J Korea Industr Inf Syst Res Volume 17 Number 6
http://dx.doi.org/10.9723/jksiis.2012.17.6.025

SMS를 이용하는 개선된 이중 인증 기법

(The Improved-Scheme of Two Factor Authentication using SMS)

지 선 수*
(Seon-su Ji)

요 약 시스템에 접근하려는 합법적 이용자를 구분하거나 승인하는 수단으로, 아이디(ID)와 패스워드 조합을 통한 인증 기법은 사용자에게 익숙하고, 단순하며, 비교적 수월하게 적용할 수 있다. 그러나 단일 요소를 이용하는 현재의 패스워드 인증 기법은 강력한 보안을 제공하지 않으며, 관리의 허술함으로 많은 문제점을 포함하고 있다. 또한 개별 사용자에게 패스워드 관리에 대한 모든 책임을 부과할 수 없기 때문에 보안성이 강화된 개선된 인증 기법이 필요하다. 이 논문에서는 반응시간의 적절한 범위를 확인하고, 수신 장치를 통해 SMS를 이용한 양방향 이중 인증의 새롭고, 개선된 기법을 제안한다.

핵심주제어 : 반응시간, 이중 인증, 일방향 해시함수, 일회용 패스워드, SMS, SMS 게이트웨이

Abstract Passwords are a common method of identifying and authenticating a user who wishes to log on to a secure system. Password-based authentication techniques, however, do not provide strong security and recognized as being an poor form of protection. It is not all the responsibility of the user to control password and to protect its confidentiality. In this paper, confirm an appropriate response time and I propose a new and improved method of implementing two factor authentication using SMS via receiving apparatus(mobile and email).

Key Words : One Time Password(OTP), One way Hash Function, Response Time, SMS, SMS Gateway, Two Factor Authentication

1. 서 론

언제 어디에서든 손쉽게 접근할 수 있는 인터넷 환경에서의 전자상거래와 SNS가 활성화되면서 이에 따른 보안위협이 기하급수적으로 증가되고, 개인 정보보안에 대한 중요도가 강화되고 있는 추세이다. 특히 모바일 환경에서 적극 공세형(high profile) 표적 공격, 모바일 취약점(vulnerabilities) 증가, 개인정보를 활용하여 특정 인물에게 맞춤식 공격을 하는 웨일링(whaling) 등 더욱 정교해진 공격 형태로 위협하고 있다. 이중 중대한 보안 취약점을 이용한 공격이 3배로 증가하는 등 최근 보안 환경이 급격하게 변하고 있는 것으로 나타났다. 정보보호 기술이 발전하고 있지만 대부분은 공격자에 대한 사후 대응기술이라고 볼 수 있다. 즉 사용자 인증에 대한 대응기술은 보안전문가보다는 공격자가 주도하고, 이를 모방한 기술은 재탄생되어 누구나 사용할 수 있기 때문에 완벽한 보안은 존재할 수 없다[1][2]. 그러므로 보안전문가들은 취약

* 강릉원주대학교 정보기술공학과(ssji@gwnu.ac.kr)

점 분석과 보안성 및 신뢰성을 강화시킨 인증 기법을 통해 공격자들로 부터 적극적 방어와 예방효과를 극대화하려는 방향으로 연구되어지고, 기술이 개발되고 있다.

사용자들의 보안 관리가 완벽하지 않은 현재의 상황에서 PC를 통해 이루어지는 일방향 인증 체계는 - 인간은 기억 한계, 효율성과 편리성만을 추구하고, 심리적 문제 등- 여러 가지 제약이 있을 수밖에 없다. 그럼에도 불구하고 시스템에 접근하려는 합법적 이용자를 구분하거나 승인하는 수단으로 일방향 인증(single factor authentication) 방식이 사용되어지고 있다. 즉 아이디(ID)와 패스워드 조합을 통한 인증 기법은 사용자에게 익숙하고, 단순하여, 비교적 수월하게 적용할 수 있다. 이용자들이 인증정보를 비슷하게 사용하고 있는 환경에서 주기적으로 패스워드를 변경하고 강력하게 구성하도록 유도하는 것은 현실적으로 매우 어렵고, 실행 불가능하게 보인다. 또한 개별 사용자에게 패스워드 관리에 대한 모든 책임을 부과할 수 없기 때문에 보안성이 강화되고, 개선된 인증 기법이 필요하다. 즉 보안성 강화와 편의성의 최대화에 기반을 두고, 현재의 아이디와 패스워드만을 사용하는 일방향 인증 방식에서 SMS(short message service)를 기반으로 하는 양방향 이중 인증(two factor authentication) [3][4] 방식으로 인증을 강화할 필요가 있다.

이 논문에서는 강력한 패스워드를 구현하며, SMS를 이용한 개선된 이중 인증 기법을 제안한다. 논문에서의 구성은 다음과 같다. 2장에서 SMS를 이용한 이중 인증 관련 연구에 대하여 조사한다. 3장에서는 반응시간의 적절한 범위를 확인한다. 보안성 강화와 편의성의 최대화를 기반으로 하는 강력하고, SMS를 이용한 양방향 이중 인증 방식을 구현하며, 예방적, 방어적 차원에서 SMS 반응시간을 제한하는 적극적인 보안을 구현하는 개선된 방법을 제안한다. 4장에서 예상되는 적용 결과를 가지고, 결론을 제시한다.

2. 관련연구

일반적으로 인터넷을 통한 자동화된 업무와 원격 서비스들은 합법적인 사용자의 신원을 증명하기 위해 사용자에게 아이디와 패스워드를 요구한다. 그러나 안전하지 못한 채널로 전송되는 사용자의 인증정보는 공격자에 의해 탈취되어 데이터 위변조와 범죄에 악용되고, 막대한 경제적 손실이 발생되어 사회적, 국가적 문제로 확대될 수 있다. 이러한 현실적인 문제가 있음에도 불구하고 보안이 취약한 환경을 완벽하게 개선하는 것은 불가능하다. 때문에 안전하고, 보안성이 강화된 사용자 인증을 위한 연구는 끊임없이 요구되고 있다.

사기성 해킹인 피싱(phishing), 어깨 넘어 훔쳐보기(shoulder surfing) 등을 효과적으로 방어하기 위해 일회용 암호의 개념을 그래픽으로 표현한 GOTP (graphic one time password)[5]와 SMS를 이용한 이중 인증방식이 매우 효율적일 수 있음을 제시하였다. 특히 일반 사용자들이 항상 소지하고 신뢰하는 모바일 기기를 통한 SMS와 일회용 패스워드(OTP)를 기반으로 하는 이중 인증은 보안성을 증가시킬 수 있다는 것을 보였다. 즉 사용자에게 생성된 일회용 암호를 보내기 위해 SMS 서버를 이용하며, 사용자는 웹서버에 8글자 OTP 정보를 입력함으로서 비용 효율적인(cost effective) 면에서 매우 효과적인 인증 시스템임을 확인하였다[4].

SMS 게이트웨이를 통해 메시지를 분배하며, 웹 인터페이스와 암호화 서비스가 제공되는 효율적이고 소유의 기반이 확실한 SMS 시스템을 제안하였다. 이를 이용하여 생성된 OTP는 짧은 시간 내에 유효하며, 해커로부터 추측이 불가능한 패스워드가 될 수 있음을 보였다[6]. 휴대폰을 사용한 소프트웨어 토큰 시스템을 양방향 인증을 구현하는 방법으로 하였으며, 이때 설명한 보통의 사용자는 SMS 서버에서의 소프트웨어적인 동작 등으로 60초 이후에 동작이 반응하며, 생성된지 600초 이내에 SMS를 통해 수신된 OTP가 사용될 수 있도록 하는 이용시간 제한을 제시하였다. 이때 보안성을 높이기 위해 사용자에게 전송된 OTP는 저장이 될 수 없도록 하였다. 또한 중간자 공격을 예방하기 위해 256비트 키를 이용하여 SMS 문자를 암호화할 것을 제안하였다[7].

네트워크 환경에서 정보교환의 성격과 위험 수준에 따라 지금까지 아이디와 패스워드를 이용하는 단일 요소 인증으로 일정 수준의 성과를 얻을 수 있었다. 그러나 현재 대부분의 인터넷 환경에서 다중 인증(multi factor authentication)이나 계층적 보안(layered security) 기법의 적용으로 변경되어 가는 추세이며, 이러한 이중 인증 기법은 미래의 필수적인 도구가 될 것이다. 특히 클라우드 환경에서 보안의 심리적 관점

과 신뢰성·보안성·편리성이 강화된 보안 체계를 동시에 고려하는 보안 관리가 필요하다.

3. SMS를 이용한 패스워드 설계

SMS를 이용하는 양방향 이중 인증 방식을 사용하며, 예방적, 방어적 차원에서 SMS 반응시간을 제한하는 적극적인 보안을 구현하는 개선된 방법을 고려한다. 이때 Aloul-Zahidi-El·Hajj가 제안한 이중 인증 알고리즘[7]을 참고한다.

3.1 제안된 방법

입력한 패스워드에 아이디의 일부 정보와 제한된 반응시간 범위 안에서 확인문자를 시간차에 의해 추가하는 새롭고, 개선된 일회용 패스워드를 적용하는 양방향 이중 인증 확장 알고리즘을 제안한다.

1단계 : Alice의 최초 아이디(id_A), 패스워드(pw_A), n개로 구성된 확인문자(fd_A), SMS 수신 장치(R_{SMS_A}), 입력 제한시간($response\_time = r_t$), 최초 등록시간(reg_{time_A}) 등을 서버에 등록한다. Alice의 fd_A와 최초 등록시간을 참조하여 id_A중 m개를 임의로 선택하여 salt 시스템을 적용($id_A^{'}$)하고, 해시함수를 이용한 변형된 일회용 패스워드($pw_A^{'}$)를 계산한다. 이때 $id_A^{'}$와 pw_A 정보에 일정 시간이 지난 후 fd_A가 추가되어 $pw_A^{'}$가 계산되도록 한다. $pw_A^{'}$를 서버에 저장한다.

$$Registered\{id_A, pw_A, fd_A, r_t, R_{SMS_A}\}$$
$$id_A | reg_{time_A} \rightarrow id_A^{'}$$
$$h(P(id_A^{'}, pw_A, fd_A)) \rightarrow pw_A^{'}$$
$$Save \;\; pw_A^{'}$$

여기에서 $P()$는 순열을 표시하며, $h()$는 $MD5$를 이용한 일방향 해시함수이다. 또한 SMS 수신 장치는 모바일 전화번호, 이메일 주소 등 SMS를 송수신할 수 있는 도구를 의미한다.

2단계 : Bob은 웹사이트에 접근하기 위해 아이디(id_B)와 패스워드(pw_B)를 입력한다. reg_{time_B}, salt 시스템을 적용하여 $id_B^{'}$를 선택한다. 일정한 시간이 지난 후(Pre_time)에 SMS 서버에서 등록된 수신 장치(R_{SMS_B})를 참조하여 Bob에게 '계정이 승인되도록 확인문자를 입력하시오'를 통보한다. 잠시 후에 Bob은 주어진 제한시간 범위 내에서 SMS 수신 장치를 이용하여 확인문자(fd_B)를 송신하거나 입력한다. 다음이 작동된다.

$$Input \; \{id_B, pw_B\}$$
$$id_B | reg_{time_B} \rightarrow id_B^{'}$$
$$After \; receives \; SMS,$$
$$\quad Send \;\; fd_B \;\; to \;\; server$$
$$\quad if(lo_{time} \leq response\_time \leq up_{time})$$
$$\quad\quad if(fd_A = Input(fd_B) | r_t)\{$$
$$\quad\quad\quad h(P(id_B^{'}, pw_B, fd_B)) \rightarrow pw_B^{'}$$
$$\quad\quad\quad \}$$
$$\quad else\{Reenter\,(id,\; pw)\;\; and$$
$$\quad\quad Check\; number\; of\; unsuccessful\; retries$$
$$\quad\quad \}$$

fd_B가 입력되는 것이 제한시간 영역을 벗어날 경우 아이디와 패스워드를 재입력하도록 요구하며, 이때 재시도 횟수를 계산한다.

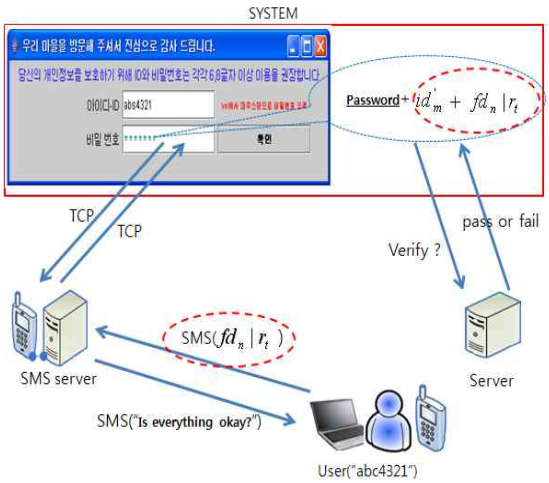
3단계 : 2단계에서 계산한 $pw_B^{'}$와 서버에 저장된 $pw_A^{'}$가 일치하는지를 확인한다.

$$Verify \;\; pw_B^{'} \oplus pw_A^{'} = 0 \,?\;\; Pass \;\; \text{or} \;\; Fail$$
$$go \;\; to \;\; [first \;\; step]$$

$pw_B^{'}$와 $pw_A^{'}$가 일치할 경우 Alice와 Bob은 동일인으로 판단하고, 시스템 접근을 허용한다. 여기에서 $\oplus$는 XOR 함수이다.

<그림 1>에서 제안된 알고리즘의 구현과정을 표현하였다. 그림에서 점선으로 표시된 영역은 논문에서 제안한 부분으로서 합법적인 사용자의 아이디에서 추

출된 일부 정보와 패스워드를 기반으로 하고, 일정한 시간이 지난 후에 시간차에 따라 확인문자가 추가되어 변경되고, 반응시간이 반영되어 확장되는 일회용 패스워드를 적용한다.



<그림 1> $id_m^{'}$, pw, fd_n, r_t 등을 적용한 OTP 구현도

SMS를 수신한 후 확인문자 fd_n을 송신하기까지의 반응시간을 확인하기 위해 ex-Gaussian 분포를 이용한 모의실험을 하였다. 참고로 ex-Gaussian 분포의 확률밀도함수(probability density function)는 (1)식으로 표현할 수 있다[8].

$$f(t) = \frac{1}{\tau\sqrt{2\pi}} e^{\left(\frac{\sigma^2}{2\tau^2} - \frac{t-\mu}{\tau}\right)} \int_{-\infty}^{\frac{t-\mu}{\sigma} - \frac{\sigma}{\tau}} e^{-\frac{y^2}{2}} dy \quad (1)$$

여기에서 t는 시간, μ는 정규분포의 평균, σ^2은 정규분포의 분산, $\tau(\tau \gg \sigma \gg 0)$는 평균과 표준편차 사이의 선형관계를 나타내는 지수적 요소이다. 또한 ex-Gaussian 분포의 평균과 분산은 (2)와 (3)식으로 각각 나타낼 수 있다.

$$mean_{ex_{-G}} = \mu + \tau \quad (2)$$

$$variance_{ex_{-G}} = \sigma^2 + \tau^2 \quad (3)$$

이 논문에서는 Heathcote, Popiel, Mewhort[8]가 적용한 수식과 모수를 사용하여 모의실험을 하였다. 이때 $\mu = 5$, $\sigma = 1.0$, $\tau = 1.0$으로 초기화하였으며, Box-Muller 변환법을 이용하였다. 또한 실제 반응시간을 확인하기 위해 135명의 SMS 사용자를 대상으로 평균 반응시간을 측정하였다.

<표 1> SMS 수신 후에 사용자의 평균 반응시간(③)

구분	τ	반응시간(ms)	
		μ_{ex-G}	σ_{ex-G}
모의실험	1.0	6,031	2,017
	1.2	6,302	2,445
	1.5	6,519	3,215
	2.5	7,507	7,459
실제적용		9,768	6,512

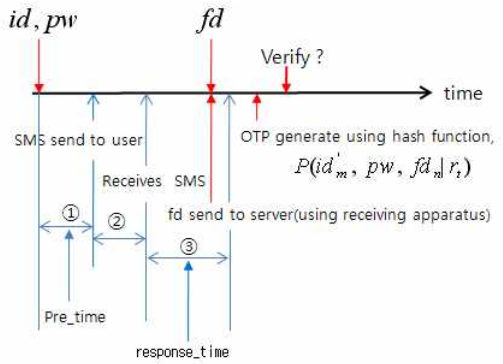
<표 1>에서와 같이 반응시간은 τ값이 증가함에 따라 평균과 분산이 근접하게 되고, 시차적으로 더 큰 가변성을 나타낸다[8]. 즉 τ값에 따라 지수적 특성이 결정됨을 확인하였다. 또한 실제 적용에 있어 반응시간은 약간의 차이가 있으며, SMS를 수신한 후 사용자는 대략 10초 내외에서 반응함을 확인하였다.

3.2 적용 및 결과

생성된 일회용 패스워드는 입력된 아이디에서 선택한 m자리 정보, n개의 확인문자, 패스워드 정보를 기반으로 한다. 즉 최초 등록시간에 따라 그 위치 조합을 다르게 한 후 $P(id_m^{'}, pw, fd_n | r_t)$의 결과에 해시 알고리즘을 적용하였다. 그리고 알고리즘을 구현하는 과정은 J2SE와 MatLab을 이용하였다. 여기에서 SMS 송수신 장비는 개인이 항상 관리하며, 가장 신뢰할 수 있는 장비임을 전제로 한다. 그리고 기본적인 검사를 위해 모바일 전화를 이용하며, SMS 서버를 통해 SMS를 송수신할 수 있다. 또한 같은 방법으로 이메일 주소를 이용하여 SMS 서버를 통해 SMS를 수신할 수도 있다.

<그림 2>에서 시차적 단계에 의해 인증자료가 추가되면서 해시함수를 통하여 생성되는 OTP를 이용하는 양방향 이중 인증 과정을 표시하였다. 공격자에게 애매 모호성을 가중시키기 위해 패스워드가 입력된 후 일정한 시간이 지난 후(①) SMS 서버에서 메시지를

송신한다고 가정한다. 여기에서 신뢰성 인증과 심리적 효과를 강화하기 위해 패스워드 및 확인문자 입력 기회 횟수와 반응시간의 범위를 제한한다. 또한 $m=3$, $n=1$, $Pre\_time \geq 5(sec)$ 이상으로 설정하였다.



<그림 2> 시차적 단계에 따라 OTP가 생성되는 과정

웹사이트에 접근하고자 아이디와 패스워드를 입력하면 인증을 위해 다음의 절차를 거치도록 한다. [첫 번째] 사용자 반응시간의 신뢰성과 안전성을 높이기 위해 Pre_time이 고려된 후(①) 일정 시간이 경과한 다음(②), SMS 서버로부터 SMS를 수신한 후에 사용자가 확인문자를 보내기까지의 응답시간(③)을 150초($25\,sec \leq ① + ② + ③ \leq 150\,sec$) 이내로 제한하여 자동으로 로그인 과정을 차단할 수 있도록 한다. reg_{time}을 이용한 난수에 따라 Pre_time과 r_t의 제한시간이 변동될 수 있도록 한다. [두 번째] 시간차에 따라 아이디의 일부 정보(id'_m), 등록된 패스워드, 제한된 시간 범위 안에서 확인문자($fd_n | r_t$) 등이 입력된 정보를 기반으로 하여, 주어진 일정한 시간 후에 해시함수를 이용한 암호화 과정을 거쳐 새로운 일회용 패스워드를 생성하도록 한다.

<표 2>에서와 같이 동일한 패스워드를 입력하더라도 <그림 2>와 같은 시간차 입력 정보의 조합방식에 따라 결과가 다른 일회용 패스워드가 구성된다. 즉 입력된 패스워드(目)에 아이디의 일부분 정보(□)와 SMS를 통한 확인문자 정보(▥)의 순서조합과 시간차 정보에 따라 다르게 추가되어 확장된 일회용 패스워드를 이용한다.

입력되는 모든 정보가 암호화되며, reg_{time}, id'_m, pw, $fd_n | r_t$, Pre_time 등을 참고로 하며, 시간차에 따라 입력된 정보를 기반으로 하여 생성된 OTP를 관리함으로서 내·외부적 및 이상적 요인에 의한 정보유출 가능성을 최소로 억제할 수 있다. <표 3>에서 패스워드 요소 적용에 따라 기존의 방법과 제안된 방법의 개선 효과를 제시하였다.

<표 2> 인증정보의 순서조합에 따라 확장되고, 변형된 OTP

입력 정보				변형된 OTP			
1차		시간	2차	형태			pw'
pw	id'	(r_t)	fd				
cba9753	u12	(…)	3	目+□	…	+▥	?Q┐琢!Q쬘戮A┐ca [B@13
				□+目	…	+▥	∀맨◂?亘b痒e?Rg‹ f5d@7
				▥+	…	目+□	[B@13 ?Q┐琢!Q쬘戮A┐ca
				▥+	…	□+目	f5d@7 ∀맨◂?亘b痒e?Rg‹

<표 3> 패스워드 요소 적용에 따른 효과

구분	P/W	OTP+P/W[7]	OTP+P/W $+fd_n \mid r_t$
적용성	높음	높음	높음
보안성	낮음	높음	높음
정보엔트로피	낮음	높음	높음
입력제한시간	-	존재	존재
심리적효과	-	높음	높음
사전/중간자 공격	높음	존재	낮음
키로깅위협	높음	낮음	낮음

x개의 패스워드를 적용할 경우 $x+(m+n)$개의 패스워드를 사용할 때와 동일한 효과가 있다. 패스워드를 입력한 후 일정한 제한된 시간 범위(r_t) 내에서 SMS의 수신자료(fd_n)를 추가하여 새롭게 생성된 일회용 패스워드를 관리함으로서 중간자 공격에 강력하게 대응할 수 있다. 즉 로그인 제한시간을 150초 이내로 하며, 패스워드에 $(m+n)$개의 글자가 시간차에 따라 추가되어 순서, 조합되므로 사용자에게는 기억의 부담을 주지 않으면서, 공격자에게는 입력되는 패스워드의 추측뿐만 아니라 SMS 수신기기를 통하는 인증자료와 입력제한의 시간차까지 추측해야 하는 무겁고,

어려운 부담을 줄 수 있다. 또한 정보엔트로피가 $0.12(x+m+n)$으로 증가되고, 입력 제한시간 r_t 정보가 추가되어 공격자에게 혼돈과 확산을 가중시킬 수 있다. 결론적으로 공격자가 인증정보를 파악하기가 불가능에 가깝다.

4. 결 론

새로운 기법의 보안기술을 개발하여 기술적인 취약점에 대응하고 예방할수록 많은 공격자들은 보안정도가 가장 허술한 이용자 로그인 요소를 탈취하려고 시도할 것이다. 그러므로 본 논문에서 제안된 방법인 로그인 요소의 양방향 이중 인증 즉, 아이디에서 선택한 일부 정보, 패스워드, SMS 수신기기를 통한 시간차 입력 정보에 의한 확인문자 등을 기반으로 하여 변경되고, 확장된 일회용 패스워드를 이용함으로서 사전공격 및 중간자 공격에 대한 차단을 완벽하게 할 수 있다. SMS를 수신한 후 사용자의 반응시간을 효과적이고, 적절하게 제한하여 심리적 효과와 보안성을 강화시킬 수 있다. 또한 정보엔트로피가 증가되어 사용자에게는 기억의 부담을 추가하지 않으면서, 공격자에게는 추측과 계산의 불확실성을 크게 확대시킬 수 있다.

참 고 문 헌

[1] 지선수, 이희춘, "최종 승인시간을 이용하는 개선된 패스워드 기법", 한국산업정보학회논문지, 제16권, 제3호, pp. 57-63, 2011.

[2] 한국 IBM, *X-Force 2011년 중반기 보안 동향 및 리스크 보고서*, 2011. 10. 5.

[3] D. A. Marra, "A Strong Authentication Mechanism for Consumer-Facing Online Transactions", MIT, Department of EECS Chisec Group, 2005.

[4] GPayments Pty Limited, *Two-Factor Authentication : An essential guide in the fight against Internet fraud* [Online] Available www.gpayments.com/, GPayments White Paper, February 2006.

[5] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", Paper presented at the 2010 International Conference on CyberWorlds, Singapore, October 2010.

[6] V. K. Katankar and V. M. Thakre, "Short Message Service using SMS Gateway", IJCSE, Vol. 2, No. 4, 2010.

[7] F. Aloul, S. Zahidi and W. El-Hajj, "Multi Factor Authentication Using Mobile Phones", International Journal of Mathematics and Computer Science, Vol. 4 , No. 2, pp. 65-80, 2009.

[8] A. Heathcote, S. J. Popiel and D. J. K. Mewhort, "Analysis of Response Time Distributions: An Example Using the Stroop Task", Psychological Bulletin, Vol. 109, Issue 2, pp. 340-347, 1991.

지 선 수(Seon-su Ji)

- 정회원
- 1984년 충남대학교 계산통계학과(학사)
- 1986년 중앙대학교 응용통계학과(석사)
- 1993년 중앙대학교 응용통계학과(박사)
- 2006년 명지대학교 컴퓨터공학과(박사수료)
- (현)강릉원주대학교 정보기술공학과 교수
- 관심분야 : 혼잡제어, 정보보안(암호키, 정보은닉), 스테가노그래피

논 문 접 수 일 : 2012년 05월 31일
1차수정완료일 : 2012년 07월 25일
2차수정완료일 : 2012년 09월 21일
게 재 확 정 일 : 2012년 10월 23일