ABSTRACT

Today, the use of wearable devices is becoming a thing inherent in the daily activities of urban communities. In practice, wearable communications may contain sensitive information regarding a user's health record, so authentication and confidentiality of data exchanged must be guaranteed. In addition, the success of authentication between users, wearable devices and smartphones is very important because there are various threats of attack on the authentication process. Based on previous studies, it was found that the security functionality of user impersonation attack is not owned by lightweight authentication protocols in the current wearable communication environment. So this research undertakes the design of a lightweight authentication protocol to be immune to user impersonation attacks to supplement the lack of security functionality in previous protocols with the support of performing a formal analysis using the Scyther Tool. The research method used is a Research Library supported by conducting protocol security test experiment. The developed protocol utilizes a modified and customized S-NCI key establishment protocol scheme to meet all targeted security functionality. The research resulted that the lightweight authentication protocol generated was immune to the impersonation attacks of users, then was able to add two new functionalities that added wearable devices and added smartphones.

Keywords: *wearable device, lightweight authentication protocol, user impersonation attack, scyther tool, key establishment.*