ABSTRAK

Dengan semakin berkembang dan populernya jaringan nirkabel, menyebabkan munculnya isu-isu keamanan pada jaringan nirkabel. Serangan terhadap jaringan nirkabel pun semakin berkembang.

Studi literatur ini mengeksplorasi lebih dalam terhadap proses enkripsi pada WEP, metode enkripsi yang digunakan, serta celah keamanan pada WEP diantaranya terletak pada initialization vector (IV) yang hanya sebesar 24 bit, besar IV ini terlalu pendek, sehingga kemungkinan terjadi perulangan kunci hanya dalam waktu beberapa jam saja. Selain itu proses enkripsi RC4 memiliki kunci yang lemah, dan digunakan secara berulang-ulang pada proses enkripsi.

Hasil yang dicapai diantaranya adalah ditemukannya beberapa kelemahan pada WEP, yaitu : kesalahan managemen IV, keterbatasan *numerical* 24-bit pada IV, dan WEP tidak dapat menyaring *replay paket* yang dikirimkan. Celah keamanan tersebut bisa menyebabkan terjadinya serangan, seperti : WEP *brute force, bit-flipping,* FMS *attack,* dan *Initialization Vector* (IV) *replay attack.* Untuk mencegah terjadinya serangan tersebut, terdapat beberapa solusi yang bisa digunakan, yaitu : melakukan pembatasan MAC *address* dan IP *address,* menggunakan ebtable dan ARP, melakukan perubahan kunci WEP secara berkala, menggunakan *captive portal,* serta memposisikan semua *access point* diluar *firewall* yang melindungi jaringan utama.

Kata kunci : Enkripsi, *Wired Equivalent Privacy* (WEP), *security* (keamanan), Kelemahan RC4, *Rivest Code* 4 (RC4), Kelemahan WEP.