Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1159

어깨너머공격 모델링 및 보안 키패드 취약점 분석*

김 성 환,† 박 민 수, 김 승 주‡
고려대학교 정보보호대학원

Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes*

Sung-hwan Kim,† Min-su Park, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

스마트폰, 태블릿 PC와 같은 스마트 기기들의 사용이 증가하면서 애플리케이션을 이용한 금융 업무 등 중요 업무를 해당 스마트 기기를 이용하여 처리하는 경우가 많아지고 있으며, 이러한 정보를 획득 할 수 있는 여러 공격들이 존재하고 있다. 그 중 사회공학기법인 어깨너머공격은 해킹 기술과 같은 특정 컴퓨터 기술 없이도 직접적으로 정보를 획득할 수 있어 강력한 공격 방법으로 꼽힐 수 있다. 그러나 지금까지의 어깨너머공격은 사용자 모르게 정보를 엿보는 행위라는 단순한 정의밖에 존재하지 않았다. 또한, 국제표준인 공통평가기준(CC)의 공통평가방법론(CEM)에서 제공하는 attack potential 방법론은 어깨너머공격에 대한 내성을 정량적으로 나타내지 못하는 한계를 가지고 있다. 이에 본 연구에서는 어깨너머공격에 필요한 공격조건들을 나열하고 공통평가기준에서 제공하는 공격 성공 가능성(attack potential)의 방법론을 차용하여 어깨너머공격까지 공격 성공 가능성을 계산할 수 있도록 이를 포함할 수 있는 공격 성공 가능성을 제안한다. 더불어, 현재 스마트 기기들에 제공되고 있는 모바일뱅킹 애플리케이션의 보안 키패드인 쿼티 키패드와 숫자 키패드의 안전성을 분석하고 공격 시나리오를 기반으로 하여 현재 제공되고 있는 모바일뱅킹 애플리케이션들의 어깨너머공격에 대한 공격 성공 가능성을 알아본다.

ABSTRACT

As the use of smartphones and tablet PCs has exploded in recent years, there are many occasions where such devices are used for treating sensitive data such as financial transactions. Naturally, many types of attacks have evolved that target these devices. An attacker can capture a password by direct observation without using any skills in cracking. This is referred to as shoulder surfing and is one of the most effective methods. There has been only a crude definition of shoulder surfing. For example, the Common Evaluation Methodology(CEM) attack potential of Common Criteria (CC), an international standard, does not quantitatively express the strength of an authentication method against shoulder surfing. In this paper, we introduce a shoulder surfing risk calculation method supplements CC. Risk is calculated first by checking vulnerability conditions one by one and the method of the CC attack potential is applied for quantitative expression. We present a case study for security-enhanced QWERTY keyboard and numeric keypad input methods, and the commercially used mobile banking applications are analyzed for shoulder surfing risks.

Keywords: Shoulder surfing attack, Attack potential, Security Keypad

접수일(2014년 8월 21일), 수정일(2014년 10월 14일), 게재확정일(2014년 11월 3일)

* 본 연구는 방위사업청과 국방과학연구소의 지원(계약번호 UD100002KD) 및 교육과학기술부와 한국연구재단의 지역혁신인력양성사업으로 수행된 연구결과입니다.

† 주저자, tonykimsh@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr (Corresponding author)

I. 서 론

인터넷과 모바일, 무선통신 등의 기술이 발전하면서 모바일 단말은 점점 더 소형화되었고 통신 속도는 더욱 고속화되었다. 이에 따라 모바일 단말은 스마트폰 시대로 진화하였고, 사용자들은 공개된 SDK (Software Development Kit)를 사용하여 다양한 애플리케이션을 개발하고 콘텐츠들을 이용할 수 있게 되었다. 한국은행에서 제공한 2014년 1/4분기 국내 인터넷뱅킹서비스 이용현황에 따르면, 2009년 말부터 지속된 스마트폰의 사용증가는 2014년 1월 약 3천 7백만 명의 가입자 수를 보유하게 되었으며, 지속적으로 증가추세에 있다[1]. 스마트폰뿐만 아니라 태블릿 PC의 사용도 지속적으로 증가하여 2014년 1월 약 65만 명의 가입자 수를 보유하고 있다[2]. 이처럼 이동성과 휴대성, 편의성을 모두 지닌 스마트폰과 태블릿PC의 보급이 원활히 이뤄지고 사용량이 많아지면서 해당 스마트 기기들을 이용하여 중요한 정보를 입력하거나 처리하는 일이 많아지고 있다. 이에 따라 PC환경에서 이루어지던 스파이웨어를 통한 바이러스 감염, 불법 파일 다운로드를 통한 맬웨어 설치, 네트워크 통신을 조작하여 통신 내용을 도청하거나 중간에서 조작하는 공격기법인 중간자공격(MITM, man in the middle attack), 키로깅 공격, 사회공학적 기법을 이용한 공격들이 스마트 기기로 옮겨가고 있다. 이러한 공격기법들은 주로 경제적 손실을 입힐 수 있는 금융과 관련한 애플리케이션들을 목표로 하고 있으며, 공격자들이 가장 많이 목표로 하는 것은 공인인증서의 비밀번호나 계좌 이체 비밀번호와 같은 사용자의 중요 비밀번호이다. 국내의 2014년 1/4분기의 모바일뱅킹 이용건수 및 금액은 2,760만 건, 1조 6,634억 원으로 2013년 1/4분기에 비해 이용건수는 약 9천여 건, 이용금액은 약 4천억 원이 증가한 것으로[1], 지속적으로 증가추세에 있을 정도로 사용량이 많기 때문에 사용자들의 깊은 주의가 필요한 실정이다. 그러나 여전히 사용자들은 여러 공격들의 위험성에 대한 인식이 낮으며, 그 중 강력한 공격방법 중 하나인 어깨너머공격은 그 위험성을 나타내기 어려운 한계가 있다. 공격 성공 가능성을 적용하여 어깨너머공격을 정량적으로 나타내려 해도 기존 공통평가방법론의 공격 성공 가능성의 요소들을 기준으로는 어깨너머공격에 공격 성공 가능성 등급에 대한 판단이나 세부적인 측정이 부적절하다. 이는 어깨너머공격의 특성을 반영한 공격 요소들이 포함되어 있지 않기 때문이다. 이러한 문제점에도 불구하고, 패스워드 입력 스킴에 대한 공격들 중 어깨너머공격의 내성을 판단할 수 있는 기준은 존재하지 않는다.

이에 본 연구에서는 기존의 패스워드 입력 스킴들에 대한 공격 성공 가능성의 공격 요소들에 어깨너머공격의 공격 성공 가능성을 판단 할 수 있는 공격 요소들을 추가하여 공격 성공 가능성이 어깨너머공격의 내성까지 판단 할 수 있도록 알맞은 공격 요소가 추가된 공격 성공 가능성을 제안한다. 또한, 제시한 공격 성공 가능성을 적용한 사례로써 시중에서 제공하고 있는 모바일뱅킹 애플리케이션의 패스워드 입력 스킴을 분석 대상으로 하여 모바일뱅킹 애플리케이션의 보안 키패드가 어깨너머공격에 안전한지에 대한 안전성 여부를 분석한다.

II. 관련 연구

2.1 어깨너머공격과 패스워드 입력 스킴

어깨너머공격은 어떤 사용자가 사무실이나 사람이 붐비는 쇼핑몰, 공항, 커피숍 등에서 사용하고 있는 특정 기기(스마트폰, 노트북, PDA 등)에 대하여 사용자의 인식(awareness)이 없는 상태에서 로그인이나 민감한 정보를 볼 때 사용자 주변에서 몰래 엿보는 것을 말한다[3]. 이처럼 어깨너머공격은 사용자의 패스워드를 평문 그대로 보는 효과적인 공격 수단으로써 강력한 공격 방법이다. 그렇기 때문에, 이에 대응하기 위하여 기존의 패스워드 입력 방법 보다 어깨너머공격에 안전하도록 패스워드 입력을 스마트폰 뒤쪽에서 수행하도록 하는 입력 스킴을 개발하는 연구나 터치스크린 방식으로 패스워드를 입력할 때, 엿보기와 같은 공격에 의한 정보의 누출을 막기 위해 CoverPad를 이용하는 방법을 설계 및 구현하여 어깨너머공격에 안전한 패스워드 입력 방법을 찾는 연구가 지속적으로 이뤄지고 있다[27][31]. 특히, 정형화하여 표현하기 어려운 어깨너머공격을 CPM-GOMS 모델과 같이 정량적으로 표현 가능한 방법을 이용하여 어깨너머공격을 정형화된 모델링을 한 뒤, 쿼티 키패드의 사용성과 안전성을 검토하고 실험한 연구는 어깨너머공격과 관련하여 정형화된 연구 중 하나이다[26].

더불어, Xiaoyuan Suo 등은 기존의 패스워드 입력 스킴을 통합적으로 분석하여 웹이나 스마트폰의 사용자는 사용자 인증을 위하여 패스워드를 입력하여야 하는데 패스워드는 텍스트 기반과 그림 기반 패스

워드로 나눌 수 있다고 제안하였다[4]. 텍스트 기반 패스워드는 숫자와 문자로 이루어진 alphanumeric 패스워드를 말하며 그림 기반 패스워드는 사용자가 패스워드 등록 절차에 따라 선택하여 등록한 그림들의 집합 중 하나를 선택하거나 지나가는 방식으로 인증하는 인지 기반 그림 패스워드와 사용자가 등록 절차에 따라 만들거나 선택했던 그림을 다시 복사/재생산 하도록 요청하여 사용자가 이를 인증하는 기억 기반 그림 패스워드가 있다. 두 가지 종류의 패스워드 모두 사용자가 기억하기 쉬우면서 동시에 보안성이 높은 패스워드 생성을 목표로 하고 있다.

보안성과 유용성 측면의 패스워드 생성이 중요한 가운데 현재 모바일뱅킹 애플리케이션에서 제공되고 있는 쿼티 키패드를 분석한 기존 연구의 경우, 현재의 쿼티 키패드는 확률적 분석을 통해 랜덤 배열을 도출해 키로깅 공격 등으로 악용할 수 있는 문제점이 노출되어[18], 패스워드 보안성에 위협을 받고 있다. 그에 대한 대안으로 제시된 대부분 연구에서 현재 보안 키패드를 대체하여 그림 기반 패스워드 종류를 사용할 것을 제안하고 있다[24]. 그림 기반 패스워드는 사람의 기억력과 보안성을 초점으로 하여 패스워드의 기억력은 높게 하면서 동시에 보안성도 올라가게 하는 것을 목표로 하는데 세부적으로 기억 기반, 인지 기반, 단서가 주어진 기억 기반과 같이 3가지의 그림 기반 패스워드로 나눌 수 있다. 이러한 그림 기반 패스워드는 사용자 유용성과 보안성을 모두 만족하면서 여러 패스워드 공격에 대해 안전하게 설계하려고 한다[25]. 하지만 그림 기반 패스워드를 사용하더라도 각각의 그림 기반 패스워드들의 특성에 따라 어깨너머공격에 안전하거나 안전하지 않은 패스워드도 존재한다.

우선적으로, 인지 기반 그림 패스워드 종류 중 하나를 제안한 Sobrade, Birget 그리고 Man은 인지 기반 그림 패스워드가 기존의 텍스트 기반 패스워드보다 공격자가 인지하기 힘들기 때문에 어깨너머공격에 안전하다고 주장하였다[5][6]. Real User Corporation에서도 사용자가 미리 4개의 얼굴 그림을 선택하여 등록한 후 사용자 인증 시 9개의 얼

Table 1. Password entry scheme and possible attacks[11]

Password input scheme		Input method	User usability	Possible attacks
Text-based password	Alphanumeric password	Input text and number using keyboard	Problem that making a password easy to remember reduces security	Brute force attack, Dictionary attack, Guessing, Malicious program, Shoulder surfing attack
Picture-based password	Graphical password	Click a specific position of the picture registered in advance or enter a specific code passing a few pictures	Problem that it is difficult to remember when there are many other pictures presented together	Brute force attack, Guessing, Malicious program
	Passface	Register 4 pictures of face and select in authentication	Problem that pictures like face with characteristics are easy to remember, but they are predicable	Brute force attack, Dictionary attack, Guessing, Shoulder surfing attack
	DAS (Draw-A-Secret)	Draw and register simple pictures on a 2D grid, and draw them again in order in authentication	Problem that it is difficult for the user to remember the order of drawing	Guessing, Dictionary attack, Shoulder surfing attack
	Passdoodle	Draw a picture randomly using a stylus on the touch screen or enter a text	Easy or difficult to remember depending on what pictures the user draw	Guessing, Dictionary attack, Shoulder surfing attack
	Passlogix	Touch specific parts of a picture in the assigned order for authentication	Problem that it is difficult to remember perfectly	Brute force attack, Guessing, Shoulder surfing attack

굴 그림 중 자신이 미리 선택한 4개의 그림을 선택하는 단계를 거치는 Passface 패스워드가 기존의 텍스트 기반 패스워드 보다 어깨너머공격에 안전하다고 제안하였다[7]. 하지만 위와 같은 그림 기반 패스워드들은 이미지에 부여되는 텍스트 스트링 값을 기억해야하는 단점이나 미리 등록한 4개의 얼굴 그림을 기억하고 있다는 가정을 하는 등 사용자가 기억하기 쉬워야 하는 패스워드 특징에 맞지 않은 문제점이 있다. 두 번째로, 기억 기반 그림 패스워드에서는 Jermyn 등이 간단한 그림을 2D grid에 그린 뒤 순서대로 저장한 후 인증 시 똑같은 순서로 그리면 인증에 성공하는 DAS(Draw-A-Secret)방법을 제안하였고[8], Goldberg 등은 사용자가 터치 스크린에 랜덤하게 그림을 그려 만들거나 텍스트를 써내는 Passdoodle 기법을 제안하였으며[9], Blonder는 사용자가 이미지의 여러 위치를 클릭함으로써 패스워드가 생성되는 스킴을 설계하여 사용자가 인증을 하려면 여러 위치를 클릭하여 등록한 것과 똑같이 클릭을 해서 인증하는 Passlogix 패스워드 기법을 제안하였다[10]. 3가지 패스워드 기법 모두 기존의 텍스트 기반 패스워드 보다 어깨너머공격에 저항성을 갖도록 설계되었지만 스크린이 큰 기기에 DAS를 사용할 경우 기존 어깨너머공격과 마찬가지로 엿보기에 취약할 수 있으며, Passdoodle과 Passlogix의 경우 인지 기반 그림 패스워드 문제점과 같이 기억하기 쉬워야 하는 패스워드 특징에 맞지 않아 사용자가 패스워드를 기억하기 어려운 문제점이 발생 할 수 있다. 또한, 두 종류의 그림 기반 패스워드 모두 어깨너머공격에 안전하게는 설계되었지만 실제 사용자가 그림을 그려 입력한 패스워드가 올바르게 입력되었는지 확인을 위한 사용자 피드백 시 입력한 패스워드를 암호화 이전에 평문으로 확인시켜주는 과정이나 패스워드 입력에 익숙하지 않아 천천히 그림을 그리는 등의 과정은 어깨너머공격에 충분히 노출될 수 있고 기존 텍스트 기반 패스워드 입력 스킴과 유사한 취약점을 가지고 있다. 앞서 설명한 패스워드 입력 스킴들의 특징들을 정리하면, Table 1과 같이 나타낼 수 있다.

이와 같이 패스워드 입력 스킴의 보안성을 높여 안전한 패스워드 설계를 하는 동시에 사용자가 패스워드를 기억하기 쉽게 하려는 연구들은 지속적으로 이뤄져왔지만 안전성과 유용성의 균형을 유지하는 패스워드 입력 스킴의 개발이 미흡하였으며 어깨너머공격에 취약한 문제점을 가지고 있다. 그리고 지금까지의 패스워드 입력 스킴과 관련한 연구들은 어깨너머공격에 대한 구체적 공격 요소의 언급 없이 단순히 패스워드 자체의 안전성에만 의존한 연구들이 대부분이었다. 이런 점들을 보완 및 개선하기 위해서는 기존의 연구들에서 제시되지 않았던 패스워드 입력 스킴에 대한 어깨너머공격 안전성 여부를 판단할 수 있는 판단 기준이 필요하며, 이를 위해 다음에 소개하는 공격 성공 가능성의 방법론을 사용하도록 한다.

2.2 공격 성공 가능성(attack potential)

패스워드 입력 스킴에 대한 어깨너머공격의 안전성 기준을 도출하기 위해 본 절에서는 기존에 스마트카드나 H/W 기기 등 특정 대상에 대해 공격 여부를 정량적으로 알아볼 수 있도록 기준을 제시한 공통평가기준(Common Criteria, CC)의 공격 성공 가능성(attack potential)의 방법론을 따르도록 한다. 공격 성공 가능성이란 공통평가기준의 공통평가방법론(Criteria Evaluation Methodology, CEM)에서 제시하는 전문성, 자원 및 동기에 대한 함수로써 경과 시간, 전문지식, 공격 대상에 관한 지식, 공격에 노출되기 쉬운 기간, 장비들을 각 요소로 가지며 각각의 요소들에 값을 부여하여 공격 대상에 대한 공격 성공 가능성을 Table 3과 같이 정량적으로 나타낸다[23].

계산된 공격 성공 가능성 값의 총합의 범위 Table 2에서 볼 수 있듯 '0~20', '20~30', '30~34', '34이상'으로 나타낼 수 있으며, 값이 높을수록 공격대상에 대해 공격을 성공시키기 위해 오랜 시간을 투자하고 전문 지식 축적 및 공격대상에 대한 높은 지식을 쌓은 것으로 공격 성공 가능성이 높아 공격자가 공격에 성공할 확률이 높은 것을 의미한다. 반대로, 값이 낮을수록 공격자는 공격대상에 대해 공격 성공 가능성이 낮아 공격에 성공할 확률이 낮은 것을 의미한다.

하지만, 공통평가방법론에서 제시된 공격 성공 가능성은 패스워드 입력 스킴에 대한 공격 방법 중 하

Table 2. Vulnerability level of attack potential[23]

Range of value	Attack potential
0~20	Low
20~30	Medium
30~34	High
Over 34	Very High

Table 3. Attack potential of Common Evaluation Methodology(CEM)[23]

Attack Potential			
Elements	Description	Standard	Value
Elapsed time	The sum of time taken for an attacker to detect and develop a weak point that may exist in a target of attack and make an effort required for the attack of the target	Within 1 day	0
		Within 1 week	1
		Within 2 weeks	2
		Within 1 month	4
		Within 2 months	7
		Within 3 months	10
		Within 4 months	13
		Within 5 months	15
		Within 6 months	17
		over 6 months	19
Expertise	General level knowledge about the type of product or attack method	Layman	0
		Proficient	3
		Expert	6
		Multiple expert	8
Knowledge about target of attack	Detailed specialized knowledge related to the target of attack	Public information	0
		Restricted information	3
		Sensitive information	7
		Critical information	11
Period of easy exposure to attack	Period(chance) related to elapsed time, when an attacker can approach the target of attack	Unnecessary/Unlimited access	0
		Easy access	1
		Moderate access	4
		Difficult access	10
Equipment	An attacker can use equipment to detect or abuse vulnerability of the target of attack, which is related to specialized knowledge, so the attacker with high specialized knowledge can use equipment with attack potential	Standard equipment	0
		Specialized equipment	4
		Customized equipment	7
		Complex customized equipment	9

나인 어깨너머공격을 정량화하고 안전성 여부를 판단하기에는 필요한 공격 요소들을 포함 및 만족하지 못하는 한계가 있어 어깨너머공격과 알맞지 않다. 그렇기 때문에, 기존의 공격 성공 가능성으로 어떠한 패스워드 입력 스킴의 어깨너머공격 안전성 여부를 판단하기에는 어려운 문제점을 가지고 있으며, 이를 해결하기 위해서는 어깨너머공격의 공격 성공 가능성을 계산하기 위한 알맞은 기준이 필요하다.

III. 어깨너머공격 모델링

3.1 정형화된 공격 모델링의 필요성

패스워드에 대한 공격 기법들은 다양하게 제시되어 왔다. Table 1은 앞서 언급한 그림 기반 패스워드와 텍스트 기반 패스워드들에 가능한 공격방법들과 사용자 유용성에 대해 나타낸 것이다. 패스워드를 알아내기 위해 악성 프로그램을 설치하도록 유도하여 사용자가 입력하는 패스워드가 서버로 전송될 때의 좌표 정보를 얻어내는 키로깅 공격이나 가능한 패스워드의 조합을 모두 시도하여 사용자 패스워드를 알아내는 전수 조사 공격, 사용자들의 키가 될 가능성이 있는 값들을 하나의 거대한 사전으로 만들어 데이터를 실제 적용하였을 경우 상당히 높은 확률로 키를 알아낼 수 있는 사전 공격 등 여러 가지 패스워드 관련 공격방법들은 지금까지 끊임없이 개발되어 악용되고 있다. 그 중 어깨너머공격은 Table 1에서 제시된 내용과 같이 모든 패스워드 입력 스킴들에 대해 공격이 가능하다[11]. 그 이유는 어깨너머공격은 사용자의 정보를 눈으로 직접 엿봄으로써 해당 정보를 그대로 획득할 수 있기 때문이다.

하지만, 어깨너머공격은 사람의 지각과 인지, 시야각, 기억력 등 인간공학 측면의 공격이기 때문에 앞서 언급한 다른 공격방법들과 달리 정량적으로 표현하거나 수치화하는데 어려움이 있다. 그러나 어깨너머공격에 대한 공격 조건들의 위협요소와 공격환경

에 대한 정형화된 모델링을 통해 정량적인 표현이 가능하게 되면, 어떤 패스워드 입력 스킴에 대한 어깨너머공격에 대해 공격 성공 가능성 값을 매겨 이를 수치화 할 수 있으며, 해당 수치를 통해 패스워드 입력 스킴의 어깨너머공격에 대한 안전성 여부를 가늠할 수 있게 된다. 이는 스마트카드, ATM기기, POI, H/W 디바이스와 같은 특정 대상에 공격 성공 가능성을 적용하여 분석한 사례에서 볼 수 있듯이, 공격 대상에 대해 공격 성공 가능성 등급을 점수로 나타내어 공격 성공 가능성 여부를 판단할 수 있게 되는 것이다[28][29][30]. 하지만, 위 사례들은 앞서 말한 것과 같이 어깨너머공격에서의 공격 요소들은 기존의 공격 성공 가능성의 공격 요소들로는 나타내기 어려운 한계점이 있기 때문에 다음과 같이 요구사항의 도출이 필요하다.

3.2 정형화된 공격 모델링을 위한 요구사항 도출 및 분석

본 절에서는 패스워드 입력 스킴에 대해 어깨너머공격의 공격 성공 가능성을 나타내기 위한 기준 제시를 위해 다음과 같은 공격 요소들을 나열하고 기준값을 제시한다. 각 요소들에서 제시하는 각각의 기준값들은 공통평가방법론(CEM) 문서에 서술되어 있는 것처럼 기술 유형과 특정 환경에 따라 조정될 수 있는 특징을 반영하여 산정하였다[23]. 각 요소들의 공격 성공 가능성은 공통평가방법론에서처럼 4가지의 값(1, 4, 7, 10)으로 분류하였으며, 각각 3점의 점수 차이는 아래의 공격 요소들에서 서술하는 특징에 따른 차등 값으로 각 요소별로 어깨너머공격에 영향을 미치는데 변별력을 주는데 목적이 있다. 이는 패스워드 입력 스킴에 대한 어깨너머공격의 내성을 판단하는 평가자가 처한 환경과 악용 가능한 상태 등에 따라 다르게 산정될 수도 있는 공격 성공 가능성의 특징을 이용한 결과이다.

3.2.1 지각과 인지

일반적으로 사람은 문자(글자, 숫자)에 대하여 지각과 인지하는 과정을 거치게 된다. 이러한 과정은 어깨너머로 사용자의 중요정보를 엿보는데 있어 필수적이고 중요한 요소로써 공격자는 빠르고 정확하게 사용자가 문자를 입력하는 동작을 지각하고 인지할 수 있는 능력이 필요하다. 지각과 인지과정은 몇 가지 특징들이 존재하는데, 첫째, 어느 정도의 시간이 주어졌을 때 얼마만큼의 문자를 인지할 수 있는 것이다. 영어 사용자의 경우에는 보통 1분에 360개의 단어 즉, 초당 6단어의 속도로 문장을 읽고 인지할 수 있으며, 약 50밀리 초의 시간이 소요된다[19]. 둘째, 지각과 인지를 위해 필요한 감각기관과 이를 기억하도록 도와주는 기억 능력이다. 지각과 인지과정을 통해 얻은 문자에 대하여 짧은 시간동안 기억하고 있어야 하며, 이를 단기기억이라고 일컫는데 단기기억이란 자신이 경험한 것을 수초 동안 의식 속에 유지하는 기억을 말한다. Miller는 인간이 기억할 수 있는 용량이 7±2개의 항목이라고 주장하였으며[14], 이후 연구에서는 사람은 덩어리(chunk) 형태로 기억을 하는데 예를 들어, 숫자는 약 7개, 문자는 약 6개, 단어는 약 5개 정도를 하나의 덩어리로 기억을 한 뒤, 이를 세부적으로 나누면서 필요한 것들을 즉각적으로 기억한다고 주장하였다[15]. 이처럼 지각한 정보의 저장을 수행하는 단기기억은 어깨너머공격의 성공 여부의 중요한 부분이라고 할 수 있기 때문에 공격자의 단기기억 능력은 충분히 고려되어야 한다. 마지막으로, 앞서 설명한 단기기억에 저장된 항목들은 짧은 시간 지속되거나 단순히 시간경과에 의해 장기기억으로 옮겨지지 못하고 빠른 시간 내에 망각될 수 있다. 이 때, 맨 먼저 제시된 항목들의 회상률이 높은 초두효과(primary effect)와 마지막에 제시된 항목들의 회상률이 높은 최신효과(recency effect)가 나타날 수 있으며, 이는 공격자가 어깨너머로 엿본 정보를 얼마만큼 효율적으로 회상해내는지에 대한 중요한 요소로 작용할 수 있다[12].

이렇듯 사용자가 보안 키패드를 통해 비밀번호를 입력할 때, 어깨너머공격자는 오직 자신의 신체기관을 통한 지각과 인지 과정을 거쳐 사용자의 비밀번호를 획득할 수 있다. 그렇기 때문에, 공격자가 지각과 인지를 하는데 걸리는 시간은 사용자가 첫 번째 비밀번호를 입력하고 마지막 비밀번호를 입력할 때까지 걸리는 시간보다 적어야 성공적인 어깨너머공격을 할 수 있다. 기존 GOMS 기반 모델은 사용자 인터페이스 모델링을 위해 사용되었으며, 지각, 인지, 동작 조작들을 가정하여 주요 경로를 통해 실행 시간을 예측한다. 이를 응용하여 어깨너머공격에 적용한 STM-GOMS 연구에서 알 수 있듯이, 사용자가 보안 키패드를 이용해 눈과 손가락의 이동과 같은 대기시간을 포함해 비밀번호를 입력하는 전체 실행 시간은 약 5.8초(5,840밀리초)이며, 입력에 걸리는 총

Table 4. Attack potential about perception and recognition

Perception and recognition time	Value
Over 5.8 seconds	1
4.8~5.8 seconds	4
3.8~4.8 seconds	7
2.8~3.8 seconds	10

시간은 약 5.3초(5,280밀리초)이다. 이에 대해 공격자는 사용자가 누르는 키를 보는 눈의 움직임을 포함한 지각과 인지에 걸리는 시간은 180밀리초가 소요되며, 전체 실행 시간 동안의 공격자가 사용자의 입력을 기다리는 총 대기시간은 약2.5초(2,510밀리초), 공격자의 실제 공격 시간은 약2.8초(2,820밀리초)가 된다[19].

이처럼 공격자의 실제 공격 시간이 사용자 비밀번호 입력의 총 시간 보다 적을 경우, 어깨너머공격은 성공적으로 이뤄질 수 있음을 의미하며 공격자의 실제 공격 시간에 따라 Table 4와 같이 공격 성공 가능성을 나타낼 수 있다.

3.2.2 스크린 각도

사람들은 일반적으로 스마트폰을 볼 때, 빛에 반사되거나 흐릿하게 보이지 않는 각도에서 스마트폰의 스크린을 응시한다. 스크린의 내용이 가장 잘 보이는 각도는 스크린이 수평으로 위치하여 사용자의 시선과 90도를 이루었을 때이며, 그 때에 Fig. 1과 같이 사용자가 위치하여 신체를 통해 가려진 부분인 315도~45도를 제외한 총 270도의 범위가 어깨너머공격을 통해 스크린의 정보를 엿볼 수 있는 각도이다

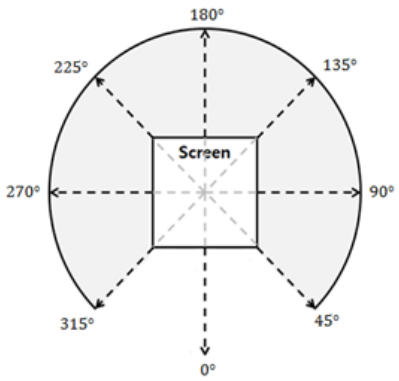

Fig. 1. Horizontal angle of screen[13]

[13]. 총 270도의 각도를 공격자가 가장 잘 엿볼 수 있는 각도로 나눌 수 있는데, 사용자를 중심으로 주변을 360도를 기준으로 45도씩 분류하고 180도를 기준으로 좌우 대칭되는 각도를 동일하게 평가한다. 사용자가 스크린을 보는 수평각 0도~45도(315도~360도) 사이에서는 스크린이 사용자에 가려져 공격자가 스크린을 볼 수 없으므로 공격 성공 가능성이 없다고 판단한다. 45도~90도(270도~315도) 사이에서는 공격자가 비스듬하지만 스크린을 사용자와 거의 비슷한 각도에서 볼 수 있으므로 입력되는 문자 또는 숫자를 정방향으로 볼 수 있다. 따라서 이때의 공격 성공 가능성이 가장 높다고 볼 수 있으며, 90도~135도(225도~270도) 사이에서는 공격자가 스크린에 입력되는 문자 또는 숫자를 90도로 기울어진 형태이거나 이보다 더 반대로 기울어진 형태로 인식하게 되므로 문자 또는 숫자를 인식하는데 45도에서 보는 것보다 어려움이 존재한다. 따라서 해당 각도 사이에서의 공격 성공 가능성은 보통으로 본다. 마지막으로 135도~180도(180도~225도) 사이에서는 공격자가 스크린을 볼 때 모든 내용이 거꾸로 뒤집어져 보이므로 입력되는 내용을 짧은 시간 내에 판단하기에 어려움이 존재하므로 공격 성공 가능성이 가장 낮다고 볼 수 있으며, Table 5와 같이 스크린 각도에 따른 공격 성공 가능성을 나타낼 수 있다.

Table 5. Attack potential about angle of screen

Screen Angle	Value
0~45(315~360) degrees	1
135~180(180~225) degrees	4
90~135(225~270) degrees	7
45~90(270~315) degrees	10

3.2.3 공간 및 거리와 가독성

공격자는 공격 대상에 대하여 적정 거리를 유지함과 동시에 어깨너머공격이 가능한 최적의 거리를 유지하도록 해야 한다. 이는 개인 공간과 문자를 알아볼 수 있는 가독성으로 고려될 수 있다.

3.2.3.1 개인공간

개인 공간이란 사람이 무의식중에 자기의 영역이라고 생각하는 공간을 일컫는다. 대부분의 사람들은 자기만의 개인 공간에 가치를 부여하고 누군가 접근

하였을 때 심리적으로 불편하거나 분노, 경계 등을 하게 된다.

이러한 개인 공간은 밀접한 거리, 개인적 거리, 사회적 거리, 공적인 거리로 아래 Fig. 2와 같이 나타낼 수 있다[16]. 밀접한 거리는 연인 및 보호자와 어린이 사이의 거리, 개인적 거리는 친한 친구, 사회적 거리는 사무적인 인간관계, 공적인 거리는 연설, 강연 등이 이뤄질 때의 거리를 나타낸다. 어깨너머공격에서 가장 중요한 사용자와 공격자의 위치 및 거리는 사용자가 인지하는 개인 공간의 범위 안에서 결정된다. 그렇기 때문에, 사용자와 공격자가 가장 가까운 거리를 갖게 되는 밀접한 거리일 때, 문자 가독성이 최적이 되며 공격 성공 가능성이 가장 높게 형성될 수 있다. 이와 반대로, 가장 먼 거리인 공적인 거리에 위치할 경우에는 공격 성공 가능성이 가장 낮게 형성될 수 있으며 이에 따라 Table 6과 같이 공격 성공 가능성을 나타낼 수 있다.

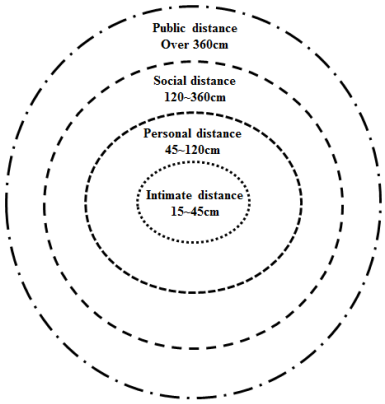

Fig. 2. Personal Space[16]

Table 6. Attack potential about personal space

Personal Space	Value
Public distance	1
Social distance	4
Personal distance	7
Intimate distance	10

3.2.3.2 문자 가독성

인간은 특정한 사물이나 대상에 짧은 시간 동안 시선을 고정하여 응시를 하며 이를 통해 형태를 알아보거나 인식한다. 글자나 문자를 인식하는 정도를 나타내는 척도를 가독성이라 하며, 눈의 응시를 통하여 문자나 숫자를 읽을 수 있는 가독성을 갖게 된다. 모니터의 경우에는 일반적인 독서의 거리(30~35cm)보다 더 멀어지기 때문에 글자의 크기가 더욱 커져야 하는데, 이는 최소한 10pt 이상으로 11pt~14pt 정도는 되어야 사용자가 읽기 편한 크기가 된다[17]. 같은 글꼴이라고 하더라도 크기에 따라 가독성과 선호도가 다를 수 있으며, 시력과 같은 신체적 조건도 영향을 미칠 수 있기 때문에 문자의 가독성은 여러 요인들을 복합적으로 고려해야 한다.

가독성에 영향을 미칠 수 있는 다른 요인들로는 글자체, 글자 크기, 배경색, 글자색, 제시방식, 조도, 시야거리, 연령, 글자 간격 등 여러 가지 요인들이 존재한다[20]. 이 중 시야거리에 따른 문자의 최소 크기는 Table 7과 같으며, 각각의 거리에 맞는 문자의 최소 크기를 만족할 때 가독 불편도가 최소가 된다. 시야 거리에 따른 글자 크기와 관련하여 시야 거리가 4배 정도의 차이가 있을 때, 최소 글자 크기가 약 15pt 정도로 가장 큰 차이를 보인 가독성 비교연구에서 나타나듯 시야 거리는 가독성에 가장 큰 영향을 미칠 수 있는 중요한 요인 중 하나이며[21], 시야 거리는 앞서 제시한 개인 공간의 범위 안에서 결정될 수 있다. 이 외에도 숫자가 글자보다 가독성이 조금 더 좋은 것으로 나타났으며, 조도에서도 밝은 경우가 어두운 경우보다 최소 가독 글자크기가 조금 더 작은 것으로 나타났다[22]. 또한, 연령이 낮을수록 글자와 숫자에 대한 가독성이 더욱 좋게 나타났는데, 시야 거리 50cm와 200cm일 때, 적정 가독 글자가 20대는 8~22pt였으며, 60대는 14~32pt로 나타났다[20]. 글꼴의 크기는 화면 크기와도 연관이 있는데 현재 모바일뱅킹 애플리케이션에서 기본적으로 제공하고 있는 쿼티 키패드의 폰트 크기가 약 9~10pt라고 할 때, 화면 크기가 큰 갤럭시 노트3(5.68인치), 갤럭시 S5(5.1인치), 갤럭시 S4(4.99인치), 아이폰 5S(4인치)의 순서대로 폰트 크기가 똑같더라도 화면 크기에 비례하여 글자가 더 크게 보이는 효과가 발생하게 된다. 이는 화면크기가 작은 스마트폰 보다 상대적으로 폰트가 크게 보여 가

Table 7. Minimum character size according to sight distance

Sight distance	Minimum size of character
20cm	1.4mm
30cm	2.1mm
40cm	2.8mm

독성이 좋은 것을 의미한다. 이는 가독성에 큰 영향을 미치는 글꼴 크기가 사용자가 사용하는 스마트폰의 기기에 따라 달라질 수 있는 것을 의미함과 동시에 상대적으로 화면 크기가 더욱 큰 스마트폰을 사용할수록 가독성은 좋지만 어깨너머공격에는 취약하다고 할 수 있다. 결과적으로 사용자가 사용하는 스마트폰의 화면 크기에 따라 Table 8과 같이 가독성에 대한 공격 성공 가능성을 나타낼 수 있다.

Table 8. Attack potential about legibility

Legibility		Value
Screen Size	4~4.5 inches	1
	4.5~5 inches	4
	5~5.5 inches	7
	5.5~6 inches	10

3.3 제안하는 공격 성공 가능성(attack potential)

제안하는 방식은 기존의 측정방식이 어깨너머공격을 고려하지 않았기 때문에, 기존의 공격 성공 가능성 측정 매트릭스에 어깨너머공격 점수를 추가한 것이다. 그렇기 때문에, 공격 성공 가능성의 등급분류는 최대한 기존 공통평가방법론의 체계를 따랐으며, 본 논문에 다음과 같이 기술하였다. 제안하는 공격 성공 가능성은 Table 9와 같이 나타낼 수 있다.

이는 기존의 공격 요소들에 더해 어깨너머공격의 공격 성공 가능성 내성을 판단할 수 있는 공격 요소 조건들이 추가된 것이다. 그럼으로써, 패스워드 입력 스킴에 대해 어깨너머공격의 공격 성공 가능성 내성을 판단할 수 없었던 기존의 공격 성공 가능성을 개선 및 보완할 수 있다. 또한, 기존의 여러 패스워드 입력 스킴들의 공격들에 대한 공격 성공 가능성뿐만 아니라 어깨너머공격이 추가된 형태로 어깨너머공격에 대한 공격 성공 가능성 등급까지 알 수 있다.

이 요소들 값의 합을 통해 기존의 어깨너머공격에 대해 정량적으로 나타낼 수 없었던 한계점을 개선하여 어깨너머공격에 알맞은 공격 성공 가능성을 정량적으로 표현할 수 있으며, Table 10에서 볼 수 있듯이 낮음(0~30), 중간(30~45), 높음(45~60), 높음 이상(60 이상)으로 나타낼 수 있다. 이를 이용하여 어깨너머공격의 공격 성공 가능성이 0~30점으로 '낮음'을 갖는 범위에 해당할 때, 어깨너머공격이 성공할 확률이 가장 낮은 것을 나타내고 반대로, 공격 성공 가능성이 60점 이상으로 '높음 이상'을 갖는 범위에 해당할 때는 어깨너머공격이 성공할 확률이 가장 높은 것으로 판단할 수 있다. 이는 공격 요소에 따른 어깨너머공격의 취약성에 대한 상대적인 차이를 반영하는 것으로 특정 환경이나 공격에 악용 가능한

Table 9. Proposed attack potential

Attack Potential		
Elements		Value
Elapsed time	Within 1 day	0
	Within 1 week	1
	Within 2 weeks	2
	Within 1 month	4
	Within 2 month	7
	Within 3 month	10
	Within 4 month	13
	Within 5 month	15
	Within 6 month	17
	over 6 months	19
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple expert	8
Knowledge about target of attack	Public information	0
	Restricted information	3
	Sensitive information	7
	Critical information	11
Period of easy exposure to attack	Unnecessary /Unlimited access	0
	Easy access	1
	Moderate access	4
	Difficult access	10
Equipment	Standard equipment	0
	Specialized equipment	4
	Customized equipment	7
	Complex customized equipment	9
Perception and recognition	Over 5.8 seconds	1
	4.8~5.8 seconds	4
	3.8~4.8 seconds	7
	2.8~3.8 seconds	10
Screen angle	0~45(315~360)	1
	135~180(180~225)	4
	90~135(225~270)	7
	45~90(270~315)	10
Personal space	Public distance	1
	Social distance	4
	Personal distance	7
	Intimate distance	10
Legibility	4~4.5 inches	1
	4.5~5 inches	4
	5~5.5 inches	7
	5.5~6 inches	10

Table 10. Vulnerability level of the proposed attack potential

Range of value	Attack potential
0~30	Low
30~45	Medium
45~60	High
Over 60	Very High

상태에 따라 평가자에 의해 변경될 수 있다.

결론적으로, 제안하는 공격 성공 가능성을 통해 기존의 일반적인 패스워드 공격 성공 가능성 등급뿐만 아니라 어깨너머공격이 추가된 공격 성공 가능성 등급을 판단할 수 있게 된다. 이는 시중의 모바일뱅킹 애플리케이션들의 쿼티 키패드에 제안하는 공격 성공 가능성을 적용할 경우, 어깨너머공격에 대한 공격 성공 가능성을 정량적으로 알 수 있으며 그에 맞는 공격 성공 가능성 등급을 알 수 있다. 해당 등급을 통해 어느 금융회사들의 모바일뱅킹 애플리케이션이 어깨너머공격에 상대적으로 더 취약한지 파악할 수 있게 된다. 이를 위해서는 다음 절에서 다루는 사용자 피드백과 피드백 제공시간과 같이 어깨너머공격에 취약한 부분을 보완 및 개선하거나 사용자 편의성과 보안성이 우수한 그림 기반 패스워드를 개발하여 사용자들이 어깨너머공격을 포함한 여러 유형의 패스워드 공격에도 안전하도록 해야 한다. 또한, 모바일뱅킹 애플리케이션과 같이 금융과 관련된 업무를 수행할 수 있는 애플리케이션의 보안성은 다른 애플리케이션들에 비해 더 높아야하며, 그에 더하여 사용자들의 보안 의식도 높아야 한다. 이를 위해, 어깨너머공격과 같이 정량적으로 표현하지 못했던 공격 기법들에 대해 정확한 수치를 나타내어 보여주고 이를 통해 사용자들은 어떠한 보안 키패드를 제공하는 금융회사의 모바일뱅킹 애플리케이션이 어깨너머공격에 안전한지에 대해 파악할 수 있게 되며, 어깨너머공격에 대한 보안 의식이 인식 및 제고될 수 있다.

IV. 보안 키패드별 안전성 분석

4.1 보안 키패드 취약점 분석

본 절에서는 현재 모바일뱅킹 애플리케이션들이 제공하고 있는 보안 키패드인 쿼티 키패드와 숫자 키패드의 안전성을 분석하고 어깨너머공격에 대한 취약점을 도출 및 분석한다. 현재 대다수의 주요 금융회사들(은행, 증권, 보험)은 모바일뱅킹 애플리케이션을 사용하여 금융 업무를 수행할 때, 계좌 및 공인인증서의 비밀번호 입력이나 보안카드 번호 입력과 같이 중요 정보를 보안 키패드인 쿼티 키패드나 랜덤 숫자 키패드를 사용하여 입력하도록 하고 있다. 하지만 쿼티 키패드와 숫자 키패드 모두 랜덤한 키패드 배열을 통해 보안성을 달성하려고 하지만 확률 값이 작은 랜덤 배열과 사용자가 입력한 패스워드를 확인시켜주는 사용자 피드백은 어깨너머공격에 취약한 보안 문제점을 가지고 있다.

4.1.1 랜덤 배열

4.1.1.1 쿼티 키패드의 랜덤 배열

공인인증서 패스워드 입력 시 모바일뱅킹 애플리케이션은 보안 키패드인 쿼티 키패드를 사용하며, 쿼티 키패드의 경우 각 행마다 1~2칸의 공백을 랜덤하게 발생시켜 안전한 입력을 유도하고 있지만 공백이 발생할 수 있는 위치에 대한 모든 경우의 수를 계산할 수 있어 공백의 랜덤성이 확률적으로 분석이 가능하다.

Fig. 3과 같이 각 행마다 총11칸으로 이루어진 키패드 배열이 발생할 수 있는데, 첫 번째 행과 두 번째 행, 네 번째 행은 1,2,3,4,5,6,7,8,9,10과 q,w,e,r,t,y,u,i,o,p 그리고 z,x,c,v,b,n,m등으로 각 10개의 키와 1칸의 공백으로 구성된다. 세 번째 행은 a,s,d,f,g,h,j,k,l로 9개의 키와 2칸의 공백으

Fig. 3. Qwerty keypads provided by mobile banking applications of the financial institutions

Table 11. The values of probability for the key layout of a qwerty keypad[18]

	①		②		③		④		⑤		⑥		⑦		⑧		⑨		⑩		⑪	
First	1	100	1	10	2	20	3	30	4	40	5	50	6	60	7	70	8	80	9	90	0	100
			2	90	3	80	4	70	5	60	6	50	7	40	8	30	9	30	0	10		
Second	q	100	q	10	w	20	e	30	r	40	t	50	y	60	u	70	i	80	0	90	p	100
			w	90	c	80	r	70	t	60	y	50	u	40	i	30	o	20	p	10		
Third	a	100	a	20	a	2.2	s	6.6	d	13.3	f	22.2	j	13.3	k	6.6	l	2.2	l	20	l	100
			s	80	s	35.6	d	46.7	f	22.2	g	55.6	h	53.4	j	46.7	k	35.6	k	80		
					d	62.2	f	46.7	g	33.3	h	22.2	g	33.3	h	46.7	j	62.2				
Fourth	z	100	z	14.3	x	28.6	c	42.9	b	42.9	n	28.6	m	14.3	m	100						
			x	85.7	c	71.4	v	57.1	v	57.1	b	71.4	n	85.7								

로 이루어진다. 공격자는 이를 확률적 분석을 통해 Table 11과 같이 각 키가 위치할 수 있는 키 분포 확률 값을 구할 수 있으며[18], 해당 확률 값을 이용하여 관찰한 입력위치의 키가 어떤 키인지 확률적으로 유추하거나 어깨너머공격을 수행하기 위해 쿼티 키패드 배열을 학습할 수 있다.

4.1.1.2 숫자 키패드의 랜덤 배열

계좌비밀번호나 보안 카드 번호를 입력할 때에 주로 사용하는 숫자 키패드는 10개의 숫자 키 배열들을 랜덤하게 구성시켜 키로깅과 같은 공격에 안전하게 설계하였다. 또한 입력되는 숫자들을 "*"와 같이 암호화시켜 중간에서 공격자에 의해 가로채더라도 암호화되어 공격자가 알아보지 못하도록 하고 있다. 앞서 분석한 쿼티 키패드와는 다르게 숫자 키패드는 랜덤성이 높아 10개의 자리가 지속적으로 바뀌어 유추가 어렵다. 이처럼 숫자 키패드는 보안성이 높게 설계가 되었으나 10개의 숫자 키가 완전히 랜덤하게 뒤섞이기 때문에 사용자가 눌러야 하는 숫자를 매번 찾아야 하며, 시간이 오래 걸리는 불편함을 초래한다. 이러한 점은 사용자의 편의성을 떨어뜨리며, 키로깅과 중간자공격과 같은 공격모델에는 안전성을 갖지만, 엿보기에 약한 4자리의 짧은 길이의 비밀번호를 사용하는 등 어깨너머공격과 같이 사용자의 직접적인 입력 상황을 관찰하여 비밀번호를 획득하는 공격에는 무용지물이 되어 안전성을 갖지 못한다.

4.1.2 사용자 피드백 및 피드백 제공시간

모바일뱅킹 애플리케이션에서 보안 키패드들은 사용자가 입력한 비밀번호를 확인시켜주는 피드백 과정이 있는데 이 과정에서도 마찬가지로 어깨너머공격에 대한 보안 취약점이 존재한다. 쿼티 키패드와 숫자 키패드 모두 사용자가 키패드를 터치하여 비밀번호를 입력할 때, 입력된 키가 서버로 전송되는 중간에 공격자에 의해 탈취되지 않도록 암호화를 하는데, 이는 Fig. 4와 같이 사용자 화면에 '*'로 표시되므로 사용자는 자신이 입력한 비밀번호가 올바르게 입력되었는지 확인하기 위하여 '*'로 암호화되기 전에 보여주는 피드백을 통해 입력문자를 확인할 수 있다. 이 때, 제공되는 피드백 시간은 사용자가 패스워드를 입력 및 확인하는데 어려움이 없도록 편의성을 고려해야 하며 동시에, 어깨너머공격과 같은 공격기법에는 안

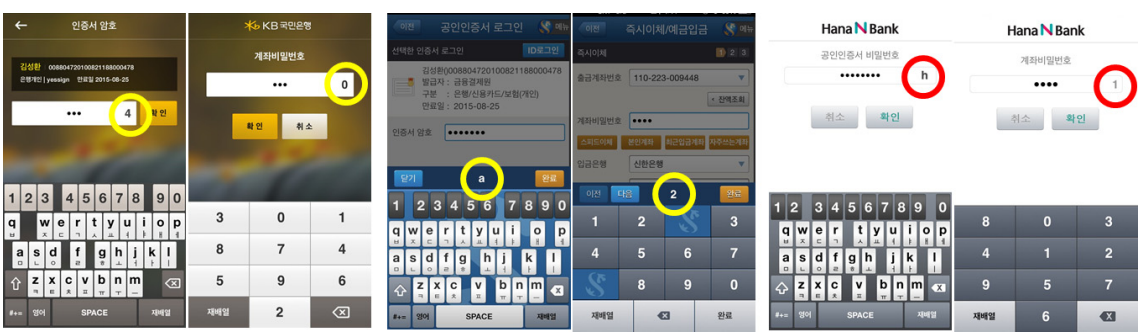

Fig 4. User feedback provided by qwerty keypads of mobile banking applications

Table 12. Time and method of user feedback of the mobile banking applications provided by each financial institution

	Financial Company	Password input keypad	Encryption	Feedback Method	Feedback Time	Shoulder Surfing Attack
Mobile Banking Application	A Bank	qwerty keypad/ number keypad	O	Keep the last letter in plain language	Unlimited	Possible during plain language feedback
	B Bank	qwerty keypad/ number keypad	O	Keep the last letter in plain language	Unlimited	Possible during plain language feedback
	C Bank	qwerty keypad/ number keypad	O	Keep the last letter in plain language	Unlimited	Possible during plain language feedback
	D Bank	qwerty keypad/ number keypad	O	Keep the last letter in plain language	Limited	Possible during plain language feedback
	E Bank	qwerty keypad/ number keypad	O	Keep the last letter in plain language	Limited	Possible during plain language feedback
	F Bank	qwerty keypad/ number keypad	O	None	None	Possible while entering password

전하도록 보안성의 균형을 이루어야 한다.

하지만 몇몇 모바일뱅킹 애플리케이션의 보안 키패드는 사용자 편의성을 위해 입력 값에 대한 피드백을 제공할 때, 사용자가 마지막에 입력한 문자를 시간제한 없이 계속해서 띄워놓고 피드백을 주기 때문에 사용자의 편의성은 증가하지만, 공격자는 사용자가 어떠한 키를 누르는지 보지 않더라도 피드백으로 제공되는 문자만 보게 되면 사용자가 입력한 문자들을 평문 그대로 볼 수 있는 문제점이 생겨 보안성이 낮아지는 결과를 초래할 수 있다.

4.2 모바일뱅킹 보안키패드에 대한 공격 성공 가능성 적용 및 분석

현재의 모바일뱅킹 보안 키패드가 어깨너머공격에 대해 얼마만큼의 공격 성공 가능성을 갖는지 분석하기 위해 다음의 공격 시나리오를 기반으로 앞서 제안한 어깨너머공격의 공격 성공 가능성을 도출하도록 한다. 제시하는 두 가지의 공격 시나리오는 가장 강력하게 어깨너머공격을 수행 및 성공할 수 있는 조건을 가정하여 구성한다.

◇ 공격 시나리오(1)
- 사용자와 공격자는 밀접한 거리에 위치
- 사용자는 갤럭시 노트3 사용
- 공격자는 사용자의 주변 지인으로 가정
- 공격자는 낮은 연령층
- 공격자는 쿼티 키패드 랜덤 배열에 대하여 학습

◇ 공격 시나리오(2)
- 사용자와 공격자는 개인적 거리에 위치
- 사용자는 갤럭시 S5 사용
- 공격자는 사용자의 주변 지인으로 가정
- 공격자는 낮은 연령층
- 공격자는 쿼티 키패드 랜덤 배열에 대하여 학습

지인의 경우, 사용자에게 근접한 위치까지 접근하는 것에 대해 큰 거부감을 느끼지 않게 되어 공격자는 가장 가독성이 좋은 위치 및 거리를 가질 수 있으며, 공격 시나리오(1)의 경우에는 화면크기가 가장 큰 스마트폰인 갤럭시 노트3를 사용하기 때문에 가독성 측면에서도 어깨너머공격에 최상의 조건을 갖추게 된다. 또한 랜덤 배열에 대한 학습을 통해 키패드

Table 13. Attack potential of each mobile banking application for each financial company according to attack scenario(1)

Attack elements / Mobile banking application	Elapsed time	Expertise	Knowledge about target of attack	Period of easy exposure to attack	Equipment	Recognition & perception	Screen angle	Personal space	Legibility	Attack potential
A bank	0	0	0	1	0	10	10	10	10	41
B bank	0	0	0	1	0	10	10	10	10	41
C bank	0	0	0	1	0	10	10	10	10	41
D bank	0	0	0	1	0	7	10	10	10	38
E bank	0	0	0	1	0	7	10	10	10	38
F bank	0	0	0	1	0	4	10	10	10	35

분포 위치에 대해 익숙하며 사용자가 비밀번호 최소 요구사항인 8자리를 사용할 때, 공격자가 인지 및 지각하는데 큰 어려움이 없게 된다. 이를 제안한 공격 성공 가능성으로 값을 적용하면 어깨너머공격에 대해 취약성 여부를 정량적으로 나타낼 수 있으며, 금융회사별 모바일뱅킹 애플리케이션에 대해 공격 성공 가능성 값은 Table 13과 같이 나타낼 수 있다.

이는 공격 시나리오에 따른 가정 사항을 이용해 공격 성공 가능성 값을 매긴 것으로 기존의 공격 성공 가능성 요소들인 경과시간, 전문지식, 공격 대상에 대한 지식, 공격에 노출되기 쉬운 기간, 장비에서는 값의 차이가 없었는데, 이는 녹화기기를 이용한 공격과 같이 어깨너머공격에 큰 영향력을 미칠 수 있는 요소는 고려하지 않았기 때문이다. 그러나 공격자가 어깨너머공격의 성공률을 높이기 위해 공격에 투자한 시간(경과시간)이 많고 각 은행사별 모바일뱅킹 키패드의 특징들을 습득하여 전문지식을 쌓는 등의 활동이 발생한다면 기존의 공격 성공 가능성의 요소들의 점수도 여러 형태로 나타날 수 있기 때문에 기존의 공격 성공 가능성의 요소들도 누락되어서는 안 된다.

제안하는 공격 성공 가능성의 요소들에서는 대부분의 공격 성공 가능성의 점수가 모두 같았지만 지각과 인지 요소의 경우에 점수의 차이가 존재하기 때문에 점수가 다르게 측정되었는데, 이는 A, B, C은행의 모바일뱅킹 애플리케이션 보안 키패드는 사용자 피드백을 시간제한 없이 계속해서 제공해주기 때문에 공격자가 입력 문자를 지각과 인지하는데 별다른 어려움이 없기 때문이다. 이에 반해, 사용자 피드백을 약 2초 정도 제공하는 D은행과 E은행 그리고 사용자 피드백을 전혀 제공하지 않는 F은행의 모바일뱅킹 보안 키패드의 경우에는 계속적으로 피드백을 주는 다른 은행사들 보다 지각과 인지에 따른 어려움이 상대적으로 크다고 할 수 있다. 따라서 사용자가 비

Table 14. Attack potential of each mobile banking application for each financial company according to attack scenario(2)

Attack elements / Mobile banking application	Elapsed time	Expertise	Knowledge about target of attack	Period of easy exposure to attack	Equipment	Recognition & perception	Screen angle	Personal space	Legibility	Attack potential
A bank	0	0	0	1	0	10	10	7	7	35
B bank	0	0	0	1	0	10	10	7	7	35
C bank	0	0	0	1	0	10	10	7	7	35
D bank	0	0	0	1	0	7	10	7	7	32
E bank	0	0	0	1	0	7	10	7	7	32
F bank	0	0	0	1	0	4	10	7	7	29

밀번호를 입력하는 총 시간보다 공격자의 실제 공격 시간이 더 길어져 어깨너머공격에 성공하지 못할 가능성이 높기 때문에 지각과 인지의 점수가 다른 금융회사들 보다 낮게 측정된 것을 알 수 있으며, A~E 은행들의 모바일뱅킹 애플리케이션들 보다 공격 성공 가능성이 낮아 상대적으로 어깨너머공격에 안전하다는 것을 알 수 있다.

공격 시나리오(2)의 경우에는 어깨너머공격에 큰 영향을 미치는 요소인 개인공간과 가독성에 관련한 부분을 공격 시나리오(1) 보다 한 단계씩 낮게 하여 그 차이점을 알 수 있도록 하였다. 그 결과, Table 14에서 볼 수 있듯이, 모든 은행사의 공격 성공 가능성 값이 6점씩 떨어져 F은행의 경우에는 공격 성공 가능성 등급이 한 단계 내려간 것을 확인 할 수 있었다. 이처럼 공격 시나리오(1)과 (2)를 비교하면 어깨너머공격자의 가장 큰 공격 요소인 가독성 부분을 달리 하여도 은행사별 모바일뱅킹 애플리케이션에서 제공하고 있는 사용자 피드백에 의한 인지 및 지각 요소의 차이는 공격 성공 가능성의 등급을 결정하는 중요한 요소라는 것을 알 수 있다.

결론적으로, 모바일뱅킹 애플리케이션들이 어깨너머공격에 상대적으로 낮은 공격 성공 가능성을 가지기 위해서는 무한한 시간동안 제공하고 있는 사용자 피드백을 유한한 시간 동안 제공하거나 다른 방법을 통해 피드백을 제공하여 사용자 유용성을 유지함과 동시에 보안성도 달성할 수 있는 새로운 보안 키패드를 개발할 필요가 있다.

V. 결 론

본 연구에서는 공통평가방법론의 공격 성공 가능성이 패스워드 입력 스킴에 대한 여러 공격들 중 어깨너머공격에 대해 정량적으로 표현하지 못하는 한계점을 개선하기 위하여 어깨너머공격에 알맞은 공격 모델링 조건을 도출하고 이에 대해 공통평가방법론과 같은 방식으로 값을 부여하였다. 그럼으로써, 기존의 공격 성공 가능성이 어깨너머공격을 정량적으로 표현하지 못한 점을 정량화하여 표현할 수 있었다. 또한, 현재 시중에서 제공하고 있는 모바일뱅킹 애플리케이션들에서 사용하고 있는 쿼티 키패드와 숫자 키패드가 어깨너머공격에 안전한지에 대하여 기존 연구와 더불어 취약점을 분석하였으며, 그 결과로 현재의 모바일뱅킹 애플리케이션들에서 제공하고 있는 쿼티 키패드와 숫자 키패드가 적은 랜덤배열과 사용자 피드백을 무한한 시간동안 제공하는 것이 어깨너머공격에 유효하다는 것을 알 수 있었다. 이를 통해 나열한 어깨너머공격의 공격조건들이 구체적으로 어떠한 값과 상황을 가질 때, 어깨너머공격이 가장 성공적으로 이루어질 수 있는지에 대해서도 알 수 있었다. 결론적으로 제안하는 어깨너머공격에 대한 공격 성공 가능성의 기준에서 모바일뱅킹 애플리케이션의 보안 키패드가 공격 성공 가능성 취약성 등급이 '낮음'에 만족하였을 때, 어깨너머공격에 가장 안전하다는 결과를 얻을 수 있었으며 현존하는 상업적 보안 키패드들도 제안하는 공격 성공 가능성의 취약성 등급이 '낮음'에 해당하도록 보안 키패드를 설계 및 구현해야 한다는 점을 알 수 있었다. 향후 연구에서는 모바일뱅킹 애플리케이션의 보안 키패드에 대한 어깨너머공격의 공격 성공 가능성 외에 다른 패스워드 공격기법들에 대해서도 공격 성공 가능성을 연구할 예정이다.

References

[1] Jeonghyuk Kim, Munseon Bae, and Ara Yang, "Usage of domestic Internet banking services in 2014 first quarter," Bank of Korea, May. 2014

[2] Jaesik Mun, "2014 Statistical information of the wireless communication subscriber," Ministry of Science, ICT and Future Planning, June. 2014.

[3] Kevin D. Mitnick and JOHNNY LONG, "No Tech Hacking: A guide to Social Engineering, Dumpster Diving, and Shoulder Surfing," SYNGRESS, pp. 27-60, Nov. 2007.

[4] Xiaoyuan Suo, Ying Zhu, and G. Scott. Owen, "Graphical Passwords: A Survey," IEEE Computer Security Applications Conference, 21st Annual, pp. 463-472, Dec. 2005.

[5] Leonardo Sobrado and Jean-Camille Birget, "Graphical Passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol.4, 2002.

[6] Sunshuang Man, Dawei Hong, and Manton Mathews, "A shoulder surfing resistant graphical password scheme,"

Proceedings of International conference on security and management, Nov. 2003.
〔7〕 Passfaces White Papers, "The Science Behind Passfaces," RealUser(www.realuser.com), June. 2005.
〔8〕 Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, "The Design and Analysis of Graphical Passwords," Proceedings of the 8th USENIX Security Symposium, Aug. 1999.
〔9〕 Joseph Goldberg, Jennifer Hagman, and Vibha Sazawal, "Doodling Our Way to Better Authentication," ACM, Proceedings of Human Factors in Computing Systems(CHI), pp. 868-869 Apr. 2002.
〔10〕 G. E. Blonder, "Graphical Passwords," Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
〔11〕 M. N. Doja and Naveen Kumar, "User Authentication Schemes for Mobile and Handheld Services," INFOCOMP Journal of Computer Science, vol.7, no.4, pp.38-47, 2008.
〔12〕 Jeongmo Lee, Eunjoo Kang, and Minsik Kim et al., "Cognitive Psychology," HAKJISA, Jan. 2009.
〔13〕 "Information Supplement: ATM Security Guidelines," PCI Security Standards Council, Jan. 2013.
〔14〕 George A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," Psychol. Rev., vol. 63, no. 2, Mar. 1956.
〔15〕 Richard M. Shiffrin and Robert M. Nosofsky, "Seven plus or minus two: A commentary on capacity limitations," Psychological Review, pp.357 - 361, Apr. 1994.
〔16〕 "Personal Space," Wikipedia, Aug. 2014.
〔17〕 Choo-Youn Chong, "Korean typography interface evaluation and development of legibility formula in smartpad device," KAIST, 2012.
〔18〕 Yunho Lee, "An Analysis on the Vulnerability of Secure Keypads for Mobile Devices," Journal of Korean Society for Internet Information, vol.14, no.3, pp. 15-21, June. 2013.
〔19〕 Sooyeon Shin and Taekyoung Kwon, "STM-GOMS Model : A Security Model for Authentication Schemes in Mobile Smart Device Environments," KIISC, vol.22, no.6 , pp. 1243-1252, Dec. 2012.
〔20〕 Inseok Lee, Seung Min Mo, Yong Ku Kong, Young Woong Song, and Myung Chul Jung, "Evaluation of Main Factors Affecting on the Legibility of One Syllable Korean Characters and Numbers," Journal of the Ergonomics Society of Korea, vol.28, no.4 pp.1-7, Nov. 2009.
〔21〕 Seung Min Mo, Young Woong Song, Inseok Lee, Myung Chul Jung, and Yonggu Jeong, "Legibility comparison of Korean characters and words," Ergonomics Society of Korea, pp.474-477, May. 2009.
〔22〕 Seung Min Mo, Daemin Kim, Young Woong Song, and Myung Chul Jung, "Evaluations of Factors Affecting Legibility," Journal of the Ergonomics Society of Korea, pp.20-23, Oct. 2008.
〔23〕 "Common Criteria: Evaluation Methodology," Version 3.1, Revision 4, Sep. 2012.
〔24〕 Arash Habibi Lashkari, Samaneh Farmand, Omar Bin Zakaria, and Rosli Saleh, "Shoulder surfing attack in graphical password authentication," International Journal of Computer Science and Information Security, Vol. 6, No.2, 2009.
〔25〕 Robert Biddle, Sonia Chiasson, and P.C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," ACM Computing Surveys, Feb. 2011.
〔26〕 Taekyoung Kwon, Sooyeon Shin, and Sarang Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected," IEEE

Transactions on Systems, Man, And Cybernetics: Systems, June. 2014.
〔27〕 Alexander De Luca, Emanuel von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, and Marcello Paolo Scipioni, and Marc Langheinrich, "Back-of-device authentication on smartphones," ACM Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp.2389-2398, 2013.
〔28〕 "Application of Attack Potential to POIs," Joint Interpretation Library, June. 2011.
〔29〕 "Application of Attack Potential to Hardware Devices with Security Boxes," Joint Interpretation Library, May. 2012.
〔30〕 "Application of Attack Potential to Smartcards," Joint Interpretation Library, Apr. 2006.
〔31〕 Qiang Yan, Jin Han, Yingjiu Li, Jianying Zhou, and Robrt H. Deng, "Designing leakage resilient password entry on touchscreen mobile devices," ACM CCS, May. 2013.

〈저자소개〉

김 성 환 (Sung-hwan Kim) 학생회원
2013년 2월: 고려대학교 경영정보학과 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보증, 금융보안, 보안공학

박 민 수 (Min-su Park) 학생회원
2010년 2월: 신라대학교 컴퓨터네트워크학과 졸업
2013년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사과정
〈관심분야〉 정보보증, 정보보호제품 보안성 평가, 디지털 포렌식, Usable Security

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security