Aplikasi one-time password menggunakan algoritma sha-i pada telnet

Andy Stiawan, author

Abstrak

Telnet adalah aplikasi remote login Internet, Telnet digunakan untuk login ke komputer lain di Internet dan mengakses berbagai macam pelayanan umum, termasuk katalog perpustakaan dan berbagai macam database, Telnet memungkinkan pengguna untuk duduk didepan komputer yang terkoneksi ke internet dan mengakses komputer lain yang juga terkoneksi ke internet. Yang menjadi masalah adalah telnet beroperasi pada lapisan jalur internet yang sangat rawan. Proses autentikasi menjadi syarat mutlak bagi penyedia layanan ini, sehingga apabila client ingin menggunakan layanan ini haruslah memasukkan Username dan password -yang selanjutnya akan dikirimkan kepada server. Layanan telnet adalah layanan yang tidak menggunakan enkripsi, sehingga password mudah untuk disadap oleh pihak yang tidak bertanggungjawab. Untuk itu salah satu cara mengatasi masalah ini adalah dengan menggunakan konsep One Time Password (OTP) dimana penggunaan password terbatas hanya untuk satu kali login,sehingga passwordnya berubah tiap kali akan login. Untuk aplikasi OTP ini digunakan algoritma hash function SHA-1 yang memiliki hasil keluaran sebesar 160 bit. Algoritma SHA-1 adalah salah saru algoritma yang digunakan pada aplikasi 01P. Algoritma ini memiliki beberapa keunggulan dibandingkan dengan algoritma untuk aplikasi OTP lainnya, diantaranya adalah algoritma ini memiliki buffer yang lebih besar, kemudian algoritma ini lebih secure walaupun prosesnya lebih lambat. Pada percobaan dilakukan pengujian dan analisa terhadap masukan berupa variasi passphrase dan challenge pada setiap keluaran password yang dihasilkan. Autentikasi OTP dengan menggunakan algoritma SHA-1 secara umum dapat mengatasi permasalahan security atau keamanan pada telnet. Hasil dari percobaan yang dilakukan yaitu dengan cara memvariasikan passphrase dan challenge untuk kemudian dianalisa hasil password OTP keluarannya ternyata menghasilkan password yang selalu berubah pada setiap kali login.