

# Obsah

Bezpečnost bezdrátové komunikace	9
Téma číslo 1: bezpečnost	10

## KAPITOLA 1

### **Základy bezpečnosti komunikačních sítí** **13**

Bezpečnost sítě	14
Bezpečnostní politika	15
Šifrování	15
Soukromý klíč	15
Veřejný klíč	17
Digitální podpisy a certifikáty	18
Autentizace	21
RADIUS: autentizace, autorizace a účtování	21
DIAMETER	23
Bezpečnostní architektura IP: IPSec	23
SSL	24
SSL versus IPSec	25
Virtuální privátní síť	25
Tunely	27
Protokol PPP a autentizace	28
L2TP a GRE	29
IPSec VPN versus SSL VPN	30
Útoky na bezpečnost sítě	31
Doporučené zdroje	32
Normy a specifikace internetové komunity	32
Organizace	33
Webové odkazy	34
Knihy	34

## KAPITOLA 2

### **Bezpečnost bezdrátové komunikace** **35**

<b>Bezpečnost bezdrátové komunikace</b>	<b>36</b>
Klasifikace bezdrátových sítí	36
Dosah	36
Podpora mobility uživatelů	37
Typy signálu	37

Optické bezdrátové sítě	38
Infračervené lokální sítě	39
Rádiové sítě	40
Výkon rádiových systémů	40
Antény	40
Kabely a konektory	41
Ztráty signálu	41
Kmitočtové pásmo	42
Porovnání bezdrátových sítí a technologií	42
Bezpečnost rádiových sítí	43
Specifika WLAN	45
Vyšší protokoly	45
Testování průniku do sítě	46
Bezpečnostní politika pro bezdrátové sítě	48
Vzdálený přístup	49
Douška na závěr	50
Doporučené zdroje	51
Normy	51
Organizace	51
Webové odkazy	51
Knihy	51

## KAPITOLA 3

# **Bezpečnost WLAN**

# **53**

Podniková versus domácí WLAN	55
WLAN ve zkratce	55
Přidružení k WLAN	57
Typy WLAN	58
Fyzická vrstva	59
MAC: protokol přístupu k médiu	59
Rámec 802.11	61
Další specifikace 802.11	62
Bezpečnost WLAN	63
Warchalking	65
SSID	66
SSID a VLAN	67
WEP	67
WEP: autentizace	68
WEP: šifrování	70
Stupně nastavení WEP	71
WEP: zabezpečení integrity dat	72
Slabiny WEP	73

Útoky na WEP	75
Filtrace MAC adres	77
IEEE 802.1x: řízení přístupu	77
RADIUS a jeho slabiny	79
EAP jako rámec pro autentizaci	81
Postup práce podle 802.1x	82
Metody autentizace EAP	84
Ochrana přenášených dat	91
WPA: dočasné řešení	92
WPA: autentizace	93
TKIP: dynamické generování klíčů	94
MIC: integrita dat	97
802.11i: komplexní zabezpečení	98
802.11i: autentizace	99
802.11i: hierarchie klíčů	99
802.11i: CCMP a AES	100
Key-caching a pre-authentication	101
Útoky na WLAN s 802.11i	101
Testování produktů podle 802.11i	101
Porovnání WEP, WPA a WPA2	102
Ad hoc sítě a jejich bezpečnost	104
Útoky na WLAN a podniková politika	104
Falešná zařízení	105
Útok typu man-in-the-middle	106
Útok s cílem odmítnutí služby: DoS	107
Ochrana: monitorování WLAN	108
Bezpečnostní audit WLAN	110
Bezpečné WLAN existují	112
Doporučené zdroje	113
Normy	113
Specifikace internetové komunity (RFC)	113
Internet-Drafts (I-D)	113
Organizace	114
Webové odkazy	114
Knihy	115

## KAPITOLA 4

# Bezpečnost v mobilních sítích

# 117

Generace mobilních sítí	118
3G	119
Bezpečnost v GSM/GPRS	121
Autentizace	122

Utajení dat	123
Bezpečnost UMTS	123
Bezpečnostní architektura UMTS	124
Bezpečnost 3GPP	124
Autentizace	125
Šifrování	127
Integrita dat	127
Bezpečnost signalizace sítě	127
Bezpečnost aplikací	127
Bezpečnostní slabiny 3G	128
Mobilní kancelář	128
Bezpečné mobilní sítě	129
Doporučené zdroje	130
Normy	130
Organizace	130
Knihy	130

## KAPITOLA 5

# **Bezpečnost hot spots a roamingu** **131**

Přístup pomocí veřejných WLAN	133
Bezpečnost vzdáleného přístupu	134
AAA v hot spots	134
Autentizace podle 802.1x/EAP	135
Autentizace přes web	136
Utajení dat	136
Mobilita a roaming	138
Roaming mezi WLAN	138
Roaming mezi přístupovými body	139
Rychlý a bezpečný roaming pro VoWLAN	140
Roaming mezi WLAN a GPRS/GSM	141
Jednotný rámec AAA	143
SIM karty pro WLAN	143
EAP-SIM pro GSM/GPRS	144
EAP-AKA pro UMTS	144
Spolupráce a normalizace karet	145
Roaming budoucnosti	145
Doporučené zdroje	146
Normy a specifikace	146
Internet-Drafts (I-D)	147
Organizace	147
Webové odkazy	147

## KAPITOLA 6

**Bezpečnost bezdrátového přístupu  
k Internetu 149**

Podnikové versus domácí síť	150
Vzdálený přístup a VPN	150
Porovnání 802.1x a VPN	151
Přístup prostřednictvím WLAN	152
Pevný bezdrátový přístup	152
802.16: WiMAX	152
Bezpečnost WiMAX	154
Mobilita do bezdrátové přístupové sítě	156
Bezpečný bezdrátový přístup	157
Doporučené zdroje	158
Normy	158
Organizace	158
Knihy	158

## KAPITOLA 7

**Bezpečnost malých sítí: Bluetooth a spol. 159**

Bluetooth	160
Bezpečnostní služby Bluetooth	162
Autentizace a šifrování Bluetooth	164
Bezpečnostní postup	165
Útoky na Bluetooth	166
Podniková bezpečnostní politika	167
Další malé bezdrátové sítě	168
Rychlé malé sítě	168
Pomalé senzorové sítě	168
Doporučené zdroje	169
Normy IEEE	169
Organizace	169
Webové odkazy	170
Knihy	170

## PŘÍLOHA A

**Zkratky 171****Rejstřík 175**