STUDY ON ANALYSIS OF COMMERCIAL MOBILE KEYPAD SCHEMES AND MODELING OF SHOULDER SURFING ATTACK

Sunghwan Kim[1], Heekyeong Noh[2], Chunghan Kim[3], and Seungjoo Kim[4]

CIST (Center for Information Security Technologies),
Korea University, Seoul, Korea
[1]tonykimsh@korea.ac.kr, [2]hknoh@korea.ac.kr,
[3]6sasimi@korea.ac.kr, [4]skim71@korea.ac.kr

ABSTRACT

As the use of smart phones 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 is currently 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 that 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-keypad 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

1. INTRODUCTION

As technologies such as the Internet, mobile, and wireless communications developed internationally, mobile devices became gradually smaller, and communications became faster. Accordingly, mobile devices evolved into the era of the smart phone, and users came to be able to develop various applications using open SDK (Software Development Kit) and then to use various contents. Referring to BOK (Bank of Korea) data, with the continued increase in the use of smart phones since the end of 2009, there were 37 million subscribers in South Korea by January 2014, and this growth has continued [1]. In addition to smart phones, the use of tablet PCs, too, has consistently increased, and there were about 650,000 subscribers as of January 2014 [2]. As a result, as smart phones and tablet PCs with mobility, portability, and convenience become distributed smoothly and there is much usage, more people enter or process important information using the relevant smart devices. Accordingly, virus infection through spyware created in the PC environment, malware installation through illegal file downloads, MITM (man in the middle attack) that intercepts user information, keystroke logging attack, and attack using social engineering techniques have all moved to smart devices. These attack techniques mostly aim at financial applications that may cause an economic loss, and attacks mostly target a user's important password such as a certificate password or account transfer password. The number and

Natarajan Meghanathan et al. (Eds) : WiMONe, NCS, SPM, CSEIT - 2014
pp. 93–112, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.41208

value of uses of mobile banking in the first quarter of 2014 were 27.6 million and 1.6634 trillion won, respectively, which were increases of nine thousand and about four hundred billion won respectively from the first quarter of 2013, and because it appears that usage will continue to increase consistently, careful attention among users is necessary [1]. In addition, in spite of an attempt to express shoulder surfing attack quantitatively by applying attack potential, it is erroneous to judge or measure the rating of attack potential in detail based on the elements of attack potential of existing CEM (Common Evaluation Methodology). This is because existing methodology does not include attack elements reflecting the characteristics of shoulder surfing attack. So there currently exists no standard by which the tolerance to shoulder surfing attack on the password input scheme can be judged.

Thus, this study proposes an attack potential that adds the attack elements through which attack potential of shoulder surfing attack can be judged to existing elements of attack potential on the password input scheme. In addition, as cases of the application of the proposed attack potential, with the password input scheme of the mobile banking applications provided in the market as subjects of analysis, this study analyzes the status of safety to determine whether the security keypads of mobile banking applications are safe from shoulder surfing attack.

2. RELATED WORK

2.1. Shoulder Surfing Attack and Password Input Scheme

Shoulder surfing attack refers to peeping around a user who is logging in or looking at sensitive information, without their awareness, when the user uses specific devices (smart phones, laptops, or PDAs) at an office, crowded shopping mall, airport, or coffee shop [3]. Thus, shoulder surfing attack is a powerful and effective means of attack for clearly observing the user password. In response to this, studies have been carried out in order either to develop an input scheme that allows users to enter their password behind their smart phones so that they are safer from shoulder surfing attack than with the existing password entry methods or to design and implement a method using a CoverPad to prevent information leak by attacks such as peeping when the users enter their password by the touch screen method [27][31]. In particular, the study that after standardized modeling of the shoulder surfing attack that is difficult to express by standardization, using a method like CPM-GOMS model, which can express it quantitatively and reviewed and tested the usability and safety of the qwerty keypad is one of the standardized studies related to shoulder surfing attack [26]. Xiaoyuan Suo et al. proposed that a password that a Web or smart phone user should enter for user authentication can be divided into a text-based one and a picture-based one [4]. The text-based password refers to an alphanumeric one consisting of numbers and characters while a picture-based password is divided into a perception-based one in which a user selects or passes one of the sets of passwords selected and registered in the procedure of password registration and a memory-based one in which a user is asked to copy or reproduce the picture created or selected by the user from among sets of pictures following the procedure of password registration. Both types of passwords aim to generate a password that the user can memorize easily and that has high security. While password generation in terms of security and usefulness is important, existing studies that analyzed the qwerty keypads used by current mobile banking applications report that the current qwerty keypads are exposed to the problem of the possibility of abuse by keystroke logging drawing random layouts through stochastic analysis [18], and thus the password security is under threat. Most studies suggest as alternatives to this to propose the use of a type of picture-based password as a substitute for the current security keypad [24]. Focusing on human memory and security, the picture-based password aims to increase the memorability of the password and, at the same time, increase security. Picture-based passwords can be concretely divided into three types: memory-based, perception-based, and memory-based with a clue. These picture-based passwords satisfy both usefulness and security and are intended for a design safe from several password attacks [25]. However, even if one uses the picture-based password, because of the characteristics of picture-based passwords, there are both safe and unsafe passwords in the case of shoulder surfing attack. First, Sobrade and Birget and Man et al., who proposed a graphical password as one of the types of perception-based picture passwords, argued that the graphical password would be safe from shoulder surfing attack since it is more difficult for an attacker to be able to recognize it as compared with existing text-based passwords [5][6], and Real User Corporation proposed that the Passface password, in which a user registers pictures of four faces in advance and chooses those four pictures from among nine pictures of faces for user authentication, would be safer than existing text-based passwords from shoulder surfing attack [7]. However, the above picture-based password has suitability problems when it comes to the essential characteristics of a password, which must be easy for the user to remember: e.g., one deficiency is that the user has to remember the character string value given to the image or has to memorize the pictures of the four pre-registered faces. Secondly, in a memory-based picture password, Jermyn et al. proposed the Draw-A-Secret (DAS) method of authentication in which a user draws simple pictures on a 2D grid, saves them in order, and then draws them in the same order for successful authentication [8]. And Goldberg et al. proposed the Passdoodle technique, in which a user draws pictures or writes characters randomly on a touch screen [9], and Blonder designed a scheme in which a password is generated by a user clicking on several positions of an image and proposed the Passlogix password technique of authentication by clicking on several positions in the same way to receive authentication [10]. All three password techniques were designed to possess greater resistance capacity against shoulder surfing attack than existing text-based passwords, but DAS, when used on a device with a large screen, may be vulnerable to peeping just as with existing shoulder surfing attack, and Passdoodle and Passlogix are not suitable for easy recall of password, as was the problem with perception-based picture passwords. So these might all lead to problems with users not being able to remember their password. In addition, both types of picture-based passwords were designed to be safe from shoulder surfing attack, but in user feedback, when checking whether the password a real user entered by drawing a picture was entered correctly, the process for validating the password entered before coding or the process of drawing a picture slowly because of unfamiliarity with password input may be exposed to shoulder surfing attack, and this has a weak point similar to that of existing text-based password schemes. Table 1 can be expressed as the schemes described above are features of the password entry.

Consequently, studies to increase security of password schemes, to design safe passwords, and to facilitate a user in remembering the password have consistently been carried out, but developing a password scheme to maintain the balance between safety and usability has been lacking, and there is the problem of vulnerability to shoulder surfing attack. Also, most studies of password schemes until now have depended simply on the password itself without mentioning detailed attack elements regarding shoulder surfing attack. To supplement and improve these points, criteria for judging the status of safety from shoulder surfing attack of password input schemes that have not been presented in existing studies are necessary, and for this purpose, the methodology of attack potential to be introduced in the following will be used.

2.2. Attack Potential

To draw safety criteria for the password input scheme from shoulder surfing attack, this section will follow the methodology of attack potential in the CC (Common Criteria) that previously presented standards so that the status of attack on specific targets such as smart cards or H/W devices can be quantitatively recognized. Attack potential refers to a function of expertise, resource, and motivation presented by CEM in the CC and consists of elapsed time, expertise, knowledge about a target of attack, period of easy exposure to attack, and equipment, and quantitatively demonstrates the attack potential of the target of attack by assigning values to each element [23].

Table 1. Password input 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 predictable	Dictionary attack, Brute force attack, Guessing, Shoulder surfing attack
	Draw-A-Secret (DAS)	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 draws	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	Guessing, Brute force attack, Shoulder surfing attack

The range of the sum of the calculated attack potential values can be expressed using the sub-ranges "0–20," "20–30," "30–34," "over 34," with higher knowledge about the target of attack being accumulated, and with high attack potential, the attacker has high attack potential. By contrast, lower values mean that the attacker has lower attack potential for the target of attack and has lower attack potential.

Table 2. Attack potential using CEM

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 month	7
		Within 3 month	10
		Within 4 month	13
		Within 5 month	15
		Within 6 month	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 take advantage of vulnerability of the target of attack, which is related to specialized knowledge, so the attacker with high specialized knowledge can use equipment with high attack potential.	Standard equipment	0
		Specialized equipment	4
		Customized equipment	7
		Complex customized equipment	9

However, the attack potential presented in CEM has limitations in that it does not include or meet attack elements necessary to quantify shoulder surfing attack, one of the attack methods for the password input scheme, nor does it judge the status of safety, and so it is not suitable for evaluating shoulder surfing attack. For this reason, existing attack potential possesses two problems: difficulty in judging the status of safety from shoulder surfing attack in a password input scheme and lack of reasonable criteria for calculating the attack potential of shoulder surfing attack.

Table 3. Vulnerability level of attack potential

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

3. SHOULDER SURFING ATTACK MODELING

3.1. Necessity of Formalized Attack Modeling

Various attack techniques on passwords have been presented in various ways. Table 1 shows the methods of attack and user usability possible for the above-mentioned picture-based password and text-based password. Various password-related attack methods have continued to be developed and executed until now. These include a) a keystroke logging attack that obtains coordinate information when the password the user enters is transferred to the server by inducing the user to install a malicious program to detect the password, b) an exhaustive search attack to detect user password by attempting all possible combinations of password, or c) a dictionary attack that can detect the key at considerably high probability when applied to a real situation by creating values that may be user key as a huge dictionary. Of them, shoulder surfing attack is possible with all password input schemes, as can be seen in the details presented in Table 1 [11]. This is because shoulder surfing attack can obtain relevant information by obtaining user information directly through peeping.

However, since shoulder surfing attack is one of the ergonomic aspects such as human perception, cognition, viewing angle, and memory, unlike with the other attack methods mentioned, there has been difficulty in quantitative expression. However, if quantitative expression is made possible through formalized modeling of threats and attack environments of attack conditions of shoulder surfing attack, a value of attack potential can be set for a shoulder surfing attack on a particular password input scheme so as to quantify that, and through the corresponding figures, whether the shoulder surfing attack on the password input scheme is safe can be determined. As seen in the cases of analysis applying attack potential to a specific target such as a smart card, ATM device, POI, or H/W device, the status of the attack potential can be judged by presenting the attack target's attack potential rating as scores [28][29][30]. However, in the above cases, as mentioned, there is a critical point in that it is difficult to present the attack elements in shoulder surfing attack using the elements of existing attack potential, so the following requirements should be drawn.

3.2. Drawing and Analyzing Requirements for Formalized Attack Modeling

This section lists the following attack elements to present standards for showing attack potential of shoulder surfing attack on the password input scheme and suggests standard values. Each standard value presented in each element was estimated, reflecting the characteristics that can be adjusted according to the type of technology and specific environment as described in the CEM document [23]. The attack potential of each element was classified into four values (1, 4, 7, 10), as with the CEM values, and the intervals of 3 points are differential values according to the characteristics described in the below attack elements, which aim to give distinction to the impacts of each element on shoulder surfing attack. This is a result of the use of the characteristics of attack potential that may be estimated differently according to the environment of the assessor who judges the tolerance of shoulder surfing attack on the password input scheme as well as the state of possible abuse.

3.2.1 Perception and recognition

In general, people go through processes of perceiving and recognizing texts (characters and numbers). As these processes are necessary and important elements in peeping over the shoulders at a user's important information, an attacker needs the ability to perceive and recognize the user's entering motions fast and accurately. The processes have a few common characteristics: first, recognition of a certain amount of texts in a given time. An English user can usually read and recognize sentences at a speed of 360 words per minute on average; that is, 6 words per second, which takes approximately 50 milliseconds [19]. Second, the sensory organs necessary for perception and recognition and the storing capacity for remembering this. One should remember the texts obtained through the processes of perception and recognition for a short time, which is called short-term memory and refers to memory that keeps one's experiences in one's consciousness for several seconds. Miller argued that the memory capacity of humans is 7 ± 2 items [32], and in a later study, he insisted that they memorize things in chunks, for example, they memorize about seven numbers, about six characters, and about five words as a chunk and immediately memorize what they need, dividing this into detail [33]. Since short-term memory carries out storing, perceived information can be said to be an important part of success in shoulder surfing attack, and so the capacity of short-term memory in an attack should be considered sufficiently. Lastly, the items stored in the above-described short-term memory may last for a short time or not be moved to long-term memory simply because of the lapsing of time and be forgotten within a short time. At this time, the recall rate for the items presented first may exhibit a high recency effect, which may act as important elements of how efficiently the attacker recalls the information peeped over the shoulder [12].

Consequently, when the user enters the password through the security keypad, the shoulder surfing attacker may obtain the user password through processes of perception and recognition only by his or her own sensory organs. Thus, the time taken for the attacker's perception and recognition should be shorter than that taken by the user between the input of the first password and that of the last one for a successful shoulder surfing attack. The existing GOMS-based model was used for user interface modeling and assumes perception, recognition, and behavior manipulations and predicts the run time through the critical path. As shown in the STM-GOMS study that applied this to shoulder surfing attack, the time, including the standby time such as that for the movement of an eye and a finger, is approximately 5.8 sec (5,840 msec.) while the total time of the input is approximately 5.3 sec (5,280 msec.). Regarding this, the time taken for the attacker's perception and recognition, including the movement of the eye that looks at the key the user presses, is 180 msec., the total time the attacker waits for the user's input during the total execution time is approximately 2.5 sec (2,510 msec.), and the time of the attacker's actual attack is approximately 2.8 sec (2,820 msec.) [19]. In this way, if the attacker's actual attack time is shorter than the total time of the user's input of password, shoulder surfing attack can be successful, and attack potential may appear, depending on the attacker's time of actual attack.

Table 4. Attack potential about perception and recognition

Perception and Recognition Time	Value
Over 5.8 sec.	1
4.8–5.8 sec.	4
3.8–4.8 sec.	7
2.8–3.8 sec.	10

3.2.2 Screen angle

People generally gaze at the screen of a smart phone reflected by light or from a looming and invisible angle. The angle from which they can see the contents of the screen best is when the screen is located horizontally and forms a 90° angle with the user's gaze—when the user is located as in Fig. 1—and the range of a total of 270°, excluding 315 to 45° hidden by the body, is the angle from which he or she can peep at the information on the screen through shoulder surfing attack [13].

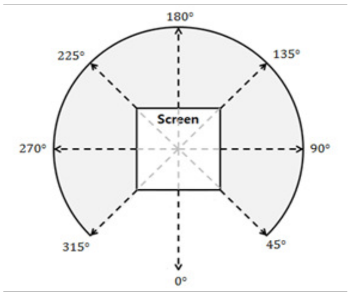

Figure 1. Horizontal angle of screen

A total of 270° can be said to be the angles from which the attacker can peep best. The 360° around the user are divided by 45°, and the angles in bilateral symmetry are evaluated as the same from 180°. In the horizontal angle between 0 and 45° (315 and 360°), from which the user looks at the screen, the screen is hidden by the user, so the attacker cannot see the screen, and thus it is judged that there is no attack potential. In the angle between 45 and 90° (270 and 315°), though oblique, the attacker can see the screen from an angle almost similar to that of the user, so he or she can see the character or number entered in the correct direction. Thus, at this time, there is the highest attack potential, and in the angle between 90 and 135° (225 and 270°), the attacker recognizes the character or number entered on the screen inclined 90° or more in the opposite direction, so it is more difficult for him or her to recognize the character or number as compared with at 45°. Thus, there is moderate attack potential in the relevant angle. Lastly, in the angle between 135 and 180° (180 and 225°), everything looks upside down when the attacker sees the screen, so it is difficult to judge the information entered within a short time, and thus this angle is judged to have the lowest attack potential.

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 Field of view

The maximum bevel angle from which a person can see the contents displayed on the screen by looking normally is called the FOV (field of view) [14]. Human eyes have an FOV of 0º in the direction of the nose, 95º in the outer direction, 0º in the upper direction, and 75º in the downward direction; and more specifically, they can be expressed by horizontal vision and vertical sight. First, horizontal vision can be shown as in Fig. 2, and the central vision, the very middle part, is called binocular vision. The FOV of binocular vision is about 0º in both the left and right directions, and since reading skills tend to decrease if it exceeds the relevant angles, one should form the FOV within in the angle of binocular vision to read texts or symbols accurately.

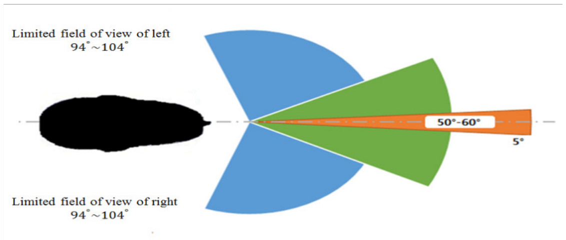

Figure 2. Horizontal FOV as seen by a man

Vertical sight can be shown as in Fig. 3, and in a seated and comfortable position for seeing, while relieving eye tension, about 15° becomes the plain sight downward, and in a standing position, 10° downward is the general sight. A total of 120 degrees, up to a maximum angle of 50° upward and up to 70° downward, are the upper and lower FOVs, respectively [15].

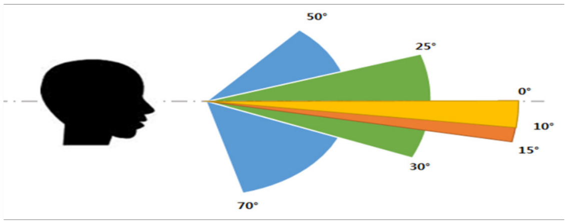

Figure 3. Vertical FOV as seen by a man

As such, a person's vision can decipher texts and symbols within the FOV range of the horizontal plane and the vertical plane. The optimal FOV is when 50 to 60° on the horizontal plane and 10 to 15° downward on the vertical plane are formed, and at this time, a sight most efficiently viewed by shoulder surfing attack is formed. Attack potential values can be shown as follows:

Table 6. Attack potential about the FOV

FOV (Field of View)		
Horizontal FOV	Vertical FOV	Value
Over 104 degrees	Over 70 degrees	1
30–104 degrees	30–70 degrees	4
0–30 degrees	15–30 degrees	7
0–5 degrees	0–15 degrees	10

3.2.4 Space and distance with legibility

The attacker should keep an appropriate distance from the target of attack and at the same time maintain the optimum distance possible for shoulder surfing attack. This should be done considering personal space and ability to recognize characters (their legibility).

3.2.4.1 Personal space

A personal space refers to the one that a person considers unconsciously to be his or her own domain. Most people give value to their own personal space, and when someone encroaches on it, they feel psychological discomfort, get angry, or alert the other person. This personal space includes intimate distance, personal distance, social distance, and public distance, shown as Fig. 4 below [16]. The intimate distance refers to the one between lovers, children, and parents; the personal distance, to the relationship between close friends; social distance, to the practical human relationship; and public distance, to the one in speeches or lectures. In shoulder surfing attack, the most important position and distance between the user and the attacker are determined within the range of the personal space that the user recognizes.

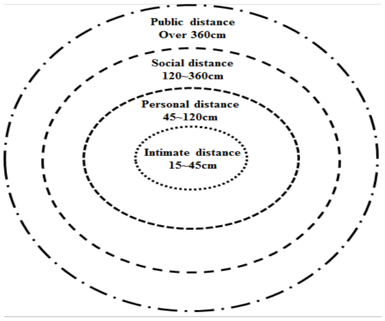

Figure 4. Personal space

Thus, when the user and the attacker are in the intimate distance (the closest distance), text legibility becomes optimum and the highest attack potential can be formed. In contrast, if they are located at the farthest distance (the public distance) the lowest attack potential may be formed, and the value of attack potential can be given accordingly.

Table 7. Attack potential about personal space

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

3.2.4.2 Text legibility

People fix their eyes, looking at a particular thing or object for a short time, and recognize or perceive the form through that. The measure of recognition of a letter or character is called legibility, and they have the ability to read legible characters or numbers through their gaze. A monitor is usually farther than the normal reading distance (30–35 cm), so the size of characters should be larger. It should be at least 10 pt., and from 11 pt. to 14 pt. is the size that the user can read comfortably [17]. Even the same font may have different legibility and preference depending on its size, and physical conditions such as sight may affect it, so text legibility should consider various complex factors. Other factors that may affect legibility include font, text size, background color, text color, method of presentation, illuminance, sight, age, and text interval [20]. Of these, the minimum size of a character according to sight distance is shown in Table 8, and when it meets the minimum size at each distance, inconvenience of legibility reaches the minimum. With regard to text size depending on sight, as shown in a comparative study of legibility in which there was the biggest difference in the minimum text size about 15 pt when there is a difference about 4 times, the sight distance is one of the most important factors impacting legibility [21], and the sight distance may be determined within the range of the above-presented personal space. Moreover, it turned out that numbers were more legible than characters and that under bright light, the minimum legible text size was a little smaller than under dull light [22].

Table 8. Minimum text size according to sight distance

Sight Distance	Minimum Size of Character
20cm	1.4mm
30cm	2.1mm
40cm	2.8mm

In addition, the younger the subject was, the better the legibility of characters and numbers was, and when the sight distance was 50 cm and 200 cm, appropriate legible characters were 8 pt. to 22 pt. for those in their 20s and 14 pt. to 32 pt. for those in their 60s [20]. The font size was related to the screen size, and when it is assumed that the font size of the qwerty keypad provided in the current mobile banking applications is approximately 9 to 10 pt, characters in the same font size looked larger in proportion to the screen size in the following order: Galaxy Note3 (5.68 inch), Galaxy S5 (5.1 inch), Galaxy S4 (4.99 inch), and iPhone 5S (4 inch). This means that fonts on smart phones with a larger screen size looked larger than the same ones on smaller smart phones, which led to better legibility. This also means that the font size that has the greatest impact on legibility may differ depending on the smart phone device the user uses, and at the same time, using a smart phone with a larger screen size leads to better legibility, although it may be more vulnerable to shoulder surfing attack. Consequently, attack potential for legibility can be shown according to the screen size of the smart phone the user uses.

Table 9. 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. Proposed Attack Potential

The proposed method adds the points of shoulder surfing attack to the existing attack potential measurement matrix since the existing measurement methods do not consider it. Thus, the classification of the rating of attack potential followed the system of the existing CEM as much as possible, as described below in this paper. The proposed attack potential can be shown as in Table 10. This added the condition of attack elements that can judge the attack potential tolerance of shoulder surfing attack to the existing attack elements. By doing so, the existing attack potential, which was not able to judge the attack potential tolerance of the shoulder surfing attack on the password input scheme, could be improved and supplemented. Moreover, it added shoulder surfing attack to the attack potential of attacks on several existing password input schemes, allowing us to demonstrate the attack potential rating of shoulder surfing attack.

This can be shown through the sum of the elements as low (0–30), medium (30–45), high (45–60), and very high (over 60), and as the sum of these values is high, the conditions that can make shoulder surfing attack succeed are met to the maximum. Using this, it can be judged that when attack potential of shoulder surfing attack falls within the “low” range at 0 to 30 points, it indicates that the probability of success in shoulder surfing attack is the lowest, while in contrast, when attack potential is over 60 points, in the range of “high or above,” it can be judged that the probability of success in shoulder surfing attack is the highest. This reflects the relative difference in vulnerability to shoulder surfing attack according to attack elements, which may be changed by the assessor, depending on the specific environment or conditions used in the attack.

Table 10. 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 months		7
	Within 3 months		10
	Within 4 months		13
	Within 5 months		15
	Within 6 months		17
	Over 6 months		19
Specialized knowledge	Layman		0
	Proficient		3
	Expert		6
	Complex 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/Limitless 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 Time	More than 5.8 sec.		1
	4.8–5.8 sec.		4
	3.8–4.8 sec.		7
	2.8–3.8 sec.		10
Screen Angle	0–45 (315–360) degrees		1
	135–180 (180–225) degrees		4
	90–135 (225–270) degrees		7
	45–90 (270–315) degrees		10
Field of View	Over 104 degrees	Over 70 degrees	1
	30–104 degrees	30–70 degrees	4
	0–30 degrees	15–30 degrees	7
	0–5 degrees	0–15 degrees	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

As a result, through the proposed attack potential, the attack potential rating to which shoulder surfing attack has been added can be judged along with the existing general password attack potential rating. If the proposed attack potential is applied to the qwerty keypad of the mobile banking applications in the market, the attack potential of shoulder surfing attack can be quantitatively known and accordingly, the attack potential rating can be known. Through relevant rating, the fact that the mobile banking applications of financial institutions are relatively more vulnerable to shoulder surfing attack can be understood. For this, the parts vulnerable to shoulder surfing attack, such as user feedback and the feedback offer time dealt with in the following section, should be supplemented and improved upon or a picture-based password with excellent user convenience and security should be developed so that users can be safe from several types of password attack including shoulder surfing attack. In addition, the security of the applications that can perform finance-related operations, such as mobile banking applications, should be higher than for other applications, and as well, their users' security consciousness should be higher. For this, the attack techniques that could not be expressed quantitatively, such as shoulder surfing attack, can be shown using exact figures, through which users can understand which security keypads provided by mobile banking applications of financial institutions are safe from shoulder surfing attack, and thus security consciousness about shoulder surfing attack can be perceived and improved.

Table 11. Vulnerability rating of the proposed attack potential

Range of Value	Attack Potential
0–30	Low
30–45	Medium
45–60	High
Over 60	Very high

4. ANALYSIS OF VULNERABILITY BY SECURITY KEYPAD

4.1 Analysis of Secure Keypad Vulnerability

This section will analyze the safety of security keypads—the qwerty keypad and the number keypad—provided by current mobile banking applications in South Korea, and determine and analyze weak points that facilitate shoulder surfing attack. Currently, most major financial institutions (banks, securities, insurance companies) ask the user to enter a password for an account and certificate or important information such as a security care number whenever he or she carries out financial tasks using a mobile banking application. Both the qwerty keypad and number keypad attempt to achieve security through random keypad layout, but random layout with small probability values and user feedback for confirming the password the user entered have security problems vulnerable to shoulder surfing attack.

4.1.1 Random Layout

4.1.1.1 Random layout of qwerty keypad

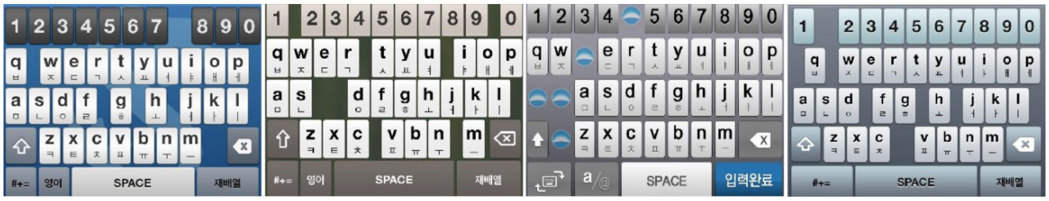

Figure 5. Qwerty keypads provided by the mobile banking applications of financial institutions in the Republic of Korea

In entering the certificate password on mobile banking applications, the user uses a security keypad, the qwerty keypad, and they generate 1 to 2 blanks randomly on each line of the qwerty keypad for safe input. But the number of cases of the positions in which a blank may be generated can be calculated, so the randomness of the blanks can be analyzed in terms of probability.

Table 12. The values of probability for the key layout of a qwerty keypad [18]

	□		□		□		□		□		□		□		□		□		□		□	
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								

As in Fig. 5, a keypad layout consisting of a total of 11 blanks on each line may be generated. Lines 1, 2, and 4 consist of 10 keys and 1 blank: 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10; q, w, e, r, t, y, u, i, o, and p; and z, x, c, v, b, n, and m. Line 3 consists of 9 keys and 2 blanks: a, s, d, f, g, h, j, k, and l. The attacker can calculate the values of the key distribution in which each key may be located through probability analysis [18], and using the relevant probability values, he or she can infer the key in the position of the observed input by probability and learn the qwerty keypad layout to carry out a shoulder surfing attack.

4.1.1.2 Random layout of number keypad

The number keypad used mainly to enter an account password or security card number consists of a random configuration of 10 number keys so that it can be safe from attacks such as keystroke logging. Also, numbers are encrypted with an asterisk (*), so even if an attacker intercepts it midway through, he or she will not be able to recognize them since they will have been encrypted. Unlike the qwerty keypad analyzed above, the number keypad possesses high randomness, so it is difficult to infer 10 digits that consistently change.

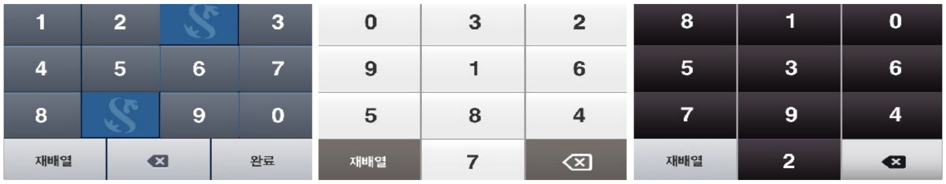

Figure 6. Random number keypad

As a result, the number keypad is designed with high security in mind, but the 10 number keys are completely randomly mixed, so the user has to find the right number to press, which leads to the inconvenience of the process taking a longer time. This deteriorates the user convenience but improves safety for attack models such as keystroke logging and MITM attack. But just like when using 4 digits, which are short and vulnerable to peeping, it is useless for preventing attacks such as shoulder surfing attack, which obtains passwords by observing the user's direct input.

4.1.2 User feedback and time of feedback

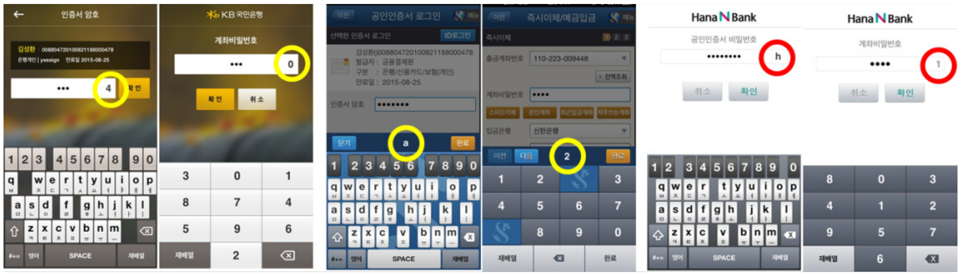

Figure 7. User feedback provided by qwerty keypads

In mobile banking applications in South Korea, security keypads have feedback processes to confirm the password the user entered, and in the processes, there are security weak points that encourage shoulder surfing attack. Both qwerty keypads and number keypads code passwords so that the keys entered are not seized by an attacker in the middle of a transmission to the server when the user touches the keypad to enter a password (that is masked using an asterisk), which is displayed before coding in order to check whether he or she entered it correctly. At this time, the suggested feedback time should consider convenience so that the user does not have any difficulty in entering and confirming his or her password, and at the same time, its security should be balanced so that it is safe from attack techniques such as shoulder surfing attack. However, since several of the security keypads of mobile banking applications continue displaying the text that the previous user entered without any time limit when they provide feedback about the values entered, the user's convenience increases, but there exists the problem that the attacker can see the text the user entered in plain text by just looking at the text provided as feedback without having to look at the key the user presses, resulting in lowering security.

Table 13. Time and method of user feedback for the mobile banking applications provided by each financial institution

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

4.2 Application and Analysis of Attack Potential for Mobile Banking Security Keypad

To determine the amount of the attack potential current mobile banking security keypads have for shoulder surfing attack, based on the following attack scenario, attack potential of the above proposed shoulder surfing attack is drawn . The proposed attack scenario is composed assuming the conditions under which shoulder surfing attack can be most powerfully carried out and successful.

◇ Attack Scenario (1)
The user and the attacker located at a close distance.
The user using Galaxy Note3.
The attacker is presumed to be the user’s close acquaintance.
The attacker in a low age group.
The attacker having learned random layout of qwerty keypad.
◇ Attack Scenario (2)
The user and the attacker located at a personal distance.
The user using Galaxy S5.
The attacker is presumed to be the user’s close acquaintance.
The attacker in a low age group.
The attacker having learned random layout of qwerty keypad.
◇ Attack Scenario (3)
The user and the attacker located at a close distance.
The user using Galaxy S5.
The attacker is presumed to be the user’s close acquaintance.
The attacker in a low age group.
The attacker having learned random layout of qwerty keypad.

The user does not have great apprehension about an acquaintance's approach to an adjacent position, so the attacker can attain the position and distance with the best legibility, and also, the user uses Galaxy Note3 with the largest screen size, so in terms of legibility, there is the optimum condition for shoulder surfing attack. In addition, through learning random layout, the attacker is familiar with the key layout, so the attacker easily recognizes and perceives them when the user uses 8 digits, the minimum requirement for a password. If values of the proposed attack potential apply, vulnerability to shoulder surfing attack can be demonstrated quantitatively. Attack potential values for mobile banking applications for each financial institution are provided in Table 14.

This is a setting of the values of attack potential according to attack scenario, and there were no differences in the values for elapsed time, specialized knowledge, knowledge about the attack target, and period to easily be exposed to attack and equipment, which are the existing elements of attack potential. And this is because the elements that might greatly affect shoulder surfing attack, such as one using a recording device, were not taken into account. However, if an attacker invests much time (elapsed time) in an attack to increase the success rate of his or her shoulder surfing attack, acquires the characteristics of the mobile banking keypad of each bank, and builds on specialized knowledge, the scores of the existing elements of attack potential may occur in several forms. So the existing elements of attack potential, also, should not be omitted.

In the proposed elements of attack potential, most attack potentials obtained the same scores, but for perception and recognition elements, there were differences in the scores, so the points were measured differently. This is because the attacker did not have any difficulty in perceiving and recognizing the text entered by the attacker, as A, B, and C Bank's mobile banking application security keypads kept providing user feedback without any time limits. In contrast, the mobile banking security keypads of D Bank and E Bank providing user feedback for about 2 seconds and that of F Bank not providing any user feedback created more difficulty in perception and recognition than other banks that keep providing feedback.

Thus, the real attack time of the attacker may be longer than the total time the user takes to enter the password, greatly reducing the likelihood that a shoulder surfing attack will be successful. Consequently, scores of perception and recognition were measured to be lower than those of other financial institutions. Accordingly, the attack potential value of F Bank's mobile banking application was 45 points, according to attack scenario (1). It had lower attack potential than other financial institutions, so it is relatively safer. Attack Scenario (2) showed the difference by lowering personal space and legibility, the elements greatly affecting shoulder surfing attack, by one step each from Attack Scenario (1). As a result, as shown in Table 15, the values of attack potential of all banks decreased by 9 points each from the results of Attack Scenario (1), and for example, in F Bank, the rating of attack potential went down one step. Along with this, Attack Scenario (3) could lead to the result shown in Table 16, with the same personal space as Scenario (1), but with legibility lowered one step, demonstrating the importance of legibility elements in shoulder surfing attack. Thus, to compare Attack Scenarios (1) and (2), even if legibility, the most important attack element of a shoulder surfing attacker, is altered, the difference in recognition and perception by the user attack provided by the mobile banking application of each bank is an important element that determines the rating of attack potential.

As a result, for mobile banking applications to have a relatively lower attack potential from shoulder surfing attack, it is necessary to provide user feedback—which is currently provided for an infinite time—for a finite time or develop a new security keypad that provides feedback through another method to maintain usefulness and achieve security at the same time.

Table 14. Attack potential of 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	Field of View	Screen angle	Personal space	Legibility	Attack potential
Bank A	0	0	0	1	0	10	10	10	10	10	51
Bank B	0	0	0	1	0	10	10	10	10	10	51
Bank C	0	0	0	1	0	10	10	10	10	10	51
Bank D	0	0	0	1	0	7	10	10	10	10	48
Bank E	0	0	0	1	0	7	10	10	10	10	48
Bank F	0	0	0	1	0	4	10	10	10	10	45

Table 15. Attack potential of 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	Field of View	Screen angle	Personal pace	Legibility	Attack potential
Bank A	0	0	0	1	0	10	7	10	7	7	42
Bank B	0	0	0	1	0	10	7	10	7	7	42
Bank C	0	0	0	1	0	10	7	10	7	7	42
Bank D	0	0	0	1	0	7	7	10	7	7	39
Bank E	0	0	0	1	0	7	7	10	7	7	39
Bank F	0	0	0	1	0	4	7	10	7	7	36

Table 16. Attack potential of mobile banking application for each financial company according to attack scenario(3)

Attack Elements / Mobile Banking Application	Elapsed time	Expertise	Knowledge about target of attack	Period of easy exposure to attack	Equipment	Recognition & perception	Field of View	Screen angle	Personal pace	Legibility	Attack potential
Bank A	0	0	0	1	0	10	10	10	10	7	48
Bank B	0	0	0	1	0	10	10	10	10	7	48
Bank C	0	0	0	1	0	10	10	10	10	7	48
Bank D	0	0	0	1	0	7	10	10	10	7	45
Bank E	0	0	0	1	0	7	10	10	10	7	45
Bank F	0	0	0	1	0	4	10	10	10	7	42

5. CONCLUSION

In this study, we revealed attack modeling conditions appropriate for shoulder surfing attack in order to improve critical points that attack potential in the CEM cannot quantitatively express with relation to shoulder surfing attack on password input scheme. In doing so, we were able quantify and express the shoulder surfing attack that could not be quantitatively expressed by the existing attack potential.

Also, we analyzed whether qwerty keypads and number keypads, used in current mobile banking applications, would be safe from shoulder surfing attack. We carried out the analysis using existing studies and their weak points and found that providing the keyboards with a less random layout and user feedback for unlimited time would be effective in preventing shoulder surfing attack. Through this, we were able to determine concrete values and situations for the listed attack conditions of shoulder surfing attack in which shoulder surfing attack could most successfully be facilitated.

As a result, we found that the security keypad of mobile banking applications was safest from shoulder surfing attack when the vulnerability rating registered “low”; and so existing commercial security keypads should be designed and implemented to have a minimum vulnerability rating of "low" for the proposed attack potential. Future studies should inquire into the attack potential of other password attack techniques in addition to the attack potential of security keypads of mobile banking applications by shoulder surfing attack.

ACKNOWLEDGEMENTS

This work was supported by the ICT R&D program of MSIP/IITP. [2014(10043959), Development of EAL4 level military fusion security solution for protecting against unauthorized accesses and ensuring a trusted execution environment in mobile devices]

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] Scott Pinzon and Kevin D. Mitnick "No Tech Hacking: A guide to Social Engineering, Dumpster Diving, and Shoulder Surfing", SYNGRESS, pp. 27-60, 2011

[4] Xiaoyuan Suo, Ying Zhu, and G. Scott. Owen, "Graphical Passwords: A Survey", IEEE, 2005

[5] L. Sobrado and J. C. irget, "Graphical Passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol.4, 2002

[6] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme", Proceedings of International conference on security and management, November, 2003

[7] RealUser, www.realuser.com, June, 2005

[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords", Proceedings of the 8th USENIX Security Symposium, 1999.

[9] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication", Proceedings of Human Factors in Computing Systems(CHI), USA, 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", 2007

[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] "Field of View", Wikipedia, September, 2014

[15] F. Row, "Landscape and Visual Impact Assessments", SLD Council, 2011

[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, v.14, no.3, June, 2013

[19] Sooyeon Shin and Taekyoung Kwon, "STM-GOMS Model : A Security Model for Authentication Schemes in Mobile Smart Device Environments", KIISC, v.22, no.6 , 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, 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, 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, Oct, 2008

[23] "Common Methodology for Information Technology Security Evaluation", 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 Aversaries Are More Powerful Than Expected”, IEEE Transactions on Systems, Man, And Cybernetics: Systems, June 2014

[27] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, and M. P. Scipioni, et al., “Back-of-device authentication on smartphones,” in Proc. CHI, 2013

[28] Joint Interpretation Library, “Application of Attack Potential to POIs”, June, 2011

[29] Joint Interpretation Library, “Application of Attack Potential to Hardware Devices with Security Boxes”, May, 2012

[30] Joint Interpretation Library, “Application of Attack Potential to Smartcards”, April, 2006

[31] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, “Designing leakageresilient password entry on touchscreen mobile devices,” in Proc. ASIACCS, 2013

[32] G. A. Miller, “The magical number seven, plus or minus two: Some limits on our capacity for processing information,” Psychol. Rev., vol. 63, no. 2

[33] Shiffrin, Richard; Robert Nosofsky (April 1994). "Seven plus or minus two: A commentary on capacity limitations.", Psychological Review. 2 101 (Centennial): 357–361, April 2012

AUTHORS

Sunghwan Kim received his B.S degree in Management Information System from Korea University(KU) of Korea, in 2013. He is currently working toward M.S degree in Financial Security, Korea University(KU), Korea. His research interests include Information Assurance, Financial Security, and Usable Security.

Heekyeong Noh received her B.S degree in Internet Information Engineering from Duksung Women’s Unviersity of Korea, in 2012. She is currently working toward M.S degree in Information Security, Korea University(KU), Korea. Her research interests include Password Security, Security Engineering, and CC(Common Criteria)

Chunghan Kim received his B.S degree in Computer Software Engineering from Kwangwoon University of Korea, in 2013. He is currently working toward M.S degree in Financial Security, Korea University, Korea. His research interests include Financial Security, Usable Security and Network Security.

Seungjoo Kim received his B.S., M.S. and Ph.D. from Sungkyunkwan University (SKKU) of Korea, in 1994, 1996 and 1999, respectively. Prior to joining the faculty at Korea University (KU) in 2011, He served as Assistant & Associate Professor at SKKU for 7 years. Before that, He served as Director of the Cryptographic Technology Team and the (CC-based) IT Security Evaluation Team of the Korea Internet & Security Agency (KISA) for 5 years. He is currently a Professor in the Graduate School of Information Security at KU, and a member of KU's Center for Information Security Technologies (CIST). Also, He is a Founder and Advisory Director of a hacker group, HARU and an international security & hacking conference, SECUINSIDE. Prof. Seungjoo Kim's research interests are mainly on cryptography, Cyber-Physical Security, IoT Security, and HCI Security. He is a corresponding author.