Sigurnost u računarskim mrežama

Ukratko o predmetu

Studijski program: RT
Šifra predmeta: 131307
Status: izborni
ESPB: 6
Semestar: letnji
Predavanja: 3 časa nedeljno
Laboratorijske vežbe: 2 časa nedeljno

Predmetni nastavnik:
dr Nemanja Maček, dipl. inž.
Kabinet: 511
e-mail: nmacek@viser.edu.rs
Termin konultacija: v. sajt Škole

Predmetni saradnik:
spec. inž. Đorđe Radujko
Kabinet: 401
e-mail: djordjer@viser.edu.rs
Termin konultacija: v. sajt Škole

Šta ćemo raditi na ovom kursu?

Cilj ovog predmeta je:

- Da se upoznate sa osnovnim konceptima informacione sigurnosti i zaštite savremenih umreženih računarskih sistema.
- Da naučite da praktično primenjujete i administrirate zaštitne mehanizme.

Šta nećemo raditi na ovom kursu?

- Mrežne barijere za ~~21 dan~~.
- Kurs kriptoanalize ~~sa doktorskih studija~~ MIT-a.

Okvirni plan rada

1. Osnovni pojmovi: pretnje, napadi, ranjivosti, sigurnosni ciljevi i usluge
2. Pojam i problem bezbednosti i modeli sigurnosti
3. Kriptologija
4. Kriptografski protokoli
5. Kontrola pristupa u računarskim mrežama: mrežne barijere
6. Kontrola pristupa u računarskim mrežama: sistemi za detekciju upada (IDS)
7. IDS sistemi zasnovani na mašinskom učenju
8. Autentifikacija i autorizacija, biometrijski sistemi
9. Filtriranje neželjene elektronske pošte
10. Zlonamerni softver i metode zaštite od zlonamernog softvera
11. Obrada metapodataka i analiza društvenih mreža pomoću grafova
12. Zaštita baza podataka i Veb aplikacija
13. Zaštita operativnih sistema
14. Odabrani sigurnosni aspekti programiranja i testiranje softvera s osvrtom na sigurnost

Materijali za predavanja i vežbe

Predavanja.

- Materijali za predavanja (beleške) se po pravilu pripremaju unapred, tako da možete da ih preuzmete pre časa sa stranice predmeta na Veb sajtu Škole.
- Obaveštenja koja se tiču predavanja i kolokvijuma objavljuju se na stranici predmeta na Veb sajtu Škole.

Vežbe.

- Materijale za laboratorijske vežbe dodeljuje predmetni saradnik.
- Obaveštenja koja se tiču vežbi predmetni saradnik objavljuje putem Moodle platforme.

Dodatna literatura za predavanja

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.
2. A. Jevremović, M. Veinović, M. Šarac, G. Šimić (2014): Zaštita u računarskim mrežama. Univerzitet Singidunum, Beograd. *
3. M. Veinović, S. Adamović (2013): Kriptologija 1. Univerzitet Singidunum, Beograd. *
4. M. Milosavljević, S. Adamović (2014): Kriptologija 2. Univerzitet Singidunum, Beograd. *
5. M. Stamp (2006): *Information Security*. John Wiley and Sons.

* Može se besplatno preuzeti sa portala: www.singipedia.com

Način ocenjivanja

- **Prisustvo** na 80% laboratorijskih vežbi.
- **Odbrana vežbi** na kraju semestra.
  - Na odbrani vežbi možete ostvariti najviše 30 poena.
  - Vežbe su odbranjene ako na odbrani ostvarite 15 ili više poena.
- **Tri kolokvijuma** ili **ispit** (pismeno polaganje).
  - Kolokvijumi se polažu u terminima predavanja.
  - Na prvom i drugom kolokvijumu možete ostvariti najviše po 25 poena, dok na trećem kolokvijumu možete ostvariti najviše 20 poena.
- Ispit ste **položili** ako ste:
  - Odbranili vežbe i na kolokvijumima u zbiru ostvarili 35 ili više poena.
  - Odbranili vežbe i na ispitu ostvarili 35 ili više poena.

Način ocenjivanja

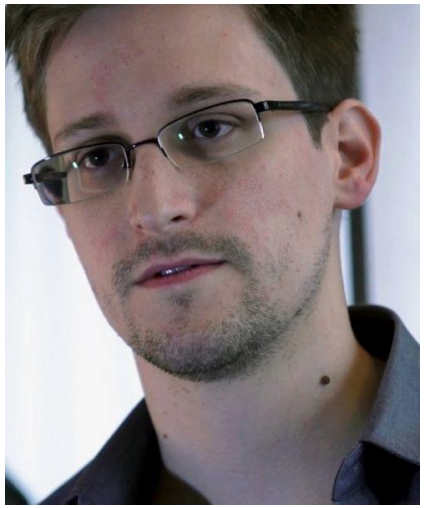
- **Formiranje ocene**:
- Poeni sa laboratorijskih vežbi se sabiraju sa poenima sa kolokvijuma ili ispita.
  - $[0, 50] \rightarrow 5$
  - $[51, 60] \rightarrow 6$
  - $[61, 70] \rightarrow 7$
  - $[71, 80] \rightarrow 8$
  - $[81, 90] \rightarrow 9$
  - $[91, 100] \rightarrow 10$

- Dodatna mogućnost za uvećanje broja poena (ne odnosi se na povećanje ocene sa 5 na 6) je izrada projektnog zadatak (praktično), na čemu u zavisnosti od složenosti možete ostvariti 10-15 poena.

Primeri narušavanja informacione sigurnosti

Primer 1.

- Edvard Snouden (Edward Snowden) nam je potvrdio ono što je trebalo da znamo (ili makar pretpostavljamo) i pre – koliko su naši privatni podaci izloženi, i kako se skupljaju i obrađuju.



* Izvor slike: Laura Poitras, Praxis Films

Primeri narušavanja informacione sigurnosti

Primer 2.

- Džulijan Asanž (Julian Assange) nam je pružio uvid u dokumenta koja su trebala da budu sakrivena od nas.

* Izvor slike: Peter Erichsen, New Media Days

Primeri narušavanja informacione sigurnosti

Primer 3.

- Džonu Brenanu, direktoru CIA, je 2015. hakovan nalog za privatnu e-poštu.
- Pritom, greška nije njegova (osim što je čuvao dokumenta osetljive sadržine na privatnom nalogu):
  - nije imao neadekvatnu lozinku,
  - nije neoprezno izložio kopiju lozinke,
  - nije poslao e-poštu pogrešnoj osobi.
- Šta se desilo?

Primeri narušavanja informacione sigurnosti

Primer 3.

- Napadač, navodno tinejdžer:
  - se u komunikaciji sa firmom Verizon predstavio kao zaposleni u firmi i tako dobio lične informacije o Brenanovom nalogu, broj njegove kreditne kartice i njegovu privatnu adresu e-pošte sa naloga firme America On-Line (AOL),
  - a zatim se u komunikaciji sa firmom AOL predstavio kao Brenan i ubedio ih da mu resetuju lozinku.
- Odgovornost za sigurnosne propuste leži na ove dve firme.

Primeri narušavanja informacione sigurnosti

Primer 4.

- Deo izjave visokog predstavnika kompanije Ford iz 2014. godine:
  - „Znamo svakog ko krši zakon, znamo kad to činite. Imamo GPS u vašim kolima, tako da znamo šta radite. Usput, ne dajemo ove podatke nikome.“

Primeri narušavanja informacione sigurnosti

Primer 5.

- Na naplatnoj rampi, softver za obradu slike automatski prepoznaje broj vaših registarskih tablica i štampa ih na karti.
- Pitanje:
  - Koliko dugo se čuvaju ovi podaci i ko može da ih koristi?

Primeri narušavanja informacione sigurnosti

Primer 6.

- Razmotrimo sledeću situaciju:
  - Niste platili „doplatnu kartu“ za parkiranje u „zoni“, i „Parking servis“ vam šalje opomenu pred utuženje.
- Pitanje:
  - Odakle „Parking servisu“ vaše ime i adresa?

Primeri narušavanja informacione sigurnosti

Primer 7.

- Korisnik koji je zaboravio lozinku zove MTS kol-centar.
- Radnik u kol-centru zahteva od korisnika da „izdiktira“ matični broj.
- Umesto da mu „resetuje“ lozinku, radnik mu saopštava lozinku preko telefona.
- Pitanja:
  - Da li radnik kol-centra ima pravo da traži informaciju poput JMBG?
  - Da li je neko drugi mogao da „izdiktira“ JMBG tog korisnika?
  - Ako se lozinke čuvaju u kriptološki zaštićenom formatu, kako je radnik kol-centra mogao da izdiktira lozinku korisniku?

Primeri narušavanja informacione sigurnosti

Primer 8.

- Deo transkripta iz reklame za „Pošte Srbije“”:
  - “Znamo vas od kad ste se rodili, kada su vam slali novac na more, i paket u vojsku ...
    Znamo kada ste se oženili, kada ste dobili na nagradnoj igri i kada ste dobili prvu penziju ...
    Znamo da ste stalno na Skajpu, da je ona u Americi, da volite Diskaveri, ... da je lakše platiti preko neta ...
    Znamo da je bolje s karticama ...
    Ko vas pozaje bolje od nas?
    Pošta Srbije.“

Izvor slike: youtube.com

Primeri narušavanja informacione bezbednosti

Razmislite o sledećem ...

- Ako direktoru CIA hakovan nalog za e-poštu, šta „obični“ ljudi mogu da očekuju?
- Koje podatke o vama skupljaju mobilni operateri, Internet provajderi i druge firme?
- Koliko dugo ih čuvaju? Zašto to rade?
- Da li to znači da vas „špijuniraju“?
- Da li smo kao društvo ostali imuni na uvide koje nam je pružio Edvard Snouden?
- Čija je odgovornost čuvanje bezbednosti vaših privatnih podataka?
- Da li je kriptografija rešenje?
- Iako ne radim ništa loše, da li bih ipak trebao da se brinem?

Hvala na pažnji

Pitanja su dobrodošla.