IMPLEMENTASI ALGORITMA RC4 DALAM PROTOKOL SAML (*SECURITY ASSERTION MARKUP LANGUAGE*) PADA LAYANAN SSO (*SINGLE SIGN ON*)

Oleh

Bagus Enggar Tiasto

1157050027

ABSTRAK

SSO (Sistem otentikasi terpusat) merupakan sebuah layanan otentikasi yang memungkinkan pengguna untuk menggunakan satu set data kredensial dalam mengakses beberapa aplikasi. SSO dapat diterapkan degan menggunakan banyak protokol salah satunya, yaitu SAML (*Security Assertion Markup Language*). SAML adalah sebuah kerangka kerja atau standar pengiriman pesan terbuka yang memungkinkan informasi identitas dan keamanan untuk dibagikan kepada setiap entitas. Data tersebut dibagikan dengan cara dikirimkan melalui jaringan dimana memungkinkan seseorang yang tidak bertanggung jawab untuk meng-*capture* data tersebut. Dan apabila data keamanan dari SSO ini telah diperoleh maka akan berakibat fatal mengingat data tersebut dapat digunakan untuk mengakses semua aplikasi dalam entitas SSO. Maka diperlukan sebuah metode pengamanan data yang handal sehingga tidak mudah dibaca oleh penyerang walaupun dengan Teknik penyerangan *dictonary attack*. Dalam penelitian ini pengamanan data dilakukan dengan menggunakan algoritma RC4 (*Rivest Cipher 4*), dan diharapkan dapat mengamankan data kredensial yang saling ditutarkan dalam entitas SSO.

Kata Kunci: *Single Sign-On* (SSO), *Security Assertion Markup Language* (SAML), Algoritma *Rivest Cipher 4* (RC4), data kredensial, *dictonary attack*.

IMPLEMENTATION OF RC4 ALGORITHM IN SAML (SECURITY ASSERTION MARKUP LANGUAGE) PROTOCOL ON SSO (SINGLE SIGN ON) SERVICE

By

Bagus Enggar Tiasto

1157050027

ABSTRACT

SSO (Single Sign-On) is an authentication service that allows users to use a set of credential data to access multiple applications. SSO can be implemented by using many protocols, one of which is SAML (Security Assertion Markup Language). SAML is a framework or open message delivery standard that allows identity and security information to be shared with each entity. The data is shared by sending it over a network which allows someone who is not responsible to capture the data. And if the security data from this SSO has been obtained it will have fatal consequences considering that the data can be used to access all applications in the SSO entity. Then we need a reliable data security method so that it is not easy to read by an attacker even with a dictonary attack technique. In this study data security is performed using the RC4 algorithm (Rivest Cipher 4), and it is expected to secure credential data that is exchanged within the SSO entity.

Keywords : Single Sign-On (SSO), Security Assertion Markup Language (SAML), Rivest Cipher 4 Algorithm (RC4), credential data, dictonary attack.