Sigurnost računalnih sustava

Computer Systems Security

Uvod i pravila

Marin Golub i Stjepan Picek

Zašto "Sigurnost računalnih sustava"?

- Računalna sigurnost (*Computer Security,* CS)
- Sigurnost računalnih sustava
  (*Computer System Security,* CSS)
- Sigurnost informacijskih sustava
  (*Information System Security*, ISS)
- Informacijska sigurnost (*Information Security*, IS)
- Kibernetička sigurnost (*Cybersecurity*)

Računalna sigurnost

- nije cilj, već oruđe za postizanje novog cilja: informacijske sigurnosti

  [Cheswick, Bellovin, Rubin, "Firewalls and Internet Security", 2002.]

Sigurnost računalnih sustava

ili kraće računalna sigurnost

- specifičan oblik sigurnosti gdje se štiti:
  - računalni sustav od nepovlasnog korištenja i osigurava se njegova raspoloživost,
  - operacijski sustav, programi i usluge (servisi) te
  - podaci pohranjeni u računalnom sustavu od nepovlasnog čitanja, mijenjanja, otkrivanja/objavljivanja ili brisanja.

Sadržaj

1. Uvod
2. Upravljanje računalnom sigurnošću
3. Kriptografske tehničke sigurnosne mjere
4. Implementacijski napadi
5. Istraživačke smjernice

Predznanje

11. poglavlje iz udžbenika L. Budin, M. Golub, D. Jakobović, L. Jelenković, Operacijski sustavi, Element, Zagreb, 2010.

- Osnove kriptografije
  - DES, 3DES, XDES, IDEA, AES
  - RSA, Diffie-Hellmanov postupak razmjene ključa
  - MD5, SHA-0, SHA-1, SHA-2
- Načini kriptiranja
- Digitalni potpis, digitalna omotnica i digitalni pečat
- Protokoli razmjene ključeva i postupci autentifikacije u (a)simetričnim sustavima
- SSL, TLS, Kerberos
- PKI
  - certifikati
  - postupak autentifikacije uz pomoć certifikata
  - X.509 autentifikacijski protokoli

Literatura 1/2

[1] B. Schneier, *Applied Cryptography*, J. Wiley & Sons, ISBN: 978-0471117094, 1996.

[2] Ross J. Anderson, *Security Engineering*, Wiley & Sons, 2nd edition, ISBN: 978-0470068526, 2008., dostupno na Internet adresi: http://www.cl.cam.ac.uk/~rja14/book.html

[3] Christof Paar, Jan Pelzl, *Understanding Cryptography*, Springer-Verlag Berlin Heidelberg, 2009.

[4] Nigel P. Smart, *Cryptography Made Simple*, Springer International Publishing, 2016.

[5] *Sigurnost računalnih sustava*, zbirka studentskih radova, dostupno na Internet adresi: http://sigurnost.zemris.fer.hr

[6] Harold F. Tipton, Mickie Krause Nozaki, *Information Security Management Handbook*, CRC Press, ISBN: 9781439853450, 6. izdanje 2011.

Literatura 2/2

[7] Norma ISO/IEC 27000, pregled skupa normi 27000 i rječnik, slobodno dostupno

[8] Norma ISO/IEC 27001, preporuke za implementaciju sustava upravljanja (prije BS 7799-2:1999) i smjernice za upravljanje rizicima prilikom uspostave sustava upravljanja sigurnošću informacija (prije BS 7799-3:2005).

[9] Norma ISO/IEC 27002 (prije ISO/IEC 17799:2005, odnosno BS 7799-1:1995), popis sigurnosnih kontrola i postupci za upravljanje sigurnošću informacija.

[10] *Zakon o elektroničkom potpisu*, donešen 17. siječnja 2002., a trenutno je na snazi zadnja verzija od 8.8.2017.

[11] R. Shirey, "Internet Security Glossary, Version 2," RFC 4949 (Informational), Aug. 2007., dostupno na Internet adresi : http://www.ietf.org/rfc/rfc4949.txt

Kako položiti ispit?

Seminar

- Nije obvezan!
- Ukoliko se seminar objavi u zborniku nekog skupa, može se priznati kao ispit.

ili

Ispit

- pismeni i usmeni