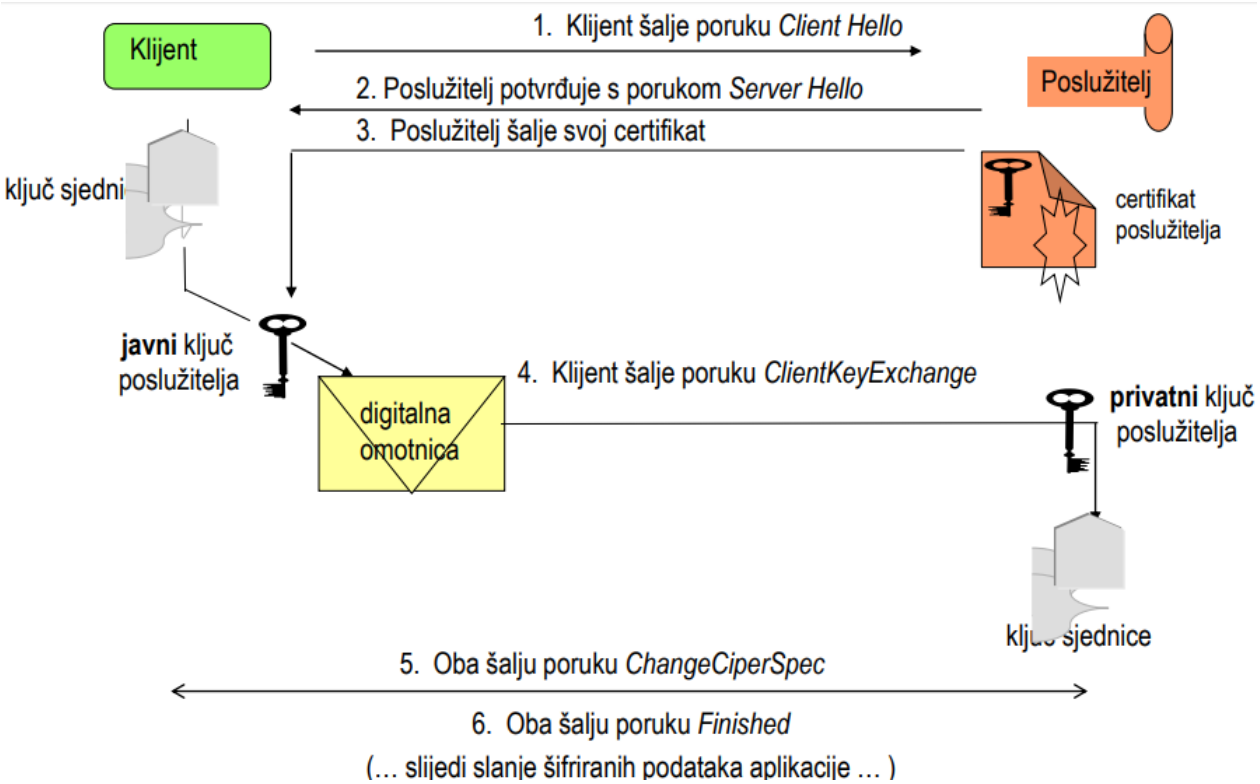
ZISIS – ZR 2016/2017

1. **(2 boda) Definirajte pojam sigurnosti.**

Kontinuirani proces čijim provođenjem se osigurava određeno stanje (sustava i/ili podataka/informacija). Željeno stanje je definirano određenim zahtjevima

2. **(4 boda) Opišite postupak uspostavljanja TLS veze. Zašto napadač ne može preuzeti certifikat neke druge stranice te ga koristiti za lažno predstavljanje?**



Zato što nema privatni ključ kojim bi dekriptirao ključ sjednice (?)

3. **(6 bodova) Navedite dvije norme za zaštitu elektroničke pošte i ukratko ih opišite.**

S/MIME

S/MIME se temelji na sustavu PKI

engl. Secure MIME

Svaki korisnik ima svoj privatni ključ i certifikat.

Korisnik može sam generirati svoj privatni i javni ključ te zatražiti izdavanje certifikata.

U korporativnim okruženjima korisnik dobija svoj privatni ključ i certifikat od odgovarajuće službe u tvrtci

Ovo je dobro rješenje za korporativna okruženja

Specifično namijenjeno zaštiti elektroničke pošte

PGP

PGP se temelji na međusobnom dijeljenju javnih ključeva bez centraliziranog nadzora.
Skraćenica od Pretty Good Privacy
Prvu verziju razvio i napisao Phil Zimmermann 1991. godine
Često se pod tim porazumijeva i program za šifriranje, potpisivanje, itd.
Normirano u sklopu RFC4880 (OpenPGP)
Pogodniji je za pojedince i slabo povezane grupe
Može se koristiti za šifriranje i potpisivanje bilo kakvih podataka
Nije specifično za poruke elektroničke pošte

4. (3 boda) Navedite svrhu voditelja sigurnosti (CISO-a).

- **Nadzor i koordinacija aktivnosti** vezanih uz sigurnost informacijskog sustava
- **Iniciranje primjene dobrih praksi i prihvaćenih standarda** vezanih uz sigurnost informacijskog sustava
- **Savjetodavna uloga** u svezi sa sigurnosti informacijskog sustava

5. (5 bodova) Koja su dva temeljna načina otkrivanja ranjivosti u računalnoj mreži? Navedite prednosti i mane sakog od načina.

Skeniranje mrežnih raspona

Nessus, OpenVAS
Jednostavno, ali opterećuje mrežu i puno lažno točnih detekcija
Jeftina, ali ne otkrivaju nužno sve ranjivosti

Penetracijska ispitivanja

Obavljaju pojedinci ili timovi koji traže ranjivosti
Cilj je i pokušati iskoristiti ranjivost, ne samo ju naći
Skuplja od skeniranja
Ne otkrivaju nužno sve ranjivosti

6. (4 boda) Objasnite:
   a. Što je sigurnost programske podrške?
   b. Što je sigurna programska podrška?
   c. Kada je sigurnost softverski problem?
   d. Čime se bavi softverska sigurnost
7. (5 bodova) Za svaku od navedenih faza sigurnog životnog ciklusa navedite ključne prakse:
   a. Zahtjevi
   b. Dizajn
   c. Implementacija
   d. Verifikacija
   e. Objava

8. (6 bodova) Što je STRIDE?

Spoofing - Korisnik se prijavljuje s podacima nekog drugog korisnika
Tampering - Unos SQL naredbe u neki input -> posljedica je promjena u bazi
Repudiation - Neidentificirani korisnik koristi proxy za sakrivanje IP adrese pa se akcije ne mogu povezati s njima
Information Disclosure - Korisnik namjerno unosi izvodi štetne akcije (unosi neispravne podatke u forme npr.) kako bi izazvao exception u procesu i mozda vidio poruku o pogresci (a to ne bi smio viditi)

Denial of Service - Korisnik namjerno unosi izvodi štetne akcije (unosi neispravne podatke u forme npr.) kako bi server bio zatrpan poslom (potrosnja memorije)
Elevation of privilege - Korisnik koristi pogreske u sigurnosti kako bi dobio pristup nekim operacijama (rucna promjena URL adrese ga vodi na neku formu za koju ne bi smio imati pristup)

9. (5 bodova) Što je DREAD?

Damage potential - moguća šteta, veličina štete bude li napad uspješan
Reproducibility – reproduktivnost, koliko je jednostavno ponoviti napad
Exploitability – iskoristivost, trud i znanje potrebnih za uspješan napad
Affected users – zahvaćeni korisnici, moguće uspjelim napadom, postotno
Discoverability - mogućnost otkrivanja, teško mjerljivo
Procjena svake prijetnje po navedenim parametrima
pojedinačno vrijednost od 1 do 10 (najmanje loše – najgore)
ukupan rizik - prosjek 5 pojedinačnih DREAD vrijednosti

10. (4 boda) Ukratko objasnite 4 osnovna postupka za razrješenje rizika.

- Izbjegavanje (Avoidance) - ne preuzeti rizik ili ukloniti uzrok
- Dijeljenje/prijenos (Sharing) - rizik u jednom dijelu nije rizik u nekom drugom
- Smanjenje, redukcija (Reduction) - prihvatiti mogućnost rizika i razviti rezervni plan
- Zadržavanje, prihvaćanje (Retention) - prihvatiti mogućnost da se rizik može dogoditi i ne činiti ništa

11. (4 boda) Objasnite postupke provjere: SAST, DAST, LAST, analiza izvornog koda.

12. (4 boda) Opišite diskrecijsko i mandatno upravljanje pristupom u bazama podataka.

Diskrecijsko upravljanje pristupom u bazama podataka
Upravljanje na temelju:
- identiteta korisnika koji zahtijeva pristup
- eksplicitnih pravila pristupa koja utvrđuju tko može izvesti koje akcije na kojim objektom sustava

Koncept vlasništva nad objektom - vlasnik objekta određuje kome se dozvoljava pristup.
Određenom korisniku potrebno je eksplicitno dodijeliti dozvolu za obavljanje određene operacije nad određenim objektom (autorizacija). Dozvole su opisane trojkama <korisnik, objekt, vrsta operacije>. Prije obavljanja svake operacije, SUBP provjerava ima li korisnik dozvolu za obavljanje operacije nad objektom (upravljanje pristupom).

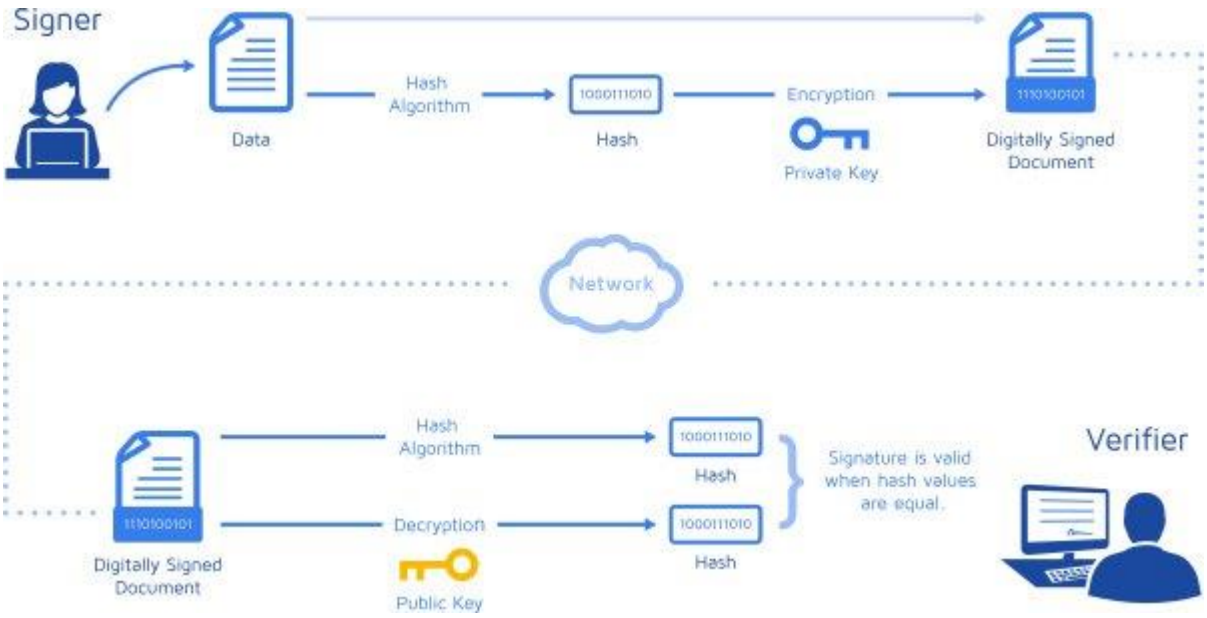
Mandatno upravljanje pristupom u bazama podataka
- sigurnosna politika na razini sustava određuje tko ima pravo pristupa, a ne vlasnik objekata
- svaki objekt dobiva oznaku klasifikacijske razine (classification level) , npr. povjerljivo, tajno... koja odražava osjetljivost informacije sadržane u objektu
- svakom korisniku dodjeljuje se oznaka razine ovlasti (clearance level)
- korisnici mogu obavljati operacije nad onim objektima za koje imaju odgovarajuću razinu ovlasti

13. (6 bodova) Napišite naredbe kojima će se obaviti sljedeće akcije:
    a. Kreiranje uloge *student*
    b. Dodjeljivanje ulozi *student* dozvole za pregledavanje podataka iz tablice *predmet*
    c. Dodjeljivanje uloge *student* korisniku *kolar*

U zadatku se podrazumijeva korištenje SUBP-a IBM informixa.

a. CREATE ROLE student;
b. GRANT SELECT ON predmet TO student;
c. GRANT student TO novak;

14. (4 boda) Skicirajte postupak digitalnog potpisivanja.



15. (2 boda) Objasnite ulogu vremenskog žiga pri digitalnom potpisivanju.

Osigurava pouzdanost digitalnog potpisa i poslije isteka valjanosti ili opoziva certifikata potpisnika, pomoću vremenskog žiga može se dokazati da je potpis napravljen prije isteka vrijednosti certifikata.
Ne može se poreći da je podnositelj zahtjeva za vremenskom oznakom bio u posjedu originalnog dokumenta u vremenu naznačenom vremenskom oznakom.

16. (4 boda) Što znate o normi PCI DSS? Navedite bar tri osnovna zahtjeva iz norme PCI DSS.

PCI DSS je sigurnosni standard za kartično poslovanje koji regulira zahtjeve koji se odnose na upravljanje sigurnošću podataka, sigurnosne procedure, mrežnu arhitekturu, oblikovanje programske potpore za obradu podataka te ostale kritične zaštitne mjere u kartičnom poslovanju.
Jezgru PCI DSS-a čini skupina načela i pratećih zahtjeva oko kojih su organizirani specifični elementi sigurnosti podataka u kartičnom poslovanju.

Zahtjev 1: Instalirati i održavati odgovarajuću konfiguraciju vatrozida (eng. firewall) radi zaštite podataka o vlasnicima kartica.
Zahtjev 2: Ne koristiti lozinke i druge sigurnosne parametre dobivene od dobavljača softverskog sigurnosnog rješenja
Zahtjev 3: Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štititi
Zahtjev 4: Tijekom prijenosa putem otvorenih, javnih mreža svi podaci o vlasniku kartice moraju se štititi šifriranjem (enkripcijom).
Zahtjev 5: Nužno je koristiti i redovito osvježavati softver za zaštitu od zlonamjernog koda, odnosno antivirusni softver

17. (2 boda) Što se u normi Web Services Security specificira u vezi XML-DSig?

Način potpisivanja poruke, korišteni ključ i rezultat potpisa.