Enhanced Authentication Scheme based on Network Location for a DRM System

Arjulie John P. Berena, Graduate School of Electronics Engineering, Nihon University
Takahito Murofushi, Graduate School of Electronics Engineering, Nihon University
Kanami Kaiho, Graduate School of Electronics Engineering, Nihon University
Masami Kihara, Faculty of the Graduate School of Electronics Engineering, Nihon University

ABSTRACT

Digital Rights Management (DRM) provides protection for copyrighted content distributed through the Internet. Copyrighted content may range from a variety of valuable digital media, such as music audio, video or digital cinema, high-resolution image, eBooks, application and game software, or a piece of valuable document. As the content is in digital format, reproduction is made easier without apparent degradation of the content quality. The primary goal of DRM then is to protect the rights of the content creators against piracy. These rights may come in wider scope and implementations that is in agreement with the content provider and the user. Such rights involve restriction on copying, modifying, distributing and other usage of the content.

In the Internet, the conventional method of authenticating a registered user or a prospective content purchaser is by means of username and password combination. However, this method poses a great deal of vulnerabilities especially now that password attacks are rampant. Moreover, phishing technique have become popular that caused substantial financial loss in recent years. Phishing is an act that fraudulently acquires sensitive information from the user by masquerading as a trustworthy entity. Fraudulently acquired information could then be used to spoof another user. With this vulnerability in the Internet, content providers face a serious problem whether the purchaser is a legitimate one or not. Enhancement of user authentication scheme is then being sought for to ensure that the content is delivered to the legitimate purchaser, and to combat illegal activities in the Internet in general.

In this paper, we describe our DRM system that consists of three entities, such as the user or the client, the Download Mediator (DMS) and the content copyright owner. Conventional online shopping involves the purchaser accessing the service provider’s web pages to browse the products available and to place an order. In our system, we introduce the use of the mobile device in accessing the contents servers, where at the same time it could provide additional user identification. Moreover, we propose the user authentication that is based on location information of the user mobile device. Aside from the information that can be derived from the subscription of the user from the mobile service provider, its current location will be used to probe its authenticity when purchasing the content. The purchaser’s location must be pre-registered as a location-enforcement policy of the system. This ensures that access outside the permitted area is prohibited, thus spoofing could also be prevented.

With the introduction of third-generation (3G) mobile phones in the past few years and soon the 4G mobile phones, mobile users have a ready access to the Internet where online shopping thus became possible. Additionally, modern mobile phones have built-in Global Positioning System (GPS) receiver that could provide location information, however, GPS signal may not be available if the user is inside the building, subway or when the signal is obstructed. With these limitations, we propose a location discrimination mechanism where a DRM server will be able to probe the location of the user mobile device. The allowable location area coverage depends on the system implementation. In this mechanism, probe packets are sent from the content server to the mobile device and sent back to the server to measure the round-trip time (RTT). Accuracy and stability of RTT measurement are the defining factors in this scheme.