A Classification of Secure and Anonymous Communication

Takuya Kawase (0810016)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 6, 2012

Keywords: Secured Communication, Anonymous Communication, Classification, Proxy, Onion-routing.

There are some secure and anonymous communication technologies that are used to keep source users and communication messages on the Internet. These technologies can perform safe communication, however, may be abused copyright infringement by file sharing software, and slander message are some examples. Therefore, it is necessaly to study the technology for controlling and monitoring. Both technologies must be in equal relation. In consequence, it is essential to clarify the relation of both technologies. In this paper, we propose a technique to compare secure and anonymous communication technologies. Thereby, the technology which poses a problem is clarified.

We defined "Secure and Anonymous Communication" as "communication which conceals some information". In addition, we call the technology of realizing this communication "Secure and Anonymous Technology". "The communication contents and types", "Communication pathway", and "Communication fact" are the information which secure and anonymous technology should take into account. Generally, secure communication corresponds to "Communication which conceals the communication contents and types" and anonymous communication corresponds to "Communication which conceals communication pathway". Advanced Encryption Standard(AES) of common-key and RSA of public-key are the typical technolo-

gies of secure communication. While, Proxy, Tor, I2P, and Freenet are the typical technologies of anonymous communication. There are techniques of hiding the target communication by random communication, and techniques of making it look like other communication using steganography. Many secure and anonymous technologies cannot be exclusively classified into these three types. Because, for example, anonymous communication may also carry out concealment of the communicative contents and kind using encryption. Additionally, this feature cannot be used for comparison, because it does not have the same function, corresponding to the same technology.

In this paper, concealing information means being able to express "A certain information is concealed to a person". Thereby, "Concealment information" and "Concealment person" were examined. It is decided to divide into the three layers(Network, Transport, Application) of TCP/IP protocol stack. As a consequence, the table has been created with 2 axis of concealment information and concealment person. We propose the method of comparing secure and anonymous technologies using this table. The table with applied secure and anonymous technologies expresses the information and a person that can be concealed. When tables with secure and anonymous technology are compared, the difference in each technology are revealed.

HyperText Transport Protocol(HTTP), HyperText Transport Protocol over Secure Socket Layer(HTTPS), Proxy, and Onion-routing of secure and anonymous technologies are applied to the table, therefore, the differences between concealment information and concealment person who of each secure and anonymous technology is able to exposed. Additionally, the information and person that are concealed is attained with a technology combination is able to expressed. However, there is a case where combination was impossible. Hence, it is necessary to propose a method to distinct where combination is applied. In addition, we have to examine the element of concealment information and concealment person. We think that it will be improved this problem, if the technologies appllied is increased. The secure and anonymous technology which threat is found by the proposed technique. Consequently, it can lead to new secure and anonymous technology which is effective and take equal relation between "secure and

anonymous technology" and "control and monitoring technology".