SECURITY ANALYSIS ON PASSWORD AUTHENTICATION SYSTEM OF WEB PORTAL

Heekyeong Noh[1], Changkuk Choi[2], Minsu Park[3], Jaeki Kim[4], Seungjoo Kim[5]

CIST (Center for Information Security Technologies),
Korea University, Seoul, Korea
[1]hknoh@korea.ac.kr, [2]nikojin@gmail.com, [3] minsoon2@korea.ac.kr,
[4] jack2@korea.ac.kr, 5skim71@korea.ac.kr

ABSTRACT

Portal site is not only providing search engine and e-mail service but also various services including blog, news, shopping, and others. The fact that average number of daily login for Korean portal site Naver is reaching 300 million suggests that many people are using portal sites. One of the most famous social network service, Facebook subscribers to reach 1.2 billion 30 million people at the time of the February 2014. With the increase in number of users followed by the diversity in types of services provided by portal sites and SNS, the attack is also increasing. Therefore, the objective of this study lies in analysing whole procedure of password authentication system of portal sites, SNS and analysing the security threat that may occur accordingly. Also, the security requirement corresponding to analysed security threat was extracted and the analysis on implementation of security requirements by portal sites and SNS was conducted.

KEYWORDS

Password Authentication System of Web Sites, Threat of Web Sites, Security Requirement of Web Sites, Attack Potential of Password Systems

1. INTRODUCTION

The dictionary definition of portal is 'entrance' or 'gateway' and the term portal site (hereafter referred to as a portal) signifies a site which plays the role of a gateway by collecting and organizing enormous quantities of internet data so that users can easily access the particular data they require. Although the original format of portals was primarily based around search engines and e-mail services, they currently provide widely varied web services such as those related to news, shopping, and blogging. Furthermore, the e-mail accounts provided by portals are used as IDs for social network services (SNSs), such as Facebook and Twitter, and other web services and applications, and even as a way to authenticate users who have forgotten their account passwords. As such, portal accounts are increasingly used not merely for e-mail communication but are connected to services providing a wide range of web-based activities.

When a portal account is used at another web service or portal, the security strength of both services decreases to that of the site with the weakest security based on the principle of

Natarajan Meghanathan et al. (Eds) : WiMONe, NCS, SPM, CSEIT - 2014
pp. 71–92, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.41207

minimization, 'since the security is entwined in a chain, the weakest security strength determines the security strength of the whole' [1]. Such a chain occurs, for example, when a user creates a Google (www.google.com) account and provides his Naver (www.naver.com) e-mail account address as personal information. A Google account requires a minimum password length of 8 characters but does not require a combination of numbers and upper and lower case letters. Naver, on the other hand, requires a minimum password length of only 6 characters and also does not require a combination of numbers and upper and lower case letters. However, the weaker password requirements of Naver accounts reduce not only the security of Naver accounts, but also of any Google account created using a Naver one. Thus, the security of the Google account is reduced to that of the Naver one, since both accounts can be hacked after obtaining the Naver password, assuming the IDs of the accounts are named the same or the linked account is known by some other means. To hack into the Google account, the attacker can simply request a password reset and request user authentication through the Naver account. At the moment, although the Naver account password is easier to obtain using a complete enumeration survey than the Google one, it is trivial for an attacker to access the Google account after acquiring the Naver one.

Therefore, an analysis of portal sites' authentication systems at member registration, login, password reset step 1, and password reset step 2, including via SNS, were conducted in this study. Security threats that may exist in the authentication procedure of each portal and SNS, and the security countermeasures against such threats were clarified. Afterwards, a quantitative analysis of attack threats and the implementation by portals of their corresponding countermeasures were conducted by applying a standardized set of security criteria to each portal.

2. RELATED WORKS

2.1. Password Authentication Systems

As online services and applications become more sophisticated, users are increasingly required to create an account to receive a service. Studies of security of authentication systems undertaken until now mainly focus on the security vulnerabilities of ID-password based authentication systems and their countermeasures. When users create distinct accounts for a different variety of services they often use the same IDs and passwords due to memory limitations and the inconvenience of managing multiple accounts differently. In such cases, there is the problem that an attacker can access the user's other accounts by just acquiring the authentication information of one [2]. Furthermore, if the account obtained is just a portal, the scale of local damage may be small, but severe damage may result when the same user's accounts at sites related to banking and payment, including internet banking and internet shopping malls, amongst others, are also obtained. Although an answer to a security question may be requested from users during the user authentication procedure for password resets if a user forgets his password, the answers to such questions can often be either too easily guessed or too difficult for even the user himself to remember. Therefore, in order to resolve such problems, studies were undertaken to improve the security of the design and selection of account registration security questions [3]. Afterwards, in order to resolve the problem of remembering several IDs, many service providers started utilizing the most frequently used e-mail address as ID. Recently, the analysis of the security threat to users' accounts and privacy was conducted in relation to such elements as the password management plans of service providers and multiple uses of the same password, and possible solutions to their weaknesses proposed [4].

Studies analysing the security of various password authentication systems have been conducted and they recommended security-hardening methods. These included CAPTCHA, after consecutive login attempts, that confirm that the login device is human-operated by requiring only human-discernible answers, salting techniques which use random numbers for the application of a password into a hash function so the password can be safely encrypted, and key strength algorithms which respond to consecutive attempts by lengthening decoding times by repeated encryption of the password with a hash function. Also, an algorithm to examine the security strength of passwords and effectively perform safer password creation was proposed. Entropy-based security assessment is available and entropy was first proposed as a concept for measuring the uncertainty and randomness for security by Claude Shannon [5]. In order to measure the entropy value of a password, the distribution of password length, text placement, numbers of letter types, and contents of the text are set as standards and the sum of all their entropies is the total entropy value [6]. Then, the method to quantitatively examine the security of passwords was proposed by the creation of a PQI (password quality indicator) which measures the security strength of passwords by considering their entropy [7].

Moreover, various methods to promptly and accurately determine password security strength were proposed to help users create strongly secure passwords. It was proven that a way to prevent successful pre-emptive attacks can be first sorting passwords into those of high and low security strength by conducting pattern analysis [8]. Using this method, users are prevented from selecting easily guessed passwords at password creation. The security strength of passwords was enhanced by comparing the password entered by the user during the password creation procedure against a list of those from dictionaries used by attackers in their pre-emptive attacks and disallowing any matching passwords [9].

However, the limitation of previous studies is that they focus on and propose countermeasures for the problems of password and ID based authentication by service providers only rather than the security threats or attacks on the password authentication system as a whole. The studies focused on the security of passwords rather than the password authentication system as a whole. Therefore, the objective of this study is to analyse the whole portal password authentication system including member registration, login, password reset step 1, and password reset step 2, conduct analysis on the security vulnerabilities of the overall system, and determine the security requirements for the countermeasures against those vulnerabilities.

2.2. Attack Potential of Common Evaluation Methodology (CEM)

Attack potential refers to a function of expertise, resource and motivation presented by Criteria Evaluation Methodology (CEM) in the CC, which consists of elapsed time, expertise, knowledge about a target of attack, period of easy exposure to attack and equipment and quantitatively shows attack potential of the target of attack by giving values to each element [10].

2.2.1. Elapsed time

Elapsed time is the total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the TOE, to develop an attack method and to sustain effort required to mount the attack against the TOE.

2.2.2. Expertise

Expertise refers to the level of generic knowledge of the underlying principles, product type or attack methods. The identified levels are as follows:

- Layman: unknowledgeable compared to experts or proficient persons, with no particular expertise

- Proficient: knowledgeable in that they are familiar with the password attack tools and methods
- Expert: familiar with implementing in password attack tools, operation algorithm of password authentication systems.

2.2.3. Knowledge of target of attack

Knowledge of the TOE refers to specific expertise in relation to the TOE. This is distinct from generic expertise, but not unrelated to it. Identified levels are as follows:

- Public: information gained from the Internet
- Restricted: knowledge that is controlled within the developer organisation and shared with other organisations under a non-disclosure agreement
- Sensitive: knowledge that is shared between discreet teams within the developer organisation, access to which is constrained only to members of the specified teams
- Critical: knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking

2.2.4. Period of easy exposure to attack

Period (chance) related to elapsed time, when an attacker can approach the target of attack.

- Unnecessary/unlimited access: the attack doesn't need any kind of opportunity to be realised because there is no risk of being detected during access to the TOE.
- Easy: access is required for less than a day
- Moderate: access is required for less than a month
- Difficult: access is required for at least a month

2.2.5. Equipment

Equipment refers to the equipment required to identify or exploit a vulnerability [11].

- Standard equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack.
- Specialised equipment is not readily available to the attacker, but could be acquired without undue effort.
- Bespoke equipment is not readily available to the public as it may need to be specially produced.
- Multiple Bespoke is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

Table 1. Password Attack Tools

Tool	Equipment Level
Cain and Abel	Standard
John the Ripper	Standard
SolarWinds	Standard
RainbowCrack	Standard
wfuzz	Standard
Medusa	Standard
THC Hydra	Standard

Table 2 identifies the factors discussed in the previous and associates numeric values with the total value of each factor.

Table 2. Attack Potential of Common Criteria

Factor		Value
Elapsed time	≤ 1 hour	1
	≤ 1 day	3
	≤ 1 week	5
	≤ 1 month	7
	≤ 6 month	10
	> 6 month	15
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple expert	8
Knowledge about target of attack	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Access to object	Non-Restricted	0
	Easy	1
	Normal	4
	Hard	10
	None	*
Equipment	None	0
	Standard	4
	Bespoke	7
	Multi bespoke	9

3. Analysis on Authentication System

This chapter conducts analysis on authentication system of portals, SNS and examines the improvement plan for authentication system. The analysis subjects of this study include Naver (www.naver.com), Nate (www.nate.com), and Daum (www.daum.net) for Korean portals and Google (www.google.com), Yahoo (www.yahoo.com), and MSN (www.msn.com) for U.S.s portals and Facebook (www.facebook.com), Twitter (www.twitter.com) for SNS. Also, authentication procedure of portal was divided into 4 steps of member registration, login, password reset-phase 1, and password reset- phase 2.

3.1. Member Registration

In order to prevent random account creation with automated registration programs, portals have been developing CAPTCHAs, mobile phone authentication and e-mail authentication. Google requires the input of a CAPTCHA without provision of e-mail and mobile phone authentication as the collection of e-mail addresses and mobile phone numbers is optional. However, if users fail to enter the CAPTCHA, mobile phone authentication is provided. MSN requires the input of a CAPTCHA and Yahoo only requests mobile phone authentication without CAPTCHA input. All

Korean portals including Naver, Nate, and Daum do not require the input of a CAPTCHA and prevent automatic registration with mobile phone or e-mail authentication. In the case of Korean portals, the number of IDs issuable to a single mobile phone number is limited to 3 to prevent random account creation. However, due to a policy restricting the number of IDs issued, attackers are stealing currently used accounts for malicious use. Contrastingly, Facebook and Twitter do not provide any system preventing automatic registration so attackers abuse the service by sending SPAM messages advertising illegal content to normal users.

Also, portals provide an overseas IP block service to block attack attempts from overseas. Provision and setting of the overseas IP address block service is under user control. Table 3 illustrates the result of a survey of the basic service provided by each company when the user has not set the overseas IP block service. Google, Naver, and Nate allow login after confirming the user through personal information, e-mail, or phone number authentication once a login attempt from an overseas IP is detected. Then, an alert e-mail is sent in order to inform users about the detection of login attempts from an overseas IP address. Yahoo and Daum allow logins without a separate user authentication procedure and send an e-mail alert to the user. However, MSN allows login with neither a user authentication procedure nor an alert e-mail.

Table 3. Prevention services of portal from Automatic registration

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
CAPTCHA	-	-	-	○	○	-	-	-
Email	-	◐	◐	-	-	-	-	-
Mobile Phone	○	◐	◐	-	-	○	-	-

3.2. Login Attempts

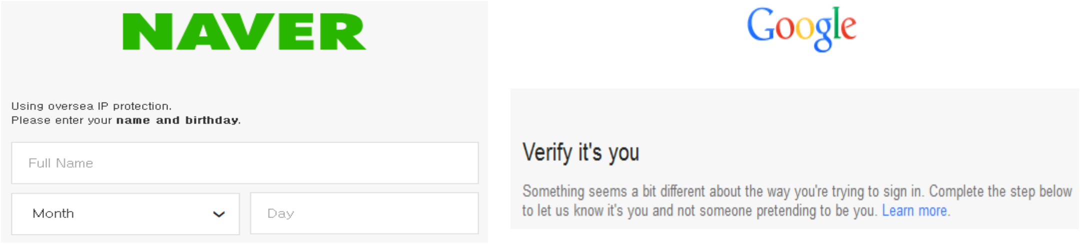
3.2.1. IP Address Security

Portals and SNS shall provide overseas IP block service in order to correspond to overseas attack attempts. Provision and setting of oversea IP address block service follows the decision of user. Table 4 illustrates the result of conducting survey on basic service provided by each company in case user did not set overseas IP block service. Google, Naver, and Nate allow login after confirming the user through personal information, e-mail, or phone number authentication once the login attempt with overseas IP is detected. Then, alert e-mail is sent in order to inform users about the detection of login attempts with overseas IP address. Facebook allows login after confirming the user through personal information. Yahoo and Daum allow login without separate user authentication procedure and send alert e-mail to the user. MSN allows login without user authentication procedure and alert e-mail.

Table 4. Status of Overseas IP protection services

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Authentication	○	○	-	○	-	-	○	-
Email Alarm	○	○	○	○	-	○	-	-

Below Fig.1 is the screen of Naver and Google to inform users about overseas login attempt. Naver conducts authentication with the input of name and date of birth and Google conducts authentication with the use of mobile phone authentication, e-mail authentication, and password hint & answer.



NAVER

Using oversea IP protection.
Please enter your **name and birthday**.

Full Name

Month

Day

Google

Verify it's you

Something seems a bit different about the way you're trying to sign in. Complete the step below to let us know it's you and not someone pretending to be you. Learn more.

Figure 1 . Block Login attempts from overseas IP – Naver, Google

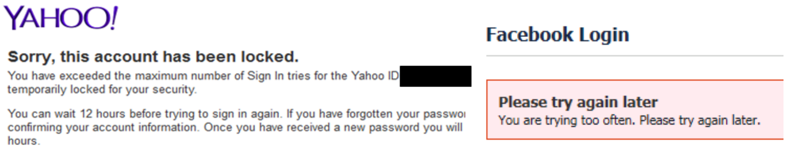
3.2.2. Consecutive Login Attempts

Attackers use bot for random login attempts to user account. All portals request the input of CAPTCHA in case of certain numbers of login failure to correspond to account hacking using the bot and request for both password and CAPTCHA when incorrect CAPTCHA value was entered. Number of login failures that requires CAPTCHA input differs according to each portal. Google requires the input of CAPTCHA with random numbers of failures and other portals request for CAPTCHA with fixed number of failures. Details on number and implementation are illustrated in Table 5.

Table 5. Threshold of account lock and CAPTCHA

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
CAPTCHA	5Times	5Times	5Times	N Times	10Times	5Times	-	-
Account Lock	-	-	○	○	○	○	○	○
Failed Count	-	-	5Times	nTimes	5Times	5Times	20Times	16Times
Lock Time	-	-	3Hours	24Hours	24Hours	12Hours	12Hours	1Hours

Also, the account shall be locked for certain period of time and additional login attempts shall be blocked with the additional login failure after the input of CAPTCHA. The account of user is protected from account hacking with the account lock of 24 hours for Google and MSN, 12 hours for Yahoo, and 3 hours for Daum. However, Naver, Nate, Facebook and Twitter do not provide account lock service. Namely, the attacker can continuously attempt for account hacking in case of Naver, Nate. Additionally, Facebook and Twitter do not request for CAPTCHA but provide account lock service. Below Fig.2 presents the alert message of Yahoo and Facebook to inform users about 12 hours account lock upon detection of consecutive login attempts.



YAHOO!

Sorry, this account has been locked.

You have exceeded the maximum number of Sign In tries for the Yahoo ID [redacted]
temporarily locked for your security.

You can wait 12 hours before trying to sign in again. If you have forgotten your passwo
confirming your account information. Once you have received a new password you will
hours.

Facebook Login

Please try again later
You are trying too often. Please try again later.

Figure 2. Lock Account – Yahoo, Facebook

3.3 Password Reset – Authentication Step 1

If a user requests a password reset, user authentication is conducted through the e-mail address registered at the time of member registration or mobile phone SMS. There are two ways to authenticate users by e-mail address. The first method is to send the URL of the password reset webpage via e-mail. An immediate password reset is available upon login to the e-mail account registered by the user and checking the e-mail. The second method is to send an authentication code composed of numbers via e-mail. The user conducts user authentication for a password reset by entering the authentication code, given in the e-mail, on the web site. The authentication by SMS takes the same format as the second method of e-mail authentication except that the authentication code is sent via SMS. All portals and SNSs limit the number of inputs to 3 or 5 per attempt to block an enumeration survey attack on the authentication code. Also, the number of authentication code transmissions per day is restricted to 5 or 10 after which a 24 hour temporary account lock occurs.

Since Google does not require a user to enter an e-mail address or mobile phone number at member registration, that information may not be available, in which case user authentication is conducted through two channel authentication. However, in the case of portals other than Google, since they do require either a mobile phone number or an e-mail address, user authentication can more easily be conducted just through authentication step 1.

3.4. Password Reset – Authentication Phase 2

Authentication phase 2 is conducted for users who cannot access to authentication code sent via e-mail or SMS in authentication phase 1. Fig 5 is the diagram of password reset- authentication phase 2 of Korean portals and Fig 6 on the right is the diagram of procedure for U.S. portals.

In the case of Korean portals, user authentication is conducted using the resident registration number in step 2. Naver, Nate, and Daum conduct user authentication through the transmission of a copy of the identification card (or input of the Resident Registration no.), name, ID, date of birth, and sex via e-mail or fax and Nate additionally uses a method to confirm the above information via ARS. In case of US portals and Twitter, user information accumulated during account use is utilized to confirm the user in step two authentication. The information requested during the authentication step 2 of Google, MSN, Facebook and Twitter is as follows. They receive a value from the user after subdividing the information below for each step and conducting user authentication by examining the consistency between the values input and registered information. In the case of Google, the input of a contact e-mail address is requested and an e-mail including the password reset URL is sent to that address if the e-mail address input by the user matches a previously registered e-mail address, regardless of the consistency of values input afterwards. Facebook requests the answer to a security question, such as "In what city or town was your mother born?", and if the user inputs the correct answer, then an e-mail including a password reset URL is sent.

- Other passwords used for the account
- Title of recently sent e-mail
- Folders other than default folder
- Receiver of recently sent e-mail
- Last 5 digits of prepaid card
- Name on credit card
- Date of last login
- Date of account creation
- Frequently used e-mail address
- Initial restoration e-mail address
- Last 4 digits of credit card number
- Expiration date

The difference in step two authentication of Korean and U.S. portals lies in the fact that there exists the means of authentication, resident registration no, in Korea and convenient user authentication is available accordingly thus there is no need to go through personal behaviour based user authentication procedure of U.S. portals.

4. ANALYSIS ON SECURITY THREAT AND SECURITY REQUIREMENT FOR PASSWORD AUTHENTICATION SYSTEM

The analysis on security threat that may occur during each authentication step of portals and SNS analyzed beforehand is conducted in this chapter. Analysis on possible security threat was conducted considering the threat that may occur during login procedure, password threat, and others.

4.1 Security Threat in Password Authentication System

4.1.1 Security Threat in Member Registration Stage

T1. Automatic Registration
Attackers make monetary gain through various methods such as sending SPAM mail for advertising, the distribution of malicious code to lure people to phishing sites and the posting of advertisements. Since more of these activities can be conducted if the attacker has more accounts available to him, accounts are created using automatic registration programs.

4.1.2 Security Threat in Login Stage

T2. Consecutive Login Attempts
The attacker attempts consecutive authentication using methods such as complete enumeration survey, password guessing, and others in order to obtain the password of user account. Complete enumeration survey is an attack method to obtain correct password by substituting all of possible password combinations and password guessing attack is a method to guess possible password by gathering information such as name, date of birth, family relations, and others of user. Also, there exists an attack method to attempt at authentication by substituting the information such as password that is most frequently used by the users.

T3. Phishing
The attacker outputs phishing site instead of normal site with method same as distribution of malicious code when users access to portals [12]. Since it is difficult for general users to distinguish phishing site from normal site, they input ID and password as normal and the attacker can obtain input ID and password at the moment.

T4. Keylogging
Keylogging is an attack technique which steals information by intercepting the information input with a keyboard, often using a keylogging program [13]. Although normally information input by keyboard is displayed on the monitor after processing by the OS, keylogging programs intercept the information and save it as a file as it is processed by the OS and subsequently leak that information by sending the file to a designated server. The attacker analyses the key sequences, and tries to identify those corresponding to portal logins to obtain IDs and passwords. For example, a large attack to control portal and SNS accounts using keylogging programs occurred in Dec 2013 in which about 2 million users' information was hacked from 93,000 web sites worldwide including 318,000 Facebook, 70,000 Google Gmail and 22,000 Twitter accounts, amongst others. The attacker obtains web site login records including web site IDs and passwords by installing keylogging programs on users' computers [14].

4.1.3 Password Reset- Authentication Phase 1

T5. Consecutive Login Attempts
By selecting e-mail authentication for user authentication at the password reset stage, the attacker may attempt consecutive logins to obtain the passwords of other accounts after gaining access to an email account. The difficulty of such an attack is lowered if e-mail account passwords are

weak, meaning of low entropy, facilitating the initial email account hacking [15]. In this way, the attacker can obtain the password of multiple user accounts using methods such as complete enumeration surveys amongst others.

T6. E-mail Sniffing
Sniffing refers to the tapping of others' network packets. Portals use e-mail and mobile phone authentication for user authentication at password reset step 1. E-mail authentication may send an authentication code or password reset URL to an e-mail address registered in advance, particularly at member registration. At that moment, if the attacker intercepts the e-mail sent by the portals or the password reset page through sniffing, then he can set a new password for the victim's account himself.

T7. Mobile Phone Tapping
Mobile phone tapping of an attack target is available if the attacker has installed malicious code on the victim's phone in advance. In this situation, when an SMS including the authentication code for password reset is sent to the victim, the attacker can obtain the authentication code for himself by tapping the victim's SMS. Thereby, the attacker can obtain authority over the user account by setting a new password for the victim's account.

4.1.4 Password Reset – Authentication Phase 2

T8. User Information Guessing
In the case of Google and MSN, user authentication is conducted using user account information when the user cannot use e-mail or mobile phone authentication. At the moment, information requested by portals can include the time of recent login, time of account creation, contact e-mail address and folder names. The attacker disguises himself as a target user by entering guessable information specific to the target. Particularly, when security questions are used, such as for Yahoo, the answers to the questions can be guessed when combining account information available from SNS accounts [16]. The attacker who thereby successfully answers security questions, often through informed guesses, can reset victims' passwords himself.

T9. Disguise as User
In case of Korean portals, user authentication at password reset- step 2 is conducted with the use of resident registration no. by receiving either Resident Registration no. or copy of identification card. However, frequent spill of personal data including Resident Registration no. makes us doubt about the effectiveness of system to conduct user authentication based on consistency of Resident Registration no. and name [17]. The attacker who obtained the Resident Registration no. of attack target can reset password after sending personal data via e-mail or fax by disguising as the attack target.

4.2 Security Requirements for Authentication System of Portals and SNS

Security affecting the security vulnerabilities of portals' and SNSs' password authentication systems at each stage, as discussed previously, are shown in Table 6.
R1. CAPTCHA

CAPTCHA is a method used to distinguish whether the user is an actual person or a computer program, using something easily distinguished by people but not computers, such as the contents of a picture showing intentionally distorted or overlapping letters [16]. Unmanned registration or authentication programs are executed automatically by computers rather than people so these automated attacks, which may try to create or access accounts, are blocked by CAPTCHAs. A complete enumeration survey attack is an attack that obtains the correct password through random substitution of the password mainly with the use of a computer program. In order to acquire portal accounts, the attacker can execute a complete enumeration survey program for consecutive login attempts. Therefore, the attack using complete enumeration survey program cannot be blocked in case of requesting the input of CAPTCHA at login.

Table 6. Security requirements that accommodate security threats

the Phasing of Security Threat / Security Requirement	Member	Login			Password Reset – Phase 1			Password Reset – Phase 2	
	T1.Automatic Registration	T2. Consecutive Login Attempts	T3. Phishing	T4. Keylogging	T5. Consecutive Login Attempts	T6.Email Sniffing	T7.Eavesdrop Smart Phone	T8.User Information Guessing	T9. Disguise as user
R1. CAPTCHA	×	×			×				
R2. Password with Enhanced Security Strength		×			×				
R3. Two channel authentication		×		×	×				
R4. Anti-Keyboard Hacking Program				×					
R5. Virtual Keyboard				×					
R6. Login IP Address Identification		×	×		×				
R7. Overseas IP Address Block		×	×						
R8. Anti-phishing and Countermeasures			×		×				
R9. Account Lock		×							
R10. Encrypted communication			×		×	×			
R11. Strength of Security Questions for Password Reset								×	×
R12. Installation of Vaccine Program (User)							×		

R2. Password with Enhanced Security Strength

The time it takes to crack a password and the difficulty of a complete enumeration survey attack is related to the user's password strength. For a user to create a password secure enough for a complete enumeration survey attack, the password should satisfy the following conditions [19].

- The inclusion of both upper and lower case letters, numbers, and special characters
- A minimum of 8 characters
- The prohibition of passwords based on guessable personal data such as the names of family members, phone numbers, etc.
- The prohibition of passwords which are the same as for other web sites

R3. Two channel authentication
Two channel authentication improves on the weak security of single channel authentication using a combination of two different authentication channels chosen from three sources: information possessed by the user, unique information or known information. The most common method is to

combine knowable information such as a password with possessed information such as OTPs, security tokens or smart phones. This approach can avoid the damage caused by ID theft through remote access.

R4. Anti-Keyboard Hacking Program

Keylogging refers to intercepting and recording the contents of users' input on either PCs or smart phones and its various methods may be based either in hardware or software, and include electronic or even acoustic technology [20]. Keylogging programs, hereafter referred to as keyloggers, are difficult to detect and delete once installed so users should take care not to install malicious programs. Vaccine programs and anti-keyboard hacking programs block the attacker from obtaining the ID and password of the user based on keyboard input. One method is to install a special security keyboard driver which outputs special characters, including '*' amongst others, to a security input window connected to the keyboard security driver and thereby transmits null values into the previous keyboard input stream so that no meaningful keyboard input can be intercepted. The second method is for a user to transmit an encrypted value from a separately installed keyboard security driver every time the user enters values into an input window with a new encryption key being created each time the user selects an input window. In this case, even if the attacker obtains the keyboard input values, he cannot know which value is associated with which true keyboard value as the stream is encrypted. The last method of evading keyloggers is instructing users to click input values with a mouse in a virtual keyboard window on the PC screen in case a keylogger is currently running. By installing these software-based technologies, users can block keyboard hacking programs.

R5. Virtual Keyboard

A virtual keyboard is a keyboard presented on screen for the input of passwords for public key certificates, and account passwords, amongst others, and is mainly used for banking transactions. Users enter input values through the on screen keyboard with a mouse click or touch in the case of smart phones or tablets. Since the keyboard structure of a virtual keyboard is created randomly, the actual value entered is not exposed even when the coordinate values are known. Thus, the attacker cannot easily obtain the actual value input from the encrypted format transmitted. Thus, password exposure can be prevented with this method even if the attacker attempts to obtain user passwords by installing a keylogger.

R6. Login IP Address Identification

User authentication is requested if the login IP deviates from the range of IP addresses saved from previous logins or if the IP addresses are different from the one of the last login. Users who succeed in user authentication are recognized as normal users and allowed account access while others are considered as attackers and denied account access.

R7. Overseas IP Address Block

SPAM mail is mostly sent from China and the account hacking of normal users in a given region is normally done from servers in that same region [21]. Therefore, portals should respond to related possible attack attempts by allowing the access of normal users through user authentication stages and then informing them of overseas login attempts from countries that they have not registered.

R8. Anti-phishing and Countermeasures

Anti-phishing methods include blocking sites presumed to be used for phishing after their detection and training users to distinguish phishing sites from normal ones. Phishing site detection methods are largely divided into searches for similar domains and HTTP traffic analysis. Phishing site detection through domain similarity can be classified into blacklist and whitelist techniques. Blacklist-based detection techniques register the addresses of servers known to be phishing sites and do not trust those addresses included. Whitelist-based detection techniques, on the other hand, register the addresses of legal servers and trust those included. HTTP traffic analysis detects sites which are disguised using links of pictures and postings from normal ones by monitoring and analyzing the HTTP traffic corresponding to requests for postings and pictures from normal sites referred to by the phishing ones.

R9. Account Lock
When an attacker conducts consecutive login attempts using a complete enumeration survey, user accounts will be obtained eventually if there is no restriction on the number of authentication attempts. Therefore, the acquisition of user accounts can be prevented by limiting the number of authentication attempts.

R10. Encrypted Communication
Encrypted communication refers to the transmission of content encrypted by means of a shared key in order to block the tapping or interception of unencrypted content by third parties. Since users who do not possess the key cannot access the plaintext, data spill can be prevented even when the packets themselves are exposed. Therefore, portals should provide encrypted communication for confidentiality, integrity, and user authentication of communications between entities.

R11. Strength of Security Questions for Password Reset
The types of security questions provided in the past were either easy for attackers to guess so insecure, such as "What is the name of your mother?" or difficult to remember so inconvenient, such as "What is your dream job?" [22]. Thus, service providers should improve user authentication security questions. Additionally, multiple security questions should be asked rather than just one, and a real person should be distinguished from an attacker by the percentage of correct answers given. Also, to improve user convenience the questions should be based on their experiences and behaviors when using their accounts so that, rather than having to actively remember the answers, a real user would just know them as a matter of course.

R12. Installation of Vaccine Program (User)
Secure smart phone use is possible when users install vaccine programs on smart phones which conduct regular inspection to pre-empt problems such as mobile phone tapping and data leakage, amongst others, which are caused by attackers using malicious programs.

5. MEASUREMENT OF THE POSSIBILITY OF SUCCESSFUL ATTACKS BY PORTAL SITE AND COMPARISON OF THE SAFETY

This chapter measures the possibility of successful attacks on the steps of the password authentication systems of each portal site based on the possibility indicators of successful attacks based on the common criteria mentioned in 2.2 and compares and analyzes their safety.

5.1. Measurement of the possibility of successful attacks by portal and SNS

This section measures the possibility of successful attacks on each portal site based on attack threats on the portal sites' password authentication systems and the security requirements created earlier.

5.1.1. Member registration

At the member registration stage, account creation using automatic member registration programs is the main attack threat. At the member registration stage, attack scenarios are similar across all portal sites because their security threats and countermeasures are similar. It takes less than one hour to create an account using automatic member registration programs. Furthermore, the general public can operate such programs because they do not require a deep knowledge of security. To prevent such attacks CAPTCHA and cell phone authentication is used. This policy is the information which was already opened. Automatic member registration programs which can overcome CAPTCHAs are classified as 'professional equipment' because they are available to only a small number of people in specific internet communities.

There are differences between Korean and overseas portal sites in terms of vulnerability to attack. It is impossible to continually create accounts on Korean portal sites, even when using automatic member registration programs, because users are restricted to three accounts per cell phone. However, overseas portal site registrations lack this restriction.

Table 7. Attack Potential of Membership Registration

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	1	1	1	1	1	1	1	1
Expertise	0	0	0	0	0	0	0	0
Knowledge of Object	0	0	0	0	0	0	0	0
Access to Object	1	1	1	0	0	0	0	0
Tools	7	7	7	7	7	7	7	7
Total	**9**	**9**	**9**	**8**	**8**	**8**	**8**	**8**

5.1.2. Log-in

Possible attack methods at the log-in stage include consecutive authentication attempts, phishing, and key logging. Attack methods are classified by attack technique when measuring the possibility of successful attacks. Since a system's overall vulnerability to attack is based on its weakest point, the overall possibility of a successful attack at each log-in stage is based on the attack technique with the minimum score.

5.1.2.1. Consecutive authentication attempts

The total time required for consecutive authentication attempts to be successful are calculated based on each portal site's password strength:

Table 8. Elapsed time for brute force attack

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	13 mins	1 hour 32 mins	6 days 4 hours	6 days 4 hours	82 days 21 hours	17 years 130 days	13 mins	13 mins

In Table 10 above, the time measurement was calculated supposing that the 'John the Ripper', attack tool, is run on an attacker's PC with a 3.4GHz Intel Core i7-2600K and assumes the use of the simplest password allowed. Naver, Facebook and Twitter take less time to attack because they use only 6-digit passwords and do not provide an account lock service. Yahoo takes the longest time because it makes use of a compulsory combination of upper and lower case letters as well as numbers. Naver and Nate were easier targets than other portal sites because they do not provide an account lock service.

Attack tools for consecutive authentication attempts are shown in Table 9. Everybody can obtain them because they are easily available on the internet and experts with enough knowledge about security can use them.

Table 9. Attack Potential of Consecutive Authentication Attempts

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	1	3	5	5	10	15	1	1
Expertise	6	6	6	6	6	6	6	6
Knowledge of Object	0	0	0	0	0	0	0	0
Access to Object	1	1	4	4	4	4	4	4
Tools	4	4	4	4	4	4	4	4
Total	**12**	**14**	**19**	**19**	**24**	**29**	**15**	**15**

5.1.2.2. Phishing

Phishing's probability of success depends on the similarity between the original sites and the special phishing sites built by attackers. If the source code of the log-in screen of a portal site is exposed, anybody can build the phishing site simply by copying the code. Otherwise, the phishing sites need to be built with web site building tools so as to be as similar as possible to the original. This process takes more time but usually only requires basic web knowledge. Google, MSN, Facebook and Twitter, take longer to attack than other portals because the source code of their log-in pages is not exposed. Because sites built by coping page sources are more similar to the original sites, attackers can obtain the passwords of more targets. Naver, Google, and MSN are applying anti-phishing technologies which give warnings about phishing or malware sites to not only tool bars, such as MSN Tool Bar-phishing filter and Naver anti phishing Toolbar, but also to browsers, such as Google Chrome. In addition, Yahoo provides a security seal service which is a phishing prevention technology that allows users to recognize that they are accessing the real site because pictures chosen by themselves in advance are presented at the log-in stage. Therefore, attacks on Naver, Google, MSN, or Yahoo are more difficult to create than those on Nate or Daum, when users take advantage of their anti-phishing technologies.

Table 10. Attack Potential of Phishing

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	3	3	3	5	5	3	5	5
Expertise	3	3	3	6	6	3	3	3
Knowledge of Object	0	0	0	3	3	0	3	3
Access to Object	4	1	1	4	4	4	1	1
Tools	4	4	4	4	4	4	4	4
Total	**14**	**11**	**11**	**22**	**22**	**17**	**16**	**16**

5.1.2.3. Key logging

All the portal sites have the same likelihood of successful attacks by key logging because it is controlled by users' browsing environments rather than a portal's security policies. User accounts can be obtained if users allow key logger programs access to run on their PCs and harvest and interpret ID and password values. The time required for key logging attacks depends on time needed to interpret the key values entered, and would usually be less than one day. Key logger programs are openly available on the internet and using them attackers can easily access the accounts of targets who read the malicious texts or spam mails which disseminate keyloggers.

Table 11. Attack Potential of Keystroke Logging

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	3	3	3	3	3	3	3	3
Expertise	3	3	3	3	3	3	3	3
Knowledge of Object	0	0	0	0	0	0	0	0
Access to Object	1	1	1	1	1	1	1	1
Tools	4	4	4	4	4	4	4	4
Total	**11**	**11**	**11**	**11**	**11**	**11**	**11**	**11**

The result showed that key logging's possibility of successful attacks is the lowest. Furthermore, all portal sites have the same vulnerability to this type of attack at the log-in stage.

5.1.3. Password reset - Phase 1

If users request a password reset, attackers can obtain their accounts by three methods, SMS wiretapping, complete enumeration surveys, and access via other e-mail accounts. Therefore, the possibility of successful attacks in the password reset step 1 of each portal site is based on the attack technique with the minimum score since security can only be as strong as its point of weakest defence.

5.1.3.1. SMS wiretapping

SMS wiretapping obtains authentication numbers as they are delivered to users' cell phones by installing wiretapping applications when users inadvertently install them during regular cell phone use. This method is effective when attacks are specifically targeted.

Malicious wiretapping applications can be created or purchased by attackers and ordinary people can easily use them. Because the authentication numbers transmitted to users by SMS for authentication via cell phone are valid for three minutes, attacks can be successful only if the authentication numbers can be obtained and the passwords reset within this time limit. Information about cell phones' weak points is considered to be openly available information because it can be obtained through on-line searches. As the success of these attacks is determined by the functionality of the malicious applications installed on users' cell phones, portals' vulnerabilities to such attacks are unaffected by their security policies. Thus, for all portal sites, the probability of this attack type being successful is the same.

Table 12. Attack Potential SMS Eavesdropping attacks

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	1	1	1	1	1	1	1	1
Expertise	0	0	0	0	0	0	0	0
Knowledge of Object	0	0	0	0	0	0	0	0
Access to Object	4	4	4	4	4	4	4	4
Tools	4	4	4	4	4	4	4	4
Total	**9**	**9**	**9**	**9**	**9**	**9**	**9**	**9**

5.1.3.2. Complete enumeration surveys of authentication numbers

It takes less time to conduct complete enumeration surveys as the number of cases is less because authentication numbers consist of 6-digit numbers. Portal sites provide account lock services if users fail in consecutive authentication of authentication numbers to respond to the complete enumeration surveys. The detailed contents are shown in Table 13. However, the accessibility to authentication numbers is difficult because there are the only five to ten chances to enter them in one million 6-digit numbers of cases as they are randomly transmitted in request repeat unlike the fixed passwords. And it can be found that it takes more than 6 months to attack authentication numbers.

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Input	5 times	5 times	5 times	3 times	3 times	3 times	3 times	3 times
Transmission	10 times	10 times	10 times	5 times	5 times	5 times	5 times	5 times
Account Lock	24 hours	24 hours	24 hours	24 hours	24 hours	24 hours	24 hours	24 hours

Although the tools, knowledge levels, and skill required for complete enumeration survey attacks on authentication numbers are the same as for consecutive authentication attempts, the time limit and targets of attacks depend on the policies of particular portal sites regarding the authentication number and its input or transmission.

Table 13. Attack Potential of Bruteforce Validation Code

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	15	15	15	15	15	15	15	15
Expertise	3	3	3	3	3	3	3	3
Knowledge of Object	0	0	0	0	0	0	0	0
Access to Object	10	10	10	10	10	10	10	10
Tools	4	4	4	4	4	4	4	4
Total	**32**	**32**	**32**	**32**	**32**	**32**	**32**	**32**

5.1.3.3. Accessibility to other e-mail accounts

Access via other e-mail accounts is a possible attack method if users choose to identify themselves for the purpose of password resets through e-mail authentication. Each portal site uses e-mail authentication methods like Table 17. Yahoo is immune to this attack because it only accepts cell phone authentication so email authentication is impossible.

Table 14. E-mail Authentication

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Authentication Method	Code	URL	Code	URL	Code	-	URL	URL
Open	1^{st} character	All	1^{st} character	1^{st} character	All	-	1^{st} character	2 characters

The time required for attacks through access via other e-mail accounts depends on portal sites' distribution of information to other accounts. Log-in attempts on the accounts used for this type of attack have the same possibility of success as normal log-in attacks on these sites. Because Nate and MSN make available the information of other accounts which transmit emails to them for identification, and it takes a short time to attack these portals, accessibility to other accounts is easier through them as attackers can attempt attacks on related accounts without assumption. Furthermore, for attacks via other accounts the attackers can use information they have obtained by themselves directly rather than though specific tools, so specialized security knowledge is not required.

Table 15. Attack Potential of E-mail Account attack

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	3	1	3	3	1	-	3	3
Expertise	0	0	0	0	0	-	0	0
Knowledge of Object	0	0	0	0	0	-	0	0
Access to Object	4	1	4	4	1		4	4
Tools	0	0	0	0	0	-	0	0
Total	**7**	**2**	**7**	**7**	**2**	**-**	**7**	**7**

From the previous analysis of the possibility of successful attacks during password reset Step 1, it can be concluded that the possibility of successful attacks using accessibility from other e-mail accounts is higher than the other methods. Therefore, the possibility of successful attacks in password reset step 1 is the same as the possibility of successful attacks exploiting the accessibility from other e-mail accounts.

5.2.4. Password reset – Step 2

Until August 2013 korean portal sites had provided for identification processes that utilize social security numbers. However, they had not provided phase 2 authentication services. To compare the safety of Korean and overseas portal sites, this paper measured the possibility of successful attacks on identification processes through the collection of social security numbers or information to answer social security questions.

Social security numbers are available to only a small number of people through distributors. The attackers who have obtained the social security numbers of attack targets can obtain their account information and receive their passwords from portal sites by forging or using them. It takes less than one week to attack targets, including searching for their IDs and checking their social security numbers and, furthermore, this attack can be easily carried out without specialist security knowledge.

The overseas portal sites verify users through questions based on their experiences or behavior during account use. Although attackers can guess the answers after collating information about users readily available on the internet, it takes experts about one week to collect and analyze the information. Special tools for the attacks are not required. However, the answers to the questions are considered important information because it is information which is remembered and known without special effort.

Table 16. Attack Potential of Password Reset-2nd Phase

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Elapsed Time	5	5	5	5	5	5	5	5
Expertise	0	0	0	3	3	3	3	3
Knowledge of Object	3	3	3	11	11	11	11	11
Access to Object	4	4	4	4	4	4	4	4
Tools	0	0	0	0	0	0	0	0
Total	**12**	**12**	**12**	**23**	**23**	**23**	**23**	**23**

5.2. Comparison and analysis of password authentication systems of portal sites based on the possibility of successful attacks

The safety of password authentication systems of portal sites is compared and analyzed based on the possibility of successful attacks measured in the previous section. The table which finally analyzed the possibility of successful attacks by step is as follow. Comparison of the safety by step of password authentication systems was analyzed that the safety of password reset Step 1 is lowest. It's because the vulnerability in the log-in stage is frequently used in attacks while attackers can more easily obtain passwords when it is actually done.

Table 17 Attack Score of Password Authentication Systems

	Naver	Nate	Daum	Google	MSN	Yahoo	Facebook	Twitter
Membership Registration	9	9	9	8	8	8	8	8
Login	11	11	11	11	11	11	11	11
Authentication phase 1	7	2	7	7	2	9	7	7
Authentication phase 2	12	12	12	23	23	23	23	23

A method to compare the safety of the Korean and overseas portal sites by step and strengthen them is as follow. The member registration stage can be found that the Korean portal sites are safer than the overseas ones because they limit the number of IDs. The possibility of successful attacks about attack scenarios of consecutive authentication attempts, key logging, and phishing was measured in the log-in stage. Key logging was analyzed to be all the same values in all the portal sites. The Korean portal sites and two of SNSs have found to be vulnerable to key logging attacks because they do not provide the methods which can respond to key logging attacks. The overseas portal sites can be found to be more vulnerable to consecutive authentication attempts than the Korean ones. It's because Facebook, Twitter, Naver and Nate do not provide account lock services and their password strength is lower than that of the overseas portal sites. They should improve their password strength and provide the account lock services to complement this. Phishing attacks of Naver, Google, MSN, and Yahoo have found to be safer than Nate, Daum, Facebook and Twitter because they provide the technologies to respond to them. However, the Korean portal sites and Yahoo were analyzed that phishing sites can easily be built because their source codes are exposed. They need to make their source codes' interpretation difficult to complement them and Naver and Daum should provide their own anti-phishing technologies.

Because possible SMS wiretapping attacks in password resent step 1 are related to the safety of user smart phones, users can be safe from the applicable attacks as it is recommended to install vaccine in them. Complete enumeration attacks of authentication numbers could be found to be safe because the Korean and overseas portal sites all limit the number of input and transmission of authentication numbers. If specific users are targets of attacks, attackers can more easily obtain passwords than the log-in stage by utilizing the accessibility to them through other e-mail accounts of the authentication stage through the e-mails in password reset step 1. If other accounts registered by users are exposed, the time required can be more reduced than the cases that they are not opened. And if password strength of the registered accounts is lower than that of the accounts that users try to reissue, the attack level of difficulty get to be lower if attackers attack the applicable accounts. Therefore, Nate and MSN that other account information is exposed should improve the safety just by exposing the partial accounts.

For the password reset step 2 service of the Korean portal sites, the authentication method which use social security numbers before Aug. 2014 was analyzed. As personal information leaks frequently occurred, the social security numbers are circulating the market. And attackers can easily obtain them. Therefore, password reset by attackers disguised as users had no major difficulties. The overseas portal sites are safer than the Korean ones as it is difficult for attackers to guess right answers because the information contents of users are not opened because they are based on the experiences that they just know.

6. CONCLUSION

This paper analyzed the authentication systems of Naver, Nate, Daum, Google, MSN, and Yahoo, the main Korean and overseas portal sites, and clarified existing security threats and the security improvements necessary to remedy them, and analyzed the application of the security requirements which were drawn in each portal site to them. From the analysis of the password authentication systems of the Korean and overseas portal sites it was found that the Korean portals Naver and Nate are more vulnerable to complete enumeration attacks than the overseas ones because they do not provide account lock services. However, it was also found that the foreign portals did not provide a service blocking logins or the identification services from overseas, except Google. This may be because for users with malicious intent, the creation of new accounts is preferred over attempts to seize existing users' accounts because the number of multiple IDs which can be created has no limit. However, because the motivation for attacks seizing users' accounts is not only their acquisition for sending spam mails but also accessing the private user information they contain, protection against this should be improved. Furthermore it has been found that both Korean and overseas portal sites do not force users to make safe passwords. Because exploiting weak passwords is an attack method not only at log-in but also password reset step 1, all the portal sites should make creating safe passwords compulsory. The Korean portals should also improve the convenience of users who do not use their cell phones for authentication at password reset step 2 by using user behavior-based authentication methods or develop new methods as the overseas portal sites have done.

This paper analyzed the entire process of password authentication on Korean and overseas portal sites, explained their potential security vulnerabilities, and proposed security-hardening solutions for each process. Moreover, it quantitatively compared and analyzed the safety of the password authentication systems of the major Korean and overseas portal sites by the creation and use of a standardized set of criteria to express the possibility of successful attacks.

ACKNOWLEDGEMENTS

This work was supported by the ICT R&D program of MSIP/IITP. [2014(10043959), Development of EAL4 level military fusion security solution for protecting against unauthorized accesses and ensuring a trusted execution environment in mobile devices]

REFERENCES

[1] Bruce Schneier, “Applied Cryptography”, John Wiley & Sons, 1996.

[2] Perlman, Radia, and Charlie Kaufman. “User-centric PKI”. Proceedings of the 7th Symposium on Identity and Trust on the Internet. ACM, 2008.

[3] Just, Mike, and David Aspinall. “Personal Choice and Challenge Questions: A Security and Usability Assessment”. Poceedings of the 5th Symposium on Usable Privacy and Security. ACM, 2009.

[4] Jin, Lei, Hassan Takabi, and James BD Joshi. “Analysing security and privacy issues of using e-mail address as identity.” International Journal of Information Privacy, Security and Integrity, 1.1. 34-58. 2011.

[5] C.E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, 1948, pp. 379–423.

[6] Komanduri, Saranga, et al. "Of passwords and people: measuring the effect of password-composition policies." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2011.

[7] Ma, Wanli, et al. "Password entropy and password quality." Network and System Security (NSS), 2010 4th International Conference on. IEEE, 2010.

[8] Yan, Jianxin Jeff. "A note on proactive password checking." Proceedings of the 2001 workshop on New security paradigms. ACM, 2001.

[9] Bishop, Matt. "Proactive password checking." 4th Workshop on Computer Security Incident Handling. 1992.

[10] “Common Methodology for Information Technology Security Evaluation.” Common Criteria, Version 3.1. 2009.07.

[11] Cazier, Joseph A., and B. Dawn Medlin. "Password security: An empirical investigation into e-commerce passwords and their crack times." Information Systems Security 15.6. pp.45-55. 2006.

[12] Ji Sun Shin, “Study on Anti-Phishing Solutions, Related Researches and Future Directions,” Journal of The Korea Institute of Information Security & Cryptology, Vol.23, No.6, Dec.2013.

[13] Leijten, Mariëlle, and Luuk Van Waes. "Keystroke Logging in Writing Research Using Inputlog to Analyze and Visualize Writing Processes." Written Communication 30.3, pp.358-392, 2013.

[14] “2014 Trustwave Global Security Report“, Trustwave, 2014

[15] Dell'Amico, Matteo, Pietro Michiardi, and Yves Roudier. “Password strength: An empirical analysis.” INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.

[16] Irani, Danesh, et al. "Modeling unintended personal-information leakage from multiple online social networks." Internet Computing, IEEE 15.3 ,pp.13-19. 2011.

[17] HyeongKyu Lee, “The Problems and Reformation of the Personal Identification by the Resident Registration Number on the Internet”, Hanyang Law Review, Vol. 23-1, pp.341~371, 2012. February.

[18] Von Ahn, Luis, et al. “CAPTCHA: Using hard AI problems for security.” Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003. 294-311.

[19] Jin, Lei and Takabi, Hassan and Joshi, James B.D, “Analysing security and privacy issues of using e-mail address as identity,” International Journal of Information Privacy, Security and Integrity, 1 (1). pp. 34-58. 2011.

[20] Goring, Stuart P., Joseph R. Rabaiotti, and Antonia J. Jones. "Anti-keylogging measures for secure Internet login: an example of the law of unintended consequences." Computers & Security 26.6. pp.421-426. 2007.

[21] “Kaspersky Releases Q1 Spam Report,” Kaspersky, 2014.

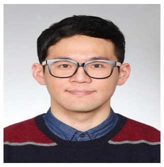
[22] Jin, Lei and Takabi, Hassan and Joshi, James B.D, “Analysing security and privacy issues of using e-mail address as identity,” International Journal of Information Privacy, Security and Integrity, 1 (1). pp. 34-58. 2011

AUTHORS

Heekyeong Noh received her B.S degree in Internet Information Engineering from Duksung Women’s Unviersity of Korea, in 2012. She is currently working toward M.S degree in Information Security, Korea University(KU), Korea. Her research interests include password security, security engineering, and Common Criteria(CC)

Changkuk Choi received his B.S degree in Department of Chemical Engineering from Kwang Woon University of Korea, in 2000. He is currently working toward Ph.D degree in Information Security, Korea University(KU), Korea. His research interests include hacking, CCTV security.

Minsu Park received his B.S degree in Computer Network from Silla University of Korea, in 2010 and also received his M.S degree in Information Security from Korea University(KU) of Korea in 2013. He is currently working toward Ph.D degree in Information Security, Korea University(KU), Korea. His research interests include information assuarance, digital forensic, and usable security.



Jaeki Kim received his B.S. (2013) in Computer Engineering from Hanyang University ERICA in Korea. and, He served as Security Technology Team of the INetCop for 1 years. also, He participated a program for the training next-generation's best IT security leaders, called 'Best of the Best' 2nd (2013). His research interests include Android Security and Embedded devices Security. He is now a graduate student at CIST SANE LAB, Korea University.

Seungjoo Kim received his B.S., M.S. and Ph.D. from Sungkyunkwan University (SKKU) of Korea, in 1994, 1996 and 1999, respectively. Prior to joining the faculty at Korea University (KU) in 2011, He served as Assistant & Associate Professor at SKKU for 7 years. Before that, He served as Director of the Cryptographic Technology Team and the (CC-based) IT Security Evaluation Team of the Korea Internet & Security Agency (KISA) for 5 years. He is currently a Professor in the Graduate School of Information Security at KU, and a member of KU's Center for Information Security Technologies (CIST). Also, He is a Founder and Advisory Director of a hacker group, HARU and an international security & hacking conference, SECUINSIDE. Prof. Seungjoo Kim's research interests are mainly on cryptography, Cyber-Physical Security, IoT Security, and HCI Security. He is a corresponding author.