PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN MENGGUNAKAN *AUTHENTICATION, AUTHORIZATION, ACCOUNTING* (AAA) DALAM MENCEGAH SERANGAN *RANDOM* MAC *ADDRESSS*

Ariansyah Arifin

ABSTRAK

Wireless LAN salah satu tipe jaringan yang paling banyak digunakan karena kemudahannya. Namun dalam pengguaan jaringan ini, sering kali muncul beberapa masalah. salah satunya adalah fitur di *end device* yaitu Random MAC Address. Pada beberapa perangkat *end device* baru, seperti android 10, 12, iOS 16, windows 10. Konfigurasi default atau tidak default di pengaturan jaringannya adalah ada *Random* MAC *Address*. Terkadang fitur ini membuat *Network administrator* kesulitan pada saat mengatur *user*, membuat *IP Address pool* cepat habis karena MAC *Address* yang dipergunakan *user* yaitu berubah-ubah. Apalagi bila mengimplementasikan beberapa fitur manajemen jaringan seperti bandwidth *management*, *firewall* dan lain-lain akan sulit. Tujuan dalam penelitian ini adalah membuat pengamanan *Wireless* LAN yang ditingkatkan dan manajemen jaringan untuk dapat mencegah serangan *Random* MAC *Address*. Dengan melakukan penerapan metode protokol keamanan *Authentication, Authorization, Accounting* (AAA), serta dikombinasikan dengan metode protokol otentikasi EAP PEAP-MSCHAPv2. Dengan metode tersebut, hasil penelitian ini menunjukkan bahwa sistem keamanan baru (EAP-PEAP MSCHAPv2 (AAA)) memiliki tingkat kesulitan koneksi yang lebih tinggi, dengan nilai rata-rata sebesar 2,70 dibandingkan dengan sistem keamanan sebelumnya (WPA2-PSK) yang memiliki nilai rata-rata sebesar 2,21. Nilai rata-rata yang lebih tinggi mengindikasikan peningkatan ketahanan terhadap serangan, menunjukkan kemampuan sistem keamanan baru dalam mencegah serangan *Random* MAC *Address*. Dalam hal kecepatan akses website, sistem keamanan baru mencapai nilai rata-rata yang lebih tinggi dibandingkan dengan sistem sebelumnya pada berbagai website seperti YouTube, Leads UPN Veteran Jakarta, email Google, dan Speedtest by Ookla.Temuan penelitian mengungkap perbedaan signifikan dalam kemampuan antara WPA2-PSK dan EAP-PEAP MSCHAPv2 (AAA) dalam mencegah dampak serangan *Random* MAC *Address* dan menjaga kinerja jaringan. WPA2-PSK mengalami masalah serius ketika pengguna "*Forget* WiFi" dan menghubungkan kembali, yang mengakibatkan habisnya alamat IP dan pembatasan bandwidth. Sebaliknya, EAP-PEAP MSCHAPv2 (AAA) menunjukkan resistansi yang lebih baik terhadap serangan "*Forget* WiFi", Sistem ini menjaga ketersediaan alamat IP, menjaga kualitas layanan jaringan yang baik, dan membatasi akses yang tidak sah.

Kata Kunci : *Wireless* LAN, Perangkat *End device*, *Random* MAC *Address*, IP Address Pool, AAA, EAP-PEAP MSCHAPv2, WPA2-PSK.

SECURITY OF WIRELESS LAN NETWORKS USING AUTHENTICATION, AUTHORIZATION, ACCOUNTING (AAA) IN PREVENTING RANDOM* MAC *ADDRESSS ATTACKS

Ariansyah Arifin

ABSTRACT

Wireless LAN is one of the most widely used network types because of its convenience. But in the use of this network, problems often arise. one of them is a feature on the end device, namely the Random MAC Address. On some new end devices, such as Android 10, 12, iOS 16, Windows 10. The default or non-default configuration in the network settings is that there is a Random MAC Address. Sometimes this feature makes it difficult for network administrators to manage users, causing the IP address pool to run out quickly because the MAC address used by the user changes. Especially if implementing several network management features such as bandwidth management, firewalls and others will be difficult. The purpose of this research is to make enhanced Wireless LAN security and network management to be able to prevent Random MAC Address attacks. By implementing the Authentication, Authorization, Accounting (AAA) security protocol method, and combined with the PEAP-MSCHAPv2 EAP authentication protocol method. With this method, the results of this study indicate that the new security system (EAP-PEAP MSCHAPv2 (AAA)) has a higher connection difficulty level, with an average value of 2.70 compared to the previous security system (WPA2-PSK) which has the average value of 2.21. A higher average value indicates increased resistance to attacks, indicating the ability of the new security system to prevent Random MAC Address attacks. In terms of website access speed, the new security system achieves higher average scores compared to the previous system on various websites such as YouTube, Leads UPN Veteran Jakarta, Google email, and Speedtest by Ookla. The research findings reveal significant differences in capabilities between WPA2-PSK and EAP-PEAP MSCHAPv2 (AAA) in preventing the impact of Random MAC Address attacks and maintaining network performance. WPA2-PSK encountered a serious problem when users "Forget WiFi" and reconnected, resulting in exhausted IP addresses and bandwidth throttling. On the other hand, EAP-PEAP MSCHAPv2 (AAA) shows better resistance to "Forget WiFi" attacks. This system maintains IP address availability, maintains good quality of network service, and restricts unauthorized access.

Keywords *: Wireless LAN, End device, Random* MAC *Address, AAA, EAP-PEAP MSCHAPv2, WPA2-PSK*