Universitas Indonesia Library >> UI - Skripsi Open

Analisa dan perbandingan hasil implementasi algoritma MD5 dan SHA-1 pada sistem keamanan autentikasi simple-O = Analysis and comparison the result of the MD5 and SHA-1 algorithm implementation in simple-O authentication system security

Ahmad Shaugi, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20309779&lokasi=lokal

---

Abstrak

Simple-O, suatu aplikasi essay grading yang dikembangkan di Departemen Teknik Elektro Universitas Indonesia, menggunakan algoritma MD5+salt untuk melakukan proteksi terhadap data password user yang tersimpan pada databasenya. Namun dengan banyaknya kelemahan yang terdapat pada algoritma MD5, maka diterapkan algoritma SHA-1+salt pada aplikasi ini, yang kemudian dibandingkan dengan algoritma sebelumnya yaitu MD5+salt. Pengujian meliputi pengukuran waktu dan estimasi waktu brute force untuk masing-masing algoritma, serta mengukur processing time dan CPU usage saat melakukan login ke dalam system.

Hasil pengujian brute force menunjukkan bahwa penerapan algoritma SHA-1 lebih kuat terhadap serangan brute force dibandingkan dengan MD5. Selisih processing time SHA-1+salt dengan MD5+salt berkisar antara 0.001 detik hingga 0.002 detik untuk tiap variasi panjang password. Sedangkan selisih CPU usage SHA-1+salt dengan MD5+salt sebesar 0.545%, 0.985%, dan 1.69% masing-masing untuk password sepanjang 8, 9, dan 10 karakter. Hasil ini menunjukkan bahwa penerapan algoritma SHA-1+salt tidak akan membebani kinerja aplikasi Simple-O.

.....Simple-O, an essay grading application that was developed at the Department of Electrical Engineering University of Indonesia, using MD5+salt algorithm to perform protection for password of user's which stored on its database. But with so many flaws contained in the MD5 algorithm, then SHA-1+salt algorithm was implemented in this application, which is then compared with the previous algorithm MD5+salt. The tests include measurements of time and estimated time of brute force for each algorithm, and measure the processing time and CPU usage when logging into the system.

The test results show that the application of brute force algorithm SHA-1 is more robust against brute force attacks than MD5. Difference in processing time SHA-1+salt with MD5+salt was ranged from 0.001 seconds to 0.002 seconds for each length variation of the password. While the difference in CPU usage of SHA-1+salt with MD5+salt is 0.545%, 0.985%, and 1.69% respectively for the password with 8, 9, and 10 characters length. These results indicate that the implementation of the algorithm SHA-1+salt does not impose on the performance of Simple-O application.