Hindawi
Security and Communication Networks
Volume 2018, Article ID 4296934, 14 pages
https://doi.org/10.1155/2018/4296934

Review Article

Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures

Xin Su[1], **Ziyu Wang**[2], **Xiaofeng Liu**[1], **Chang Choi**[3], **and Dongmin Choi**[4]

[1]*College of IOT Engineering, Changzhou Key Laboratory of Robotics and Intelligent Technology, Hohai University, Changzhou 213022, China*
[2]*Nanjing Ivtime, Co., Ltd., Nanjing 210000, China*
[3]*Department of Computer Engineering and IT Research Institute, Chosun University, Gwangju 61452, Republic of Korea*
[4]*Division of Undeclared Majors, Chosun University, Gwangju 61452, Republic of Korea*

Correspondence should be addressed to Dongmin Choi; jdmcc@chosun.ac.kr

Received 20 February 2018; Accepted 7 May 2018; Published 31 May 2018

Academic Editor: Pino Caballero-Gil

Including mobile environment, conventional security mechanisms have been adapted to satisfy the needs of users. However, the device environment-IoT-based number of connected devices is quite different to the previous traditional desktop PC- or mobile-based environment. Based on the IoT, different kinds of smart and mobile devices are fully connected automatically via device controller, such as smartphone. Therefore, controller must be secure compared to conventional security mechanism. According to the existing security threats, these are quite different from the previous ones. Thus, the countermeasures applied should be changed. However, the smart device-based authentication techniques that have been proposed to date are not adequate in terms of usability and security. From the viewpoint of usability, the environment is based on mobility, and thus devices are designed and developed to enhance their owners' efficiency. Thus, in all applications, there is a need to consider usability, even when the application is a security mechanism. Typically, mobility is emphasized over security. However, considering that the major characteristic of a device controller is deeply related to its owner's private information, a security technique that is robust to all kinds of attacks is mandatory. In this paper, we focus on security. First, in terms of security achievement, we investigate and categorize conventional attacks and emerging issues and then analyze conventional and existing countermeasures, respectively. Finally, as countermeasure concepts, we propose several representative methods.

1. Introduction

As mobile-based technologies continue to develop and propel society further into the information age, our surroundings are rapidly becoming ubiquitous mobile environments. According to the changes in the mobile-based society, increasing numbers of people are becoming mobile-based. Thus, it is a well-known fact that mobile devices are pervasive in today's global environment. The smartphone, a representative mobile device, provides various applications related to our daily life, which expand our living radius more efficiently. Moreover, IoT devices are fully connected via device controller, called smartphone. As an IoT device controller, smartphone gives various applications to users through widely developed applicable software and hardware products. Consequently, users feel increasingly drawn to use it in their daily lives in IoT environment via smartphone. The major parts of future IoT network infrastructure will be based on high-speed cellular networks that will be available everywhere, even in hostile places. Subsequently, the number of persons connecting to the Internet wirelessly will surpass the number connecting via wired infrastructure. Concomitant with the growth in mobile-related techniques, security and privacy issues will also increase. Likewise, the parts of human everyday life associated with IoT infrastructure will increase over time, and, thus, IoT devices will change from simple information-processing terminals to assisting and guiding their owners' whole lives as private secretaries. As a result, the information stored on IoT devices is more closely related to personal privacy. Hence, security and privacy issues are more important compared to non-IoT infrastructure-based society. In addition, today's device controllers include various

sensors to serve a variety of applications that deal with human biometric information, because some of these sensors collect and manage fingerprint, voice, iris, signature, and even behavior patterns. These types of information are unique information that can be used to verify the legitimacy of a user. Moreover, in accordance with development trends, developers are increasingly focusing on human biometric information for user identification and healthcare services [1, 2]. In accordance with the changes in the types of information handled by device controllers, attack patterns have also changed. Compared to the traditional attack patterns, attacks today tend to focus on human error. Thus, traditional and existing attack countermeasure schemes may not be suitable for emerging attack issues. Therefore, it is worth noting that security techniques must search wider and deeper than before. The remainder of this paper is organized as follows. In Section 2, we introduce related work, from traditional security threats to existing countermeasures. In Section 3, we show the drawbacks and downsides associated with existing countermeasures. In Section 4, we present countermeasure concepts and proposals that ensure resilience against emerging security threats. In Section 5, we present comparative results. Finally, we conclude the paper in Section 6 with a brief discussion.

2. Related Work

Much work has been carried out analyzing security threats. In this section, we categorize security threats and countermeasures. First, we divide security threats into two groups, traditional and emerging models, and then associate countermeasures with each security threat.

2.1. Traditional Threat Models

2.1.1. Guessing. Typically, users can access their systems with their own ID/password. In password guessing attacks, users' access rights are compromised by the two types of attack models discussed below.

Brute Force. In brute force attacks, the attacker continuously and repeatedly tries every possible passcode combination until the correct passcode is found. In scenarios where the passcode is short, only a short time is needed for the attacker to succeed, whereas a long passcode requires more time [3, 4].

Dictionary. In contrast to the brute force attack type, dictionary attacks try the most probable passcodes. Typically, many people have a tendency to choose short/meaningful words with no concern of being exposed. Thus, dictionary attacks try to find passcodes comprising word/phrases appearing in a dictionary [5, 6].

2.1.2. Replay. In replay attacks, successfully transferred valid data packets are delayed or repeated in order for attackers to get inside and pretend to be a legitimate user. Replay attacks are well known and thus countermeasures to avoid such attacks have been determined. However, in mobile authentication environments, replay attacks are being applied as a new type of attack [7, 8].

2.1.3. Spyware. Spyware is predominantly used for malicious purposes, with the aim of hiding from users, such as gathering information, tracking the behavior of users, and monitoring systems without the users' consent. From desktop PCs to mobile devices, spyware is a typical method for fulfilling the malicious purpose of attackers [9, 10].

2.2. Traditional Countermeasures

2.2.1. Text-Based Password. Passwords based on text are commonly used, even though the vulnerabilities are well known.

One of the factors influencing the security level of such passwords is their length. Long passwords take a long time for attackers to crack. However, users tend to use short passwords that are easier to remember [11].

To ensure adequate security, the following rules should be adhered to when using text-based passwords [12]:

(i) Do not use less than eight characters (more is better).

(ii) Do not use words that have meaning (meaningless is better).

(iii) Do not store them externally (keeping them only in your mind is better).

(iv) Do not unify (a unique password for each system is better).

(v) Do not maintain them over a long period (changing them periodically is better).

2.2.2. Personal Identification Number. Personal Identification Numbers (PINs) are commonly used for banking services, credit card authentication, mobile phone unlock systems, door lock systems, and so forth. A PIN comprises numeric keys only and typically ranges from four to eight digits [13, 14].

2.2.3. One-Time Password. A One-Time Password (OTP) is valid for one login session only and is not storable. An OTP is algorithmically generated based on time or mathematics for timely use. There are two approaches: static and dynamic. The static approach uses a document with a list of codes, whereas the dynamic approach may utilize methods such as SMS, hardware, and software tokens [15, 16].

2.3. Emerging Threat Models. As the number of mobile users continues to increase, the number of persons who want to connect to the Internet or use various online-based application services is also increasing. As is well known, mobile devices in public places are not as safe as wired network-connected devices that are located in secured spaces. However, unlike previous types of attacks, emerging attacks occur everywhere, even in secured places. This is because emerging threats are focused on the structural defects of mobile devices and the vulnerabilities of their owners. Therefore, we divide the threats into two types, owner and device, where owner means human errors and device means screen size and touch function.

Owner vulnerability, in other words, human errors, means the weakness induced by human mistakes. In most

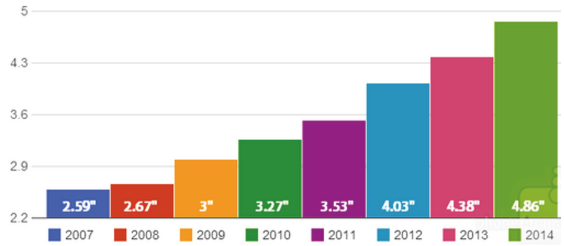


Figure 1: Trend in smartphone screen size.

cases, persons who use a mobile device do not take into account their surroundings, which may cause serious problems. One example of a device's structural defect is screen size greater than four or five inches. With a larger screen size for displaying information, a touch mechanism is also present on the screen. Typically, owners input secure information via touchable screen keypad to communicate with the device. Most structural defects, including owner vulnerabilities, result from this factor. Figure 1 shows the trend in smartphone screen size over time [17].

As screen sizes are bigger than before, owners should try their best to protect the information displayed onscreen from attackers.

2.3.1. Shoulder Surfing. For getting information, shoulder surfing uses direct observation techniques via the naked eyes. Nowadays, shoulder surfing is most effective, because it is easy to look over someone's shoulder when that mobile user is looking at the device screen without worrying about his/her surroundings.

There are two types of shoulder surfing attacks: single-attacker-based shoulder surfing with naked eyes and multiple-attacker-based shoulder surfing with naked eyes. Figure 2 illustrates the differences between these two attack types.

(i) Single Attacker. Single naked-eye-based shoulder surfing is commonly used by a single attacker. Preparing the attack incurs no cost for the attacker, but it is powerful enough to obtain the user's secret information [18, 19].

(ii) Multiple Attackers. In the case of single attack, the success rate is low. In contrast, when an attacker cooperates with other attackers to get users' secret information, even when the attacker only obtains some part of the secret information, they can combine the parts with each other. In this manner, they obtain all the information with a higher success rate compared to the single attacker.

2.3.2. Recording. The basic concept underlying recording is shoulder surfing. Shoulder surfing is based on naked human eyes only. As shown in Figure 3, recording is an extended peeking concept using all kinds of recording devices for the attack. It can also be divided into two types: single and multiple recording devices.

(i) Single Device. Single device recording is commonly used by a single attacker. Preparing for the attack incurs minimal cost for the attacker, but it is more powerful than single shoulder surfing because of the replayable video data.

(ii) Multiple Devices. As with the multiple shoulder surfing attack, single attacker or multiple attackers cooperate with each other with their video recording devices to obtain users' secret information. Thus, even though one attacker or device obtains only a part of the secret information, they can combine the parts with each other. Then, the entire information is obtained with a higher success rate than in the single case [20].

2.3.3. Hybrid. As shown in Figure 4, a hybrid attack is a combination of shoulder surfing and recording.

In this scenario, the naked eyes and multiple recording devices are used to obtain the password.

2.3.4. Smudge. The smudge attack is focused on the oily residue on the smartphone. Typically, a person who touches the screen uses their finger to touch the screen for usability. However, in the case of key arrays where the virtual keypad displayed on the screen is unchangeable, it is harmful. This is because finger touch positions can be restored by tracing the oily residue. In addition, in the case of pattern lock, it can be easily restored to the original onscreen pattern shape and direction, as shown in Figure 5 [21, 22].

2.3.5. Password Guessing with Sensors. Password guessing attacks use mobile device embedded sensors for guessing and obtaining secret information. Assume that a user inputs his/her own password or pattern using touch screen; if the attacker captures the touch sensors, he/she might get the information from the sensor data. Through the information, he/she can guess the key position or pattern in reverse [23, 24].

2.4. Existing Attack Countermeasures. Recently, in order to ensure safety against the various attacks occurring against mobile devices, researchers have proposed various concepts and mechanisms according to cost and security level [25]:

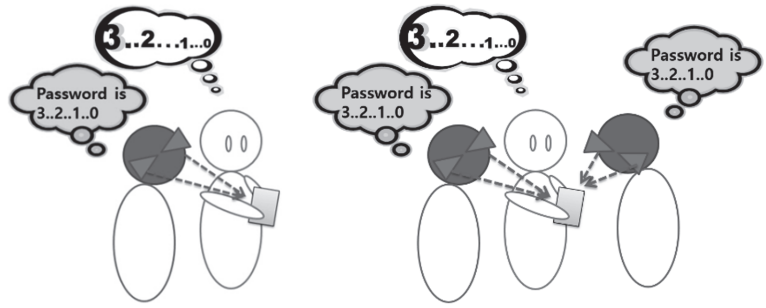
(i) High security with low cost—keystroke dynamics

(ii) High security with high cost—physical biometrics, token, and smart cards

(iii) Low security with low cost—password and PIN

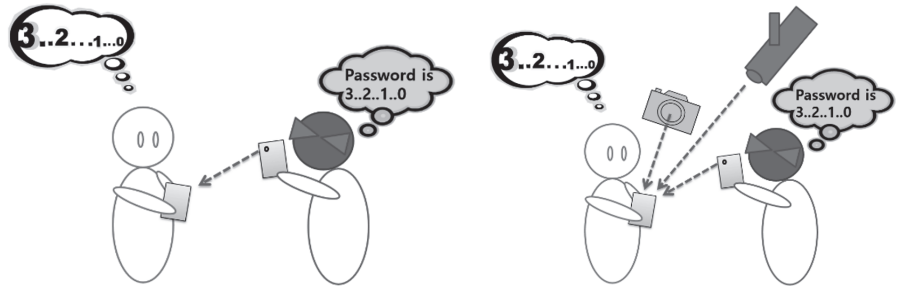
However, compared to the existing security mechanisms, several mechanisms are still not suitable owing to the higher cost. Thus, in this section, we omit several high-cost mechanisms such as token, smart card, and some physical biometrics.

2.4.1. Graphical Password. Many types of graphical password authentication mechanisms have been proposed by researchers. One such type is pattern-based mechanism [26]. Nowadays, many modified versions of pattern-based authentication mechanisms have been proposed with appealing advantages. Google has developed and imported a pattern-lock algorithm into their Android OS-based smartphones, and it is typically used worldwide.



(a) Single (b) Multiple

Figure 2: Comparison of shoulder surfing types.



(a) Single (b) Multiple

Figure 3: Comparison of single and multiple recording attack types.

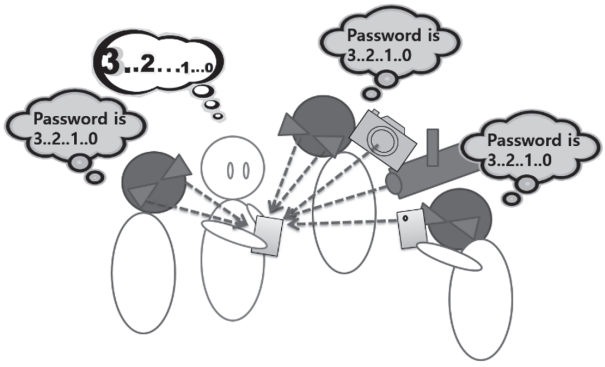


Figure 4: Hybrid attack scenario.

2.4.2. Fingerprint. Starting a few years ago, fingerprint modules have been embedded in mobile devices and developed with higher recognition rate and higher processing speed. Thus, fingerprint authentication is more suitable for mobile devices [27].

2.4.3. Voice. Based on differences in the voice signature of humans, researchers have proposed various person-identifying mechanisms. Das et al. even proposed a related algorithm for cellular phones [28].

2.4.4. Signature. Signature recognition is divided into two types: 2D-based and 3D-based.

Two-dimensional signature recognition is the traditional technique used to authenticate users. Nowadays, mobile-based 2D signature recognition mechanism is based on touchscreen. In the 3D-based mechanism, as shown in Figure 6, users take a magnetic object in hand, and then a compass sensor embedded in the mobile device checks the variances in the magnetic field. The mobile device verifies the user in accordance with the information of the changing log of the magnetic field [29, 30].

2.4.5. Behavior. With the network connection, network service providers can verify users by comparing their behavior profile. The profile is made by the service provider, and typically it has the user's interaction pattern with the service. Without the network connection, the mobile device checks the user's interaction with applications to identify whether the user is legitimate [31].

2.4.6. Keystroke Dynamics. On the basis of the concept of the keypad and keyboard typing pattern being different, the authentication mechanism verifies user. In contrast to typical authentication mechanisms, keystroke dynamics continuously check and verify users in the background. For one-time authentication, users register their password pattern for algorithmic learning. Figure 7 shows an example of keystroke pattern recognition [32].

3. Drawbacks and Countermeasures

3.1. Text Password

Drawbacks: various kinds of emerging attacks

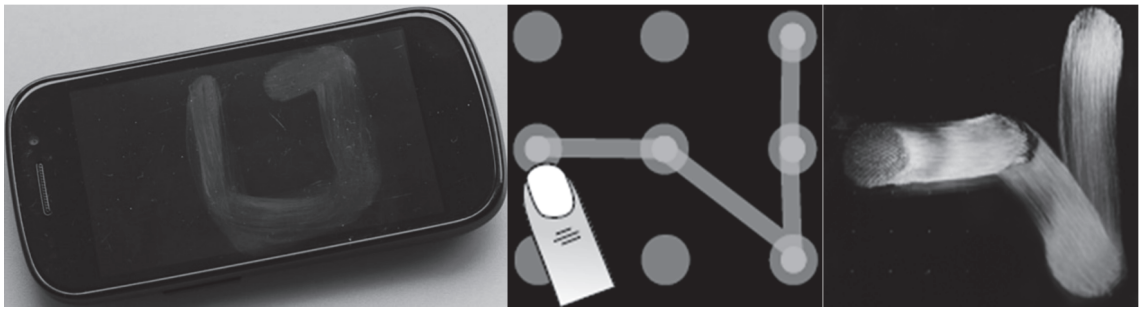
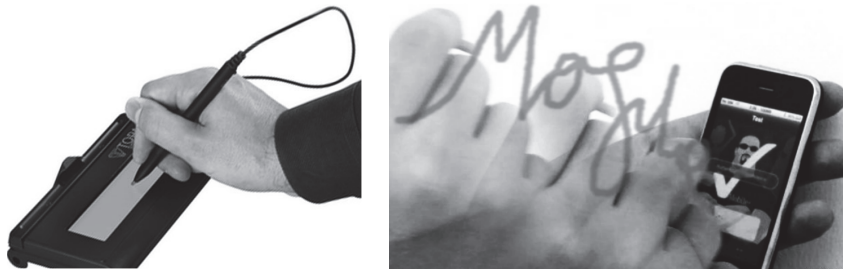


Figure 5: Imprinted finger direction on smartphone touch screen along with pattern direction.



(a) 2D touchpad signature (b) 3D magnetic signature

Figure 6: Signature comparison.

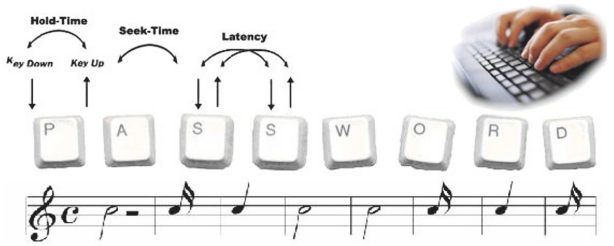


Figure 7: Example of keystroke pattern recognition.

Text passwords are vulnerable to traditional password guessing, shoulder surfing, recording, smudge, and password guessing with sensors. Once the secret information is exposed, it is over.

Countermeasures: information hiding, algorithm or mechanism combination, and indirect input method.

Wiping all information in the password mechanism which could give a clue for guessing the password is mandatory. Thus, the screen size or display window should display less information with a small area. Typically, the password input method is a virtual keypad or keyboard. Thus, a small keypad is required for higher resiliency against shoulder surfing, recording, and smudge.

3.2. Graphical Password

Drawbacks: shoulder surfing, recording, smudge, and password guessing with sensors

In this case, there is little or no information for guiding users to input password displayed on the screen of the mobile device. However, even though the password is not composed of textual information, it is still vulnerable to shoulder surfing, smudge, and password guessing with sensors. This is because graphical components are also easy for the attacker to remember. Thus, the attacker can easily obtain the information using electronic replayable recording devices.

Countermeasures: information hiding, algorithm, or mechanism combination

The development of nonvisible user graphical password authentication scheme can be a countermeasure. Typically, graphical components are visible. Thus, compared to text-based password, graphical password may be more vulnerable in specified conditions. Assuming that the graphical password-using user predefined a picture selection mechanism, whereas in the case of text-based password a shoulder surfing attacker may experience difficulty obtaining the original password from a long distance, a picture is larger than text. Thus, a shoulder surfing attacker may get the passcode from a long distance. Therefore, the use of one or more authentication mechanisms in concert with a graphical passcode is required.

3.3. PIN

Drawbacks: various kinds of emerging attacks

As with text password mechanisms, PINs are vulnerable to traditional password guessing, shoulder surfing, recording,

smudge, and password guessing with sensors. Moreover, a PIN utilizes only four to eight digits for user authentication. Thus, it is harmful when exposed. Even when only one or two digits are exposed, attackers can easily guess the whole secret information, because the number of cases is small compared the text password mechanisms.

Countermeasures: information hiding, algorithm or mechanism combination, and indirect input method

The direct password input method is not mandatory. In the case of social engineering attack scenarios, the attacker could see the user's behavior, while the user is operating his/her mobile device, including password input actions. If the mechanisms involve direct password input procedure, all kinds of display information, including user guide information, should be hidden against the emerging attack types. The best way to do this is to develop an indirect password input method. In the case of indirect input, guessing all the information through the displayed information only is difficult. Therefore, traditional PIN codes can support personal identification and authentication combined with an indirect input mechanism.

3.4. Fingerprint

Drawbacks: fake fingerprint and smudge

This method is still expensive and vulnerable to fake fingerprints [33]. Even though mobile device makers have produced flagship models with this technology, the higher price is not appropriate for mainstream users. Further, fingerprint is still vulnerable to fake fingerprint. Therefore, it is not very attractive at this time [32].

Countermeasures: algorithm or mechanism combination

To develop fake fingerprint resilient module, a combination of one or two more authentication mechanisms for identifying the correct owner is required. The development of high-resolution fingerprint detection device for detecting whole fingers is also required. However, these are only temporary solutions; therefore, it is mandatory to use two-way authentication.

3.5. Voice

Drawbacks: recording and environmental problems

Voice is vulnerable and may not be able to identify the owner if the owner's voice has changed owing to environmental reasons, such as fatigue, cold, and flu. Further, recording attacks may be able to circumvent voice recognition as attackers could record the user's voice when the user is logging into his/her device with his/her voice.

Countermeasures: algorithm or mechanism combination

It is not mandatory to use voice recognition mechanism for user verification only. In addition, it is recommended that it not be used for user verification with high proportion when the authentication mechanism uses two or more authentication mechanisms for user verification.

3.6. Signature

Drawbacks: recording, password guessing with sensors, and need for extra devices

A signature has been a typical way of verifying a legitimate user for a long time. However, with plain 2D, it is easy to imitate original signature characteristics. Thus, signature-based user authentication schemes in which information is written in 3D space, in short 3D signature, are being proposed. However, successful 3D signature schemes require extra devices to collect magnetic variation information.

Countermeasures: combination of authentication scheme and development of new types of signature authentication schemes

The security vulnerability of traditional 2D-based signature is well known. Thus, in the case of 2D signatures, one or more user verification mechanisms should be combined. In the case of 3D-based signatures, researchers still do not have sufficient results from their proposals, and they are still in the development stage. However, most 3D-based signature mechanisms use device embedded sensors, and they are thus reasonable.

3.7. Behaviors

Drawbacks: password guessing with sensors

User behavior patterns can be sensed and stored via device-embedded sensors as a kind of pattern data. Let us assume the case of mobile device application operation. Most applications typically are activated by the user's finger touch. Even if the user does not use the application via the touch screen, they can use other types of sensors such as gyro, gesture, accelerometer, magnetic, and light. Thus, at least one sensor can be used for user input in the mobile environment. However, sensors also enable vulnerability to password guessing. User behavior patterns that are recorded in real time are difficult to protect by encryption techniques because of hardware and power source limitations. Hence, before the sensor data profiling process, the raw sensor data can easily be captured by attackers using password guessing. Even in cases after the process of data profiling, exposure to common attacks using malicious codes is easy.

Countermeasures: no encryption in mobile device, selective use of raw data profiling by server, and combination of multisensor data

In order to reduce meaningless energy consumption, data encrypting and profiling tasks should be carried out on the server. Mobile devices should conserve their energy and be used only for detecting or sensing owner's behaviors. Then, some selected part of the data extracted from each sensor's raw data should be transferred to the server via algorithmic selection. Using the selected data, the server could profile and encrypt the data for authentication usage and then transfer these data to the mobile device. On receiving the data, the mobile device could use them to compare the current user's behavior pattern.

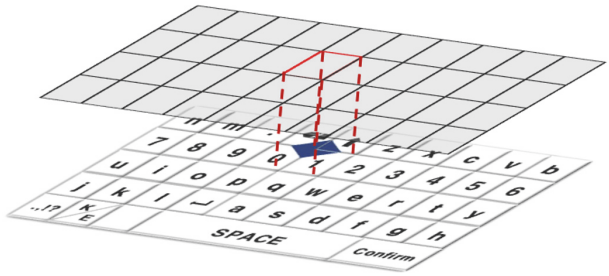


Figure 8: Grid mesh, pointer, and circular keyboard layout.

3.8. Keystroke Dynamics

Drawbacks: shoulder surfing, recording, and password guessing with sensors

Keystroke dynamics technique is visible and recordable. Thus, it is vulnerable when the legitimate user is inputting his/her passcode with a unique keystroke pattern in public places. Even in secret places, the typing sound also can be rhythmically generated. Thus, keystroke dynamics are also vulnerable.

Countermeasures: hiding visible information and applying sound shadowing technique

All kinds of visible information can give a clue to attackers as to how to circumvent the secure scheme. Thus, without the core contents appearing on the screen to guide the user, other information must disappear. Moreover, there should be a solution that enables hiding of the original keystroke pattern. The typical passcode input scheme does not consider hiding the original keystroke pattern. Thus, it is vulnerable when the attacker uses sound-based password guessing.

4. Proposals Related to Countermeasure Concepts

Among the existing attack countermeasures, we chose the five existing security mechanisms most commonly used worldwide. We briefly explain our proposals for ensuring that systems are robust to emerging attacks according to each proposal.

4.1. Text Password Robust to Emerging Attacks

(i) Combination of Circular Keypad and Grid Mesh Pointer. Our proposal is based on circular keypad and grid mesh. A circular keypad layout has no boundary; all edges of the keypad are connected with each other. Moreover, it can move every direction on the mobile screen as it is edgeless. Thus, it would appear to be circulating in every direction.

For secure input, a grid mesh that includes a secret pointer overlaps the circular keypad. The secret pointer location does not appear onscreen, and it is selected by the user in the registration stage. Figure 8 shows the proposed circular keypad-based grid mesh with secret pointer mechanism.

With this mechanism, the user should know the secret pointer location and password and then choose his/her password using the secret pointer. Figure 9 shows how the password is chosen via secret pointer in our proposed mechanism.

Figure 9(a) illustrates how a user inputs the letter "k" with the secret pointer. The grid mesh is fixed, and the keypad is freely moved in any direction. Thus, to choose the letter "k," the user slides the circular keypad to the right three grid spaces, as shown in Figure 9(b). Finally, the user slides the keypad up two grid spaces and then touches the edge of the screen to choose the letter.

(ii) Combination of Floating Keypad and Stick Pointers. The second proposal uses a combination of floating keypad and pointer array. As with the combination of circular keypad and grid mesh pointer, the floating keypad and pointer array can duplicate each other, as shown in Figure 10. At the registration stage, users define the size of the pointer array, choose a real pointer for password input, which makes the others fake pointers, and then register their secret information, password. At the user verification stage, users input their password using the real pointer. As shown in Figures 10(a)–10(c), the robustness of the proposal depends on the size of the pointer array.

4.2. Graphical Password Robust to Emerging Attacks

(i) Layered Pattern-Based Pattern Recognition Scheme. To deal with the problem of imprinted oily residue, our proposed scheme introduces an infinite layered concept called "pattern layer."

As shown in Figure 11, our concept is based on layer level. When users view the screen, they will see nine dots, same as the Google pattern lock. However, when the user is drawing his/her pattern, the pattern can be divided into many layers, which makes it difficult for an attacker to exploit, even if the pattern drawing motion and oily residue are being exposed. Figure 12 shows some example of layered pattern structures.

During pattern registration, putting a part of the pattern on the first layer is not required. Moreover, between two layers on which a pattern is drawn, space is available to put a number of blank (nonpattern) layers. Thus, the amount of combination is decided by user selection, which makes the proposed system more robust than the existing pattern drawing scheme.

(ii) Pattern with 3D Touch Scheme. Another way to make the pattern-based scheme more robust is to introduce 3D touch sensor combination.

The 3D touch sensor embedded in the newest iPhone series was developed in 2015.

According to the 3D touch function sensitive test application, it can recognize various pressure levels. Hence, instead of a number of pattern layers, we could apply 3D touch sensor data to verify the user. Figure 13 shows a pattern drawing with pressure level sensing.

As shown in Figure 13, let us assume that the whole pattern is a "Z" shape, and the first and third strokes are

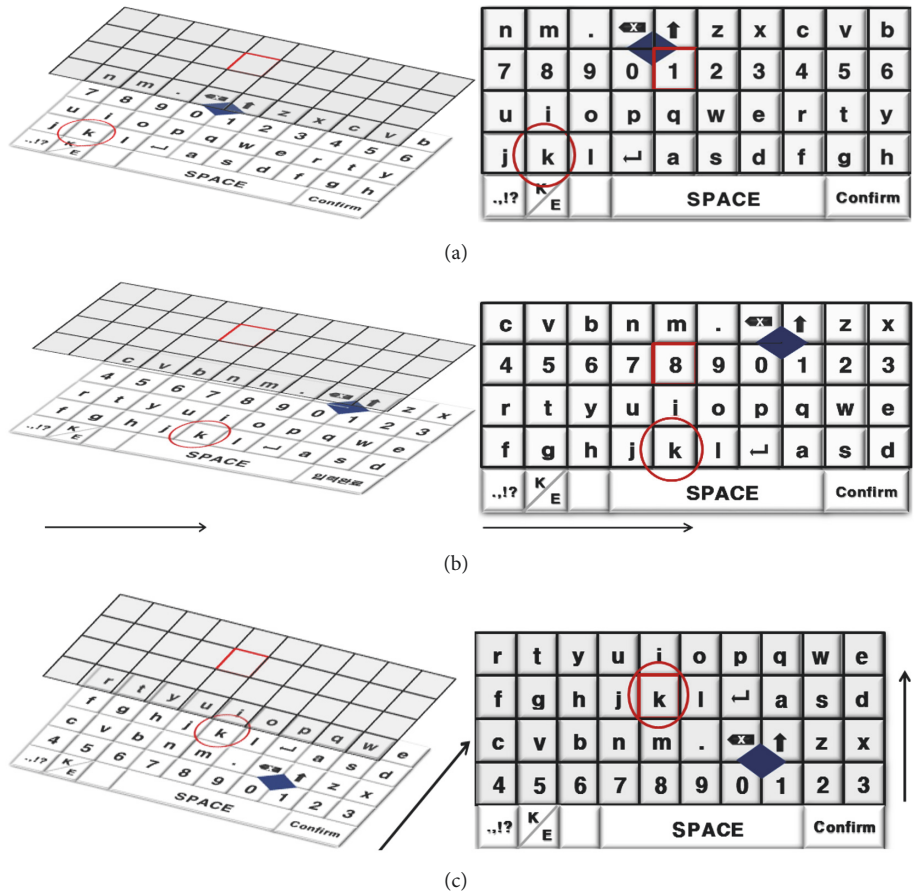


Figure 9: How to use grid pointer for input letter "k."

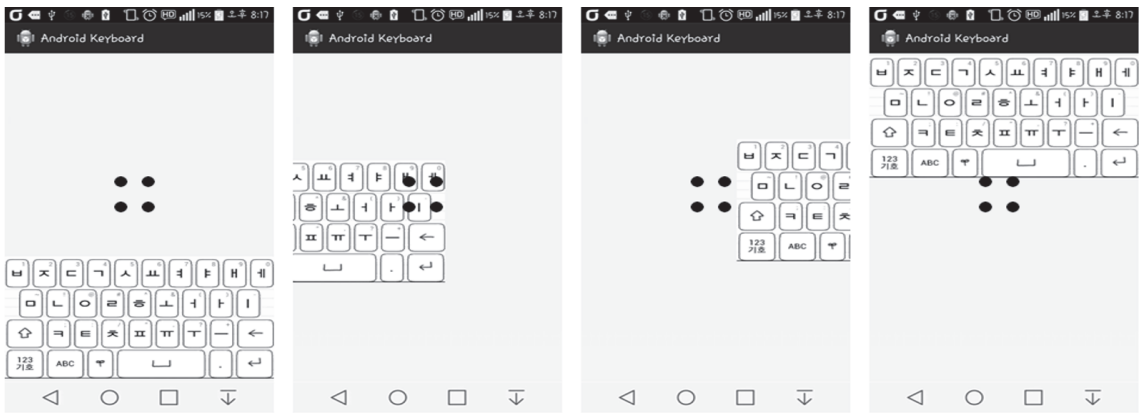
registered with high pressure. In other words, at the registration stage, users registered this pattern with the pressure information that is divided into three sections. The first section is drawn with high pressure, the second section is with low pressure, and the third section is with high pressure. Before the registration, the value of high and low pressure was defined by the user. Then, the user verifies it as shown in Figure 13(b). The pattern in section one was drawn with high finger pressure that is sensed by the pressure sensor in the device screen. During the second pass through with the finger, users do not draw with high pressure. Finally, in the third section, the user draws with high pressure. Therefore, even in the case of shoulder surfing, attackers cannot guess the exact pressure information. Moreover, with the complicated pattern and pressure pattern, it is more difficult to be exposed.

4.3. PIN Code Robust to Emerging Attacks

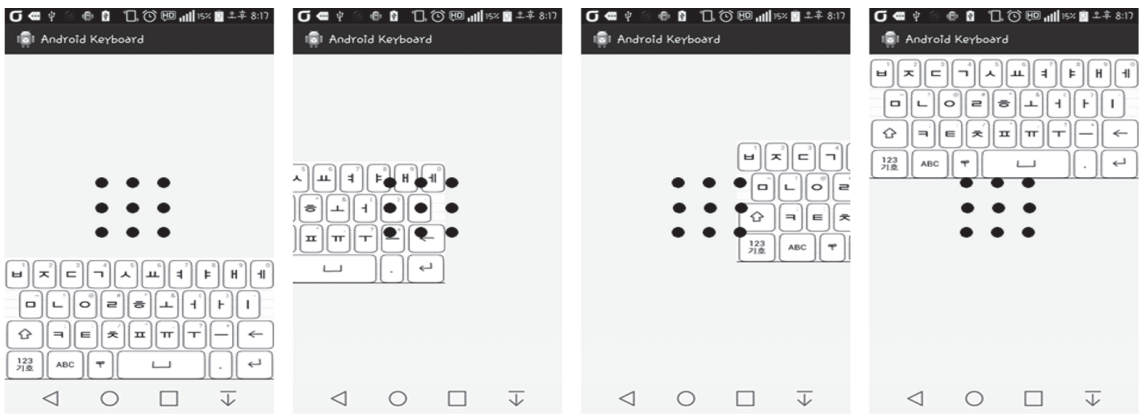
(i) Combination of Image Array and Circular PIN-Based Scheme. This scheme is similar to our proposal for robust text password. Figure 14 shows the proposed scheme robust to emerging attacks. The position of the PIN numbers appearing onscreen is randomly changed at every touch. In addition, the PIN code needs to be input with the user-selected image pointer or pointer sequence. Thus, there may be a need to remember PIN and image pointer or pointer sequence. Each PIN number digit must be connected with its own image pointer, and reusing of image pointer is allowed for every PIN digit. Therefore, the minimum length of our scheme is PIN length + one image pointer. The maximum length is allowed up to PIN length + maximum image pointer length equal to the length of PIN. Like this, our proposal gives various ways to choose between robustness and usability.

4.4. Signature Recognition Robust to Emerging Attacks

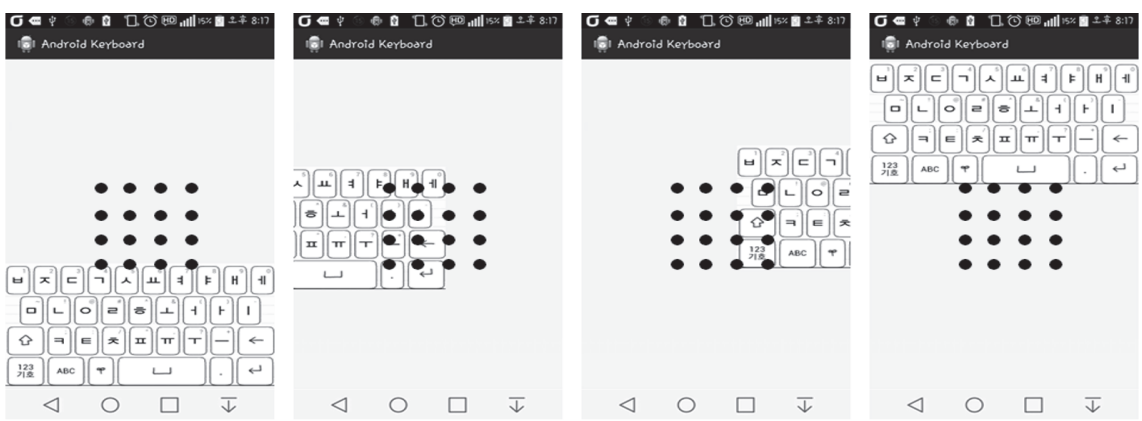
(i) Three-Dimensional Trace with Multisensor-Combination-Based Scheme. In contrast to the 2D-based handwritten signature recognition scheme, the 3D-based scheme traces the user's signature drawing pattern in three-dimensional space. Hence, 3D signature drawing information includes more information that is not detected in 2D-based schemes. Therefore, it is harder to counterfeit than 2D-based schemes. In addition, as shown in Figure 15(a), users may see their signature while writing on the tablet or touchscreen in 2D-based schemes, and this causes vulnerability to emerging attacks. However, as shown in Figure 15(b), no visible tracing action is needed in 3D-based scheme while the users are writing their signature in the air.



(a) 2 × 2 stick pointers



(b) 3 × 3 stick pointers



(c) 4 × 4 stick pointers

Figure 10: Floating keypad and stick pointers layout.

4.5. Fingerprint Recognition Robust to Fake Attacks and Emerging Attacks

(i) Combination of Fingerprint and Heart-Rate Mechanism. Typically, fingerprint authentication techniques are based on a single fingerprint module embedded on the backside or bottom of the device. However, it is vulnerable to fake attacks. Thus, we applied a heart-rate measurement technique for smartphones in order to identify whether a person is real. As shown in Figure 16, the smartphone-based heart-rate measurement technique utilizes a camera and flash. After combining the light and image, the blood flow rate is detected and can then be used for heart-rate calculation. In other words, the heart-rate detection technique can also detect a real person. Thus, combining heart-rate detection and fingerprint module is mandatory to make a robust scheme against fake attacks. Consequently, defending against fake attacks is the best way to defend against emerging attacks

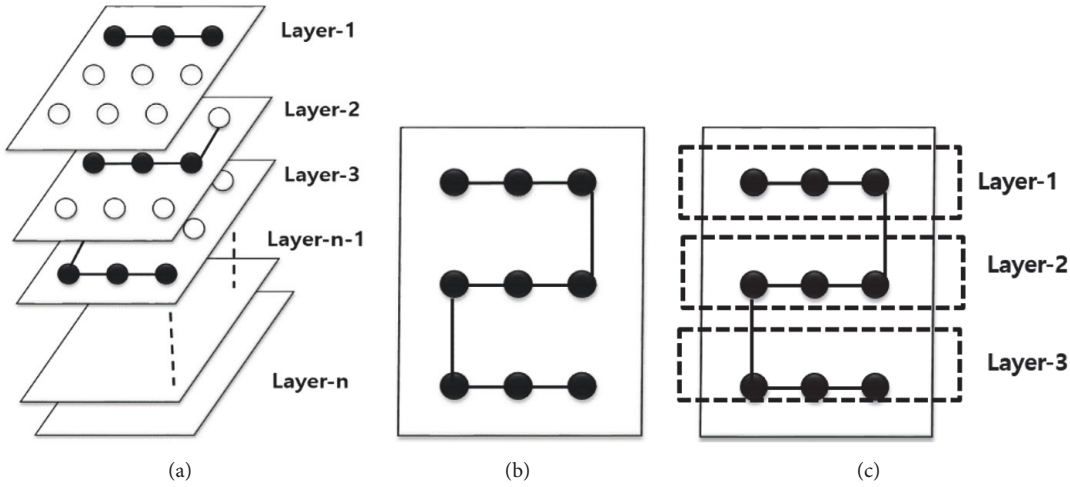


Figure 11: Layered pattern structure: (a) layer level in depth, (b) top view, and (c) top view with layer information.

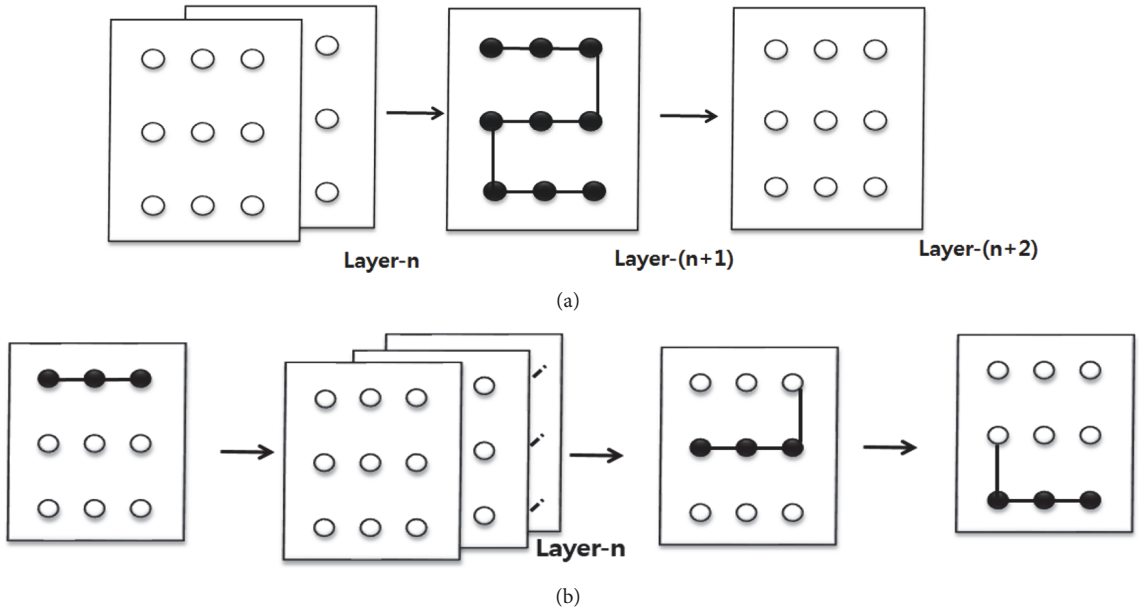


Figure 12: Other layer pattern registration methods: (a) n-layer shift before pattern drawing and (b) n-layer shift during pattern drawing.

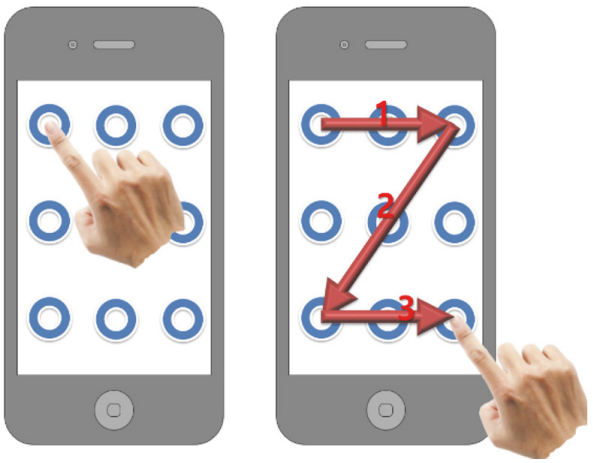
because emerging attacks consider oily residue from the owner's fingerprint only.

5. Comparative Analysis

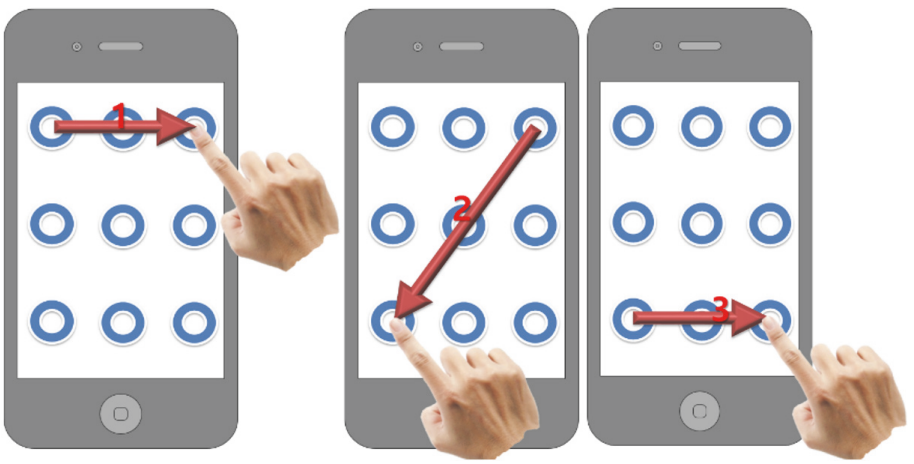
In this section, we analyze each proposed scheme in accordance with privacy and usability compared to the existing schemes. For the evaluation of usability, we simulated and tested the existing and proposed schemes layout structure using MIT App Inventor 2. Then, we checked the schemes against a checklist. In the security comparison, we compared related existing and proposed schemes according to the emerging attack categorization addressed in Section 2.

Table 1 compares the robustness of the existing and proposed schemes against possible emerging attacks. We assigned a number to each of the existing and proposed schemes for convenience: (1) existing text password, (2) proposed combination of circular keypad and grid mesh pointer, (3) proposed combination of floating keypad and stick pointers, (4) existing graphical password, (5) proposed layered pattern-based pattern recognition scheme, (6) proposed pattern with 3D touch scheme, (7) existing PIN code, (8) proposed combination of image array and circular PIN-based scheme, (9) existing signature recognition, (10) proposed 3D trace with multisensor-combination-based scheme, (11) existing fingerprint recognition, and (12) proposed combination of fingerprint and heart-rate mechanism. For the comparison, we used the initials "G," "M," and "B" to denote good, moderate, and bad for each item, respectively.

As shown in Table 1, the proposed schemes have higher security levels than existing schemes except for the sensor item. This is because the proposed scheme did not assume

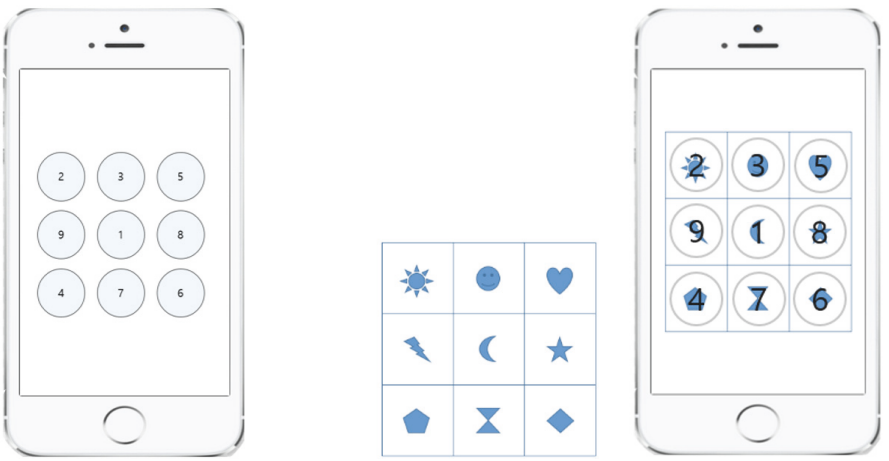


(a) Whole pattern drawing



(b) Example of pattern drawing sequence and pressure differences

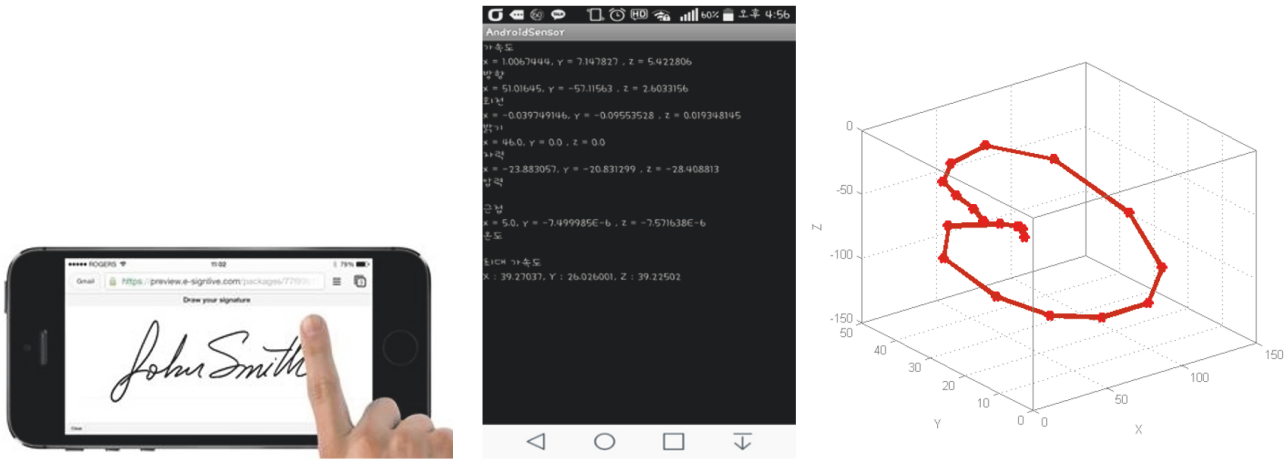
Figure 13: Pattern drawing with pressure.



(a) Normal PIN and image pointer grid set

(b) PIN overlay on image pointer

Figure 14: Proposed PIN scheme.



(a) Example of 2D signature

(b) Example of 3D signature

Figure 15: Proposed 3D signature scheme.

Table 1: Security comparison.

Existing and Proposed Schemes		Possible Emerging Attacks						
		Shoulder surfing		Recording		Hybrid	Smudge	Password guessing with sensors
		single	multiple	single	multiple			
Text	1	B	B	B	B	B	B	B
	2	G	G	G	G	G	G	G
	3	G	M	G	M	M	G	G
Graphical	4	B	B	B	B	B	B	B
	5	G	G	G	M	M	G	M
	6	G	G	G	G	M	G	B
PIN	7	B	B	B	B	B	B	B
	8	G	G	G	M	M	G	G
Signature	9	M	M	B	B	B	M	B
	10	G	G	G	G	G	G	B
Fingerprint	11	G	G	G	G	G	B	G
	12	G	G	G	G	G	G	G

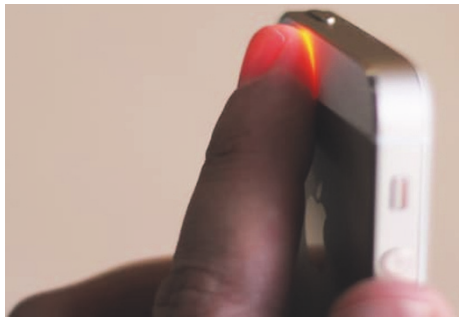


Figure 16: Heart-rate detection with camera and flash.

data protection. Thus, it would give a better result if it considered data encryption. Table 2 shows the usability comparison.

As shown in Table 2, most of the existing schemes have user-friendly characteristics. Because of this point, a number of users do not want to change from their traditional scheme to a more secure scheme. During the comparison, we found that user-behavior-based schemes have many possibilities to expand their application. User behavior is a kind of human biometrics, and behavior is based on accumulated human behavior pattern, which is naturally optimized for many years for each person. This is the reason why the user feels that this kind of scheme is user-friendly.

Finally, Table 3 shows the proposed schemes' advantages and disadvantages from users' experience.

As shown in Table 3, most of the proposed schemes have a low input speed problem and a memory problem. Apart from these problems, participants gave positive reactions. Thus, we expect that the proposed schemes will get more positive results following input speed and memory improvements.

6. Conclusions

In recent times, the mobile device-based market has been increasing continuously. However, opportunities for creating damage have also increased along with the size of the market.

Table 2: Usability comparison.

Existing and proposed schemes		Possible metrics classification					
		Easy registration	Typing speed	Typing error	Easy to understand	Easy to remember	Login speed
Text	1	G	G	M	G	G	G
	2	G	M	G	M	M	M
	3	G	M	G	M	M	M
Graphical	4	G	G	G	G	G	G
	5	M	B	M	M	B	B
	6	G	G	G	G	G	G
PIN	7	G	G	G	G	G	G
	8	M	M	G	M	M	M
Signature	9	G	G	G	G	G	G
	10	G	G	M	G	G	G
Fingerprint	11	G	G	G	G	G	G
	12	G	G	G	G	G	G

Table 3: Comparison table of proposed schemes.

Category	Proposed	Advantages	Disadvantages
Text password	Circular keypad with grid mesh pointer	Display no password on screen Very hard to estimate or trace	Low input speed Remember longer password information
	Floating keypad with stick pointers	Display no password on screen Hard to estimate or trace	Low input speed Remember longer password information
Graphical password	Layered pattern	Hard to estimate or trace	Low drawing speed Remember more information about layers Need more functions for moving between the layers
	Pattern with 3D touch	Very hard to estimate or trace Higher speed compared to layered pattern	Remember more information about section pressures Need 3D sensor-embedded device
PIN	Image array and circular PIN combination	Randomly repositioned PIN code Hard to estimate or trace	Low input speed Remember more information about password/image combination
Signature	Sensor-based 3D signature	High speed No need for optional device	Need higher algorithmic sensible detection process
Fingerprint	Fingerprint with heart-rate detection	Robust to fake attack No need for optional device	Depending on mobile device structure

This paper focused on emerging security threats targeting mobile device structure defects and human errors and highlighted the vulnerabilities in existing schemes. Subsequently, schemes were proposed in accordance with each category and were shown to exhibit robust results against emerging attacks compared to existing schemes. However, although our schemes are very secure, their usability is still insufficient. Therefore, in future work, we plan to modify our schemes to make them more acceptable to users. Our objective is to improve the schemes up to at least the existing user experience level of the well-known schemes. In addition, we determined that human biometric-based schemes are more reasonable, user-friendly, and robust to verify users. Thus, we also plan to develop a novel human biometric-based scheme.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Natural Science Foundation of Jiangsu Province (Grant BK20160287) and in part by the Key Research and Development Program of Jiangsu (Grants BE2017071 and BE2017647). It was also supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (no. 2017R1E1A1A01077913) and by the MIST (Ministry of Science & ICT), Korea, under the National Program for Excellence in SW supervised by the IITP (Institute for Information & Communications Technology Promotion) (2017-0-00137).

References

[1] T. Wang, Y. Chen, M. Zhang, J. Chen, and H. Snoussi, "Internal transfer learning for improving performance in human action

recognition for small datasets," *IEEE Access*, vol. 5, pp. 17627–17633, 2017.

[2] T. Wang and H. Snoussi, "Detection of abnormal visual events via global optical flow orientation histogram," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 988–998, 2014.

[3] https://en.wikipedia.org/wiki/Brute-force_attack.

[4] I. Kim, "Keypad against brute force attacks on smartphones," *IET Information Security*, vol. 6, no. 2, pp. 71–76, 2012.

[5] https://en.wikipedia.org/wiki/Dictionary_attack.

[6] A. K. Kyaw, F. Sioquim, and J. Joseph, "Dictionary attack on wordpress: security and forensic analysis," in *Proceedings of the 2nd International Conference on Information Security and Cyber Forensics (InfoSec '15)*, pp. 158–164, November 2015.

[7] H. Shin, D. Kim, and J. Hur, "Secure pattern-based authentication against shoulder surfing attack in smart devices," in *Proceedings of the 7th International Conference on Ubiquitous and Future Networks (ICUFN '15)*, pp. 13–18, July 2015.

[8] https://en.wikipedia.org/wiki/Replay_attack.

[9] https://www.ftc.gov/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-other-software.

[10] E. Darbanian and G. D. Fard, "A graphical password against spyware and shoulder-surfing attacks," in *Proceedings of the 20th International Symposium on Computer Science and Software Engineering (CSSE '15)*, pp. 1–6, August 2015.

[11] A. Adams and M. A. Sasse, "Users are not the enemy: why users comprise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, no. 12, pp. 41–46, 1999.

[12] T.-S. Wu, M.-L. Lee, H.-Y. Lin, and C.-Y. Wang, "Shoulder-surfing-proof graphical password authentication scheme," *International Journal of Information Security*, vol. 13, no. 3, pp. 245–254, 2014.

[13] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking PINs," in *Financial Cryptography (LNCS)*, pp. 25–40, Springer, New York, NY, USA, 2012.

[14] https://en.wikipedia.org/wiki/Personal_identification_number.

[15] https://en.wikipedia.org/wiki/One-time_password.

[16] J. A. Vila, J. Serna-Olvera, L. Fernández, M. Medina, and A. Sfakianakis, "A professional view on ebanking authentication: challenges and recommendations," in *Proceedings of the 9th International Conference on Information Assurance and Security (IAS '13)*, pp. 43–48, December 2013.

[17] G. Perna, "How does screen size effect viewer's response to various types of media?" screenMediaUCSD, March 2015, http://screenmediaucsd.wikispaces.com/-/Term%20Wiki%20WI15/Team%2016/How+does+screen+size+effect+viewer%27+response+to+various+types+of+media%3F.

[18] H. Kim, H. Seo, Y. Lee, and T. Park, "Implementation of secure virtual financial keypad for shoulder surfing attack," *Korea Institute of Information Security and Cryptography*, vol. 23, no. 6, pp. 21–29, 2013.

[19] H.-M. Sun, S.-T. Chen, J.-H. Yeh, and C.-Y. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180–193, 2018.

[20] T. Takada, "FakePointer: an authentication scheme for improving security against peeping attacks using video cameras," in *Proceedings of the 2nd International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM '08)*, pp. 395–400, Valencia, Spain, September 2008.

[21] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proceedings of the USENIX Conference on Offensive Technologies*, pp. 1–7, 2010.

[22] S. Shankland, Reverse smudge engineering foils android unlock security, http://www.cnet.com/news/reverse-smudge-engineering-foils-android-unlock-security/.

[23] L. Cai and H. Chen, "TouchLogger: inferring keystrokes on touch screen from smartphone motion," in *Proceedings of the 6th USENIX Conference on Hot Topics in Security*, 2011.

[24] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury, "Tapprints: your finger taps have fingerprints," in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services (MobiSys '12)*, pp. 323–336, Ambleside, UK, June 2012.

[25] P. S. Teh, A. B. J. Teoh, C. Tee, and T. S. Ong, "Keystroke dynamics in password authentication enhancement," *Expert Systems with Applications*, vol. 37, no. 12, pp. 8618–8627, 2010.

[26] C. E. Larsen, R. Trip, and C. R. Johnson, "Direct, Gesture-based Actions from Device's Lock Screen," US 8136053 B1, http://www.google.com/patents/US8136053.

[27] N. L. Clarke, S. M. Furnell, P. M. Rodwell, and P. L. Reynolds, "Acceptance of subscriber authentication methods for mobile telephony devices," *Computers & Security*, vol. 21, no. 3, pp. 220–228, 2002.

[28] A. Das, O. K. Manyam, M. Tapaswi, and V. Taranalli, "Multilingual spoken-password based user authentication in emerging economies using cellular phone networks," in *Proceedings of the IEEE Workshop on Spoken Language Technology (SLT '08)*, pp. 5–8, IEEE, December 2008.

[29] K.-H. Kamer, A. Yuksel, A. Jahnbekam, M. Roshan-del, and D. Skirpo, "MagiSign: user identification/authentication based on 3D around device magnetic signatures," in *Proceedings of Ubicomm*, pp. 31–34, 2010.

[30] H. Ketabdar, P. Moghadam, B. Naderi, and M. Roshandel, "Magnetic signatures in air for mobile devices," in *Proceedings of the 14th ACM International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '12)*, pp. 185–188, September 2012.

[31] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," in *Proceedings of the 10th European Conference on Information Warfare and Security (ECIW '11)*, pp. 307–314, July 2011.

[32] Deepnet Security, "Keystroke Recognition," http://www.deepnetsecurity.com/authenticators/biometrics/typesense/.

[33] J. Kil, "Iphone and galaxy phone penetrated by fake fingerprint," http://www.etnews.com/20160217000327.