# 결함-허용 기법을 이용한 신분확인 방안

공 병 운†, 이 경 현‡
†부경대학교 전산정보학과, ‡부경대학교 전자컴퓨터정보통신공학부

# An Authentication Scheme using the Fault-Tolerant System

Byung-un Kong†, Kyung-hyune Rhee‡
† Dept. of Computer Information, PKNU
‡ Division of Electronics, Computer and Information Communication Engineering, PKNU

**요 약**

본 논문에서는 인터넷과 같은 가상 공간에서 사용자의 신분을 확인하기 위해서 결함-허용기법을 이용해 본인의 신분을 확인하는 인증 기법을 제안한다. 제안 기법은 기존 패스워드 기법에 의존하는 신분 확인 기법을 다수의 질문-응답 기법으로 전환함으로써 인간의 기억력 한계와 패스워드 강도 사이의 trade-off를 고려한 방안으로 다양한 질문의 형태에 따라 확률에 근거하여 신분을 확인하는 방안으로 가상 공간에서의 인터넷 뱅킹 및 다양한 전자상거래 응용 등에 직·간접적으로 활용될 수 있다. 또한 실용적인 측면의 응용을 위해 다양한 종류의 질문을 구성하여 이에 대한 경험적 정답 확률을 고려한 신분 확인 확률도 산출하였다.

## 1. 서론

최근 가상 공간을 무대로 하는 전자상거래가 일반인에게 급속하게 확산되고 있다. 인터넷 이용자가 폭발적으로 늘어나고 컴퓨터 및 통신기술이 발전하면서 전자상거래는 시.공간적 제약을 받는 기존 상거래의 제한적인 영역을 대체하는 수단이 되고 있다. 즉 현실세계에서 상거래나 서비스의 제공은 인간을 중심으로 이루어지지만, 가상 세계에서는 인간이 만든 컴퓨터와 네트워크라는 도구로 모든 서비스가 제공되고 이를 이용한 상거래도 이루어지므로 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. 즉, 신뢰에 대한 문제는 정보화 사회 전반을 붕괴시킬 수 있는 기본적이면서도 중대한 한 요소라 할 수 있다. 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[2, 3]. 계정을 관리하는 방법에는 사용자 ID와 패스워드를 요구하는 경우가 대부분이며, 이 때 사용되는 패스워드의 길이는 6~10자 정도이다. 이 방식은 인간의 기억력에 의존하고 있으며, 이 경우 망각을 피하기 위해 기록을 해두거나 기억하기 쉬운 패스워드를 선택하는 경우가 흔히 발생한다. 패스워드 방식에서는 가능한 공격에 대비하기 위하여 알파벳 문자에 숫자와 문자의 조합이나, 긴 패스워드의 사용, 심지어는 특수 문자의 사용도 의무화하는 경우가 있다. 즉, 복잡한 패스워드일수록 공격에 강한 반면, 인간의 두뇌는 이러한 의미 없는 숫자, 문자, 특수 문자의 조합을 오래 기억하는 것은 사실상 힘들다.

본 논문에서는 인터넷과 같은 가상 공간에서 본인의 신분확인 및 패스워드의 분실이나 변경을 위한 효율적인 방안을 제안한다. 제안 방안은 본인확인 절차를 사용자 스스로의 생활경험 혹은 개인의 독특한 성향과 관련된 문제[2]를 미리 등록해 두고 패스워드 관리를 담당하는 시스템에서 본인확인을 원하는 사용자에게 여러 가지 문제를 시도(Challenge) 형태로 물어보고 응답(Response)에 대해 결함허용관점에서 분석 한 후 본인을 확인하는 정보보호시스템 구현을 목적으로 한다.

본 논문의 구성은 다음과 같다. 제 2 절에서는 기존 신분확인 방안에 대해서 기술하고, 제 3 절에서는 결함허용기법에 대해서 기술하고, 제 4 절에서는 결함허용기법을 이용한 신분확인 기법에 대해서 기술하고, 마지막 5절에서 결론을 맺는다.

## 2. 기존 신분확인 방안

컴퓨터 사용자의 정당성을 확인하거나, 요구하는 서비스에 대한 정당성을 확인하는 사용자 신분 확인의 메커니즘은 컴퓨터 시스템에 대한 접근 제어 및 중요 서비스 제공여부에 대한 판단 기법으로 현재 패스워드를 가장 많이 사용하고 있다. 그 이외의 신분 확인 기법으로 생체적인 방법, 동적인 패스워드 기법 등이 있는데 이들 중 네트워크 환경에서는 주로 일반 패스워드와 동적인 패스워드 기법이 사용되고 있다.

◆ 네트워크에서 신분확인

(1) 일반적인 패스워드 기법

인터넷상에 연결되어 있는 수많은 서버들 중에 유닉스 계열이 단연 제일 많다. 최근 윈도우즈 NT 등도 서버로써 구축되고 있으나 대부분의 시스템은 유닉스 기반의 전통적인 계정과 패스워드 메커니즘을 이용하여 사용자 신분을 확인하고 있다. 유닉스뿐만 아니라 네트웍에 연결되어 서비스를 제공하는 시스템에서 주로 사용하는 방식이 패스워드에 의한 방식이 일반적인데, 이 방식의 한계점은 인간의 기억력에 의존하고 있으며 동일한 패스워드를 반복적으로 사용함으로써 노출될 위험성이 있으며 사용자가 패스워드를 분실하였을 경우 본인의 신분확인 방안이 인터넷과 같은 네트워으로 불가능하다.

(2) 동적인 신분확인 기법

매 회 접속 시마다 일정한 함수 관계에 의하여 패스워드를 새로 생성하는 기법으로 Codebook Challenge Response 방식 등이 있으며 주로 일 방향 함수를 이용한다. 일회용 패스워드 생성기와 같은 소프트웨어 혹은 하드웨어 장비가 필요한 경우가 많고 한번 동기화에 실패 할 경우 복구에 문제점이 있으며 비용도 많이 드는 단점이 있다. 그러나 보다 안전한 시스템을 구성하기 위하여 최근에 많이 도입되고 있다.

◆ 로컬에서의 신분확인 기법(생체 인식 기법)

사용자 신분을 확인하는 또 다른 방법은 패스워드를 이용하지 않고, 인간의 신체적인 특성을 나타내는 바이오메트릭(biometrics)의 특성을 이용하는 메커니즘이 있다. 뛰어난 변별력을 가지고 있으며, 속이거나 도난 당하거나 잃어버릴 염려가 없다는 장점이 있으며, 일부 상용화된 제품도 있다. 그러나 구현에 어려움이 따르고, 비용이 많이 들며, 기술적인 한계 또한 있는 현실이다. 정부나 군사적 목적의 응용 등 특별한 보안도가 요구되는 경우에 제한적으로 사용되고 있으며, 네트워크 상에서 사용하기에는 제한적이다.

## 3. 결함허용기법

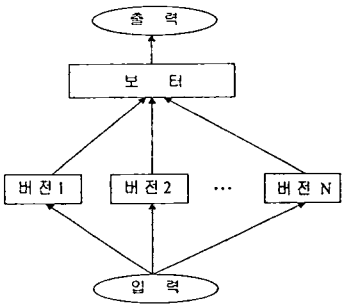
결함허용기법(Fault-Tolerant Scheme)이란 하드웨어의 오 동작 또는 소프트웨어의 오류가 일어날지라도 주어진 기능을 올바르게 수행할 수 있는 시스템을 말한다. 일반적으로 믿을만한 컴퓨터 시스템이란 크게 두 가지로 나누어 볼 수 있다. 첫째는 결함을 가지지 않는 컴퓨터 시스템이며, 그 다음은 컴퓨터 시스템 내에 결함을 가지고 있다하더라도 옳은 정보를 제공할 수 있는 능력을 가진 컴퓨터 시스템을 말한다.

결함허용 기법은 하드웨어 결함허용 기법, 소프트웨어 결함허용 기법 등 시스템 구성 요소별로 구분할 수 있다. 모든 기법들이 근본적으로 중복(redundant) 기법의 사용에 근거를 두고 있다. 하드웨어 신뢰도를 증가시키기 위한 노력은 오래 전부터 계속되어 왔으며, 하드웨어의 설계는 그 결함률을 감소시키는 결함허용 구조를 개발하는 방향으로 발전되었다. 그러나 최근에 소프트웨어 신뢰성의 중요성을 인식하게 되었으며, 대부분의 소프트웨어 엔지니어들은 결함이 없는 완전한 소프트웨어를 개발하는 것은 불가능하다고 인식하게 되었다.

여러 종류의 결함허용 소프트웨어의 개발을 위한 연구가 계속되어 왔는데, 본 논문에서는 N 버전 프로그래밍 기법에 대해[5, 6] 간략히 살펴보기로 한다.

◆ N 버전 프로그래밍 기법

N 버전 프로그래밍 기법은 각기 다른 조건과 다른 알고리즘 하에서 설계된 N개의 프로그램이 연속적으로 실행되어진다. <그림 1>에서 보는바와 같이 N개의 서로 다른 버전의 프로그램이 실행된 후 결과를 놓고 보팅하기 위해 보터가 필요하다. 이때 대다수의 버전이 같은 결과를 출력하였다면 보팅은 성공하게 되고 그 결과는 옳은 결과로 간주된다.




<그림 1>

## 4. 결함허용기법을 이용한 신분확인 기법

본 절에서는 개인의 독특한 경험과 성향을 기반으로 하고 있는 일련의 질문과 대답을 결함허용 기법 중에서 N 버전 프로그래밍 기법을 사용하여 신분확인을 하는 기법에 대해 알아보고자 한다. N 버전 프로그래밍 기법에서 각각의 버전과 보터를 본 논문에서는 질문과 정보보호시스템으로 고려하고 있다. 예를 들어, n개의 질문이 있다고 할 때 k개만큼의 대답을 올바르게 맞추었다면 정보보호시스템에 대한 사용자 신분확인이 이루어지는 것으로 간주할 수 있다.

### 4.1 질문을 만드는 원칙

본 논문에서 제안하는 가장 핵심적인 요소는 얼마나 좋은 질문을 만드는가 하는 것이며, 그 질문이 얼마나 개인적인 것인가 하는 것이 매우 중요하다. 즉 쉬운 질문에 대한 답은 기억하기 쉽지만 공격자가 추측하기 쉬운 것이 될 것이다. 따라서 좋은 질문의 조건은 사용자 본인에게는 쉬운 것이어야 하며, 공격자에게는 추측하기가 어려운 것이어야 한다.

### 4.2 질문의 예

(1) 개인의 경험에 의한 질문

개인의 경험 또는 성향에 대한 질문으로 자신만 대답 할 수 있는 유일한 질문형식이다.

▶ 내가 해외 여행 중 소지품을 두고 온 장소는?

▶ 내가 어머니께 처음 드린 선물은?

▶ 내가 여자친구에게 처음 보낸 시 제목은?

(2) 연산기호(AND)를 이용한 기법

한 질문에서 두 개 이상의 답을 요구하는 문장형식으로 개인의 취미 및 취향에 역점을 두는 질문 형식이다.

▶ 내가 제일 좋아하는 인물 이름과 작품은?

▶ 내가 처음 이사했던 장소 및 전화번호는?

▶ 내가 좋아하는 연예인 남자 및 여자는?

(3) 숫자 , 문자 , 특수문자 조합기법

개인의 특별한 사항에 대한 질문으로 질의의 답변으로 숫자, 문자 조합으로 구성되어 있다.

▶ 내가 수강하는 강의사이트의 식별이름(ID)은?

▶ 내가 소유하고 있는 캐비넷 도어 식별이름(ID)은?

▶ 내가 갖고 있는 메일서버의 패스워드는?

(4) 고유명사를 이용한 기법

개인이 소장하고 있는 시스템, 자격증 등 특별한 부분을 질의하는 형식이다.

▶ 내가 갖고 있는 자격증 번호(여러 개중 자신만 인정하는 자격증)는?

▶ 내가 갖고 있는 통장 번호(여러 개중 자신만 인정하는 통장 번호)는?

▶ 내가 즐겨 찾는 사이트 IP 번호는?

(5) 연상 작용을 이용한 기법

개인적인 특성으로 지난날 갖은 경험을 전개하는 문장 속에서 느낄 수 있는 감각적인 응답 형식의 질의이다.

▶ 바다만 보면 항상 떠오르는….

▶ 산에만 가면 항상 생각나는….

▶ 시골에 가면 느끼는 마음은….

(6) 노래가사를 변조

개인이 즐겨 부르는 노래 가사의 일부분을 개인적인 취향으로 바꾸어서 질의하는 형식이다.

▶ 앉으나 서나 당신(주님)생각 앉으나….

▶ 가는 세월(사람) 그 누구가 막을 수가….

(7) 틀린 그림 찾기

개인이 갖고있는 친구나 연인 및 가족사진의 부분을 찾는 형식의 질의이다.

▶ 다음 사진의 일부분은 누구일까요?

▶ 다음 그림을 보고 장소가 어디일까요?

(8) 자신의 문장을 이용한 기법

개인이 쓴 시 또는 소설의 일부분을 전개하여 문장을 질의하는 형식이다.

▶ 다음은 내가 쓴 시의 일부분이다 어떤 의미가 담겨 있나요?

▶ 다음은 내가 쓴 수필의 일부분이다 수필의 제목은?

질문의 예에서 살펴보듯이 얼마나 개인적인가에 따라 본인에게 맞추기 쉽고 공격자는 추측하기 어렵다. 그러나 시간의 경과함에 따라 본인 기억력 한계로 인해 정확하게 답변할 수 없을 것을 감안하여 위의 예문 각 질문에 대해 본인이 맞출 확률을 아래와 같이 나눌 수 있다.

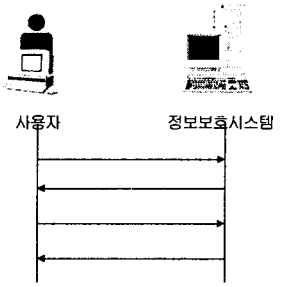
▶본인이 맞출 확률이 0.9 : (1),(4),(7)

▶본인이 맞출 확률이 0.8 : (2),(3),(6)

▶본인이 맞출 확률이 0.7 : (5),(8)

### 4.3 신분확인 절차

본 절에서는 신분확인 및 사용자가 패스워드 변경 시 또는 패스워드를 분실했을 경우, 만들어진 질문을 이용하여 개인의 신분을 확인하는 방법에 대해 논의하기로 한다. 먼저 정보보호시스템의 기본적인 동작 절차는 다음과 같이 수행된다.




① 사용자는 $n$개의 질문 $q_1, q_2, \cdots, q_n$과 각각의 질문에 대한 답 $a_1, a_2 \cdots, a_n$을 정보보호시스템에 보낸다.

② 정보보호시스템은 사용자가 패스워드 분실했을 경우 또는 변경을 요구했을 때 $n$개의 질문 $q_1, q_2, \cdots, q_n$을 사용자에게 보낸다.

③ 사용자는 질문에 대한 대답 $a_1', a_2' \cdots, a_n'$을 정보보호시스템에 보낸다.

④ 정보보호시스템은 사용자의 대답을 이용하여 적절한 보안 수준을 검토한 후 본인확인 및 패스워드 변경을 허락한다.

결함허용 기법을 이용하여 정보보호시스템의 보안성 수준을 결정하기 위해 다음과 같은 정의를 한다.

· 시스템의 보안성 : $S$

· 전체 문제의 수 : $N$

· 사용자가 질문을 맞출 확률 : $P(s)$

· 사용자에게 제시되는 문제 수 : $n$
· 사용자가 인증 받기 위해 맞추어야 할 문제 수 : k

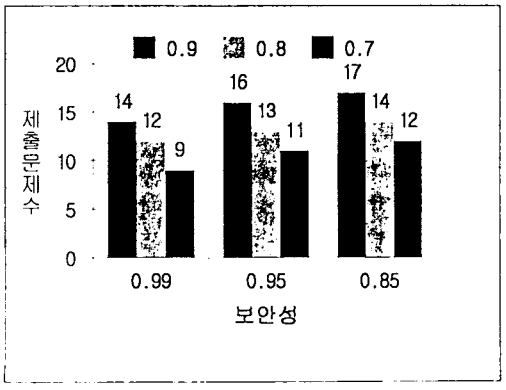
$P(s)$, $n$, $k$가 주어졌을 때 정보보호시스템에서 비로소 $n$만큼 일치하기를 원한다면 정보보호시스템의 보안성은 다음과 같은 식으로 나타낼 수 있다.

$$S = \sum_{n=k}^{N} \sum_{t=k}^{n} \binom{n}{t} (p(s))^t (1-p(s))^{n-t}$$

<표1>은 질문을 맞출 확률을 각각 달리했을 때의 정보 보호시스템의 보안성을 보여 준다.

| N | 질문을 맞출 확률 | | | | | |
|---|---|---|---|---|---|---|
| | $n$ | 0.7 | $n$ | 0.8 | $n$ | 0.9 |
| 10 | 4 | 0.9894 | 5 | 0.9837 | 6 | 0.9984 |
| | 6 | 0.8497 | 7 | 0.8791 | 8 | 0.9298 |
| | 8 | 0.3829 | 8 | 0.6778 | 10 | 0.3489 |
| 20 | 9 | 0.9948 | 12 | 0.9900 | 14 | 0.9976 |
| | 11 | 0.9520 | 13 | 0.9678 | 16 | 0.9568 |
| | 12 | 0.8866 | 14 | 0.9133 | 17 | 0.8670 |
| | 20 | 0.0007 | 20 | 0.0115 | 20 | 0.1216 |
| 30 | 17 | 0.9600 | 18 | 0.9969 | 24 | 0.9742 |
| | 19 | 0.8409 | 22 | 0.8714 | 26 | 0.8245 |
| | 21 | 0.5888 | 24 | 0.6070 | 28 | 0.4114 |
| | 23 | 0.2814 | 26 | 0.2552 | 30 | 0.1424 |
| 40 | 22 | 0.9852 | 28 | 0.9568 | 33 | 0.9581 |
| | 25 | 0.8849 | 30 | 0.8392 | 34 | 0.9005 |
| | 27 | 0.7033 | 32 | 0.5931 | 36 | 0.6290 |
| | 30 | 0.3087 | 35 | 0.1613 | 39 | 0.0804 |
| 50 | 30 | 0.9522 | 35 | 0.9692 | 41 | 0.9755 |
| | 32 | 0.8594 | 37 | 0.8894 | 43 | 0.8779 |
| | 34 | 0.6839 | 41 | 0.4437 | 45 | 0.6161 |
| | 37 | 0.3279 | 44 | 0.1034 | 47 | 0.2503 |
| 60 | 37 | 0.9368 | 40 | 0.9951 | 42 | 0.9999 |
| | 39 | 0.8382 | 43 | 0.9573 | 50 | 0.9658 |
| | 42 | 0.5632 | 49 | 0.4486 | 52 | 0.8584 |
| | 48 | 0.0568 | 51 | 0.2132 | 55 | 0.4372 |

질문의 각 확률과 전체문제 20개로써 그래프로 나타내면 아래와 같다.




## 4.4 질문의 Upgrade

질문의 답이 얼마나 개인적인 경험이라고 해도 사용회수 또는 시간 경과에 따라 본인이 맞출 확률이 100% 되기는 어렵다. 에빙 하우스의 망각곡선[1]에 따르면 인간은 기억한 후 첫 이틀동안에 66% 1개월이 지나면 79%를 망각해 버린다고 한다. 이런 망각곡선은 반복을 통해 기억을 극대화 할 수 있다. 그러면 질문의 문제 및 답을 바꾸어야 할 주기를 에빙 하우스의 망각곡선에서 살펴보면 사용자가 일주일동안 3회 이상 사용 시 95%를, 일주일동안 1회사용 시 75%, 1개월 동안 1회사용 시 50%, 6개월 동안 1회사용 시 30%를 유지한다고 보면 질문의 Upgrade는 사용회수에 따라 결정되어 질 수 있다는 것을 알 수 있다.

## 5. 결론

본 논문에서는 네트워크 환경 상에서 사용자의 신분을 확인하기 위한 여러 신분 확인 기법에 대해 살펴보고, 적용 가능한 결함 허용기법의 N 버전 프로그래밍 기법을 논의하였다. 이를 이용하여 독특한 경험과 성향을 기반으로 하는 새로운 신분확인 방안을 제안하였다. 본 제안 방안에서는 사용자가 작성한 질문과 대답을 정보보호 시스템에 저장시킨 후 본인확인 및 사용자의 패스워드 변경 시 또는 패스워드를 분실했을 시에 사용자 본인임을 인증하기 위해 결합허용 기법을 도입하고 있다.

현재 인터넷 상에서 개인 프라이버시의 침해는 심각한 수준이며, 이를 악용한 많은 다양한 범죄 및 공격 사례들이 등장하고 있다. 가상 공간에서의 신분확인 기법은 가치이전을 수반하는 전자상거래 및 인터넷 뱅킹에 있어서 선행적으로 구현되어야 할 필수 서비스이며, 주요 정보 전달 측면에서 매우 중요한 부분이라 할 수 있다. 따라서, 본 논문의 제안 시스템이 실제 구현된다면 가상 공간에서의 개인 신분확인에 적용할 수 있을 뿐만 아니라 Home LAN 시스템, 유·무선 전자상거래와 같은 인터넷 응용 등에 폭넓게 적용되어질 수 있을 것으로 사료된다.

## 참고문헌

[1] http://minsscape.co.kr
[2] Carl Ellison, Chris Hall, Randy Milbert, Bruce Schneier, Protecting Secret Keys with Personal Entropy, Elsevier Science, 1999.
[3] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84-88, February, 1981.
[4] E. gabber, P. Gibbons, Y.Matias, and A. Mayer. how to make personalized web browsing simple, secure, and anonymous. In proceedings of Financial Cryptography '97, 1997.
[5] L.Chen and A. Aviziens, "N-Version Programming : A Fault Tolerant Approach to Reliability of Software Operation", The 8th Annual International Conference on Fault-Tolerant Computing, Toulous, France, pp. 237-245, 1978.
[6] T. Anderson, P.A.Lee, "Fault Tolrance Priciples and practice", Prentice-Hall Inc., 1981.