Elektroničko poslovanje i digitalne inovacije

ELEKTRONIČKO PLAĆANJE

SADRŽAJ

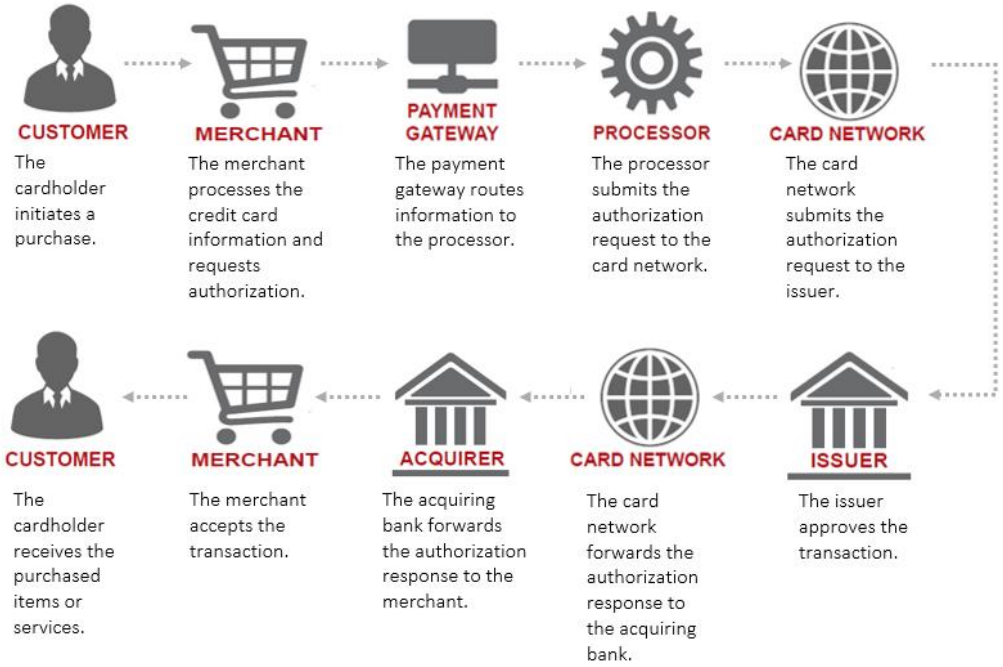
- Što je e-plaćanje
- Aspekti e-plaćanja
- Metode e-plaćanja
- Zahtjevi e-plaćanja
- Rizici e-plaćanja
- E-novac i mikroplaćanje
- Sigurnost i privatnost
  - Sustavi zaštite e-poslovanja
  - Protokoli
  - Digitalni potpis

ŠTO JE E-PLAĆANJE

- Elektroničke platne transakcije su platne transakcije inicirane i izvršene na način koji uključuje korištenje elektroničke platforme ili uređaja (primjerice internet, mobilne aplikacije, POS uređaji…).
  - Elektronička platna transakcija je svako kartično plaćanje, kreditni transfer, plaćanje mobitelom i dr. koje je inicirano i izvršeno na način koji uključuje korištenje elektroničke platforme ili uređaja.
- Kod platne transakcije s udaljenosti također je riječ o elektroničkim platnim transakcijama, ali propisan je i dodatni kriterij da se takve transakcije izvršavaju preko interneta ili uređaja koji se koriste za komunikaciju na daljinu.
  - Platne transakcije s udaljenosti posebno su definirane jer zbog samog načina iniciranja takvih transakcija postoji veći rizik od prijevare, pa su za takve platne transakcije propisani dodatni zahtjevi sigurnosti (pouzdana autentifikacija klijenta, koja uključuje tzv. dinamičke elemente, odnosno elemente koji transakciju povezuju s određenim iznosom i određenim primateljem plaćanja kojeg je odredio platitelj pri iniciranju transakcije).
  - Ako se elektroničke platne transakcije iniciraju preko interneta (kreditni transfer preko internetskog bankarstva, plaćanje platnom karticom na internetu) ili uređaja kojim se može koristiti za plaćanje na daljinu (plaćanje mobitelom u slučaju kad se koristi internetski preglednik), tada govorimo o platnim transakcijama s udaljenosti.
- U slučaju kad se elektroničke platne transakcije iniciraju preko POS uređaja u trgovini ili mobitela korištenjem NFC tehnologije (engl. *Near Field Comunication*, tehnologija za beskontaktno plaćanje), nije riječ o platnim transakcijama s udaljenosti.

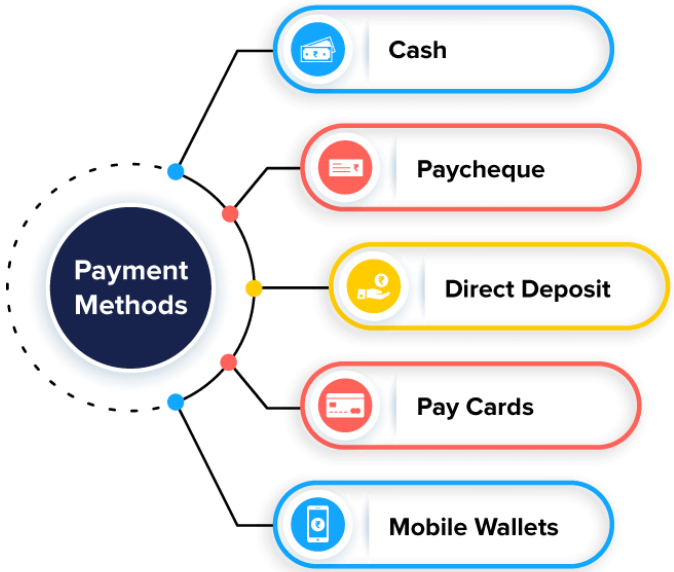
ASPEKTI E-PLAĆANJA

- Ima 4 aspekta:
  - Kako je novac prezentiran
  - Kako je transfer obavljen
    - OFFLINE
    - ONLINE
  - 3. Odnos sa središnjom bankom
  - 4. Sigurnost



METODE PLAĆANJA

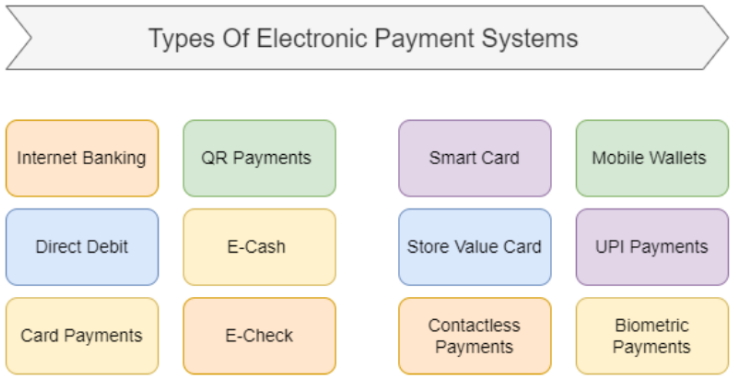
1. Prijenos gotovine
2. Ček
3. Transferi vrijednosti (žiro), međubančani transferi (EFT)
4. Kreditne kartice
5. Kartice za plaćanje (Telefonske kartice)
6. Agregacija (akumulacija, npr. *Qpass*)
7. Posrednici (npr. *PayPal*)
8. Mikroplaćanja / Sustavi zapisivanja (npr. *Milicent*)
9. Žetoni (npr. *Flooz, Beenz*)
10. Offline plaćanje
11. Online plaćanje

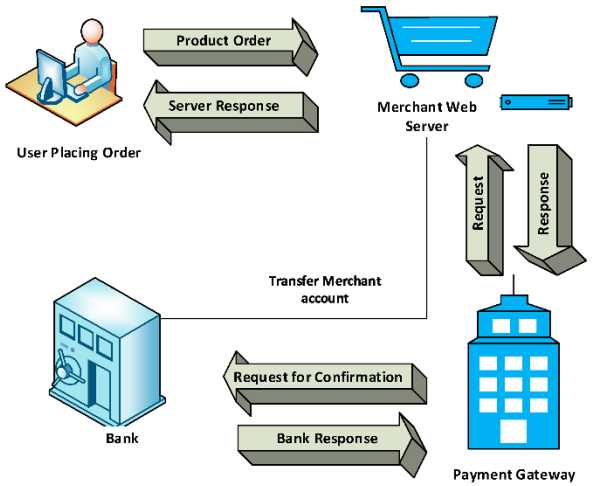


- **Zadatak:** Pronađite po jedan primjer (različit od postojećih) za svaku od gore navedenih metoda plaćanja.

METODE ONLINE PLAĆANJA

1. Aplikacije
2. E-novčanik
3. QR kod
4. Kreditna kartica
5. E-gotovina (digitalni novac)
6. E-bankarstvo i m-bankarstvo
7. NFC
8. Blockchain

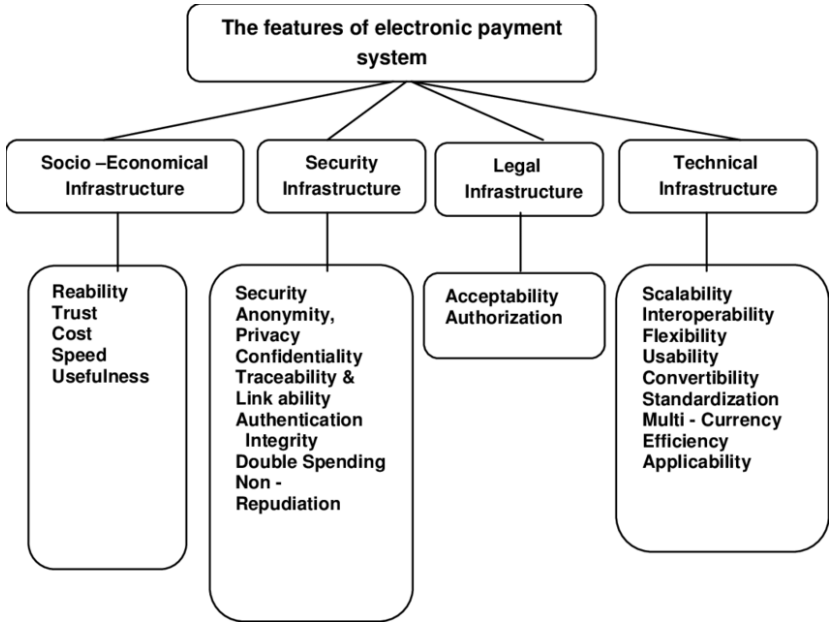




- **Zadatak:** Pronađite i opišite po jedan primjer sustava za svaku od gore navedenih metoda e-plaćanja.

ZAHTJEVI E-PLAĆANJA

- Temeljni zahtjevi za sustav e-plaćanja:
  - Fizička podrška (pametne kartice, datoteke, enkriptirani stringovi)
  - Prezentacija vrijednosti (brojevi)
  - Lokacija pohranjene vrijednosti (banka, e-novčanik)
  - Tko prihvaća novac?
  - Način korištenja (udaljen, licem u lice)
  - Načini plaćanja (prijenos vrijednosti)
  - Vjerodostojnost (je li ukraden, dvostruko korišten)
  - Sigurnost
  - Praćenje (anonimnost, privatnost)
  - Skalabilnost, trošak

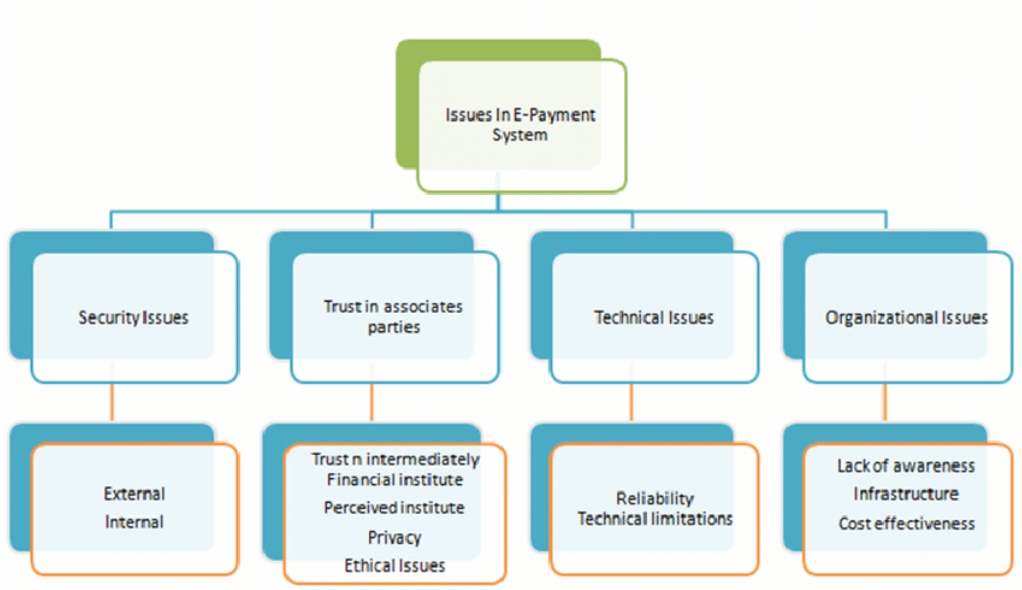


ZAHTJEVI E-PLAĆANJA

- Temeljni zahtjevi za sustav e-plaćanja:
  - Brzina
  - Niski troškovi
  - Jedinstvo novca i robe (novac i roba su izmijenjeni po principu oboje ii ništa)
  - Općenitost transakcije
  - Prihvaćanje od kupca
  - Međuoperabilnost (sklopovska i sistemska)
  - Usklađenost sa zakonom

RIZICI E-PLAĆANJA

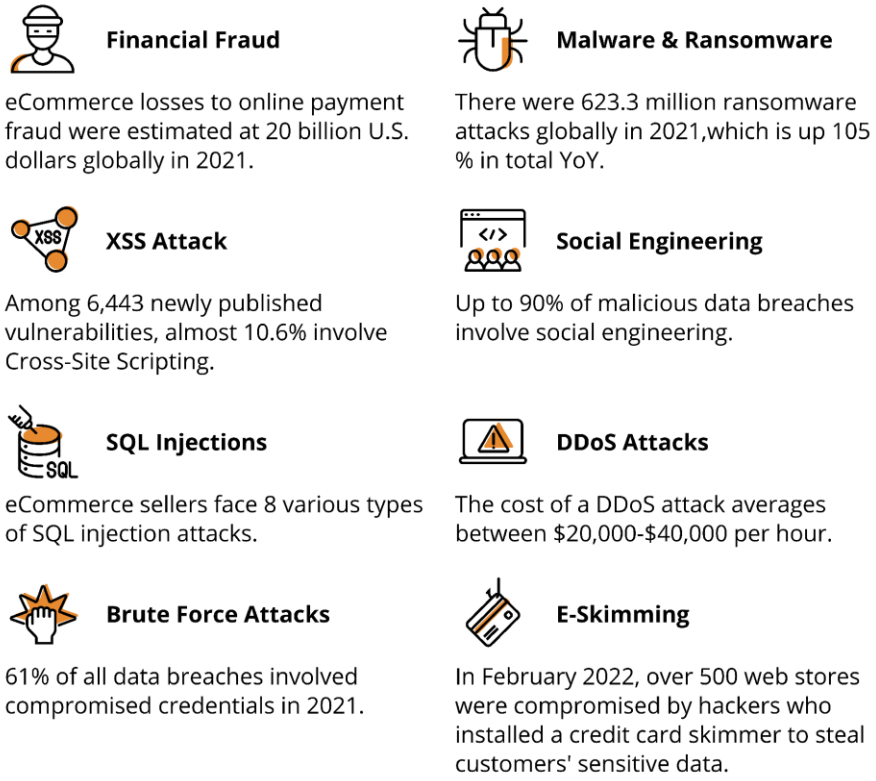
- **Operativni (pouzdanost i integritet)**
  - Sigurnost (neovlašteno korištenje)
  - Krađa od zaposlenika
  - Nepropisno korištenje od strane kupca
  - Rizik osiguravatelja usluge (*service provider*)
  - Zastarijevanje sustava
- **Reputacijski**
  - Negativno javno mišljenje i gubitak posla
  - Slabosti sustava
  - Probijanje sigurnosti
  - Neuspjesi sličnih sustava
- **Sistematski**
  - Rizik da će neispunjavanje obveze propagirati kroz sustav, uzrokujući neispunjavanje obveza na drugim razinama



RIZICI E-PLAĆANJA

Sveučilište u Rijeci
Fakultet informatike i digitalnih tehnologija

- **Legalni (kršenje zakona, nejasnoće, sankcije)**
  - Pranje novca
  - Kršenje privatnosti
  - Strani zakoni
- **Bankarski**
  - Krediti (neplaćanja, insolventnost)
  - Likvidnost (potražnja za e-novcem)
  - Kamata
  - Tržište (inflacija, strane valute)
- **Kriminalni**
  - Prijevara
  - Krađa
  - Zaokruživanje (nelegalno korištenje floata-a)



E-NOVAC U PRIMJENI

- DigiCash
  - Sustav elektroničkog novca koji je stvorio DigiCash se zove *eCash*. To je simbolički sustav, koji koristi slijepi potpis za postizanje anonimnosti.
- Billpoint
  - Osim elektroničkih plaćanja obavlja i klasičnu naplatu kartica.
- PayPal
  - Sustav u masovnoj primjeni. Omogućava pretvaranje novca s kreditne kartice ili bankovnog računa u e-novac. Korisnici mogu stvoriti i virtualnu debitnu karticu te plaćati direktno na račune u bankama.
- Mondex
  - Sustav elektroničke gotovine koji se temelji na tehnologiji pametnih kartica. Na kartici se nalazi procesor i memorija, koji implementiraju elektronički novčanik.

QUICK SUSTAV PLAĆANJA

1. Kupac odabire proizvode na Web-u i odabire "Quick payment" opciju.
2. Trgovčev server kontaktira server plaćanja, odašilje klijentovu IP adresu i vrijednost transakcije, kratak opis proizvoda i ID trgovca.
3. Server plaćanja "zaključava" trgovca za transakciju, kontaktira "novčanik" preko TCP-a na posebnom portu napravljenom za Quick Internet plaćanje.
4. Klijent računalo pristupa čitaču i traži kupčevu Quick karticu.
5. Prije nego se kartica tereti s iznosom, klijent računalo prikazuje poruku koja opisuje naručena dobra i ukupan iznos te dozvoljava kupcu da odustane.

MIKROPLAĆANJA

- Zamjena za gotovinu
  - Jeftinije
  - Brže
  - Jednostavnije za izračun, provjeru i slijedivost
- Male transakcije - transakcije imaju nizak iznos (npr. manje od 10kn)
  - Telefon
  - Kocka
  - Lutrija
  - Parking
  - Članci
- Ostale značajke:
  - Plaćanje na daljinu
  - Nema fizičkih dobara, nego samo informacija
  - Velik broj transakcija

SUSTAVI MIKROPLAĆANJA

- Svaki sustav ima 3 osnovna elementa:
  1. kupac
  2. prodavač
  3. posrednik
     - financijska institucija koja kupcu izdaje enkriptirani string, a prodavaču uzima string i daje mu novac
- Vrste sustava:
  - PAYWORD
  - MICROMINT
  - MILICENT
- **Zadatak:** istražiti osobine i način funkcioniranja ova tri sustava mikroplaćanja.

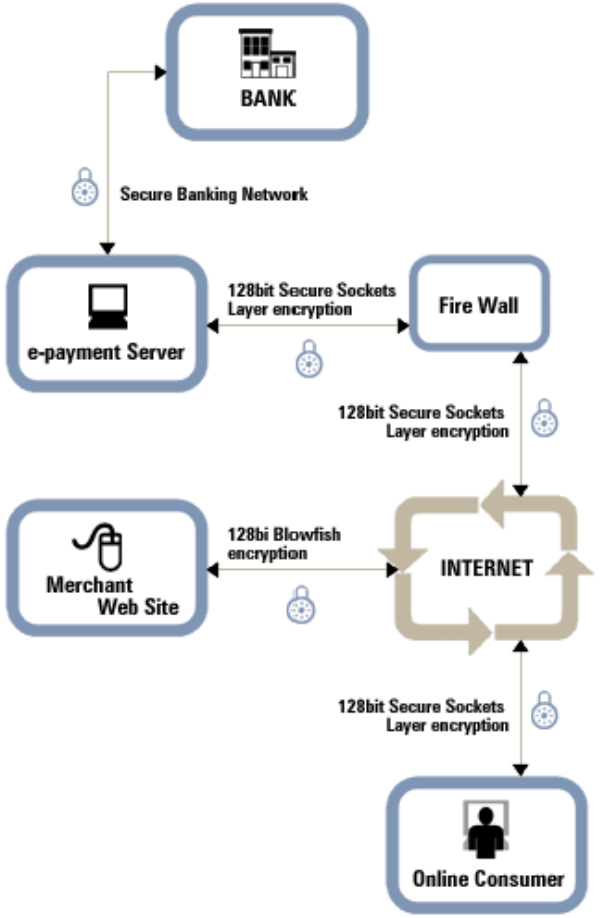
SIGURNOST I PRIVATNOST

Sveučilište u Rijeci
Fakultet informatike
i digitalnih tehnologija

- Informacije koje su od velike važnosti tvrtci potrebno je bolje zaštititi, pa se zbog toga ne koriste isti stupnjevi sigurnosti za sve informacije.
- Sigurnosni programi se trebaju temeljiti na:
  - sprječavanju neovlaštenog pristupa povjerljivim informacijama tvrtke,
  - potrebi konzistentnosti izmijenjenih podataka u svim bazama koje sadrže te podatke,
  - omogućavanju izmjene podataka samo ovlaštenim osobama za takve izmjene,
  - pristupačnosti ovlaštenim osobama na korištenje, i
  - popravljivosti sustava od neovlaštenog upada u sustav.

SUSTAVI ZAŠTITE E-POSLOVANJA

- Tvrtke koje su orijentirane isključivo na e-poslovanje, poslovanje obavljaju najvećim djelom preko računalne mreže.
- Kada govorimo o zaštiti tvrtki orijentiranih isključivo e-poslovanju, zapravo mislimo na zaštitu računalnih mreža, uređaja koji čine te računalne mreže i uređaja koji komuniciraju u toj računalnoj mreži.
- Zaštita e-poslovanja temelji se na:
  - Antivirusnim programima,
  - Zaštitnim barijerama, te
  - IDS/IPS sustavima.



SUSTAVI ZAŠTITE E-POSLOVANJA

- Najviše napada na tvrtke dolazi s interneta te je potrebno tvrtku dobro zaštititi od paketa koji dolaze s interneta.
- Prvu provjeru paketa koji su došli s interneta izvršava zaštitna barijera s podešenim IDS sustavom, za rad sa zaštitnom barijerom.
- Paketi potom dolaze do sklopke (eng. *switch*) koja usmjerava pakete dalje kroz mrežu.
- Na sklopci se paketima koji su došli s interneta pridružuju paketi koji su došli s ekstraneta i oni zajedno putuju do druge provjere paketa.
- Druga provjera paketa sastoji se od podešenog IPS sustava, zaštitne barijere i antivirusnog programa koji izvršavaju provjeru paketa.
- Zatim paketi dolaze do sklopke koja usmjerava pakete ili prema intranetu ili prema administratoru mreže.
  - Centralno računalo s povjerljivim informacijama za tvrtku ponekad može biti na mjestu administratora.
  - Također, postoji mogućnost obostranog toka paketa, a sklopka može proslijediti i podatke s intraneta prema administratoru i obratno.

ANTIVIRUSNI PROGRAMI

- Antivirusni program je softver koji omogućava zaštitu i skeniranje sustava od poznatih inačica virusa i poznatih programa koji mogu nanijeti štetu računalu.
- Antivirusni program može pronaći, izdvojiti i obrisati, uz odobrenje korisnika, poznatu inačicu zlonamjernog programa.
- Potrebno je paziti pri instaliranju i konfiguriranju različitih antivirusnih programa koji se koriste za zaštitu e-poslovanja, kako oni ne bi npr. zaustavili sav promet na zaštitnoj barijeri.
- Primjeri antivirusnog programa su:
  - Avast, McAfee, TotalAV, NordVPN, Norton, Bitdefender, Avira, ...

ZAŠTITNE BARIJERE

- Zastitne barijere (*eng. Firewalls*) štite mreže od neovlaštenog skeniranja i upada u mrežu.
- Potrebno ih je dobro podesiti i održavati, kako bi što učinkovitije štitile - kako same podatke zaštitne barijere, tako i podatke mreže.
- Što manje napadač zna o samoj barijeri, to će je teže zloupotrijebiti.
- Zaštitne barijere su ponekad neprobojne napadačima pa im pokušavaju neovlašteno pristupiti i/ili ih zaobići.
  - Na primjer, ako napadač ima korisničko ime i lozinku na zaštitnoj barijeri korisnika, on može ući u zaštitnu barijeru.
- **Zadatak:** pronađite i opišite 2 primjera zaštitnih barijera.

IDS/IPS SUSTAVI

- Sustav koji automatizirano prati mrežne i sistemske događaje u svrhu detekcije kršenja sigurnosne politike naziva se sustav za detekciju upada na sustav (eng. *intrusion detection system – IDS*).
  - Takav sustav nije zadužen za sprječavanje upada na sustav.
- Za sprječavanje upada u sustav koristi se sustav za sprječavanje upada (*eng. intrusion preventions system – IPS*), koji najčešće kao jedan od svojih dijelova sadrži i sustav za detekciju upada.
- Najčešće programska rješenja posjeduju elemente i za detekciju i za sprječavanje, stoga se radi o sustavima za detekciju i sprječavanje upada (IPDS).
- Najvažnija uloga takvih sustava jest bilježenje, tj. identificiranje mogućih sigurnosnih incidenata te bilježenje njihovog konteksta. Tek kada je mogući sigurnosni incident zabilježen, sustav pokušava spriječiti upad.

IDS/IPS SUSTAVI

Sveučilište u Rijeci
Fakultet informatike i digitalnih tehnologija

- IDS sustavi dijele se na NIDS i HIDS sustave, tj. sustave za detekciju mrežnih upada i sustave za detekciju upada na lokalno računalo :
  - **NIDS sustavi** nadziru mrežni sloj operacijskog sustava kako bi detektirali zlonamjerne uzorke mrežnog prometa – npr. pretraživanje mrežnih priključaka, nagli porast mrežnog prometa i sl. Najčešće se promatraju osjetljivi dijelovi mreže, npr. dijelovi mreže koji najviše komuniciraju s vanjskim svijetom.
  - **HIDS sustavi** nadziru izmjene datotečnog sustava, sistemske pozive, aplikacijske zapise i sl.
- Prema načinu detekcije postoje sustavi koji pronalaze upade pomoću:
  - **Statističke analize tj. detekcije anomalija** – sustavi koji na temelju bilješki koje su prikupili pri normalnom radu sustava detektiraju neobične događaje.
    - Nedostatak ovog načina jest da sustav mora duže vrijeme „učiti" normalno ponašanje sustava, pri čemu postoji i mogućnost krivog učenja. Prednost mu je što može otkriti prethodno nezabilježene vrste napada.
  - **Usporedbe potpisa** – sustavi koji događaje uspoređuju s predefiniranim obrascima napada.
    - Nedostatak ovog načina je ta da obrazac napada mora biti poznat kako bi se njegov potpis mogao usporediti s trenutnim događajima u sustavu. Prednost ovog načina rada jest pouzdanost detekcije (manji broj lažnih detekcija).
- Neke od temeljnih metoda kojima se koriste dijelovi sustava za sprečavanje upada (nakon što je on detektiran) su:
  - Blokiranje prometa iz smjera napada, podizanje alarma, zaključavanje dijela sustava pod napadom, ...

IDPS SUSTAVI

- IDPS sustavi mogu otkriti uspješan napad na sustav od strane napadača, mogu zabilježiti način napada za buduće reference, mogu otkriti skeniranje sustava u cilju napada na sustav, mogu pratiti velike prijenose podataka u računalnoj mreži (na primjer, ako netko, neovlašteno, želi iz tvrtke uzeti veliku količinu podataka) i sve to prijavljuju administratoru sustava.
  - Neki IDPS sustavi se mogu podesiti da rade sa zaštitnim barijerama, kako bi pratili promet paketa iz tvrtke i u tvrtku, u cilju bolje zaštite tvrtke.
- Izvješća o upozorenju se mogu slati administratoru preko: e-maila, SNMP-ovih poruka o upozorenju i sl. Izvješće o upozorenju sastoji se samo od osnovnih informacija o upozorenju, dok se ostatak izvješća može pročitati na IDPS-u.
- Postoji mogućnost, ako se IDPS sustav na računalnoj mreži stavi iza zaštitne barijere, da sustav zaustavi zlonamjerni promet koji je zaštitna barijera pustila u sustav tvrtke (npr. zbog loše konfiguracije).
- Postoji mogućnost, ako je neka nepoznata inačica zlonamjernog programa ušla u sustav i ne izvršava zadaće koje je administrator IDPS sustavu naveo kao zlonamjerne, da IDPS sustav neće biti u stanju otkriti taj zlonamjerni program.
  - Nedostatak otkrivanja putem poznatih obrazaca ponašanja je da IDPS sustav nije u stanju prepoznati prijetnju s novim, odnosno prethodno nepoznatim, obrascima ponašanja.

IDPS SUSTAVI

- IDPS sustave prema načinu na koji nadziru sustave i mjestu gdje su implementirani dijelimo na one koji:
  - **nadziru mrežni promet za određeni dio računalne mreže**
    - sustav se često smješta iza zaštitne barijere
  - **nadziru bežični promet i bežične protokole**
    - sustav se često smješta unutar dometa tvrtkine bežične mreže
  - **nadziru tvrtkin mrežni promet**
    - sustav se često smješta na mjestu na kojem može najbolje nadzirati tok mrežnih informacija
  - **nadziru centralno računalo i/ili server**
    - sustav se često smješta na centralno računalo i/ili server i nadzire prijavu i sumnjive radnje na centralnom računalu i/ili serveru

IDPS SUSTAVI

- Tipični dijelovi IDPS sustava su:
  - pokazivač ili posrednik
    - služe za nadzor računalnih mreža i/ili sustava i analizu prikupljenih podatka
  - server za upravljanje
    - centralni uređaj koji upravlja podacima koje dobije od pokazivača i posrednika
  - server s bazom podataka
    - služi za upis podataka u bazu, a u bazu se upisuju podaci koje su zabilježili pokazivači, posrednici i serveri za upravljanje
  - upravljačka ploča
    - program koji omogućava korisnicima i administratorima IDPS sustava upravljanje IDPS sustavom i čitanje izvještaja IDPS sustava
- **Zadatak:** pronađite i opišite 2 primjera IDPS sustava.

PROTOKOLI

- Protokole, prema razini na kojoj se primjenjuju, dijelimo na:
  - Aplikacijske
    - koriste ih aplikacije na mreži (npr. protokoli za dohvat web stranica)
  - Transportne
    - koriste se za poboljšavanje transporta paketa na mreži (npr. protokoli za sprječavanje gubitka paketa)
  - Mrežne
    - koriste se za prijenos paketa unutar mreže (npr. prijenos paketa s jednog računala na server)
  - Podatkovne
    - omogućavaju prijenos podatkovnih paketa u mreži (npr. prijenos oblika slova)
- Protokole dijelimo i na:
  - kriptografske protokole - koriste kriptografske metode za zaštitu podataka (npr. IPSec i SSH protokoli)
  - protokole koji ne koriste sigurnosnu zaštitu podataka koje prenose (npr. TCP/IP i UDP protokoli ne sifriraju podatke)

TCP/IP I UDP PROTOKOLI

- Računala za povezivanje na Internet koriste TCP/IP protokol.
- **TCP/IP protokol** se sastoji od dvije razine:
  - TCP (eng. *Transmission Control Protocol*) sastavlja pakete koji se šalju računalnom mrežom i ponovno sastavlja podatke od paketa koji su dostavljeni s računalne mreže.
  - IP (eng. *Internet Protocol*) upravlja adresiranjem paketa, odnosno šalje podatke na konačno odredište u obliku nekoliko sastavljenih paketa.
- TCP/IP protokol može biti primijenjen na svim računalnim mrežama (internet, intranet i ekstranet).
- IP protokol se primjenjuje na mrežnoj razini. TCP i UDP protokoli se primjenjuju na transportnoj razini.
- **UDP (eng. *User Datagram Protocol*)** komunikacijski protokol pruža nepouzdanu uslugu slanja paketa s jednog glavnog računala na drugo.
  - Koristi se s IP protokolom.
  - Koristi se za npr. prijenos videa, jer gubitak određenih podataka ne mora puno naštetiti kvaliteti videa.
  - Poruke kod kojih je bitan redoslijed slanja ne treba slati UDP protokolom, jer on ne može poslati poruke u točno određenom redoslijedu.
- Prenošenje povjerljivih informacija u e-poslovanju ne bi se trebalo obavljati preko UDP i TCP/IP protokola, jer oni ne osiguravaju dovoljnu zaštitu podacima.
  - Protokoli UDP i TCP/IP su više za komunikaciju koja nije povjerljiva i falsificiranjem neće oštetiti tvrtkino poslovanje.

SSH PROTOKOL

- SSH (eng. *Secure Shell*) je protokol aplikacijske razine.
- Omogućava rad na računalu koje je udaljeno.
- Koristi kriptografsku zaštitu podataka koje šalje računalnom mrežom te omogućava provjeru identiteta i cjelovitosti podataka poslanih u računalnu mrežu.
- Koristi se za kontrolu web ili drugih vrsta udaljenih servera i ostalih uređaja računalne mreže.
- Koristi digitalne certifikate i lozinke za povezivanje na udaljene uređaje.
- Nedostatak SSH protokola je što podrazumijeva da su uređaji na mreži pouzdani kad se spaja na njih, i ne provjerava pouzdanost podataka koje šalje.
- SSH protokol ima široku primjenu u e-poslovanju, za povezivanje na uređaje na računalnoj mreži.

IPSEC PROTOKOL

- IPSec (eng. *Internet Protocol Security*) sadrži skup protokola koji omogućavaju siguran prijenos podataka kroz nesigurne računalne mreže.
- Implementira se na mrežnom sloju, a koristi se za povezivanje i uspostavljanje privatnih računalnih mreža.
- Krajnje točke na računalnoj mreži, koje pakiraju i raspakiraju IPSec komunikaciju, trebaju podržavati IPSec protokol.
  - IPSec protokol zahtijeva od krajnjih korisnika da specificiraju koje kriptografske metode za šifriranje će krajnje točke u komunikaciji s IPSec protokolom koristiti.
  - Uspostavljanje komunikacije nije moguće samo s IPSec protokolom - potrebno je denfirati dodatne protokole koji mogu raditi s IPSec protokolom, kako bi se komunikacija između dvije krajnje točke mogla izvršiti.
- IPSec protokol ugrađuje se u računalnu mrežu korištenjem AH (eng. *Authentication Header*) i/ili ESP (eng. *Encapsulated Security Payload*) protokola.
  - AH ne može omogućiti privatnost IP paketa, jer ne šifrira podatke koje dobiva od protokola.
  - ESP šalje šifrirane sve podatke i dodaje provjeru identiteta na paket koji šalje.
  - AH i ESP protokoli mogu se koristiti i u brzom prijenosu podataka i u tuneliranju.
  - Kombinacija AH i ESP protokola koristi se u brzom prijenosu podataka, ako je potrebno osigurati izrazito siguran prijenos povjerljivih podataka tvrtke.

SNMP I SIP PROTOKOLI

- **SNMP (eng. *Simple Network Management Protocol*)** je protokol koji služi za upavljanje i nadziranje izvršavanja funkcija uređaja na računalnoj mreži.
  - Oslanja se na UDP protokol.
  - Učinkovitiji od ostalih protokola koji imaju slične zadaće jer se komunikacija obavlja u binarnom obliku, za razliku od ostalih sličnih protokola.
  - Prijetnje koje su usmjerene na SNMP protokol su u obliku presretanja, prisluškivanja i izmjena paketa koje SNMP protokol šalje uređajima na računalnoj mreži.
  - Uređaji koji ne podržavaju TCP/IP protokole ne mogu koristiti SNMP protokol,
    - Zbog toga su uvedeni posrednički programi (eng. *proxy agent*) koji posreduju u komunikaciji između administratora i uređaja na računalnim mrežama.
- **SIP (eng. *Session Initiation Protocol*)** je protokol koji se često koristi od strane VoIP usluge.
  - Koristi se za kontrolu perioda u kojem se razmjenjuju podaci između korisnika.
  - Kontrolira uspostavljanje veze, mogućnosti veze, podešavanja veze i upravljanje vezom u kojoj se podaci izmjenjuju između korisnika.
  - Može prepoznati vrstu uređaja koji se koriste u odvijanju komunikacije (npr. mobilni uređaj) te na osnovu te informacije odlučuje hoće li se slati samo zvuk, video i sl.

DIGITALNI POTPIS

- Digitalni potpis je digitalni kod koji služi za zaštitu poruka koje se elektronički prenose putem javne mreže.
- Osigurava tri osobine dokumenta: autentičnost, neoporecivost, izvornost.
- Svrha digitalnog potpisa:
  - Omogućiti identifikaciju pošiljaoca
  - Osigurati autentičnost sadržaja poruke
- Temelji se na kriptografiji:
  - Ne može se krivotvoriti (samo pošiljatelj zna svoj privatni ključ)
  - Autentičan je (svojstven je jednoj osobi)
  - Nije ga moguće ponovno koristiti (vrijedi samo za određeni dokument, sadrži djelove dokumenta)
  - Nepromjenjiv je
  - Ne može se poreći

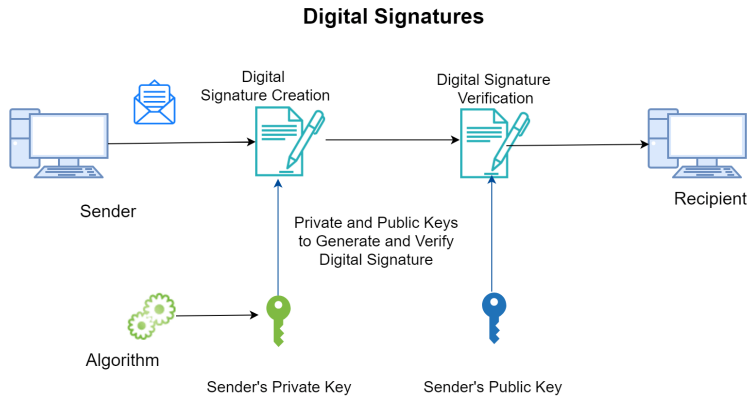
DIGITALNI POTPIS

- Razlika između slijepog i digitalnog potpisa - dokument je digitalno potpisan kod oba, ali kod slijepog ne vidimo sadržaj koji potpisujemo.
- **Zadatak:** Navedite i opišite 3 primjera upotrebe digitalnog potpisa.
- Načini realizacije digitalnog potpisa:
  1. Kriptografski sustav s tajnim ključem
  2. Kriptografski sustav s javnim ključem - RSA algoritam
  3. Algoritam digitalnog potpisa – DSA algoritam

DIGITALNI POTPIS

1. Kriptografski sustav s tajnim ključem

- Problem distribucije javnog ključa je kako povezati javni ključ s vlasnikom.
- Rješenje je izdavanje certifikata - to je elektronički dokument koji identificira pojedinca, računalo ili neki drugi entitet koji posjeduje javni ključ.
  - Treba povezati par ključeva s njihovim vlasnikom.
  - Izdavač certifikata ili *Certificate Authority* (CA).
- Elementi certifikata su: verzija, serijski broj, identifikacijska oznaka algoritma digitalnog potpisa, ime ovlaštenog certifikatora (CA), vrijeme trajanja certifikata, vlasnik javnog ključa.
  - Certifikator (CA) – kreira i opoziva certifikate te objavljuje listu aktulanih i opzvanih certifikata
  - Registrator (RA) – provjerava i jamči identitet korisnika te odobrava zahtjeve za izdavanje certifikata
  - Pošiljatelj – dobiva certifikat od CA te koristi tajni ključ za izradu digitalnog potpisa
  - Registar Certifikata – sadrži aktualne i opozvane certifikate



DIGITALNI POTPIS

2. **Kriptografski sustav s javnim ključem - RSA algoritam**

a) Hash funkcijom Ivan računa sažetak poruke koju šalje Ani

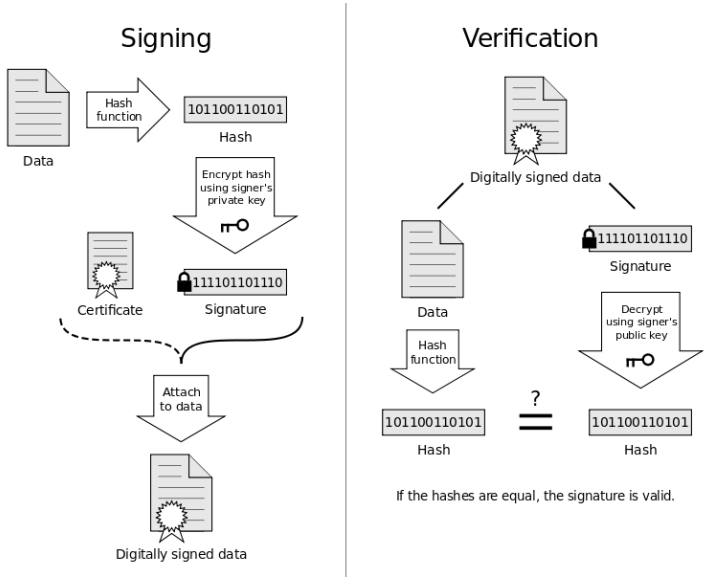
b) Ivan kriptira svojim tajnim ključem sažetak poruke i na taj način kreira digitalni potpis

c) Zajedno s originalnim dokumentom, Ivan šalje i digitalni potpis

d) Ana dobiva Ivanovu potpisanu poruku, a iz originalne poruke izračuna sažetak

e) Ana dekriptira digitalni potpis Ivanovim javnim ključem te uspoređuje dekriptirani sažetak s onim koji je sama izračunala.

   a) Ako su jednaki, Ana je sigurna da je Ivan poslao poruku i da se poruka nije mijenjala tokom slanja (integritet poruke). Ivan ne može poreći da je on poslao poruku, jer se digitalni potpis može dekriptirati samo njegovim javim ključem, a kriptirati njegovim tajnim ključem.



DIGITALNI POTPIS

3. **Algoritam digitalnog potpisa – DSA algoritam**

- Defiira proces kreiranja (generiranja) i provjere (verifikacije) digitalnog potpisa
- Razvijen od strane National Security Agency – NSA
- National Institute of Standards and Tehnology (NITS) ga je standardizirao unutar posebnog standarda za digitalni potpis (Digital Signature Standard -DSS)
- Sigurnost DSA temelji se na problemu izračunavanja diskretnog algoritma
- Koristi se ključ veličine 1024 bita te se primjenjuje na hash vrijednosti, a ne na cijeli dokument