ABSTRAKSI

Protocol AAA yang paling dikenal dan banyak digunakan adalah RADIUS (Remote Authentication Dial-in User Service). Protocol ini dikembangkan pada pertengahan 1990-an oleh Livingston enterprise untuk menyediakan layanan authentikasi dan akunting bagi perangkat NAS. Attribute fungsionalnya diantaranya Operasi yang berdasarkan client-server, dalam hal kemanan jaringan RADIUS menggunakan shared secret key dan adanya enkripsi message untuk mencegah para hacker membaca paket data, authentikasi yang fleksibel dimana RADIUS ini mendukung berbagai mekanisme authentikasi termasuk PAP dan CHAP. Adanya pasangan attribute/value, pesan RADIUS membawa informasi AAA dikodekan dalam field type-length-value yang disebut dengan attribute.

Attribute fungsional diatas mengandung beberapa kelemahan yang akan kita analisa nanti, yang berakibat menurunnya performansi suatu jaringan akses dalam hal ini jaringan OWLAN dikarenakan proses authentikasinya. Tugas akhir ini akan membahas dan menganalisa tingkat keamanan komunikasi data yang dapat diberikan oleh protocol RADIUS dalam membawa authentikasi di suatu jaringan akses.

Dari hasil analisa diperoleh bahwa teknik perlindungan terhadap user-password sangat lemah dalam segala hal. Harusnya tidak digunakan stream chipper, dan harusnya juga tidak digunakan MD5 sebagai suatu chipper primitive. Response authenticator adalah hal yang sangat bagus, tetapi sayangnya sangat jarang diiplementasikan Paket access-request tidak diauthentikasi sama sekali. Banyak implementasi client yang tidak menciptakan request authenticator yang cukup acak. Banyak administrator memilih shared secret RADIUS dengan entropy informasi yang tidak mencukupi. Banyak implementasi client dan host secara artificial membatasi penggunaan keyspace dari shared secret.