ABSTRACT

The use of passwords in order to identify someone to make a connection or login is the most popular schemes today. But when we send the password on an unsecure line will invite trouble. A problem that may arise is stolen passwords by other parties. When the parties get their password is unauthorized and get into the system by illegitimate and transact such other person then it will be fatal.

With technology based on the hash and HMAC then we do research for the encoding of the password can be sent via an insecure path. Some attacks are considered in this study was wiretapping and replay attacks. With this scheme we are expected to perform authentication on an insecure path.

Kata kunci: otentikasi, *password*, challenge-response, fungsi hash

xii+72 pages; 32 figures; 7 tables; 1 attachments;
Bibliography: 18 (1996-2010)

ABSTRAKSI

Penggunaan password dalam rangka untuk mengidentifikasi seseorang untuk melakukan koneksi atau login adalah skema yang paling popular saat ini. Tapi bila kita mengirimkan password pada jalur yang tidak aman maka akan mengundang masalah. Masalah yang kemungkinan timbul adalah tercurinya password oleh pihak lain. Bila pihak yang mendapatkan password tersebut adalah pihak yang tidak berwenang dan masuk ke dalam system dengan cara tidak sah dan melakukan transaksi seperti orang lain maka akan berakibat fatal.

Dengan berdasarkan teknologi hash dan HMAC maka kita melakukan penelitian agar dapat pengkodean terhadap password yang dikirm melalui jalur yang tidak aman. Beberapa serangan yang dipertimbankan dalam penelitian ini adalah penyadapan dan *replay attack.* Dengan skema ini diharapkan kita dapat melakukan otentikasi pada jalur yang tidak aman.

Kata kunci: otentikasi, *password*, challenge-response, fungsi hash

xii+72 halaman; 32 gambar; 7 tabel; 1 lampiran;
Daftar acuan: 18 (1996-2010)