Impact Assessment of Password Reset PRMitM attack with Two-factor Authentication

Kota Sasa
Graduate School of Advanced Mathematical Sciences, Meiji University, Japan.

Hiroaki Kikuchi
School of Interdisciplinary Mathematical Sciences, Meiji University, Japan.

***Abstract*—In 2017, Gelernter et al. identified the "password-reset man-in-the-middle" attack, which can take over a user's account during two-factor authentication. In this attack, a password reset request is sent via an SMS message instead of an expected authentication request, and the user enters a reset code at the malicious man-in-the-middle website without recognizing that the code resets the password. Following this publication, most vulnerable websites attempted to remove the vulnerability. However, it is still not clear whether these attempts were sufficient to prevent careless users from being attacked. In this paper, we describe the results of an investigation involving domestic major websites that were vulnerable to this type of attack. To clarify the causes of vulnerability, we conducted experiments with 180 subjects. The SMS-message parameters were "with/without warning", "numeric/alphanumeric code", and "one/two messages", and subjects were tested to see if they input the reset code into the fake website. We report on the successful-attack ratios and the behavior of subjects.**

***Index Terms*—two-factor authentication, PRMitM**

I. Introduction

The most widely used user-authentication method involves passwords. Secret passwords or passphrases linked to a user's account help to prevent intruders from taking control of the user's resources. However, password-based authentication has some known vulnerabilities. The first problem is the reuse of passwords. According to Das et al [1], 43–51% of users reuse the same password for multiple services. Ur et al. [2] reported that most users react positively to the reuse of password. The average user prefers very simple passwords to avoid being compromised [3]. The second problem involves forgotten passwords. Users are more likely to forget a complicated password, even though it is known to be more secure. Yans [4] reported that 65% of users are apt to forget their passwords. Consequently, system providers need to provide recovery mechanisms for those who somehow forget their password.

Two-factor authentication (2FA) is the most popular method of recovering a forgotten password. Users are authenticated by combining multiple factors such as "what they know" and "what they have". If a user requests a password reset, the service provider will typically send a message via email to confirm that the user really requested the password reset. This does not work for those who forget not only the service's password but also the password to be used for email. Therefore, as a widely used alternative, 2FA can send the confirmation message via SMS to the phone number submitted to the service provider when enrolling in the service. In general, smartphones offer useful and secure access to Internet-based applications.

However, in 2017, Gelernter et al. [5] identified a vulnerability called the password-reset man-in-the-middle (PRMitM) attack. This can take over a user's account via an SMS-based password-reset process. In this type of "man-in-the-middle attack", the victim is convinced that the SMS message is simply a confirmation of a new registration sent from the attacker's website. However, it is actually a confirmation of a password reset for the target service account. If the victim enters the code contained in the SMS message, the account can be reset and be taken over by the attacker.

After the publication of Gelernter et al.'s work, many vulnerable websites fixed the password-reset mechanism, aiming to prevent such PRMitM attacks. However, we claim that some websites have not yet warned users sufficiently and the risk of suffering a PRMitM attack remains. Our investigation of the top 200 websites revealed that 17 websites were vulnerable to PRMitM attacks with significant probability and that 12 websites included no warning in the SMS message. Moreover, to make countermeasures effective, we should also consider human factors such as demographic properties (age, sex), knowledge (IT literacy, security skill), and individual characteristics (careful, lazy, or optimistic). For example, some users do not pay sufficient attention to warning messages and are more easily compromised by a PRMitM attack. It is therefore important to clarify which warning methods are effective in preserving the security of a website.

In this paper, we address issues related to PRMitM attacks. First, we investigated some major websites to check if the website was vulnerable to PRMitM attacks. Second, we conducted a user case study with about 180 demographically diverse subjects. This involved the use of "toy" websites that could send fake SMS-based password-reset messages, thereby clarifying which people and factors are most effectively targeted by PRMitM attackers. The main objective of our study is to clarify the most significant human factors and SMS attributes for successful-attack strategies.

Our contributions are as follows.

1) *Investigate the PRMitM vulnerability of major websites.* We compile statistics for potentially vulnerable websites and estimate the impact of an attack based on our analysis and available information.

2) *Evaluate significant human factors in a vulnerability to PRMitM attacks.* With about 180 subjects, our user study identifies new relationships between human characteristics and the risk of being compromised. For example, we found that some groups of subjects who update their passwords very frequently are more likely to be compromised by PRMitM attacks. From our epidemiological analysis, the odds ratio of risk of PRMitM attack is 11.59 times higher than for those who do not update passwords so often.
3) *Explore effective SMS factors that prevent a risk of being compromised by PRMitM attacks.* For example, the appearance of a reset code comprising only alphabetic or only numeric characters increases the risk of being compromised by a factor of 1.86.

The remainder of our paper is organized as follows. In Section II we define the fundamental notions of 2FA and PRMitM. We highlight several security threats in the password-reset sequence in Section III. The results of our investigation of major websites with respect to PRMitM attack are reported in Section IV. In Section V, we describe our human-factor experiments involving 180 subjects. Section VI evaluates the risks of being compromised by PRMitM attacks and estimates the impact of an attack based on our experimental results. We offer conclusions in Section VII.

II. PRMITM ATTACK

A. 2FA

2FA is an authentication method that combines biometric, device, and/or other information with a password. For example, with password generators for Internet banking, we are often required to use a one-time password generator, in addition to account and password information. The most popular method involves the use of a phone-based SMS rather than a dedicated password-generator device. 2FA is believed to offer enhanced security. However, in some situations, it may actually increase the risk of being compromised.

B. Reasons for being subject to an PRMitM attack

In 2017, Gelernter et al. [5] identified the PRMitM attack, which can take over a user's account by using 2FA via SMS. The PRMitM attack exploits the fact that a password-reset message can be indistinguishable from a new account-enrollment message.

Fig.1 shows an outline of a PRMitM attack. User A has an account A on target website C. The attacker makes a fake website that requires 2FA. User A registers his phone number with user information into the attacker's website B. The attacker requests a password reset to website C using the phone number of user A. The corresponding account A's reset code is sent to user A via SMS from target website C, requesting a reset-code input from A. User A believes that it is the genuine code for registering on website B. Therefore, user A enters the reset code, enabling user A's account to be stolen. User A is not even aware of having been attacked.

TABLE I
EXAMPLES OF VULNERABLE RESET CODES VIA SMS [5]

Site	SMS text
(1) Yandex	Your confirmation code is XXXXXX. Please enter it in the text field.
(2) Linkedin	Your LinkedIn verification code is XXXXXX

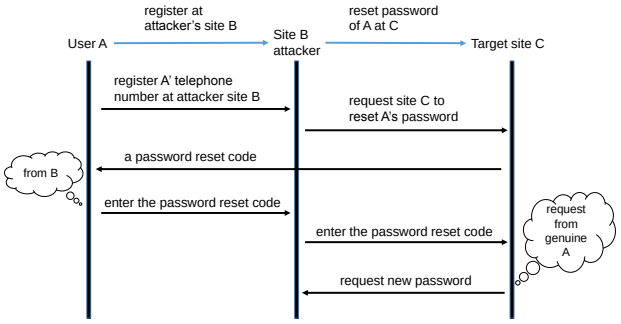

Fig. 1. Illustration of a basic PRMitM attack

Gelernter et al. suggested three reasons for PRMitM vulnerability:

1) no service name specified in the SMS message;
2) no warning accompanying the password-reset request;
3) no secret question.

Table I shows examples of SMS messages used in the past. In Example (1), the sender of the SMS is unknown. In (2), the user does not know why the SMS has been sent. In (3), the attacker does not use a valid phone number but uses the same secret question as the target website. Gelernter et al. conducted experiments to investigate the effects of PRMitM attacks on 536 subjects. The findings were as follows:

1) 90.5% of users read only the reset code itself;
2) users were convinced that the attacker's website was chained to the target website if they noticed a company name
3) 79.5% of users input the reset code even if the SMS contained a warning message.

Gelernter et al. suggested that the password-reset SMS should specify the service-provider name and a warning about PRMitM attacks, encouraging users to check if the code is for a password reset. They also recommended using a URL for password reset instead of an SMS reset code. If the attacker then tries to make the user reset the password by requiring the user to enter a URL, this could appear suspicious and would be less likely to invoke the PRMitM attack.

C. Security Behavior Intentions Scale (SeBIS)

SeBIS is a survey to measure security knowledge and behavior proposed by Egelman et al. [6]. In our study, we

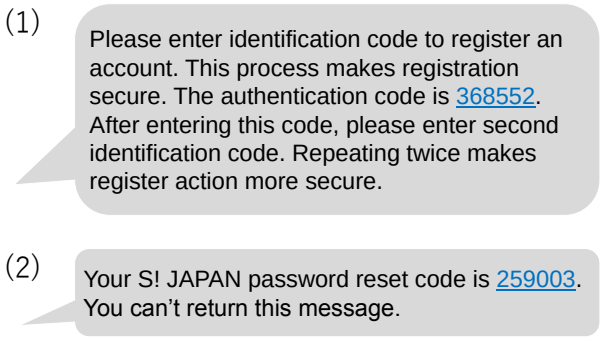

Fig. 2. Basic long SMS attack

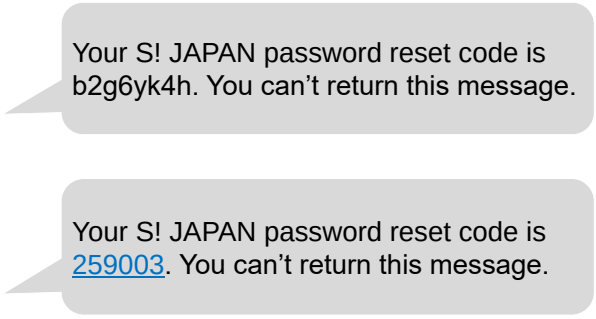

Fig. 3. Alphanumeric and numeric codes

replaced negative questions by their positive equivalents when the original questions were translated into Japanese. Table X lists the modified SeBIS questions.

III. Potential Risks

A. Human elements

Vulnerability to PRMitM attacks depends on individual characteristics [7] [8]. For example, users who lack security knowledge or do not read their SMS messages carefully are likely to be vulnerable to PRMitM attacks. Gelernter et al. [5] did not consider the effect of human factors, user profiles, or SMS-reading behavior on attack vulnerability. In particular, the attack-success ratio will depend on both users' security knowledge and their care in reading SMS messages. In this study, we examine the potential risk of PRMitM attack in terms of security knowledge and SMS-related behavior.

B. Long SMS attacks

Users are not able to read and understand messages that are very long [9]. A *long SMS attack* exploits this aspect of user behavior. In a long SMS attack, the victim is forced to read a long message and enter a code several times. Given multiple messages, a user might carelessly read a second input message and type a code because the second procedure seems to be the same as the first [10], enabling account A to be hacked. Fig.2 shows an SMS message used in such an attack. User A enters the code in (1), sent by attacker B, to register on attacker's website B. Next, (2) is a message sent from target website C via attacker B's request. User A inputs the code without noticing the service name. Furthermore, message (1) and the subsequent message (2) are not displayed on the same screen, which makes it difficult to distinguish the two messages.

C. Numeric authentication code

The iPhone OS and some versions of Android OS automatically recognize continuous numbers as phone numbers and present the numbers as a link. Fig.3 shows alphanumeric and numeric codes. The former is more secure because the alphanumeric reset code is not emphasized as a link [11].

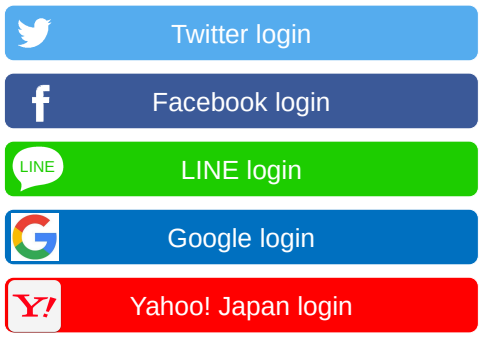

Fig. 4. example of login for OpenID registration (nikoniko douga)

D. ID connections

ID federations such as openID [12] (see Fig. 4 "nikoniko douga") are vulnerable to PRMitM. Attacker B plays the role of the relying party in an ID federation attack on user A, pretending to be website C of the ID provider. Here, account A can receive the reset code and be taken over.

E. Link-via-SMS (LVS)

The countermeasure of replacing the SMS by a URL reset, as proposed by Gelernter et al., has these problems:

1) short URLs cannot easily be judged as genuine or fake;
2) we cannot check the SMS sender from the SMS message;
3) a URL code can be a new phishing target for LVS.

Therefore, we argue that LVS should not be used as a substitute for the SMS password-reset code.

IV. Investigation of Major Domestic Websites

A. Purpose

We investigated major Japanese domestic websites with respect to PRMitM vulnerability and assessed the feasibility of PRMitM attacks via these websites.

TABLE II
TOP 200 WEBSITE STATISTICAL INFORMATION

No account	27					
Available account	173	No SMS	145			
		Available SMS	28	No warning	15	Yahoo JAPAN
				warning	12	Twitter
				URL	1	Instagram
Total	200					

TABLE III
SERVICE NAME AND TEXT OF SMS MESSAGES CONTAINING NO WARNING

Name	Alexa rank	SMS message
Google	1	G-910957 is your Google verification code.
Yahoo JAPAN	4	Verification code : 375403 Please enter the code. Yahoo! JAPAN
Amazon	5	Your Amazon verification code is160973.
LinkedIn	63	LinkedIn verification code is 「123512」

B. Method

We investigated the top 200 websites of Alexa Japan [13] from August 18th to December 13th, 2017. We tested websites by using the following three-item check sheet.

1) Is account registration available?
2) Is password reset via SMS used?
3) Is a warning given if the SMS specifies a password reset.

C. Results

Table II shows the investigation result. There were no websites that omitted the service name. However, there were 17 websites that offered an SMS password reset without warning (omitting duplicates, there were four such websites). Table III shows the service name and text of SMS messages containing no warning.

There were 11 websites that did not offer user registration.

D. Disscussion

In the survey results, there were 15 websites that omit warnings. For example, Yahoo! JAPAN [14] does not register a phone number when creating an account. If users want to register a phone number, they need to add it after registration. Amazon does not register phone numbers in the absence of an application dedicated to smartphones. Twitter and Facebook enable account creation using a phone number, however these SMS message is written a warning. Therefore, it is not the case that using SMS messages without warnings is necessarily vulnerable.

V. USER EXPERIMENTS ON POTENTIAL RISK

A. Purpose

These experiments aimed to clarify the behavior of users when entering a password-reset code.

B. Method

In these experiments, the subjects registered with toy websites and received SMS messages about their registration. The subjects were enrolled via the crowdsourcing service "CrowdWorks" [15]. Table IV shows the ages and sex of the subjects. To send an SMS message, we used a programmable SMS service from twilio [16]. The subjects' attributes included a name, a password, and a phone number. There were four toy websites for registration. Whenever a code request was received via SMS, the subjects were allowed to cancel their registration if they were suspicious. The experimental websites were set up using our laboratory server with TLS.

Fig. 5. Registration screen in experiment (1)

Subjects were requested to register for the four toy websites listed in Table VI The experiment compromised the following steps;

1) User registration (Fig. 5 shows this input screen).
2) Users were required to choose "enter" or "cancel" after receiving an SMS verification code.
3) A set of subjects was divided into five groups and SMS messages were sent according to Table VII ("warning", "numeric", and "alphanumeric" were defined in Section III).The long SMS group received two SMS messages. After the first SMS, a type 1 or type 2 SMS was sent.
4) The websites have the same contents but different communication.

Each time a subject accessed a toy website, they answered the two questions shown in Table V. The sender company name was included in all SMS messages. After finishing all tasks, subjects responded to the SeBIS survey.

For these experiments, we set type 0 as the baseline condition. In terms of the vulnerability ratio, any significant difference between type 1 and type 2 (or between type 3 and type 4) must be caused by the difference between entering numeric and alphanumeric codes. Similarly, any significant difference between type 1 and type 3 (or between type 2 and type 4) implies that a long SMS attack is a practical threat. To assess how carefully subjects read SMS messages when entering reset codes, we measured the response times.

C. Experimental results

Table VIII gives the experiment results. A successful attack ratio is defined as the proportion of subjects who allows the

TABLE IV
AGE AND SEX OF SUBJECTS

	Male	Female
Under 20 years old	1	2
20's	32	32
30's	25	39
40's	21	16
50 years and over	11	5
Total	90	94

TABLE V
AVERAGES FOR USABILITY AND SECURITY

	Question1 usability	Question2 security
(1) S! Japan	5.98	4.14
(2) Cowtter	5.83	5.03
(3) Majebook	5.19	4.64

attacker to reset password, i.e.,

$$R_x = \frac{\text{number of vulnerable users for } x}{\text{population of } x}$$

Let x and R_x be a type of SMS in Table VII and the sccessful ratio in x, respectively. For example of attack, we have the successful attack ratio for type1 as B in (3).

$$R_{type1} = \frac{30}{38}$$

To summarize the effect of the type of SMS on the successful-attack ratio, Table VIII shows the conditions for each inspected item.

shows the results and reasons for cancellation of registration. Fig. 6 shows the distribution of the response times when choosing "enter" or "cancel". Because types 3 and 4 involve two inputs, they take longer than types 0, 1, or 2. Table X shows the SeBIS results for "enter" or "cancel" in a (3) attack. Fig. 7 shows the SeBIS total score.

TABLE VI
REGISTRATION EXPERIMENT WEBSITES AND MEASUREMENT PURPOSES

	(1)	(2)	(3)(Attack)	(4)
Name	S! JAPAN	Cowtter	Majebook	Mstagram
Operation	N/A	Cowtter verification code	S! JAPAN reset code	Mstagram verification code
Purpose	Registration practice	SMS practice	Investigation of factors for password reset	Survey of the impact of SSL

TABLE VII
TYPE OF PASSWORD RESET CODE

type	Warning	Number	Alphanumeric	Long	Subjects
0	√	×	√	√	37
1	×	×	√	√	38
2	×	√	×	√	40
3	×	×	√	×	35
4	×	√	×	×	34

TABLE VIII
SUCCESSFUL ATTACK RATIO FOR EACH TYPE

type	SMS	Enter	Cancel	Successful attack ratio[%]
0	No warning	35	2	94.6
1	Short Numeric	30	8	78.9
2	Short Alphanumeric	28	12	70.0
3	Long Numeric	28	7	80.0
4	Long Alphanumeric	22	12	64.7

TABLE IX
REASON FOR CANCELLATION

Reason	number of people
I did not understand the mechanism well.	10
Written as S! JAPAN	14
Written as password reset	16
The first SMS was long	1

D. Ethics

In our experiments, we used only experimental purpose ("toy") websites and at no time did we attack real websites. Before participating in the experiments, the subjects consented to the acquisition of their personal information (see Appendix).

For these experiments, we obtained the subjects' phone numbers and outsourced the sending of SMS messages [16] with the subjects' agreement. Consequently, we did not compromise any of the policies of CrowdWorks.

VI. EVALUATION

A. Effects of human elements

We set up the null hypothesis as "the vulnerable websites are independent of condition x" and performed chi-squared tests of one degree of freedom to check whether differences under various conditions were statistically significant. Table XI shows the results, where * and *** indicate p $<$0.1 (significance level 10%) and p $<$0.01 (significance level 1%), respectively. There was a significant difference (p = 0.09 $<$0.1) between type 0 and type 1, i.e., we recognize that warnings affect password-reset attack ratios. Using alphanumeric codes

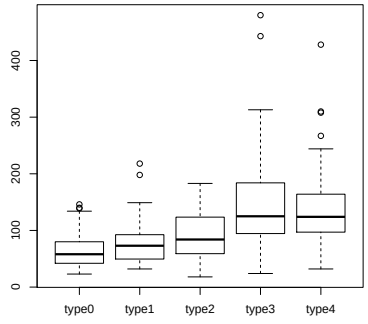

Fig. 6. Distribution of answer times for each type

TABLE X
SEBIS INDEX

Number	Questions	μ	σ
1	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.44	1.745
2	I use a password/passcode to unlock my laptop or tablet.	3.97	1.583
3	I manually lock my computer screen when I step away from it.	2.65	1.580
4	I use a PIN or passcode to unlock my mobile phone.	3.38	1.823
5	I change my passwords frequently	2.30	0.932
7	I use different passwords for different accounts that I have.	3.01	1.302
8	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	3.51	1.534
9	I include special characters in my password except prohibited.	1.89	1.108
10	When someone sends me a link, I don't open it without first verifying where it goes.	3.61	1.206
11	I know what website I'm visiting by looking at the URL bar, rather than its look and feel.	2.72	1.115
12	I never submit information to websites unless first verifying that it will be sent securely (e.g., SSL, " https:// ", a lock icon).	3.18	1.261
13	When browsing websites, I mouse overs links to see where they go, before clicking them.	2.93	1.233
14	If I discover a security problem, I stop what I was doing.	3.52	1.135
15	When I'm prompted about a software update, I install it right away.	3.52	1.141
16	I try to make sure that the programs I use are up-to-date.	3.21	1.137
18	I verify that my anti-virus software has been regularly updating itself.	3.49	1.292
Total		50.3	10.314

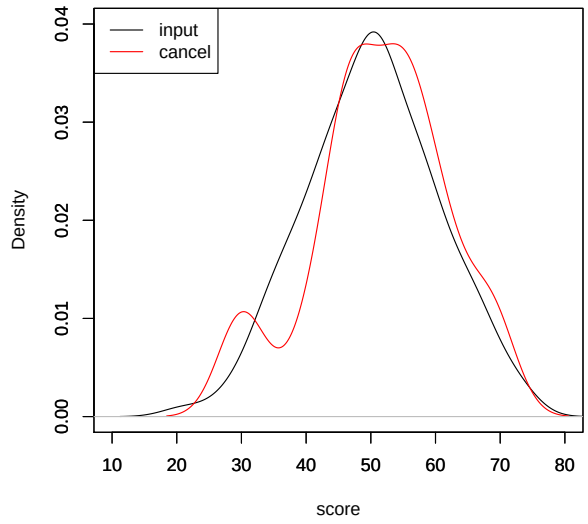

Fig. 7. SeBIS score distribution for security orientation and successful attack ratios of subjects who either cancel or input

reduced the successful-attack ratio, but there was no significant difference between numeric and alphanumeric (p = 0.14 >0.1). Nor was there a significant difference between long SMS and short SMS (p = 0.94 >0.1). On the other hand, there was a significant difference between http and https access (p <0.001), which demonstrates that users can clearly recognize a difference between http and https.

1) Differences between "enter" and "cancel": Table XII shows the successful-attack ratio R for reset attacks with various user attributes. The ratio is distributed between 70% and 80%. The highest R rate is for those subjects aged 50 years and over and forgetting to register with Facebook. It could be that they do not really understand the risks involved or how entering a reset code works.

TABLE XI
SUCCESSFUL ATTACK RATIOS BY SMS TYPE

type		Enter	Cancel	Successful attack ratio[%]	χ	P value
0	No warning	35	2	94.6	2.7333	0.09828*
1	Warning	30	8	78.9		
1+3	Number	58	15	79.5	2.088	0.1485
2+4	Alphanumeric	50	24	67.6		
1+2	Short	50	19	72.5	0.0053	0.9421
3+4	Long	58	20	74.4		
Enter 4	http	164	20	89.1	24.2937	8.27e-07***
Enter 2	https	124	60	67.3		

TABLE XII
SUCCESSFUL ATTACK RATIOS BY USER ATTRIBUTES

		Enter	Cancel	Total	Successful attack ratio[%]
Sex	Male	66	24	90	73
	Female	77	17	94	82
Age	Under 20 years old	2	1	3	67
	20's	48	16	64	75
	30's	50	14	64	78
	40's	27	10	37	73
	50 years and over	16	0	16	100
Did you register phone number	Yes	27	7	37	73
	No	95	31	126	75
	Forget	21	3	24	88
Did you register phone number in Facebook	Yes	41	12	53	77
	No	85	29	114	75
	Forget	17	0	17	100
Did you register phone number in Yahoo	Yes	39	7	46	85
	No	74	28	102	73
	Forget	30	6	36	83
Smartphone models	iPhone	57	17	74	77
	Android	64	16	80	80
	Others	22	8	30	73

2) SeBIS and successful attack ratio: There was no significant difference between "enter" and "cancel" with respect to SeBIS scores. The subjects' average score was 50.3. Therefore, we can regard a score of 50 as a threshold and divide subject scores by the threshold, as shown in Table XIII.

To identify the main factors in vulnerability, we performed a logistic regression analysis to derive a logistic model for which

$$\log \frac{p}{1-p} = \beta_0 + \beta_1 x_1 + \cdots + \beta_{18} x_{18}.$$

Here, the probability p is the objective variable and the explanatory variables are the SMS types (x_1, x_2, x_3), usability ($x_{1,1}$, $x_{2,1}$, $x_{3,1}$), the sense of security ($x_{1,2}$, $x_{2,2}$, $x_{3,2}$), SeBIS answers (x_{q1}, x_{q2}, $\cdots$ x_{q18}). Table XIV gives the significant results. For example, the adjusted odds ratio of damage probability for no warning($x_1 = 0$) to that with a warning($x_1 = 1$) is

$$\frac{\Pr(\text{Vulnerable} \mid \text{No warning})}{\Pr(\text{Safe} \mid \text{No warning})} = e^{\beta_1} = 0.286.$$

Note that this did not reach the level of significance. However, one interesting result was that xq5 (SeBIS Q5 "I

TABLE XIII
SUCCESSFUL ATTACK RATION FOR SEBIS SCORES

Score	Enter	Cancel	Successful attack ratio[%]
Over 50	66	21	75.9
Under 50	54	18	75.0

TABLE XIV
LOGISTIC REGRESSION ANALYSIS(A PART)

	Estimateβ	Std. Error	z value	Pr($>\|z\|$)
(Intercept) x_0	-1.68	4.64	-0.36	0.717 *
x_1	-1.25	163	-077	0.443
x_2	-3.31	1.60	-2.07	0.038 *
x_3	-4.46	1.93	-2.31	0.021 *
x_4	-4.05	1.82	-2.23	0.026 *
$x_{1,1}$	1.21	0.46	2.54	0.011 *
$x_{1,2}$	0.88	0.36	2.47	0.013 *
$x_{2,2}$	-1.35	0.45	-2.99	0.002***
$x_{3,1}$	-0.65	0.30	-2.18	0.029 *
$x_{3,2}$	1.63	0.36	4.54	5.61e-06 ***
x_{q5}	2.45	0.71	3.44	0.00058 ***
x_{q8}	-0.58	0.29	-1.97	0.048 *
x_{q10}	-0.98	0.46	-2.10	0.0362 *

change my passwords only when necessary") was significant (p = 0.00058 <0.001). This odds ratio was

$$e^{2.45} = 11.59.$$

It implies that users changing their passwords very frequently are more likely to be attacked by a factor of more than 11.6. It is conceivable that these users are less cautious after getting used to entering reset codes. SeBIS Q8 is "When I create a new online account, I try to use a password that goes beyond the website's minimum requirements". Users preferring longer passwords reduced the risk by a factor of 0.56. We found that vulnerable users tend to set minimum-length passwords. SeBIS Q10 is "When someone sends me a link, I open it after first verifying where it goes". This also reduces the risk by a factor of 0.37. We found that vulnerable users tend to click first, without verifying the link's destination.

3) The element of time: There was no difference between types 0, 1, and 2 and types 3 and 4 with respect to the time taken to enter a code. There appear to be no time effects, whether being attacked or responding to numeric or alphanumeric codes. It is conceivable that subjects read all SMS messages in just a few seconds.

B. Impact evaluation of PRMitM attacks

Impact evaluation of PRMitM attack Based on our results, we can estimate the degree to which actual service providers are vulnerable to PRMitM attacks. For example, the SMS messages from Yahoo! JAPAN contain no warning, and use a numeric reset code. In this case, the odds ratio between type 0 and type 1 is

$$\frac{35}{2} / \frac{30}{8} = 4.67.$$

TABLE XV
ATTRIBUTE DEPENDENCE ON SEBIS SCORE

		Over 50	Under 50	Total
Sex	Male	51	34	85
	Female	36	38	74
Age	Under 20 years old	2	0	2
	20's	26	19	45
	20's	31	33	64
	20's	17	17	34
	50 years and over	11	3	14
Did you register phone number in Twitter	Yes	15	13	28
	No	61	50	111
	Forget	11	9	20
Did you register phone number in Facebook	Yes	27	19	46
	No	54	48	102
	Forget	6	5	11
Did you register phone number in Yahoo	Yes	25	17	42
	No	49	38	87
	Forget	13	17	30
Smartphone models	iPhone	30	23	53
	Android	41	35	76
	Others	16	14	30

Therefore, without a warning, the risk of subjects being attacked is more than 4.67 times greater than with a warning. Yahoo! JAPAN had 36.14 million active users in September 2016 [17]. From Table XII, the proportion of subjects who registered phone numbers with Yahoo! JAPAN was about 26%, giving about 9.25 million registered phone numbers.

$$3614 \cdot 0.256 = 925.184,$$

about 9.25 million. For the case of no warning,

$$925 \cdot \frac{35}{37} = 875.$$

Therefore, there's a possibility that 8.75 million users are vulnerable. If there are warnings, we have

$$925 \cdot \frac{30}{38} = 730.3,$$

thus reducing the vulnerable cohort to 7.303 million users.

Table XV shows the attributions depend on SeBIS score.

VII. CONCLUTIONS

We examined PRMitM attacks using 2FA password-reset messages sent by SMS. We surveyed the risk of PRMitM attack on major Japanese websites and experiments were carried out to assess the potential PRMitM threat. We found that 17 of these websites used password-reset requests via SMS, with 12 websites having no warnings within such SMS messages. We found that the PRMitM risk factor was 4.6 times higher in the no-warning case, 1.86 times higher for numeric-only reset codes, and 0.91 times higher for the long SMS case. (However, the reset-code type and long SMS issue did not reach 10% significance.) We also found that users who changed their passwords very frequently were more likely to be attacked by a factor of 11.59 times. Because warnings alone do not prevent users being attacked, we should therefore consider more secure password-reset methods.

REFERENCES

[1] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The Tangled Web of Password Reuse. In Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS), 2014.

[2] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. "I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), pp. 123 – 140, 2015.

[3] A. Adams and M. A. Sasse, "Users Are Not The Enemy," Commun. ACM, vol. 42, no. 12, pp. 40 – 46, 1999.

[4] J. J. Yan, A. F. Blackwell, R. J. Anderson, and A. Grant: Password memorability and security: Empirical results, IEEE Security and Privacy, vol. 2, no. 5, pp. 25 – 31, 2004.

[5] Nethanel Gelernter, Senia Kalma, Bar Magnezi, Hen Porcilan: The Password Reset MitM Attack, IEEE Security and Privacy 2017

[6] Serge Egelman, Eyal Peer: Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS), SIGCHI Conference on Human Factors in Computing Systems (CHI' 15).

[7] Joireman, J., Shaffer, M. J., Balliet, D., and Strathman, A. Promotion orientation explains why future-oriented people exercise and eat healthy evidence from the two-factor consideration of future consequences-14 scale. Personality and Social Psychology Bulletin 38, 10, pp. 1272 – 1287 (2012).

[8] Patton, J. H., Stanford, M. S., et al., Factor structure of the barratt impulsiveness scale. Journal of clinical psychology 51, 6 (1995), pp. 768 – 774.

[9] Harald Weinreich, Hartmut Obendorf, Eelco Herder, and Matthias Mayer. Not quite the average: An empirical study of web use. ACM Transactions on the Web, 1(2):26, 2, 2008.

[10] A. Treisman and G. Gelade. A feature-integration theory of attention. Cognitive Psychology, 12, 1 (1980).

[11] J. Wolfe and T. Horowitz. What attributes guide the deployment of visual attention and how do they do it?, Nature Reviews Neuroscience, 5, 6 (2004), 495 – 501.

[12] OpenID Japan，https://www.openid.or.jp/

[13] Japanese major website by Alexa，https://www.alexa.com/topsites/countries/JP

[14] Yahoo! Japan，https://www.yahoo.co.jp/

[15] Crowdworks，https://crowdworks.jp/

[16] Twilio，https://twilio.kddi-web.com/

[17] paymentnavi，http://www.paymentnavi.com/paymentnews/61930.html

APPENDIX

This describes the purpose of using personal information and how personal information is handled. The personal information acquired during the experiments is used for the following purposes.

1) a usability study of account registration,
2) a security study of account registration,
3) a study of two-factor authentication for smartphones,
4) a security study of dependence on IT knowledge

We will be using your phone number and the security questionnaires you answered. The personal information relates only to sending SMS messages. Research results will appear only in the published paper. We will outsource personal information to SMS transmission service organizations that send the SMS messages. The personal information you provide will be handled properly and disposed of promptly. We will not provide personal information to any third party.