PENGGUNAAN ALGORITMA CHALLENGE RESPONSE IDENTIFICATION UNTUK AUTENTIKASI ENTITAS PADA INTRANET MESSAGES

Wikaria Gazali, Djunaidy Santoso, Randy Tjandra

ABSTRAK

Password diasosiasikan dengan sebuah entitas, adapun pengertiannya adalah sebuah string yang biasanya terdiri dari 6-10 karakter yang mudah diingat oleh pemiliknya dan rahasia bersama dengan sistem, sebagai bukti keabsahan dari identitas seseorang. Tetapi orang kurang menyadari akan pentingnya suatu password yang aman agar password yang dimiliki tidak mudah diketahui. Oleh karena itu, dibutuhkan suatu mekanisme skema autentikasi yang kuat untuk melindungi password yang dimiliki pengguna.

Mekanisme Challenge Response dapat digunakan untuk menjaga kemananan password. Ide dari algoritma challenge response identification adalah pemilik pesan (claimant) dan penerima pesan (verifier) membuktikan keabsahan identitasnya masing-masing. Langkah ini dilakukan dengan mengadakan respon bagi suatu challenge tertentu. Challenge umumnya suatu karakter yang dipilih secara random dan rahasia. Karakter random yang digunakan berfungsi untuk menyediakan suatu keunikan dan jaminan untuk menghindari adanya serangan attacker.

Sistem yang dirancang adalah sejenis intranet messages yang berbasis client-server Sistem diimplementasikan dengan menggunakan bahasa pemprograman VB 6.0 dan microsoft acces xp sebagai basis data. Server berfungsi sebagai penyimpan basis data yang berisi data mengenai identitas pengguna dan pesan yang dipertukarkan d iantara pengguna. Client adalah tempat pengguna meminta layanan fasilitas sistem. Fasilitas yang disediakan adalah fasilitas pengiriman pesan dan pengecekan pesan yang masuk untuk pengguna tersebut. Dalam sistem algoritma challenge response digunakan adalah algoritma challenge response dengan menggunakan kunci simetrik dan fungsi MAC sebagi autentikator. Tujuan yang ingin dicapai adalah entitas yang melakukan login ke sistem dijamin keabsahannya.