Implementasi autentikasi aplikasi web menggunakan on-time password

Yoppie Agitya Krisnanto, author

Abstrak

Saat ini penggunaan situs web semakin meluas. mulai dari kalangan pribadi, organisasi, perusahaan,. lembaga pemerintahan. sampai negara. Ada kalanya pemilik situs web ingin menjaga halaman web-nya agar hanya bisa dimasuki oleh pengguna tertentu saja. Hal ini dapat diwujudkan dengan menggunakan proses autentikasi. Proses autentikasi umumnya menggunakan user nama dan password Proses ini menggunakan password yang tidak dienkripsi, sehingga dengan mudah mendapat ancaman nerwork sniffing (penyadapan), replay attack (pengulangan) dan masquerade (penyamaran) oleh para penyusup. Hal tersebut menjadi kendala bagi pengguna situs web yang memerlukan tingkat keamanan tinggi seperti on-line banking, karena menggunakan jaringan komputer yang sifatnya publik dan global. Untuk mengatasi kelemahan tersebut digunakan proses autentikasi dengan 0ne-Time Password (OTP), yang mana digunakan password yang selalu berubah pada setiap pmses autentikasi. Autentikasi dengan OTP memerlukan kalkulator yang digunakan untuk menghitung password sebagai output dari perhitungan jumlah literasi, challenge, dan passphrase yang dimiliki pengguna. Sistem OTP memanfaatkan sifat tidak dapat dibalik (non-invertability dari fungsi secure hash. Pada skripsi ini algoritma secure hash yang digunakan adalah Message Digest-5 yang telah digunakan oleh Bell Communications Research Centre. Pad a skripsi ini dilakukan penerapan proses autentikasi aplikas1 web dengan OTP menggunakan bahasa pemrograman Visual Basic dan ASP (Active Server Pages). Dari program yang dihasilkan akan di1akukan uji coba dan analisa terhadap one-time password yang dihasilkan dari masukan berupa jumlah iterasi, passphrase, dan challange yang berbeda, serta analisa faktor keamanan. Autentikasi aplikasi web dengan OTP ini dapat mengatasi ancaman network sniffing, replay attack dan masquerade, tetapi masih memiliki ke1emahan terhadap ancaman identity interception (penangkapan identitas), dan repudiation (penolakan). Selain itu pengguna yang tidak berhak yang berusaha melakukan proses autentikasi dengan jalan mencoba-coba password memiliki peluang yang sangat kecil untuk berhasil.