Implementation of Management System to Ensure Self-imposed Control for the Personally Identifiable Information

Yong-Nyuo Shin

Dept.of Computer Engineering, Hanyang Cyber University

ynshin@hycu.ac.kr

Abstract

Personally Identifiable Information (PII) is any information that identifies or can be used to identify, contact, or locate that person to whom such information pertains or that is or might be linked to a natural person directly or indirectly [1]. In order to recognize data processed within information and communication technologies as PII, it should be determined at which stage the information identifies, or can be associated with, an individual. In the International Standard as privacy framework and privacy architecture framework, several PII was categorized such as biometric identifier, national identifiers, financial profile and customer number [7]. As the Protection of Personal Data Act is in force in Korea, the subject of protection responsibility is increased, and continuous efforts are made to protect privacy in overseas countries, as can be seen by standard drafts related to privacy protection. This paper is designed to show an effective web based PII Management System to ensure self-imposed control for domestic circumstances in Korea.

Keywords: *Privacy, Personally Identifiable Information, Self-imposed Control, Privacy architecture framework*

1. Introduction

As the Act on the Protection of Personal Data is in force in Korea, nearly all businesses and government agencies need to mandate the use of privacy assessments before establishing certain new databases to data breach protection. Guided Security Impact Assessments can assess current level of information security against leading practices in international standards such as privacy framework, privacy architecture framework and more. For this reason, it is time for the governmental/public agency and private company to make thorough preparations. Organizations are given a detailed report with a sample action plan suitable for the IT security staff, and a high-level report suitable for senior management. For doing this, we provide the web based protection mechanism let the employees protect information autonomy because they can access the related web site whenever they want to follow the rule or regulation which is related Personal Information Protection Act System to ensure self-imposed control. Also it is very effective way to find those who violate the privacy law and reduce the hostility toward auditing. Chapter 2 explains a concept of the privacy architecture framework standardization in ISO/IEC JTC1 SC27 Working Group 5. Chapter 3 shows a privacy self-diagnosis tool on the protection of personal data. Chapter 4 shows the function for delivering the specific commands to the individual agents to maintain the consistency of the policy. In the conclusion, we describe the future study tasks are reviewed.

2. Privacy Architecture Framework

Since 2005, ISO/IEC JTC1 SC27 Working Group 5 has been performing standardization to protect privacy, the fundamental right of the individual, and concentrating on the standardization of a privacy architecture framework to implement the privacy framework. As many privacy violation cases have been reported at home and abroad, such as the collection of user location information via mobile device and Google's street view, the privacy reference architecture has been drawing attention, in order to create a privacy framework, which is the international standard to protect privacy, and implement the framework. The privacy framework [2] is intended to help an organization to define its privacy control requirements related to personally identifiable information within its information and communication technology environment by: relating all described information privacy aspects to existing security guidelines. The privacy reference architecture [3] provides guidelines on how to develop, implement and operate information and communication technology systems with built-in privacy safeguarding controls; is a resource containing a consistent set of architectural best practices for managing PII in information and communication technology systems. Guided Security Impact Assessments can assess current level of information security against privacy architecture framework provides follows in three perspective. First, it provides a consistent, high-level approach to the implementation of privacy safeguarding controls for the processing of PII in ICT systems. Secondly, it provides guidance for planning, designing and building ICT system architectures that more effectively facilitate the privacy of individuals by helping to prevent inappropriate processing of an individual's PII. Finally, it shows how privacy enhancing technologies (PETs) can be used to enhance the implementation of privacy controls.

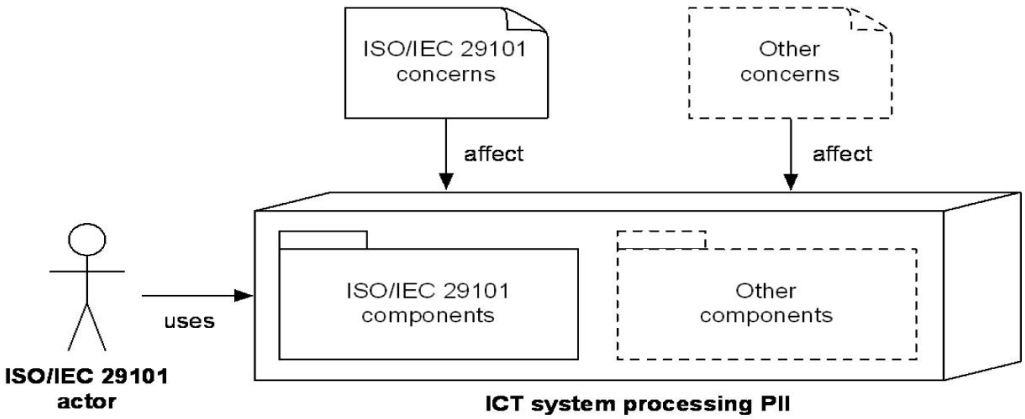

Figure 1. Elements of the Privacy Architecture Framework

3. Privacy Self-Diagnosis Tool for Supporting Rules and Policy

To run the program, the user should access to the web service using internet explorer as shown in Figure 1. Also, the user of privacy finder has to login first using id and password. After login, the user can check the history of running. The privacy protection software applies the rule to apply the privacy control to the system, in order to satisfy the requirement proposed by the privacy framework and reference architecture. The rule must always be included in the policy. If the rule is not included in the policy, it cannot be transferred to the agent. Applying the rule means including the rule in the particular policy. A regular

expression changes the particular set of characters or the string into symbols, and is used to define the expression rule used to describe a set of strings accurately, or to define the grammar of the language, or to designate the string to search. Rules are managed, such as addition, modification, deletion, change, and application to the policy. The content of the rule is a regular expression or keyword, which is included in the policy and sent to the PC, and is used by the PC to detect a regular expression and keyword designated by the file in the PC based on the regular expression and keyboard in question [4].

3.1. Relation between Privacy Rules and Policies

The privacy protection software applies the rule to apply the privacy control to the system, in order to satisfy the requirement proposed by the privacy framework and reference architecture. The rule must always be included in the policy. If the rule is not included in the policy, it cannot be transferred to the agent. Applying the rule means including the rule in the particular policy. A regular expression changes the particular set of characters or the string into symbols, and is used to define the expression rule used to describe a set of strings accurately, or to define the grammar of the language, or to designate the string to search. Rules are managed, such as addition, modification, deletion, change, and application to the policy. The content of the rule is a regular expression or keyword, which is included in the policy and sent to the agent, and is used by the agent to detect a regular expression and keyword designated by the file in the agent PC, based on the regular expression and keyboard in question. When entering a regular expression, the expression that fits into the standard regular expression should be entered. The agent will not execute the expression automatically, if it is not suitable for the regular expression such as * and ?. Furthermore, the personal information will not be detected properly if the expression is incorrect. If the rule has been transferred to the agent already, because the rule in question is included in the policy when modifying, deleting, or applying the rule, the changed rule will be sent to the agent and applied, if the agent in question is online. If the agent is offline, the changed rule is sent to the agent when the agent connects. Regular expressions are the text patterns which are composed of special characters which are alternatively known as general characters (Example: a-z characters) and Meta characters. The pattern explains multiple numbers of character strings which are sought while searching text in the Table 1.

Table 1. Regular Expressions

Expressions	Matches
/^₩s*$/	Find a blank line.
/₩d{2}-₩d{5}/	Execute the validity test about the ID number that is consisting of 2 digit number, hyphen and extra 5 digit number (example: XX-XXXXX).
/<₩s*(₩S+)(₩s[^>]*)?>[₩s₩S]*<₩s*₩/₩1₩s*>/	Find the HTML tag.

When detection occurs: it will be recorded immediately in the database and sent to the administrator email. PII processing flow models should be developed as an integral component of a privacy risk assessment. The PII processing flow diagram may not only show the areas where PII is collected, transferred, used, stored or disposed of but can also show areas where the PII has a higher level of sensitivity or importance and, as a consequence, requires the implementation of stronger safeguarding measures. Categorizing data into PII and non-PII is the minimum requirement at this stage but various industries may also require the classification of PII into subsets of categories that need special protection schemes (*e.g.*, certain health data of an individual that requires specific protection). Classification and control concerns within an ICT system should include: we identify and categorizing PII among the data and quantify the number of PII principals and the amount and sensitivity of the PII stored. Also we provide the control transfers and internal copies of PII. Logging actions performed on the PII enables the PII controller to audit that the PII has been processed according to the applicable policies. Additionally, a detailed history of access requests to PII can help check for leaks or unauthorized behavior.

3.2. Security policy Settings

It can be set to respond the USB security when the USB is connected, disconnected and using files from the USB. It is possible to send information about connection, disconnection and file usage to the administrator through mails as detection occurs.

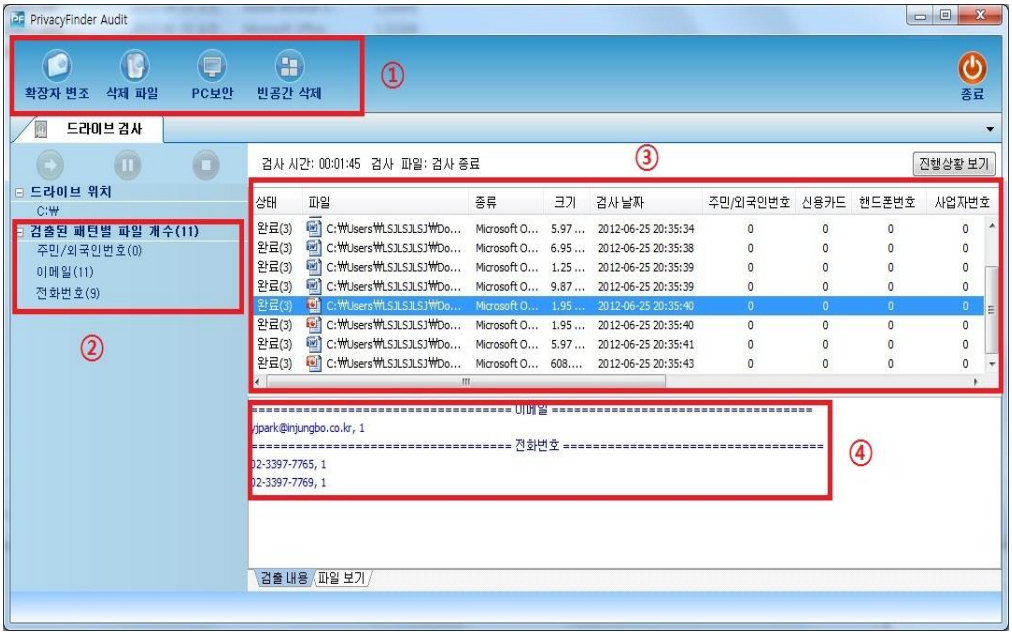

Figure 2. Screen Shot of the Searching Result for PII

In addition, various policies can be set, and statistics can be checked by date and user through the web page, as shown in Figure 3.

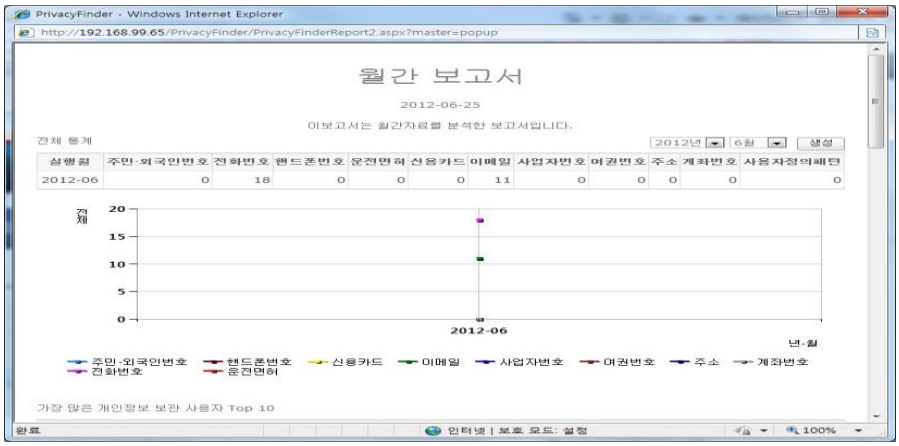

Figure 3. Screen Shot of the Monthly Report for the Web Based PII Management

For the USB connection, when the USB media is connected to a computer, the information is sent to the server, and is recorded in the database. For the USB disconnection, when the USB media is disconnected from a computer, the information is sent to the server, and is recorded in the database. Also for the use files from USB, when the files in the USB are created, deleted and modified, the information is sent to the server, and is recorded in the database. After running privacy finder as user's choice using ActiveX format, the policies are acting as the administrator's setting. The policy can be included such as target of searching, lists of searching, searching method. All installed driver will progress the search automatically. If the personal information is found, the search details will be sent to the process server and saved in the MS SQL server. Table 2 shows the result of searched personal information.

Table 2. The Result of Searched PII

Security attributes	Description
Search time	Time at which the personal information is searched
Policy	Identifier of the personal information search policy
Rule	Regular expression identifier used to search the personal information
Search file information	Other information such as the position, size, and format of the file containing the personal information
Search times	Number of times that the personal information is searched
Search content	Paragraph in the file containing the searched personal information
Search result	Successful/Failed research
Response result	Successful/Failed deletion of the searched target file

An efficient policy will prevent the exposure of the personal and confidential information of the enterprise, encrypt the personal information file or delete it permanently, and manage the status of the personal information and confidential information. Through self-diagnosis of the user, the user's awareness about protecting

the important information saved in the business PC can be enhanced, and the privacy protection obligation can be carried out.

4. Remote Command Execution

In this paper, we provide the function for delivering the specific commands to the individual agents and the majority of agents to use the pop-up menu by right-clicking from the agent tree. Frequently used digital data, timeline analysis, and agent information are same as clicking buttons on toolbar of selected agents. If the commands are delivered to the checked agent, commands will be delivered to the server and the server will send the commands to each agent. The completion about the commands will appear at the bottom of the manager log window if the execution of the commands is complete.

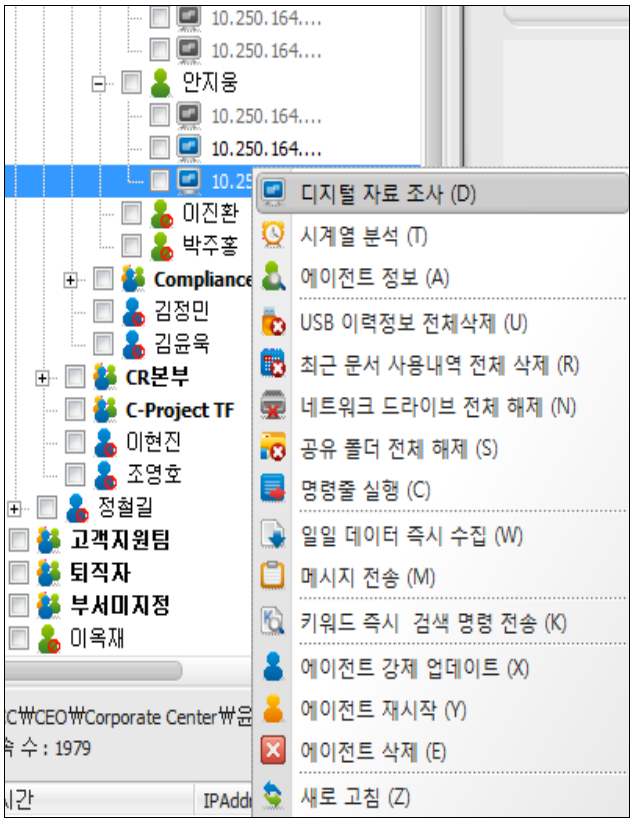

Figure 4. Screenshot of the Pop-up of Right-clicking the Agent Tree

Investigation of the digital data provides real-time screen of the selected agents, the details and the imaging of the hard disk, remote file download, file search, file preview (check the contents of the file documents, the contents of the compressed file), and reports as shown Figure 5. Investigation of the digital data can be executed immediately if it is connected to the agents. The connected agents can execute through real-time communication with the managers' executed PC without the server. It is possible to investigate all disk drives remotely; you can check the investigated explorer in the form of appearance in the local disk. It is possible to check the details of the individual files as a summary of the contents of the document preview function, text and hex view. In

addition, the timeline for the selected folder can be created and a graph can be represented depending on the date and time created.

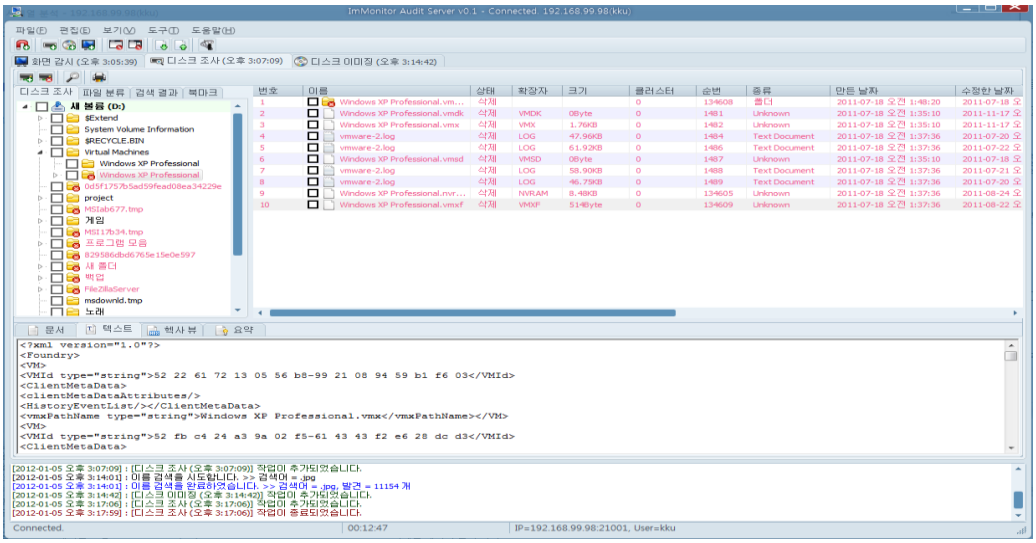

Figure 5. Disk Investigation- Screenshot of the Completion of the Investigation

Also we provide the report including daily status, weekly status, monthly status and log occurrence rate of each agent that it can be printed the log occurrence rates of all agents within the inquiry period as shown Figure 6. The longer the report creating time, the longer the inquiry period. The contents of the report become lengthened so it is necessary to have a sufficient inquiry period. If there is over 1000 data of rates, numbers and details, it will show top 1000. Administrator can receive the daily reports through the administrator mail about the used file contents from the daily occurred print contents, keyword detection contents, USB connection/disconnection contents and the USB. Incoming emails will be sent to the address that you enter in the Email Manager Administration window of the SuperAdmin.

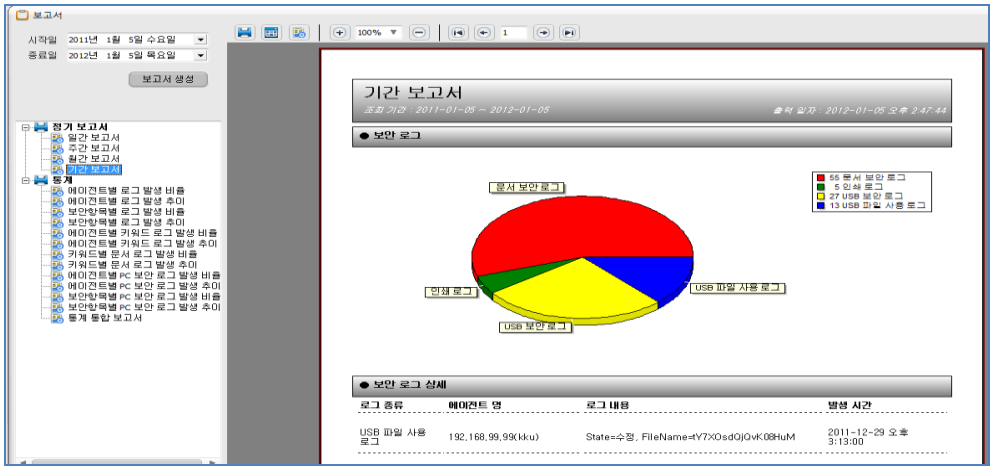

Figure 6. Screenshot of Daily to Period Reports

5. Conclusion

ISO/IEC JTC1 SC27 Working Group 5 has been performing standardization to protect privacy and concentrating on the standardization of a privacy architecture framework to implement the privacy framework. The privacy architecture framework provides guidelines on how to develop, implement and operate information and communication technology systems with built-in privacy safeguarding controls; is a resource containing a consistent set of architectural best practices for managing PII in information and communication technology systems [3]. In order to implement and test the ISO 29101[4], the system was implemented that performs various functions as described in this paper. Also we show the web based protection mechanism to protect PII. Compared with client-server model, web based implementation can help not to infringe the right of self-determination. Protecting personally identifiable information is protecting the basic rights of the public, and is closely related to the concept of protecting personal assets in the knowledge society. As many privacy violation cases have been reported at home and abroad, such as the collection of user location information via smartphones and Google's street view, the privacy architecture framework has been drawing attention, in order to create a privacy framework, which is the international standard to protect privacy, and implement the framework. In this paper, we proposed a policy-based operating tool and apply it to the actual operating environment, which satisfies the safeguard control proposed by the privacy framework and privacy reference architecture. Also we proposed an investigation of the digital data providing real-time screen of the selected agents, the details and the imaging of the hard disk, remote file download, file search, file preview and reports.

References

[1] ISO/IEC JTC1 SC27 WG5 "Study Period Vocabulary", SC27 N9401, **(2011)**.
[2] ISO/IEC JTC1 SC27 International Standard, "Privacy Framework", SC27, **(2012)**.
[3] ISO/IEC JTC1 SC27 "Privacy Reference Architecture", SC27 N9228, **(2011)**.
[4] Y.-N. Shin and W. Chang Shin, "A Security Reference Model for the Construction of Mobile Banking Services based on the SmartPhone", International Journal of Fuzzy Logic and Intelligent Systems, vol. 11, no. 4, **(2011)**, pp. 229-237.
[5] Y. -N. Shin, "Standard Implementation for Privacy Framework and Privacy Reference Architecture for Protecting Personally Identifiable Information", International Journal of Fuzzy Logic and Intelligent Systems , vol. 11, no. 3, **(2011)**, pp. 197-203.
[6] S. A. El-said, K. F. A. Hussein and M. M. Fouad, "Confidentiality and Privacy for Videos Storage and Transmission", IJAST, vol. 28, **(2011)**, pp. 67-88.
[7] Y. -N. Shin, D. -K. Lim and S. -J. Shin, "A study on biometric standards for adaptation of the national infrastrucuture", International Journal of security and its applications, vol. 6, no. 2, **(2012)**, pp. 155-160.

Authors

Yong-Nyuo Shin received her PhD degree in computer science from Korea University in 2008, Republic of Korea. Currently, she is a professor at Department of Computer Science, Hangyang Cyber University. Also, she is an editor for efforts and continued support in the progressing for much standardization, such as ITU-T SG17, ISO/IEC JTC1 SC27 and SC37. Her current research interests are telebiometrics, authentication technologies and privacy.