Ocena możliwości wykorzystania WLAN w srodowisku o podwyzszonym zagrozeniu

Wstęp…….4

Rozdział I.
Zagrozenia i mozliwe ataki na siec WLAN

1.1. Wardriving …….7
1.2. Nieautoryzowane punkty dostepowe (rogue AP)……. 9
1.3. Atak Man in the Middle – MitM („Przechwycenie sesji”) …….10
1.4. Anulowanie uwierzytelnien i skojarzen……. 12
1.5. Atak DoS…….13
1.6. Zagrozenia w trybie ad-hoc……. 16

Rozdział II.
Systemy zabezpieczen stosowane w sieciach WLAN.

2.1. Technologie sieci bezprzewodowych i ich wlasciwosci……. 20
2.2. Zabezpieczenia wykorzystywane w warstwie lacza danych …….24
2.3. Wspólpraca sieci bezprzewodowych …….31

Rozdział III.
Sposoby uwierzytelniania abonentów w sieciach WLAN

3.1. Uwierzytelnianie otwarte – SSID …….37

3.2. Uwierzytelnianie na podstawie adresu MAC …….38
3.3. Uwierzytelnianie – RADIUS …….39
3.4. Mechanizmy uwierzytelniania 802.1x (EAP)……. 42

Rozdział IV.
Propozycja zabezpieczen sieci WLAN

4.1. System autentykacji uzytkowników WLAN …….49
4.2. Zabezpieczenie transmisji danych w sieci WLAN……. 50
4.3 Bezpieczeństwo fizyczne sieci WLAN …….51

Podsumowanie……. 55
Bibliografia …….56
Spis rysunków i tabel……. 57