



Poglavlje 1: Pretnje, napadi, sigurnost i metode zaštite	1
1.1 Napadi i pretnje	2
1.2 Šta je sigurnost?	9
1.3 Klasifikovanje informacija	17
1.4 Metode zaštite	19
Poglavlje 2: Sigurnosne arhitekture i modeli	25
2.1 Osnove sigurnosnih arhitektura	26
2.2 Pojam i problem bezbednosti i modeli sigurnosti	35
Poglavlje 3: Kriptografija	43
3.1 Matematičke osnove (neophodne za izučavanje kriptografije)	44
3.2 Osnovni kriptografski pojmovi i klasična kriptografija	55
3.3 Simetrični blokovski algoritmi	67
3.4 Pseudoslučajne sekvence i protočno šifrovanje	97
3.5 Heš funkcije	106
3.6 Kriptografija s javnim ključevima	115
3.7 Sertifikati i infrastruktura javnih ključeva	124
3.8 Kriptografski softver	132
3.9 Vežbe za programere	164
Poglavlje 4: Sigurnosni protokoli	173
4.1 Šta su kriptografski protokoli i čemu služe?	174
4.2 Protokol Secure Sockets Layer (SSL)	176
4.3 IPSec	186
4.4 Protokoli za proveru identiteta	198
Poglavlje 5: Mrežne barijere	209
5.1 Osnovni pojmovi o računarskim mrežama	210
5.2 Šta je mrežna barijera?	214
5.3 iptables	226
5.4 Skeniranje portova – provera konfiguracije mrežne barijere	237

5.5 Squid proksi server	240
5.6 Kućna rešenja – mrežne barijere za Windows XP	241
5.7 Filtriranje paketa pomoću Cisco rutera	247
5.8 Šifrovali ste podatke i postavili mrežnu barijeru. Šta dalje?	255
Poglavlje 6: Sistemi za otkrivanje i sprečavanje upada	257
6.1 Sistemi za otkrivanje upada (IDS)	258
6.2 Teorija sistema za otkrivanje upada	277
6.3 Sistemi za sprečavanje upada (IPS)	283
6.4 Primena sistema s veštačkom inteligencijom	288
Poglavlje 7: Zlonamerni programi	295
7.1 Vrste zlonamernih programa.	296
7.2 Zaštita od zlonamernih programa.	316
7.3 Rootkit	322
Poglavlje 8: Elektronsko poslovanje i sigurnost na Internetu	333
8.1 Infrastruktura zaštite u elektronskoj trgovini	334
8.2 Neželjena elektronska pošta, pecanje i farming	348
8.3 Sigurnost VoIP mreža	357
8.4 Sigurnost P2P mreža	364
Poglavlje 9: Sigurnost bežičnih i mobilnih mreža	371
9.1 Uvod u bežične mreže	372
9.2 WEP	379
9.3 802.1x, EAP, WPA, 802.11i i drugi standardi.	389
9.4 Alati za napadanje bežičnih mreža i dodatne reference	399
9.5 Sigurnost GSM mreža	401
9.6 Sigurnost Bluetooth tehnologije	415
Poglavlje 10: Sigurnost i zaštita operativnih sistema.	427
10.1 Opšti pregled zaštite i sigurnosnih mehanizama.	428
10.2 Sigurnost i zaštita operativnog sistema Linux.	437
10.3 Sigurnost i zaštita operativnih sistema Windows 2000/XP/2003	463
Poglavlje 11: Sigurnost baza podataka	479
11.1 Kontrola pristupa	480
11.2 Ostali aspekti zaštite	489
11.3 Napad SQL injection.	491

Poglavlje 12: Sigurnosni aspekti programiranja	503
12.1 Uvodne napomene	504
12.2 C/C++ i problem prekoračenja bafera	505
12.3 Sigurnosni aspekti programiranja na jeziku Java	520
12.4 .NET tehnologija i Security Development Lifecycle	538
12.5 Zaštita softvera	542
Poglavlje 13: Nadzor računarskih mreža	549
13.1 Uvodne napomene	550
13.2 Simple Network Management Protocol (SNMP)	551
13.3 Alati za nadzor mreža	565
Poglavlje 14: Organizacione, fizičke i pravne metode zaštite, društveni aspekti	573
14.1 Organizacione metode zaštite	574
14.2 Fizičke metode zaštite	578
14.3 Pravni aspekti sigurnosti	583
14.4 Društveni aspekti sigurnosti	592
Poglavlje 15: Planiranje održanja kontinuiteta posla i oporavka od nesreća.	599
15.1 Planiranje održanja kontinuiteta posla	600
15.2 Planiranje oporavka od nesreće.	608
15.3 Arhiviranje i izrada rezervnih kopija podataka	616
15.4 Forenzička analiza.	620
Poglavlje 16: Etičko hakerisanje i ispitivanje mogućnosti proboja. . .	627
16.1 Etičko hakerisanje	628
16.2 Ispitivanje mogućnosti proboja.	638
Dodatak A: Sigurnosni standardi i programi sertifikacije	653
A.1 Sigurnosni standardi.	654
A.2 Programi sertifikacije	661
Dodatak B: Besplatni alati, alati otvorenog koda i razni resursi koji se tiču sigurnosti.	665
B.1 Besplatan softver i softver otvorenog koda.	666
B.2 Razni resursi, knjige i Web stranice	680

Dodatak C: Kriptografske tablice	683
Dodatak D: Izvorni kôd	691
D.1 Pronalaženje ključa Hilove šifre na osnovu otvorenog teksta i šifrata.	692
D.2 Kriptoanaliza Vigenèreove šifre	694
D.3 Kriptoanaliza algoritma RSA	696
D.4 Napad na RSA kriptosistem u kome se ponavlja vrednost n	699
D.5 Određivanje diskretnog logaritma u konačnom polju	701
D.6 ElGamalov kriptosistem (primer 1)	703
D.7 ElGamalov kriptosistem (primer 2)	706
D.8 ElGamalov digitalni potpis.	713
D.9 Diffie-Hellmanov protokol za razmenu ključeva	715
D.10 RSA generator pseudoslučajnih sekvenci.	716
D.11 Generator pseudoslučajnih sekvenci (diskretan logaritamski problem)	717
D.12 BBS generator.	718
Dodatak E: Lozinke za pristup konfiguraciji BIOS-a	719
E.1 Lozinke za oporavak	720
Literatura	723
Spisak termina korišćenih u knjizi	731
Indeks	741