JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 9 : 2073~2081, Sep. 2013

# 재활심리분석시스템의 폭주서비스 감내를 위한 지연기반 인증모델

임호찬[1] · 김영수[2*]

# Delay based Authentication Model for Flooding of Service Tolerance of Rehabilitation Psychology Analysis System

**Ho-chan Lim[1] · Young-soo Kim[2*]**

[1] Department of Psychological Rehabilitation, Korea Nazarene University, Cheonan 331-718, Korea
[2] Research and Business Foundation, Korea Nazarene University, Cheonan 331-718, Korea

## 요 약

급변하는 사회 속에서 개인의 심리적, 정신적 건강과 개인이 속한 가정이나 학교, 직장에서 일어나는 부적응 문제를 해결하기 위한 온라인 개인 심리검사의 수요가 증가되고 있다. 하지만 인터넷 기반 심리검사는 악의적인 공격자에 의해 폭주서비스를 통한 서비스 거부공격의 취약성이 존재한다. 따라서 서비스 거부공격을 억제하고 합법적인 사용자에게 최대한의 보안성과 가용성을 제공할 수 있는 시스템의 능력이 요구된다. 이의 해결책으로 지연 프로토콜을 수용한 부하가중 인증모델을 제안하고 검증하였다. 제안 모델은 인증의 점진적인 강화 기법을 사용해서 급속하게 증가하고 있는 서비스거부공격을 억제하고 서비스의 지속성을 보장함으로써 보안서버시스템의 신뢰성을 높여 줄 수 있을 것으로 기대된다.

## ABSTRACT

Today's rapidly changing society can lead to maladaptive behaviors. In the situations, rehabilitation psychology analysis using the on-line test be needed to solve the problem. However, Internet-based rehabilitation psychology analysis by a malicious attacker may still be vulnerable to denial-of-service attacks. The service flooding attacks render the server incapable of providing its service to legitimate clients. Therefore the importance of implementing systems that prevent denial of service attacks and provide service to legitimate users cannot be overemphasized. In this paper, we propose a puzzle protocol which applies to authentication model. our gradually strengthening authentication model improves the availability and continuity of services and prevent denial of service attacks and we implement flooding of service tolerance system to verify the efficiency of our model. This system is expected to be ensure in the promotion of reliability.

**키워드** : 재활심리, 심리분석, 서비스거부공격, 인증시스템, 지연프로토콜

Key word : Rehabilitation psychology, Psychology analysis, Denial of service attacks, Delay protocol

접수일자 : 2013. 08. 07 심사완료일자 : 2013. 08. 20 게재확정일자 : 2013. 08. 30

*** Corresponding Author** Young-Soo Kim (E-mail: experkim@gmail.com, Tel:+82-41-576-2278
Research and Business Foundation, Korea Nazarene University, Cheonan 331-718, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.9.2073 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

## Ⅰ. 서 론

인터넷 기반 심리검사는 지필 심리검사보다 검사 대상자인 내담자의 지능, 학력, 성격, 흥미 등 검사과정에서 다양한 정보수집이 가능하여 효과적인 심리검사 결과를 도출한다. 또한 상담현장에서 활용되는 심리검사 결과는 내담자의 심리적 장애나 어려움을 이해하고 문제해결에 유용한 정보를 제공한다. 오늘날 정신상담을 받기 위해서 많은 사용자들은 심리분석 시스템에 접속하여 온라인 검사를 통해 서비스를 받는다. 하지만 서비스 폭주로 야기되는 심리분석 결과서비스 장애는 상담서비스의 주요한 위협이 되고 있다. 더욱이 인터넷이 기업의 주요 네트워크 인프라로 활용되면서 서비스 장애로 인하여 합법적인 사용자의 서비스가 거부되고 기업의 경제적 손실과 기업 이미지가 손상되고 있다. 이의 해결을 위해서 사용자가 요청하는 서비스의 인증을 통해서 사용을 제한함으로써 서비스 거부 공격을 감내할 수 있는 방법이 일반적으로 사용되고 있다[1]. 그러나 인증 프로토콜은 인증정보의 저장을 위한 메모리 공간과 검증을 위한 연산 리소스를 필요로 한다. 적대적인 사용자가 암호화된 위조서명을 포함하는 패킷을 반복해서 대량으로 전송하는 경우에 서버는 위조된 서명을 검증하기 위한 인증 프로토콜을 개시하고 인증정보의 유지와 연산을 위해서 리소스를 과다하게 사용하게 되고 이로 인한 과부하로 서비스의 제공이 중단된다. 이와 같이 대부분의 인증 프로토콜은 서비스 거부공격에 취약하다[2]. 따라서 이러한 불법적인 공격에 대한 인증 프로토콜의 견고성과 리소스의 보안성을 확보하고 서비스를 지속적으로 제공할 수 있는 시스템의 능력이 요구된다. 이에 대한 한 가지 해결책으로 인증 프로토콜의 수행 초기에 사용자의 이름과 패스워드를 통한 약한 인증을 사용하고 검증된 후에 공개키를 이용한 암호화기법을 사용하는 강한 인증을 수행하는 방법이 있다[3]. 이를 위한 응용 모델로 퍼즐과 인증프로토콜을 사용한 폭주서비스 공격에 감내할 수 있는 아키텍처를 제안하고 구현한다.

퍼즐을 응용한 인증기술은 서버가 인증서비스를 요청하는 클라이언트에게 부하를 주는 약한 인증의 형태인 퍼즐의 해답을 제출할 것을 요구하고 검증을 수행한 후에 강한 인증을 계속해서 수행하는 메커니즘을 사용하고 있다[4]. 따라서 합법적인 사용자는 단일 서비스 요청에 대한 하나의 퍼즐에 대한 해의 계산이 요청됨으로 무시할 정도의 적은 연산 리소스를 소모하는 반면 적대적인 사용자는 서비스 폭주를 통한 서비스 거부 공격을 수행하기 위해서 대규모 퍼즐에 대한 해의 계산이 요구됨으로서 연산시간이 증가하고 이로 인한 전송이 지연됨으로써 서비스 폭주 공격을 제어하는 기술이다[5]. 이러한 퍼즐응용시스템은 보안서비스에 대한 폭주 감내 기능의 향상을 위하여 보안서버시스템의 배후에서 인증 프로토콜과 통합되어 사용될 필요성이 있다.

이를 위하여 본 논문에서는 그림 1과 같은 방법에 따라 공개키를 이용하는 암호화기법을 이용하는 인증모델을 기반으로 해쉬함수를 이용하는 부하가중모델을 수용한 지연기반 부하가중 인증모델을 제안하고 이를 사용하여 서비스 폭주 감내를 위한 인증시스템을 구현하여 모델의 실용성을 검증한다.

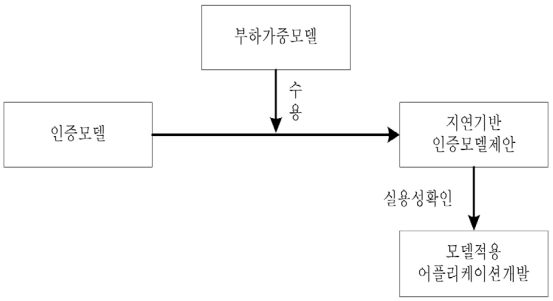


**그림 1.** 연구 접근 모델
**Fig. 1** The model of research approach

본 논문은 다음과 같이 구성된다. 2절에서는 접근통제시스템의 인증모델과 부하가중시스템의 퍼즐 모델을 분석하고 3절에서는 퍼즐을 사용한 지연기반 인증시스템의 응용모델을 제안한다. 4절에서는 모델의 실용성을 검증하기 위하여 폭주서비스 감내 시스템을 구현하고 검증한다. 5절에서는 결론과 시사점을 기술한다.

## Ⅱ. 인증시스템의 연구 모델

### 2.1. 접근제어시스템의 인증 모델

인터넷 기반 재활심리분석시스템은 내담자와의 신속한 상담서비스를 제공하기 위한 사용자의 온라인 접속이 증가하고 있다. 또한 인터넷이 분산시스템을 위한 인프라로 폭넓게 사용되고 단일의 서버시스템이 수백

만 다수 사용자의 서비스 요청을 제공하도록 설계되어 있어서 서비스 거부 공격에 대한 취약성과 해커의 위협에 노출되어 있다. 따라서 이의 해결을 위한 접근통제의 필요성이 확대되고 있다.

접근통제시스템은 그림 2와 같고 클라이언트시스템은 사용자 정보로부터 생성한 인증토큰을 서비스요청과 함께 전송하면 보안서버시스템의 접근통제메커니즘은 접근권한리스트내의 정보에 대한 비밀등급과 사용자의 권한을 표시하는 인증토큰내의 인가등급의 비교를 통하여 리소스의 접근에 대한 통제를 수행한다. 접근통제를 위한 필터링 구조는 메시지의 출처와 컨텐트 그리고 목적지에 따라서 서비스 요청에 대한 수용여부를 결정한다.

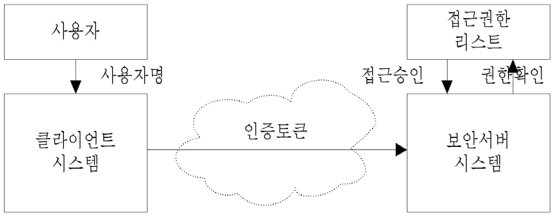


그림 2. 접근제어시스템의 보안 모델
Fig. 2 The security model of access control system

이와 같은 접근통제 모델은 모든 서비스 요청을 중앙의 단일 시스템에 의하여 통제하는 필터링 구조로 설계되기 때문에 악의적인 서비스 패킷의 폐기 속도보다 고속의 패킷을 전송하는 서비스 거부 공격에는 취약성을 보인다. 또한 접근제어를 강화하면 사용자의 가용성이 제한되므로 보안성과 가용성을 동시에 고려할 수 있는 접근방법이 제시되어야 한다. 접근통제 시스템에서 사용자의 권한을 표시하는 인증토큰은 인증과정을 통해 획득하는 정보를 포함하는 구조체로 그림 3과 같고 공개키 기반의 암호화 시스템을 사용하는 강한 인증 방식이 일반적으로 사용되고 있다.

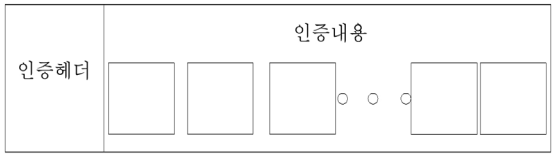


**그림 3.** 인증토큰의 구조
**Fig. 3** The architecture of authentication token

강한 인증은 비암호화 방식의 패스워드를 사용하는 약한 인증과는 달리 공개키 암호화시스템을 사용하고 각 사용자의 신원은 복호화 및 전자서명에 사용되는 개인키의 소유여부를 확인함으로써 식별된다. 공개키 암호화 시스템은 그림 4와 같고 사용자는 공개키와 개인키를 생성하고 공개키를 정보 근원지 역할을 수행하는 공개 키 디렉토리에 보관하고 개인키는 사용자가 관리한다. 공개키를 이용하는 전자봉투(Digital Enveloping) 응용은 송신자가 공개키 디렉토리로부터 수신자의 공개키를 획득하여 메시지를 암호화하여 전송한다. 수신자는 자신이 보관하고 있는 개인키를 사용하여 수신한 메시지를 복호화함으로써 기밀성을 보장한다. 디지털서명(Digital Signature) 응용은 송신자가 보낸 메시지를 수신자가 송신자 이외의 사람에 의해서 서명되지 않았음을 검증할 수 있도록 한다. 이를 위하여 송신자는 자신의 개인키를 사용하여 생성한 암호화 서명값을 전송하면 수신자는 공개 디렉토리로부터 송신자의 개인키를 사용하여 서명값을 복호화함으로써 서명을 검증한다.

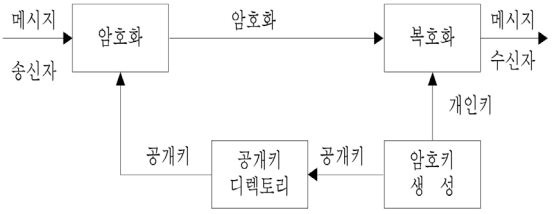


**그림 4.** 암호화시스템의 인증 모델
**Fig. 4** The authentication model of cryptosystem

공개키 기반의 암호화 방식을 사용한 인증은 공개키와 개인키를 사용한 메시지의 암호화와 복호화에 많은 시간이 소요되는 단점을 가지고 있어서 적대적인 사용자가 위조된 개인키를 사용한 암호화 서명값을 포함하는 메시지를 대규모로 전송하면 서버는 위조된 모든 서명값을 검증하기 위한 복호화 과정을 수행함으로써 연산 리소스가 고갈되고 이로 인한 서비스의 제공이 중지된다. 이와 같이 공개키 기반의 암호화방식을 사용하는 인증은 서비스 거부공격에 취약하다[6]. 따라서 전자서명과 같은 강한 인증 프로토콜의 개시 초기에 연산 리소스가 매우 적게 소요되는 약한 인증을 수행하고 성공한 인증서비스 요청에 한해서 인증 프로토콜을 계속 수행될 수 있는 메커니즘이 요청된다.

### 2.2. 부하가중 인증모델

상담서비스를 받기 위해 용자는 온라인을 통해 심리분석시스템에 접속한다. 하지만 서비스 거부 공격을 수행하는 적대적인 사용자는 보안서버시스템의 암호화기반 인증 프로토콜이 암・복호화의 연산에 많은 연산 리소스를 필요로 한다는 특성을 이용해서 다수의 불법적인 인증 프로토콜을 개시하고 서버시스템을 과부하 상태로 만들어 합법적인 사용자의 서비스가 거부 되도록 만든다[7]. 이를 해결하기 위한 대안으로 리소스를 많이 필요로 하는 인증 프로토콜의 암호화 연산을 수행하기 전에 서비스를 요청한 클라이언트에게 암호학적 퍼즐을 해결할 것을 요청하는 부하가중 모델을 사용한다. 퍼즐을 사용한 부하가중모델은 보통 그림 5와 같은 해쉬기반의 인증 방식을 이용하여 구현한다[8]. 이는 해쉬함수가 단순한 암호학적 연산이고 다양한 범용 하드웨어를 사용해서 계산할 수 있는 특성을 가지고 있기 때문이다.

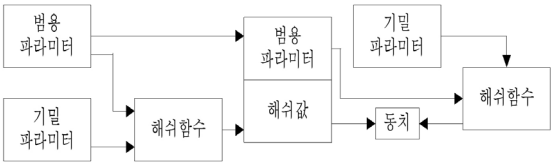


**그림 5.** 해쉬인증 방식의 부하가중 모델
**Fig. 5** The weighted overload model of hash authentication method

서버는 퍼즐의 송신주체로서 범용파라미터와 기밀파라미터를 해쉬함수의 입력값으로 사용하여 계산된 결과치인 해쉬값를 생성한 후에 기밀 파라미터는 폐기하고 범용파라미터와 해쉬값를 클라이언트에게 전송한다. 클라이언트는 퍼즐의 수신주체로서 해쉬값으로 부터 해쉬함수의 기밀 파라미터 값을 역으로 계산하기 위하여 무작위 값의 대입연산을 반복 수행한다. 따라서 서버는 검증을 위해서 수신한 기밀파라미터와 범용파라미터의 값을 사용하여 신속한 퍼즐의 해를 산출하여 검증을 수행할 수 있다. 이는 서버가 기밀 파라미터에 대한 비밀정보를 이용함으로써 계산을 신속하고 용이하게 수행할 수 있고 비교적 연산시간이 짧은 반면 클라이언트는 값의 반복대입을 통한 기밀파리미터의 값를 계산하므로 해의 탐색에 긴 처리시간이 소요된다. 퍼즐 프로토콜의 동작은 그림 6과 같이 표현된다. 서버시스템은 서비스를 요청한 클라이언트시스템에게 퍼즐을 전송하고 수신한 퍼즐에 대한 해답의 검증이 성공하면 서비스를 제공한다. 클라이언트는 퍼즐의 해를 계산하고 이를 서버에게 전송한다. 서비스의 요청을 단순히 폐기하는 필터링 메커니즘과는 달리 클라이언트에게 부하를 가중시켜 공격의 속도를 지연시킴으로써 서버가 폭주서비스로 인하여 기능이 마비되는 것을 억제한다.

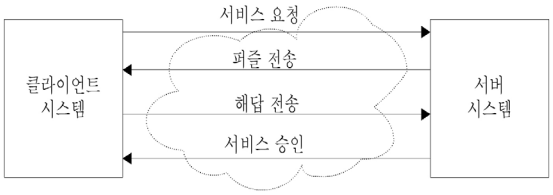


**그림 6.** 부하가중 프로토콜의 동작
**Fig. 6** The operation of weighted overload protocol

서버는 클라이언트에 대한 부하의 크기를 결정하는 퍼즐의 난이도 수준을 설정할 수 있어야 하고 퍼즐의 생성과 검증은 클라이언트가 퍼즐의 해를 계산하는데 소요되는 시간보다 작아야 한다. 이는 서버가 퍼즐의 난이도를 사용하여 대기상태인 요청 서비스로 인한 부하의 크기에 의존해서 클라이언트에게 부하를 가중시킴으로써 대규모 공격을 억제하는 효과를 달성할 수 있는 반면 클라이언트는 서버가 심각한 과부하 상태인 경우에도 일정수준의 서비스를 제공받을 수 있는 이점을 제공한다. 퍼즐의 효율성을 확대하기 위하여 퍼즐 프로토콜은 서비스 요청에 한해서 퍼즐을 전송하는 대신 서버가 퍼즐을 클라이언트에게 브로드캐스팅함으로써 시작할 수 있다[9].

## Ⅲ. 재활심리분석시스템의 지연기반 부하가중 인증모델

### 3.1. 지연기반 부하가중 인증 프로토콜

상담이나 재활이 필요한 내담자들이 심리분석시스템에 접속하여 자신의 심리 상태 및 정신적인 상태를 파악하기 위해 심리검사를 실시한다. 악의적인 사용자는 심리분석시스템에 폭주서비스를 야기함으로써 심리검사가 필요한 내담자의 서비스에 대한 거부 공격을 수행한다.

적대적인 사용자는 전자상거래를 위한 웹사이트의 사용은 가능하게 하면서 쇼핑 행위를 완료할 수 없도록 결제를 위한 보안서버시스템의 배후에서 서비스 거부 공격을 수행한다. 이는 보안서버시스템이 클라이언트로 하여금 선행작업을 요구하지 않고 과대한 처리시간이 요구되는 암・복호화 연산을 수행하기 때문이다. 보안서버시스템에 대한 서비스 거부공격에 대한 해결책으로 그림 7과 같은 퍼즐을 사용한 지연기반 부하가중 인증모델을 제안한다. 보안서버시스템에 대한 사용자의 인증요청 이후에 퍼즐 프로토콜을 구현하고 서버가 과부하상태인 경우에 클라이언트에게 암호학적 퍼즐을 전송한다. 보안서버시스템은 공개키 기반 암호화 기법을 사용하는 인증 프로토콜을 계속하기 전에 퍼즐해에 대한 응답을 기다린다. 퍼즐해에 대한 검증이 성공한 인증요청에 한해서 인증 프로토콜의 진행을 계속하고 검증에 실패한 인증 요청은 폐기한다. 서버의 부하상태가 정상이면 퍼즐 프로토콜을 우회하여 인증 프로토콜을 계속 수행한다.

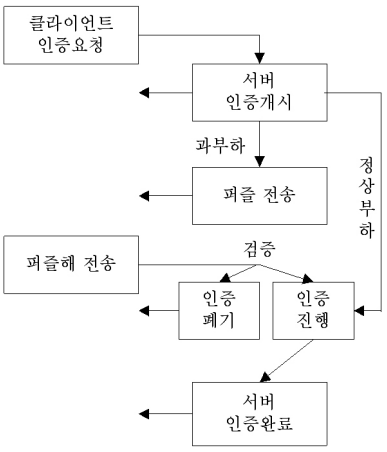


**그림 7.** 인증시스템의 부하가중 응용 프로토콜
**Fig. 7** The applied weighted overload protocol of authentication system

### 3.2. 지연기반 부하가중 인증모델의 구조

재활심리분석시스템은 내담자가 접근하여 심리검사를 받을 수 있도록 서비스를 보장하여야 한다. 공격자의 폭주서비스를 감내하기 위해 퍼즐을 통해 지연기반 부하가중 인증 모델을 제안하고 이를 구현한다. 이를 위한 시스템 아키텍쳐는 그림 8과 같다.

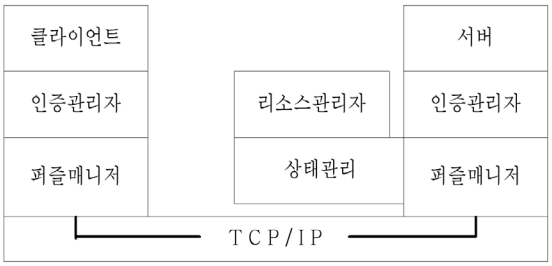


**그림 8.** 지연기반 인증 모델의 응용 아키텍쳐
**Fig. 8** The application architecture of delay based authentication model

지연기반 부하가중 인증모델에 대한 응용 아키텍쳐의 상태관리객체가 제공하는 서비스는 그림 9와 같고 리소스 관리자와 상호작용을 위한 인터페이스를 수행하고 리소스 관리자가 미리 필터링한 보안서버시스템의 지연 시간을 재필터링하여 그림 10과 같은 데이터 구조체에 폭주상태와 경계상태 그리고 정상상태에 대한 모드값을 캡슐화하여 퍼즐관리자에게 전송한다.

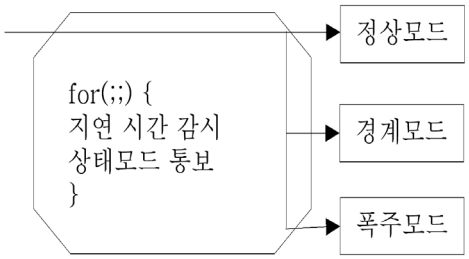


**그림 9.** 상태관리객체의 서비스
**Fig. 9** The service of state control object

**그림 10.** 상태관리객체의 데이터 구조
**Fig. 10** The data structure of state control object

인증관리자는 그림 11과 같고 클라이언트을 위한 인증관리자는 공개키 기반의 암호화 기법을 사용한 디지털 서명과 같은 인증정보를 구성하는 반면 서버를 위해

서는 디지털 서명의 인증정보를 검증하는 역할을 수행한다.

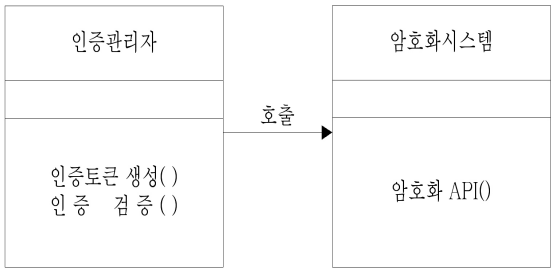


**그림 11.** 인증 관리자의 서비스 모델
**Fig. 11** The service model of authentication manager

퍼즐관리자의 제어 기능은 그림 12와 같고 서버시스템이 정상모드인 경우에는 인증 프로토콜의 진행을 계속하는 반면 경계모드와 폭주모드인 경우에는 퍼즐프로토콜을 수행시키는데 퍼즐의 난이도로서 경계모드는 제로비트수를 10으로 설정하고 폭주모드인 경우에는 제로비트수가 15인 퍼즐을 생성하여 클라이언트에게 전송하고 이후 수신한 퍼즐해를 검증하는 기능을 수행하는 반면 클라이언트를 위한 퍼즐관리자는 퍼즐해를 산출한는 역할을 수행한다.

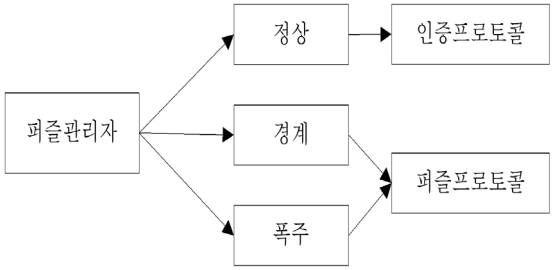


**그림 12.** 퍼즐관리자의 제어 모델
**Fig. 12** The control model of puzzle manager

퍼즐관리자는 퍼즐해에 대한 검증을 수행하고 실패한 인증 요청에 대해서는 그림 13과 같이 필터링 메커니즘을 사용하여 요청을 폐기한다. 필터링은 인증 프로토콜의 진행과 중단을 결정하는 메커니즘으로 보안서버시스템의 연산리소스에 대한 액세스를 통제한다. 클라이언트와 서버 사이에 송수신 되는 퍼즐에 대한 구조체는 그림 14와 같다.

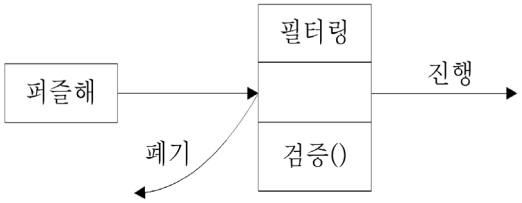


**그림 13.** 퍼즐관리자의 필터링 모델
**Fig. 13** The filtering model of puzzle manager

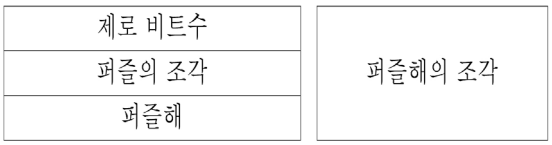


**그림 14.** 퍼즐의 구조체
**Fig. 14** The architecture of puzzle

퍼즐을 구성하는 메시지의 포맷은 난이도를 표현하는 제로 비트수와 범용파라미터로 사용하는 퍼즐조각과 퍼즐해가 되는 해쉬값을 적재할 수 있는 필드를 포함하는 반면 퍼즐해의 구조체는 퍼즐해를 산출하는데 필요한 기밀파라미터와 범용파라미터 값을 적재할 수 있도록 설계하였다. 따라서 서버는 부하의 정도에 따라 난이도를 설정함으로써 클라이언트의 부하를 가중시킬 수 있고 요청전송을 지연시킬 수 있다. 또한 서버는 퍼즐해의 산출을 위한 해쉬함수의 모든 파라미터를 수신함으로써 신속하고 손쉽게 퍼즐해를 계산하여 검증을 수행할 수 있는 반면 클라이언트는 해쉬값을 생성하는데 필요한 기밀 파라미터의 값을 반복 대입을 통하여 탐색하므로 상대적으로 연산시간이 길어지게 된다.

## Ⅳ. 재활심리분석시스템의 지연기반 부하가중 인증모델 설계 및 검증

### 4.1. 지연기반 부하가중 인증모델의 설계

지연기반 부하가중 인증모델을 적용한 인증시스템의 사례로서 메시지 보안 시스템의 인증 프로토콜 설계 및 구현[10]에 관한 연구 개발 시스템인 NMAP (New Message Authentication Protocol)을 선정하였다. NMAP는 암호방식에 기초를 둔 인증 프로토콜로 그림 15와 같이 클라이언트와 응용서버는 보안서버시스템의 인증

서비스와 암호 서비스를 사용하여 인증토큰의 구성과 검증을 수행한다.

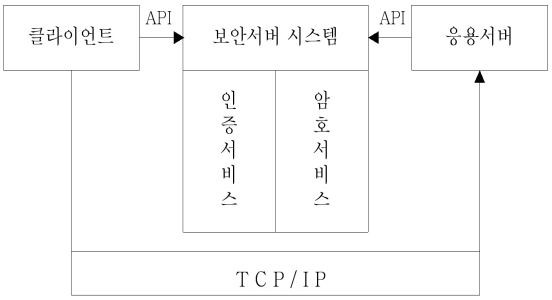


**그림 15.** NMAP 인증시스템의 아키텍쳐
**Fig. 15** The architecture of NMAP authentication system

NMAP의 인증시스템에 지연기반 부하가중 인증모델의 응용 아키텍쳐를 통합한 응용시스템구조는 그림 16과 같다. 클라이언트의 인증요청은 서버의 부하정도에 따라서 퍼즐프로토콜이 제공하는 서비스를 사용하여 약한 인증에 대한 선행작업을 수행하도록 설계하였다.

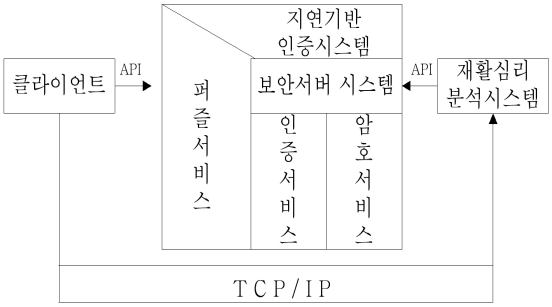


**그림 16.** 지연기반 인증시스템
**Fig. 16** The delay based authentication system

### 4.2. 지연기반 부하가중 인증모델의 검증

내담자의 심리검사를 서비스하는 심리분석시스템에서 폭주서비스에 감내하기 위해 제안된 지연기반 부하가중 인증모델의 실용성을 확인하기 위한 검증방식은 인증모듈을 사용한 NMAP 인증시스템과 인증모듈과 퍼즐 모듈을 이용한 지연기반 인증시스템을 구현하고 비교 분석하는 방식을 적용하였다. 그림 17은 비교우위의 검증을 위한 실용성 평가 모델을 보여주고 있다.

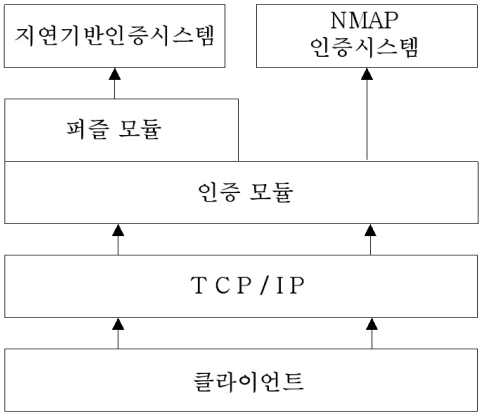


**그림 17.** 실용성 평가 모델
**Fig. 17** The evaluation model of practicality

제안 모델의 실용성을 확인하기 위한 모의실험은 초당 평균 74개의 1024 bit의 공개키 연산을 수행하는 보안서버시스템을 구축하고 초당 275KByte의 전송속도를 갖는 단일의 클라이언트를 사용하여 실험하였다.

퍼즐과 퍼즐해는 해쉬함수인 MD5를 사용하여 계산하였고 이를 구성하는 구조체의 파라미터는 표 1과 같다. 퍼즐의 해는 파라미터에 대한 비트문자열을 결합한 결합문자열을 해쉬함수의 입력값으로 하여 계산된 해쉬값을 사용하였다.

**표 1.** 파라미터의 구성요소
**Table. 1** The components of parameter

| 유형 | 전송 파라미터 |
|---|---|
| 퍼즐 | 클라이언트식별자, 서버난수, 해쉬값 |
| 퍼즐해 | 클라이언트식별자, 서버난수, 기밀파라미터 |

클라이언트는 해쉬함수에 클라이언트식별자와 범용 파라미터인 서버의 난수 그리고 기밀파라미터값의 결합문자열을 입력값으로 하여 생성된 해쉬값이 수신한 해쉬값과 동치가 될 때까지 반복대입을 통하여 기밀파라미터를 계산한다.

시스템의 상태모드는 정상과 경계 그리고 폭주로 구별하고 이에 대응하는 퍼즐의 난이도는 표 2와 같이 쉬움, 보통, 어려움으로 구성하여 실험하였다. 쉬움은 퍼즐의 구조체 필드인 제로비트 수를 5로, 보통은 10 그리고 어려움은 15로 설정하여 실험하였다.

**표 2.** 퍼즐 난이도의 파라미터
**Table. 2** The parameter of difficulty of puzzle

| 구분 | 값 | | |
|---|---|---|---|
| 상태모드 | 정상 | 경계 | 폭주 |
| 난이도 | 쉬움 | 보통 | 어려움 |
| 제로비트수 | 5 | 10 | 15 |

실험의 결과치는 표 3과 같다. NMAP 인증시스템은 사용자의 인증요청에 대하여 평균 162개까지 처리할 수 있으나 275개의 인증요청이 대기상태에 도달하면 NMAP 인증시스템은 부하로 인하여 서비스가 중단됨을 확인하였다. 그러나 지연기반인증시스템은 인증요청의 갯수가 100개 이상이면 서비스 경계상태로 150개 이상이면 폭주상태로 간주하여 퍼즐 프로토콜을 구동하는 환경하에서 평균 130개의 연결요청을 처리하고 서비스 폭주로 인한 시스템의 중단은 발생하지 않는 것을 확인하였다.

**표 3.** 인증요청의 오퍼레이션 수
**Table. 3** The operation number of authentication request

| 구분 | 평균갯수 | 폭주갯수 |
|---|---|---|
| NMAP인증시스템 | 162 | 275 |
| 지연기반인증시스템 | 130 | 폭주부재 |

따라서 퍼즐을 응용한 부하가중 인증시스템이 보안서버시스템의 서비스 거부 공격에 대한 해결책으로 적합하다는 것을 확인할 수 있다. 또한 합법적인 클라이언트는 최고 성능을 약간 희생하는 대신 중단없는 서비스를 제공받을 수 있으므로 일시에 큰 서비스 품질의 저하를 경험하지 않아도 되는 이점을 제공한다.

## Ⅴ. 결 론

인터넷 기술의 발달과 사회적 문화적 환경의 급변으로 인해 인간에 대한 존엄이 사라지고, 가정불화와 왕따와 같은 사회적이 배척으로 인해 많은 사람들이 정신적으로 심리적으로 불안한 상태에 빠져 있다. 자신이 우울증이나 불안한 상태에 있음에도 이를 인지하지 못하고 있어 상황이 더욱 심각해 가고 있다. 전통적인 지필 심리검사는 사회적 편견이나 부정확하고 주관적인 판단의 여지가 있다.

인터넷을 활용하여 심리검사를 실시하였을 때 검사의 신속한 결과를 도출하고, 검사항목에 대한 반응결과에 따라 심리적 특정을 알 수 있다. 폭주에 감내할 수 있는 재활심리분석시스템을 활용한 심리검사결과는 내담자의 문제를 해결하는데 지속적인 정보를 제공함으로써 효과적인 상담이 가능하다.

상용화되어 운영되고 있는 보안시스템은 기밀성과 무결성 그리고 가용성과 같은 보안성을 보장하는 반면 서비스 거부 공격에는 취약한 특성을 가지고 있다. 특히 공개키 기반 암호화 기법을 사용하는 인증시스템은 암복호화 속도가 느리기 때문에 인증요청의 폭주로 인해서 서비스가 중단되는 위험에 노출되어 있다. 따라서 서비스 거부공격을 억제하고 인증의 점진적인 강화를 통해서 합법적인 사용자에게 최대한의 보안성과 가용성을 제공할 수 있는 시스템의 능력이 요구된다. 이의 해결책으로 인증시스템에 퍼즐 프로토콜을 수용한 부하가중 인증모델을 제안하고 검증하였다. 퍼즐을 응용한 인증 프로토콜은 보안서버시스템이 과부하 상태인 경우에 클라이언트에게 퍼즐의 해결을 요구함으로써 불법적인 사용자에게는 부하를 가중시켜 서비스 거부 공격을 억제시키고 합법적인 사용자에게는 지속적으로 일정수준의 서비스를 제공하여 가용성을 보장하는 이점을 제공한다.

본 논문에서 제안하고 있는 퍼즐을 응용한 지연기반 부하가중 인증 모델은 인증 프로토콜의 상위계층에 퍼즐프로토콜을 계층적으로 분리 구현함으로써 향후 기능에 대한 확장의 용이성과 모듈의 재사용성을 향상시킬 수 있도록 하였다. 또한 급속하게 증가하고 있는 서비스거부공격을 억제하고 서비스의 지속성을 보장함으로써 보안서버시스템의 신뢰성과 보안성을 높여 줄 수 있을 것으로 기대된다. 향후 서비스 품질(QoS: Quality of Service) 메커니즘의 지원과 다양한 보안 시스템과의 통합을 위한 인터페이스의 개발에 대한 연구가 필요하다.

**감사의 글**

본 연구는 2013년도 나사렛대학교 학술연구지원에 의하여 수행된 논문임.

## REFERENCE


[ 1 ] Krawcyzk, H., “The Order of Encryption and Authentication for Protecting Communications,” In Proc. Crypto '01, 2010.

[ 2 ] Kargl, F., J. Maier, and M. Weber, “Protecting Web Servers from Distributed Denial of Service Attacks,” in World Wide Web, pp. 252-262, 2011.

[ 3 ] Shari, L., “A Framework for Security Requirements,” Computer & Security, Vol.10, pp.511-523, 1991

[ 4 ] Catherine, M., “A formal framework and evaluation method for network denial of service,” In Proc. 12th IEEE Computer Security Foundations Workshop, pp.4-13, 2011.

[ 5 ] Jhon, B., J. Ari, “Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks,” Proceedings of the Network and Distributed Systems Security Symposium, Feb., 2012.

[ 6 ] Boneh, D., M. Franklin, “Identity based encryption from the Weil paring,” Advances in Cryptology: Crypto, pp.213-229, 2011.

[ 7 ] Pasi, E., “Denial of Service in Public Key Protocols,” Helsinki University of Technology 2010.

[ 8 ] Tuomas, A., N. Pekka and L. Jussipekka, “DOS-resistant Authentication with Client Puzzles,” Proceedings of the International Workshop on Security Protocols, April 2012.

[ 9 ] Dean, D. and A. Stubblefield, “Using Client Puzzles to Protect TLS,” in 10th Annual USENIX Security Symposium, 2010.

[10] Young-Soo, Kim, Heung-Sik Choi,"Security Model and Application of Persistent Object using Type Information in Integrated Environment of Distributed System," *The Korea Institute of Martime Information & Communication & Sciences*, vol.4, no.1, pp661-669. June. 2004.

### 임 호 찬(Ho-chan Lim)

1995년 8월 경북대학교 심리학과 박사
1998년 3월~현재 나사렛대학교심리재활학과교수
※주관심분야: 심리검사, 재활심리시스템, 미술치료

### 김 영 수(Young-soo Kim)

2003년 8월 국민대학교 정보관리학과 박사
2013년 3월~현재 나사렛대학교산학협력단교수
※주관심분야: 재활심리시스템, 인터넷응용, 정보보안