Implementasi dan analisis perbandingan operasi protokol pinkas-sander (PS), van oorschot-stubblebine (VS) dan password guessing resistant protocol (PGRP) pada layanan single sign on (SSO) untuk menyediakan skema otentikasi password yang aman bagi privasi pengguna = Implementation and comparative analysis of pinkas-sander (PS) protocol, van oorschot-stubblebine (VS) and password guessing resistant protocol (PGRP) on single sign on (SSO) service operation for providing secured password based authentication scheme towa

Arie Valdano T., author

Abstrak

Dewasa ini, otentikasi berbasis password telah digunakan berbagai situs penyedia layanan berbasis web. Hal ini disebabkan kemudahan yang diberikan layanan Single Sign On (SSO) untuk memberikan akses ke berbagai aplikasi web melalui satu kali otentikasi password. Namun, layanan SSO memiliki kerentanan terhadap serangan password guessing, terutama serangan brute force dan dictionary attack. Penerapan protokol login berupa protokol Pinkas-Sander (PS), protokol van Oorchot-Stubblebine (VS) dan Password Guessing Resistant Protocol (PGRP) pada layanan SSO bertujuan untuk menyediakan layanan otentikasi berbasis password yang aman dan terpercaya bagi pengguna. Hal ini dipertimbangkan berdasarkan beberapa aspek, seperti keamanan (security), keberdayagunaan (usability) dan konsumsi sumber daya komputasi. Hasil pengujian menunjukkan bahwa protokol PGRP mendukung tiga aspek tersebut dengan baik. Protokol PGRP hanya memunculkan tiga kali CAPTCHA saat pengguna melakukan login secara benar menggunakan tiga akun berbeda, sedangkan protokol PS dan protokol VS memunculkan CAPTCHA sebanyak 30 kali. Selain itu, protokol PGRP menghasilkan utilisasi memory server otentikasi lebih kecil dibandingkan protokol PS dan protokol VS. Hal ini ditunjukkan oleh nilai rata-rata dari protokol PS memiliki selisih nilai utilisasi memory sebesar 226,1 kB ? 706,35 kB lebih kecil dibandingkan protokol PS dan protokol VS. Dengan demikian, protokol PGRP direkomendasikan untuk diterapkan pada layanan SSO.
<hr>Nowadays, password based authentication have been used by various web service provider. It is due to the convenience of Single Sign On (SSO) service to permit a user to access into multiple web applications through password authentication at once. However, password based authentication prone to password guessing attacks, especially brute force and dictionary attack. The implementation of login protocol as PS protocol, VS protocol and Password Guessing Resistant Protocol (PGRP) in SSO service aim to provide a secured and trustworthy password based authentication service for legitimated users. It will be considered based on several aspect including security, usability and computation resource consumption.
The experiment's result show that PGRP is able to support the three aspect of SSO service. PGRP protocol only challenged CAPTCHA three times when user use three different account, whereas PS protocol and VS protocol challenged CAPTCHA 30 times. In addition, PGRP protocol result memory utilization of authentication server less than protocol PS and protocol VS. It was showed by average value of memory utilization about 226.1 kB to 706.35 kB less than PS protocol and VS protocol. Thus, PGRP protocol is recommended to be implemented on SSO service.