ABSTRACT

The best-known and most widely deployed AAA protocol is RADIUS--an acronym for Remote Access Dial-In User Service. It was developed in the mid-1990s by Livingston Enterprises to provide authentication and accounting services to their NAS devices. Its functional attributes consist of Client-server-based operations. In the network security, All communications are authenticated by virtue of a shared secret key. In addition, user passwords contained in RADIUS messages are encrypted to prevent hackers from reading them by snooping the network. RADIUS can support multiple authentication mechanisms, including PAP and CHAP. RADIUS messages carry AAA information encoded in type-length-value fields, called attributes (or attribute/value pairs).

It functional attribute consist of some weaknesses that we will analize on this final project, those weaknesses may cause performance's degradation based on the authentication process of the access network,in these case the network that we examine are OWLAN. These final project will analize the security level of the data communication in the authentication process that given by RADIUS protocol in an access network.

From the result of the analysis,obtained that protection technic for the user-password atibute is very weak in every condition. It must not use the stream chipper, and also must not used MD5 as a chipper primitive. Response authenticator is a very goo thing but its very rarely implemented. Access-request packet are not authenticated at all. There are a lot of client implementation that not create sufficient randomness request authenticator. Administrator used to choose shared secret RADIUS with sufficient randomness entropy information. In many client-host implementastion artificially limit the used of keyspace of a shared secret.