Estimating Resident Registration Numbers of Individuals in Korea: Revisited

Heeyoul Kim[1†], Ki-Woong Park[2†], Daeseon Choi[3], and Younho Lee[4*]
[1] Department of Computer Science, Kyonggi University, Korea
[e-mail: heeyoul.kim@kyonggi.ac.kr]
[2]Department of Computer and Information Security, Sejong University, Korea
[e-mail: woongbak@sejong.ac.kr]
[3]Department of Medical Information, Kongju National University, Chungnam, Korea
[e-mail: sunchoi@kongju.ac.kr]
[4] ITM Programme, Department of Industrial and Systems Engineering, SeoulTech, Korea
[e-mail: younholee@seoultech.ac.kr]
[†]Co-first authors
*Corresponding author: Younho Lee

Received December 15, 2017; revised January 12, 2018; accepted January 26, 2018; published June 30, 2018

Abstract

Choi et al's work [1] in 2015 demonstrated that the resident registration numbers (RRNs) of individuals could be conveniently estimated through their personal information that is ordinarily disclosed in social network services. As a follow-up to the study, we introduce the status of the RRN system in Korea in terms of its use in the online environment, particularly focusing on their secure use. We demonstrate that it is still vulnerable against a straightforward attack. We establish that we can determine the RRNs of the current president Moon Jae-In and the world-class singer PSY.

Keywords: Resident Registration Number, Web service attacks, Personal Information Security, Information Security

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (NRF-2016R1C1B2011022, NRF-2016R1A4A1011761).

http://doi.org/10.3837/tiis.2018.06.027 **ISSN : 1976-7277**

1. Introduction

The resident registration number (RRN) that the government issues to each individual at birth in Korea is used for various purposes to manage personal information and contains important personal information that should not be leaked, such as the date of birth, gender, and place of registration. It can serve as an identifier of an individual in both the online and offline environments. However, as the internet became active in the 2000s[1], online service providers abused the uniqueness of the RRN and used it as confidential information for identifying the user. Consequently, malicious attackers attempted to obtain the RRN of general users for identity theft; as a result, numerous online identity theft cases using the leaked RRNs have occurred [1].

To prevent the misuse of RRNs, the Revised Personal Information Protection Act [2], enforced in 2014, stringently restricted the collection and use of RRNs. In particular, the collection of RRNs is prohibited except for certain fields designated by law. Since then, online services have not received the permission to obtain the RRNs of users in accordance with the revised law. In addition, these service providers enhanced their systems through technical security improvement such that the systems cannot be used for the collection of RRNs by malicious entities.

However, notwithstanding the enforcement of these laws, Choi et al reported that malicious attackers could determine the RRN of users owing to the characteristics of the RRNs and the security breach of online services. They have established the feasibility of identifying the RRNs of Korean celebrities [1].

This study describes the changes in the use of RRNs in the Korean online system after the study [1] and reaffirms the existence of security vulnerabilities related to RRNs. Subsequent to the study of [1], an improvement in Korea's online use of RRNs in terms of security is the removal of the modules that can be used to verify the RRNs of individuals who use online services. However, a few credit rating agencies and government websites still have modules to validate RRNs.

Based on this, in this study, we identified a site that is legally permitted to collect RRNs and examined whether the RRNs of individuals can be obtained through the automated use of the RRN verification module on this site. Although it is challenging (compared with the RRN verification module used in [1]) to utilize automated programs owing to the use of JavaScript in the identified module, we have overcome this challenge by using selenium [3], a most recent web automation verification tool in Python environment; moreover, we have verified that the RRN verification module can be used automatically.

Using the code for the automated use of RRN verification module, we have created a program that can be used to identify the RRN of a target person. In our experiment, we could identify the RRNs of two celebrities in Korea: President Moon Jae-In and the singer PSY, who is renowned for his globally popular song "Gangnam Style." In each of these cases, the time we consumed to identify the RRN was less than 10 min, which demonstrates the severity of the security vulnerability of the current RRN system for online use.

The rest of this paper is organized as follows: Section 2 includes an introduction to the RRN system and a description of the related research on RRN exposure. Section 3 discusses the methods used to obtain RRNs and describes the results. Section 4 discusses means to prevent the leakage of RRNs. Section 5 concludes the paper.

[1] According to [4], the internet became widely used since 2000s.

2. Related Work and Motivation

In this section, we introduce the Korean RRN system and describe the related research on the security of the national identification numbers similar to RRN. Finally, we describe the motivation for this paper.

2.1 The Resident Registration Number (RRN) system in Korea

In Korea, each citizen obtains a RRN when he/she is born. The RRN is unique to every citizen and is generally used for personal identification purposes. Particularly, in Korea, certain surnames such as Kim, Lee, and Park are used by numerous individuals. Moreover, traditionally, members of the same family tend to use similar letters in part of their first names. Therefore, there are numerous individuals in Korea with the same name. Therefore, it is essential to assign a unique ID to each person in order to identify her/him. The RRN system was activated in South Korea in the 1960s in response to the frequent armed espionage by North Korea, to enhance the detection of North Korean agents [5]. In 1975, the Korea Development Institute (KDI) modified the US social security number system to fit the Korean situation and established the 13-digit resident registration number system in its current form.

The structure of an RRN is shown in **Fig. 1**. The first six digits represent the date of birth. The first digit of the remaining seven digits contains information about the sex and about the first two digits of the birth year: while an odd number denotes male, an even number denotes female; moreover, while the digits 1 and 2 imply birth in the 1900s, 3 and 4 imply birth in the 2000s. The digits 5–6 and 7–8 are similarly used for registered foreigners and foreign nationals, respectively. Moreover, C in **Fig. 1** is calculated by the following equation. If all the digits in an RNN except the last digit are specified (denoted as a[1]–a[12]), the following formula can be used to derive C:

$$C = (11 - ((\sum_{i=1}^{8}(i+1)a[i] + \sum_{i=9}^{12}(i-7)a[i]) \bmod 11)) \bmod 10$$

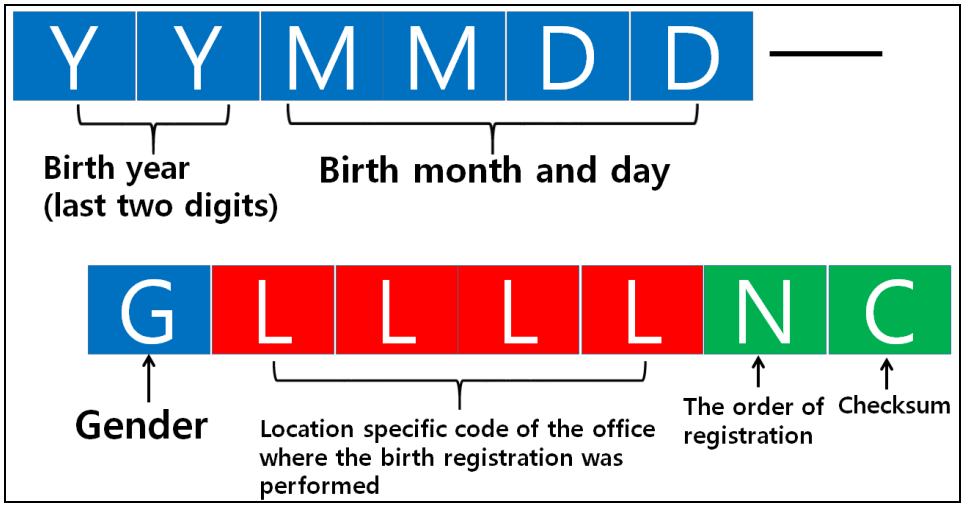

Fig. 1. Structure of RRN

The RRNs were collected and used for various purposes without restriction until the revision of the Personal Information Protection Act in Aug 2014. **Table 1** presents the use of RRNs before the amendment of the law [7]. A key point here is that they were used as credentials for self-certification and for verifying adulthood. They were abused for such authentication purposes, stored in numerous internet services, and, owing to their ineffective

management, have been exposed by malicious attackers. According to [6], in 2017, the RRNs more than the Korean population were leaked to malicious attackers during 2011~2014.

Table 1. Utilization of RRN (before revision of Personal Information Protection Act in Aug 2014) [6]

Areas of use		Where to use
Public sector		- Used in legal forms - Used to look up the data related to work by the national and local governments - National Police Agency, National Pension Service, National Pension Corporation, National Health Insurance Corporation, Ministry of Public Administration and Security, Ministry of Land, Transport and Maritime Affairs, Ministry of Knowledge Economy, Blue House, Local Government, Military Manpower Administration
Private sector	Financial institution	- Collect and use RRNs to examine whether the parties are the real persons in the financial transactions such as credit card issuance and fund transfer.
	Insurance business	- Identification of policyholders and insured individuals, calculation of insurance premiums, calculation of insurance benefits, insurance accident investigations, etc. - For individual insurance companies to periodically exchange personal information with insurance development institutes, insurance associations, bank associations, and national institutions using individuals' RRNs and to provide personal information to police, courts, tax offices, and military manpower at irregular intervals - Exchanging related information with other insurance companies, medical institutions, credit information companies, etc. in order to conduct insurance accident assessment, inspections, medical examination, self-certification, and duplicate insurance proportional reimbursement examination.
	Medical business	- Medical institutions collect and use the RRN of patients and employees based on medical law, national health insurance law, etc. - Public sector and medical institutions use RRNs to link personal information, while public institutions refer to the Insurance Evaluation and Assessment Service, the Korean Nursing Association, the Public Health Center, the National Statistical Office, the National Health Insurance Corporation, and the Health Insurance Evaluation and Evaluation Center. -
	Communication service businesses	- For identifying individuals for membership subscription/termination and the collection of communication service cost - Used as a link to exchange personal information with public sector institutions such as the Ministry of Public Administration and Security, Ministry of Health and Welfare, National Tax Service, the police, and Korea Information and Communications Promotion Association
	Others	- Used for general purchasing, membership registration, and marketing purposes in general companies and various organizations providing goods and services - Used for the purpose of name authentication, duplicate registration prevention, adult authentication, etc.

After the amendment of the Personal Information Protection Act, the collection of resident registration numbers was stringently limited by law. **Table 2** summarizes the operators and their statutes regarding permission to collect RRNs [7].

Table 2. Ground laws of cases that permit collection and use of RRNs

Ground law		Content	Applicable entities
Act on Real Name Financial Transactions and Confidentiality	Article 3	Financial companies have the obligation to verify the name and RRN on the resident registration card of the financial transaction entity.	Banks, insurance companies, credit card companies, etc.
Credit Information Protection Act	Article 34	Credit rating and personal information management companies can collect personal information such as RRN after obtaining consent from the user as well as manage and provide personal credit information based on it.	Banks, insurance companies, card companies
E-Commerce Consumer Protection Act	Article 6	E-commerce and telecommunications operators must preserve transaction records and related personal information.	Electronic financier
Electronic financial transaction law	Articles 6,7,16	- A financial institution or an electronic financier must verify the identity of the user for electronic financial transactions. - A financial institution or an electronic financier must preserve the information about an electronic financial transaction counterparty. - Those who use e-money over 50 000 won should provide their names and RRNs to the transaction counterparty.	Electronic financier
Tax Exemption Restriction Act	Article 126-3	For the issuance of cash receipts, businesses can collect and use RRNs.	Cash receipt issuer
VAT law	Article 16	- When issuing a tax invoice to a person who has been provided with goods and services, the address / name / RRN of the person should be supplied in the tax invoice. - When a taxpayer declares a deductible tax credit to a tax office under the jurisdiction of the taxation authority, the taxpayer's RRN should be provided. - When a telecommunication vendor reports an entity (supplementary communication carrier) that handles VAT payment, etc. to the relevant taxation office, it is necessary to include the RRN of the telecommunication vendor in the entity selection report.	Those who supply goods or services (general business operators)
Income tax law	Article 145	- If it is required to issue a withholding receipt at the time of payment, it is mandatory to include the RRN of the recipient in the receipt. - When submitting the payment statement for other income, etc. to the tax office of the jurisdiction, the RRN of the other-income earners should be specified.	Withholding agent

Medical law	Enforcement rule articles 9,12,14	Hospitals shall include the RRN of the patient in items such as medical certificate, prescription, and medical records.	Hospital
Insurance Business Act	Article 102 of the Enforcement Decree	An individual entrusted by the Financial Services Commission and Financial Supervisory Service can process unique identification information, including RRNs, for the performance of business.	Insurance Association
Qualifications Framework Act	Articles 23,24	The qualification manager can collect and use RRN for management purpose and as an item described in the qualification certificate.	Officially Qualified Qualification Management Authorities
Customs Act	Article 254	The overseas purchasing agent and the overseas shipping agent shall list the RRNs of shippers importing goods when the import declaration forms are written and can collect and use the RRNs when the importing shippers are the purchasers.	Overseas Purchasing Agent, Overseas Shipping Agent
Employment Insurance Act	Article 41 of the Enforcement Decree and Article 60	- When the employer conducts vocational competency development training for the employee, the employer can apply for support in incurring the expenses of the vocational competency development training, and the institution that carries out the vocational competency development training can pay the training cost to the trainee. The worker's RRN should be mentioned in the statutory form to be submitted for application.	Employer or training organization
Telecommunications Business Law	Article 83	When the investigation agency requests for communication data in accordance with the Telecommunications Business Act, the telecommunication operators should submit the RRN of the individual to whom the data pertains.	Telecommunication operator
Electronic Signature Act	Article 15	The issuer's RRN is required when an official digital certificate is issued.	Certified Certificate Authority
Broadcasting law	Article 65	An individual requesting disclosure of information to a broadcasting company shall notify the broadcasting company of the individual's RRN.	Broadcasting company
Act on Special Measures for the Promotion of Venture Business	Article 15	The RRNs of the shareholders are included in the contract document when the stock exchange contract of the venture company is prepared.	Venture company

For the purposes mentioned in **Table 2**, RRNs are exceptionally collected and used. These online services continue to collect them online, and a few of these collection modules include the capability to verify whether the entered name and RRN are correctly matched.

2.2 Work related to estimation of national identification numbers

The current state of research on the security vulnerability of the Korean RNN system, in particular the extraction of the RRNs of users by reasoning based on open public user information, is as follows. To our knowledge, [1] is the first study of attacks attempting to derive the RRNs of individual based on public information through inference and learning. This study demonstrates that it is feasible to derive a user's RRN by using the public information of the user in social network services such as Facebook and a real-name authentication site in which one can verify whether the derived name for a particular RRN matches with the actual name available at the site. Based on this, the feasibility of deducing the RRNs of celebrities was demonstrated.

[8] analyzed the distribution of RRNs excluding the date of birth, gender, and checksum information by using the RRNs of Koreans leaked to Chinese web sites. The researchers then used the derived distribution information of these RRNs to efficiently select candidate numbers to be tested in order to determine a person's RRN when only the name, birthday, and gender of the person are exposed. The selected candidate numbers are verified in order using the real-name authentication site. However, this study did not exploit the fact that the part of the RRN to be inferred was related to the information regarding the place where the user was registered when he/she was born. As the verification order is determined straightforwardly with the distribution of the RRNs that are collected from the Chinese web sites, it is necessary to use the RRN verification module more than a few thousand times on an average to derive the RRN of a target user. [6] discussed the current state of the RRN system and the problems caused by leakage of the RRNs through the external attacks by the systems and recommended the solutions for these.

The studies on the security of national-level personal identification number outside Korea are as follows. [9] introduced the Personal Identification Number (PIN) system used in Sweden and described the advantages of linking PINs to medical information for research. In addition, it discussed the problem encountered when incorrect PIN and medical information are connected and claimed that the social benefit from the connection of the PIN and medical information is higher than the ethical problem that can occur by the use of the PIN. In addition, the Norwegian, Danish, and Finnish PINs are introduced. [10] proposed a straightforward scheme that uses secret PINs and device-dependent random numbers to protect the US Social Security Number from eavesdropping when they are used in electronic devices.

[11] studied unique personal identifiers used at the national level. The study described that in numerous countries, national-level personal identifiers are used primarily for identification and authentication purposes and that it can be used for various other purposes such as immigration, voting, taxation and administration, social security and health care management, verification of personal information such as age, date of birth, etc. In this research, the threats and attack models against the use of unique personal identifiers are discussed. Moreover, based on the discussion result and the motivation of attackers, the security and privacy requirements to consider when creating personal identification number methods are addressed. Then, the cases of various countries were introduced. This study focuses particularly on the case of Estonia. The identifiers used in Estonia are open to public use although there is a problem of privacy breach because the identifiers contain the holders' birthdate information. For authentication and digital signatures, a pair of private keys (one for authentication and the other for generating an electronic signature) can be used. They are stored on an individual ID card and are protected by a separate PIN against malicious accesses. Therefore, the personal identifier has only the PIN as the unique identifier of the personal information, and based on this, it can be used for classification and connection of the personal information managed in

various places. According to [11], this numbering scheme has been used for over a decade; however, no major security issues have been observed.

[12] introduced a Unique Identifier (UID) project in India based on bio-signals. In this paper, the authors derived the security and functional requirements of the unique identification number system from the US SSN cases. Moreover, the advantages and disadvantages of using various bio-signals as UIDs are analyzed, and the points to be considered when implementing UID systems are discussed. [13] demonstrated the feasibility of deducing the social security number of a number of individuals using various publicly available data.

2.3 Motivation

This study investigates whether the risk of RRN leakage online is present notwithstanding whether the online environment has been strengthened in terms of the security against attacks on RRNs since 2014. This study extends [1] as a follow-up study. We discuss whether the protection of RRNs is strengthened in the online environment compared with the environment of [1]. The goal of this research is to verify the likelihood of exposure of users' RRNs in the current situation using feasible attack methods and finally to determine whether the current online environment protects the resident registration number adequately. This study is aimed at forming a theoretical basis for the evaluation of the current RRN system in the future. We hope that the results of this study will serve as the basis for government decisions.

3. Main Result

3.1 Change of online environment in Korea since 2015 in terms of protection of RRN

This subsection discusses whether vulnerabilities continue to be present in in various online environments, which were exploited in the RRN estimation attack discussed in [1]. The first is related to the disclosure of personal information of the users who have been attacked. As the RRN is composed of the user's personal information, the more the personal information is exposed, the higher the accuracy of the RRN estimation by the attacker. It is conjectured that numerous enhancements have been achieved in connection with this field. In particular, social network services such as Facebook have been improved to permit enhanced personal information protection by providing more granular access control policies to external users and users when disclosing their personal information to the outside.

However, we could verify that the online environment in Korea still exposes a substantial amount of personal information about celebrities. We can conveniently identify the personal information of celebrities from Naver (http://www.naver.com), the portal site with the highest share in Korea, as shown in **Fig. 2**. The figure shows an example of revelation of personal information of celebrities on the Naver website. Using the personal information of the celebrities described in **Fig. 2**, it is feasible to acquire a substantial amount of information about their RRNs. The left side of **Fig. 2** presents the information of Moon Jae-in, who is the current president of the Republic of Korea. (A) in **Fig. 2** presents the date of birth and place of birth of the person. With (A), we can conveniently derive the first six digits of his RRN because they refer to the birthdate. Moreover, we can significantly reduce the search space for the digits L_1–L_4 (in **Fig. 1**) in the RRN with the aid of the birthplace information. In particular, only a few candidates remain for the (L_1, L_2) digit pair from among 100 feasible combinations.

The right side in **Fig. 2** presents a Korean singer PSY, who gained worldwide recognition through a song called 'Gangnam Style'. Similar to the case on the left, we can obtain his

information from www.naver.com. However, in this case, unlike the case on the left, there is no information on his birthplace; therefore, it is challenging to obtain the information on L_1–L_4 in the RRN. However, as www.naver.com also discloses the educational information of the individual, it is feasible to deduce the birth place of the person based on the name of the elementary school he graduated from, shown in (C) in the figure: from an examination of the location of the school, we can derive that PSY was probably born in the Gangnam-gu district.

Fig. 2. Examples of personal information disclosure by Korean celebrities at www.naver.com. (A) represents the birth date and the place of birth of the president Moon Jae-In, (B) represents the birth date of PSY, and (C) represents the name of the elementary school from which PSY graduated

Secondly, we discuss the changes in the online environment regarding the security of the systems in the Internet in terms of feasibility of estimation of RRNs. As a key element for successful attack used in the study of [1], a RRN verification module accessible via the Internet is required. There are numerous security improvements in this respect. Compared to the situation in 2014, wherein a number of government websites maintained the RRN verification modules, most of the government websites no longer support them. Moreover, it is no longer feasible to verify the RRN on the website of the Korea University Admission Office, which was used to launch an attack in [1].

Therefore, we start looking for an RRN verification module in two directions. First, we investigate the online services of exceptional providers, which are permitted the use and collection of RRNs, listed in **Table 2**. As a result, we could verify that an RRN/username match verification module is provided on AllCredit's website (www.allcredit.co.kr) [14], which offers services of credit evaluation and credit information provision. **Fig. 3** shows the RRN verification module provided by AllCredit as of Dec 5, 2017. We have used this to determine whether particular RRN/name pairs are correctly matched or note.

Secondly, we analyze web sites that provided real name authentication in the past and examine whether the real name authentication page can be accessed by a bypass method even if the real name authentication function cannot be used through the normal route. We have identified a page [15] through Google search and verified that the page can also be used for RRN verification.

3.2 Estimating RRNs in the current online environment

In this subsection, we derive the RRNs of the president of Korea and the singer PSY (whose Korean name is Park Jae-Sang, as presented in **Fig. 2**) based on the security vulnerability to RRN inference attack in the current internet environment in Korea (described in the previous subsection).

We attempted to automate the use of AllCredit website's RRN verification module described in the previous section. First, we attempted to automatically input and verify a large number of RRN/name pairs using the python modules used in [1]. However, as the user input is processed using the JavaScript functions that are implemented with the external JavaScript functions and modules in the web page where the RRN verification module is present, the corresponding attempt could not be made. Thus, we have developed a method to automatically provide user-input to input widgets on the web page with a Selenium webdriver [3] such that the corresponding RRN verification module can be executed in an automatic manner. The Selenium webdriver is a tool for automated testing of web applications. It enables users to test their web application by providing input information to the input forms such that it appears as if the user is typing information directly on the keyboard and clicking objects directly with the mouse. As of December 2017, Selenium webdriver provides customized drivers for automation of various web browsers including Chrome, Firefox, Microsoft Internet Explorer, and Safari. They enable automated input to web pages provided through each web browser. Unlike the technique used in [1], if the Selenium webdriver is used, buttons implemented by JavaScript function calls can also be clicked in automatically. Based on this Selenium webdriver technology, we execute the code presented in **Fig. 4** through the web page on the AllCredit website on which the RRN verification module is present and deduce the RRNs of the president of the Republic of Korea Mr. Moon Jae-In and PSY.

Fig. 3. RRN verification module on AllCredit website (http://www.allcredit.co.kr) ((A): input box to enter name, (B): input box to enter RRN)

Details of the code of the proposed implementation presented in **Fig. 4** are provided below[2].

[2] The description of the generalized version of this algorithm is given in [1].

(A) to (F) below correspond to the same notations in the figure:

(A) The code imports the necessary modules.
(B) The code loads the necessary Selenium drivers to provide automated user input for pages within the Chrome browser. Then, go to the main page of www.allcredit.co.kr.
(C) On the main page, the code prompts you to access the page that contains the module for verifying your RRN. As a result, the web page on the right side of **Fig. 4** is displayed.
(D) The code sets three check-boxes at the bottom of the web page being visited.
(E) The code stores the name of the RRN inference target in name; p1 stores the first half (birth date) of the RRN, and the other half (gender, area code, registration order, checksum) is stored in pt2.
(F) Put the values stored in name, p1, and pt2 in the input forms on the web page.
(G) Execute the JavaScript function fnSearchSSn (). (= Similar effect as pressing "OK" button during an actual user input)
(H) The code displays the currently-tested RRN in the console window. By utilizing the fact that an alert box pops-up when an incorrect pair of RRN/name is entered by the user, the code concludes that the pair is correct if the alert box does not pop-up. In case no alert box pops-up, the program exits.

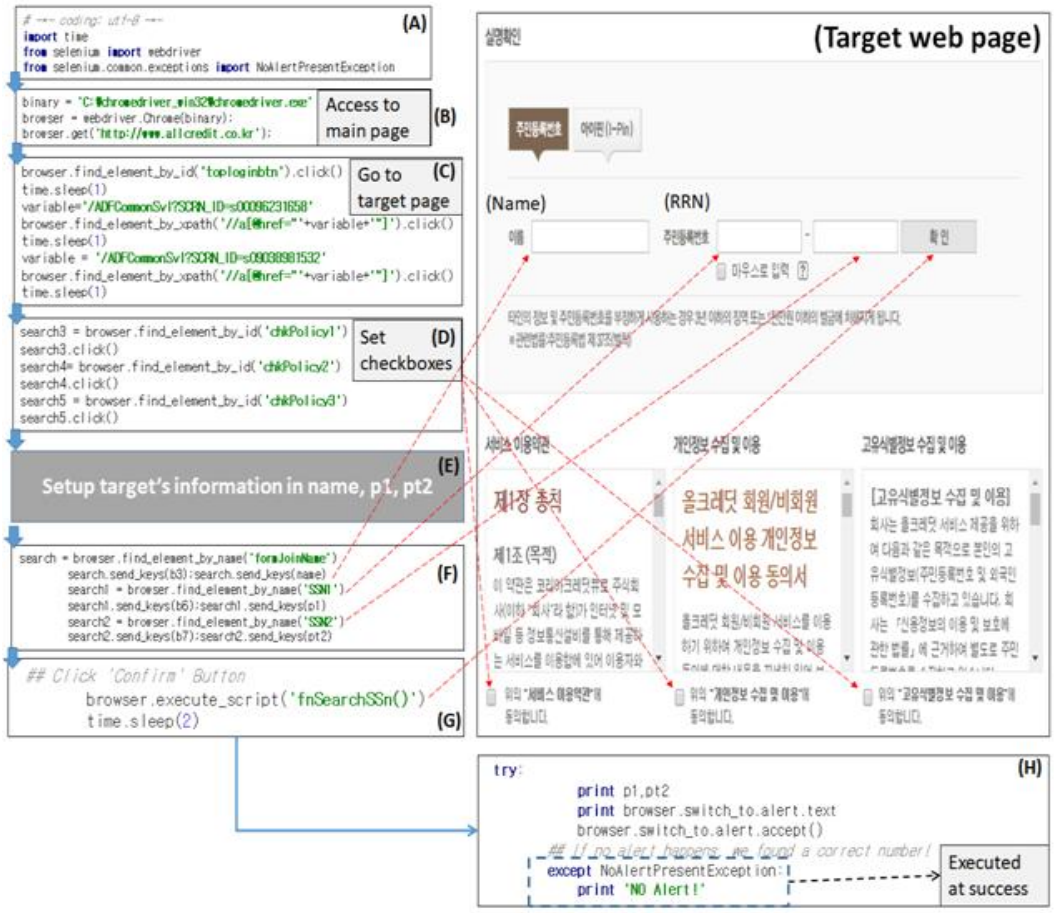

Fig. 4. Main implementation of the RRN inference module through AllCredit website

Step (E) determines the sequence of RRN values to be tested such that the code can determine the correct RRN of the attack target with the least number of verification module calls. In the code used in the experiment, if the RRN / name pair is incorrect after (H), the execution returns to (E); the next candidate RRN is identified, and the remaining steps are repeated.

We explain the method to determine the order in which candidate RRNs are to be searched in the entire possible RRN space of the target user in order to implement (E). For convenient explanation, we use the case of President Moon as an example. **Fig. 5** presents a strategy for inferring the RRN of President Moon Jae-in. In the figure, C is a checksum; therefore, it can be identified if the remaining numbers are determined. We observe from **Fig. 5** that we need to deduce only the digits from L_1 to L_4 as the other digits can be derived based on the information available in the published information in www.naver.com. According to the information in [5], there are only four feasible pairs of L_1 and L_2 values (09,10,11,12). Therefore, it is feasible to determine the RRN of President Moon by testing the candidate RRN through up to 400 executions of the RRN verification module. In the experiment, we determined the RRN of President Moon Jae-In to be 530124-110□□01 through 155 executions of the RRN verification module. Similarly, PSY's RRN was determined as 771231-106□□18 through 283 such executions[3].

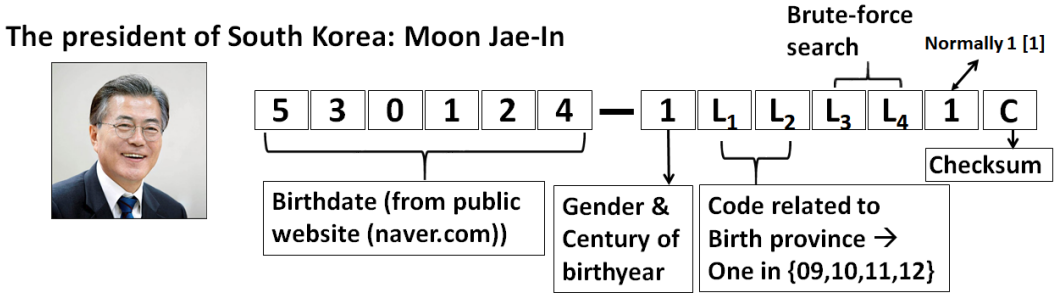

Fig. 5. Strategy to determine order of candidate RRNs to be tested: case of President Moon Jae-in

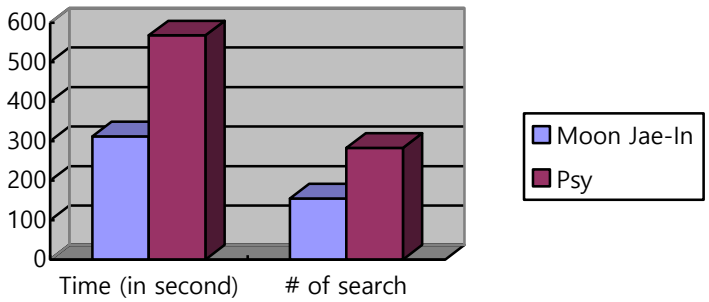

Fig. 6. Performance of our experiment: required time to derive the RRNs of celebrities

Fig. 6 shows the time spent in the experiment for deriving the RRN of each of the target user and the number of times the RRN verification module was executed. In both the cases, we observe that the RRN was determined in less than approximately 10 min. Depending on the

[3] We used □s to describe some of the target users' RRNs' digits in order to provide the privacy of the target users' RRNs.

first two digits of the location-dependent part, the required search time was decided. For example, it was the second candidate value in the case of Moon Jae-In, while it was the 6th in the case of PSY.

5. Conclusion

In this study, we introduced Korea's RRN system and examined the problems of this system in terms of security and the Korean society's attempts to improve the system. Through this study, it was determined that the current RRN system continues to exhibit a problem in online use. Particularly, RRNs are still used for real name authentication; therefore, it can be verified that the RRNs of individuals can be conveniently leaked using the RRN verification module in real name authentication systems.

It is important to prevent the exposure of RRNs to the public in order to ensure the protection of personal information. However, as the RRNs of a substantial number of Koreans are already exposed to the public owing to numerous system security incidents and lack of public awareness, we recommend that the Korean government consider replacing the present RRN system with a new one in which the RRN will not contain personal information of the holder. This will prevent the social and economic cost incurred owing to the undesirable exposure of individuals' RRNs.

References

[1] D. Choi, Y. Lee, Y. Park, S. Kim, "Estimating Korean Residence Registration Numbers from Public Information on SNS," *IEICE Transactions on Communication*, vol. 98, no. 4, pp. 1070-1086, 2015. Article (CrossRefLink)

[2] Partial Amendment of Personal Information Protection Act, No. 12504, 24th Mar., 2014. Available at: Article (CrossRefLink)

[3] Selenium WebDriver. Available at: Article (CrossRefLink)

[4] Tech musings, "The incredible growth of the Internet since 2000," Oct., 2010. Article (CrossRefLink)

[5] Namu wiki, Residence Registration Number. Article (CrossRefLink)

[6] Y. Kim, H. Lee, H. Ko, K. Kim, J. Kim et al., "A Study on Improvement of Individual Identification System: Focusing on Resident Registration Number," *Korea Development Institute Report*, June 2014. (written in Korean)

[7] Korean Personal Information Protection Association, "Resident Registration Collection Acceptance Act," 2014. (written in Korean)

[8] Y. Song, H. Kim, and J. Huh, "On the Guessability of Resident Registration Numbers in South Korea," in *Proc. of Australasian Conference on Information Security and Privacy (ACISP) 2016*, LNCS vol. 9722, pp. 128-138. Article (CrossRefLink)

[9] J. F. Ludvigsson, P. O. Olausson, B. U. Pettersson, and A. Ekbom, "The Swedish personal identity number: possibilities and pitfalls in healthcare and medical research," *European Journal of Epidemiology*, vol. 24, issue 11, pp. 659-667, 2009.Article (CrossRefLink)

[10] Deena L. Millsapp, "Protecting Social Security Numbers from Identity Theft," US Patent Application Publication, NO:US 20070110282 A1, May 17, 2007.

[11] A. Martin and I. Martinovic, "Security and Privacy Impacts of a Unique Personal Identifier," *Cyber Studies Programme, Working Paper Series – No. 4*, University of Oxford, 2016. Article (CrossRefLink))

[12] H. Rengamani, P. Kumaraguru, R. Chakraborty, and H. R. Rao, "The Unique Identification Number Project: Challenges and Recommendations," in *Proc. of ICEB 2010, LNCS vol. 6005*, pp.

146-153, 2010. Article (CrossRefLink)
[13] A. Acquisiti, and R. Gross, "Predicting Social Security numbers from public data," in *Proc. of National Academy of Sciences*, vol. 106, no. 27, pp. 10975-10980, 2009. Article (CrossRefLink)
[14] AllCredit: A credit rating web service managed by Korea Credit Bureau Ltd.
Available at: Article (CrossRefLink)
[15] Unused page in the web site managed by National People's Liberation Committee: the real name check page: available at Article (CrossRefLink)
[16] R. B. Black, "Legislating U. S. Data Privacy in the Context of National Identification Numbers: Models from South Africa and the United Kingdom," *Cornell International Journal*, Vol. 34: Issue. 2, Article 4. Available at: Article (CrossRefLink)

Heeyoul Kim received the B.E. degree in Computer Science from KAIST, Korea, in 2000, the M.S. degree in Computer Science from KAIST in 2002, and the Ph.D. degree in computer science from KAIST in 2007. From 2007 to 2008, with the Samsung Electronics as a senior engineer. Since 2009 he has been a faculty member of Division of Computer Science at Kyonggi University. His main research interests include application security such as secure group communication and digital rights management.

Ki-Woong Park, received the BS degree in computer science from Yonsei University in 2005, and the MS and PhD degrees in electrical engineering from KAIST in 2007 and 2012, respectively. He is an assistant professor in the information security department at Sejong University. He worked as a researcher National Security Reserch Institute in 2012. His research interests include system security issues for a real cloud and mobile computing systems. He is a member of the IEEE and ACM.

Daeseon Choi received the BS in computer engineering from Dongguk University, Rep. of Korea, in 1995, the MS in computer engineering from POSTECH, Rep. of Korea in 1997, and the PhD in computer science from KAIST, Rep. of Korea in 2009. From 1999 to 2014, he was a member of research staff with ETRI, Daejeon, Rep. of Korea. Since 2014, he has been an associate professor in the department of Medical Record & Health Information Management. His main research areas are ID management, mobile security, and Fintech Security.

Younho Lee received the BS, MS, and PhD in computer science from KAIST, Rep. of Korea, in 2000, 2002, and 2006, respectively. He worked as a visiting postdoctoral researcher at the GeorgiaTech Information Security Center from 2007 to 2009. From 2009 to 2013, he was an assistant professor in the Department of Information and Communication Engineering, Yeungnam University, Rep. of Korea. Currently, he is an associate professor in the Information Technology Management Division, Seoul National University of Science and Technology, Korea. His research interests include network security, applied cryptography, and Fintech security.