ABSTRAK

Randy Aprilia
Teknik Elektro

Analisis Performansi Keccak Message Authentication Code Sebagai Metode Autentikasi Pesan Pensinyalan Mobile IPv6

Autentikasi pensinyalan Mobile IPv6 yang disarankan RFC 6275 saat ini menggunakan Secure Hash Algorithm 1 (SHA-1). SHA-1 sudah diketahui memiliki beberapa celah keamanan. Terdapat fungsi hash baru yang memperbaiki celah tersebut yaitu SHA-3 (Keccak). Penelitian ini melakukan analisis performansi SHA-3 sebagai metode autentikasi pensinyalan Mobile IPv6. Hasil yang didapat untuk waktu autentikasi rata-rata pensinyalan Binding Update sebesar 34.65375 ms, dan pensinyalan Binding Acknowledgment sebesar 24.43812 ms untuk SHA-3. Besar paket autentikasi Mobile IPv6 menggunakan SHA-3 sebesar 124 byte untuk Binding Update dan 108 byte untuk Binding Acknowledgment. Waktu rata-rata proses handover Mobile IPv6 secara keseluruhan menggunakan SHA-3 sebesar 4.50 detik, dan SHA-1 sebesar 4.51 detik. Dengan waktu proses keseluruhan tidak berbeda jauh dengan SHA-1, namun memiliki tingkat keamanan yang baik dibandingkan dengan SHA-1, SHA-3 cocok digunakan sebagai pengganti SHA-1 untuk autentikasi pensinyalan Mobile IPv6.

Kata kunci: Mobile IPv6, SHA-1, SHA-3, MAC, Pensinyalan

ABSTRACT

Randy Aprilia
Teknik Elektro

Performance Analysis of Keccak Message Authentication Code for Mobile IPv6 Signaling Authentication Method

The current IPv6 Mobile signaling authentication proposed by RFC 6275 currently uses Secure Hash Algorithm 1 (SHA-1). SHA-1 is known to have several security weaknesses. There is a new hash function that fixes this weaknesses, namely SHA-3 (Keccak). This study analyzes the performance of SHA-3 as a MIPv6 signaling authentication method. The results obtained for average processing time Binding Update message is 34,65375 ms, and Binding Acknowledgment is 24,43812 ms for SHA-3. Packet size of Mobile IPv6 authentication is 124 bytes for Binding Update and 108 bytes for Acknowledgment Binding using SHA-3. The average time of the IPv6 overall handover process using SHA-3 is 4.50 seconds, and SHA-1 is 4.51 seconds. With a small processing time difference, but have a good level of security compared to SHA-1, SHA-3 is suitable for use as a substitute for SHA-1.

Keywords: Mobile IPv6, SHA-1, SHA-3, MAC, Signaling