Do Authentication Websites Adopt Friendly Password Registration Error Message Design?

Masahiro Fujita
Mitsubishi Electric Corporation

Tadakazu Yamanaka
Mitsubishi Electric Corporation

Nori Matsuda
Mitsubishi Electric Corporation

Ayako Yoshimura
Mitsubishi Electric Corporation

Akira Kanaoka
Toho University

Abstract

Many user experience (UX) guidelines provide design rules for friendly error message design. User authentication systems display a password registration error message (PREM) when a user inputs a password that breaches the password composition policy. From this, a research question arises: "Do authentication websites adopt friendly error message design based on the design rules?" In response, we defined two friendly PREM design requirements with reference to the guidelines. Consequent to a fact-finding survey involving 231 websites, we confirmed that only approximately 35% of websites satisfy the friendly design requirements, i.e., most authentication websites do not follow the design rules in the guidelines. Based on the result, we provide a new research direction in the field of password registration error messaging.

1 Introduction

Improving user experience (UX) [1] is an essential consideration for systems design that also holds for security systems [11]. Many guidelines (e.g., [2, 5, 7, 8]) have been published to improve the UX and provide system developers with rules for friendly design. These give rise to a research question: "Does the design of security systems follow the rules in the guidelines"? Unfortunately, to our knowledge, no study has yet answered this question clearly, i.e., no study has surveyed whether the design of security systems follows the guidelines.

As the first step in answering the question, we focus on the design of password registration error messages. Most authentication systems adopt a password composition policy, such as "at least 12 alphanumeric characters", to eliminate weak passwords. When a user inputs an invalid password that breaches the password registration form's policy, an error message is displayed, such as "Please input at least 12 characters." We term this the "password registration error message (PREM)" and survey the design of such messages. Based on the result of the survey, we answer the following research question: "**Do authentication websites adopt friendly PREM designs based on the design rules?**" We also provide a new research direction in the field of PREM design based on the result.

2 Methodology

The PREM design was surveyed by following these three steps: (1) Definition of design requirements, (2) Collection of authentication websites, and (3) Checking websites.

2.1 Definition of design requirements

We extracted the design rules that are strongly related to PREM design from the guidelines, and then defined two friendly PREM design requirements based on the rules. This step was conducted based on discussions with some of the experts on usable security.

Following this step, we defined the following two requirements.

Requirement 1 (Friendly-timing)**.** The guidelines [5, 8] recommend that an error message should be displayed automatically after the user inputs a password and be placed closer to the area with which it is associated. It is difficult to check if a message is "placed closer to an area form". This is because "closer" depends on the user environment, such as the

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

[1] User's perceptions and responses that result from the use and/or anticipated use of a system, product, or service [1]

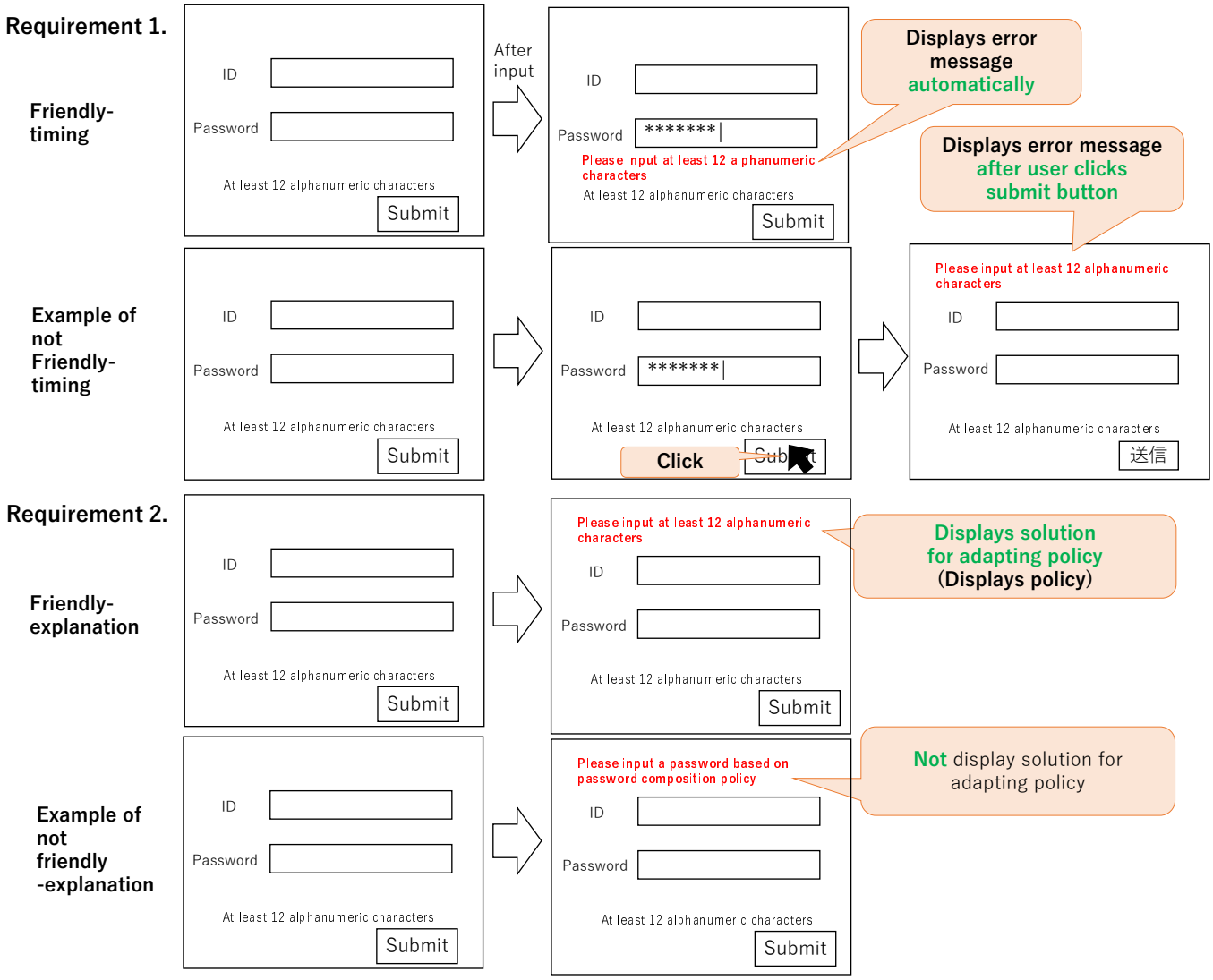

Figure 1: Examples of websites that satisfy the friendly-timing and friendly-explanation requirements.

display size or browser screen size. Therefore, we focused only on "displayed automatically." From the aforementioned analysis, we defined the first requirement:

A PREM should be displayed automatically after a user has input an invalid password.

Requirement 2 (Friendly-explanation)**.** The guidelines [2, 8] recommend that an error message should have a solution to escape the erroneous situation. To exit a password registration error dialog, the user should input a valid password that follows the password composition policy. Therefore, we defined the message that enables the user to exit the situation as equal to a message containing the password composition policy. From the aforementioned analysis, we defined the second requirement:

A PREM should contain the password composition policy.

Figure 1 shows examples of websites that satisfy the friendly-timing and friendly-explanation requirements.

2.2 Obtaining authentication websites

We used a crowdsourcing service to obtain the URLs of authentication websites, being those that contain an authentication page. They were obtained as follows.

- We used a Japanese crowdsourcing service, Lancers [6].
- We conducted the task on November 9th, 2019.
- We requested each worker to report up to five URLs of authentication websites.
- We paid each worker 100 Japanese yen per valid URL.

Table 1: Result of survey

	Friendly-timing	Not friendly-timing	Total
Friendly-explanation	80	54	134
Not friendly-explanation	33	64	97
Total	113	118	231

Table 2: Types of websites not satisfying requirement 2

Type	Total
No policy	33
Unreachable	34
Check mistake	17
Message inconsistency	10
No error message	3

2.3 Checking websites

One of the authors of this paper checked each authentication website. The checking procedure for an authentication website was as follows:

1. Access the user registration page on the authentication website.
2. Read the password composition policy on the page.
3. Input to the password input form an invalid password that breaches the policy.
    - For example, if "only alphanumeric characters can be used" is the policy, "p@ssword" can be input as the invalid password.
4. If a PREM is displayed after the input, record the message and terminate the procedure.
5. Click the submit button to move to the next page. Note that all other forms except the password input form are empty.
6. Record the PREM displayed on the next page.

If the procedure is terminated in 4, we judged that the authentication webpage satisfied requirement 1 (friendly-timing). If the recorded message contains the password composition policy, we judged that the authentication webpage satisfied requirement 2 (friendly-explanation).

3 Result

We collected 231 websites with password composition policies and checked them all. Table 1 summarizes the result of the survey.

The websites that failed to satisfy requirement 2 (friendly-explanation) can be classified into the following five types (Table 2).

No policy
A PREM was displayed, but the message did not contain the password composition policy.

Unreachable
An error that referenced the uncompleted form(s) was displayed e.g., "please fill out all forms" or "please fill out ID form". This had a higher priority than the PREM. Therefore, the password error message was not displayed. Note that all other forms except the password input form were empty.

Check mistake
An invalid password was input into the form yet was judged as valid. Therefore, the PREM was not displayed. For example, the password composition policy was "only alphanumeric characters can be used", but "p@ssword" was accepted.

Message inconsistency
The password error message containing the password composition policy was displayed but differed from the one on the registration page. For example, "only alphanumeric characters can be used" was used as the password composition policy, and "p@ssword" was input into the form. The password error message was displayed, but read "please input valid password composed of alphanumeric characters **and symbols(_,)**."

No error message
The user registration was faulty, but no error message was displayed.

4 Discussion

4.1 Answer to research question

The survey found that only approximately 35% of websites satisfy the friendly design requirements. Therefore, we obtained the following answer to the research question: **Most (approximately 65%) of the authentication websites did not adopt the friendly PREM design.**

The websites gave users extra time to complete the registration form. If a website did not satisfy requirement 1, an extra user operation was required, e.g., "click the submit button ", to call the PREM on the website." If a website did not satisfy requirement 2, an extra user operation was also required, e.g. "look for the password composition policy on the page, to recheck the policy." We recommend that websites should be corrected to satisfy requirements 1 and/or 2 to reduce the extra time required.

To correct them, we should solve a new research question: **"Why do developers of authentication systems not follow the rules in the UX guidelines?"**.

The investigation of the new question is a future undertaking, but is expected to involve the following factors. Regarding requirement 1, the password validation check may be implemented on the authentication server, not in the web browser [10]. In this implementation, the server acquires the password from the web browser, validates whether the password follows the password composition policy, and sends the validation result to the web browser. Clicking the submit button may trigger the password to be sent from the web browser to the server. Regarding requirement 2, the check mistake or message inconsistency are the implementation mistakes by the developers. This suggests that more support, such as more specific test tools for the developers, is needed to prevent implementation mistakes.

4.2 Limitation

The authentication websites were collected by a Japanese crowdsourcing service. Almost all websites (228/231) are Japanese websites. Surveys involving English or other language websites might result in different outcomes.

This paper is the first work on the security design survey of PREMs. We focused only on two design rules that are regarded as primitive and basic. We found that most authentication systems do not even follow the primitive and basic rules. An additional survey focusing on the other rules is an essential future work, which raises the possibility of gaining more interesting findings.

4.3 Ethics

We carefully considered privacy concerns in the survey. We requested workers to input the URL only. Most URLs do not contain information to identify individuals, but several URLs contain a personal identifier, such as "https://localhost/login/**smith**". Therefore, we advised the workers to avoid inputting URLs that contained personal identifiers. Consequently, the workers could not be identified from their answers. In addition to this instruction, before checking websites, we reviewed whether each answer did not contain a personal identifier. In this survey, no URL contained such identifiers.

5 Related Works

Shay et al. examined how password-registration error feedback affects password security and usability [9]. Their feedback implementation is similar to that for friendly-timing. However, they did not survey the number of websites that implement this feedback and did not discuss the relationship between the feedback and the design rules in the UX guidelines.

Bonneau and Preibusch pointed out that attackers can identify a target's account by using the insecure login-related message that is displayed on the login page [3]. Hasegawa et al. evaluated the user impact of the attack through a user study [4]. These works are related to error messages but focus on the threats posed by login error messages, not on the UX being decreased by the PREMs. Additionally, they also did not mention the design rules.

In the field of Human Computer Interaction (HCI), extra time given by an unfriendly interface is called "penalty time" [12]. A web page that does not satisfy requirements 1 and/or 2 gives the penalty time to users.

6 Conclusions

In this work, we defined two friendly PREM design requirements, friendly-timing and friendly-explanation based on the design rules in the UX guidelines. Consequent to a fact-finding survey involving 231 websites, we confirmed that only approximately 35% of websites satisfy the friendly-design requirements; most authentication websites do not follow the design rules in the guidelines. Based on the result, we offer the following new research question: "Why do developers of authentication systems not follow the rules in the UX guidelines?"

References

[1] *ISO 9241-11:2018: Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. International Organization for Standardization, 2018.

[2] Nick Babich. How to Write and Design User-Friendly Error Messages. https://xd.adobe.com/ideas/process/information-architecture/error-message-design-ux/, 2020.

[3] Joseph Bonneau and Sören Preibusch. The Password Thicket: technical and market failures in human authentication on the web. 01 2013.

[4] Ayako Akiyama Hasegawa, Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, and Tatsuya Mori. Addressing the Privacy Threat to Identify Existence of a Target's Account on Sensitive Services.

[5] Rachel Krause. How to Report Errors in Forms: 10 Design Guidelines. https://www.nngroup.com/articles/errors-forms-design-guidelines/, 2019.

[6] Lancers. Lancers. http://lancers.jp/.

[7] Michael J. Metts and Andy Welfle. *Writing Is Designing: Words and the User Experience*. Rosenfeld Media, 2020.

[8] Saadia Minhas. How to Write Good Error Messages. https://uxplanet.org/how-to-write-good-error-messages-858e4551cd4, 2018.

[9] Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, and Blase Ur. A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2903–2912, 2015.

[10] Taku Sugai, Toshihiro Ohigashi, Yoshio Kakizaki, and Akira Kanaoka. Password strength measurement without password disclosure. In *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)*, pages 157–164, 2019.

[11] Ranjeet Tay. Designing Effective Security UX: If It's Not Usable, It's Not Secure. In *RSA Conferenece*, 2019.

[12] Shota Yamanaka, Keisuke Yokota, and Takanori Komatsu. Time-penalty impact on effective index of difficulty and throughputs in pointing tasks. In *Human-Computer Interaction – INTERACT 2021*, pages 100–121, 2021.