

---

# Obsah

<b>Předmluva</b>	<b>11</b>
------------------	-----------

<b>Úvod</b>	<b>13</b>
-------------	-----------

Proč jsem tuto knihu napsal	13
-----------------------------	----

Organizace	14
------------	----

kapitola 1

<b>Potřeba zabezpečení bezdrátových sítí</b>	<b>17</b>
--	-----------

Úvod	17
------	----

Bezpečnost ve vrstvách	18
------------------------	----

Na velikosti záleží – co chráníte?	18
------------------------------------	----

Hledání černých přístupových bodů	19
-----------------------------------	----

Bezdrátové sítě v kostce	20
--------------------------	----

Vysílání SSID	20
---------------	----

Filtrace MAC adres	22
--------------------	----

Protokol WEP (Wired Equivalent Privacy)	23
---	----

Autentizace sdíleným klíčem	24
-----------------------------	----

Protokol WPA (Wi-Fi Protected Access)	24
---------------------------------------	----

Pozor – stěny mají uši	24
------------------------	----

Dlouhé uši	25
------------	----

Omezení úniku rádiového signálu	25
---------------------------------	----

Shrnutí	26
---------	----

kapitola 2

<b>Úvod do bezdrátových sítí</b>	<b>27</b>
----------------------------------	-----------

Úvod	27
------	----

Doby před 802.11	27
------------------	----

802.11 (1997)	28
---------------	----

Rozprostřené spektrum	28
-----------------------	----

FHSS	29
------	----

DSSS	30
------	----

802.11b	32
---------	----

<b>Vzájemná kompatibilita</b>	<b>33</b>
<b>Kritické množství</b>	<b>34</b>
<b>802.11a</b>	<b>34</b>
<b>802.11g</b>	<b>36</b>
<b>Další pracovní skupiny</b>	<b>37</b>
<b>Specifikace 802.11</b>	<b>37</b>
<b>Příběh o dvou topologiích</b>	<b>37</b>
<b>IBSS, též režim ad-hoc</b>	<b>38</b>
<b>BSS/ESS, též režim infrastruktury</b>	<b>39</b>
<b>CSMA/CA</b>	<b>40</b>
<b>RTS/CTS</b>	<b>41</b>
<b>Fragmentace</b>	<b>42</b>
<b>Shrnutí</b>	<b>43</b>

## kapitola 3

**Zranitelnost protokolu WEP 45**

<b>Úvod</b>	<b>45</b>
<b>WEP v kostce</b>	<b>45</b>
<b>Dešifrování zprávy</b>	<b>46</b>
<b>Odkud se bere inicializační vektor?</b>	<b>47</b>
<b>Vysvětlení operace XOR</b>	<b>47</b>
<b>Problémy se správou klíče</b>	<b>48</b>
<b>Proudová šifra RC4</b>	<b>48</b>
<b>Kolize inicializačního vektoru</b>	<b>49</b>
<b>Injekce zprávy</b>	<b>50</b>
<b>Podvržená autentizace</b>	<b>50</b>
<b>Útoky hrubou silou</b>	<b>51</b>
<b>Rozluštění WEPového klíče</b>	<b>52</b>
<b>Útok hrubou silou versus útok FMS</b>	<b>52</b>
<b>Efektivní útok FMS</b>	<b>53</b>
<b>Poznámka k zařízením Orinoco</b>	<b>53</b>
<b>A co teď?</b>	<b>55</b>
<b>Shrnutí</b>	<b>55</b>

## kapitola 4

**War driving: nástroje a techniky 57**

<b>Úvod</b>	<b>57</b>
<b>Co to je „war driving“?</b>	<b>57</b>
<b>Jak to funguje</b>	<b>58</b>
<b>Hledání AP</b>	<b>59</b>
<b>Potřebné zařízení</b>	<b>60</b>

Volba hardwaru	62
Volba softwaru	64
<b>Bezdrátový odposlech</b>	<b>66</b>
<b>Co s tím vším?</b>	<b>69</b>
<b>Etická poznámka</b>	<b>69</b>
<b>War chalking</b>	<b>69</b>
<b>Shrnutí</b>	<b>70</b>

## kapitola 5

**802.11i, WPA, TKIP a AES 71**

Úvod	71
WPA jako záchrana	72
TKIP	73
TKIP podrobněji	73
Mixování paketového klíče	73
Michael – funkce kontroly integrity	75
Větší prostor inicializačního vektoru	75
WPA pro domácí použití	75
Budoucnost WPA	75
802.11i a AES	76
Nová šifra, AES-CCMP	76
Nový MIC	76
Nový šifrovací mechanismus	77
Shrnutí	77

## kapitola 6

**802.1x 79**

Úvod	79
Odkud se 802.1x vzal?	79
Přichází EAP	79
Základní 802.1x	80
Vinen, dokud se neprokáže nevina	81
Autentizační konverzace protokolu 802.1x	81
802.1x a řešení bezpečnostních problémů	82
Tím to ale nekončí!	83
Autentizační metody protokolu EAP	83
MD5	84
LEAP	84
TLS	85
TTLS	85
PEAP	86
Konkurenční standardy	86
Shrnutí	87

## kapitola 7

<b>Propojení bezdrátové a metalické sítě</b>	<b>89</b>
Úvod	89
Ocenění aktiv	89
Přístup ve vrstvách	90
Více SSID	90
802.1x versus VPN	90
Ukázkové projekty	91
Shrnutí	92

## kapitola 8

<b>Implementace VPN v bezdrátovém prostředí</b>	<b>93</b>
Úvod	93
PPTP versus L2TP/IPSec	94
PPTP: Point-to-Point Tunneling Protocol	94
L2TP: Layer 2 Tunneling Protocol a IPsec	94
Volba autentizačního protokolu	95
Vytvoření serveru VPN	96
Nastavení serveru VPN	96
Ruční nastavení serveru	98
Nastavení statického směrování	99
Zvýšení počtu portů PPTP a L2TP	100
Nastavení filtrace provozu	101
Přiřazení telefonního čísla	103
Nastavení zásad vzdáleného přístupu	104
Nastavení klienta	107
Nevýhody VPN	108
Shrnutí	108

## kapitola 9

<b>Zabezpečení a správa domácího prostředí</b>	<b>109</b>
Úvod	109
Základní bezpečnostní opatření	109
Mimo bezpečnost: Správa sítě	110
Našlapaný AP?	110

<b>LEAF (Linux Embedded Appliance Firewall)</b>	<b>111</b>
První krok: Stažení souborů	111
Druhý krok: Nachystání hardwaru	112
Třetí krok: Odstranění a přidání balíčků a modulů	112
Čtvrtý krok: Nastavení síťových parametrů	114
Pátý krok: Nastavení firewallu	115
Skutečný příklad	116
A co teď?	118
<b>Podpora bezdrátových zařízení v Beringu</b>	<b>119</b>
Karty Orinoco	120
Karty Prism	121
Zábava s Beringem	121
<b>Sputnik</b>	<b>121</b>
<b>ReefEdge Dolphin</b>	<b>122</b>
<b>Shrnutí</b>	<b>124</b>

## kapitola 10

## **Zabezpečení produkčního prostředí**

**125**

Úvod	125
Připomenutí 802.1x	125
Nastavení autentizačního serveru	126
Nastavení certifikačního úřadu	131
Nastavení autentizátora	139
Nastavení žadatele	139
Vše je hotovo	143
Použití EAP-TLS na serveru Windows 2000	143
Shrnutí	144

## kapitola 11

## **Nastavení bezpečného veřejného přístupového bodu: stavíme přístupový bod na Linuxu**

**145**

Úvod	145
Ovladač HostAP Prism pro Linux	146
NoCat	146
Pebble	148
Jiné minidistribuce	149
Hardwarové možnosti	149

<b>LEAF</b>	<b>150</b>
Nezapomeňte na zálohu!	153
<b>Diagnostické tipy</b>	<b>154</b>
<b>Shrnutí</b>	<b>154</b>

dodatek A

## **Seznámení s rádiovými technologiemi** **155**

<b>Historie rádiových vln</b>	<b>155</b>
<b>Elektromagnetismus</b>	<b>155</b>
<b>Indukce</b>	<b>156</b>
<b>Vodivost</b>	<b>156</b>
<b>Rádiové vlny</b>	<b>157</b>
<b>Struktura vlny</b>	<b>157</b>
<b>Modulace</b>	<b>158</b>
Amplitudová modulace	159
Frekvenční modulace	159
Digitální modulace	160
FSK (Frequency-Shift Keying)	160
<b>Útlum</b>	<b>160</b>
<b>Antény</b>	<b>161</b>
<b>Jak antény fungují</b>	<b>162</b>
<b>Různé druhy antén</b>	<b>162</b>
<b>Typy antén</b>	<b>163</b>
Isotropní anténa	163
<b>Všesměrové antény</b>	<b>164</b>
Patch antény, panelové a sektorové antény	164
Parabolické síťové antény	165
Yagi antény	166
Vivato	167
<b>Shrnutí</b>	<b>167</b>

dodatek B

## **Typy rámců protokolu 802.11** **169**

<b>Administrativní rámce</b>	<b>169</b>
<b>Řídící rámce</b>	<b>170</b>
<b>Datové rámce</b>	<b>170</b>

## **Rejstřík** **171**