

Impact Assessment of Password Reset PRMitM Attack with Two-Factor Authentication

Kota Sasa, Hiroaki Kikuchi

Graduate School of Advanced Mathematical Sciences, Meiji University, Japan
yamatanaka41@gmail.com, kikn@meiji.ac.jp

Abstract

Two factor authentication is widely used, to send a confirmation message via Short Message Service (SMS). Two factor authentication is believed as more secure than a simple password authentication because it prevents intrusion even if your password was compromised. However, SMS is used not only for an authentication when registering an account but for resetting password, too. Hence, in 2017, Gelernter proposed the Password Reset Min-in-the middle attack (PRMitM), which can take over a user's account by using Two Factor Authentication via SMS. 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. Two factor authentication was believed to improve security, however, it makes the site more vulnerable than before. Even after their publication, not all vulnerable websites addressed the vulnerability. Hence, it is still not clear if these attempts were sufficient to prevent victims from being attacked. In this paper, we report the comprehensive analysis results of an investigation of vulnerable major websites to PRMitM attack. To identify 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 show the successful-attack ratios and the typical behaviors of vulnerable subjects. Some of main results include that Vulnerable users do not remember whether they have registered accounts or not and users who frequently change their passwords are 11.6 times more vulnerable to users who do not change much.

Keywords: Two-factor authentication, PRMitM

1 Introduction

A password is the most commonly used authentication method. Users using web services use passwords to prevent their accounts from being

unauthorized access or being account theft. However, many vulnerabilities in password authentication have been revealed and web services were compromised. 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. Having a too simple password is also a serious problem. Recent studies have reported that Windows NTLM password consisting of under 8 character can be cracked in under 2.5 hours [3]. However, the average user prefers very simple passwords to avoid being compromised [4]. Another problem is a human factor that careless person forgets passwords easily. Yan et al. [5] reported that 65% of users are apt to forget their passwords. Hence, means are provided for resetting the password.

Two-factor authentication (2FA) is the most popular method of recovering a forgotten password. 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. However, if he also forgets his email password, he cannot get either. Hence, the failure can be prevented by sending the confirmation message via SMS instead of email. SMS is to the phone number of the smart phone.

However, Gelernter et al. [6] 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 the conventional method, the password-reset process is vulnerable. Moreover, since this method does not require users entering a password, it is hard to be noticed that it is being attacked.

After the publication of Gelernter et al.'s work [6], many vulnerable websites revised the SMS message. However, we claim that some websites have not yet fixed well. Our investigation of the top 200 websites revealed that 28 websites adopt SMS-based password-reset process and 12 of them were vulnerable to PRMitM attacks. Moreover, to make countermeasures effective, we should also consider human factors such as IT literacy and individual characteristics (careful, lazy, or optimistic). For example, the personal characteristics such as "neurotic tendency" and

“anxiety tendency” are likely to be vulnerable by phishing mail attack [7]. In phishing mail, PRMitM attack considering human’s carelessness will improve the risk of compromised. It is therefore important to clarify which warning methods are effective in preserving the security of a website.

Human factors are closely related with social engineering attacks [24]. Social engineering attack is an art of manipulating the people who has less knowledge about phishing or fraud. This motivates us to study the work. Especially, we are interested in who is more likely to be victim of the PRMitM attack. The chance to be attacked depends on individuals. The difference of probability to be attacked comes from the diversity of personal characteristics. If we happen to know the primal factors to be attacked, we can warn the most vulnerable type of users against the PRMitM and reduce the loss by the attack.

Our contributions are as follows:

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.

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.

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.

2 Prmitm Attack

2.1 2FA

2FA is an authentication method that combines biometric, device, and/or other information with a password. In conventional authentication, our method was only password. However, password only authentication has many vulnerabilities. So, attackers tried various attacks. 2FA can protect accounts from these attacks.

The most popular method involves the use of a phone-based SMS rather than a dedicated password-generator device. 2FA is considered to improve security. However, under certain conditions, the probability of being attacked goes up.

2.2 Reasons for Being Subject to An PRMitM Attack

In 2017, Gelernter et al. [6] identified the PRMitM attack, which can take over a user’s account by using 2FA via SMS. New user registration is one of scenes using 2FA. The procedure is as follows.

(1) A new user who wants making a registration enters necessary information, e.g., name, password, and phone number etc., and sends these information.

(2) A temporal password is sent to him via SMS.

(3) He enters the temporal password to login.

On the other hand, password reset using 2FA is processed as follows.

(1) A user who forgets password sends a password reset request.

(2) A temporal password is sent to him via SMS.

(3) He enter the temporal password to reset his password.

These procedures are similar. The PRMitM attack exploits the similarity between these methods

Figure 1 shows a series of the flow of a PRMitM attack. With the assumption, user X has an account X on target website Z . The attacker makes a fake website that requires 2FA. The procedure of PRMitM attack is as follows.

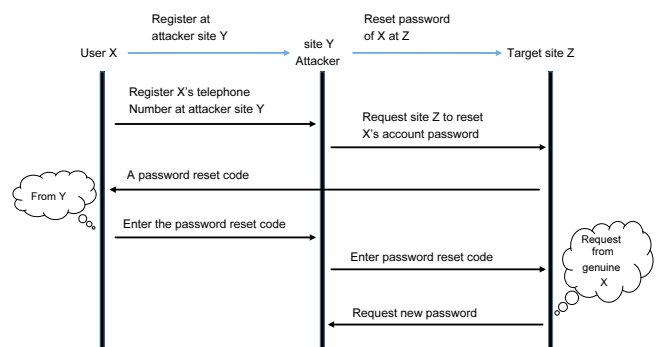


Figure 1. Illustration of a basic PRMitM attack

(1) User X attempts to register to fake site Y , which was prepared by the attacker..

(2) The attacker requests a password reset to the target site Z using the phone number of user Z on behave of him.

(3) Site Z thinks that X is requesting a password reset and sends back to him a verification code for his account.

(4) User X thinks that code was sent by Y and enters the reset code in the attacker site Y .

(5) Y can change the password and takes over X 's account.

User X cannot be even aware of having been attacked. Gelernter et al. pointed out three vulnerabilities:

(1) Just a code. Message contains only the code, without mentioning both the reset process and the sending website.

(2) Sender and a code. The sending website is mentioned with the code, but there is no evidence of the password reset process.

Table 1 shows examples of SMS messages used in the past. In case of (1), a user can't judge who send the code. In (2), a user misunderstand the purpose of the code sent.

Table 1. Examples of vulnerable reset codes via SMS [6]

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

Gelernter et al. suggested that the password-reset SMS should specify the sender name and do not send the code as clear text against PRMitM. It makes users to be careful and they notice if the code is for a password reset. They also recommended that sending a URL for resetting password instead of an SMS reset code. In PRMitM attacks, if the URL is used to reset the password, the attacker would have to let the user enter the URL. It is very strange. Hence, most users could be feel odd and would deal with that coolly.

2.3 Security Behavior Intentions Scale (SeBIS)

We conducted a questionnaire survey, called SeBIS, which examine subject's security knowledge and behavior proposed by Egelman and Peer [8]. SeBIS consists of 18 questions to be answered in 5 score. The sixth and seventeenth of the 18 are equivalent questions for judging whether the users answers the question honestly. Table 2 shows the example of the pair of questions. In our study, we replaced negative questions by the corresponding positive equivalents when the original English sentences were translated into Japanese. Table 13 lists the modified SeBIS questions except sixth and seventeenth.

Table 2. The sixth and seventeenth SeBIS questions

	Question
6	Select always to confirm that you answer the question correctly.
17	As an answer to this question, please select always.

3 Potential Risks

3.1 Human Factor

Individual characteristics have an impact on PRMitM attacks [9-10]. For example, users who don't know enough about security knowledge or carelessly read SMS message easy to be vulnerable to PRMitM attacks. Gelernter et al. [6] did not consider the effect of human factor and user profiles, or SMS message

style. Especially, whether or not users read SMS message will depends on users' security knowledge. In this study, we focus on human elements and SMS-related behavior to clarify the potential risk of PRMitM attack.

3.2 Long SMS Attacks

Warning message may help a user who uses 2FA for the first time to reset his password. However, too many 2FAs could fail to warn user because 2FA is repeated the same procedure every time. Krol et al. showed that 80% users ignore security warning and 45% users don't read warning message because they think that it is annoying [11]. This observation suggests us a new attack, called a long SMS attack which exploiting user's characteristics.

Long SMS attack is an attack that forces the victim to enter the code twice. For the first time, attacker Y sends a long SMS message, like a fake confirmation code (1) in Figure 2, and then victim X enters the code. After that step, the normal PRMitM attack is executed with a message (2). The intention of the attack is as follows.

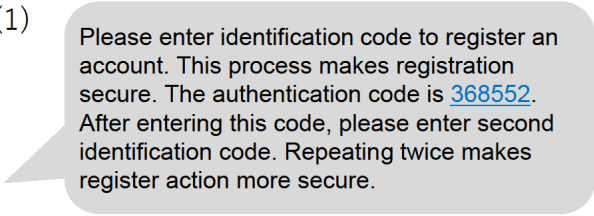
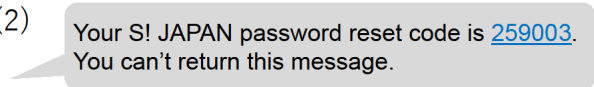
- (1)  Please enter identification code to register an account. This process makes registration secure. The authentication code is [368552](#). After entering this code, please enter second identification code. Repeating twice makes register action more secure.
- (2)  Your SI JAPAN password reset code is [259003](#). You can't return this message.

Figure 2. Basic long SMS attack

(1) It makes the victim not to read the second SMS message because he tired in reading the first one

(2) The victim becomes careless because he gets used to the first procedure

Average user is not able to read and understand too long and comprecated messages [12]. Hence, given multiple messages, a victim user might carelessly read a second input message and type a code because the victim tired and the second procedure seems to be the same as the first one [13].

3.3 Numeric Authentication Code

The iPhone and some Android devices have a default function that automatically recognizes a number as a phone number and creates a link to call phone. In PRMitM, this function must be vulnerable. See Figure 3 showing sample alphanumeric and numeric codes. The latter is more danger because the numeric reset code is too emphasized to read warning message [14]. Victims find the code only without noticing the warning.

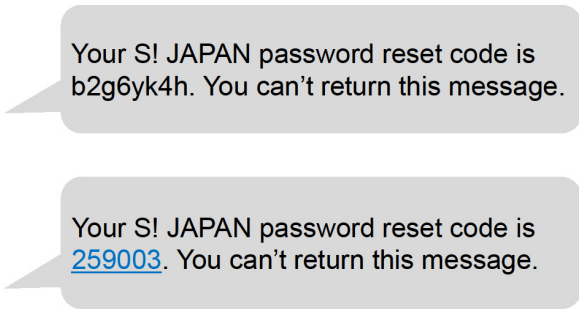


Figure 3. Alphanumeric and numeric codes

3.4 Link-via-SMS (LVS)

Gelernter et al. claimed that it would be safe to reset the URL link instead of the reset code, but there is a problem for the following reasons:

- (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.

Hence, we argue that LVS is not secure enough to be used in place of the SMS password reset code.

4 Investigation of Major Domestic Websites

4.1 Purpose

After being suggested PRMitM, many vulnerable websites had already fixed the vulnerability. However, some improved message are still not kind to the user. We investigated major Japanese domestic websites to clarify vulnerable websites to PRMitM.

4.2 Method

We investigated the top 200 websites of Alexa Japan [15] from August 13th to August 26th, 2019. We classified websites into some classes, by means of three features of “Is it possible to create a user account?”, “Is SMS used for password reset?” and “Is there a warning written on the password reset SMS message?”. The top 20 positions of the surveyed websites are shown in Table 3.

4.3 Results

Table 4 shows the investigation result. All services that could reset password via SMS contained the service name in SMS message. However, there were 18 websites with no warning (unique websites are only five. Because 18 websites contain the duplicated services at different domains.). Table 5 shows SMS message and service name that contain no warning. There were 26 websites that did not offer user registration.

Table 3. Top 20 website of Japanese ranking

rank	name	URL
1	Google	http://www.google.co.jp/
2	Youtube	http://www.youtube.com/
3	Yahoo Japan	http://www.yahoo.co.jp/
4	Amazon	http://www.amazon.co.jp/
5	Google	http://www.google.com/
6	Facebook	http://www.facebook.com/
7	Wikipedia	https://www.wikipedia.org/
8	Rakuten	http://www.rakuten.co.jp/
9	tmail	https://www.tmall.com/
10	qq	http://www.qq.com/
11	niconico	https://www.nicovideo.jp/
12	Baidu	http://www.baidu.com/
13	SOHU	http://sohu.com/
14	Amazon	http://www.amazon.com/
15	taobao	https://world.taobao.com/
16	Twitter	http://www.twitter.com/
17	tmail	https://login.tmall.com/
18	Yahoo	https://www.yahoo.com/
19	FC2	http://www.fc2.com/
20	jd	https://www.jd.com/

Table 4. Top 200 website statistical information

No account	26				
		No SMS	145		
Available account	174	Available SMS	29	No warning	18
				warning	9
				URL	2
Total	200				

Table 5. Service name and SMS messages without warning

Name	Alexa rank	SMS message
Google	1	G-910957 is your Google verification code.
Yahoo JAPAN	3	Verification code: 375403 Please enter the code. Yahoo! JAPAN
Amazon	4	Your Amazon verification code is 160973.
LinkedIn	131	LinkedIn verification code is 「123512」
Coconala	193	[coconala] please enter the code 860670

4.4 Discussion

In the survey results, there were 18 websites that omit warnings. It is assumed that one of the reason is that a phone number is optional for registration in some sites. For example, in Yahoo! JAPAN, it is not necessary to register a phone number when creating new account. After registration, users who wish to add can register phone number later. Amazon allows users to register their phone number only using dedicated app. On the other hand, Twitter and Facebook allow users to registered only when telephone number contain warning in password reset SMS message. Therefore, using SMS messages without warning is not necessarily vulnerable.

5 User Experiments on Potential Risk

5.1 Purpose

The purposes of the experiment are the following.

1. To clarify the danger SMS message.
2. To clarify features of vulnerable users.

5.2 Method

In this experiments, the 184 subjects were enrolled via the crowdsourcing service ‘CrowdWorks’ [16]. We let them register with toy websites. Table 6 shows the ages and sex of the subjects. To send an SMS message, we used a programmable SMS service from twilio [17]. At first, subjects got the following explanation of the experiment:

Table 6. 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

- This is a survey experiment on security awareness
- Please register 4 toy websites
- There may be vulnerable websites among them
- If you think the website is vulnerable, please skip a registration.

Actually, PRMitM attack was done at the third registration for all subjects. We regard users who enter the reset code in the third website as vulnerable user.

We conduct the experiment in the following steps. First, subjects enter a name, a password, and a phone number in the screen in Figure 4. Next, SMS message with a code is sent to subject’s smart phone. Subjects choose enter the code if he thinks it’s safe, cancel the registration if he thinks the website is vulnerable. The operation performs by the subjects on the four toy sites is shown in the Table 7 and explained as follows.

Table 7. Experiment websites and code type and purposes

	(1)	(2)	(3) (Attack)	(4)
Name	S! JAPAN	Cowtter	Majebook	Mstagram
Code sent by SMS message	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

Welcom to **Sasa! JAPAN**

Please enter registration information and click new registration button.

Figure 4. Registration screen in experiment (1)

- (1) only first procedure (no SMS message).
- (2) receiving verification code.
- (3) receiving password reset code to S! Japan.
- (4) receiving verification code in different communication.

In third website, one of the five SMS styles was sent. SMS messages are showed in Table 8. The long SMS group received two SMS messages. First message is long and second one is a type 1 or type 2 SMS. Each time a subject accessed a toy website, they answered the two questions shown in Table 9. These questions answered in 7 scorers, the higher score the better the evaluation. All messages included the sender’s name. After all tasks were completed, subjects took the SeBIS survey.

Table 8. Type of password reset code

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

Table 9. 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

5.3 Experimental Results

Table 10 gives the experiment results. A successful attack ratio is defined as the proportion of subjects who allows the 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 8 and the successful ratio in x , respectively. For example of attack, we have the successful attack ratio for type1 as Y in (3).

Table 10. 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

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

To summarize the effect of the type of SMS on the successful-attack ratio, Table 10 shows the conditions for each inspected item.

The reasons of cancellation are shown in Table 11. Although there may have been some subjects canceling for more than two reasons, we cannot accept more than two.

Table 11. 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

Table 12 shows the successful-attack ratio R for reset attacks with various user attributes. It is distributed around 70% and 80% overall. The higher R is 50 years and over and users who does not remember registering in Facebook, Twitter, and Yahoo Japan.

Table 13 shows the SeBIS results for “enter” or “cancel” in a (3) attack. Figure 5 shows the SeBIS total score.

Table 12. 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
	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

Table 13. SeBIS index

	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 upto-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

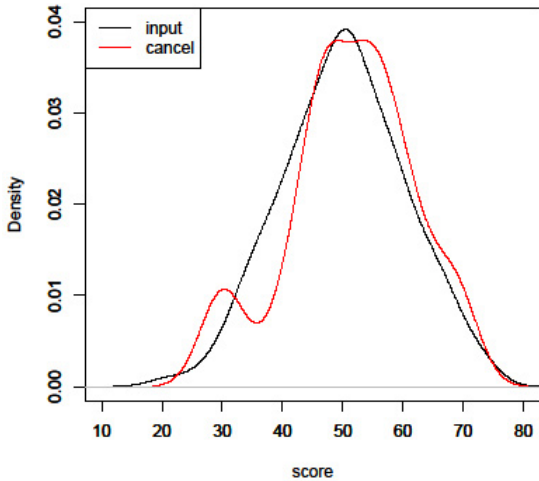


Figure 5. SeBIS score distribution of cancel or input

5.4 Ethics

In this experiment, (“toy”) websites was used, and no password reset attack was performed on the actual web site. The subjects participating in the experiment agreed with the information acquired on the web before the experiment starts. For example, personal information is only used in this study, we don’t disclose information to any third parties. To send out

SMS, we entrust an SMS sending service provider [17].

5.5 Discussion

5.5.1 Effects of Human Factor

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 14 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 recognized that warnings affect password-reset attack ratios. Numeric codes increased the successful-attack ratio than alphanumeric ones. However, there was no significant difference between numeric and alphanumeric ($p = 0.14 > 0.1$). There was no 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 shows that users are careful when the communication is encrypted.

Table 14. 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		

5.5.2 SeBIS and Successful Attack Ratio

Since average score of all subjects was 50.3, the number of subjects who “enter” or “cancel” with a threshold value of 50 is shown in Table 15. There was no significant difference between “enter” and “cancel” with respect to SeBIS scores. In this result, security knowledge does not affect the successful-attack ratio in PRMitM.

Table 15. Successful attack ration for SeBIS scores

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

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

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

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 ($x_{1,2}, x_{2,2}, x_{3,2}$), age ($x_{4,0}$), sex ($x_{4,01}$), whether numbers are registered in Twitter, Facebook, Yahoo ($x_{4,1}, x_{4,2}, x_{4,3}$), can you use a phone number to create an account for a famous service ($x_{4,4}$), can you use a phone number to create an account for a non-famous service ($x_{4,5}$), what kind of cell phone used ($x_{4,7}$), SeBIS answers ($x_{q1}, x_{q2}, \dots, x_{q18}$).

Table 16 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

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

Table 16. Logistic regression analysis

	Estimate β	Std. Error	z value	Pr(> z)
(Intercept)	-1.68	4.64	-0.36	0.717 *
x_0				
x_1	-1.25	1.63	-0.77	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 *
$x_{2,1}$	0.59	0.48	1.23	0.219 *
$x_{2,2}$	-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 ***
$x_{4,0}$	0.65	0.45	1.46	0.145
$x_{4,01}$	-0.33	0.83	-0.39	0.694
$x_{4,1}$	-0.55	0.57	-0.96	0.339
$x_{4,2}$	0.23	0.40	0.58	0.564
$x_{4,3}$	-0.58	0.53	-1.11	0.269
$x_{4,4}$	-0.29	0.28	-1.03	0.302
$x_{4,5}$	0.47	0.32	1.49	0.137
$x_{4,7}$	0.65	0.70	0.93	0.350
xq_1	0.01	0.28	0.02	0.981
xq_2	-0.54	0.34	-1.60	0.110
xq_3	0.29	0.26	1.09	0.278
xq_4	0.15	0.29	0.52	0.601
xq_5	2.45	0.71	3.44	0.00058 ***
xq_7	-0.57	0.44	-1.28	0.199
xq_8	-0.58	0.29	-1.97	0.048 *
xq_9	0.41	0.37	1.13	0.259
xq_{10}	-0.98	0.46	-2.10	0.0362 *
xq_{11}	-0.33	0.37	-0.89	0.376
xq_{12}	0.41	0.40	1.01	0.314
xq_{13}	-0.34	0.41	-0.82	0.414
xq_{14}	0.22	0.34	0.64	0.524
xq_{15}	-0.24	0.44	-0.55	0.581
xq_{16}	0.85	0.45	1.87	0.060
xq_{18}	-1.27	0.45	-2.81	0.004965 **

Note that this did not reach the level of significance. However, one interesting result was that x_{q5} (SeBIS Q5 “I 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. Although it is recommended to change passwords frequently, it was the opposite result. As one of the causes, we suggest that users who frequently change password are get used to change the operation. Users familiar with the 2FA knows that it is safe to enter the code, and hence would not read the message carefully. Another cause may be that users frequently forgetting passwords does not matter if it is stolen. 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. 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. Always careful users are careful even when reading SMS. SeBIS Q18 is “I verify that my anti-virus software has been regularly updating itself”. This also reduces the risk by a factor of 0.28. This also means that the higher the attentiveness is, the less likely to be attacked.

5.6 Impact Evaluation of PRMitM Attacks

From the results of this study, we considered Yahoo Japan, a company without warning, as an example of how PRMitM attack will affect. In this case, the odds ratio between type 0 and type 1 is

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

Therefore, in the case of no warning, it is likely to be attacked 4.67 times more than with warning. Yahoo! JAPAN had over 40 million monthly active users in 2017 [18]. From Table 12, subjects who registered phone number in Yahoo! JAPAN were about 26%, giving about 10.4 million registered phone numbers.

$$40 \cdot 0.26 = 10.4,$$

about 10.4 million. For the case of no warning,

$$10.4 \cdot \frac{35}{37} = 9.8.$$

Therefore, there are 9.8 million potentially vulnerable users. However, by changing the password reset message to a warning, we have

$$10.4 \cdot \frac{30}{38} = 8.2,$$

thus reducing the vulnerable cohort to 8.2 million users.

5.7 Risk Factor in Future

From 200 sites, there are only 28 websites using SMS verification. Does this fact imply that risk of RPMitM attack is too low to be reduced by adding warning message in SMS? The answer is no. Nowadays, as security important is getting acknowledged more than before, the use of 2FA must increase. For instance, the 7pay smartphone payment service, which was launched by the major convenience store operator in Japan, was compromised and about 900 registered users lost about 55 million Japanese Yen [25].

According to the report, if 2FA is deployed with the 7pay system, the cyber incident can be prevented. Hence, we claim that the use of 2FA with SMS increases and the risk of PRMitM should be considered more seriously.

6 Related Works

The MitM attack is related with other techniques that may be used to address the password reset vulnerability.

The simplest one is CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) test at the websites. Egele et al. [19] proposed Captcha challenges at the website to prevent users to visit from other website in [20]. Similar techniques were used by Koobface to prevent compromised users to attack the other website. Several styles of Captcha have been studied so far. Ximenes et al. [21] utilized phonetic punning riddles found on Knock-Knock Jokes (KK jokes). Their system tests a user to differentiate real KK jokes from synthesized KK jokes. Unfortunately, it only has restrictive security, e.g., a random guess attack will succeed over 10%. Kamoshida and Kikuchi [22] proposed methods using a feeling of strangeness between natural phrases and machine-generated phrases.

They use machinesynthesized phrases and machine-translated phrases as machine-generated phrases, respectively. They leverage strings of private documents in order to prevent adversaries from finding out their sources. They cannot limitlessly generate brand-new tests since the amount of private documents is finite. Yamada et al. [23] propose an “onomatopoeia CAPTCHA” that applies onomatopoeia, i.e., words containing sounds similar to the noises they describe. Humans usually understand a given onomatopoeia unconsciously and use it in daily conversation. Thus, it is clearly easy for humans to solve, while it is hard for computers because the mechanisms to recognize onomatopoeia are not very clear even now.

Phishing is one of attacks to exploit the PRMitM attack. It is a technique that fake website convinces victim as the original website. In [7], Halevi et al. showed that the most vulnerable personality characteristics in phishing mail attacks are “neurotic tendency” and “anxiety tendency” based on their empirical analysis.

In 2017, National Institute of Standards and Technology (NIST) updated the digital identity guidelines (NIST Special Publication 800 63B) [26], where they suggests that not to require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a evidence of authenticator compromise.

Accordingly, National center of Incident readiness and Strategy for Cybersecurity (NISC) encourages the same practice to Japanese organizations [27]. Finally, Ministry of Communication (MIC) suggests longer life of strong password [28].

7 Conclusion

We have studied the PRMitM attacks using 2FA

password-reset messages sent by SMS. Based on the investigation of Japanese top 200 websites, we estimated the risk of PRMitM attack. Our study found that vulnerable 18 websites having no warnings within SMS messages out of 29 websites that accept password a SMS message for requesting password reset.

Our user study of 180 subjects revealed that the PRMitM risk factor was 4.6 times higher in the no warning case, 0.91 times higher for the long SMS case and 1.86 times higher for numeric-only reset. It is interested to remark that users who change password only when necessary were less likely to be attacked by a factor of 11.59 times. In other words, frequently update password uses are more likely to be compromised by PRMitM. One possible cause of the behavior is that the user who updates password too frequently is getting used to change it without carefully reading message in SMS. Therefore, the attack can be prevented by making SMS for confirmation of password reset to be distinguished via its appearance, e.g., different background color. With new SMS in background color, even careless user may notice that current password is going to be changed and easily avoid the PRMitM attack.

Our future works include that a study of human factors for vulnerable against phishing and PRMitM attacks, a explore for more secure password-reset methods, and new method for user authentication free from password reset.

References

- [1] A. Das, J. Bonneau, M. Caesar, N. Borisov, X. Wang, The Tangled Web of Password Reuse, *2014 Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, 2014, pp. 1-15.
- [2] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, L. F. Cranor, I Added “!” at the End to Make It Secure: Observing Password Creation in the Lab, *Symposium on Usable Privacy and Security (SOUPS)*, Ottawa, Canada, 2015, pp. 123-140.
- [3] The Register, *Use an 8-char Windows NTLM Password? Don't. Every Single One Can be Cracked in under 2.5hrs*, https://www.theregister.co.uk/2019/02/14/password_length/, 2019
- [4] A. Adams and M. A. Sasse, Users Are Not The Enemy, *Communications of the ACM*, Vol. 42, No. 12, pp. 40-46, December, 1999.
- [5] J. J. Yan, A. F. Blackwell, R. J. Anderson, A. Grant, Password Memorability and Security: Empirical Results, *IEEE Security and Privacy*, Vol. 2, No. 5, pp. 25-31, September-October, 2004.
- [6] N. Gelernter, S. Kalma, B. Magnezi, H. Porcilan, The Password Reset MitM Attack, *IEEE Security and Privacy*, San Jose, CA, 2017, pp. 251- 267.
- [7] T. Halevi, J. Lewis, N. D. Memon, A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits,

- 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, 2013, pp. 737-744.
- [8] S. Egelman, E. Peer, Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS), *SIGCHI Conference on Human Factors in Computing Systems (CHI'15)*, Seoul, Republic of Korea, 2015, pp. 2873-2882.
- [9] J. Joireman, M. J. Shaffer, D. Balliet, A. Strathman, 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*, Vol. 38, No. 10, pp. 1272-1287, October, 2012.
- [10] J. H. Patton, M. S. Stanford, E. S. Barratt, Factor Structure of the barratt Impulsiveness Scale, *Journal of clinical psychology*, Vol. 51, No. 6, pp. 768-774, November, 1995.
- [11] K. Krol, M. Moroz, M. A. Sasse, Don't Work. Can't Work? Why It's Time to Rethink Security Warnings, *7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Cork, Ireland, 2012, pp. 1-8.
- [12] H. Weinreich, H. Obendorf, E. Herder, M. Mayer, Not Quite the Average: An Empirical Study of Web Use, *ACM Transactions on the Web*, Vol. 2, No. 2, pp. 1-32, February, 2008.
- [13] A. Treisman, G. Gelade, A Feature-integration Theory of Attention, *Cognitive Psychology*, Vol. 12, No. 1, pp. 97-136, January, 1980.
- [14] J. Wolfe, T. Horowitz, What Attributes Guide the Deployment of Visual Attention and How Do they Do it?, *Nature Reviews Neuroscience*, Vol. 5, No. 6, pp. 495-501, June, 2004.
- [15] Japanese major website by Alexa, <https://www.alexa.com/topsites/countries/JP>.
- [16] Crowdworks, <https://crowdworks.jp>.
- [17] Twilio, <https://twilio.kddi-web.com/>.
- [18] <https://about.yahoo.co.jp/ir/jp/overview/strength/>.
- [19] M. Egele, L. Bilge, E. Kirda, C. Kruegel, Captcha Smuggling: Hijacking Web Browsing Sessions to Create Captcha Farms, *Proceedings of the 2010 ACM Symposium on Applied Computing*, Sierre, Switzerland, 2010, pp. 1865-1870.
- [20] K. Thomas, D. M. Nicol, The Koobface Botnet and the Rise of Social Malware, *2010 5th International Conference on Malicious and Unwanted Software (MALWARE)*, Nancy, Lorraine, France, 2010, pp. 63-70.
- [21] P. Ximenes, A. Santos, M. Fernandez, J. Celestino, A Captcha in the Text Domain, *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, Montpellier, France, 2006, pp. 605-615.
- [22] Y. Kamoshida, H. Kikuchi, Word Salad Captcha - Application and Evaluation of Synthesized Sentences, *15th International Conference on Network-Based Information Systems*, Melbourne, VIC, Australia, 2012, pp. 799-804.
- [23] M. Yamada, R. Shigeno, H. Kikuchi, M. Sakamoto, Evaluation and Development of Onomatopoeia CAPTCHAs, *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, Belfast, UK, 2018, pp. 1-2.
- [24] S. Gupta, A. Singhal, A. Kapoor, A Literature Survey on Social Engineering Attacks: Phishing Attack, *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, India, 2016, pp. 537-540.
- [25] The Japan News by the Yomiuri Shimbun, *7pay Shut down after 4 Days in Wake of Security Misstep*, <https://the-japannews.com/news/article/0005855014>, August, 2019.
- [26] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, M. F. Theofanos, *Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST Special Publication 800-63B, June, 2017.
- [27] National Center of Incident Readiness and Strategy for Cybersecurity (NISC), *Information Security Handbook for Network Beginners*, <https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all-eng.pdf>, 2017.
- [28] MIC, *Information Security Site for Citizens*, <http://www.soumu.go.jp/mainsosiki/johotsusin/security/basic/privacy/01-2.html>, 2013.

Biographies



Kota Sasa received Bachelor of Science and Master of Mathematical Sciences from Meiji University in 2017 and 2019.



Hiroaki Kikuchi received B.E., M.E. and Ph.D. degrees from Meiji University in 1988, 1990 and 1994. After he working in Fujitsu Laboratories Ltd. in 1990, he had worked in Tokai university from 1994 through 2013. He is currently a professor at Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences, Meiji University. He was a visiting researcher of the school of computer science, Carnegie Mellon University in 1997. His main research interests are network security, cryptographic protocol, privacy-preserving data mining, and fuzzy logic. He received the Best Paper Award for Young Researcher of Japan Society for Fuzzy Theory and Intelligent Informatics in 1990, the Best Paper Award for Young Researcher of IPSJ National Convention in 1993, the Best Paper Award of Symposium on Cryptography and Information Security in 1996, the IPSJ Research and Development Award in 2003, the Journal of Information Processing (JIP) Outstanding paper Award in 2010 and 2017 and the IEEE AINA Best Paper Award in 2013. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan (IEICE), the Information Processing Society of Japan (IPSJ), the Japan Society for Fuzzy Theory and Systems (SOFT), IEEE and ACM. He receives Information Processing Society of Japan (IPSJ) Fellow.