Humanics information security

Humanics Information Security

Masakatsu Nishigaki

Graduate School of Science and Technology, Shizuoka University
3-5-1 Johoku, Naka, Hamamatsu 432-8011, JAPAN
nisigaki@inf.shizuoka.ac.jp

Abstract

So far, information security has been focusing mainly on how to improve security and safety technologies. As people are becoming connected with a larger amount of cyber equipment, however, the human aspect in cyber security and safety has gained more attention as an essential issue. In other words, both security and usability of ICT systems have recently become much more critical to achieve. Nevertheless, as everybody knows, security and usability have a trade-off relationship. Even when a security technology offers a high security level for an ICT system, if it greatly degrades the usability, the security technology will not be used. However, it is not always true that we can never accept any difficulty or bother. If a security technology burdens a user but the user does not notice the burden or even enjoys it, there is no problem. How people feel is key. Against this background, my colleagues and I have been studying how to combine security technologies and human factors, specifically cognitive and psychological characteristics. We call the concept “humanics information security.” This paper describes our pilot studies and explains how our humanics information security approach can effectively achieve both security and usability for ICT systems.

Keywords： security, usability, user authentication, CAPTCHA, humanics, psychology.

1 Introduction

Suppose that a content provider is selling downloadable movies online. The content provider encrypts the movies with a key to protect data from eavesdroppers. The provider gives the key to a purchaser who pays money so that only purchaser can decrypt and enjoy watching the movies. An eavesdropper without the key cannot view the data by only eavesdropping encrypted movies. However, if the purchaser is malicious, the purchaser can make copies of the decrypted movies and share the data illegally. Thus, encryption is a vital technique to keep out eavesdroppers, but its effect on bad-faith purchasers is limited.

This is not only a problem in illegal content sharing. In almost all cases, no such single security technique alone is perfect. To make an ICT (information and communication technology) system secure, we have to use many techniques simultaneously and use the right technique in the right place [27]. In other words, system security is achieved by orchestrating various security techniques properly.

Besides, we need to consider one more factor: who uses the ICT systems. The answer is, of course, human beings. At the same time, we need to consider who attacks the ICT systems. The answer is, unfortunately, human beings again. Therefore, any system security that does not consider user characteristics is pointless. The orchestration of security techniques must be ensured from viewpoints of both legitimate and malicious users.

What is important here is that this orchestration is a critical challenge involving a trade-off between security and usability. The higher security is pursued, the more usability is reduced, and vice versa. For instance, a multi-password authentication will enhance the security level of an ICT system, but it is very difficult and bothersome for us to remember many passwords and enter them one-by-one many times over. This might push users to use easy passwords, thus eventually degrading the security level of the ICT system.

Nevertheless, it is not true that we can never accept any difficulty or bother. Easy video games are often unexciting to gamers, who tend to have fun playing challenging games. People usually do not want to get up early for work, but anglers happily do so to go fishing. In these ways, even if a person has a difficult and/or bothersome task to perform, if he/she enjoys or desires carrying it out, the task is naturally accomplished. The first and fundamental principle of ICT system design is, of course, to reduce security and safety risks as much as possible. But, I believe that consideration of such human characteristics described above is equally as important and indispensable to abolish the trade-off between security and usability in ICT system design.

This is an eccentric example, but what if authentication is your hobby and you love to punch in passwords? Perhaps, in your spare time you would enjoy punching in your password again and again. In such situations where the user wants to say "I want to enter the password," the user will not feel annoyed at entering a password for authentication any more. More typically, he/she will want to perform password authentication again and again. Another interesting possibility arises from the fact that humans have a possessive nature [28]. A person often has a strong sense of satisfaction feeling that there is a rare article that only he/she owns. Therefore, if we can direct the user's possessive nature toward digital contents that he/she owns, we can also greatly reduce security incidents such as the illegal sharing of copied contents mentioned at the beginning of this chapter.

Against this background, my colleagues and I have been studying how to combine security technologies and human factors, specifically cognitive and psychological characteristics, in designing ICT systems. We call the concept "humanics information security." I do not want to confine the meaning of humanics information security, but a concrete definition of it can be "exploitation of the power of human factors to induce useful behavior of users during use of ICT systems" and/or "exploitation of the power of human factors to enhance human ability for achieving secure use of ICT systems." Giving examples from the pilot studies in which my colleagues and I have been engaged, this paper explains how the humanics information security approach can effectively achieve both security and usability of ICT systems.

The IoT (Internet of Things) has been accelerating cyber-physical fusion. In a pervasive computing/networking environment, we will freely be able to go back and forth between cyber and physical worlds anytime, anywhere. However, we must not forget that every time we get into cyber space, user authentication is required. In this sense, our life in a pervasive cyber environment means that everywhere we go, we need to perform user authentication. User authentication is a security technology that is on the front line of human-computer interactions and directly affects the quality of the user experience and relates to human factors. Therefore, this paper focuses mainly on user authentication enhanced with humanics information security.

Nowadays, unauthorized accesses are carried out by not only malicious people but also malicious automated programs as known as malware. This means that for trustworthy computing/networking platforms, distinguishing between humans and machines is as important as distinguishing between user A and user B. CAPTCHA (completely automated public Turing test to tell computers and humans apart) is essential technology for this aim and is already widely used [1]. CAPTCHA is included in the category of user authentication in the sense of function that passes only legitimate users. However, human aspects are reflected more clearly and straightforwardly on CAPTCHA, since to filter out machines, it is required to understand what humans are. This is more accurately described in Chapter 4, explaining how humanics information security enhances CAPTCHAs.

2 Image-based user authentication using cognitive aspects

2.1 Cartoon character authentication using experiential knowledge

In general, when faced with a problem he/she has solved before, a person can quickly solve the problem at first glance by using his/her experience. As an example, let us consider the "Where's Wally?" ("Where's Waldo?" in the US) series of picture books by Martin Handford [2]. In the books, each two-page spread contains a picture of a great mass of people drawn in detail. The goal is to find the character Wally in the group of people depicted. The first time the reader searches for Wally, he/she does not know where Wally is and cannot find Wally without thoroughly scanning all the people in the picture. However, once the reader finds Wally, the next time he/she can immediately identify Wally's location. Our experience says that finding Wally again becomes relatively easy even several days after we first found him.

We can utilize this cognitive ability of human beings to discern if a user is a legitimate user. During registration, a user is asked to solve a Where's-Wally?-type quiz. During authentication, a user is presented again with the same Where's-Wally?-type quiz to solve. If the user is legitimate, he/she will be able to identify immediately the Wally-type character's position in the authentication phase's quiz. Therefore, the response time (fast or slow) in solving the authentication phase's quiz identifies him/her as the registered user or an imposter.

On the basis of this idea, we implemented the cartoon-character authentication system shown in Figure 1 [3]. In Where's Wally?, the correct character is obviously Wally. However, if the correct character in our authentication scheme is known by an imposter, he/she can identify the position of the correct character during the authentication phase's quiz image. Thus, our system has a user choose his/her favorite character during registration. The user will be authenticated as legitimate on the basis of two pieces of secret information: which character is the correct one (pass-character), and where it is (pass-location).

Like Where's Wally?, the cartoon character authentication system can be implemented with a game-like entertainment. To be more exact, the registration phase quiz is a game exactly like Where's Wally? That is why, even if the user is required to change the pass-character and/or the pass-location regularly and perform a task of re-remembering, our system enables the user to enjoy a game-like task in the registration phase each time. We believe that this sort of game-like security system using cute characters is especially suitable for nurturing security consciousness in young children.

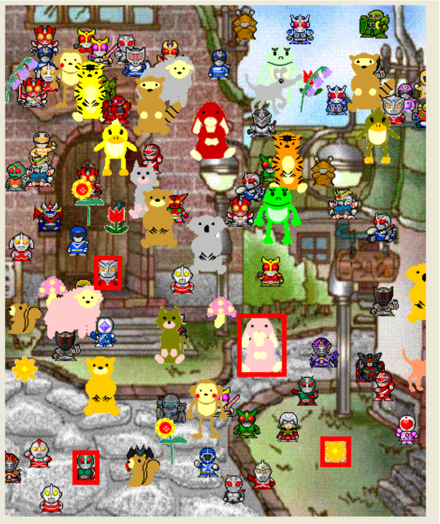


Figure 1 Example of Cartoon Character Authentication System

2.2 Blurred image authentication using one-wayness in cognition

Various types of image-based user authentication systems have been studied that use "pass-images" instead of passwords to reduce the burden of memorizing passwords. Authentication based on the recognition of pass-images [4][5][6][7][8], in which a user is asked to choose his/her pass-image among several decoy-images, is effective since people are much better at recognizing previously seen images than accurately recalling passwords. However, remembering the correct image is easy not just for the legitimate user but also for a peeper. Because the pass-image itself is displayed on the authentication screen, if an attacker peeps at the image chosen by the legitimate user during authentication, the attacker can easily remember the pass-image. In such a way, peeping attacks pose a threat to almost all image-based authentication systems.

Our strategy to make remembering the pass-image difficult for the peeper is to use images that have been obfuscated by a process similar to mosaic-blurring so that, at first glance, the image has no meaning. While humans excel at remembering images, this ability is limited to remembering meaningful images. Remembering images for which the meaning is not clear (i.e. cannot be verbalized) is considerably difficult. Therefore, the peeping attacker has difficulty remembering the blurred pass-image of another person.

However, legitimate users also have difficulty remembering meaningless images. That is why we present a meaningful original image before it is blurred to only the legitimate user during pass-image registration. The user remembers this original image along with the blurred image based on it. Because the blurred image retains features of the original image to a certain degree, the legitimate user picks out meaning from the original image in the blurred image since he/she has looked at the original image. As a result, the legitimate user can recognize the blurred image as meaningful and easily remember it as the pass-image.

This is equivalent to the legitimate user learning the schema for the blurred pass-image. In cognitive psychology, a schema is a mental structure representing how a person recognizes and remembers information [9]. We constantly and unconsciously filter information obtained from the outside world through schemas to recognize the information. Once a user learns the schema for a blurred image, from then on, he/she can easily re-recognize the meaning in the blurred image by utilizing the schema. Figure 2 shows examples of an original image and a blurred image based on it.

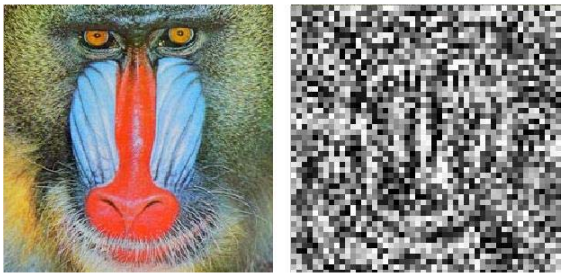


Figure 2　Original image (left) and blurred image (right) [10]

On the basis of this idea, we implemented a blurred-image authentication system [10], as shown in Figure 3. Our system maintains a higher authentication success rate with legitimate users while also having a higher resistance against peeping attacks than existing image authentication systems, which use original images only.

More specifically, our system can be enhanced by permitting users to memorize a number of pass-images and using a different pass-image at each authentication trial. By doing so, peeping attacks are expected to become much more difficult, even if the attackers are allowed to take a photo or video of the legitimate users' authentication screen several times. Here, having to memorize many pass-images increases users' memory load. A solution to reduce the burden is to extract a certain number of images from a video sequence to produce unclear pass-images from them. Only legitimate users were allowed to view the video sequence in their registration phase so that they could easily memorize the unclear pass-images [11].

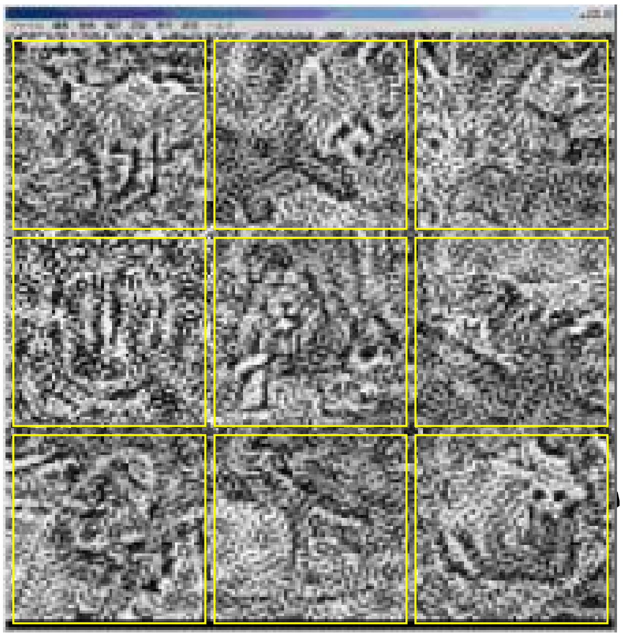


Figure 3　Example of authentication system using blurred images [11]

3 Password enhancement using gamification

Passwords should be long, complex, and random. Although we know that these long, complex, random strings are not easy to memorize for humans, the existing studies have reported that logging in with a password frequently [29] and/or training of punching password [14] could be an effective means of memorizing strong passwords. Users can learn even an unconscious knowledge through 30 to 45 minutes of SLSL (serial interception sequence learning) task, and then can use it as a password [30]. Judging from those findings, it can be expected that "repetition" is a key factor for password hardening.

Similarly, video game players often memorize commands naturally while repeatedly inputting them into games. So, what will happen if we consider the command as a password? This inspires us an idea that users will be able to naturally memorize a complex command (password) while playing a game if a game system prepares a complex command and requires users to input it again and again throughout the game. For example, let us discuss a role-playing battle game that prepares a command for using a special attack. While playing the game, each time a player encounters an enemy, he/she repeatedly inputs the command to invoke the attack. As the game progresses, the player will naturally memorize the command. The command can be used as a login password on a Web site or a master password for a password manager.

The idea of "reward" also can encourage a user to memorize much stronger passwords. For instance, in the role-playing game we described above, let us consider that the more complex the players input commands, the bigger the reward they can receive. This works as follows. A video game player (user) is allowed to register a command (password) in the game so that he/she can use a special attack by inputting the command. The power of the special attack is determined according to the complexity of the command. Let us say, if the player registers a short and easy command, the special attack is twice as powerful as an ordinary attack. If he/she registers a long and complex command, the special attack is ten times as powerful as an ordinary attack. Since players want to use the strongest attack possible, they will try to register and memorize much stronger commands (passwords).

On the basis of this idea, we implemented a simple dungeon exploration game [12]. The dungeon has some floors (1F, 2F, etc.) and a maze in each floor. Users need to explore the dungeon as deeply as possible. This game has three views: Dungeon (Figure 4), Battle (Figure 5), and Command Check (Figure 6).

In Dungeon View, the player moves by pressing the up, down, right, and left keys. Each floor has three items. If the player collects them and moves to the stairs, he/she is able to move to the next floor. While exploring the dungeon, the player encounters an enemy with a constant probability (=5.0 %), and then the game goes to Battle View immediately.

In Battle View, the player attacks the enemy by inputting as many characters of a command as possible from the beginning of the attack command. The player and the enemy have battle status: Hit Points and Attack Points. For the player, the Hit Points are always set to 30, and the Attack Points are equal to the number of characters inputted by the player. For the enemy, the Attack Points are always set to 10, and the Hit Points are equal to three times the player's current floor level (e.g., the enemy on 4F has 12 Hit Points). The player and the enemy attack each other in turn three times. If the Hit Points of the enemy go below zero, the player wins the battle. The game then goes back to Dungeon View and goes on without any penalty. On the other hand, if the Hit Points of the player go below zero, the player loses the battle result. The games goes back to Dungeon View, and the number of gained items is reset and the player is sent to the initial position on the current floor.

In Command Check View, the player can check the attack command registered on the system. If players click the button at the lower right of Dungeon View, they are able to move to Command Check View (they are unable to move from Battle View to this view).

We asked five university students to play our game in their free time for three days [13]. In this experiment, the command registered on the system was set by the experimenter (i.e., author) as a random string with 30 characters: N3mf8-%x$RQk$QeV)NMbnn*[sT(WW/. All subjects successfully memorized at least 13 random characters. Surprisingly, four of the five subjects successfully memorized all 30 random characters. The results of the questionnaire conducted after the experiment suggested that the subjects had a positive impression of our game: "I was able to memorize the command gradually and naturally; when I encountered an enemy which I didn't beat, I tried to memorize a longer command."

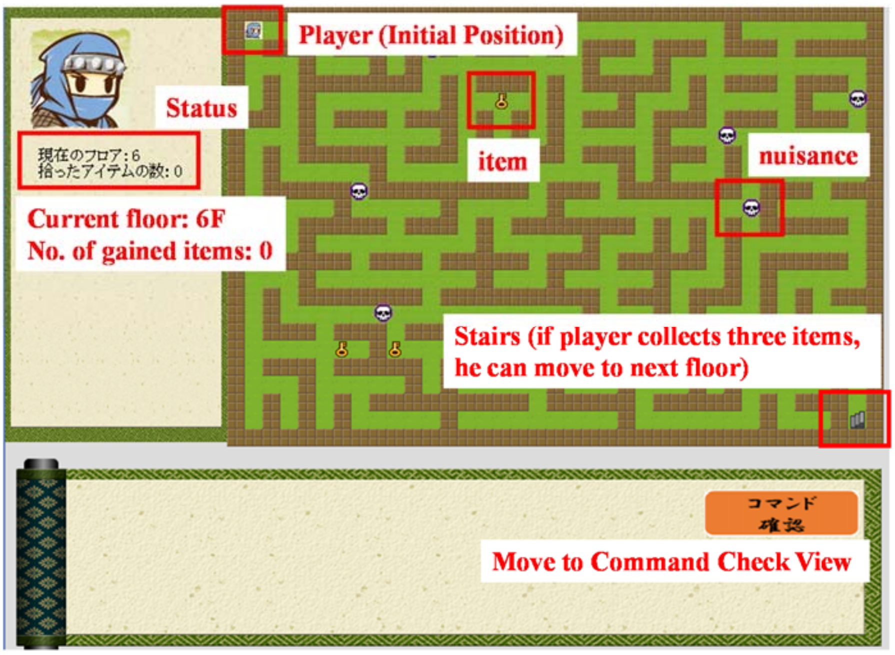
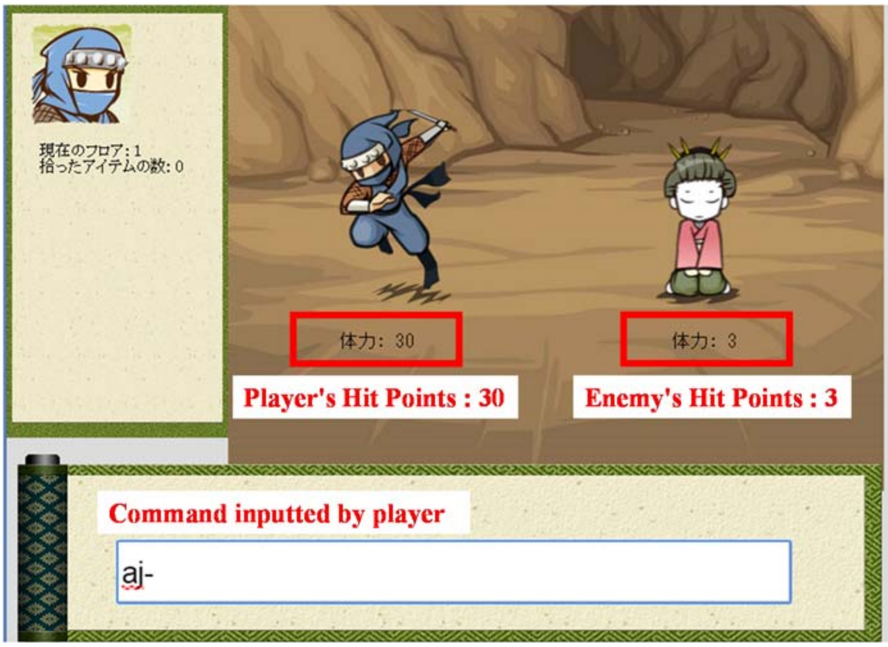
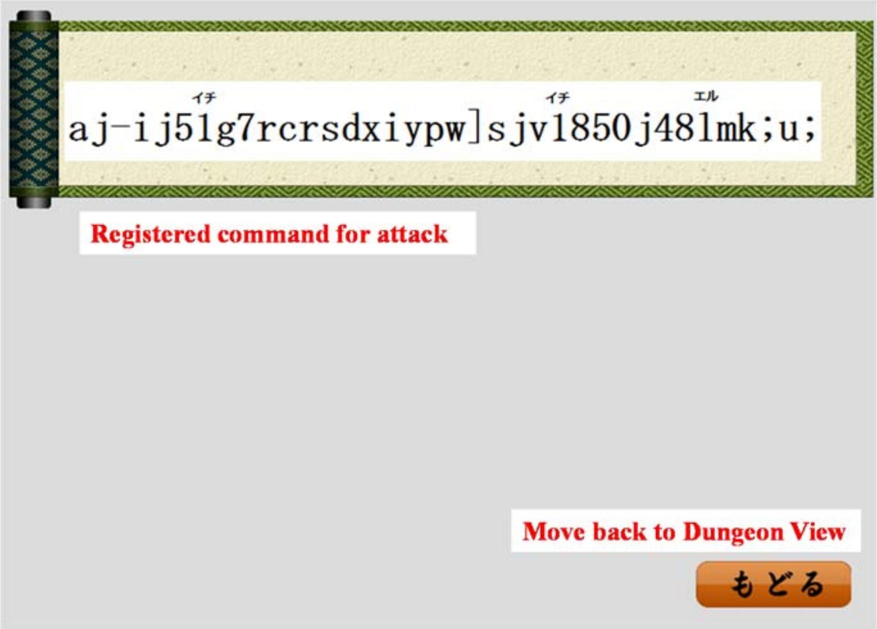

現在のフロア:6
拾ったアイテムの数: 0
Player (Initial Position)
Status
item
nuisance
Current floor: 6F
No. of gained items: 0
Stairs (if player collects three items, he can move to next floor)
コマンド
確認
Move to Command Check View

Figure 4 Dungeon View of role-playing battle game [12]



aj-

Figure 5　Battle View of role-playing battle game [12]



aj-ij51g7rcrsdxiypw]sjv1850j481mk;u;

Figure 6　Command Check View of role-playing battle game [12]

Bonneau et al. reported that a 56-bit random password is a reasonable strength for most practical scenarios [14]. All subjects memorized at least 13 random characters, which have an entropy of about 80 bits. In particular, four subjects memorized 30 random characters, which have much bigger entropy than the 56-bit random password. These results suggest that our game enables users to memorize a sufficiently strong password. It should be noted here that the passwords acquires by the battle game can be easily forgettable. A question for future study is how to retain the passwords for later use.

4 CAPTCHA using human senses

4.1 Four-panel Cartoon CAPTCHA using sense of humor

The great expansion of Web services has unfortunately given rise to malware abusing Web services and/or consuming Web resources. To cope with this, Turing tests play an important role in discriminating humans from malware, and the CAPTCHA [1] system has been widely implemented.

Most Web sites utilize text-recognition-based CAPTCHA used on Google or image-recognition-based CAPTCHAs such as Asirra [15] to stop malware from interfering with them. However, an OCR (optical character reader) and machine learning can solve these CAPTCHAs [31][16][17]. CAPTCHAs utilizing high-level human recognition abilities are needed to counter these malware [18].

While we desire to enhance CAPTCHA safety, we of course must be conscious of the trade-off between safety and usability. If a CAPTCHA system has high resistance to malware but is difficult for humans to read, then it cannot be used. Furthermore, CAPTCHA tests can be an annoyance for users who feel bothered to prove “I am a human” at every Web accesses. Therefore, CAPTCHA systems should also be designed to be user-friendly.

To overcome these above mentioned challenges all at once, we focus on human beings’ advanced cognitive ability to understand humor, or “get the joke,” and use this ability as a Turing test. As a specific example, we implemented a CAPTCHA using a four-panel cartoon [19][20] that is presented as four randomly rearranged panels, and users that can sort them into the correct order are then identified as human. Even if the panels of a four-panel cartoon are rearranged randomly, a human can understand the meaning of the pictures and utterances in each panel and thereby rearrange the panels into the correct order to create a funny story (Figure 7). For malware, however, even if image processing and natural language processing abilities are developed to the level where the computer could recognize the meaning of the pictures and utterances, it would still be difficult for the computer to rearrange the four panels into the correct order unless it also was able to understand humor. Furthermore, because reading cartoons is fun and entertaining for humans, a Four-panel Cartoon CAPTCHA will most likely be seen as an agreeable and enjoyable Turing test that does not adversely affect the convenience for users.

From the results of our user experiment, the average correct response rate for Four-panel Cartoon CAPTCHA using cartoons with a clear storyline was close to 100%. However, among the four-panel cartoons used in the experiment, there were some cartoons in which the storyline is rather garbled and/or similar panels are repeated twice or more, and thereby the subjects failed to arrange the panels correctly. We can therefore see that four-panel cartoons need to be carefully selected to improve the correct response rate for users. Four-panel Cartoon CAPTCHAs took longer to solve than conventional text-recognition-based CAPTCHAs. Reducing the response time is a future work. However, we believe that if the authentication process itself is enjoyable for the legitimate user (a human), then a slightly longer response time will be accepted.

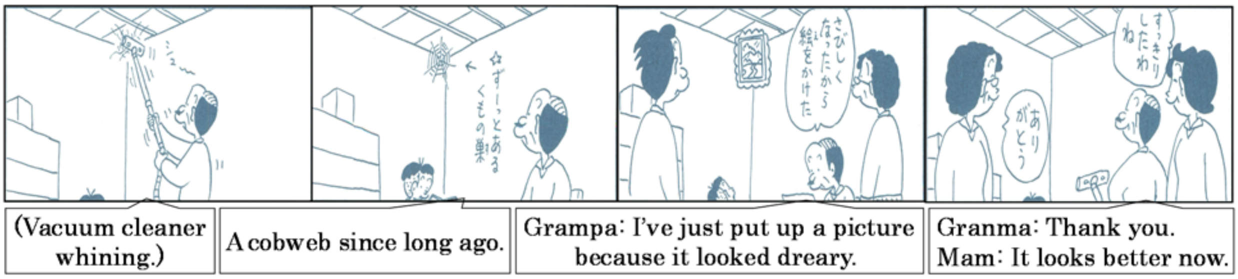

☆ずーっとあるくもの巣
さびしくなったから絵をかけた
すっきりしたわね
ありがとう
(Vacuum cleaner whining.)
A cobweb since long ago.
Grampa: I've just put up a picture because it looked dreary.
Granma: Thank you.
Mam: It looks better now.

Figure 7 Example of Four-panel Cartoon CAPTCHA
(Source: From left to right: the second panel, first panel, forth panel, and third panel of four-panel cartoon from the comic [21] p.80)

4.2 Gamified CAPTCHA using sense of entertainment

We believe that entertainment is a good driving-force for enhancing usability of security technologies, and this motivates us to explore how to leverage the entertainment value of Four-panel Cartoon CAPTCHA. Gamified CAPTCHA [22] is a derivation of Four-panel Cartoon CAPTCHA that uses videos instead of cartoons. Gamified CAPTCHA plays a video in which the scenes have been swapped around. The human will be able to pick out the swapped scenes by recognizing the inconsistency in the movie. By contrast, it will be difficult for malware to solve Gamified CAPTCHA unless the malware can recognize the inconsistency in a story with swapped scenes.

Figure 8 shows a conceptual sketch of Gamified CAPTCHA using an animated movie "Tom and Jerry." The original storyline of this movie was as follows. Scene 1: the mouse passed a bomb to the cat. Scene 2: the cat ignited the bomb. Scene 3: the bomb was exploded. In this example, a CAPTCHA test is generated by swapping the second and third scenes. With Scene 2 and Scene 3 swapped, users (humans) will be able to recognize the scenes are out of order: an explosion scene comes before igniting the bomb. The movie is played without sound in order to avoid making a jumping sound which may clue the malware into the swapped scenes.

We implemented a Gamified CAPTCHA system and conducted basic user experiment. Interestingly, many subjects reported that finding swapped scenes was felt like solving video-based quizzes. Basically, failure to answer a CAPTCHA test correctly is directly linked to a decrease in usability, resulting in frustration for many users. For Gamified CAPTCHA, on the other hand, even if the user cannot correctly answer, the user would be expected to feel encouraged to repeat the test due to the fun nature of the quiz. Subjects often said “Please let me try one more time!” when they tried the quiz, and these words are more likely to be uttered when they failed to answer correctly. It was confirmed through this user experiment that subjects did not tend to mind redoing the Gamified CAPTCHA.

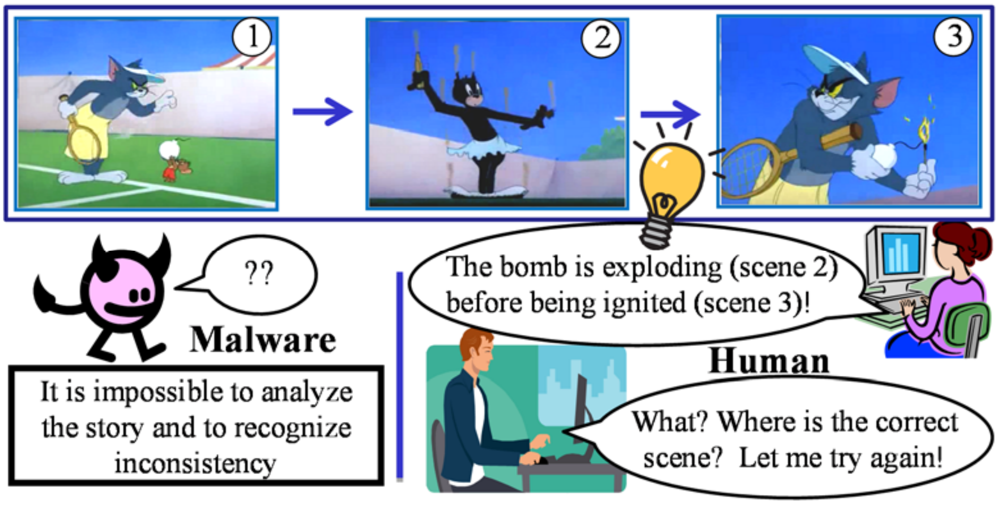

①
②
③
??
Malware
It is impossible to analyze the story and to recognize inconsistency
The bomb is exploding (scene 2) before being ignited (scene 3)!
Human
What? Where is the correct scene? Let me try again!

Figure 8 Conceptual sketch of Gamified CAPTCHA [22]
(Source: “Tennis Chumps” from Tom and Jerry DVD [23])

4.3 Chimera CAPTCHA using sense of strangeness

Humans gain common sense through their daily life. We feel “something is wrong” when in a situation that contradicts common sense. So far computers with common sense have not been realized. Thus, feeling that something is wrong must be a high-level human recognition ability that state-of-the-art malware cannot imitate. CAPTCHA systems can identify whether a user is human or malware by asking the user to discriminate “objects that accord with common sense” from “objects that do not accord with common sense”.

However, it has been difficult to give clear definitions of “objects that accord with common sense” and “objects that do not accord with common sense.” To solve this problem, we use 3D (three-dimensional) models. Most 3D models are generated by modeling objects from the real world. Therefore, 3D models function essentially identically to common sense, and 3D models can be used as objects that accord with common sense.

One possible way to generate unusual objects that do not accord with common sense is deformation of 3D models. Although there are various ways of deforming 3D models, we use “merging.” Specifically, the objects that humans feel are strange (described as “chimera objects”) are generated by merging two 3D models. For example, when a dog merges with a chair, a chimera object is generated as seen in Figure 9.

On the basis of this idea, we implemented “Chimera CAPTCHA” [24], in which the user is presented with a question image consisting of a chimera 3D object and some ordinary 3D objects. Chimera CAPTCHA requests users to click the chimera object in the question image. Humans can click it easily, because chimera objects, which differ in appearance from ones that accord with common sense, cause a feeling of strangeness. An example image of a Chimera CAPTCHA that shows one chimera among seven objects is shown in Figure 10. In the lower right of Figure 10, there is a chimera object: a dog and an ambulance are merged.

As already mentioned, to counter sophisticated malware, CAPTCHAs are needed that exploit a high-level human recognition ability. However, this is not a straightforward process. This is because CAPTCHAs inherently contain a contradiction: Web servers (computers) should be able to automatically generate the CAPTCHA questions that malware (computers) cannot understand. Four-panel Cartoon CAPTCHA is one of the typical examples: what Web servers can do is just a permutation of panels; Web servers cannot create four-panel cartoons themselves even if there are plenty number of 3D models. On the other hand, Chimera CAPTCHA makes it possible to generate chimera objects easily: what Web servers do is just to project the two 3D models, A and B, onto a point in the two-dimensional plane; then, the models merge, and humans can recognize them as a chimera object.

A typical attack against Chimera CAPTCHA is malware extracting all objects from a question image and finding the chimera object. Namely, malware may try to find a merged object in an image. However, Chimera CAPTCHA has tolerance against this attack for two reasons. First, a question image will include occluded objects. For example, in the upper left of Figure 10, a cat is occluded by a chair. Humans have spatial reasoning ability, which enables us to distinguish between merged objects and occluded objects. In contrast, computers do not so far have an adequate level of this ability, and therefore malware cannot distinguish between them. Second, the real world contains many merged objects. For example, in the lower left of Figure 10, the ornamental plant consists of leaves and a pot. These objects are “usual” merged objects, in contrast with “unusual” merged objects (chimera objects) that our system generates. Even if the image analysis technologies are advanced and the computers can recognize whether an object is a merged object or not, it is still possible to assume that malware cannot recognize whether the merged object is a usual or unusual merged object.

We carried out basic experiment in which seven human subjects solved the challenges of Chimera CAPTCHA. The results showed that the correct response rate is 90.5 % and the average response time per challenge is 5.7 seconds. The usability is satisfactory.

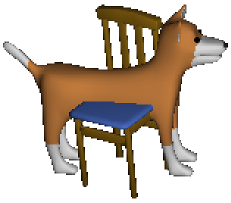


Figure 9 Chimera object merged from dog and chair [24]

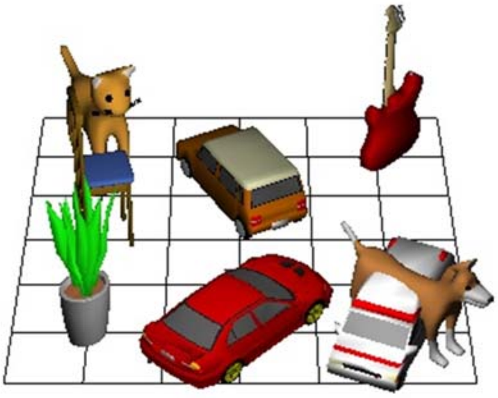


Figure 10 Example of Chimera CAPTCHA [24]

5 Conclusion

In this paper, I described the pilot studies of "humanics information security" in which my colleagues and I have been engaged so far. Humanics information security seeks "positive-sum" combinations to ensure both security and usability by creating security technologies that utilize the power of humans' cognitive and psychological characteristics to induce security-conscious behavior of users during use of ICT systems and/or to design secure and enjoyable schemes for users of ICT systems. User authentication and CAPTCHA tests are security technologies that are on the front line of human-computer interactions and directly affect human beings. This is why our studies focused mainly on user authentication and CAPTCHA enhanced with humanics information security. For image-based user authentication, using cognitive aspects such as experiential knowledge and schema can make the user authentication fun and tolerant. For password authentication, using entertainment factors can enhance a user's ability to memorize a stronger password. For CAPTCHA, using human senses such as our senses of humor and strangeness can improve both the security and the usability.

Acknowledgments

I would like to express my gratitude to all the coauthors I have worked with so far. I sincerely thank Prof. Takeo Isarida of Shizuoka Sangyo University for his valuable advice regarding psychology. I would like to thank the authors of the free 3D models [25][26] and 2D material images used in our systems. These studies were partially supported by JSPS KAKENHI Grant Number JP21300021, JP21650015, JP25280046. I would like to extend my appreciation to Prof. Marek R. Ogiela for offering me this opportunity for contribution.

References

[27] Marek Romuald Ogiela, Urszula Ogiela: Linguistic Approach to Cryptographic Data Sharing, Proceedings of 2008 International Conference on Future Generation Communication and Networking, vol.1, pp.377-380, 2008 (DOI: 10.1109/FGCN.2008.89).

[28] Lidia Ogiela, Marek Romuald Ogiela: Beginnings of Cognitive Science, Chapter 1 in Advances in Cognitive Information Systems, vol.17 of Cognitive Systems Monographs, pp.1-18, 2012.

[1] The Official CAPTCHA Site, http://www.captcha.net

[2] Martin Handford: Where's Wally?, Walker Books (London), 1987.

[3] Masaomi Hanai, Itsukazu Nakamura, Hideki Yoshida, Masakazu Soga, Masakatsu Nishigaki: A user authentication system based on prior experience of the authentication task, IPSJ Special Interest Group Technical Report, 2004-CSEC-24-34, pp.193-198, 2004. (in Japanese)

[4] Rachna Dhamija, Adrian Perrig: Deja Vu: A User Study Using Images for Authentication, 9th USENIX Security Symposium, pp.45-58, 2000.

[5] Trevor Pering, Murali Sundar, John Light, and Roy Want: Photographic Authentication through Untrusted Terminals, IEEE Pervasive Computing, vol.2. no.1, pp.30-36, 2003.

[6] Tetsuji Takada, Hideki Koike: Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images, LNCS 2795, Proceedings of 2003 International Symposium on Human-Computer Interaction with Mobile Devices and Services (Springer LNCS 2795), pp.347-351, 2003.

[7] Real User Corporation.: PassFaces, http://www.realuser.com

[8] Mnemonic Security, Inc.: Personal Verification Software Mnemonic Guard, http://www.mneme.co.jp/english/index.html

[9] W. F. Brewer.: Schemata., In R. A. Wilson & F. C.Keil (Eds.), MIT Encyclopedia of the Cognitive Sciences, , The MIT Press (Cambridge), pp.729-730, 1999.

[10] Atsushi Harada, Takeo Isarida, Tadanori Mizuno, Masakatsu Nishigaki: A User Authentication System Using Schema of Visual Memory, Proceedings of 2006 International Workshop on Biologically Inspired Approaches to Advanced Information Technology (Springer LNCS 3853), pp.338-345, Springer, 2006.

[11] Takumi Yamamoto, Atsushi Harada, Takeo Isarida, Masakatsu Nishigaki: Improvement of User Authentication Using Schema of Visual Memory: Exploitation of "Schema of Story", Proceedings of 2008 IEEE International Conference on Advanced Information Networking and Applications, pp.40-47, 2008.

[12] Masahiro Fujita, Mako Yamada, Shiori Arimura, Yuki Ikeya, Masakatsu Nishigaki: An Attempt to Memorize Strong Passwords while Playing Games, Proceedings of 2015 International Conference on Network-Based Information Systems, pp.264-268, 2015.

[13] Masahiro Fujita, Mako Yamada, Masakatsu Nishigaki: Implementation and Initial Evaluation of Game in Which Password Enhancement Factor is Embedded, Proceedings of 2016 International Conference on Human-Computer Interaction (Springer LNCS 617), pp.476-481, 2016.

[14] Josep Bonneau, Stuart Schecheter: Towards reliable storage of 56-bit secrets in human memory, 23rd USENIX Security Symposium, pp.607-623, 2014.

[15] Microsoft Research: ASIRRA, http://research.microsoft.com/en-us/um/redmond/projects/asirra/

[16] Jeff Yan, Ahmad Salah El Ahmad: Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms, Proceedings of 2007 Computer Security Applications Conference, pp.279-291, 2007.

[17] Philippe Golle: Machine Learning Attacks Against the ASIRRA CAPTCHA, Proceedings of 2008 ACM CSS, pp.535-542, 2008.

[18] Takumi Yamamoto, Doug Tygar, Masakatsu Nishigaki: CAPTCHA Using Strangeness in Machine Translation, Proceedings of 2010 IEEE International Conference on Advanced Information Networking and Applications, pp.430-437, 2010.

[19] Takumi Yamamoto, Tokuichiro Suzuki, Masakatsu Nishigaki: A Proposal of Four-panel cartoon CAPTCHA: The Concept, Proceedings of 2010 International Workshop on Trustworthy Computing, pp.575-577, 2010.

[20] Takumi Yamamoto, Tokuichiro Suzuki, Masakatsu Nishigaki: A Proposal of Four-panel cartoon CAPTCHA, Proceedings of 2011 IEEE International Conference on Advanced Information Networking and Applications, pp.159-166, 2011.

[21] Masashi Ueda: Shin Kobo-chan, vol.7, Houbunsha (Tokyo), 2006 (in Japanese)

[22] Junya Kani, Masakatsu Nishigaki: Gamified CAPTCHA, Proceedings of 2013 International Conference on Human-Computer Interaction (Springer LNCS 8030), pp.39-48, 2013.

[23] Tom and Jerry DVD, vol.7, Warnerbros. Entertainment Inc. (Burbank).

[24] Masahiro Fujita, Yuki Ikeya, Junya Kani, Masakatsu Nishigaki: Chimera CAPTCHA: A Proposal of CAPTCHA Using Strangeness in Merged Objects, Proceedings of 2015 International Conference on Human-Computer Interaction (Springer LNCS 8533), pp.48-58, 2016.

[25] Metaseko-Sozai, http://sakura.hippy.jp/meta/

[26] TurboSquid, http://www.turbosquid.com/

[29] Rick Wash, Emilee Rader, Ruthie Berman, Zac Wellmer: Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites, 12th Symposium on Usable Privacy and Security, pp.175-188, 2016.

[30] Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, Patrick Lincoln: Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks, 21st USENIX Security Symposium, pp.129-141, 2012.

[31] Elie Bursztein, Matthieu Martin, John Clifford Mitchell: Text-based CAPTCHA Strengths and Weaknesses, ACM Computer and Communication security 2011, pp.125-138, 2011.