SIGURNOST RAČUNALNIH SUSTAVA, 2020/2021

ZADATCI ZA PRIPREMU ZA MEĐUISPIT
15.04.2021.

1. Definirajte osnovne pojmove.
    a) Kada neki od sigurnosnih zahtjeva više nije ispunjen kažemo da se desio _____.
    b) Koja su tri temeljna sigurnosna zahtjeva: _____.
    c) Sigurnosni zahtjev da podatak ne smije vidjeti neovlaštena osoba nazivamo _____.

2. Na traku za pričuvnu pohranu (engl. backup) pohranjeni su podaci o poslovanju tvrtke te potom tu traku kurir prenosi na rezervnu lokaciju kako bi podaci bili sačuvani u slučaju havarije na primarnoj lokaciji. Odgovorite na sljedeća pitanja:
    a) Navedite barem jednu ranjivost tijekom prijenosa _____
    b) Navedite barem jednu prijetnju traci tijekom prijenosa _____
    c) Navedite osnovnu zaštitu koju bi ste primijenili tijekom prijenosa trake, a koja bi spriječila najveći broj prijetnji: _____

3. Navedite motivaciju (ciljeve) za svaku od sljedećih grupa izvora prijetnji:
    a) Napredne ustrajne prijetnje: _____
    b) Kibernetički kriminal: _____
    c) Haktivisti: _____

4. Statička analiza je:
    a) Analiza izvornog koda s ciljem detekcije sigurnosnih propusta
    b) Analiza izvršnog koda s ciljem detekcije ponašanja programa tijekom izvršavanja
    c) Analiza izvršavanja programa kada na njega nisu dovedeni ulazni podaci
    d) Analiza izvornog koda s ciljem detekcije sintaktičkih grešaka

5. Napisali ste sljedeći kod u nekom programskom jeziku:

```
x = 3;
y = 'SRS';
z = x + y;
```

Ako se radi o strogo tipiziranom programskom jeziku koji vrši provjeru tijekom izvođenja, što će se ispisati?

a) Greška prilikom prevođenja
b) Greška tijekom izvođenja
c) Samo brojevna vrijednost obzirom da se koristi operacija zbrajanja

6. Napisali ste kod:

```
1: ispitProlaz = true;
2: try {
3:  points = provjeriBodove();
4: if (bodovi < 50){
5:    ispitProlaz = false;
6:  }
7: }
8: catch (Exception ex)
9: {
10:  //write error
11: }
```

Ako metoda provjeriBodove() može baciti grešku, što bi trebalo popraviti u kodu da bi ispravno radio i da zadovoljimo princip sigurnog ispadanja (Fail Securely):

a) Trebali bi dodati uvjet else{ ispitProlaz = true;} nakon linije 6
b) Trebali bi izraz na liniji 1 zamijeniti sa ispitProlaz = false;
c) Trebali bi zamijeniti izraz na liniji 1 sa ispitProlaz = false; i dodati uvjet else{ ispitProlaz = true;} nakon linije 6
d) Ne bi trebalo mijenjati ništa, ovako će raditi ispravno i bez grešaka

7. Izlistavanjem datoteka vidite da datoteka srs_ispit.txt ima postavljene ovlasti r w - r- - r - x. Hoće li vanjski korisnici (other) moći pročitati datoteku?
   a) da
   b) ne
   c) nije definirano za vanjske korisnike

8. Slijedi isječak iz teksta objavljenog 2014. godine na srednje.hr:

   Stefan Crnojević 16-godišnj je genijalac koji bez imalo muke razbije svaku računalnu šifru ili kod te se, zahvaljujući svom talentu, redovito okiti kakvom medaljom, a nedavno je postao svjetski prvak. Mladi Beograđanin koji posjeduje zavidne matematičke i programerske sposobnosti govori kako ne smije otkrivati svoje metode jer je kriptografija ipak znanost zavijena velom tajni.

   Na temelju isječka možemo zaključiti da mladi Stefan nije svjestan:
   a) Kirchhoffovog zakona
   b) Kerckhoffog principa
   c) Diffie-Hellmanove razmjene ključeva
   d) Merkle-Damgard konstrukcije
   e) Rivest-Shamir-Adelman algoritma

9. Koje od sljedećih su ispravni parovi ključeva za kriptosustav "Obični RSA"?
   a) (5,65),(1,65)
   b) (3,45),(11,45)
   c) (3,45),(27,65)
   d) (35,65),(11,65)
   e) (7,45),(13,45)
   f) (3,65),(22,65)
   g) (3,65),(29,65)
   h) (19,65),(43,65)

10. Zadan je sljedeći pseudo kod kojem je cilj šifriranje poruke proizvoljne duljine simetričnom šifrom:

    Ulaz:

    - m je poruka koju je potrebno šifrirati
    - k je simetrični ključ veličine 16 bajtova

    Postupak šifriranja:

    1. nadopuni poruku m tako da joj je veličina višekratnik od 16 bajtova;
    2. izračunaj SHA256(m) i dodaj tih 32 bajta na kraj poruke m;
    3. iv = slučajno odabranih 16 bajtova;
    4. $m_1, m_2, \ldots, m_k$ = rastav od m na blokove veličine 16 bajtova;
    5. za svaki i=1, …, k izračunaj c_i = AES128(iv+i, k) XOR m_i (+ označava obično zbrajanje);
    6. spoji blokove iv, $c_1, c_2, \ldots, c_k$ u šifrat c;

Pitanja:

a) Opišite odgovarajući postupak dešifriranja.
b) Pruža li ovakav postupak šifriranja svojstvo povjerljivosti? Ako da, iznesite zašto, ako ne, detaljno opišite scenarij u kojem je svojstvo povjerljivosti narušeno.
c) Pruža li ovakav postupak šifriranja svojstvo integriteta? Ako da, iznesite zašto, ako ne, detaljno opišite jedan scenarij u kojem je svojstvo integriteta narušeno.
d) Ako postupak ne pruža oba svojstva, opišite jedan način šifriranja poruke proizvoljne duljine tako da su oba svojstva zadovoljena.

11. Zadan je sljedeći pseudo kod kojem je cilj šifriranje poruke proizvoljne duljine asimetričnom šifrom:

Ulaz:

- m je poruka koju je potrebno šifrirati
- (e, N) je javni RSA ključ, N ima 2048 bitova

Postupak šifriranja:

1. nadopuni poruku m tako da joj je veličina višekratnik od 16 bajtova;
2. $m_1, m_2, \ldots, m_k$ = rastav od m na blokove veličine 16 bajtova;
3. za svaki i=1, …, k izračunaj $c_i = m_i$^e MOD N;
4. spoji blokove $c_1, c_2, \ldots, c_k$ u c;

Pitanja:

a) Opišite odgovarajući postupak dešifriranja.
b) Pruža li ovakav postupak šifriranja svojstvo povjerljivosti protiv napadača koji zna samo javni ključ? Ako da, iznesite zašto, ako ne, detaljno opišite jedan scenarij u kojem je svojstvo povjerljivosti narušeno.
c) Opišite jedan način šifriranja poruke proizvoljne duljine tako da je zadovoljeno svojstvo semantičke sigurnosti protiv napada odabranim skrivenim tekstom.

12. Dolje je zadan isječak koda koji sa standardnog ulaza čita niz brojeva i ispisuje pročitani niz na standardni izlaz. Programer je, nažalost, napravio *off-by*-one grešku u *for* petljama. Kod je preveden te se koristi na Linux x86-64 sustavu gdje funkcijski stog raste prema dolje te su kasnije deklarirane lokalne varijable smještene na nižim adresama.

```
void procitaj_niz() {
  int i;
  int n;
  int niz[10];

  printf("Upisite broj elemenata niza: ");
  scanf("%d", &n);
```

```
  // Cuo sam za prelijevanje, treba provjeriti velicinu niza
  if (n > 10) {
    printf("Previse elemenata!");
    return ;
  }

  // Procitaj elemente.
  for (i=0; i<=n; i++)
    scanf("%d", &niz[i]);

  // Ispisi elemente
  for (i=0; i<=n; i++)
    printf("%d\n", niz[i]);
}
```

Pitanja:

a) Pretpostavimo da sustav ima uključene “Write-XOR-Execute" i “ASLR” zaštite. Detaljno opišite napad u kojem napadač može doći do sadržaja memorije *čitavog* funkcijskog stoga procesa. Skicirajte sadržaj bitnog dijela memorije procesa tijekom ključnih koraka napada.

b) Pretpostavimo da sustav nema uključene “Write-XOR-Execute" i “ASLR” zaštite. Detaljno opišite napad u kojem napadač može izvršiti kod po vlastitom izboru. Skicirajte sadržaj bitnog dijela memorije procesa tijekom ključnih koraka napada.

c) Objasnite na primjeru napada iz podzadatka b) kako se od napada preljeva međuspremnika možemo obraniti koristeći kanarince.