PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN PROTOKOL EAP-TTLS DAN OTENTIKASI MSCHAPV2 PADA FAKULTAS ILMU KOMPUTER UPN VETERAN JAKARTA

Kukuh Bagas Permadi

ABSTRAK

Penggunaan pada protokol WPA memiliki dua proses, antara lain adalah otentikasi serta enkripsi. Pada tingkat *network* dengan infrastuktur yang besar serta dengan lalu lintas *network* yang tinggi sama halnya dengan universitas, kantor perusahaan atau tempat umum lainnya yang menggunakan *wireless* LAN, proses otentikasi merupakan proses yang pertama kali yang dilakukan agar pengguna jaringan *wireless* LAN dapat mengakses jaringan *internet*. Maka dari itu, tidak hanya aman namun proses otentikasi bisa beroperasi dengan cepat. Solusi dari penelitian ini adalah dengan menerapkan Protokol IEEE 802.1x EAP dengan *Extensible Authentication Protocol – Tunneled Transport Layer Security* (EAP-TTLS) untuk membuat *secure tunnel* (terowongan keamanan) dalam pertukaran kunci pada jaringan *wireless*, serta dengan *inner authentication Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAPv2). Luaran yang dihasilkan pada penelitian ini adalah membangun suatu keamanan pada jaringan *wireless* terpusat pada Fakultas Ilmu Komputer UPN Veteran Jakarta.

Kata Kunci: IEEE 802.1x EAP, EAP-TTLS, MSCHAPv2, RADIUS *Server*, *Wireless* LAN.

SECURING THE WIRELESS LAN NETWORK WITH EAP-TTLS PROTOCOL AND MSCHAPV2 AUTHENTICATION IN THE FACULTY OF COMPUTER SCIENCE UPN VETERAN JAKARTA

Kukuh Bagas Permadi

ABSTRACT

The use of the WPA protocol has two processes, including authentication and encryption. At the network level with large infrastructure and high network traffic as well as universities, corporate offices or other public places that use wireless LANs, the authentication process is the first process done so that wireless LAN network users can access the internet network. Therefore, it is not only safe but the authentication process can operate quickly. The solution of this research is to implement the IEEE 802.1x EAP Protocol with Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS) to create a secure tunnel (security tunnel) in key exchange on a wireless network, as well as with the inner authentication of the Microsoft Challenge Handshake Authentication Protocol. Version 2 (MSCHAPv2). The output produced in this study is to build a security on a centralized wireless network at the Faculty of Computer Science UPN Veteran Jakarta.

Keywords: IEEE 802.1x EAP, EAP-TTLS, MSCHAPv2, RADIUS *Server*, *Wireless* LAN.