

SIGURNOST RAČUNARSKIH MREŽA (SRM)

Uvodno predavanje

Predmet: Sigurnost računarskih mreža (SRM)

2

- Visoka škola elektrotehnike i računarstva strukovnih studija
- VI semestar, treća godina
- Smerovi: **RT**, NRT, EPO
- Status predmeta: izborni
- Šifra predmeta : 130410
- ESPB bodovi: 6
 - ▣ European Credit Transfer and Accumulation System (ECTS)

Nastavnici

3

- Profesor:
 - ▣ mr **Dragan Pleskonjić**, dipl. ing.

- Saradnici:
 - ▣ **Marko Carić**, dipl. mat.
 - ▣ **Predrag Gavrilović**
 - ▣ Ranije: Nemanja Maček, sada na predmetu “Sigurnost informacionih sistema”

mr Dragan Pleskonjić, dipl. ing.

4

- **Profesor – VIŠER**
- **CEO** (Chief Executive Officer) & **Security Architect** at GTECH Belgrade Branch, previously **BEG Finsoft** (branch of Finsoft Ltd, UK London based company, acquired by GTECH)
- Member of **IEEE Computer Society**, **ACM** and **ACM SIGSAC** (Special Interest Group on Security, Audit and Control)
- Reviewer for scientific and technical journals (Elsevier Computers and Security, ComSIS etc.)
- Objavio više knjiga, stručnih i naučnih radova, projekata, softverskih paketa, recenzija, patentnih aplikacija itd.
- Inicirao i vodio razvoj brojnih softverskih projekata i projekata iz oblasti sigurnosti za USA, UK, EU kompanije.

Internet lokacije

5

- www.conwex.info/draganp/
- www.conwex.info/Dragan_Pleskonjic.html
- www.viser.edu.rs/profesori.php?id=79
- Dragan on Security (blog) www.conwex.info/blog/

- Finsoft Ltd: www.finsoft.com
- GTECH: www.gtech.com
- Lottomatica Group www.lottomaticagroup.com

Web strana predmeta SRM

6

- Zvanična Web strana:
www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige: www.conwex.info/draganp/books.html

SRM - Cilj predmeta

7

- **Cilj** predmeta je da se studenti upoznaju sa izvorima ugrožavanja sigurnosti računarskih sistema i mreža, sigurnosnim mehanizmima, metodama, tehnikama i procedurama zaštite u računarskim sistemima, mrežama i informacionim sistemima. Ovo se posebno odnosi na Internet i intranet mrežno okruženje i njegove specifičnosti.

Poželjni preduslovi

8

- Operativni sistemi
- Računarske mreže
- Protokoli u računarskim mrežama
- Programiranje
- Baze podataka
- Matematika
- Sigurnost informacionih sistema

- Napomena: Ovo nisu eliminatorni uslovi.*

Metod nastave

9

- Predavanja

- Vežbe
 - ▣ Auditorne
 - ▣ Laboratorijske

Predavanja

10

- **0. Uvod, upoznavanje, anketa**

- **1. Pretnje, napadi, sigurnost i metode zaštite**
 - Napadi i pretnje
 - Šta je sigurnost?
 - Klasifikacija informacija
 - Metode zaštite

- **2. Sigurnosne arhitekture i modeli**
 - Osnove sigurnosnih arhitektura
 - Pojam i problem bezbednosti i modeli sigurnosti

Predavanja - nastavak

11

□ 3. Kriptografija

- Matematičke osnove (neophodne za izučavanje kriptografije)
- Osnovni kriptografski pojmovi i klasična kriptografija
- Simetrični blokovski algoritmi
- Pseudoslučajne sekvence i protočno šifrovanje
- Heš funkcije
- Kriptografija s javnim ključevima
- Sertifikati i infrastruktura javnih ključeva
- Kriptografski softver

Predavanja - nastavak

12

□ 4. Sigurnosni protokoli

- Šta su kriptografski protokoli i čemu služe?
- Protokol Secure Sockets Layer (SSL)
- IPSec
- Protokoli za proveru identiteta

□ 5. Mrežne barijere

- Osnovni pojmovi o računarskim mrežama
- Šta je mrežna barijera?
- iptables
- Skeniranje portova - provera konfiguracije mrežne barijere
- Squid proksi server
- Kućna rešenja – mrežne barijere za Windows XP / Vista / W7
- Filtriranje paketa pomoću Cisco rutera

Predavanja - nastavak

13

- **6. Sistemi za otkrivanje i sprečavanje upada**
 - Sistemi za otkrivanje upada (IDS)
 - Teorija sistema za otkrivanje upada
 - Sistemi za sprečavanje upada (IPS)
 - Primena sistema sa veštačkom inteligencijom

- **7. Zlonamerni programi**
 - Vrste zlonamernih programa
 - Zaštita od zlonamernih programa
 - Rootkit

Predavanja - nastavak

14

- **8. Elektronsko poslovanje i sigurnost na Internetu**
 - Infrastruktura zaštite u elektronskoj trgovini
 - Neželjena elektronska pošta i pecanje
 - Sigurnost VoIP mreža
 - Sigurnost P2P mreža

- **9. Sigurnost bežičnih i mobilnih mreža**
 - Uvod u bežične mreže
 - WEP
 - 802.1x, EAP, WPA, 802.11i i drugi standardi
 - Alati za napadanje bežičnih mreža i dodatne reference
 - Sigurnost GSM mreža
 - Bluetooth sigurnost

Predavanja - nastavak

15

- **10. Sigurnost i zaštita operativnih sistema**
 - Opšti pregled zaštite i sigurnosnih mehanizama
 - Sigurnost i zaštita operativnog sistema Linux
 - Sigurnost i zaštita operativnih sistema Windows XP / Vista / W7

- **11. Sigurnost baza podataka**
 - Kontrola pristupa
 - Ostali aspekti zaštite
 - Napad SQL injection

Predavanja - nastavak

16

- **12. Sigurnosni aspekti programiranja**
 - Uvodne napomene
 - C/C++ i problem prekoračenja bafera
 - Sigurnosni aspekti programiranja na jeziku Java
 - .NET platforma i Security Development Lifecycle
 - Zaštita softvera

Predavanja - nastavak

17

- **13. Nadzor računarskih mreža**
 - Uvodne napomene
 - Simple Network Management Protocol (SNMP)
 - Alati za nadzor mreža

- **14. Organizacione, fizičke i pravne metode zaštite, društveni aspekti**
 - Organizacione metode zaštite
 - Fizičke metode zaštite
 - Pravni aspekti sigurnosti
 - Društveni aspekti sigurnosti

Predavanja - nastavak

18

- **15. Planiranje održanja kontinuiteta posla i oporavka od nesreća**
 - Planiranje održanja kontinuiteta posla
 - Planiranje oporavka od nesreće
 - Rezervne kopije podataka
 - Forenzička analiza

- **16. Etičko hakerisanje i ispitivanje mogućnosti proboja**
 - Etičko hakerisanje
 - Ispitivanje mogućnosti proboja

Vežbe

19

1. Kriptoanaliza
 2. Infrastruktura javnih ključeva (PKI)
 3. SSL sigurnosni protokol
 4. Sistemi za otkrivanje upada (IDS)
 5. Mrežne barijere
 6. Zlonamerni softver
 7. Sigurnost bežičnih mreža
 8. *SQL injection* i web sigurnost
 9. Prekoračenje bafera
 10. Sigurnost operativnih sistema
 11. Etičko hakerisanje i testiranje mogućnosti proboja
- Napomena:* Više o vežbama na prvom času vežbi. Moguće su promene redosleda i sadržaja vežbi.

Pravila ponašanja na predavanjima

20

- ❑ Izbegavajte ulaženje posle početka predavanja ili izlaženje u toku predavanja (dozvoljeno samo u opravdanim slučajevima).
- ❑ Upotreba mobilnih telefona i drugih elektronskih uređaja za vreme predavanja je zabranjena (osim laptopova za zabeleške).
- ❑ Očekuje se tišina i pažnja.
- ❑ Očekuje se redovno prisustvo predavanjima, koje je u interesu studenata.
- ❑ Pitanja možete postavljati u toku predavanja ili na kraju predavanja u vreme ostavljeno za pitanja.

Provera znanja i ocenjivanje

21

- Aktivnost i rezultati na vežbama se prate i ocenjuju od strane saradnika koji drže vežbe. Da bi se pristupilo pismenom delu ispita, neophodno je odbraniti vežbe. Rezultat se izražava kao OV.
- Ispit se polaže pismeno i usmeno.
- Pismeni ispit se zadaje u vidu testa sa pitanjima i zadacima. Pismeni ispit je eliminatoran (sa pragom 50%) i preduslov je za izlazak na usmeni ispit. Rezultat se izražava kao OP.
- Svi koji polože pismeni, mogu da pristupe usmenom delu ispita u pravilu nedelju dana nakon pismenog ispita.
- Položeni pismeni deo ispita se priznaje do kraja predavanja i vežbi za sledeću generaciju studenata (u pravilu do kraja maja meseca iduće godine). Nakon toga se pismeni ispit mora ponovo polagati.

Seminarski radovi

22

- U toku semestra ili kasnije, studenti mogu da urade seminarski rad.
- Seminarski rad mogu zadati profesor i asistenti. Takođe i studenti mogu sami da predlože teme seminarskih radova. Profesor odobrava temu seminarskog rada.
- **Uspešno urađen i odbranjen** seminarski rad može pomoći da se konačna ocena poveća.
- Teme: www.conwex.info/draganp/SRM_seminarski_radovi.html
- Studenti seminarski rad predaju u papirnoj i elektronskoj formi (kao i praktičan rad, ukoliko postoji), i Open Office/MS Office/PDF dokumenat, obima 15-25 stranica (nije ograničenje)
- Studenti brane seminarski rad na predavanjima ili vežbama; nakon odbrane, odrađen seminarski rad se evidentira u indeksu studenta.
- Ukoliko se seminarski rad ne završi u toku trajanja semestra, onda se njegova odbrana vrši u terminu ispitnog roka.

Kako se formira ocena?

23

- Ocena se formira na sledeći način:
 - $O = 0.3 OV + 0.3 OP + 0.4 OU$
 - ▣ Svaki deo ispita mora biti urađen sa min 50% za prolaz
 - $OV \in [6..10]$ ocena aktivnosti i rezultata na vežbama
 - $OP \in [6..10]$ ocena na pismenom ispitu
 - $OU \in [6..10]$ ocena na usmenom ispitu
- Napomena: Svaki deo ispita ima prag prolaznosti od 50%.
- Seminarski rad može pomoći da se ocena poveća do faktora 0.3.
- Posedovanje nekog od priznatih sertifikata iz ove oblasti, kao što su CISSP, CEH, CCSP, CISA i slično, može pomoći da se ocena poveća do faktora 0.4.

Literatura (resursi *on-line*):

24

- Resursi za preuzimanje (*download*):
www.conwex.info/draganp/teaching.html
- Informacije o knjigama:
www.conwex.info/draganp/books.html
- **Napomena:** *On-line* resursi će biti ažurirani tokom godine

Literatura

25

- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **“Sigurnost računarskih sistema i mreža”**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik

- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2
- www.comsis.org/ComSIS/Vol4No1/BookPreview/Book.htm

Sigurnost računarskih sistema i mreža

26



Copyright © 2005-2010 Dragan Pleskonjic. All Rights Reserved.

Sadržaj knjige

27

- Predgovor
- 1. Pretnje, napadi, sigurnost i metode zaštite
- 2. Sigurnosne arhitekture i modeli
- 3. Kriptografija
- 4. Sigurnosni protokoli
- 5. Mrežne barijere
- 6. Sistemi za otkrivanje i sprečavanje upada
- 7. Zlonamerni programi
- 8. Elektronsko poslovanje i sigurnost na Internetu

Sadržaj knjige... nastavak

28

- 9. Sigurnost bežičnih i mobilnih mreža
- 10. Sigurnost i zaštita operativnih sistema
- 11. Sigurnost baza podataka
- 12. Sigurnosni aspekti programiranja
- 13. Nadzor računarskih mreža
- 14. Organizacione, fizičke i pravne metode zaštite, društveni aspekti
- 15: Planiranje održanja kontinuiteta posla i oporavka od nesreća
- 16: Etičko hakerisanje i ispitivanje mogućnosti proboja

Sadržaj knjige... nastavak

29

- A: Sigurnosni standardi i programi sertifikacije
- B: Besplatni i open-source alati i razni resursi koji se tiču sigurnosti
- C: Kriptografske tablice
- D: Izvorni kod
- E: Lozinke za pristup konfiguraciji BIOS-a
- Literatura
- Rečnik termina i skraćenica
- Indeks termina

Literatura - nastavak

30

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **“Sigurnost računarskih mreža”**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **“Sigurnost računarskih mreža - priručnik za laboratorijske vežbe”**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **“Sigurnost računarskih mreža - zbirka rešenih zadataka”**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html



Dodatna literatura

31

- **Cryptography and Network Security**
4/E (4th Edition)
William Stallings
Prentice Hall, 2006

- **Applied Cryptography**
Second Edition
Bruce Schneier
John Wiley & Sons, 1996

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
Ronald L. Krutz, Russell Dean Vines
John Wiley & Sons, 2001

- Druge knjige i razni *online* resursi

- **Napomena:** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

32

?

Anketa i razgovor

33

- Anketa sa osnovnim pitanjima koja služi da se proceni predznanje i prethodno obrazovanje slušalaca kursa. Prvenstveno se odnosi na predmete koji su značajni za praćenje nastave iz ovog predmeta
- Pojedinačno predstavljanje studenata