ABSTRAK

Muhammad Akbar Sidiq

Teknik Elektro

Implementasi Algoritma SHA-2 Dan AES Sebagai Sistem Keamanan Pada Proses Pensinyalan *Mobile* IPv6

Berdasarkan data statistik, mengakses Internet melalui perangkat *mobile* merupakan salah satu yang paling populer di mana setengah dari lalu lintas web di seluruh dunia menggunakan perangkat *mobile*. Teknologi *Mobile* IP dapat digunakan sebagai protokol dalam menjaga konektifitas walaupun perangkat berpindah saluran koneksi dari jaringan yang terhubung ke jaringan yang baru. Namun komunikasi pada MIPv6 (*Mobile* IPv6) beresiko terhadap serangan. Metode untuk mencegah serangan pada proses pensinyalan MIPv6 dapat menggunakan IPsec dengan metode *tunnel* menggunakan protokol ESP (*Encapsulating Security Payload*) yang telah mendukung enkripsi dan otentikasi. Algoritma enkripsi 3-DES dan algoritma otentikasi SHA-1 merupakan yang paling umum digunakan hingga saat ini. Algoritma 3-DES dan SHA-1 dianggap telah memiliki celah keamanan sehingga diperlukan suatu algoritma pembaharuan. Penelitian ini menggunakan AES dan SHA-2 sebagai algoritma yang diimplementasikan pada IPsec yang merupakan pembaharuan dari 3-DES dan SHA-1. Berdasarkan penelitan yang dilakukan, AES dan SHA-2 mempunyai tingkat keamanan yang lebih unggul dibandingkan dengan 3-DES dan SHA-1 terhadap kriptanalisis. AES dan SHA-2 juga lebih unggul secara performa keseluruhan dibandingkan 3DES dan SHA-1 dengan nilai *throughput* masing-masing 41,47 Mbit/s dan 25,88 Mbit/s. Selain itu AES dan SHA-2 juga memiliki rata-rata nilai *delay* dan *jitter* yang lebih kecil dengan nilai masing-masing 0,189 ms dan 0,218 ms.

Kata Kunci: MIPv6, IPsec, AES, SHA-2, 3-DES, SHA-1

ABSTRACT

Muhammad Akbar Sidiq

Electrical Engineering

Implementation of SHA-2 And AES Algorithm As A Security System In The Mobile IPv6 Signaling Process

Based on statistical data, accessing the internet via mobile devices is one of the most popular where half of the worldwide web traffic uses a mobile account. Mobile IP technology can be used as a protocol to maintain connectivity even if the device changes connection channels from the network that is connected to the new network. However communication on MIPv6 (Mobile IPv6) is at risk of attack. The method to prevent attacks on the MIPv6 signaling process can use IPsec with the tunnel method using the ESP (Encapsulating Security Payload) protocol that supports encryption and authentication. The 3-DES encryption algorithm and the SHA-1 authentication algorithm are the most commonly used today. This study uses AES and SHA-2 which are updates from 3-DES and SHA-1 as algorithms implemented in IPsec. Based on the research conducted, AES and SHA-2 have a higher level of security compared to 3-DES and SHA-1 against cryptanalysis. AES and SHA-2 are also superior in overall performance compared to 3DES and SHA-1 with respectively of throughput values is 41,47 Mbit/s and 25,88 Mbit/s. In addition, AES and SHA-2 also have smaller average delay and jitter with respectively of values is 0,189 ms and 0,218 ms.

Keywords: MIPv6, IPsec, AES, SHA-2, 3-DES, SHA-1