Analisis ketahanan protokol ieee 802 11w terhadap serangan pada management frame = Robustness analysis of ieee 802 11w against management frame attack / Samuel Parlindungan Ulysses

Samuel Parlindungan Ulysses, author

Abstrak

ABSTRAK
Jaringan nirkabel (wireless) sekarang ini sudah menjadi media komunikasi yang sangat sering digunakan. Namun kepopuleran media ini dibayangi oleh berbagai macam masalah keamanan yang dapat merugikan penggunanya. Masalah yang muncul adalah serangan pada management frame. Serangan ini memanfaatkan kelemahan baik access point maupun client yang frame wifi-nya sama-sama tidak dienkripsi, sehingga attacker dapat melakukan spoofed frame wifi dan membuat router dan client saling terputus koneksinya. Pada skripsi ini, diajukan sebuah rancangan untuk melakukan mitigasi terhadap serangan management frame dengan menggunakan protokol IEEE 802.11w. Rancangan IEEE 802.11w ini membuat frame wifi dari client dan router tervalidasi, sehingga router dan client dapat mengalami koneksi meskipun mendapat serangan pada management frame. Dalam skripsi ini dibahas dan dianalisis betapa berbahayanya serangan pada management frame yang dapat menyerap bandwidth setelah sukses memutuskan koneksi. Selain itu dibahas pula pergerakan management frame saat serangan dilakukan dan saat protokol IEEE 802.11w dijalankan. Selanjutnya dianalisis juga perbandingan throughput saat normal dan dilakukan serangan, serta perbandingan throughput IEEE 802.11 dengan IEEE 802.11w saat diserang. Saat serangan pada management frame berhasil ada perlawanan yang dilakukan, yaitu attempt to reconnect, namun ratio-nya dibandingkan dengan deauthentication frame sangatlah kecil. Berdasarkan penelitian ini dapat ditarik kesimpulan bahwa deauthentication attack memutuskan client dan router yang tidak diimplementasikan IEEE 802.11w. Hal ini disebabkan pada saat diimplementasikan IEEE 802.11w terdapat action frame sebagai tanda validasi integrity check yang dilakukan secara checksum pada tiap deauthentication frame. Ratio dari action frame adalah 49,6%. Ratio ini sangat tinggi apabila dibandingkan dengan ratio management frame untuk attempt to reconnect.
<hr>
ABSTRACT
Wireless network nowadays has become a common medium of communication. However, there are many security issues that arise. One of them is management frame attack that can disconnect wifi. This attack uses the vulnerability of both client and router’s unencrypted wifi frame. As the result, the attacker can manipulate and spoof wifi frame and make both router and client disconnected. In this research, a plan is proposed to mitigate management frame attack by using IEEE 802.11w. This standard validates wifi frame both client and router. Therefore, the router and client can be associated, authenticated, and connected although they are attacked. In this work, it is analyzed how dangerous the management frame attack is, because attacker can increase his throughput after disconnecting other clients. Moreover, it is also explained the comparison of the movement of the management frame in IEEE 802.11 and IEEE 802.11w while attacked. Furthermore, it is analyzed the comparison of the normal throughput IEEE 802.11 and under-attacked IEEE 802.11w’s throughput. Actually when the management frame attack launched, there is

management frame attempting to reconnect. Nevertheless, the ratio is very small if compared to the deauthentication frame. From this work, it can be concluded that deauthentication attack can disconnect the connection if the router and client are not implemented with IEEE 802.11w. However, if both router and client are implemented with IEEE 802.11w, attacker can not disconnect it. This happens because in IEEE 802.11w, there is action frame that is produced which shows that the validation of the integrity check is successfull. The ratio of the action frame is 49,6%. As it can be seen, the ratio of action frame is very high compared to the management frame which is used to attempt to reconnect.