Journal of Information Processing Vol.28 1030–1046 (Dec. 2020)

[DOI: 10.2197/ipsjjip.28.1030]

Regular Paper

Addressing the Privacy Threat to Identify Existence of a Target's Account on Sensitive Services

Ayako Akiyama Hasegawa[1,a)] Takuya Watanabe[1,b)] Eitaro Shioji[1,c)] Mitsuaki Akiyama[1,d)]
Tatsuya Mori[2,3,4,e)]

Received: March 10, 2020, Accepted: June 1, 2020

Abstract: Online service providers exert tremendous effort to protect users' accounts against sensitive data breaches. Although threats from complete outsiders, such as account hijacking for monetization, still occur, recent studies have shed light on threats to privacy from insiders. In this study, we focus on these latter threats. Specifically, we present the first comprehensive study of an attack from insiders that identifies the existence of a target's account by using the target's email address and the insecure login-related messages that are displayed. Such a threat may violate intimates' or acquaintances' privacy because the kinds of service accounts a user has implies his/her personal preferences or situation. We conducted surveys regarding user expectations and behaviors on online services and an extensive measurement study of login-related messages on online services that are considered sensitive. We found that over 80% of participants answered that they have sensitive services and that almost all services were vulnerable to our attack. Moreover, about half the participants who have sensitive services were insecurely registered on them, thus could be potential victims. Finally, we recommend ways for online service providers to improve login-related messages and for users to take appropriate defensive actions. We also report our responsible disclosure process.

Keywords: usable security, account security, privacy, insider attack, login

1. Introduction

With the systematization of cyber-crime ecosystem, serious data breaches have been dramatically increasing [2], [3], [4], [5]. The spread of such incidents has turned people's attention to the importance of privacy-protection mechanisms. In fact, legal regulation on privacy protection such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), have become enforceable. This social and legal background makes account security to protect user accounts against sensitive data breaches a major mission for online service providers. To protect user accounts, they exert tremendous effort in adopting techniques to secure account authentication, such as password-composition policy, password-strength metering, rate-limiting (i.e., lockout, blocking, and CAPTCHA), multi-factor authentication, and two-step verification [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17].

An attack to determine the existence of a user's account on a target website generates a list of registered user IDs for a password-guessing attack [18]. When an attacker inputs a target's email address as a user ID in a login screen, he/she can identify the existence of a target's account if explicit messages are displayed. For example, "Incorrect password" tells users that the input email address is valid while the input password is not. In this study, we advocate that the fundamental cause of the defects of login-related functions is not explicit messages but the *inconsistency* of displayed messages for registered/unregistered user IDs. In our preliminary investigation on actual services, we distinguished the potentially insecure login-related messages in *login*, *password recovery*, and *account creation* functions, that displayed inconsistent messages for registered/unregistered user IDs. If any one of these three types of functions on a service displays inconsistent messages, the service is considered insecure. By leveraging the defects of these functions, a potential attacker is able to deterministically distinguish whether the target has an account on the service.

In the typical threat model, an attacker is an outsider who performs a password-guessing attack in a brute-force manner to compromise a large number of accounts. Although threats from outsiders still continue, recent studies have shed light on privacy abuse by insiders, i.e., partners, family, friends, co-workers, and acquaintances [19], [20], [21], [22], [23], [24], [25], [26], [27], [28]. On the basis of the changes in the profiles of attackers, we discuss the following privacy issue on online services. The kinds of service accounts a user has implies his/her personal preferences or situation. For instance, an attacker can infer a target's sexual orientation when the target has an account on a dating

[1] NTT Secure Platform Laboratories, Musashino, Tokyo 180–8585, Japan
[2] Waseda University, Shinjuku, Tokyo 169–8555, Japan
[3] NICT, Koganei, Tokyo 184–0015, Japan
[4] RIKEN AIP, Chuo, Tokyo 103–0027, Japan
[a)] ayako.hasegawa.vg@hco.ntt.co.jp
[b)] takuya.watanabe.yf@hco.ntt.co.jp
[c)] eitaro.shioji.es@hco.ntt.co.jp
[d)] akiyama@ieee.org
[e)] mori@nsl.cs.waseda.ac.jp

This paper is the extended version of the paper presented at ACSAC'19 [1].

service for sexual minorities. Insiders who are not technically skilled attackers can also easily take advantage of the defects of login-related messages since high-level technical skills such as statistics and programming are not needed. Service providers must prevent leakage of information such as *who* has an account on *what* service. The above mentioned security techniques (e.g., CAPTCHA) can protect login-related functions against an outsider attack in a brute-force manner, but the intrinsic problem of login-related functions has not yet been solved. Furthermore, these security techniques are not effective against an insider attack involving a small number of attempts, e.g., targeting a specific user.

From combining the new threat model and the defects of login-related messages, we present the first comprehensive study of an attack identifying intimates' or acquaintances' account existence (called the account-existence attack). Given the above emerging privacy threats and our presented practical attack, we ask three research questions (RQs):

RQ1: What services do users consider sensitive?

RQ2: Are such sensitive services secure against our attack to identify the existence of a target's account?

RQ3: How much does our account-existence attack actually impact user privacy?

Answering these RQs can help service providers understand the impact of our account-existence attack, make services secure, and provide insights into practical countermeasures. We addressed these RQs through surveys regarding user expectations and behaviors on online services and a measurement study on the login-related messages of online services that are considered sensitive. To answer RQ1, we conducted a survey on Amazon Mechanical Turk (MTurk) [29] and found that 81.6% (501/614) of participants answered that there were *sensitive* services that they would not want others to know they used. To answer RQ2, we conducted a measurement study on 87 services including popular and sensitive services given in the user study regarding RQ1. We systematically examined three types of login-related functions on both websites and mobile apps corresponding to a specific service through the different stages in the account lifecycle. We collected over 1.1k login-related messages. Surprisingly, we found that 98.9% (86/87) of services were vulnerable to our account-existence attack. In most cases, an account-creation function displays inconsistent messages. We also found that changing an email address effectively defends against our attack. To answer RQ3, we conducted another survey on MTurk ($N = 447$) to explore user expectations and user privacy-protecting behaviors on sensitive services. We found that 45.2% (166/367) of participants who have sensitive services behaved insecurely (i.e., registering an email address known to others on sensitive services), thus could be potential victims.

We make the following contributions in this study:

- We present the first comprehensive study of an attack from insiders that identifies the existence of their intimates' or acquaintances' accounts. The attack requires only a small number of attempts, making it easy to accomplish the aim manually.
- We conduct a comprehensive measurement study on online services and reveal that almost all online services, regardless of whether they are sensitive, are vulnerable to our account-existence attack.
- We quantify the impact of our account-existence attack on the basis of user expectations and privacy-protecting behaviors on sensitive services. We reveal i) the representative reasons for the participants not wanting others to know they use sensitive services, ii) that 25.3% of participants expressed the motivations of potential perpetrators, and iii) that 45.2% of participants who have sensitive services could be potential victims.
- We give practical recommendations for service providers and users. Providers of services considered sensitive should change inconsistent login-related messages to consistent ones to make their services secure. Users should register or change to an email address not known to others. We improve de facto standardized web security guidelines and notify providers of sensitive services for responsible disclosure.

The rest of this paper is organized as follows. We explain our threat model and show the attack flow in Section 2. In Section 3, we explain our exploratory user study to investigate sensitive services. We discuss measuring the success rate of our attack on actual services in Section 4. In Section 5, we explain our main user study to measure the percentages of potential victims and perpetrators. We make recommendations for providers and users and discuss the limitations and ethics of our study in Section 6. In Section 7, we discuss related work. Finally, we conclude our study in Section 8.

2. Threat Model

2.1 Overview

The threat model we discuss in this study differs from the typical one (i.e., compromising of accounts) in terms of *class of attacker*, *goal of attack*, and *manner of attack*.

Class of attacker: In the typical threat model, an attack is performed by outsiders, who are strangers of a target. However, we discuss an attack performed by insiders, who are intimates or acquaintances of a target such as partners, family, friends, and coworkers. We assume that insiders know a target's email address or phone number.

Goal of attack: Outsiders aim at mass compromising of accounts for monetization. On the other hand, insiders, who are covered by our threat model, aim to snoop on the target's privacy. The goal in our threat model is identifying the existence of a target's account on a specific sensitive service rather than compromising it. What kinds of service accounts a target has implies his/her personal preferences or situation. Thus, an attacker can infer a preference or situation that a target may keep secret deliberately on the basis of the target having an account on a specific sensitive service. We investigate why users would be uncomfortable with their account's existence being known to others in Section 5.

Manner of attack: The manner of attack by outsiders is first to acquire a bulk email address list exposed by data breaches and conduct login attempts in a brute-force manner, e.g., dictionary attacks and password reuse attacks. On the other hand, the manner of attack by insiders is extremely simple. In our threat

model, an attacker checks only whether a target's email address or phone number is registered on a specific sensitive service as a user ID. Specifically, an attacker leverages *messages* displayed on the screens of login-related functions, which are introduced in Section 2.2. If a service displays inconsistent messages for registered/unregistered user IDs, an attacker can identify whether a target's email address or phone number is registered as a user ID by comparing the messages. This attack requires only a small number of attempts, which is easy to perform manually. Thus, existing countermeasures such as CAPTCHA, which aim to prevent an outsider attack, are ineffective against this manual attack.

2.2 Defects of Login-Related Messages

In our threat model, an attacker abuses defects of login-related messages to identify a target's account existence. The fundamental cause of the defects is not explicit messages but the inconsistency of displayed messages for registered/unregistered user IDs. Even if displayed messages do not directly indicate a reason for an error, an attacker can identify an account's existence on the basis of inconsistency. In our preliminary investigation on actual services, we discovered potentially insecure login-related messages in *login*, *password recovery*, and *account creation* functions, which displayed inconsistent messages for registered/unregistered user IDs. Next, we explain defects in each login-related function.

2.2.1 Login

A standard login screen requires a user ID (email address, username, or phone number) and password combination. The login screen has two types of login-error states other than input format error: L–R a registered user ID and incorrect password were received, and L–UR an unregistered user ID was received (**Table 1**). If the messages in L–R and L–UR are inconsistent, an attacker can recognize the error states and consequently identify the existence of a target's account. For instance, if a login screen outputs "Incorrect password" as an error message in L–R and "That user ID doesn't exist" as an error message in L–UR, the former error message enables an attacker to identify a registered user ID. Such a service is vulnerable to our account-existence attack. A login screen that outputs a *consistent* message, such as "Incorrect user ID or password" (Table 1 L–SM) in L–R and L–UR, is secure against our attack because an attacker cannot recognize the internal states or account existence.

2.2.2 Password Recovery

Online services provide a password-recovery function for users who have forgotten their passwords. A password-recovery screen has an input form for an email address. This screen also has two types of normal/error states: PR–R a registered email address was received, and PR–UR an unregistered email address was received (Table 1). For instance, if a password-recovery screen outputs "We just sent you a password-reset link" as a message in PR–R and "This email address doesn't exist in our database" as an error message in PR–UR, the former message enables an attacker to identify a registered user ID. A password-recovery screen that outputs a consistent message, such as "If that email address is in our database, we'll send you an email to reset your password" (Table 1 PR-SM) in PR–R and PR–UR, is secure against our attack.

2.2.3 Account Creation

Each user on a service should have a user ID that is unique. Therefore, online services prevent overlapped registration when a user tries to create a new account with a user ID that is already registered. Thus, an account-creation screen also has two types of error/normal states other than input format error: AC–R creating a new account failed because the input user ID is registered, and AC–UR a new account was created with the input user ID (Table 1). For instance, if an account-creation screen outputs "This user ID is already in use" as an error message in AC–R and "Welcome! You have signed up successfully" as a message in AC–UR, the former error message enables an attacker to identify a registered user ID. An account-creation screen that outputs a consistent message, such as "A link to activate your account has been emailed to ⟨input email address⟩" (AC–SM in Table 1) in AC–R and A–UR, is secure against our attack.

2.3 Attack Flow

We assume that an attacker, who is an insider of the target (i.e., an intimate or acquaintance), knows the target's email address or phone number and abuses it as a user ID. As shown in **Fig. 1**, our attack flow has two separate phases: finding vulnerable services (Phase I) and identifying the existence of the target's account (Phase II). Note that this attack flow does not need high-level technical skills such as statistics and programming. Thus, anyone who notices the defects and knows the target's email address or phone number can perform our attack. We describe the attack flow of our account-existence attack using the target's email address as a user ID.

2.3.1 Phase I: Finding Vulnerable Services

First, an attacker prepares two of his/her email addresses, which are not registered on services at this time. Next, the attacker enumerates which sensitive services he/she wants to find out whether the target has an account on or not. The attacker then visits each account-creation screen on the service websites or mobile apps, creates an account with one of the email addresses, and also collects the displayed message. Then he/she log outs from the service. Next, the attacker collects the pair of messages of each login-related function (i.e., login, password recovery, and account creation) with the registered/unregistered email addresses on sensitive services in the following way.

Login messages: The attacker inputs the registered email address and an arbitrary incorrect password that satisfies the password-composition policy into the login screen and collects the displayed message. Next, the attacker inputs the unregistered email address and an arbitrary password that satisfies the policy into the login screen and then collects the displayed message.

Password-recovery messages: The attacker inputs the registered email address into the password-recovery screen and then collects displayed message. Next, the attacker inputs the unregistered email address into the password-recovery screen and then collects the displayed message.

Account-creation messages: The attacker inputs the registered email address, an arbitrary incorrect password that satisfies the policy, and arbitrary personal information that satisfies format va-

Table 1 Examples of secure and insecure output messages in login-related functions.

Function	Input information	Output message (insecure)	Output message (secure)
Login	[L–R] Registered user ID with incorrect password	[L–R–IM] "Incorrect password"	[L–SM] "Incorrect user ID or password"
	[L–UR] Unregistered user ID with arbitrary password	[L–UR–IM] "That user ID doesn't exist"	
Password recovery	[PR–R] Registered email address	[PR–R–IM] "We just sent you a password-reset link"	[PR–SM] "If that email address is in our database, we'll send you an email to reset your password"
	[PR–UR] Unregistered email address	[PR–UR–IM] "This email address doesn't exist in our database"	
Account creation	[AC–R] Registered user ID	[AC–R–IM] "This user ID is already in use"	[AC–SM] "A link to activate your account has been emailed to ⟨input email address⟩"
	[AC–UR] Unregistered user ID	[AC–UR–IM] "Welcome! You have signed up successfully"	

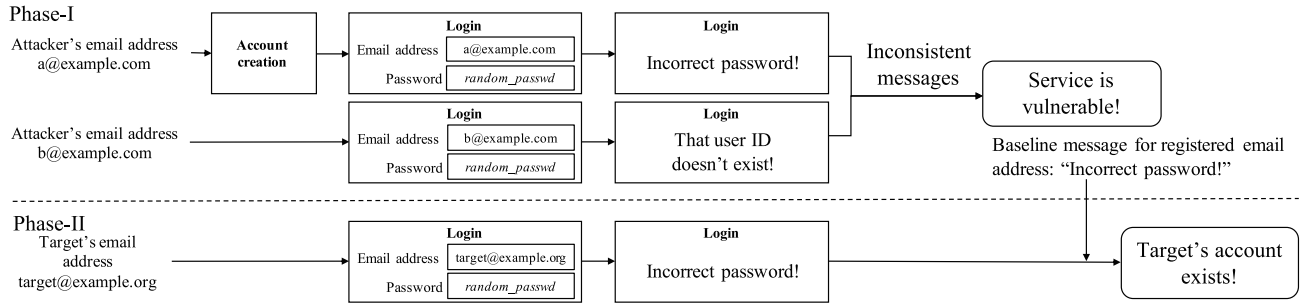


Fig. 1 Example of attack flow in login function.

lidity into the account-creation screen and then collects the displayed message. The attacker has already collected the account-creation message with an unregistered email address when he/she created an account.

A login-related function is insecure if its two collected messages are inconsistent, and a service is vulnerable if any one of three types of login-related functions is insecure. The attacker uses these two inconsistent messages as baseline messages to be compared with login-related messages for the target email address in Phase II.

2.3.2 Phase II: Identifying the Existence of the Target's Account

The attacker inputs the target's email address to the input form of the login-related function where he/she found a defect in Phase I and then collects the displayed message. The attacker compares the above message with the baseline messages. If the message for the target email address matches the baseline message for the registered email address, the attacker can identify the existence of the target's account.

3. Exploratory User Study

To answer **RQ1** (What services do users consider sensitive?), we designed an exploratory user study. Through this study, we enumerated potential sensitive services and grasped users' basic expectations toward online services to determine whether further in-depth studies about our account-existence attack are worth pursuing for **RQ2** and **RQ3**.

3.1 Methodology

We asked participants a multiple-choice question: "Among online services, are there any that you would feel uncomfortable if other people find out that you have an account on?"

We provided 11 choices of service categories: career change, cloud storage, dating, financial, forum, healthcare, porn, shopping, social networking, other, and never. We considered the above categories as potentially sensitive from interviews with our co-workers who are security and privacy researchers. We also provided optional open-ended forms for providing specific service names in each category.

We also told participants (1) to assume that other people can only find out whether or not you have an account on the service but cannot find out specific details such as how you use that service, and (2) that you are allowed to answer about services you do not have an account on, because we tried to collect various kinds of potentially sensitive services. The full questionnaire of this survey is shown in Appendix A.1.

We recruited participants ($N = 614$) from MTurk. We limited participants to U.S. residents with a HIT approval rating of over 97%. We compensated participants US$1.0 for completing the survey, well exceeding the U.S. federal minimum wage standards. Participants finished this survey in 1.9 minutes on average. We conducted this survey in June 2018.

3.2 Results

Table 2 shows the sensitive service categories obtained from our participants. As a result, 81.6% (501/614) of participants selected one or more sensitive service categories. In particular, dating (54.4%) and porn (50.5%) were the top two selected categories. Dating included services provided for sexual minorities, particular occupations, and religions. Porn also included services provided for particular sexual propensities. Social networking (19.9%), career change (17.6%), forum (14.3%), and financial (12.5%) were selected by more than one in eight participants. The forum category included services related to sex life, sperm banks, hate speech, and side jobs. Although few participants selected shopping (8.8%), healthcare (4.6%), and cloud storage (4.4%), shopping and healthcare also include services that should be considered sensitive. For example, shopping includes services

Table 2 Participants' answers for sensitive service categories (multiple choices allowed, $N = 614$).

Category	% Participants	
Dating	54.4%	81.6%
Porn	50.5%	
Social Networking	19.9%	
Career change	17.6%	
Forum	14.3%	
Financial	12.5%	
Shopping	8.8%	
Healthcare	4.6%	
Cloud storage	4.4%	
Other	3.9%	
Never		18.4%

for selling adult goods, and healthcare includes highly sensitive services for sexually transmitted disease (STD) testing, other diseases, and birth control. Other (3.9%) included services related to online gaming, crowd-sourcing services, supplemental nutrition assistance program (SNAP) benefits, and terrorism. In total, 267 unique service names were provided by 405 participants. Note that some services were mentioned across multiple categories.

Summary for RQ1: We found that 81.6% (501/614) of participants answered that there are sensitive services. Specifically, six categories (dating, porn, social networking, career change, forum, and financial) were selected by more than one in eight participants. We collected 267 actual sensitive services across each category.

4. Measurement Study of Login-related Messages

To answer **RQ2** (Are such sensitive services secure against our attack to identify the existence of a target's account?), we examined to what extent actual services that users consider sensitive are vulnerable to our account-existence attack.

4.1 Methodology

4.1.1 Service Selection

We selected candidates for our measurement study from the 267 sensitive services provided by the participants in our exploratory user study by the following procedure. We first set the number of services for each category in accordance with the percentage distribution in Table 2. Then, for each category, we selected specific services as candidates in descending order of the number of participants who provided the service names, except the several services for which we were not able to create accounts (the reasons are described in Section 6.4). Through this procedure, 84 sensitive services were selected as candidates. We assumed these selected candidates are sufficient to understand the circumstances surrounding sensitive services because they cover 86.7% (351/405) of participants who provided one or more sensitive service names.

We were also concerned about whether sensitive services are more secure than others, i.e., popular services. Therefore, we conducted comparative analysis of both sensitive and popular services. For selecting the candidates of popular services, we used the list of Alexa Top Global Sites [*1]. Note that some sensitive services selected as candidates were also ranked high in the list of Alexa. We excluded services whose login-related screens were written in a language other than English. In addition, we excluded paid services. We also selected a single representative service from a *service group* that shares the same user ID, e.g., Google's services and localized services. The list of Alexa Top Global Sites often contains services written in Chinese and localized services, most of which were unfortunately excluded in our measurement study. Through this procedure, 45 popular services were also selected as candidates starting from the top 135 of the Alexa list.

[*1] The list was obtained on July 23rd, 2018.

Table 3 User IDs of sensitive/popular services.

	#	Email address	Username	Phone number
Sensitive	84	82.1%	42.9%	9.5%
Popular	45	77.8%	46.7%	17.8%
Total	109	79.8%	44.0%	8.3%

In summary, the candidates were 109 unique services: 84 sensitive and 45 popular, of which 20 were both. We then investigated the types of user IDs used in these services because our account-existence attack focuses on services permitting email addresses or phone numbers as user IDs, as discussed in Section 2. The results from the 109 services are listed in **Table 3** (for more details, see Table A·1 in Appendix A.3). We found that email addresses are widely used on actual services as user IDs; services permitting email addresses as user IDs accounted for 79.8% (87/109). Thus, we finally examined the above services in our measurement study: 87 unique services including 69 sensitive and 35 popular, of which 17 were both. More details of these sensitive services are provided in Table A·4 in Appendix A.4. For a complementary survey, we further examined the services permitting only usernames as user IDs and provide the results in Appendix A.6.

4.1.2 Evaluation Process

Our systematic evaluation focused on messages of three types of login-related functions: login, password recovery, and account creation. We evaluated messages from these functions in the two different stages of an account lifecycle: *before registration* and *after registration*. This evaluation revealed the basic security level of the services. We also extended this evaluation to further stages: *update* (i.e., changing the registered email address) and *account closure*. We argue that the last two stages are potential defensive actions for users who already have accounts on insecure sensitive services. Through these extended evaluations, we measured the effectiveness of potential defensive actions. We conducted the evaluation process manually in accordance with our threat model in which the attackers do not necessarily need to automate our attack due to it only needing a small number of attempts on specific services. There are various obstacles to automate the evaluation process on the login-related screens, e.g., account-creation screens require various types of personal information and preferences related to service contents.

When examining services, we should consider how users currently access them. In addition to web browsers on PCs, mobile apps have become a major tool for using services, and many services provide dedicated apps, so an attacker may also perform our attack via dedicated apps. We examined both websites and mobile apps corresponding to the selected services. We collected

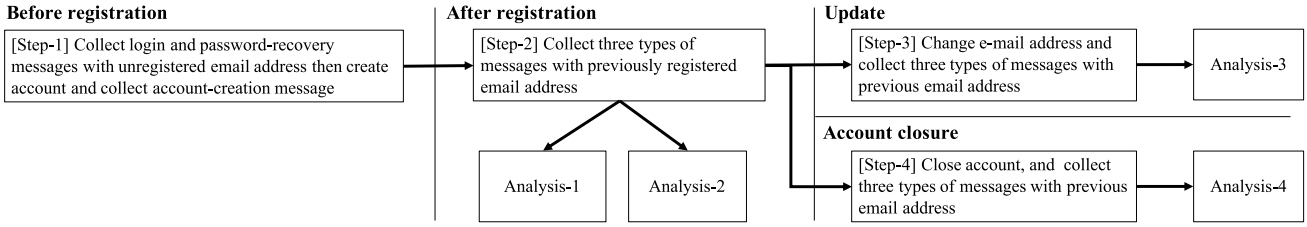


Fig. 2 Overview of evaluation process for each service.

Table 4 Summary of evaluating messages of three types of login-related functions of websites(Analysis-1).

Category	#	Insecure							Totally secure
		$\overline{\mathbf{L}} \cap \overline{\mathbf{PR}} \cap \overline{\mathbf{AC}}$	$\mathbf{L} \cap \overline{\mathbf{PR}} \cap \overline{\mathbf{AC}}$	$\overline{\mathbf{L}} \cap \mathbf{PR} \cap \overline{\mathbf{AC}}$	$\overline{\mathbf{L}} \cap \overline{\mathbf{PR}} \cap \mathbf{AC}$	$\mathbf{L} \cap \mathbf{PR} \cap \overline{\mathbf{AC}}$	$\mathbf{L} \cap \overline{\mathbf{PR}} \cap \mathbf{AC}$	$\overline{\mathbf{L}} \cap \mathbf{PR} \cap \mathbf{AC}$	$\mathbf{L} \cap \mathbf{PR} \cap \mathbf{AC}$
Dating	14	0.0%	21.4%	7.1%	0.0%	**71.4%**	0.0%	0.0%	0.0%
Porn	10	10.0%	**60.0%**	0.0%	0.0%	30.0%	0.0%	0.0%	0.0%
Social networking	9	11.1%	**55.6%**	11.1%	22.2%	0.0%	0.0%	0.0%	0.0%
Career change	9	22.2%	22.2%	0.0%	0.0%	**55.6%**	0.0%	0.0%	0.0%
Forum	7	**85.7%**	14.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Financial	4	0.0%	25.0%	0.0%	0.0%	**75.0%**	0.0%	0.0%	0.0%
Shopping	7	28.6%	**57.1%**	0.0%	0.0%	14.3%	0.0%	0.0%	0.0%
Healthcare	5	20.0%	**60.0%**	0.0%	0.0%	20.0%	0.0%	0.0%	0.0%
Cloud storage	4	**50.0%**	25.0%	0.0%	0.0%	25.0%	0.0%	0.0%	0.0%
Sensitive	69	21.7%	**39.1%**	2.9%	2.9%	33.3%	0.0%	0.0%	0.0%
Popular	35	**37.1%**	28.6%	2.9%	5.7%	22.9%	0.0%	0.0%	2.9%
Total	87	24.1%	**37.9%**	2.3%	2.3%	32.2%	0.0%	0.0%	1.1%

L, **PR**, and **AC** are sets of services with secure login, password-recovery, and account-creation functions, respectively.

mobile apps available from the Google Play store. Note that the policy of Google Play prohibits apps corresponding to porn services.

Figure 2 gives an overview of the evaluation process for each service. This evaluation preliminarily required preparation of the email address to be used for registration. We call this the *signaling* email address. The process involves four steps and four analyses. In Step–1, we collect the messages of login and password recovery in a service with an unregistered email address, which is our prepared signaling email address. For a login message, we input an arbitrary password that satisfies the password-composition policy required by the service. Next, we create an account with the signaling email address and collect the messages on the account-creation screen, which are also analyzed later as account-creation messages. We then log out of the service. In Step–2, we collect the messages of three types of functions with the signaling email address. Note that we input an arbitrary incorrect password that satisfies the policy required by the service in login screens. Similarly, we input an arbitrary incorrect password that satisfies the policy and arbitrary personal information (e.g., gender, date of birth, and location) that satisfies format validity in account-creation screens. Steps–1 and –2 are followed on both websites and mobile apps corresponding to the service.

For Analysis–1, we compare the messages in each function of websites collected in Steps–1 and –2. We determine each function to be secure or insecure in accordance with whether the messages collected in Steps–1 and –2 are consistent or not. For the overall evaluation output, if all three functions are secure, we define the service as *totally secure*. If any function is insecure, we define the service as *insecure* because our account-existence attack is able to succeed. For Analysis–2, we compare the messages in each function of mobile apps in the same way as in Analysis–1. We then further compare the numbers of secure functions of websites and mobile apps.

Next, we independently conducted similar examinations in different registration stages: after update (Step–3) and after account closure (Step–4). In Steps–3 and –4, 42 and 60 randomly selected insecure services are examined, respectively. We prepared two distinct signaling email addresses for each service in Steps–3 and –4. In Step–3, we change the registered email address (i.e., the signaling email address) to another one, which is also ours, and after at least 72 hours, we collect the messages of the three functions on each website with the signaling email address. For Analysis–3, we compare the messages in each function collected in Steps–1 and –3. If the messages in Steps–1 and –3 are consistent (i.e., the services treat previously registered email addresses in the same way as unregistered email addresses), it means that changing the email addresses effectively removes the threat of attack. In Step–4, we delete the account on which the signaling email address is registered, and after at least 72 hours, we collect the messages of the three functions on each website with the signaling email address. For Analysis–4, we compare the messages in each function collected in Steps–1 and –4. If the messages in Steps–1 and –4 are consistent (i.e., the services treat previously registered email addresses in the same way as unregistered email addresses), it means that account closure effectively removes the threat of attack.

We conducted this study from July to August 2018. Through this evaluation process, we collected 1,146 login-related messages (for more details, see Table A·5 in Appendix A.5).

4.2 Results

4.2.1 Analysis–1: Inconsistent Messages of Login-related Functions

The results of evaluating the messages of three types of login-related function of websites are listed in **Tables 4** and **5**. Surpris-

Table 6 Summary of evaluating messages of three types of login-related functions of mobile apps (Analysis-2).

Category	#	Insecure							Totally secure
		$\overline{\mathbf{L}} \cap \overline{\mathbf{PR}} \cap \overline{\mathbf{AC}}$	$\mathbf{L} \cap \overline{\mathbf{PR}} \cap \overline{\mathbf{AC}}$	$\overline{\mathbf{L}} \cap \mathbf{PR} \cap \overline{\mathbf{AC}}$	$\overline{\mathbf{L}} \cap \overline{\mathbf{PR}} \cap \mathbf{AC}$	$\mathbf{L} \cap \mathbf{PR} \cap \overline{\mathbf{AC}}$	$\mathbf{L} \cap \overline{\mathbf{PR}} \cap \mathbf{AC}$	$\overline{\mathbf{L}} \cap \mathbf{PR} \cap \mathbf{AC}$	$\mathbf{L} \cap \mathbf{PR} \cap \mathbf{AC}$
Dating	13	0.0%	23.1%	7.7%	0.0%	**69.2%**	0.0%	0.0%	0.0%
Social networking	8	**62.5%**	25.9%	0.0%	0.0%	0.0%	12.5%	0.0%	0.0%
Career change	6	16.7%	0.0%	0.0%	0.0%	**83.3%**	0.0%	0.0%	0.0%
Forum	2	**50.0%**	0.0%	**50.0%**	0.0%	0.0%	0.0%	0.0%	0.0%
Financial	4	0.0%	25.0%	0.0%	0.0%	**50.0%**	0.0%	0.0%	25.0%
Shopping	6	33.3%	**66.7%**	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Healthcare	3	**100.0%**	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Cloud storage	4	**50.0%**	25.0%	0.0%	0.0%	25.0%	0.0%	0.0%	0.0%
Sensitive	46	30.4%	23.9%	4.3%	0.0%	**37.0%**	2.2%	0.0%	2.2%
Popular	31	**54.8%**	25.8%	3.2%	0.0%	12.9%	0.0%	0.0%	3.2%
Total	63	**33.3%**	25.4%	4.8%	0.0%	31.7%	1.6%	0.0%	3.2%

L, **PR**, and **AC** are sets of services with secure login, password-recovery, and account-creation functions, respectively.

Table 5 Percentages of secure secure login-related functions on websites (Analysis-1).

	#	L	PR	AC
Sensitive	69	72.5%	36.2%	2.9%
Popular	35	54.3%	25.7%	8.6%
Total	87	71.3%	35.6%	3.4%

ingly, we found that many services were partially secure but determined 0.0% (0/69) of sensitive services and only 2.9% (1/35) of popular services to be totally secure. In other words, almost all services were vulnerable to our account-existence attack on websites. The only secure service we found through our measurement study was *craigslist*, which is a forum service that has been running for over two decades.

As shown in Table 5, far fewer services had secure account-creation functions on websites than had secure login and password-recovery functions. Only 2.9% (2/69) and 8.6% (3/35) of sensitive and popular services displayed secure account-creation messages on websites. This result indicates an attacker can perform our attack extremely efficiently if he/she starts to examine the defects of the account-creation function.

As shown in Table 4, over half of the services in dating, career change, and financial displayed both secure login and password-recovery messages. This indicates that these services made an effort to emphasize security and privacy. Sensitive services tended to be slightly more secure than popular services listed in Alexa Top Global Sites, except for craigslist, which was the only secure service in our measurement study. For example, all three types of functions were insecure more often on popular services (37.1%) than sensitive services (21.7%).

We found some interesting cases in terms of inconsistency. For example, some insecure services did not proceed to the next screen when we input a registered email address in the account-creation screen. Even in this case, an attacker can identify the account's existence after comparing such inconsistent performance.

4.2.2 Analysis–2: Websites vs. Mobile Apps

We examined mobile apps available in Google Play; 63 out of 87 services (including 46 out of 69 sensitive services and 31 out of 35 popular services) provide mobile apps.

The results of evaluating the messages of the three login-related functions of mobile apps are listed in **Table 6**. Similar to the results for websites accessed with browsers, almost all the services accessed with mobile apps were vulnerable to our account-existence attack: only 2.2% (1/46) of sensitive services and 3.2% (1/31) of popular services were totally secure. Note that craigslist's mobile app displays secure messages in all three types of functions, so it is completely secure against our attack.

Table 7 How secure mobile apps are compared with websites (Analysis-2).

	#	Same level	Less secure	More secure
Sensitive	46	71.7%	19.6%	8.7%
Popular	31	71.0%	22.6%	6.5%
Total	63	71.4%	19.0%	9.5%

Table 8 Percentages of secure login-related functions on websites and mobile apps (Analysis-2).

	#	L	PR	AC
Websites	63	69.8%	42.9%	4.8%
Mobile apps	63	61.9%	39.7%	4.8%

We compare the security level of mobile apps and websites. **Table 7** summarizes the results. We found that 71.4% (45/63) of mobile apps had the same security level, i.e., the same number of secure functions, as the corresponding websites. Among the services whose websites and mobile apps had different security levels, the mobile apps tended to be less secure than the websites. This is due to the login function of mobile apps. As shown in **Table 8**, among 63 services that have mobile apps, the percentage of services whose login function was secure on mobile apps (61.9%) is somewhat lower than that of websites (69.8%). On websites, many services display the input forms for both user ID (e.g., email address) and password on a single login screen. On some mobile apps, the input forms are separated into two login screens (**Fig. 3** (a)). For instance, the first login screen displays the input form for user ID, and if a registered user ID is input, the second one displays the input form for the password. If an unregistered user ID is input, an error message such as "That user ID doesn't exist" is displayed. In addition, we found two mobile apps that had an insecure login procedure. They displayed a shared input screen for login and account creation (Fig. 3 (b)). If a registered user ID is input, they display a login screen and request users to input the password. If an unregistered user ID is input, they display an account-creation screen and request users to set the password. Although these login procedures may be designed for user-friendliness, they unfortunately also result in defects against our account-existence attack.

4.2.3 Analysis–3: Changing Email Addresses

Among 42 randomly selected insecure services, 40 provide a

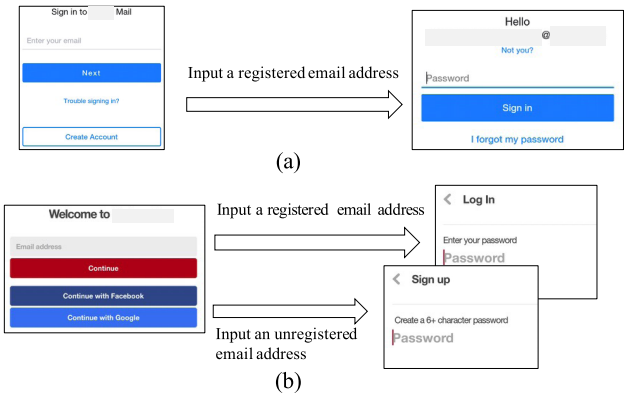


Fig. 3 Insecure login screen of mobile apps.

function to change email addresses; thus, we selected these 40 services for this analysis.

When we input previous email addresses, login-related messages consistent with the ones for unregistered email addresses were displayed in the three types of functions and thus our attack using previous email addresses was no longer successful in 92.5% (37/40) of services. In the remaining 7.5% (3/40) of services, the login-related messages for a registered email address were displayed (e.g., "An account already exists with that email address" in the account-creation function). Through this analysis, we confirmed that changing registered email addresses to ones not known to others is effective against our attack on most services.

4.2.4 Analysis–4: Account Closure

Among 60 randomly selected insecure services, 42 provide a function to close accounts. We selected these 42 services for this analysis and excluded the other 18, because 10 do not provide such a function and the other 8 require users to contact a support center. Especially, a small number of services in porn and shopping categories provide an account-closure function.

Account closure was effective in only 47.6% (20/42) of the services, so the results revealed that account closure was less effective than changing email addresses. The messages were inconsistent with ones for registered email addresses or changed to announce the account closure, e.g., "This account has been deleted." This means our attack was still successful.

Summary for RQ2: Through our measurement study, we revealed that almost all services regardless of whether they are sensitive or popular are vulnerable to our attack to identify the existence of a target's account. Specifically, only a small number of services displayed secure account–creation messages. About 19–22% of services had mobile apps that were less secure than the websites. Email-address changing, a possible defensive action, was effective in 92.5% of services; however, account closure was effective in only 47.6% of services.

5. User Study to Understand User Expectations

In our second user study, we focused on detailed user expectations toward online privacy and privacy-protecting behaviors on sensitive services. We quantified the impact of our account-existence attack through the results obtained from this study and our measurement study to answer RQ3: "How much does our account-existence attack actually impact user privacy?"

5.1 Methodology

The survey contained nine open- and closed-ended questions regarding demographics, services considered sensitive, reasons for not wanting others to know their use of sensitive services, motivation for violating intimates' or acquaintances' privacy, and privacy-protecting behaviors on sensitive services. The full questionnaire of this survey is shown in Appendix A.2.

We recruited participants from MTurk and limited them to U.S. residents with a HIT approval rating of over 97%. We compensated participants US$2.0 for completing the survey to well exceed the U.S. federal minimum wage standards. In addition, we informed them that we were going to pay a US$1.0 bonus to participants who wrote detailed explanations in the instructions of our survey. Participants finished this survey in 8.8 minutes on average, and most participants were actually compensated US$3.0 in total.

We removed 24 respondents who gave careless or incomplete answers, i.e., less meaningful sentences for open-ended questions and unnecessary answers. In the following analyses, we use the data responded by the remaining 447 participants. Of these 447 participants, 53.7% were male, 45.2% were female, and 1.1% selected "Other" or "Prefer not to say." Regarding age, 9.6% were 18–24, 44.5% 25–34, 22.6% 35–44, 12.8% 45–54, 6.9% 55–64, and 3.5% over 65. They had a certain number of online service accounts: 0–9 (34.7%), 10–19 (29.3%), 20–29 (17.4%), 30–39 (9.6%), 40–49 (3.4%), and more than 50 (5.6%).

We conducted this survey in August 2018.

5.2 Results

5.2.1 Reasons Regarding Sensitive Services

After demographic questions, we asked the same question as our exploratory user study; whether there are sensitive services that they would not want others to know they used. The results are approximately the same as those of our exploratory user study: 82.1% (367/447) of participants answered that there are such sensitive services [*2]. Then we asked them who they would not want to find out about their accounts' existence on sensitive services and why as an optional question. Many participants selected business acquaintances, i.e., *co-workers* (66.6%), *bosses* (63.9%), and *employers* (59.6%); private acquaintances, i.e., *friends* (59.9%), *family members* other than one's partner (64.5%), *partner* (including wife, husband, girlfriend, and boyfriend) (41.0%); *on-line friends* (33.1%); and *acquaintances* (41.6%). Some participants mentioned ex-partners, bank loan officers, and pastors as *other* (4.5%). We performed inductive thematic analysis on 267 explanations as the reasons. The final codebook had a total of three themes. Coding reliability for two independent coders was Cohen's kappa $k = 0.84$.

In 85.4% (228/267) of the explanations, participants considered the use of sensitive services to be personal information so

[*2] Our results were not biased by any monetary incentive, i.e., we also prepared an open-ended question for participants who answered there are no sensitive services, so all participants had a chance to receive the bonus.

they would be *embarrassed* with others knowing about it. Many participants would not want their family or friends to know they use dating and porn services. For example, one said, "*Dating sites mean that I can't find a date normally [...]*" In addition, one participant who did not want anyone to know she uses porn services commented that "*Because porn is still taboo and especially because I'm a woman.*" For the same reason, one participant who did not want his/her friends to know he/she uses forum services commented that, "*They might laugh at my interests.*" Another participant who did not want his/her friends and acquaintances to know he/she uses financial services commented that, "*I have accounts with a number of payday loan companies [...]*" In 11.6% (31/267) of the explanations, participants mentioned *effect on work* such as personal reputation, bonuses, promotion, firing, and job hunting. They did not want their bosses, employers, or co-workers to know they use porn or career change services. For instance, one said, "*It might damage my reputation and how they view me professionally, weakening my potential promotions and contacts in the future*" and another said, "*I don't want them to know that I am looking for another job.*" *Immoral behavior*, e.g., a participant saying, "*I'm married so I shouldn't be on dating sites. [...]*", was also mentioned in 3.0% (8/267) of the explanations.

5.2.2 Motivations of Potential Perpetrators

Attacks may occur among intimates or acquaintances, so people could be either victims or perpetrators. To understand the motivations of potential perpetrators, we asked participants "*Have you ever wanted to know if someone, whose email address you know, has an account on some online services?*" Note that we did not directly tell participants about our account-existence attack or ask whether they had performed our attack for ethical reasons. Considering that our attack does not require any high-level technical skills and almost all services are vulnerable to it, we avoided instigating them to perform our attack through this user study.

We found that 25.3% (113/447) of participants expressed such a desire. We collected 38 optional explanations as the motivations from them. The motivations to perform insider attacks varied [27]. We conducted deductive thematic analysis on the basis of the study and Cohen's kappa coefficient was $k = 0.85$.

The motivation mentioned in 63.2% (24/38) of the explanations is classified as *jealousy* [27]. Participants mentioned their interest in whether their partners, ex-partners, and crushes use dating services. For instance, one said, "*[...] I wanted to know if a current boyfriend had a profile on an online dating site*" and another said, "*A girl that I know that I have had a crush on since high school. I have her email, and always wonder if she has any sort of account on online dating services.*" In 34.2% (13/38) of the explanations, participants admitted wanting to pry on family, friends, and business acquaintances, which is classified as a *curiosity* [27]. For instance, one said, "*I have wanted to know whether coworkers were considering career changes/looking at job-search sites*" and another said, "*I would just want to see what friends I have use what sites so I can talk to them more about it.*" There was a unique explanation regarding *worry* about intimates and acquaintances, which was not previously mentioned in previous work on insider attacks [27]. One expressed his/her parental feeling: "*I have wanted to know my son's information [...] as to make sure he isn't into things that might cause him harm.*"

Table 9 Email addresses registered on sensitive services ($N = 367$).

Types of a registered email address	%
(i) The same email address as for non-sensitive services, which anyone who knows me may know	30.5%
(ii) The same email address as for non-sensitive services, which no one who knows me knows	15.0%
(iii) Different email address(es) from those for non-sensitive services, one of which anyone who knows me may know	14.7%
(iv) Different email address(es) from those for non-sensitive services, none of which anyone who knows me knows	39.5%
(v) Other	0.3%

We revealed a latent desire to violate intimates' and acquaintances' privacy inherent in users' minds. Our account-existence attack does not require high-level technical skills, so anyone who knows the target's email address can become a perpetrator if he/she wants. Note that social desirability bias might have affected their answers, i.e., the percentage of the participants who have such a desire might be higher than in our results.

5.2.3 Users' Privacy-protecting Behaviors on Sensitive Services

To quantify potential victims, we clarified how many participants securely created their accounts on services they considered sensitive. Specifically, we asked participants who have one or more sensitive services what kind of email address they register for sensitive services. The results are listed in **Table 9**. The 45.2% (166/367) of participants who selected (i) and (iii) register email addresses that are known to others. Based on the results discussed in Section 4, these participants' privacy can be easily violated by insiders who know their email address. On the other hand, the 54.5% (200/367) of participants who selected (ii) and (iv) are secure; they register email addresses that are not known to others.

Participants who selected (iii) and (iv) (54.2%) cautiously register different email addresses for sensitive and for non-sensitive services. Although these participants want to protect themselves against latent privacy threats, those who selected (iii) are unfortunately not secure against our attack. Note that one participant selected (v), – mentioning that he/she inputs invalid email addresses.

Summary for RQ3: Through this user study, we found that the reasons for not wanting others to know they use sensitive services were embarrassment, effect on work, and immoral behavior. As potential perpetrators of our account-existence attack, 25.3% (113/447) of participants represented such a desire. Among participants who had one or more sensitive services, 45.2% (166/367) registered email addresses known to others; thus, they could be potential victims.

6. Discussion

6.1 Privacy and Usability

Login messages: Users can immediately understand the reason for login failure when the login screen displays L–R–IM or L–UR–IM in Table 1, which are insecure messages, e.g., "That user ID doesn't exist" (L–UR–IM). On the other hand, a secure message such as "Incorrect email address or password" (L–SM in

Table 1) interferes with users' understanding of the reason for login failure. This may result in an increase in login attempts, but we consider appropriate descriptions and navigation reduce the burden of secure messages faced by users. For example, a login screen instructs a user to input the email address on a password-recovery screen and checks whether a password-reset mail is delivered (if a password-reset mail is delivered, the input email address is considered valid).

Password-recovery messages: Users can immediately recognize the error of password recovery when the password-recovery screen displays "This e-mail address doesn't exist in our database" (PR–UR–IM in Table 1), which is an insecure message. However, a secure message such as "If that address is in our database, we'll send you an email to reset your password" (PR–SM in Table 1) is not very useful because users cannot recognize whether the password recovery was successful until checking their email.

Account-creation messages: If an account-creation screen displays a secure message such as "A link to activate your account has been emailed to ⟨input email address⟩" (AC–SM in Table 1), users cannot immediately complete creating an account; they have to leave the screen, check their email, and click the activation link provided in the message. We found that many services forced users to carry out email-based verification before using services to prevent throwaway accounts. For such services, adopting secure messaging does not significantly burden users.

Messages after email-address change and account closure: Insecure messages after email-address change and account closure, e.g., "This user account has been deleted," are useful for users who have forgotten their previous actions; however, this type of insecure message results in keeping a service permanently vulnerable.

Whether to prioritize reducing threats to privacy or improving usability depends on not only the policy of the service provider but also the frequency of encountering the threat, severity of the threat, and user privacy concerns. Services that users consider sensitive should adopt secure messages in login-related functions. Given user expectations toward sensitive services in our user studies, prioritizing reducing threats to privacy is a rational choice for providers that offer services considered sensitive.

6.2 Recommendations for Service Providers

We recommended two best practices for online service providers.

Consistent message: Services should prevent attackers from identifying the existence of a user's account. Login, password-recovery, and account creation screens should display consistent messages whatever the user IDs they receive at any stage in the account lifecycle (before registration, after registration, update, and account closure). Examples are shown in Table 1 L–SM, PR–SM, and AC–SM.

User choice: A compromise solution for services that cannot be clearly classified as sensitive or non-sensitive is giving choices of messaging type to users: privacy- or usability-aware messages. Users who are concerned about privacy may select the former, whereas users who are not may select the latter. Services should inform users of the risk and provide the choices when users create their accounts.

We also recommended against the following three *inappropriate* practices.

Prohibiting using email address as user ID: A non-email user ID is not a solution because of using email-based contact information and re-using user IDs. We found almost all online services use an email address as contact information regardless of the types of user IDs (for details, see Tables A·2 and A·3 in Appendix A.3). An attacker can still abuse the messages of password recovery and account creation with a target email address on services permitting an email address as contact information. Furthermore, if a target re-uses his/her non-email user ID across services, an attacker can still abuse the user's privacy; user ID re-using allows for linking accounts on different services.

Rate-limiting such as CAPTCHA and lockout: Rate-limiting of login attempts is ineffective against attacks by insiders. An attacker who wants to violate intimates' or acquaintances' privacy can manually perform an attack with a small number of attempts, although the above defenses prevent only automated and large numbers of attempts.

Single-Sign-On: Users on sensitive services may not accept single-sign-on to delegate authentication to third parties. OpenID is one solution to provide stronger authentication and is recommended by Bonneau and Preibusch [18], but this solution is not appropriate for sensitive services. The survey results of user expectations indicate that many users do not want to link identities across sensitive and non-sensitive services.

6.3 Recommendations for Users

Almost all services are currently vulnerable to our account-existence attack. Users should understand the threat to privacy and take appropriate defensive actions. A practical method against this attack is registering dedicated email addresses (e.g., throw-away email address and email alias) for sensitive services, which are not known to others and impossible to guess. This can eliminate the threat to privacy even though creating and managing such dedicated email addresses is slightly time-consuming. Password managers are able to help users manage various user ID and password pairs for each service. *Sign In with Apple*[*3] is a promising solution to make it easy for users to log in to services with dedicated email addresses, which are randomly generated with this solution for each service.

For users who have already registered an email address known to others on sensitive services, changing the email address to one that is not known to others is effective in 92.5% of services; however, account closure is effective in only 47.6% of services.

6.4 Limitations

Unexamined sensitive services: We could not examine certain services mentioned by participants because they require social security numbers (SSNs), identification, etc., for account creation. Such services are credit cards, STD testing, and SNAP benefits. We examined six STD testing services' password-recovery func-

[*3] https://developer.apple.com/sign-in-with-apple/

tions, with which we could check PR-UR messages without creating accounts. We found that 50.0% (3/6) displayed PR-UR messages, which seem to be insecure.

Demographics of participants: As with many human-centered security and privacy studies, the use of MTurk may not reflect the actual demographics of the U.S. population using the Internet. Our participants skewed toward young adults.

Potential victims in practice: In our user studies, we allowed the participants to answer about services they do not have an account on. Thus, the actual percentage of potential victims in practice might be lower than in our results.

User expectations and behaviors on each sensitive service: We designed our second user study to be as concise as possible to keep participants' attention. Thus, our revealed user expectations and behaviors were not for each sensitive service but sensitive services as a whole. The difference in user expectations and behaviors on their different sensitive services is the limitation in this work.

6.5 Research Ethics and Disclosure

6.5.1 Study Designs with Ethical Considerations

We carefully designed our measurement study. We conducted minimal login-related attempts to minimize additional load on the actual services. To reduce the risk that our experiment would be considered harmful (e.g., possible password guessing) and affect actual user accounts, we input our experimental email addresses and never input email addresses possibly owned by third parties. Therefore, no user was actually involved in our experiment. Our user study designs were ethically reviewed and approved by our institutional review board (IRB).

6.5.2 Guideline Improvements

The defects we focused on in this study were not just typical vulnerabilities derived from specific software but design issues across existing services. To facilitate countermeasures for diverse stakeholders of online services, we discussed with vulnerability coordinators regarding responsible disclosure and a plan for cooperating with global web security communities, such as Open Web Application Security Project (OWASP), to improve developer and tester guidelines for securing websites and mobile apps, e.g., adding descriptions of our problem statement and countermeasures. After confirming that the descriptions of the defects were insufficient in the OWASP Authentication Cheat Sheet [30] and Application Security Verification Standard (ASVS) [31], we posted the issues to provide information about the defects on their GitHub community pages. On the Authentication Cheat Sheet page, we added the descriptions on the problem and countermeasures in the *Authentication and Error Messages* section; on the ASVS page [31], we added a reference to the description in the above cheat sheet, in September 2019. Furthermore, we discussed with the Information-technology Promotion Agency, Japan (IPA). In response to our report, they created a plan of improving the guidelines for securing websites (i.e., How to Secure Your Web Site [*4]).

[*4] https://www.ipa.go.jp/files/000017318.pdf

Table 10 Response rate by contact point.

Contact point	#	Alexa (Med)	Response rate
Bug bounty platform	9	112.0	100.0%
Security or privacy team	22	1,461.0	40.9%
Customer support	37	13,373.0	13.5%
Total	68	4064.5	33.8%

Table 11 Response rate by Alexa ranking.

Alexa ranking	#	Response rate
1–100	15	73.3%
101–1,000	9	55.6%
1,001–10,000	17	23.5%
10,001–100,000	16	6.3%
100,001–	11	18.2%
Total	68	33.8%

6.5.3 Notification to Service Providers

We also notified service providers having the defects of the problems and solutions we derived.

Notification process: First, we explored the contact points of service providers. Service providers have three possible contact points: bug bounty platform, security or privacy team, and customer support. If a provider has a bug bounty platform, such as HackerOne and Bugcrowd, we sent notification messages via the platform. If not, we sent notification messages via a contact form or email to the security or privacy teams in preference to customer support teams. Next, we informed them about our threat model and the type of functions that we had found insecure on each service in our measurement study. We also added the URL of OWASP Authentication Cheat Sheet that we had improved to inform them about the details of appropriate countermeasures. We finally notified all 68 providers of sensitive services for which we found defects through our measurement study, except one provider that had the same contact point as another service. If we did not receive a response from providers even a few months after the first notification was sent, we messaged them again. We conducted these notifications from October to November 2019 (the first notification) and in February 2020 (the second notification).

Notification results: **Tables 10** and **11** show the response rates for the 68 providers we contacted regarding the response rates by contact point and Alexa ranking, respectively. The response rate, which includes the providers that responded at least once, differs among contact points. Only 13.5% (5/37) of providers we contacted through their customer support team responded. Most are small providers with a low Alexa ranking. Thus, we assume that they do not have a sufficient security management system. As shown in Table 11, the services with a low Alexa ranking responded less often. A few providers showed a willingness to modify the defects immediately. Other providers argued that the defects were an acceptable risk in accord with their privacy policies and had no plan to modify them immediately. However, we believe that our notifications and improvements of guidelines will be useful for improving security of their services in the future, as some providers mentioned.

7. Related work

7.1 Account Security

Various defensive techniques have been adopted on accounts, including password-composition policies [6], [7], [8],

[9], [11], password-strength metering [12], multi-factor authentication [13], [15], [16], and rate-limiting, such as lockout [14], blocking, and CAPTCHA [10], [17]. Bonneau and Preibusch [18] investigated how widespread these countermeasures are by conducting a large scale survey of 150 popular websites in 2010 and found 126 did not have any restriction mechanism against password-guessing attacks. In 2018, Lu et al. extensively investigated authentication rate-limiting mechanisms and revealed that 131 of 192 investigated services allow frequent and unsuccessful login attempts without restriction mechanisms [32]. This result indicated that restriction mechanisms have not been widely adopted in websites about a decade after Bonneau and Preibusch's study [18].

Bonneau and Preibusch [18] also mentioned the messages displayed on the login screens of these websites. Our study significantly differed in the following ways. We comprehensively reviewed three types of login-related functions as well as services on both websites and mobile apps. Login-related functions are recommended to be protected by rate-limiting mechanisms against probing in a brute-force manner [18], [32], but this restriction mechanism is not effective against our account-existence attack by an insider. This is because it can be performed manually and requires a small number of attempts, unlike outsider password-guessing attacks. We advocate that an intrinsic solution is displaying consistent messages for registered/unregistered user IDs. We also examined sensitive services given by the participants of a user study as well as popular services and evaluated the impact of our account-existence attack through a user study.

Bortz et al. [33] demonstrated that the difference in service response time between a registered user and unregistered user can be exploited to identify the existence of a target on a service. Schrittwieser et al. [34] also demonstrated that the address-book-importing feature of short message service (SMS) applications can be abused to identify the existence of a target's phone number on a service. Other studies focusing on account identification include those on history stealing [35], abuses of the friend search function [36], targeted advertisement [37], and user blocking [38]. These attacks have any of three essential properties: timing side-channel [33], [38], cross-site request forgery (CSRF) [33], [35], [38], and service-specific functionalities [34], [36], [37], [38]. Timing side-channel is a statistical property requiring speculative attempts. In contrast, our account-existence attack is deterministic, requiring a small number of attempts. A CSRF-based attack requires the target to access an attacker-prepared script with a browser while logged in to the target web service, which is much more restrictive and difficult to perform than our account-existence attack. Attacks based on service-specific functionalities (such as friend search, custom advertising interface, and user block) mainly target services with rich functionalities such as social networking sites, while our account-existence attack is applicable to any service with ID-password login.

Perito et al. [39] found that users tend to reuse the same or similar usernames among multiple services, making account-linking attacks increasingly effective. Such prevalence of username reusing can be regarded as a major issue because reusing email addresses, which are often known to insiders, as user IDs or contact information makes a user susceptible to our account-existence attack.

7.2 Privacy Abuse by Insiders

Recent studies have shed light on privacy abuse by insiders. Several studies have reported privacy abuse in the context of intimate partner abuse (IPA[*5]). Freed et al. [21] examined the offensive techniques used in IPA by interviewing IPA survivors and experts. Matthews et al. [20] examined victims' security behaviors. These results indicate that insiders use unsophisticated techniques such as physical threats and installation of surveillance tools (spyware). Chatterjee et al. [19] found that some spyware app developers encourage their use in IPA. From the viewpoint of psychology, Arikewuyo et al. [40] found that lack of trust affected cell phone snooping in IPA. For victims of IPA, Freed et al. [41] and Havron et al. [42] explored and proposed practical clinical approaches to help them.

Various kinds of privacy abuse have been reported in the context of not only IPA but also a wider range of relationships (i.e., intimates and acquaintances). Studies on cyber stalking on social networks [22], [23] reported the harm caused by insiders such as ex-partners and acquaintances. Users taking a survey on smartphone locking [24], [25] reported protecting their privacy from insiders as a reason for locking their phones. Muslukhov et al. [26] identified that unauthorized physical access to smartphones by insiders is also considered a threat. Usmani et al. [27] found that 24 and 21% of participants in their study had been attackers and victims, respectively, of unauthorized insider access to Facebook accounts. Marques et al. [28] further revealed the detailed situations of unauthorized insider access. The results of these studies indicate that attacks by insiders have become common. Since our account-existence attack also does not require any high-level technical skills, is can be performed by insiders.

8. Conclusion and Future Work

This study highlighted a new threat from insiders to account security: inconsistent login-related messages on sensitive services may threaten user privacy. We assessed the impact of our attack to identify the existence of a target's account (account-existence attack) on the basis of our user studies and measurement study on actual services. Over 80% of participants answered that there are sensitive services and had diverse reasons for believing so. We revealed that almost all services displayed insecure messages and were vulnerable to our account-existence attack. We found that about half of the participants who have one or more sensitive services behave insecurely on sensitive services and could be potential victims. We provided recommendations for both service providers and users. The fundamental solution is that services considered sensitive, which we revealed through our user study, should display consistent messages in login-related functions. Future research will require further investigation into developer and user aspects of consistent messaging, i.e., why developers have not adopted consistent messages, how they should

[*5] Not to be confused with the Information-technology Promotion Agency introduced in Section 6.5.

adopt them, and how users can understand and behave in accordance with such messages.

References

[1] Hasegawa, A.A., Watanabe, T., Shioji, E. and Akiyama, M.: I Know What You Did Last Login: Inconsistent Messages Tell Existence of a Target's Account to Insiders, *Proc. 35th Annual Computer Security Applications Conference* (*ACSAC'19*) (2019).

[2] Ablon, L., Heaton, P., Lavery, D. and Romanosky, S.: Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information, *Proc. 15th Annual Workshop on the Economics of Information Security* (*WEIS'16*) (2016).

[3] Zou, Y., Mhaidli, A.H., McCall, A. and Schaub, F.: "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach, *Proc. 14th USENIX Conference on Usable Privacy and Security* (*SOUPS'18*), pp.197–216 (2018).

[4] Karunakaran, S., Thomas, K., Bursztein, E. and Comanescu, O.: Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data, *Proc. 14th USENIX Conference on Usable Privacy and Security* (*SOUPS'18*), pp.217–229 (2018).

[5] González, F., Yu, Y., Figueroa, A., López, C. and Aragon, C.: Global reactions to the Cambridge analytica scandal: A cross-language social media study, *Proc. Web Conference 2019* (*WWW'19 Companion*) (2019).

[6] Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F. and Lopez, J.: Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms, *Proc. 2012 IEEE Symposium on Security and Privacy* (*S&P'12*), pp.523–537 (2012).

[7] Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F. and Egelman, S.: Of Passwords and People: Measuring the Effect of Password-Composition Policies, *Proc. 2011 ACM SIGCHI Conference on Human Factors in Computing Systems* (*CHI'11*), pp.2595–2604 (2011).

[8] Pinkas, B. and Sander, T.: Securing passwords against dictionary attacks, *Proc. 9th ACM Conference on Computer and Communications Security* (*CCS'02*), pp.161–170 (2002).

[9] Florêncio, D., Herley, C. and Van Oorschot, P.C.: An Administrator's Guide to Internet Password Research, *Proc. 28th USENIX Conference on Large Installation System Administration*, *LISA'14*, pp.35–52 (2014).

[10] von Ahn, L., Blum, M., Hopper, N.J. and Langford, J.: CAPTCHA: Using Hard AI Problems for Security, *EUROCRYPT*, Lecture Notes in Computer Science, Vol.2656, pp.294–311, Springer (2003).

[11] Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F.: Designing Password Policies for Strength and Usability, *ACM Trans. Information and System Security*, Vol.18, No.4, pp.13:1–13:34 (2016).

[12] Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L.F., Dixon, H., Naeini, P.E., Habib, H., Johnson, N. and Melicher, W.: Design and Evaluation of a Data-Driven Password Meter, *Proc. 2017 ACM SIGCHI Conference on Human Factors in Computing Systems* (*CHI'17*), pp.3775–3786 (2017).

[13] Grosse, E. and Upadhyay, M.: Authentication at Scale, *IEEE Security and Privacy*, Vol.11, pp.15–22 (2013).

[14] Alsaleh, M., Mannan, M. and van Oorschot, P.C.: Revisiting Defenses against Large-Scale Online Password Guessing Attacks, *IEEE Trans. Dependable and Secure Computing*, Vol.9, pp.128–141 (2012).

[15] Aloul, F., Zahidi, S. and El-Hajj, W.: Two Factor Authentication Using Mobile Phones, *Proc. 7th IEEE/ACS International Conference on Computer Systems and Applications* (*AICCSA'09*) (2009).

[16] Karapanos, N., Marforio, C., Soriente, C. and Čapkun, S.: Soundproof: usable two-factor authentication based on ambient sound, *Proc. 24th USENIX Conference on Security Symposium* (*SEC'15*) (2015).

[17] von Ahn, L., Maurer, B., McMillen, C., Abraham, D. and Blum, M.: reCAPTCHA: Human-Based Character Recognition via Web Security Measures, *Science*, Vol.321, pp.1465–1468 (2008).

[18] Bonneau, J. and Preibusch, S.: The password thicket: technical and market failures in human authentication on the web, *Proc. 9th Workshop on the Economics of Information Security* (*WEIS'10*) (2010).

[19] Chatterjee, R., Doerflery, P., Orgadz, H., Havronx, S., Palmer, J., Freed, D., Levyx, K., Dell, N., McCoyy, D. and Ristenpart, T.: The Spyware Used in Intimate Partner Violence, *Proc. 2018 IEEE Symposium on Security and Privacy* (*S&P'18*), pp.993–1010 (2018).

[20] Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J.P., Shelton, M., Manthorne, C., Churchill, E.F. and Consolvo, S.: Stories from Survivors: Privacy & Security Practices when coping with Intimate Partner Abuse, *Proc. 2017 ACM SIGCHI Conference on Human Factors in Computing Systems* (*CHI'17*), pp.2189–2201 (2017).

[21] Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N.: "A Stalker's Paradise": How intimate Partner Abusers Exploit Technology, *Proc. 2018 ACM SIGCHI Conference on Human Factors in Computing Systems* (*CHI'18*), No.667 (2018).

[22] Dreßing, H., Bailer, J., Anders, A., Wagner, H. and Gallas, C.: Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims, *Cyberpsychology, Behavior, and Social Networking*, Vol.17, No.2 (2014).

[23] Lyndon, A., Bonds-Raacke, J. and Cratty, A.D.: College students' Facebook stalking of ex-partners, *Cyberpsychology, Behavior, and Social Networking*, Vol.14, No.12 (2011).

[24] Harbach, M., Zezschwitz, E.V., Fichtner, A., Luca, A.D. and Smith, M.: It's a hard lock life: a field study of smartphone (un)locking behavior and risk perception, *Proc. 10th USENIX Conference on Usable Privacy and Security* (*SOUPS'14*), pp.213–230 (2014).

[25] Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S. and Wagner, D.: Are you ready to lock? Understanding User Motivations for Smartphone Locking Behaviors, *Proc. 2014 ACM SIGSAC Conference on Computer and Communications Security* (*CCS'14*), pp.750–761 (2014).

[26] Muslukhov, I., Boshmaf, Y., Kuo, C., Technologies, V., Lester, J. and Beznosov, K.: Know your enemy: The risk of unauthorized access in smartphones by insiders, *Proc. 15th International Conference on Human-computer Interaction with Mobile Devices and Services* (*MobileHCI'13*), pp.271–280 (2013).

[27] Usmani, W.A., Marques, D., Beschastnikh, I., Beznosov, K., Guerreiro, T. and Carriço, L.: Characterizing Social Insider Attacks on Facebook, *Proc. 2017 ACM SIGCHI Conference on Human Factors in Computing Systems* (*CHI'17*), pp.3810–3820 (2017).

[28] Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I. and Beznosov, K.: Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones, *Proc. 2019 ACM SIGCHI Conference on Human Factors in Computing Systems* (*CHI'19*) (2019).

[29] Amazon: Amazon Mechanical Turk (2005), available from ⟨https://www.mturk.com/⟩ (accessed 2019-06-14).

[30] OWASP: Authentication Cheat Sheet (Cheat Sheet Series), available from ⟨https://www.owasp.org/index.php/Authentication_Cheat_Sheet⟩ (accessed 2019-09-17).

[31] OWASP: ASVS (Application Security Verification Standard Project), available from ⟨https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project⟩ (accessed 2019-09-17).

[32] Lu, B., Zhang, X., Ling, Z., Zhang, Y. and Lin, Z.: A Measurement Study of Authentication Rate-Limiting Mechanisms of Modern Websites, *Proc. 34th Annual Computer Security Applications Conference* (*ACSAC'18*), pp.89–100 (2018).

[33] Bortz, A., Boneh, D. and Nandy, P.: Exposing private information by timing web applications, *Proc. 16th International Conference on World Wide Web* (*WWW'07*), pp.621–628 (2007).

[34] Schrittwieser, S., Fruhwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M. and Weippl, E.: Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications, *Proc. 19th Annual Network & Distributed System Security Symposium* (*NDSS'12*) (2012).

[35] Wondracek, G., Holz, T., Kirda, E. and Kruegel, C.: A Practical Attack to De-anonymize Social Network Users, *Proc. 2010 IEEE Symposium on Security and Privacy* (*S&P'10*), pp.223–238 (2010).

[36] Balduzzi, M., Platzer, C., Holz, T., Kirda, E., Balzarotti, D. and Kruegel, C.: Abusing Social Networks for Automated User Profiling, *Proc. 13th International Symposium on Recent Advances in Intrusion Detection* (*RAID'10*) (2010).

[37] Venkatadri, G., Andreou, A., Liu, Y., Mislove, A., Gummadi, K.P., Loiseau, P. and Goga, O.: Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface, *Proc. 2018 IEEE Symposium on Security and Privacy* (*S&P'18*) (2018).

[38] Watanabe, T., Shioji, E., Akiyama, M., Sasaoka, K., Yagi, T. and Mori, T.: User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts, *Proc. 3rd IEEE European Symposium on Security and Privacy* (*EuroS&P'18*) (2018).

[39] Perito, D., Castelluccia, C., Kaafar, M.A. and Manils, P.: How unique and traceable are usernames?, *Proc. 11th International Conference on Privacy Enhancing Technologies* (*PETS'11*), pp.1–17 (2011).

[40] Arikewuyo, A.O., Eluwole, K.K. and Özad, B.: Influence of Lack of Trust on Romantic Relationship Problems: The Mediating Role of Partner Cell Phone Snooping, *Psychological Reports* (*in press*) (2020).

[41] Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T. and Dell, N.: "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence, *Proc. ACM on Human-Computer Interaction*, Vol.3, No.CSCW, Article 202 (2019).

[42] Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N. and

Ristenpart, T.: Clinical Computer Security for Victims of Intimate Partner Violence, *Proc. 28th USENIX Security Symposium* (*USENIX Security'19*) (2019).

Appendix

A.1 Questionnaire (Exploratory User Study)

Among online services, are there any that you would feel uncomfortable if other people find out that you have an account on? Please select the appropriate categories of such services from the following choices (multiple choices allowed).
If the category you are looking for is missing from the list, please select "Other" and specify the services categories/names.
We would also appreciate it if you could give us the specific names of the services which you have chosen the categories for.

[Notes]

Please assume that other people can only find out whether or not you have an account on the service but cannot find out specific details such as how you use that service.
You are also allowed to answer about services you do not have an account on.

- □ Career change
  Service names [ ]
- □ Cloud storage
  Service names [ ]
- □ Dating
  Service names [ ]
- □ Financial
  Service names [ ]
- □ Forum
  Service names [ ]
- □ Healthcare
  Service names [ ]
- □ Porn
  Service names [ ]
- □ Shopping
  Service names [ ]
- □ Social networking
  Service names [ ]
- □ Other
  Service categories or names [ ]
- □ Never

A.2 Questionnaire (User Study to Understand Users Expectations)

The purpose of this survey is to investigate users' usage of online services and perceptions about Internet privacy. This survey consists of 9 questions, some of which are descriptive, and can be done by anyone. We're going to give a bonus ($1) to those who answer in detail.

Question 1
How old are you? [ ]

Question 2
What is your gender?

- ○ Male
- ○ Female
- ○ Other
- ○ Prefer not to say

Question 3
How many online service accounts do you have?
Include: Online services you don't use anymore but haven't deleted your account on.
Exclude: Online services you have already deleted your account on.

- ○ 0–9
- ○ 10–19
- ○ 20–29
- ○ 30–39
- ○ 40–49
- ○ 50–59
- ○ 60–69
- ○ 70 or more

Question 4
Among online services, are there any that you would feel uncomfortable if other people find out that you have an account on? Please select the appropriate categories of such services from the following choices (multiple choices allowed).

[Notes]

Please assume that other people can only find out whether or not you have an account on the service but cannot find out specific details such as how you use that service.
You are also allowed to answer about services you do not have an account on.

- □ Career change
- □ Cloud storage
- □ Dating
- □ Financial
- □ Forum
- □ Healthcare
- □ Porn
- □ Shopping
- □ Social networking
- □ Other
  Service categories [ ]
- □ Never

Question 5
Have you ever wanted to know if someone, whose email address you know, has an account on some online services?
Exclude the case(s) where you have wanted to identify their account names or find out how they use the service(s).

- ○ Yes
  Whose information have you ever wanted to know? And why? Please specify. (If you do not mind) [ ]
- ○ No

Question 6
Answer this question only if you answered "Never" to Question 4.
Do you have any concerns about your privacy on online services?

- ○ Yes
  Please specify about the concerns. [ ]

○ No
Please specify what you think about your privacy on online services. [ ]

Question 7

Answer this question only if you answered anything except "Never" to Question 4.

You answered that there some online services that you would feel uncomfortable with other people finding out you have an account on.

Who would you feel uncomfortable with finding out that you have an account on the service(s)?

□ Partner (e.g., your wife, husband, girlfriend, boyfriend)
□ Family except for your partner
□ Friends (who you have met in real)
□ On-line friends (who you haven't met in real)
□ Acquaintances
□ Co-workers
□ Bosses
□ Employers
□ Other
Please specify. [ ]

And why would you feel uncomfortable with them finding out?
Please specify. (If you do not mind) [ ]

Question 8

Answer this question only if you answered anything except "Never" to Question 4.

How do you create accounts on such sensitive online services?

8.1 Login ID or contact information (email address)

○ I register the same email address as on non-sensitive services, which anyone who knows me may know.
○ I register the same email address as on non-sensitive services, which no one who knows me knows.
○ I register different email address(es) from those on non-sensitive services, one of which anyone who knows me may know.
○ I register different email address(es) from those on non-sensitive services, none of which anyone who knows me knows.
○ Other
Please specify. [ ]

8.2 Password

○ I set weaker passwords than on non-sensitive services.
○ I set the same passwords as on non-sensitive services.
○ I set passwords of similar strength to those on non-sensitive services.
○ I set stronger passwords than on non-sensitive services.
○ Other
Please specify. [ ]

Question 9

Do you delete online service accounts when you no longer use them?

Please select the most appropriate choice.

○ I always delete accounts.
○ I often delete accounts.
○ I occasionally delete accounts.
○ I never delete accounts and leave them open.

A.3 Types of User IDs and Required Information

Table A·1, which shows the details of Table 3, shows types of user IDs used on 109 candidates of sensitive and popular services in our measurement study. About one third of the services permit users to use several types of user ID (Type (II), (IV), and (V)).

In our measurement study (Section 4), we examined 87 services permitting email addresses as user ID (Type (I), (II), (IV), and (V).) In addition, among 21 services permitting only usernames as user IDs (Type (III)), 12 selected services are examined in Appendix A.6.

Many services required various kinds of user personal information other than the information used as the user ID for account creation. **Table A·2** shows required personal information for account creation on 109 candidate services. Note that we did not count the information if entering it was optional. Almost all services (94.0% of sensitive and 91.1% of popular services) require a user email address as contact information. **Table A·3** shows required information for password recovery. Almost all services also require email addresses for password recovery. These results indicate that an attacker can perform our attack on password recovery and account creation functions by using a target's email

Table A·1 Types of user IDs used on online services.

Type	Email	Username	Phone	% Services
(I)	✓			49.5% (54/109)
(II)	✓	✓		22.9% (25/109)
(III)		✓		19.3% (21/109)
(IV)	✓		✓	5.5% (6/109)
(V)	✓	✓	✓	1.8% (2/109)
(VI)			✓	0.9% (1/109)
	79.8% (87/109)	44.0% (48/109)	8.3% (9/109)	100.0% (109/109)

Table A·2 Required information for account creation.

Information	Sensitive (N = 84)	Popular (N = 45)
Email address	94.0%	91.1%
Name	46.4%	42.2%
Username	45.2%	46.7%
Birth date or age	44.0%	40.0%
Location	40.5%	20.0%
Gender	35.7%	15.6%
Phone number	10.7%	13.3%
Language	4.8%	4.4%
Secret question	2.4%	2.2%
Other	15.5%	0.0%

Table A·3 Required information for password recovery.

Email	Username	Phone	Others	% Services
✓				72.5% (79/109)
✓	✓			15.6% (17/109)
✓		✓		6.4% (7/109)
✓	✓	✓		2.8% (3/109)
		✓		0.9% (1/109)
✓✓	✓✓			0.9% (1/109)
	✓✓		✓✓	0.9% (1/109)
98.2% (107/109)	20.2% (22/109)	11.0% (12/109)	0.9% (1/109)	100% (109/109)

Single checkmarks: required any one of the marked information
Double checkmarks: required both of the marked information

Table A·4 Details of our dataset (sensitive services).

Category	#	Alexa ranking					% Included in popular dataset
		1–100	101–1,000	1,001–10,000	10,001–100,000	100,001–	
Dating	14	0.0%	7.1%	35.7%	50.0%	7.1%	0.0%
Porn	10	30.0%	10.0%	20.0%	30.0%	10.0%	30.0%
Social networking	9	66.7%	0.0%	11.1%	22.2%	0.0%	66.7%
Career change	9	11.1%	22.2%	55.6%	0.0%	11.1%	11.1%
Forum	7	14.3%	0.0%	14.3%	28.6%	42.9%	14.3%
Financial	4	0.0%	25.0%	50.0%	0.0%	25.0%	0.0%
Shopping	7	28.6%	42.9%	0.0%	28.6%	0.0%	28.6%
Healthcare	5	0.0%	0.0%	20.0%	0.0%	80.0%	0.0%
Cloud storage	4	75.0%	25.0%	0.0%	0.0%	0.0%	100.0%
Total (Sensitive)	69	23.2%	13.0%	24.6%	23.2%	15.9%	24.6%

Table A·5 The number of the collected messages in our measurement study.

Step		# Service	# Functions	# Messages
Step–1	Web	87	3	261
	Mobile	63	3	189
Step–2	Web	87	3	261
	Mobile	63	3	189
Step–3	Web	40	3	120
Step–4	Web	42	3	126
Total				1146

address regardless of types of user IDs.

A.4 Details of Our Dataset

Table A·4 shows the details of the dataset (69 sensitive services) for our measurement study. It consists of the services that our participants mentioned in our exploratory user study. Alexa ranking of these services widely spreads: top 1–100 (23.2%), 101–1,000 (13.0%), 1,001–10,000 (24.6%), 10,001–100,000 (23.2%), and more than 100,001 (15.9%). Most services in the social networking and cloud storage categories are also included in the popular services dataset.

A.5 Collected Messages in Our Measurement study

In our measurement study (Section 4), we collected login-related messages through four steps as shown in Fig. 2. **Table A·5** shows a breakdown of the number of collected messages in each step. We collected 1,164 messages in total.

A.6 Feasibility of Our Account-existence Attack on Non-Email User ID Services

In Section 4, we discussed online services permitting email addresses as user IDs. In this section, we further discuss the feasibility of our account-existence attack regarding usernames and phone numbers.

A.6.1 Username

About 20% of the candidates permit only usernames as user IDs as shown in Table A·1. Thus, we further examined messages of password-recovery and account-creation functions on these services with our signaling email address because these two functions probably require email addresses for contact information even though email addresses are not user IDs. We randomly selected 12 services permitting only usernames as user IDs. When collecting the account-creation messages on these services with our signaling email address, we input an unregistered username, an arbitrary incorrect password that satisfies the password-composition policy, and arbitrary personal information that satisfies format validity. As a result, we found that 50.0% (6/12) of these services were insecure, i.e., at least one function (password recovery or account creation) was insecure.

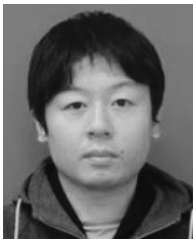
Furthermore, if an attacker knows a target's username on sensitive services, e.g., the target reuses the same username on social networking services (usernames are often open to the public) and sensitive services, an attacker could use the username as a user ID for our account-existence attack. According to Perito et al. [39], users tend to reuse the same or similar usernames among multiple services.

A.6.2 Phone Number

In 8.3% (9/109) of the candidates, phone numbers are permitted to be used as user IDs; only 0.9% (1/109) of the candidates mandated only phone numbers as user IDs. Although we actually did not examine login-related functions with a *signaling* phone number, a phone number could be used for our attack as a User ID instead of an email address if an attacker knows the target's phone number.

Ayako Akiyama Hasegawa received her B.S. and M.S. degrees in information science from Ochanomizu University in 2013 and 2015, respectively. She also received her B.S. degree in human science from Musashino University in 2019. She is currently a researcher at NTT Secure Platform Laboratories, Tokyo, Japan. Her current research interests are mainly on usable security and privacy.

Takuya Watanabe recieved M.E. degree in computer science and engineering from Waseda University, Japan in 2016. Since joining Nippon Telegraph and Telephone Corporation (NTT) in 2016, he has been engaged in research of consumer security and privacy. He is now with the Cyber Security Project of NTT Secure Platform Laboratories.



Eitaro Shioji received his B.E. degree in Computer Science and M.E. degree in Communications and Integrated Systems from Tokyo Institute of Technology in 2008 and 2010, respectively. Since joining Nippon Telegraph and Telephone Corporation (NTT) in 2010, he has been engaged in research and development on computer security. His research interests include systems and software security, binary analysis, and reverse engineering.

Mitsuaki Akiyama received his M.E. and Ph.D. degrees in information science from Nara Institute of Science and Technology, Japan in 2007 and 2013. Since joining Nippon Telegraph and Telephone Corporation (NTT) in 2007, he has been engaged in research and development on cybersecurity. He is currently a Senior Distinguished Researcher with the Cyber Security Project of NTT Secure Platform Laboratories. His research interests include cybersecurity measurement, offensive security, and usable security and privacy.

Tatsuya Mori is currently a professor at Waseda University, Tokyo, Japan. He received B.E. and M.E. degrees in applied physics, and Ph.D. degree in information science from the Waseda University, in 1997, 1999 and 2005, respectively. He joined NTT lab in 1999. Since then, he has been engaged in the research of measurement and analysis of networks and cyber security. From Mar 2007 to Mar 2008, he was a visiting researcher at the University of Wisconsin-Madison. He received Telecom System Technology Award from TAF in 2010 and Best Paper Awards from IEICE and IEEE/ACM COMSNETS in 2009 and 2010, respectively. Dr. Mori is a member of ACM, IEEE, IEICE, and IPSJ.