



Spis treści

Wprowadzenie.....	19
Rozdział 1. Przegląd zabezpieczania sieci WLAN	23
WLAN z perspektywy	23
Elementy sieci WLAN i terminologia.....	25
Standardy WLAN	28
Bezpieczeństwo WLAN.....	28
Model koncepcyjny domeny bezpieczeństwa WLAN.....	28
Poruszanie się po książce i rozdziałach	31
Podsumowanie	32
Rozdział 2. Podstawy mechaniki i mechanizmów bezpieczeństwa.....	33
Mechanika zabezpieczeń.....	33
Mechanizmy poufności	35
Szyfrowanie przy użyciu klucza symetrycznego.....	35
Szyfrowanie asymetryczne	40
Mocne i słabe strony algorytmów szyfrowania	44
Mechanizmy integralności	45
Funkcje mieszające	45
Podpisy cyfrowe	47
Zarządzanie kluczami	50
Protokoły uwierzytelniania i identyfikacji.....	55
Protokoły uwierzytelniania PPP	55
PPP Password Authentication Protocol.....	56
PPP Challenge Handshake Authentication Protocol	58
PPP Extensible Authentication Protocol	61
Protokół TACACS+.....	62
Uwierzytelnianie TACACS+.....	63
Autoryzacja TACACS+.....	64
Rejestrowanie kont TACACS+	64
Transakcje TACACS+.....	65
Protokół RADIUS.....	66
Uwierzytelnianie RADIUS.....	66
Autoryzacja RADIUS.....	66
Rejestrowanie kont RADIUS	67
Transakcje RADIUS.....	67
Protokół Kerberos	68
Żądanie uwierzytelnienia Kerberos i odpowiedź	69
Żądanie i odpowiedź aplikacji Kerberos	70
Ipv6	72

Struktura i reprezentacja adresu IPv6.....	73
Nagłówek IPv6.....	73
Skalowalność.....	74
Przejsście.....	74
IPSec.....	74
Nagłówek uwierzytelniania.....	75
Encapsulated Security Payload.....	75
Związki bezpieczeństwa.....	75
Zarządzanie kluczami.....	76
Podsumowanie.....	76
Rozdział 3. Standardy WLAN.....	77
Organizacje standaryzacyjne, pozycja, kontekst i wpływ.....	77
IEEE.....	78
Standardy IEEE 802.....	78
Wi-Fi Alliance.....	82
Ogólny opis WPA.....	83
Wireless LAN Association.....	85
Sprzęt, fale radiowe i modulacja.....	85
Regulacje FCC.....	85
Technologie radiowe w 802.11.....	86
Krótka dyskusja o najistotniejszych standardach.....	87
IEEE 802.11.....	87
IEEE 802.11b.....	88
Alokacja kanałów.....	88
IEEE 802.11a.....	88
IEEE 802.11g.....	90
IEEE 802.11f.....	91
IEEE 802.11e.....	91
Zdolności QoS.....	92
Mechanizmy QoS.....	92
Jednostki powiązane z QoS.....	93
Związki oparte na zdolnościach QoS.....	93
IEEE 802.11k.....	93
IEEE 802.11h.....	94
Europejskie organizacje standaryzacyjne i regulacje: ERO.....	95
Europejskie organizacje standaryzacyjne i regulacje: ETSI.....	95
Szczegóły 802.11h.....	96
Light Weight Access Point Protocol.....	97
Podsumowanie.....	97
Rozdział 4. Podstawy WLAN.....	99
WLAN: elementy i charakterystyki.....	99
Podstawowa topologia WLAN.....	102
Elementy składowe WLAN.....	104
Usługi.....	104
Ramki.....	107
Diagram stanów WLAN.....	109

Podstawowa choreografia	111
Ramki nawigacyjne.....	111
Ramki sondy	112
Ramki uwierzytelniania	113
Anulowanie uwierzytelnienia	116
Ramki skojarzenia.....	117
Ramki ponowienia skojarzenia	119
Ramki anulowania skojarzenia	120
Ramki danych	121
Kody statusu i przyczyny	121
WEP	125
Podsumowanie	126
Rozdział 5. Podstawowe metody uwierzytelniania i prywatności WLAN.....	127
Mechanika uwierzytelniania	127
Uwierzytelnianie otwarte	129
Model i założenia zaufania	130
Obsługa infrastruktury AAA	130
Aplikacje, słabe punkty i środki zaradcze	130
Śledzenie i rejestrowanie kont	130
Uwierzytelnianie na podstawie adresu MAC.....	131
Model i założenia zaufania	132
Obsługa infrastruktury AAA	132
Śledzenie i rejestrowanie kont	132
Aplikacje, słabe punkty i środki zaradcze	132
Uwierzytelnianie przy użyciu klucza współużytkowanego	133
Działanie protokołu.....	133
Model i założenia zaufania	134
Obsługa infrastruktury AAA	134
Śledzenie i rejestracja kont	135
Aplikacje, słabe punkty i środki zaradcze	135
Mechanika prywatności w WEP	136
Model przetwarzania WEP	137
Algorytm RC4	137
Dane i integralność	138
Ziarno i długość klucza	138
Generowanie IV.....	139
Generowanie i selekcja kluczy	139
Pakowanie.....	140
Deszyfrowanie.....	140
Słabości	140
Podsumowanie	140
Rozdział 6. Słabe punkty w sieciach bezprzewodowych	141
Cele atakującego	142
Schematy ataków	142
Rekonesans	143
DoS.....	144
Dostęp do sieci	144

Ataki rozpoznawcze.....	146
Sniffing i SSID	147
Narzędzia do sniffingu.....	148
Prismdump.....	149
Ethereal i Tcpdump	149
Sniffery komercyjne.....	149
Wardriving i narzędzia	149
Network Stumbler i Mini Stumbler.....	150
Narzędzia dla Macintosha	151
Kismet	151
Wellenreiter	152
bsd-airtools	153
Ataki DoS.....	154
Ataki z anulowaniem uwierzytelnień i skojarzeń	155
Atak Transmit Duration.....	156
Ataki na mechanizmy uwierzytelniania	156
Ataki na mechanizm uwierzytelniania z kluczem współużytkowanym	156
Podszywanie się pod adres MAC	157
Odkrywanie strumienia klucza WEP i czystego tekstu	157
Słowniki strumieni kluczy	158
Metody odkrywania strumieni kluczy RC4.....	158
Atak jawnym tekstem.....	158
Kolizje IV i paradoks dnia urodzin	159
Atak z reakcją.....	160
Atak z indukcją.....	160
Sposoby wykorzystania odkrytych strumieni kluczy	161
Wpuszczanie pakietów: wybór własnego IV	161
Modyfikacja komunikatu i odpowiedź.....	162
Deszyfrowanie.....	162
Krótko o rozwiązaniach.....	162
Ataki w celu odkrycia klucza WEP	163
Ataki słownikowe	163
Atak Fluhrer-Mantin-Shamir.....	164
Narzędzia FMS.....	165
Ataki na protokoły EAP.....	166
Podsumowanie tematu 802.1x i EAP	167
Słownikowy atak na LEAP.....	167
Atak pośrednika na protokół PEAP.....	169
Podstawiane punkty dostępowe	170
Bezpieczeństwo trybu ad-hoc	171
Podsumowanie	172
Rozdział 7. Protokoły uwierzytelniania EAP dla sieci WLAN	173
Mechanizmy kontroli dostępu i uwierzytelniania	173
Model trójstronny	174
Warstwowy schemat uwierzytelniania	176
EAP	180
Ramki, komunikaty i schemat działania EAP	180

Mechanizmy uwierzytelniania EAP	186
EAP-MD5	186
EAP-OTP	188
EAP-GTC	188
EAP-TLS	188
EAP-TTLS	192
PEAP	193
Format ramki PEAP	194
Arbitralna wymiana parametrów PEAP	194
Schemat działania PEAP	196
802.1x: wprowadzenie i ogólne zasady	199
EAPOL	200
Cisco LEAP (EAP-Cisco Wireless)	201
EAP-FAST	203
Format ramki EAP-FAST	205
Schemat działania EAP-FAST	206
Podsumowanie	208
Rozdział 8. Protokoły szyfrowania i integralności danych dla sieci WLAN	209
IEEE 802.11i	210
Protokoły szyfrowania	211
WEP	211
RC4	213
Hermetyzacja WEP	215
Dehermetyzacja WEP	217
TKIP (802.11i/WPA)	218
Michael MIC (802.11i/WPA)	219
Przeciwdziałanie atakom powtórzeniowym	221
Algorytm mieszania klucza	222
Konstrukcja pakietu TKIP	224
Hermetyzacja TKIP	224
Dehermetyzacja TKIP	225
CCMP	226
Hermetyzacja CCMP	227
Dehermetyzacja CCMP	229
Algorytm CCM	230
Zarządzanie kluczami	232
Ustanawianie klucza głównego	232
Hierarchia kluczy	233
Hierarchia klucza par	234
Hierarchia klucza grupowego	236
Wymiana klucza	237
Uzgadnianie 4-kierunkowe	237
Uzgadnianie klucza grupy	238
Związki bezpieczeństwa	239
PMKSA	239
PTKSA	239
GTKSA	240

Niszczenie związku bezpieczeństwa	240
WPA i protokoły Cisco	240
Protokoły Cisco	240
WPA	241
Rozwiązania problemów z bezpieczeństwem	242
Rekonesans	242
Ataki DoS	242
Ataki na uwierzytelnianie z kluczem współużytkowanym	242
Podszywanie się pod adresy MAC	242
Modyfikacja i powtarzanie komunikatów	243
Odkrywanie kluczy WEP metodą słownikową	243
Odkrywanie klucza strumienia WEP	243
Atak Fluhrer-Manitin-Shamir na słabe klucze	243
Podstawiane punkty dostępowe	243
Rozważania na temat bezpieczeństwa EAP	244
Podsumowanie	244
Rozdział 9. SWAN: wdrażanie kompleksowych zabezpieczeń	247
Ogólne omówienie funkcji bezpieczeństwa SWAN	247
Tryby wdrożeniowe WLAN i funkcje zabezpieczające	249
Uwierzytelnianie struktury SWAN	254
Zarządzanie radiowe i wykrywanie intruzów	256
SWAN Fast Secure Roaming (CCKM)	259
Lokalna usługa 802.1x uwierzytelniania RADIUS	264
Podsumowanie	266
Rozdział 10. Wskazówki dotyczące projektowania bezpiecznych sieci WLAN	269
Podstawy projektu WLAN	269
Polityka bezpieczeństwa WLAN	270
Obsługa urządzeń	270
Obsługa uwierzytelniania	271
Umiejscowienie usług sieciowych	271
Mobilność	271
Obsługa aplikacji	272
Zarządzanie punktami dostępowymi	272
Projekt pokrycia radiowego	272
Dostęp wielogrupowy	273
Ogólne zalecenia dotyczące bezpieczeństwa	273
Zalecenia dotyczące punktów dostępowych	273
Zalecenia dotyczące klientów WLAN	274
Zalecenia dotyczące infrastruktury	274
Wdrażanie nowych sieci WLAN	275
Rozwiązania wbudowane	276
Łagodzenie zagrożeń	277
Podstawy projektu i wbudowane zabezpieczenia	278
Nakładki VPN	279
Przeciwdziałanie zagrożeniom	280
Technologie nakładkowe VPN	281

Podstawy projektu i nakładki VPN	284
Projekt łączący VPN i wbudowane mechanizmy bezpieczeństwa	285
Przeciwdziałanie zagrożeniom	286
Podstawy projektu oraz połączenie VPN i wbudowanych mechanizmów zabezpieczających	287
Integracja z istniejącym wdrożeniem	289
Urządzenia umożliwiające uaktualnianie do WPA, współpracujące tylko z WEP oraz pre-WEP	289
Wdrożenia zintegrowane	290
Przeciwdziałanie zagrożeniom	292
Podstawy projektu	293
Rozważania na temat projektu SWAN z centralnym przełączaniem	295
Projekt kontroli wstępu	296
Podsumowanie	298
Rozdział 11. Operacyjne i projektowe wnioski na temat zabezpieczania sieci WLAN...	299
Wykrywanie i ochrona przed fałszywymi punktami dostępowymi	299
Wykrywanie fałszywych punktów dostępowych SWAN	300
Ręczne wykrywanie fałszywych punktów dostępowych	301
Sieciowe wykrywanie fałszywych punktów dostępowych	303
Skalowanie usług WLAN	304
Zalecane rozwiązania RADIUS	304
Zalecane rozwiązania VPN	307
Tworzenie klastrów IPSec VPN	308
Zewnętrzne urządzenie równoważące IPSec	310
Zewnętrzne równoważenie obciążenia SSL	312
Dostęp dla gości	313
Wymagania w zakresie dostępu dla gości korporacyjnych	313
Otwarte uwierzytelnianie gości WLAN	313
Separacja ruchu sieciowego gości na krawędzi sieci korporacyjnej	313
Łączność plug-and-play	313
Kwestie kosztów i bezpieczeństwa	313
Projekt mechanizmu dostępu dla gości	314
Podsumowanie	316
Rozdział 12. Przykłady i wskazówki na temat konfiguracji zabezpieczeń WLAN.....	317
Produkty Cisco Enterprise Class Wireless LAN	318
Punkt dostępowy Cisco Aironet AP1200	318
Punkt dostępowy Cisco Aironet AP1100	318
Punkt dostępowy Cisco Aironet AP350	319
Most Cisco Aironet BR350	319
Most Cisco Aironet BR1410	319
Urządzenia Cisco Aironet 802.11b/a/g i Cisco Client Extensions-Enabled	319
Cisco Secure Access Server	320
Cisco Wireless LAN Solution Engine	320
Catalyst 6500 Wireless LAN Services Module	321
Metody zabezpieczania WLAN: wskazówki i przykłady konfiguracji	321
Przeglądanie stron interfejsu graficznego HTML	321

Wskazówki i przykłady konfiguracji IOS CLI	323
Konfiguracja otwarta/bez WEP	323
Konfiguracja otwarta/z WEP i WPA-PSK	323
Konfiguracja uwierzytelniania na podstawie adresu MAC	326
Konfiguracja EAP z dynamicznym WEP	327
Konfiguracja WPA-DOT1x	335
Konfiguracja IPSec VPN w sieci WLAN	340
Konfiguracja zestawu profili bezpieczeństwa (SSID/VLAN)	343
Bezprzełączeniowe wdrożenie SWAN: wskazówki i przykłady konfiguracji	348
Podstawowa konfiguracja WDS	348
Konfiguracja Fast Secure Roaming (CKKM)	350
Konfiguracja agregacji RF i wykrywanie podstawionych punktów dostępowych	353
Konfiguracja uwierzytelniania lokalnego (usługa RADIUS Fall-Back)	356
Zabezpieczanie łącz most-most	357
Wskazówki na temat konfiguracji zarządzania zabezpieczoną siecią WLAN	359
Wdrożenie SWAN z centralnym przełączaniem: wskazówki i przykłady konfiguracji	362
Podsumowanie	366
Rozdział 13. Przykłady wdrożeń WLAN	367
Przykłady wdrożeń w dużych środowiskach korporacyjnych	367
Przykład I wdrożenia WLAN w dużym środowisku korporacyjnym	368
Szczegóły wdrożenia zabezpieczeń WLAN	369
Integracja przewodowej/bezprzewodowej sieci LAN oraz szczegóły infrastruktury WLAN i zarządzania użytkownikami	369
Szczegóły implementacji AAA oraz infrastruktury zewnętrznej bazy danych użytkowników	370
Szczegóły wdrożenia usług VoIP i obsługi gości	372
Podsumowanie przykładu I wdrożenia korporacyjnej sieci WLAN	374
Przykład II wdrożenia WLAN w dużym środowisku korporacyjnym	374
Integracja przewodowej LAN z bezprzewodową	376
Problemy wdrożeniowe	376
Szczegóły implementacji infrastruktury AAA	377
Podsumowanie przykładu II wdrożenia korporacyjnej sieci WLAN	377
Przykłady wdrożeń pionowych	377
Przykład I wdrożenia WLAN w placówce handlowej	379
Szczegóły wdrożenia zabezpieczeń WLAN	379
Szczegóły implementacji WDS i infrastruktury AAA	382
Problemy wdrożeniowe	382
Podsumowanie przykładu I wdrożenia WLAN w sieci handlowej	383
Przykład II wdrożenia WLAN w placówce handlowej	383
Przykład wdrożenia WLAN w placówce uniwersyteckiej	386
Przykład I wdrożenia WLAN w placówce finansowej	389
Przykład II wdrożenia WLAN w placówce finansowej	391
Przykład I wdrożenia WLAN w sieci placówek służby zdrowia	393
Przykład II wdrożenia WLAN w sieci placówek służby zdrowia	396
Przykład wdrożenia WLAN w placówce produkcyjnej	399
Przykłady wdrożeń WLAN w małych i średnich firmach oraz SOHO	402
Przykład wdrożenia WLAN w firmie średniej wielkości	402

Przykład wdrożenia WLAN w małym biurze.....	402
Przykład wdrożenia WLAN w biurze typu SOHO.....	403
Przykłady wdrożenia punktów aktywnych (publiczna WLAN).....	404
Przykład wdrożenia punktu aktywnego WLAN w kawiarni	404
Przykład wdrożenia punktu aktywnego WLAN w porcie lotniczym	407
Podsumowanie	408
Dodatek A. Zasoby i źródła informacji.....	411
Skorowidz	415