Sigurnost računala i podataka  
DRUGI kolokvij, 3/2/2012

Molimo budite što koncizniji u vašim odgovorima; koristite do *tri kratke* rečenice. Napominjemo da nije nužno rješiti sve zadatke za ostvarivanje maksimalne odnosno visoke ocjene.

## Uvod

1. Definiraj pojam *autentifikacije* (eng. *authentication*). (0.5 pt)
2. Opiši dva fundamentalno različita načina/koncepta koja se mogu koristiti za autentifikaciju korisnika. Budi kratak/kratka; jedna rečenica po konceptu je dovoljna. (0.5 pt)
3. Klasificiraj svaki od sljedećih scenarija kao primjer narušavanja *privatnosti* (eng. *confidentiality*), *integriteta* (eng. *integrity*), *dostupnosti* (eng., *avaliability*), ili kombinacije navedenog.
   1. Ivan prepiše Anin izvještaj.
   2. Markoonesposobi Perino računalo.
   3. Lucija promjeni iznos na Ivanovom čeku iz 100,00kn u 1.000,00 kn.
   4. Ivana lažira Lukin potpis na ugovoru.
   5. Pero preuzme Ivaninu IP adresu da ostvari pristup Ivaninom računalu.

(1 pt)

1. Je li zaštita *privatnosti* (eng. *confidentiality*) podataka osigurava zaštitu *integriteta* (eng. *integrity*) tih podataka? (0.5 pt)
2. Daj primjer situacije u kojoj narušavanje *privatnosti* (eng. *confidentiality*) vodi narušavanju *integriteta* (eng. *integrity*). (1 pt)

## Kriptografija

1. Navedi osnovnu razliku između simetričnih i asimetričnih kriptografskih sustava. (0.5 pt)
2. Obrazloži zašto dani simetrični kriptografski sustav koji koristi 67 bitni enkripcijski ključ nije siguran. Dvije rečenice bi trebale biti dovoljne. (0.5 pt)
3. Čemu služe ditigalni certifikati? Budi koncizan/koncizna u odgovoru. (0.5 pt)
4. **\***Ivana i Marko imaju *javne ključeve* (eng. *public keys*) koji su spremljeni u odgovarajućoj datoteci na serveru. Ivana i Marko koriste navedene javne i odgovarajuće *privatne ključeve* (eng. *private keys*) da bi razmjenjivale autentificirane i privatne poruke. Napadač Neno želi pročitati njihove poruke ali ne može probiti/pogoditi Ivanine i Markove privatne ključeve. Međutim, napadač Neno može upasti u server i modificirati datoteku u kojoj su pohranjeni Ivanini i Markovi javni ključevi.
   1. Kako Neno treba promjeniti navedenu datoteku da bi mogao čitati poruke (narušiti povjerljivost) između Marka i Ivane?
   2. Kako bi Ivana i Marko mogli detektirati ovaj Nenin pokušaj? (2 pt)

## Kontrola pristupa (eng. Access Control)

1. Koji problem rješava kontrola pristupa? (0.5 pt)
2. Navedi osnovu razliku između *diskrecijske kontrole pristupa* (eng. *discretionary access control*) i *obavezne kontrole prisutpa* (eng. *mandatory access control*). Budi koncizan/koncizna.

(0.5 pt)

1. U rečenici opiši ulogu *reference monitor-a* u sustavu kontrole pristupa. (0.5 pt)
2. Odgovori je li sljedeća izjava točna. *Matricama kontrole pristupa* (eng. *access control matrices*) možemo reprezentirati sve ono što možemo reprezentirati *listama kontrole pristupa* (eng. *access control lists - ACL*). Obrazloži odgovor u jednoj rečenici. (1 pt)
3. **\***Ivana može čitati i pisati u datoteku *x*, može čitati datoteku *y*, i može izvršavati datoteku *z*. Ante može čitati datoteku *x*, može čitati i pisati u datoteku *y* a ne može pristupati datoteci *z*.
   1. Napišite *access control liste* (ACLs) za ovaj scenarij. Nakon toga odgovorite koja lista (ACL) je povezana sa kojom datotekom?
   2. Napišite *capability liste* za ovaj scenarij. Nakon toga odgovorite s čime je povezana svaka od ovih lista?

(2 pt)

## Maliciozni softver (Malware)

1. Definiraj termin *računalni crv* (eng. *computer worm*) i navedi razliku u odnosu na *računalni virus* (eng. *computer virus*). (0.5 pt)
2. Opiši tipične operacije računalnog crva (eng. computer worm) kroz njegov cijeli životni ciklus.

(0.5 pt)

1. Opiši vrstu i značaj (visinu) štete koju može uzrokovati računalni crv i navedi tri kontrole za ograničavanje/ublažavanje iste. (1 pt)
2. Objasni kako računalni virus izbjegava situaciju u kojoj bi više puta inficirao isti sustav odnosno istu *.exe* datoteku. *Virus želi izbjeći ovu situaciju jer bi mogao upasti u beskonačnu petlju te se u konačnici ne proširiti na druge programe.* (0.5 pt)
3. **\***Promatrani računalni sustav implementira *Bell-LaPadula* model obavezne kontrole pristupa (eng. *mandatory access control*). Prisjetimo se, Bell-LaPadula model za zaštitu povjerljivosti je zasnovan (odnosno koristi) *read-down* i *write-up* principe. Odgovori, kako se računalni virus može prošititi ako
   1. se virus inicijalno nalazi u dijelu/odjeljku računalnog sustava koji nosi oznaku *low-level* (ostali odjeljci sustava dominiraju odjeljak u kojem se nalazi virus)?
   2. se virus inicijalno nalazi u dijelu/odjeljku računalnog sustava koji nosi oznaku *high-level* (u odjeljku koji dominira ostale odjeljke)?

(3 pt)