하여 둔 것
* 참조신호 : 시스템이 정해서 사용자에게로 보내주는 변수
* 참조변수 : 사용자가 정한 변수로써 시스템과 사용자가 공유할 수 있는 데이터로써 통신을 하지 않고 알 수 있는 것으로 년, 월, 일, 시, 분 등
* 패스워드 입력방법 : 사용자가 입력할 때 패스워드, 참조신호, 참조변수, 채널 등으로 이루어진 계산방법과 해석과 순서를 정해 입력(표현)하는 방법
* 응답시간 : 사용자가 입력방법대로 계산하여 결과를 입력하는데 까지 걸리는 시간
* 간접적인 패스워드 입력방법 : 사용자가 알고 있는 것을 등록되어 있는 내용을 그대로 입력하는 것이 아니고 방법대로 처리한 결과를 입력하는 것으로, 즉 어떤 계산식이 등록되어 있다면 계산식을 입력하는 것이 아닌 계산한 답을 입력하고, 특정시간에 특정한 것을 눌러야 된다면 특정한 시간에 특정한 것을 누르는 것으로 패스워드를 입력하는 방법

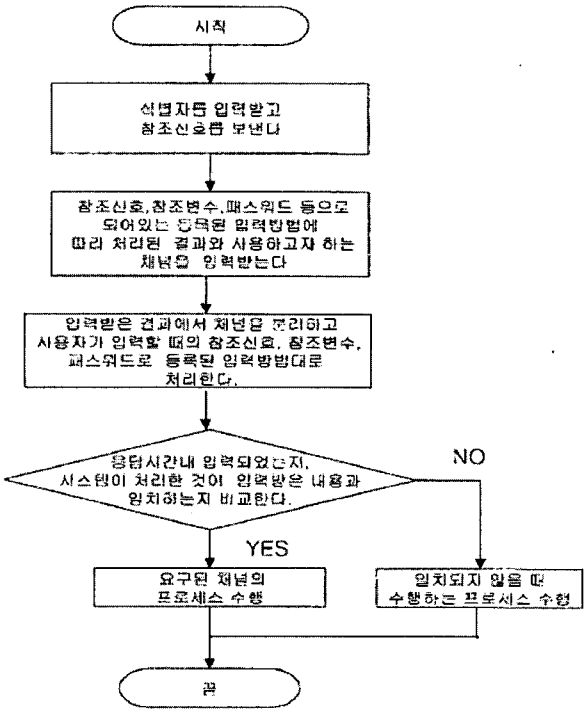
3.3 브레인키의 인증 방식 및 절차

본 연구는 기존의 사용자의 확인을 위해 패스워드를 사용하는 패스워드 제어시스템에서 사용하는 [무엇을 알고 있느냐]를 확인하는 방법에서 어떤 것을 알고 있는지를 직접 확인하는 것이 아니라 알고 있는 방법을 통해 처리한 결과만

을 입력하도록 하고, 알고 있는 것을 간접적으로 확인함으로써 사용자를 확인하는 것이다. 이와 같은 본 인증 방식을 보다 쉽게 설명하면, 예를 들어 시스템과 약속해서 알고 있는 것이 어떤 수식이라면 그 수식을 직접 입력하는 것이 아니라 해당 시스템에서 제공하는 숫자 등을 그 수식에 대입하여 계산된 결과만 입력하는 것이다. 또한 본 연구는 기존에 한 식별자에 대해 사용권한이 패스워드로 구분되지 않고 모든 권한이 모두 한 패스워드에 달려 있던 것을 사용자가 동일 식별자에 대해서도 사용권한을 채널을 통해 구분할 수 있도록 한 것이다. 이는 사용자가 가지고 있는 여러 식별자를 주민등록번호와 같은 몇 개의 식별자로 통합시킬 때 특히 유용하며, 한 번의 패스워드 통과로 모든 권한을 획득하는 위험을 줄이고, 도용자가 한 사용자의 권한을 모두 획득했는지 알기 어렵도록 하기 위한 효과적이 수단이 되는 바, 사용자 별로는 몇 개의 채널만 사용하겠지만 도용자의 입장에서는 공표된 모든 채널에 대해 점검을 해야 될 것이므로 무작위적으로 접근할 수 없는 수단으로 작용하게 된다. 즉, 일반적으로 채널의 프로세스에는 사용자의 위치를 파악해서 신고하는 채널도 있고, 권한내용을 허위로 표현하는 채널이나, 접근하는 시스템을 정지시키는 채널 등 사용목적에 따라 여러 채널을 둘 수 있으므로 도용자에게 사용자가 채널의 내용을 알려주더라도 사실유무를 확인할 수 있는 수단이 없어 도용하는 것을 저지시킬 수 있게 된다. 또한 본 연구의 다른 특징은 컴퓨터나 자동화된 로봇과 같은 장치를 통해 무작위적으로 식별자에 대한 패스워드를 알아내려고 할 때에 찾고자 하는 패스워드가 입력되었을 때도 인지하지 못하고 끝까지 수행하게 되거나 수행시간의 조정으로 무작위적으로 찾는 시간을 길게 하기 위하여 패스워드를 통해 사용자를 확인할 때에 사용자가 정한 응답시간을 지키는지 확인하는 데에 있다.

함수형 패스워드 제어시스템은 식별자(ID)에 대한 패스워드를 저장하는 패스워드저장소와, 동일 식별자에 대한 패스워드를 기본변수로 만든 수식이나 함수를 저장하는 패스워드 입력방법 저장소와, 사용자가 입력할 때 참조하는 변수를 저장하는 참조변수저장소와 참조신호를 관리하는 참조신호관리장치와, 이를 표시하는 출력장치와, 식별자에 대한 권리 행사의 종류를 정한 채널저장소와, 사용자가 결과를 입력하는 입력장치와, 입력하는 반응시간을 저장하는 반응시간 저장소와, 입력한 반응시간과 입력된 결과를 비교·해석하여 등록되어 있는 패스워드와 계산식을 알고 있는지를 확인한 후 사용자가 요구한 해당 채널의 프로세스를 수행하고 통제 및 관리하는 중앙처리장치와, 수행 시 필요한 임시저장소와, 외부와 연결되는 출력포트, 그리고 이들 상호간 신호를 주고받는 통신 선으로 구성된다.

이와 같이 구성된 함수형 패스워드 제어시스템을 통한 사용자의 확인 방법은 그림 1의 패스워드 제어시스템의 흐름도와 같이 사용자가 사용하고자 하는 식별자를 입력하는 단계, 사용자가 입력할 때 패스워드, 참조신호, 참조변수, 상수와 채널로 이루어진 계산방법과 해석과 순서를 정해 표현하는 방법에 의해 입력되어져야 할 결과를 입력하는 단계, 사



(그림 1) 사용자 확인방법 인증흐름도

용자로부터 입력된 결과를 유효한 것과 채널을 분류하고 응답시간을 계산하는 약속된 방법에 따라 재계산하는 단계, 입력된 응답시간이 사용자가 정한 응답시간내인지 판단하고 시스템이 계산한 결과와 해석하고 비교하는 단계, 결과가 맞으면 식별자에 대한 사용자를 확인한 것으로 간주하여 함께 요구된 채널의 프로세스를 수행하는 단계로 이루어지며, 사용자가 입력한 결과가 시스템이 계산한 결과와 일치하지 않을 경우는 사용자가 아닐 때 처리하는 프로세스를 수행하는 단계를 포함한다.

다음 과정으로 패스워드 입력방법을 설정하는 방법에 대해서 설명한다.

등록된 패스워드가 10진수로 되어 있고 N자리로 되어 있으면 패스워드 P는

$$P = P_0 \times 10^0 + P_1 \times 10^1 + ... + P_{N-1} \times 10^{N-1} + P_N \times 10^N$$

채널번호 Ch는 Ch = { Ch1, Ch2, ... }
참조신호가 10진수 N자리로 되어 있으면

참조신호 S는

$$S = S_0 \times 10^0 + S_1 \times 10^1 + ... + S_{N-1} \times 10^{N-1} + S_N \times 10^N$$

참조변수 V를 날짜와 시간으로만 했을 경우
참조변수 V는

$$V = \{D_1, D_2 .... D_{30}, D_{31}\}$$

패스워드 입력방법 I는

$$I = f(P_0, P_1 \cdots P_{N-1}, P_N, Ch_1, Ch_2, \cdots Ch_N, S_0, S_1 \cdots S_{N-1}, S_N, D_1, D_{31}, H_1 \cdots H_{24}, 1, 2 \cdots 9, 0)$$

로 표현할 수 있으며, 입력방법은 사용자가 정하는 것으로, 예를 들면

$$I = P_0 \times S_1 Mod10, P_1 \times S_1 Mod10, Chn, (P_2 + S_1) Mod10, P_{N-1}, P_N \times S_1 Mod100$$

로 설정할 수 있다.

이와 같이 설정한 경우 숫자로 이루어진 몇 자리수의 결과(Sol)는

$$Sol = \{10^{N+Ch+1}\}$$

이므로 만약 등록된 패스워드가 4자리였다면 4자리에서 7자리 또는 그 이상의 자리수가 될 것이다.

채널을 입력하지 않고 각 자리 별로 가감승제 거듭제곱 등에 나오는 특정수의 나머지수로 입력을 하면 4자리수로 입력되겠지만 입력되어지는 결과에 본인이 아닌 관찰자의 입장에서는 관찰했다가 다음에 사용하기 위해서는 역으로 사용자가 정한 입력방법과 참조신호와 참조변수 및 패스워드 외에도 입력 식을 알아야 사용할 수 있는데 입력한 내용으로 이를 유추해 알아내기는 거의 불가능하게 되며, 따라서 결과를 도출해내기 위한 상기 요소 중에서 어느 하나라도 모를 경우에는 결과값을 우연히 맞출 확률밖에 없으며, 관찰한 후에도 결국 우연히 맞출 확률만이 존재하게 된다.

본 연구의 간접적인 방법에 의하여 일회용 패스워드를 생성하기 위한 서버가 필요하다. 서버는 다음과 같은 응용 프로그램 및 데이터 베이스가 필요하다.

- 패스워드를 저장하는 패스워드 데이터베이스
- 통일 식별자에 대한 패스워드를 기본변수로 만든 수식이나 함수를 저장하는 패스워드 입력방법 데이터베이스
- 사용자가 입력할 때 참조하는 변수를 저장하는 참조변수 데이터 베이스
- 참조신호를 관리하는 참조신호관리 프로그램
- 식별자에 대한 권리 행사의 종류를 정한 채널 데이터베이스
- 입력하는 반응시간을 저장하는 반응시간 데이터베이스
- 입력한 반응시간과 입력된 결과를 비교 해석하여 등록되어 있는 패스워드와 계산식을 알고 있는지를 확인한 후 사용자가 요구한 해당 채널의 프로세스를 수행하는 통제 관리 프로그램

여기서 참조신호란 패스워드 시스템이 사용자에게 보내는 변수이고, 참조변수란 약속된 변수를 의미한다. 채널은 사용자의 권리를 여러 개로 구분하여 둔 것을 말한다. 예를 들어 다섯 개의 채널을 두고 각 채널에 다른 가능들을 부여할 수 있다.

보통 모든 권리를 부여하는 정상 채널, 계좌 잔액 조회만 할 수 있는 권리만 제공하는 채널이나 강제에 의해 패스워드가 도용당할 경우 도용자가 패스워드를 입력할 때 신고할 수 있는 보호 채널 등을 등록할 수 있다. 채널 이용은 사용자가 이용할 채널을 선택하고 채널번호를 패스워드에 부여할 수 있다.

사용자 인증 과정은 다음과 같이 할 수 있다.

가. 사용자는 식별자(주민등록번호, ID, 계좌번호, 카드번호 등)를 일회용 패스워드 서버에 전송한다.

나. 식별자를 받은 서버는 식별자에 대한 참조신호를 사용자에게 보내고 이 참조신호를 임시 저장한다.

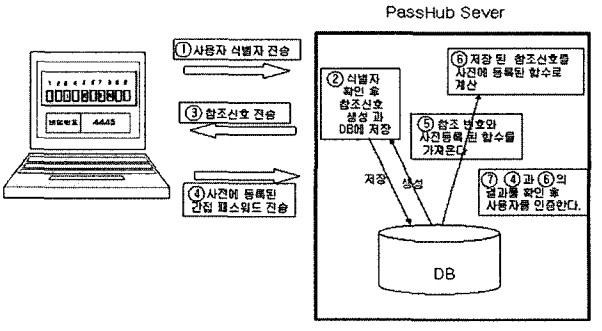
다. 사용자는 사전에 등록된 간접적인 패스워드 입력방식에 따라 패스워드, 참조신호, 참조변수, 상수와 채널로 이루어진 계산방법과 해석과 순서를 정해 표현하는 방법에 의해 입력되어야 할 결과를 서버에 다시 전송한다.

라. 서버는 위에서 언급한 임시 저장한 참조신호를 가지고 사용자와 똑같은 연산 을 하여 사용자가 보낸 간접 패스워드와 비교하여 사용자를 인증한다. 이때 서버는 사용자로부터 입력된 결과를 유효한 것과 채널을 분류하고 응답시간을 계산하는 약속된 방법에 따라 재계산하고, 입력된 응답시간이 사용자가 정한 응답시간 내인지 판단하고 시스템이 계산한 결과와 해석하고 비교하여, 결과가 맞으면 식별자에 대한 사용자를 확인한 것으로 간주하여 함께 요구된 채널의 프로세스를 수행한다.

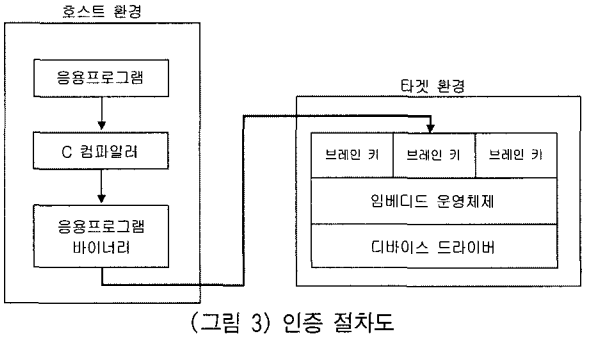
아래 그림들은 본 연구에 따른 패스워드를 통한 사용자 확인 방법에 대한 인증 절차 도를 나타내었다.

3.4 임베디드 시스템 적용 방식

인증 시스템은 임베디드 시스템 환경하에서 구동 될 수 있다.



(그림 2) 인증 절차도



(그림 3) 인증 절차도

브레인 키의 핵심 코드를 타켓 시스템에서 구동하게 하여 호스트에서 관리하 주게 되어 있다. 따라서 브레인 키는 독립적으로 수행되게 되어 있다.

3.5 브레인키의 참조신호 발생방식

pseudorandom number를 사용하는 통상적인 몬테 칼로 적분법은 주어진 점의 개수가 n이라고 할 때 수렴속도가 n의 제곱근에 반비례하지만 quasi-random number를 사용하는 quasi-Monte Carlo 적분법은 그 수렴속도가 n에 반비례하므로 금융수학에서는 quasi-Monte Carlo 적분법을 사용할 수 있는 경우에는 이 방법을 사용하는 것을 권하고 있다.

난수란 규칙성이 배제된 숫자를 의미한다. 난수 발생기에 난수를 발생시키는 시작점을 제공하면 난수 발생기는 이 시작점을 기준으로 하여 난수를 발생시킨다. 따라서 시작점을 바꾸면 생성되는 난수도 달라진다. 완전한 난수를 만들기 위해서는 난수 생성기에게 전달되는 시작점 또한 예측 불가능한 난수여야 하는 것이다.

함수형 패스워드 제어시스템에서는 난수 발생기의 시작점으로 쓰기 위해 시간 값과 난수 데이터베이스 테이블을 이용한다. 난수 발생기가 실행될 시점의 시간은 예측할 수 없기 때문에 시간 값을 응용한 난수 데이터베이스 테이블을 참조하여 시작점으로 사용한다면 완전한 난수를 만들 수 있다고 본다.

또한 난수는 브레인키의 사용특성에 따라 난수의 중복을 허용하거나 허용하지 않을 수 있다. 그러나 패스허브는 중복 값의 허용을 1회로 한정하고 있다. 고정 값 0부터 9사이에 부여하는 난수 값이 상호 독립적인 경우는 브레인키 사용을 제한적으로 사용하는 경우이다. 브레인키 인증엔진에서 사용자의 패스워드를 인증하는 경우에는 중복 값을 허용하되 해킹을 대비하여 중복 값은 1개 번호로 한정하고 있다.

그러므로 기존의 난수발생함수 rand, srand등를 이용하여 난수를 발생시켜도 시간함수와 자체의 난수발생테이블을 이용하기 때문에 사용자에게 보여주는 값을 매번 갱신 시키더라도 그 난수 값은 같은 룰로 사용자에게 보여지지 않는다.

이렇게 발행한 난수는 해당 세션의 로그테이블에 저장되고 난수 값을 이미지 값으로 변환하여 사용자에게는 이미지로 전송한다.

ATM, PDA등과 같이 독립형인 경우는 난수 발생 초기값을 시간함수만을 사용하여 난수를 발행시키며 난수간에는 발행하는 숫자가 상호 독립적이 되도록 중복 발행하지는 않는다.

난수 발행 시 공격자가 이런 현상을 관찰하거나 조작할 수 없도록 권고하고 있다. 시스템 클럭을 사용하는 경우는 공격자가 랜덤 비트열을 생성한 시간을 예측하여 공격할 수도 있기 때문이다.

- 시스템 클럭
- 키보드 입력 간격 또는 마우스 움직임 간격
- 입출력 버퍼의 내용
- 시스템 부하, 네트워크 통계와 같은
- 운영체제에서 사용하는 값

보안에서 사용하는 난수 알고리즘에 의해 난수를 발생할 필요가 없으므로 다음과 같이 난수가 발생되는 규칙을 정하였다.

가. 시스템에서 난수가 발생해서 단말기로 보내는 경우는 경로 해킹을 방지하기 위해서 발생된 난수를 그래픽화를 하고 이를 난수DB에 저장하여 두고, 사용자 인증 시에 그래픽화 된 난수를 무작위로 추출하여 사용자에게 보내준다.

나. 난수는 자리 별로 각기 생성되지만 같은 난수가 2개를 초과하면 다른 난수가 발생되도록 하였다.

다. 수요 처에 따라 자리 별로 각기 생성되지만 중복되는 난수가 없는 난수 발생기의 제작이 필요하다.

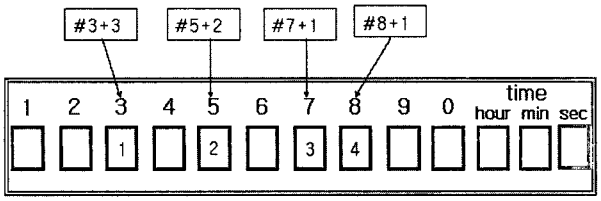
3.6 브레인키의 패스워드 함수등록 유형

사용자 관점에서 브레인키의 함수등록 유형을 분류하면 다음과 같다. 전체 치환(대응)방식, 부분 치환(대응)방식, 영숫자 방식, 음계적용방식, 한글자음적용방식, 참조변수적용방식, 함수적용방식으로 나눌 수 있으며 이중 사용자가 편의대로 선택하여 등록한다.

- 단순치환방식은 기존의 비밀번호 고정수를 전부 난수에 대응하는 방식으로 비밀번호를 사용하는 방식이다. 단순치환방식은 오프라인이나 카드 결제시 주변을 의식함이 없이 비밀번호를 사용할 경우 효과가 있다.
- 부분치환방식은 고정수 패스워드 중 일부만 참조신호를 적용하여 패스워드를 설정하여 사용하는 방식이다.
- 사칙연산 적용방식은 특정 참조신호에 사칙연산을 적용하는 방식으로 이 방식을 이용하면 치환방식 설정보다 보안이 한층 강화된다.
- 영숫자 방식은 숫자로 이루어진 패스워드가 아닌 영숫자 패스워드를 사용할 경우에 적용된다. 부분치환과 사칙연산도 동시에 적용할 수 있다.
- 음계방식은 음계로 패스워드를 등록하는 방식이다. 영숫자를 음계로 대응하는 방식으로 부분치환과 사칙연산도 영숫자 방식과 동일하게 적용 가능하다.
- 한글적용방식은 패스워드를 한글로 사용할 경우에 적용합니다. 한글 자음 첫 자리로 패스워드를 구분하는 방식으로 패스워드를 한글문장으로 등록하는 경우 유용하다. 부분치환과 사칙연산도 영숫자 방식과 동일하게 적용 가능하다.
- 참조변수 적용방식은 주가지수나 시간 등 참조변수를 패스워드에 이용할 경우 유용하다. 참조변수에 사칙연산을 적용하면 보안성이 더욱 강화된다.
- 함수방식은 일반적으로 패스워드 각 자리수에 함수(논리함수와 더미함수등)를 쉽게 등록, 사용할 수 있도록 제공하는 기능이다.

4. 구현 및 사례연구

소비자가 단말기에 서버로부터 참조신호를 받아서 간접적으로 입력하는 것은 사용자가 미리 지정한 방법에 따른다. 예를 들면 위의 (그림 4)처럼 index 3에는 3을 더하고, in-



(그림 4) 참조신호 사례

dex 5에는 2, index 7과 8에는 1을 더하는 함수로 지정하였고, 서버가 각 index에1234 라는 참조신호를 보내면 사용자는 4445를 패스워드로 입력하면 된다. 다음 번에는 다른 참조신호가 보내지며, 사용자는 그 참조신호를 앞에서 정의한 함수에 따라 계산한 후에 패스워드를 입력하면 된다.

이와 같은 간접적인 패스워드 입력을 통한 사용자 확인방법은 식별자에 대한 사용자의 확인과 인증을 사용자가 알고 있는 것을 확인하는 방법을 이용하는 산업의 여러 분야에 범용적으로 응용될 수 있는 것으로, 그 중 폰뱅킹(Phone Banking)에 적용한 예를 자세히 설명을 하면 다음과 같다.

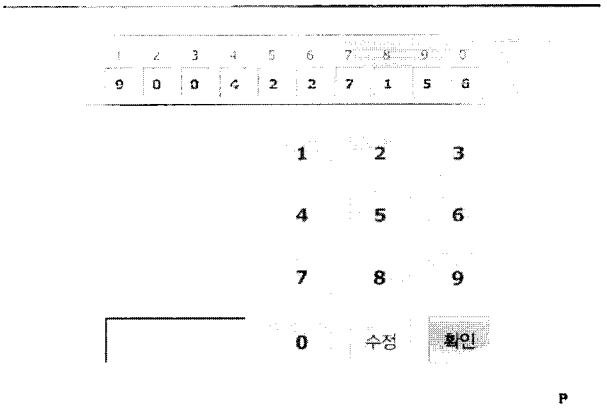
폰뱅킹 서비스를 받고자 하는 사용자는 자동응답시스템(ARS)에 전화로 접속을 한 뒤 사용할 계좌번호를 누른다. 패스워드 제어시스템의 참조신호관리장치에서 참조신호를 임의의 숫자를 선별하여 하나 또는 그 이상의 숫자를 순차적으로 자동응답시스템(ARS)으로 보내고 패스워드 제어시스템의 임시저장소에 참조신호내용과 보낸 시각을 임시 저장하며, 자동응답시스템(ARS)은 참조신호를 음성으로 들려준다.

한편 이미 등록되어 있는 패스워드가 예를 들면 1234이고, 등록되어 있는 패스워드 입력방법이 예를 들면 패스워드 + 300 - 참조번호 * 10 + 채널번호이며, 원하고자 하는 거래 즉, 10만원 미만 거래를 채널번호 3으로 등록했었다고 가정하면 계산결과값인 15293을 입력하면 패스워드 제어시스템에서는 비밀번호 입력방법 저장소에서 채널이 입력되는 부분을 파악하여 마지막에 입력된 채널번호를 임시저장소에 저장하고 비밀번호저장소에서 비밀번호와 임시저장소에서 사용자에게 보낸 참조신호와 채널번호를 대입하여 입력방법 저장소의 해당되는 식별자가 입력되어야 할 내용을 계산한 후 사용자가 입력한 내용과 비교한다.

상기에서 사용자 입력 값과 패스워드 제어시스템의 자체 계산 값을 비교하여 일치되면 사용자가 참조신호를 받고 입력하기까지의 응답시간을 계산하여 사용자가 정한 응답범위 내이면 응답시간 저장소에 저장하고 요구한 해당채널의 권한 내에서 사용권한을 행사할 수 있도록 해당 채널의 해당 프로세스를 수행한다.

해당 채널의 기능은 시스템에서 제공하는 수많은 프로세스로써 사용자와 시스템간 사전에 약속되어 있는 선택한 프로세스의 한가지인 바, 일 예로 상기 사용자가 요구한 프로세스는 10만원 이상의 거래를 선택하면 서비스를 중단하게 하는 것을 요구한 채널 3의 프로세스를 수행한다.

그리고 사용자 입력 값과 패스워드 제어시스템의 자체 계산 값을 비교하여 일치하지 않으면 일치하지 않을 때의 프로세스(예를 들면 처음으로 되돌아가는 것 등)를 수행하게 된다.



(그림 5) 브레인 키 구현물

응답시간 설정 및 확인 부분은 개인 컴퓨터나 현금 자동입출금기 같은 디스플레이가 있는 장치나 시스템에 대해서는 전화기와 같은 단말기보다 좀더 효과적으로 구성할 수 있다.

즉, 시스템에서 보내주는 참조신호로 설정 후 작동하기 시작하는 타이머를 1개 또는 복수 개를 설치하고 사용자는 타이머를 변수로 하여 설정되도록 수식을 등록 할 수도 있는 바, 특정숫자 사이일 때는 아무 의미 없는 숫자나 문자를 아무렇게나 간주함으로써 관찰자를 혼란 시키게끔 할 수도 있고, 특정채널은 타이머 중 한 숫자가 특정숫자일 때 입력해야만 유효하도록 등록하는 등 여러 가지로 관찰자를 따돌릴 수 있도록 구성할 수가 있다.

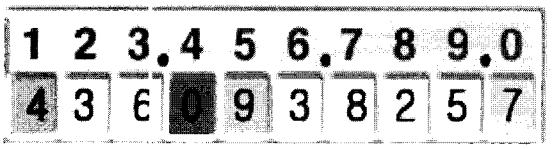
패스워드를 입력할 때 참조하는 변수는 적용되는 곳에 특성에 따라 여러 가지로 설정할 수 있는 것으로, 방문객의 수를 공표하는 경우는 사용자의 경우 본인이 입장했을 때의 방문객 카운터의 마지막 자리 수를 참조할 수 있고, 주식계좌의 경우는 종합주가지수를 참조할 수도 있으며, 본인의 보유주식수로 할 수도 있다.

그리고 은행의 경우 계좌 이체 시에 사용되는 이체패스워드는 보내는 계좌의 특정자리를 참조변수로 할 수도 있다. 따라서 참조변수는 시스템과 사용자가 공유할 수 있는 것이라면 무엇이든지 설정이 가능하다.

패스워드 입력방법은 사용자의 기호에 따라 마음대로 정할 수 있는 것으로, 상기와 같은 방법 외에 패스워드 변경을 주기적으로 원하는 사용자는 날짜나 시간 등을 변수로 쓸 수도 있고, 참조신호와 참조변수 및 비밀번호 등으로 이루어지는 수식을 이용할 수도 있으며, 참조신호 숫자만큼 패스워드와는 무관한 숫자를 입력도중에 삽입하는 방법을 선택할 수도 있고, 사용하고자 하는 채널의 위치를 패스워드 앞뒤나 패스워드 중간에 입력하는 방법을 선택할 수도 있다.

참조변수도 보이는 그대로 사용하지 않고 수식으로 가감승제 하거나 특정함수로 변형해서 참조할 수도 있다. 따라서 참조변수는 패스워드 제어시스템과 사용자가 공유할 수 있는 참조변수로 설정할 수 있고, 패스워드를 입력하는 방법도 사용자가 임의로 설정할 수 있다.

폰뱅킹의 예에서 입력하는 15293의 결과는 수많은 패스워드와 수많은 수식의 조합으로 나올 수 있는 결과와 동일하다. 따라서 사용자가 아닌 제 3자의 입장에서는 알 수 없다.



(그림 6) 패스워드 조합의 예

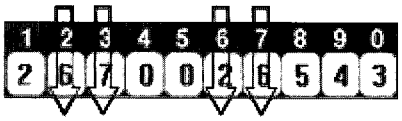
좀더 패스워드 제어시스템의 성능을 높이고자 한다면 참조신호를 몇 가지를 주어 각 사용자마다 특정순서에 있는 숫자를 선택하거나 몇 개를 조합해서 함수를 쓰도록 할 수도 있다. 또한 참조번호를 부여한 후 입력되는 시간을 측정하여 자료화하면 통계적인 방법에 의해 사용자 확인을 좀더 세밀하게 할 수 있다.

참조신호를 받아서 자동으로 수행되는 프로그램의 공격을 막기 위해서는 참조신호를 그래픽이나 영상자료의 형태로 보내는 방안 등도 고려할 수 있다. 따라서 사용자의 입장에서는 본인이 설정해둔 방법대로 간단하게 입력하지만 도용자의 입장에서는 과연 어느 것이 참조변수로 하여 계산되어 나온 것이고, 또 어느 것이 무의미한 숫자이고, 어느 것이 채널인지를 입력되는 결과의 숫자를 가지고는 사용자가 알고 있는 패스워드와 패스워드 입력방법과 요구한 채널을 알 수가 없다. 또한 패스워드는 자원을 제공하는 관리처(은행이나 신용카드사, 전자상거래 사이트 등) 또는 암호화되어 있는 사용자의 소지품(예를 들면 스마트카드, 전자 서명키 등)에 따로 보관하여 두고, 사용자의 패스워드 입력방법만을 따로 관리하는 제 3자 입장에서 객관적으로 사용자 확인을 중계하는 인증기관을 운영할 수도 있다.

여기에서 패스워드 입력방법의 보관방법은 패스워드 보관방법과 다른 암호화로 변형 보관하는 방법이 제시된다. 예를 들어 폐쇄형 스마트카드의 경우 스마트카드와 스마트카드 리더기를 패스워드 제어시스템으로 구성할 때는 패스워드 제어시스템을 양쪽으로 배분하여 구성하고 사용자 확인을 할 때 상기에 언급된 방법으로 패스워드 입력방법에 대한 결과를 입력받음으로써 사용자가 인증되는 방법으로 구성하면 된다. 따라서 본 연구의 개념은 산업상의 여러 분야에 응용될 수 있는 것으로 디지털 도어락 등 단일기기는 물론이고, 출입문의 통제관리 시스템이나 통신이나 파일, 디지털 서명키, 스마트카드 및 카드리더기 등의 각종 암호화와 복호화의 키워드로 활용될 수 있으며, 인터넷 전자상거래에서 활용되는 각종 사용자의 확인이나 전자금융거래, 신용카드조회기, ATM 단말기, 그리고 휴대폰이나 PDA 등의 소형 무선통신기 및 양방향 TV 등 상호 신호를 주고받는 분야에 광범위하게 적용할 수 있는 것인 바, 이것은 그 분야에 통상적인 지식을 가진 자이면 본 기술의 요지에 벗어나지 않는 범위 내에서 그에 맞는 패스워드 제어시스템을 용이하게 구성할 수 있을 것이다.

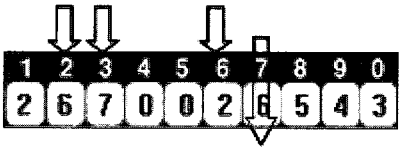
4.1 사례1 : 전체치환방식

전체치환방식은 선택한 비밀번호를 대응하는 참조신호 값만을 비밀번호를 사용할 경우에 쓰는 방식으로 아래 그림은 2367에 대응하는 참조 신호 값으로 비밀번호를 설정한 경우의 예로 6726이 올바른 비밀번호로 인증된다



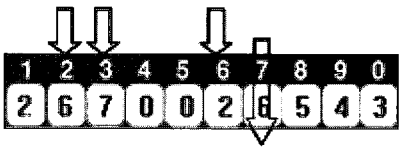
4.2 부분치환방식

부분치환방식은 선택한 비밀번호를 대응하는 참조신호 값과 고정수를 혼합하여 사용하여 비밀번호를 사용할 경우에 쓰는 방식으로 아래 그림은 236 고정수에 7에 대응하는 참조신호값으로 비밀번호를 설정한 경우의 예로 6726이 올바른 비밀번호로 인증된다



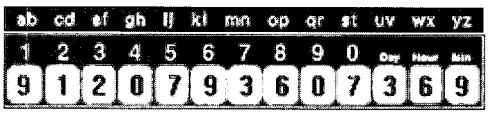
4.3 사칙연산방식

비밀번호에 대응하는 참조 신호 값에 사칙연산을 적용함으로써 비밀번호의 예측을 어렵게 하는 방식이다. 2, 3, 6, (참조 신호 값-7)을 선택한 후 (참조 신호 값-7)에 +1을 연산한 경우이다. 이 경우에는 비밀번호는 그림 예에서와 같이 2367이 올바른 비밀번호로 인증된다. 감산할 경우에는 값이 마이너스로 나올 경우 절대값이 인증 값이 되며 나눗셈을 할 경우에는 몫만 인증 값이 된다.



4.4 영숫자 치환방식

영숫자 치환방식은 선택한 비밀번호를 대응하는 참조 신호값과 영숫자를 혼합하여 사용하여 비밀번호를 사용할 경우에 쓰는 방식으로 마우스만을 사용하여 고정수나 영숫자부를 선택한다. 영숫자로 비밀번호를 기본 설정한 후 이중 일부 자릿수에 난수 및 사칙연산을 적용할 수 있는 방식으로 난수값에는 사칙연산을 적용함으로써 단순 숫자방식보다 비밀번호의 예측을 더욱 어렵게 하는 방식이다. 단, 참조 신호 값에만 사칙연산을 적용한다. 특정 영문자를 참조신호로 설정한 경우는 그에 대응하는 하단 난수값과 동일하다. 즉, 즉, 영문자 a를 난수로 설정하면 #a 는 #1과 같다.



비밀번호를 영숫자 Korea1234로 등록한 후 이중 8번째수 3을 참조 신호 값로 등록한 후 (간략하게 Korea12(#3)4로 표기) 난수(#3)에 더하기 5를 적용한 예이다.

정상패스워드 > Korea12(#3)4 ☞ Korea12(2+5)4 ☞ Korea1274

즉, Korea1274가 정상 패스워드이다.

간단한 함수 외에 복잡한 함수적용방식을 포함하여 사용자를 인증하도록 브레인키에는 적용하였으나 일반적으로 사용자가 적용하기에 적당한 4가지 사례만을 제시하였다.

5. 결 론

현재 일회용 패스워드는 국내에서 초기 시장이 형성 중에 있으나 토큰 등의 가격 이 비싸서 이를 대치할 수 있는 연구가 시장 확장을 위해 필수적이 될 것이라 판단된다. 브레인키 연구는 토큰과 같은 보조기구 없이 소프트웨어만으로 장착이 가능하여 저 비용으로 도입할 수 있는 편의성 및 안정성을 동시에 만족시킬 수 있다. 전자상거래가 활성화 될수록 본 연구의 적용범위는 계속 늘어날 것으로 보인다. 그러나 브레인키 연구의 핵심인 함수를 사용자가 정할 수 있다는 것은 도용의 가치가 높을수록 복잡한 함수를 지정하게 되고 이것은 소비자를 불편하게 하는 요인이 될 것으로 보인다. 따라서 복잡하지 않으면서 간접 패스워드를 모호하게 할 수 있는 함수를 만들어 내는 것이 사업화 성공의 중요한 요소가 된다.

5.1 연구 경쟁력

일회용 패스워드는 다음과 같은 조건을 가져야 한다.

- 복제가 불가능해야 한다.
- 사용이 편리해야 한다.
- 패스워드 유추가 불가능해야 한다.
- 가지고 있는 것과 알고 있는 것을 동시에 지원해야 한다.

브레인키 연구는 위 네 가지 조건을 충족한다. 토큰과 같은 기기를 휴대해야 하는 Challenge-Response와 Time-Synchronous 방식은 사용의 편의성에서 문제가 있다. 브레인키 연구는 인터넷뱅킹과 같은 온라인뱅킹뿐만 아니라 패스워드를 통한 인증이 필요한 곳은 어디든지 적용할 수 있는 장점을 가지고 있다. 또한 휴대기기 없이 전자금융 및 상거래용 단말기만으로 패스워드 입력이 가능하므로 사용자의 편의성에 있어서 우수하다. 또한 입력단계부터 이미 도용이 불가능하므로 통신 채널 상에서 가로채기 등의 과정 등을 통한 해킹 역시 무용지물이 될 가능성이 있다. 이것은 토큰을 이용한 일회용 패스워드에서 암호화가 필요한 알고리즘을 생략할 수 있어서 구현상에 있어서도 간단할 수 있을 것이다.

5.2 연구 독창성

사용자가 자신의 권리를 스스로 원하는 만큼 패스워드를 입력하는 방법을 사용자가 스스로 정하도록 하고 입력하는 단계에서부터 사용자가 식별자에 대한 권리의 표현을 할 수 있도록 하여 단지 패스워드를 입력하는 것만을 지켜보아서는 패스워드를 알 수 없도록 하였다. 본인이 아니면 패스워드를 다시 사용하기 어렵도록 패스워드를 입력할 때 사용자가 등록되어 있는 계산방식을 통해 계산된 결과만을 입력하는 간접적으로 알고 있는 것을 확인하는 방법을 사용하는 최초의 방법이다. 이것은 기존의 일회용 패스워드 방법은 가지고 있는 것을 통하여 사용자를 확인하는 것에 반하여 브레인키 연구는 알고 있는 것을 이용한 사용자 확인을 할 수 있는 보안연구다.

또한 브레인키 연구는 기존에 한 식별자에 대해 모든 사용권한이 모두 한 패스워드에 달려 있던 것을 사용자가 통일 식별자에 대해서도 사용권한을 패스워드에서 구분할 수 있도록 채널 개념을 도입한 것이다. 이는 사용자가 한 번의 패스워드 통과로 모든 권한을 획득하는 위험을 줄이고, 도용자가 한 사용자의 권한을 모두 획득했는지 알기 어렵도록 하기 위한 효과적인 수단이 된다. 사용자별로는 몇 개의 채널만 사용하겠지만 도용자의 입장에서는 공표된 모든 채널에 대해 점검을 해야 될 것이므로 무작위 적으로 접근할 수 없는 수단으로 작용하게 된다. 즉, 일반적으로 채널의 프로세스에는 사용자의 위치를 파악해서 신고하는 채널도 있고, 권한 내용을 허위로 표현하는 채널이나, 접근하는 시스템을 정지시키는 채널 등 사용목적에 따라 여러 채널을 둘 수 있으므로 도용자에게 사용자가 채널의 내용을 알려주더라도 사실유무를 확연할 수 있는 수단이 없어 도용하는 것을 저지시킬 수 있게 된다.

5.3 연구의 첨단성

"알고 있는 것" 중 변수에 따라 변동 할 수 있는 표현수단을 함수로 이용하면 어떤 장치로도 검색 복제가 불가능하며 표현 수단인 함수를 적당히 조합하여 사용자 능력에 따라 도용방지 정도를 결정할 수 있다. 따라서 도용가치가 높을수록 어려운 방법으로 등록할 수 있는 수단을 제공한다. 기존 패스워드 사용 시 금지되어 왔던 숫자 조합들을 응용할 수 있어서 기억이 쉽다.

OTP와 IPM은 난수 사용, 도전과 응답방식, 패스워드의 변동, 함수 사용면 에서 유사점이 있지만 다음과 같은 중요한 차이점이 있다.

이상에서 설명한 바와 같이 본 발명은 입력되는 패스워드를 지켜보더라도 원래의 패스워드는 무엇이고 어떠한 수식과 어떤 변수를 사용하여 지금 이 패스워드를 사용하고 있는지 알아낼 수 없으므로, 비디오 카메라를 몰래 설치해두었다 하더라도 도용할 수 없는 효과가 있다. 따라서 입력단계에서 이미 도용할 수 없으므로 경로상에서 가로채기 등의 과정상에서 해킹은 무용지물이 된다. 또한 사용자의 기호에 따라 패스워드가 구성되는 수준에 차이가 생기게 되어 시행착오법으로 알아내고자 할 때에 패스워드를 입력하는 방법이 개인별로 설정한 변수와 수식으로 이루어져 있으므로 엄청난 경우의 수가 발생되게 되어 컴퓨터처리를 통해서도 시간이 많이 걸리며, 찾아낸 입력 패스워드가 정확한 패스워드와 패스워드 수식으로 이루어 진 것이 아니므로 다시 사용할 수 없는 효과가 있다.

〈표 1〉 IPM과 OTP의 차이점

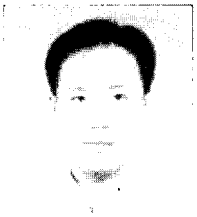
연구 명	차 이 점
Improved Password (IPM)	- 함수의 기록장소는 사람의 두뇌 속 - 함수계산은 두뇌의존형 - 사용자는 함수의 기억이 곧 생명 - 난수는 거래할 때마다 발생 - Change 난수 중 사용되는 변수는 사용자마다 다름 - 난수자체에 의미가 없음 - 모든 사용자에게 동일한 난수 제공 가능 - 수명이 없음 - 일반함수 사용 - 함수는 사용자가 정함 - 소지품 및 보조장치 불필요 - 다음세션의 난수 예측 불필요
One-time Password (OTP)	- 함수의 기록장소는 기계 속 (Token) - 함수계산은 기계의존형 - 사용자는 함수를 기억하는 것이 아님 - 난수는 Token 별로 1대1 개별적 발생 - Change 난수는 모두 사용하여 계산 - 난수의 중복 성 없음 - 모든 사용자에 동일한 난수 제공불가 - 수명이 있음 (평균 1-2년) - 해쉬함수만 사용 - 함수는 공급자가 정함 - Token의 휴대 또는 개인단말기에 보관 - 다음세션의 난수 예측 불가능 (예측 시는 도용가능)

〈표 2〉 OTP와 비교 우위성

구분	기존 일회용 패스워드	Brain Key 방식
방식	토큰방식	패스워드 입력방식
인증속도	30초	1-10초
용도	네트워크상의 로그인	사용자 인증
휴대장치	유	무
별도의 입력장치	무	무
도난분실	유	무
등록변경	재발급	변경가능
사용기간	1년	무기한
해킹프로그램	불가능	불가능
인식오차	무	무
위조	가능성 있음	불가능
통신상 해킹	무	무
DB해킹	무	무
강제사용	사용가능	사용불가능

참 고 문 헌

[1] 정보통신부, "전자거래 안전성 강화 종합대책," 2005. 9. 20.
[2] 김철, "암호학의 이해," 영풍문고, 1996.
[3] 원동호, "암호방식과 키분배," 한국 통신정보보호학회 학회지 제1권 1호, 1991.
[4] Domingue, J., Dzbor, M. and Motta, E.: Magpie: Supporting Browsing and Navigation on the Semantic Web. Proc. of Intl. Conf. on Intelligent User Interfaces (IUI). 2004. Portugal.
[5] The Report of the President's Commission on Critical Infrastructure Protection CCEB (Common Criteria Editorial Board), Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998.
[6] Eun-Ser Lee and Sun-Myoung Hwang, "Definition of Security Requirement Items and Its Process to Security and Progress Management," LNCIS 344, August 2006.
[7] Eun-Ser Lee and Sun-Myoung Hwang, "Design Implementation of Web Security Access Control System for Semantic Web Ontoloty," LNCS 3481, May 2005.
[8] 양형규, 이윤호, 손기욱, 권창영, 원동호, "영지식 상호 증명 이론 연구," 데이터 보호기술 워크 샵 논문집, 1989.
[9] Eun-Ser Lee and Sang-Ho Lee, "Design progress management for Security Requirements in Ubiqiiuous computing using COQUALMO," LNCS 3984, May 2006.
[10] Nam-deok and Cho, Eun-Ser Lee, "Design and Implementation of Semantic Web Search System using Ontology and Anchor Text," LNCS 3984, May 2006.
[11] ISO/IEC 15408-1:1999 Information technology-Security techniques-Evaluation criteria for IT security-Part 1: Introduction and general model.
[12] ISO. ISO/IEC 15408-2:1999 Information technology-Security techniques-Evaluation criteria for IT security-Part 2: Security functional requirements.
[13] ISO. ISO/IEC 15408-3:1999 Information technology-Security techniques-Evaluation criteria for IT security-Part 3: Security assurance requirements.

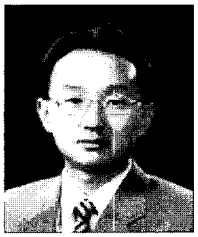


이 은 서

e-mail : eslee1@ssu.ac.kr
2001년~현 재 ISO/IEC 15504 국제 심사원
2004년 중앙대학교 컴퓨터공학과 (박사)
2004년~현재 임베디드 산업협회 전문 위원
2004년~현재 한국정보통신기술협회 위원
2005년~현재 숭실대학교 정보미디어기술 연구소 연구 교수
관심분야 : CBD, Formal method, Quality model, SPI(Defect Analysis)

문 호 영

e-mail : hymoon@korea.com
1980년~1984년 성균관대학교 물리학과 (학사)
1987년~1991년 삼일경영(경제)연구원
1999년~2001년 동양시스템즈(주) SI사업본부
2001년~2003년 삼일아이에스
2003년~2004년 ㈜메카소프트
2005년~현 재 ㈜패스허브 대표
관심분야 : 인터넷보안, 암호이론, 멀티미디어보안



이 상 호

e-mail : shlee@computing.ssu.ac.kr
1984년 서울대학교컴퓨터공학과(학사)
1986년 미국노스웨스턴대학교 전산학과 (석사)
1989년 미국노스웨스턴대학교 전산학과 (박사)
1990년~1992년 한국전자통신연구원 선임연구원
1992년~현재 숭실대학교 컴퓨터학부 교수
1999년~2000년 미국 George mason 대학교 교환 교수
관심분야 : 인터넷 데이타베이스, 데이타베이스 튜닝 및 성능평가, 웹 기술