情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

S3PAS의 교차 공격에 대한 위협성 분석*

신 동 오,[1†] 강 전 일,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

On the Security of S3PAS against Intersection Attack*

DongOh Shin,[1†] Jeonil Kang,[1] DaeHun Nyang,[1] KyungHee Lee[2‡]
[1]Inha University, [2]University of Suwon

요 약

문자와 숫자의 조합으로 이루어진 패스워드는 외우기 쉽고 사용하기 쉽지만 낮은 복잡도를 가지고 있다. 그렇기 때문에 안전하지 않은 환경에서 키보드와 같은 입력 장치를 통하여 패스워드를 그대로 입력하는 행위는 훔쳐보기와 같은 공격으로 쉽게 노출될 수 있다. 이러한 문제를 극복하고자 사용자 비밀의 형태를 다른 것으로 바꾸거나 복잡한 입력과정을 통하여 인증을 수행하는 방법들이 제안되고 있으나, 보안성과 사용자 편의성에 있어서 적합한 타협점을 찾지 못하고 있다. S3PAS는 사용자의 편의성을 만족시키면서 훔쳐보기로부터 사용자의 패스워드를 보호할 수 있는 보안성도 갖추었다고 알려진 인증기법이다. 그러나 공격자가 인증 세션을 여러 번 바라본 이후에 얻어낸 정보를 이용하여 인증을 시도하는 교차 공격에 대해서는 고려하지 않았다. 이 논문에서는 S3PAS에 대하여, 인증세션이 여러 번 공격자에게 노출되었을 때 발생할 수 있는 보안문제에 대해서 살펴보고, 사용자 실험과 모의실험을 통하여 이를 확인한다. 또한, 이러한 문제를 극복하기 위한 대안에 대하여 고찰한다.

ABSTRACT

While The passwords that combined with characters and numbers are easy to memorize and use, they have low complexity. Therefore they can easily be revealed by the shoulder-surfing attack when they are inputted through the input devices such like keyboard. To overcome these problems, many new authentication schemes, which change the user secret different form or let users input their secrets through the more complex manners, have been suggested, but it is still hard to find the balanced point between usability and security. S3PAS is one of well-known schemes which had both usability and security against shoulder-surfing attack. However, this scheme was not considered about intersection attack that the attacker tried to pass the authentication system after observing several authentication sessions. In this paper, we consider the security problem of S3PAS; what the attacker can do when he can observe the authentication sessions in several times. We confirm it through user study and experiments. And also we consider the alternative that overcomes the problem.

Keywords: Password Authentication, Alternative Password, Shoulder-surfing Resistance

I. 서 론

사용자는 길이가 짧거나 의미를 부여하여 외우기 쉬운, 그래서 공격자가 공격하기 쉬운 패스워드를 선택하는 경향이 있다. 때문에 패스워드가 공격자에게 노출되지 않도록 암호학적 기법을 이용한 인증 프로토콜을 이용하여 보안수준을 충족시키고 있다. 하지만

접수일(2010년 3월 18일), 수정일(2010년 8월 14일), 게재확정일(2010년 9월 14일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2010-0013254)
† 주저자, mannershin@isrl.kr
‡ 교신저자, khlee@suwon.ac.kr

암호학적 기법을 이용하여도 사용자가 직접 입력하는 패스워드는 악성 프로그램이나 훔쳐보기 공격으로부터 안전하지 못하다. 이러한 사실에 바탕을 두고 그 대안으로 Déjà-Vu[1], PassPoints[2], Pass-Icons[3] 같이 패스워드 대신 이미지를 이용한 그래픽 패스워드(Graphical Password) 기법들이 제안되어 왔으나 대부분이 훔쳐보기 공격에 만족스러운 보안수준을 제공하지 않고, 현재 널리 사용되어지는 패스워드 기법과 달리 실용성에 대한 문제가 아직 남아있다. Matsumoto와 Imia의 연구[4]나 Hopper와 Blum의 연구[5]는 이러한 외부 공격자로부터 사용자의 패스워드를 안전하게 보호할 수 있는 방법에 대한 것이다. 최근에는 패스워드를 입력하는 방식에서 벗어나 그래픽적인 요소를 이용하여 키로거(Key Logger)나 훔쳐보기(Shoulder-surfing 또는 Peeping), 네트워크 도청, 감춰진 카메라 등의 외부 공격에 안전하면서도 입력하기 쉬운 방법에 대한 연구도 진행되고 있다[6-8].

H. Zhao등이 제안한 S3PAS[9]는 문자를 이용하면서도 그래픽 패스워드와 유사한 인증 방법을 통해 훔쳐보기 공격으로부터 안전하도록 설계된 인증기법이다. 하지만 공격자가 사용자의 인증세션을 여러 번 바라보았을 때 교차공격에 대한 위협성에 대해서는 고려하지 않고 있다. 이 논문에서는 사용자 실험을 토대로 교차공격에 대한 S3PAS의 위협성에 대해서 살펴본다.

이 논문의 2장에서는 S3PAS와 유사한 연구들에 대한 소개와 이러한 기법들이 가진 특성을 분석하고 문제점에 대해서 살펴본다. 3장에서는 공격할 대상인 S3PAS의 기법에 대한 소개와 교차공격에 대한 안전성을 살펴본다. 4장에서는 사용자 실험을 토대로 시뮬레이션을 통해 이를 입증한다. 5장에서는 이러한 문제를 보완할 수 있는 방법 을 제시한다. 6장에서는 이 논문의 결론을 담는다.

II. 관련 연구

훔쳐보기 등의 외부 공격으로부터 안전하도록 사용자를 보호하는 인증 기법들은 그 수가 매우 많으나, 이 논문에서는 비밀을 직접 이용하지 않고 비밀을 이용하여 특정한 연산을 하는 패스워드 입력 방식에 대하여 논의한다.

2.1 PAS(Predicate-based Authentication Services)

X. Bie등이 제안한 PAS[10]는 사용자가 갖고 있는 비밀과 검증자(Verifier)로부터 전달되는 임의의 수를 이용하여 술어(Predicate)를 생성하고 이를 이용하여 인증을 한다. 인증을 위해 사용자는 두 개의 비밀을 생성하고 기억해야 한다. 인증과정은 사용자가 특정한 연산을 수행하도록 구성되어있다. 비밀의 형태는 연속된 두 자리의 숫자와 연속된 다섯 자리의 문자로 이루어져있다. 사용자의 비밀을 각각 '23 sente'와 '41 logig'로 설정했다고 하자. 인증의 첫 번째 과정은 사용자가 선택한 비밀 중에서 문자를 하나 선택하는 것이다. 사용자가 인증을 할 때 검증자는 임의의 숫자 I를 사용자에게 제시한다. 예를 들어, 검증자가 $I=15$를 제시하면 사용자는 자신이 갖고 있는 비밀의 문자열 부분에서 I번째의 문자를 찾는다. 만약 I값이 문자열의 길이 보다 크다면, 순회하여 I번째 문자를 선택한다. 비밀과 I가 위와 같을 때 각각의 비밀에서 'e'와 'g'가 선택되고, 술어는 숫자 부분과 선택된 문자의 조합인 '23e', '41g'가 된다. 두 번째 과정에서 검증자는 사용자에게 두 개의 도전 표를 제시한다. 도전 표는 5*5 셀로 구성되어 있고, 각 셀에는 임의의 문자 13개가 들어 있다. 사용자는 술어의 숫자 부분을 (x,y) 좌표처럼 사용하여 연산할 셀을 구하고, 술어의 문자가 해당 셀에 들어있는지 확인한다. 만약 들어있다면 'yes'를, 들어있지 않다면 'no'를 기억한다. 이 작업을 각각의 도전 표에 대해서 수행하면 사용자는 각 술어마다 (yes, yes), (yes, no), (no, yes), (no, no)의 쌍 중 하나를 만들 수 있게 된다. 세 번째 과정은 위에서 만든 술어의 'yes no' 쌍을 이용하여 이루어진다. 검증자는 행과 열이 (yes, yes), (yes, no), (no, yes), (no, no)로 이루어진 CAPTCHA 표를 사용자에게 제시한다. 사용자는 이 표에서 자신의 술어로 만든 'yes no' 쌍을 이용하여 하나의 셀을 선택할 수 있다. 선택한 셀의 CAPTCHA 문자를 입력함으로써 하나의 라운드가 종료된다.

이 기법에서는 SAT 계산기(solver)에 기존의 기법들이 모두 약하다는 사실을 지적하고 자신들의 기법이 SAT 계산기에 더 안전할 수 있음을 주장하고 있다. 그러나 여전히 증가된 안정성이 미미하다.

2.2 Pass-Icons

S. Wiedenbeck등이 제안한 Pass-Icons[3]는 이 논문의 주제인 S3PAS[9]의 모태가 되는 인증 방법이다. Pass-Icons에서 사용자는 자신이 인증에 사용할 Pass-Icon을 3개에서 5개 정도 선택한다. 검증

자는 사용자의 패스 아이콘들을 포함하여 아이콘들이 무작위로 배치된 이미지를 사용자에게 주고, 사용자는 배치된 아이콘들 중에서 자신이 선택한 패스 아이콘들을 모두 찾는다. 검증자가 준 이미지에는 사용자가 선택한 패스 아이콘들이 모두 들어있을 수도 있고, 그 중 일부만 들어있을 수도 있다. 사용자는 자신이 선택한 패스 아이콘들을 이용하여 머릿속으로 다각형을 그린다. 그리고 자신이 머릿속으로 그린 다각형 안에 속한 아이콘들 중 하나를 선택하면 인증이 된다. 이를 충분한 횟수만큼 반복한다.

Pass-Icons에서 사용자가 선택한 패스 아이콘들이 나타나는 경우에 대한 순서의 무작위성 때문에 공격자는 사용자의 패스 아이콘들을 쉽게 추측하지 못한다. 반면에 S3PAS에서는 순서를 갖는 패스워드 문자들을 이용하여 삼각형을 그려서 그 안에 있는 문자를 선택하는데, 이러한 특성으로 인하여 보안성은 Pass-Icons보다 낮을 수밖에 없다. 이러한 문제는 3장에서 보다 자세하게 다루도록 한다.

III. S3PAS의 소개 및 위협성 분석

3.1 표기

훔쳐보기 공격으로부터 사용자의 패스워드를 보호하기 위해 H. Zhao등은 S3PAS[9]를 제안하였다. 하지만 이 기법은 사용자의 패스워드 입력 세션을 여러 번 바라보면 패스워드가 노출되는 문제점이 존재한다. 훔쳐보기 공격은 사용자의 패스워드 입력에 사용되는 모든 요소를 훔쳐본다고 가정하기 때문에, 사용자의 패스워드를 얻어내기 위한 악의적인 프로그램(e.g. 키로거)보다 더욱 강한 공격이다. 이 논문에서는 공격자가 사용자의 인증 세션을 여러 번 바라볼 수 있다고 가정한다.

이 논문에서는 기술의 편의를 위해서 [표 1]과 같은 표기를 사용한다.

[표 1] 표기법

기호	설명
T	S3PAS 기법에서 선택가능 한 문자의 집합. 이 논문에서는 영문자의 대소문자, 숫자, 특수문자를 집합 T의 요소로 본다.
k	사용자의 패스워드 문자열
$\|m\|$	문자열 m의 길이
k_i	i번째 패스워드 문자. 인증화면에서 자신의 좌표 값 정보를 갖고 있다.
S_i	i번째 단계에서 사용자가 선택한 문자. 인증화면에서 자신의 좌표 값 정보를 갖고 있다.
P_i	계산을 통해 추정한 i번째의 패스워드 문자. 인증화면에서 자신의 좌표 값 정보를 갖고 있다.
C_i	P_i를 중심으로 패스워드의 가능성이 있는 문자들을 모아둔 후보군
C_{in}	n은 세션번호, i는 C_i에서의 i와 같다. C_{in}는 n번째 세션에서의 C_i를 의미한다.

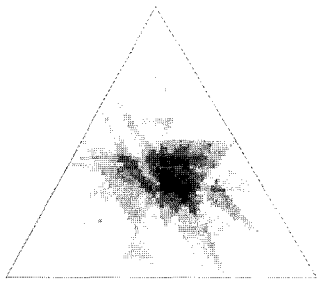
3.2 S3PAS의 기법 소개

인증을 하기 위해서 사용자는 자신의 모든 패스워드 문자를 [그림 1]과 같은 인증 화면에서 찾아야 한다. 그 후에 사용자는 "pass-triangle"이라고 불리는 삼각형을 다음과 같이 그린다. 사용자는 인증 화면에서 $1 \le i \le |k|$인 모든 자연수 i에 대해서, ($k_{i(\mathrm{mod}|k|)}$, $k_{(i+1)(\mathrm{mod}|k|)}$, $k_{(i+2)(\mathrm{mod}|k|)}$, 앞으로는 $(\mathrm{mod}|k|)$를 생략하고 설명한다.)의 세 패스워드 문자를 인증 화면에서 각각 찾고, 이를 꼭짓점으로 갖는 삼각형을 머릿속으로 그린다. 사용자는 이 삼각형 내부에 위치한 문자 중 하나를 선택하고 이를 S_i이라 한다.

이 기법은 사용자에게 S_i을 임의대로 선택하도록 요구하지만 우리가 실시한 실험에 따르면 사용자들은 삼각형 내의 임의의 문자를 선택하는 것이 아니라 일정한 패턴에 따라 S_i를 선택하였다. S_i가 일정한 패턴을 가지게 되면 공격자가 패스워드 후보군을 구하는 것이 용이해지고, 이를 통해 사용자의 패스워드를 알아낼 수 있게 된다.

!	0	?	N	]	A	}	"	@	1
O	^	z	|	#	2	{	P	_	y
~	$	a		Q	'	x	`	%	4
C	R	3	w	&	5	D	S	b	v
	6	E	T	c	u	(	7	F	U
d	e	t	)	8	G	V	B	s	*
9	H	W	g	r	+	:	I	x	h
q	,	;		y	i	p	-	<	K
Z	j	o	.	=	L	[	k	n	>
/	M	\		J		l	m	f	

[그림 1] S3PAS에서 사용되는 인증 화면



〔그림 2〕 사용자의 패턴

3.3 S3PAS 사용자 실험 및 결과

20대의 대학생 43명을 대상으로 사용자 실험을 진행하였다. 실험에는 집합 T의 요소를 무작위로 배치한 10×10 문자표와 패스워드 "ABC"를 제시하고, S3PAS에서 제안한 방법과 같이 본인 스스로 세션 패스워드를 선택하도록 하였다. 실험은 서로 다른 문자표에 대해 10회 실시되었다. 사용자 실험에 사용된 문자표가 다르므로 그에 따라 "ABC"로 그려지는 삼각형의 모양 역시 달라진다. 사용자 실험으로부터 사용자의 패턴을 찾기 위해 각 실험에 사용된 삼각형을 〔그림 2〕와 같은 정삼각형 모양으로 변환하였다. 사용자 실험에서 사용자가 선택한 점의 위치도 동시에 변환되므로 그 위치를 정삼각형 위에 표시하고 분포를 조사하였다.

사용자 실험 결과 〔그림 2〕와 같은 모양의 분포가 형성되었다. 삼각형의 무게중심 근처를 세션 패스워드로 선택하는 경향이 있었고, 삼각형의 꼭짓점은 거의 선택하지 않았다. 삼각형의 변도 많이 선택하지 않았다. 많은 피실험자들이 인증 실패에 대한 우려 때문에 세션 패스워드를 조금 더 안전하게 선택하려고 하는 경향이 있다는 것을 알 수 있었다. 우리는 사용자의 이러한 패턴을 바탕으로 시뮬레이터를 제작하였다. 시뮬레이터를 이용한 모의실험에서는 무작위로 인증화면을 만들고, 무작위로 패스워드를 생성하였다. 따라서, 패스워드의 선호도는 반영되지 않는다. 그 후 사용자의 패턴을 반영한 세션 패스워드를 자동으로 생성하였다. 이렇게 생성된 인증세션을 바탕으로 다음 장에서와 같은 교차 공격을 수행하였다.

3.4 S3PAS 기법에 대한 교차 공격

3.4.1 패스워드 추측과 후보군 모집

〔그림 2〕와 같은 사용자의 패턴을 이용하기 위해 인수 a, $(2 \le a \le 4)$가 사용된다. a의 값은 〔그림 2〕에서 나타난 사용자의 패턴별로 다르게 부여된 가중치에 따라 무작위로 결정된다. 사용자가 선택하는 세션 패스워드 S_i가 원본 패스워드 P_i와 관련하여 각 문자의 좌표 값에 대해서 다음과 같은 수식을 만족한다고 가정하면

$$S_i = (P_i + P_{i+1} + P_{i+2})/a \tag{1}$$

$k=4$일 때,

$$\begin{aligned} aS_1 &= P_1 + P_2 + P_3 \\ aS_2 &= P_2 + P_3 + P_4 \\ aS_3 &= P_3 + P_4 + P_5 = P_3 + P_4 + P_1 \\ aS_4 &= P_4 + P_5 + P_6 = P_4 + P_1 + P_2 \end{aligned} \tag{2}$$

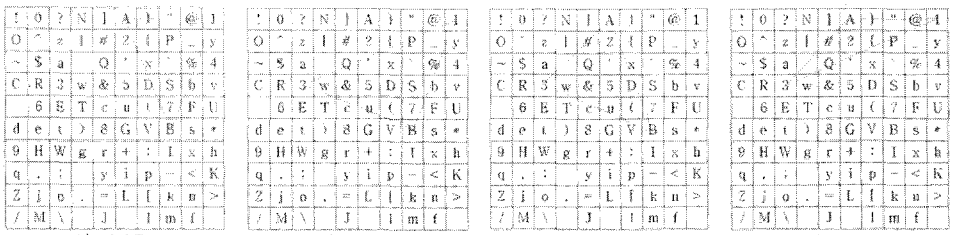
가 성립하므로 패스워드의 위치는 다음과 같이 추정할 수 있다.

$$\begin{aligned} P_1 &= \frac{a(S_1+S_3+S_4)-2(P_2+P_3+P_4)}{3} \\ &= \frac{a(S_1-2S_2+S_3+S_4)}{3} \\ P_2 &= \frac{a(S_1+S_2+S_4)-2(P_1+P_3+P_4)}{3} \\ &= \frac{a(S_1+S_2-2S_3+S_4)}{3} \\ P_3 &= \frac{a(S_1+S_2+S_3)-2(P_1+P_2+P_4)}{3} \\ &= \frac{a(S_1+S_2+S_3-2S_4)}{3} \\ P_4 &= \frac{a(S_2+S_3+S_4)-2(P_1+P_2+P_3)}{3} \\ &= \frac{a(-2S_1+S_2+S_3+S_4)}{3} \end{aligned} \tag{3}$$

이때, S_1, S_2, S_3, S_4는 사용자가 선택한 문자이므로 훔쳐보기 공격을 통해 알 수 있다. 사용자들이 무게중심 부근에 있는 문자를 세션 패스워드로 선택하는 경향이 있다는 사실로부터, 우리가 알고자 하는 사용자의 패스워드는 P_i이거나 P_i에서 가까운 곳에 존재하는 문자일 가능성이 높다.

예를 들어 〔그림 3〕처럼 패스워드가 'A1B3'이고 세션 패스워드 $S_1 \sim S_4$가 'P', 'D', '5', '2'이라고 하자.(이는 논문[9]의 예시이다.) 이를 식 (3)에 대입하여 패스워드를 추정해보면 〔표 2〕와 같다.

a가 2~4일 때 모든 문자를 C_i로 편입한다. 추정한 패스워드 문자들의 각 위치가 정확하게 일치하지는 않



1) A1B 2) 1B3 3) B3A 4) 3A1

〔그림 3〕 인증 화면과 'A1B3'에 대한 'pass-triangle'

〔표 2〕 a에 따른 추정 패스워드 문자들의 좌표

P_i \ a	2	3	4
P_1	'}' (4,0)	'A' (5,0)	'"' (7,0)
P_2	']' (6,0)	'@' (8,0)	'1' (9,0)
P_3	'(' (6,4)	's' (8,5)	'K' (9,7)
P_4	'E' (2,4)	't' (2,5)	':' (2,7)

지만 P_i 주변에 k_i가 존재함을 〔그림 1〕에서 쉽게 확인할 수 있다. 따라서 추정한 위치를 기점으로 하여 후보군 C_i를 구한다면, 적은 횟수의 훔쳐보기 공격으로도 패스워드를 알아낼 수 있을 것이다. 만약 다른 세션과의 교차 공격으로부터 얻어지는 결과가 아무것도 없다면 a의 값을 1~5처럼 다시 조절한 뒤 C_i를 다시 모집한다.

3.4.2 교차 공격

교차공격을 하기 위해서 또 다른 후보군이 필요하므로, 우리는 〔그림 4〕의 문자표에 대해서 또 하나의 후보군을 모집하였다. 예를 들어 패스워드는 동일하며, 세션 패스워드 $S_1 \sim S_4$는 T, m, 7, *라고 할 때, 앞에서와 동일한 과정을 거쳐서 C_i를 구하고, 각각의

s	:	~	%		Z	-	.	u	?
	4	|	E	$	B		t	′	j
x	)	,	r	d	b	=	f	p	〉
#	L	V	U	m	w	!	O	o	h
1	Y	T	8	7	K	3	{		9
〈	F	*	J	″	z	[	n	0	R
&	5	I	2	G	g	6	X	v	a
M	A	k	^	@	+	/	S	e	C
}	D	]	Q	H	q	P	`	N	\
c		W	:		_	y	(	i	l

〔그림 4〕 S3PAS의 인증 화면

〔표 3〕 a값의 변화에 따른 교집합 결과

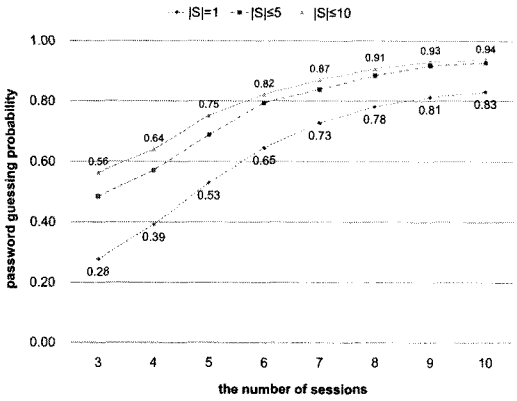
$C_1 \cap C_2$ \ a	2	3	4
$C_{11} \cap C_{21}$	{'#'}	{'A', ']'}	
$C_{12} \cap C_{22}$		{'1'}	{'1'}
$C_{13} \cap C_{23}$	{'B'}	{'B'}	{')'}
$C_{14} \cap C_{24}$		{'3', '6'}	

세션에서 구한 C_i에 대해서 교집합을 구하면 〔표 3〕과 같다.

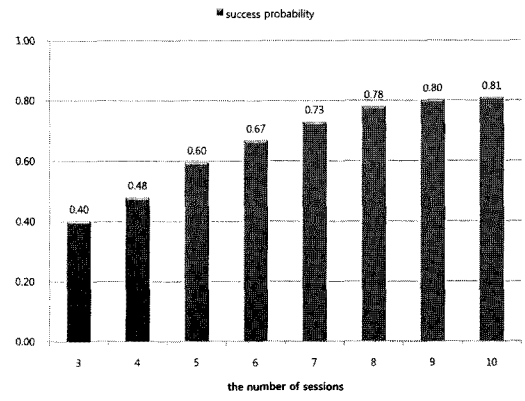
이러한 결과에서 알 수 있듯이, 각 패스워드 문자가 교집합 안에 존재한다. 우리는 이 교집합의 결과를 조합하여 임의의 패스워드 문자열로 만들고 이를 모든 세션에 대입하였다. 공격자가 바라본 모든 세션에 대해서 이 임의의 패스워드 문자열과 각 세션의 세션 패스워드로 가상의 인증을 시도해보고, 인증이 성공한다면 그 조합은 원본 패스워드일 가능성이 높다.

IV. 실험

우리는 사용자 실험을 통하여 알게 된 사용자의 입력 패턴을 모방하는 인증자 시뮬레이터를 작성하고, 자동화된 모의실험을 실시하였다. 모의실험에서는 검증자와 인증자가 공유하는 패스워드를 임의로 생성하고, 검증자는 인증 화면을 무작위로 생성하여 인증자에게 전달한다. 인증자 시뮬레이터는 패스워드와 검증자로부터 받은 인증 화면을 이용하여 사용자 실험에서 나타난 입력 패턴을 따라 세션 패스워드 $S_1 \sim S_4$를 선택하고, 이 세션 패스워드를 검증자에게 전달한다. 검증자는 인증자가 보낸 세션 패스워드가 올바른지 판단한다. 이 과정에서 공격자가 훔쳐보는 것은 인증 화면과 세션 패스워드 이다. 공격자는 훔쳐본 정보들을 이용하여 앞서 설명한 것과 같이 교차 공격을 수행하였다. 실험에서 사용자의 패스워드는 4자리로 임의로 선택하였으며, 공격자는 하나의 패스워드에 대해서 총



〔그림 5〕 관찰 횟수와 그에 따른 원본 패스워드 추정확률의 변화 ($|S|$: 추정 패스워드 집합의 원소의 개수)



〔그림 6〕 관찰 횟수와 그에 따른 통과 기대 확률

10번까지 인증 세션을 관찰하는 것으로 가정하였다. 위와 같은 실험을 독립적으로 1,000번 반복하였다.

〔그림 5〕는 공격자가 인증 세션을 관찰한 횟수와 그에 따른 패스워드 추정 확률을 보여준다.

$|S|$는 실험의 결과로 추정한 패스워드의 개수를 의미하고, 패스워드 추정 확률은 $|S|$개의 추정 패스워드 안에 원본 패스워드가 포함되는 경우만을 고려하였다.

인증 세션을 3번 바라보았을 때, $|S|=1$인 경우는 28%로, 네 번 중 한 번은 확정적으로 원본 패스워드를 알 수 있을 것이라 기대할 수 있다. 10번 정도 바라보면 약 83%의 확률로 사용자의 원본 패스워드를 알 수 있을 것이다. 이처럼 세션을 많이 바라보면 많이 바라볼수록 사용자의 패스워드를 정확히 알 수 있게 될 확률이 높아진다. $|S|\leq 5$와 $|S|\leq 10$의 그래프를 보면 그 확률에 큰 차이가 없는 것을 확인할 수 있다. 이것은 실험의 결과로 얻어진 추정 패스워드의 개수는 보통 5개 이하라는 것을 말해준다. 실험 결과로 얻어낸 추정 패스워드의 개수가 대체로 적기 때문에 공격자는 얻어진 결과로 어렵지 않게 인증을 시도할 수 있을 것이다.

〔그림 6〕은 바라본 횟수에 따른 인증 성공 기대확률을 나타낸 것이다. 인증 성공 기대확률

$$P_r[Expected\ success] = \sum_{i=1}^{\infty} \frac{1}{i} P_r[|S| = i] \qquad (4)$$

로 표현할 수 있다. 3회 바라보았을 때 공격자가 추정한 패스워드가 인증을 통과할 수 있는 기대 확률이 40%정도이다.

V. S3PAS의 안전성 향상 방법 : 추후 고려 가능한 연구방향성 제시

S3PAS의 문제는 원본 패스워드만을 이용하여 "pass-triangle"를 구성한다는 것에 있다. 사용자 실험에서 보여주었듯이 사용자들은 S3PAS 시스템에서 특정한 패턴을 보여주었고, 공격자는 이 사용자 패턴을 이용한 교차 공격을 통해 사용자의 패스워드를 〔그림 5〕와 같이 어렵지 않게 알아낼 수 있었다. 이러한 연관성은 세션 패스워드가 원본 패스워드의 특정 위치의 패스워드와 깊게 연관되었기 때문에 발생하는 것이다. 이러한 깊은 연관성을 낮추기 위해 인증 시스템에서는 "pass-triangle"을 구성하는 3개의 꼭짓점 중 하나를 무작위로 정해준 뒤 인증 화면과 같이 사용자에게 제시한다. 요즘 인터넷에서 널리 사용되는 패스워드의 길이가 6자 이상인 것을 감안하여 첫 번째 "pass-triangle"은 (k_1, k_2, R_1), 두 번째는 (k_3, k_4, R_2), i번째는 (k_{2i-1}, k_{2i}, R_i), $(R_i \in T)$ 으로 구성하여 S3PAS 시스템을 보완한다면 우리가 사용한 방법의 교차 공격으로는 사용자의 비밀번호를 추정하기 어려워진다. 또한 각각의 세션 패스워드문자에서 존재했던 원본 패스워드 문자와의 연관성이 3개에서 2개로 낮춰지게 된다.

이 보완방법은 인증 시스템이 준 임의의 꼭짓점과 사용자가 선택한 세션 패스워드를 이용하면 T에서 제외할 수 있는 문자들이 생기게 되기 때문에, 역시 다수의 인증을 훔쳐보는 공격에 대해서 문제가 발생하게 된다. 또한 공격자 역시 삼각형의 세 꼭짓점 중 인증 시스템이 주는 임의의 점을 알게 되므로, 삼각형의 평균 넓이가 7이라는 정보 및 임의의 점을 하나의 꼭짓점으로 가졌을 때 삼각형이 그려질 수 없는 위치의 문자들을 배제한 뒤 이를 이용하여 무작위 시도를 한다면 이에 대한 통과확률이 증가할 것이다. 그러나 무작

위 시도공격과 교차공격 사이에서 균형점을 찾는 것이 바람직하므로 이러한 제한은 충분히 고려될만하다 [11]. 제안하는 기법에서 가능한 문제에 대한 분석 및 연구는 추후 연구로 남긴다.

VI. 결론

이 논문에서는 S3PAS의 소개와 적은 수의 인증 세션을 바라본 공격자가 교차 공격을 통해 사용자의 패스워드를 어렵지 않게 알아낼 수 있다는 것을 보였다. 교차 공격은 주어진 집합들이 서로 다를수록 큰 효과를 보일 것이고 이를 방지하기 위해 임의성을 줄이게 되면 반대로 재전송 공격에 대해 약한 모습을 갖게 될 것이다. S3PAS에서 사용자에게 주어지는 테이블의 임의성은 재전송 공격과 교차 공격의 보안성에 밀접하게 관련되어 있으며 이들 사이에는 타협 관계가 존재한다. 더해서 사용자의 입력 또는 선택이 제한된 집합으로부터 발생한 것이라면 무차별적인 인증 시도 또한 무시할 수 없는 공격이 될 수 있으며, 이 확률을 낮추려 집합의 크기를 단순히 확장한다면 HCI (Human-Computer Interaction)관점에서 사용자의 접근성을 떨어뜨리기 때문에 설득력이 있는 기법이 되기는 힘들 것으로 보인다. 지금은 논문[11]과 같이 교차공격/무작위 시도/재전송공격이 균형을 이루는 인증 방법이 필요하다. 더 나아가 사용자 편의성이 재고된 기법이 필요한 시점이라고 할 수 있다.

참고문헌

[1] R. Dhamija and A. Perrig, "Déjà Vu: A User Study Using Images for Authentication," Proc. of 9th USENIX Security Symposium, p. 4, Aug. 2000.

[2] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskily, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical passwords system," International Journal of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), vol. 63, pp. 102-127, May 2005.

[3] S. Wiedenbeck, J. Waters, L. Sobrado, and J.C. Birget, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme," Proc. of Advanced Visual Interfaces (AVI), pp. 177-184, May 2006.

[4] T. Matsumoto and H. Imai, "Human Identification Through Insecure Channel," Proc. of EUROCRYT 91, LNCS 547, pp. 402-421, 1991.

[5] N. Hopper and M. Blum, "Secure Human Identification Protocols," Proc. of ASIACRYPT, LNCS 2248, pp. 52-66, 2001.

[6] D. Weinshall, "Cognitive Authentication Schemes Safe Against Spyware (Short Paper)," Proc. of the 2006 IEEE Symposium on Security and Privacy (S&P), pp. 1-16, May 2006.

[7] P. Golle and D. Wagner, "Cryptanalysis of a Cognitive Authentication Scheme (Extended Abstract)," Proc. of the 2007 IEEE Symposium on Security and Privacy (S&P), pp. 66-70, May 2007.

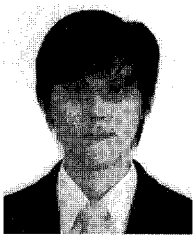
[8] H. Jameel, R.A. Shaikh, H. Lee, and S. Lee, "Human Identification Through Image Evaluation Using Secret Predicates," Proc. of The Cryptographer's Track at RSA Conference (CT-RSA), LNCS 4377, pp. 67-84, 2007.

[9] H. Zhao and X. Li, "S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), vol. 2, pp. 467-472, 2007.

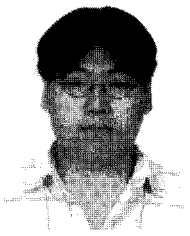
[10] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, "PAS: Predicate-based Authentication Services Against Powerful Passive Adversaries," Proc. of 2008 Annual Computer Security Applications Conference (ACSAC), pp. 433-442, Dec. 2008.

[11] 강전일, 맹영재, 양대헌, 이경희, 전인경, "행렬 상에서 문자 간 연산을 수행하는 패스워드 인증 기법," 한국정보처리학회논문지, 19(5), pp. 175-188, 2009년 10월.

〈著者紹介〉

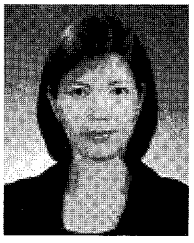


신 동 오 (DongOh Shin) 학생회원
2010년 2월: 인하대학교 컴퓨터 공학과 졸업
2010년 3월~현재: 인하대학교 정보공학과 석사 과정
〈관심분야〉 인터넷 보안, 네트워크 보안



강 전 일 (Jeonil Kang) 학생회원
2003년 2월: 인하대학교 컴퓨터 공학과 졸업
2006년 2월: 인하대학교 정보통신대학원 석사
2006년 3월~현재: 인하대학교 정보공학과 박사 과정
〈관심분야〉 RFID 보안, 생체 인식 보안, WSN 보안, 무선 인터넷 보안, 웹 인증 보안

양 대 헌 (DaeHun Nyang) 정회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 정보통신대학원 부교수
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안



이 경 희 (KyungHee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 조교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식