



*Born to cheat,
forced to pass*

PITANJA ZA ZSIS

1. Definiraj sigurnost te opiši temeljne zahtjeve

Sigurnost je kontinuirani proces čijim se provođenjem osigurava određeno stanje sustava koje je definirano zahtjevima. Tri temeljna zahtjeva su: tajnost – pristup podacima moraju imati samo autorizirane osobe, cjelovitost – očuvanje integriteta podataka i raspoloživost – podaci moraju stalno biti dostupni, a kako dodatni mogu se navesti i autentičnost i neporecivost.

2. Navedi kategorije zaštite te za svaku navedi nekoliko konkretnih primjera.

Kategorije zaštite se mogu podijeliti u 3 grupe:

- a. fizičke kontrole – nadzorne kamere, zaštitari,..
- b. tehničke kontrole – vatrozid, antivirus,..
- c. administrativne kontrole – politike, pravilnici, procedure,..

3. Što sve spada u organizacijske faktore sigurnosti?

U organizacijske faktore spadaju: nedostatak budžeta, kratki rokovi, nedostatak podrške menadžmenta, nedostatak odgovarajuće procjene rizike, nepostojanje sigurnosnih procedura...

4. Zašto su sistemski i operativni zapisi bitni za sigurnost informacijskog sustava te što sve treba osigurati da bi oni bili sigurni i upotrebljivi?

Takvi zapisi su bitni jer omogućavaju rekonstrukciju i detekciju anomalija događaja, a nužno ih je držati na zasebnom mjestu kako bi se zaštitili od neovlaštenih izmjena i satovi zapisa moraju biti usklađeni kako bi se rekonstrukcija mogla pravilno odraditi.

5. Koji je temeljni alat kojeg koristi CISO i zašto (što mu on omogućuje)?

Temeljni alat CISO-a je upravljanje rizicima što uključuje procjenu i prioritizaciju rizika te na temelju prioriteta odlučiti daljnje postupanje s rizicima. Upravljanje rizicima omogućava da se odrede rizici kojima je izložena organizacija.

6. Korisnik badmin kreirao je bazu podataka nastavabp te u njoj tablice student (matBr, ime, prezime, pbr, adresa) i ispit (...). Svima je ukinuo dozvolu za spajanje na bazu te je korisniku PUBLIC ukinuo sve dozvole za shemu public. Napiši naredbe kojima će adminbp korisniku novak omogućiti:

- a. spajanje na nastavabp bazu te korištenje sheme public

`GRANT CONNECT ON DATABASE nastavabp TO admindb;`

`GRANT USAGE ON SCHEMA public TO admindb;`

- b. pregled svih podataka u tablici student osim adrese, uz mogućnost dodjele te dozvole drugim korisnicima

`GRANT SELECT(metBr, ime, prezime, pbr) ON student TO admindb WITH GRANT OPTION;`

- c. pregled, unos, izmjenu te brisanje podataka u tablici ispit

`GRANT SELECT, INSERT, UPDATE, DELETE ON ispit TO admindb;`

- d. izmjenu podataka u tablici student, ali samo za one studente koji su iz Zadra (poštanski broj im je 23 000)

`CREATE VIEW studentiZadar AS
SELECT * FROM student WHERE pbr = 23000
WITH CHECK OPTION;
GRANT UPDATE ON studentiZadar TO admindb;`

- e. korištenje već definirane uloge nastavnik

`GRANT nastavnik TO admindb;`

7. Bell – La Padula model pripada...

- a. diskrecijskom upravljanju pristupom
b. mandatnom upravljanju pristupom
c. upravljanju pristupom baziranom na ulogama

8. Kako izgleda tipičan zapis audit trail datoteke?

Audit trail treba sadržavati podatke o tome koji događaj se dogodio, tko ga je proizveo i vrijeme događanja.

9. Što omogućuju pohranjene procedure, a da nije moguće odraditi s dozvolama nad tablicama i virtualnim tablicama? Napiši naredbu kojom se korisniku novak dodjeljuje dozvola izvođenja procedure izračunaj.

Pohranjene procedure omogućavaju zaštitu podataka od neovlaštene uporabe na razini funkcija. Korisniku se dodijeli dozvola za obavljanje procedure, a time je precizno određen način na koji se obavljaju operacije nad podacima, za razliku od davanja dozvola za UPDATE i INSERT.

10. Objasni strong-star-property u mandatnoj politici pristupa u bazama podataka

Korištenjem strong-star-property korisnik ne može čitati ni pisati po objektima koji imaju ili veću ili manju razinu sigurnosti već isključivo na svojoj sigurnosnoj razini.

11. Definirajte pojam sigurnosti

Sigurnost je kontinuirani proces čijim se provođenjem osigurava određeno stanje sustava koje je definirano zahtjevima.

12. Navedite i vrlo kratko opišite tri temeljna zahtjeva sigurnosti.

Tri temeljna zahtjeva su:

tajnost – pristup podacima moraju imati samo autorizirane osobe,

cjelovitost – očuvanje integriteta podataka i

raspoloživost – podaci moraju stalno biti dostupni za pristup

13. Što je prijetnja i ranjivost

Prijetnja i ranjivost su dva preduvjeta potrebna za nastanak incidenta. Prijetnja je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu. Ranjivost je pogreška ili slabost u sustavu koja se može iskoristiti za narušavanje sigurnosti.

14. Navedite svrhu voditelja sigurnosti (CISO-a)

CISO nadzire i koordinira aktivnosti vezane uz sigurnost, inicira primjenu dobrih praksi vezanih uz sigurnost i ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

15. Ukratko objasnite što je sigurnosni zahtjev a što slučaj zloporabe te kako se modeliraju

Sigurnosni zahtjevi su nefunkcionalni zahtjevi sustava vezani uz sigurnost, primjer takvih zahtjeva su zahtjevi za kontrolom pristupa, zahtjevi za enkripcijom i sl. Slučajevi zloporabe uključuju neautoriziran dohvati i izmjenu podataka te uskraćivanje usluge. Modeliraju se nekim od procesa poput SQUARE, TRIAD, UML grafovima, use casevima i sl.

16. Navesti koja je svrha voditelja sigurnosti (CISO) u organizacijama.

CISO nadzire i koordinira aktivnosti vezane uz sigurnost, inicira primjenu dobrih praksi vezanih uz sigurnost i ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

17. Koji je temeljni akt na kojemu se temelji sigurnost organizacije te što je njegova svrha?

Politika sigurnosti informacijskog sustava, krovni dokument koji definira što za informacijski sustav znači da je siguran.

18. Zašto je potrebno nadzirati rad voditelja sigurnosti te tko obavlja tu zadaću?

Potrebno je nadzirati CISO-a zbog sprječavanja potencijalne štete zbog neodgovornog ili zlonamjernog ponašanja i zbog poboljšanja njegovog rada.

19. Objasnite osnovne postavke BLP modela (Bell- La Padula Security Model) i ilustrirajte primjerom.

BLP model se temelji na dva načela koja osiguravaju tajnost:

Simple property – subjekt može čitati iz onih objekata kojima je njegova klasa pristupa dominantna i

star-property – subjektu može pisati u objekt samo ako je njegova klasa pristupa dominantna.

20. Objasnite što je sigurnosna politika.

Sigurnosna politika je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštiti njegove tehnološke i informacijske vrijednosti.

21. Objasnite razliku između otvorene i zatvorene politike upravljanja pristupom.

Kod otvorene politike generalno je pristup podacima dozvoljen, no pristup je uskraćen za podatke za koje postoje dodatne zabrane. Kod zatvorene politike pristup podacima je dozvoljen ukoliko korisnik ima pozitivnu dozvolu.

22. Objasnite:

a. Što je sigurnost programske podrške?

Sigurnost je kontinuirani proces čijim se provođenjem osigurava određeno stanje sustava koje je definirano zahtjevima.

b. Što je sigurna programska podrška?

Za podršku možemo reći da je sigurna kada su svi sigurnosni zahtjevi ispunjeni.

c. Kada je sigurnost softverski problem?

Sigurnost postaje softverski problem radi prevencije iznimki u slučaju da dođe do pogrešaka u projektiranju, razvoju, ugradnji, nadogradnji ili održavanju aplikacije.

d. Čime se bavi softverska sigurnost?

Softverska sigurnost se bavi softverom i osigurava da pri napadu nastavlja ispravno raditi.

23. Opišite diskrecijsko i mandatno upravljanje pristupom u bazama podataka.

Diskrecijsko upravljanje pristupom je način ograničavanja pristupa objektima na temelju identiteta i/ili grupe kojoj oni pripadaju. Mandatno upravljanje je sigurnosna politika na razini sustava koja određuje tko ima pravo pristupa, a na vlasnik objekta.

24. Za svaku od navedenih faza sigurnog životnog ciklusa navedite ključne prakse:

- a. **Zahtjevi**
Definiranje sigurnosnih zahtjeva, procjena rizika
- b. **Dizajn**
Modeliranje prijetnji, analiza površine napada
- c. **Implementacija**
Statička analiza
- d. **Verifikacija**
Dinamička analiza, fuzz testiranje
- e. **Objava**
Plan odgovora na incidente, finalni pregled

MI 2021/2022

1. Detektirajte sigurnost te navedite i opišite temeljne zahtjeve.

Sigurnost je kontinuirani proces čijim provođenjem se osigurava određeno stanje (sustava i/ili podataka/informacija). Željeno stanje je definirano određenim zahtjevima. Kada su oni ispunjeni onda kažemo da je sustav siguran, u suprotnom kažemo da se desio incident tj. da je narušena sigurnost.

Temeljni zahtjevi su: Tajnost/Povjerljivost (zaštita tajnih informacija od napada), Cjelovitost/Integritet (zaštita od neovlaštenih izmjena), Raspoloživost (zaštita od uskraćivanja dostupnosti informacija ovlaštenim korisnicima)

2. Navedite podjelu kontrola u grupe te za svaku grupu navedite nekoliko konkretnih primjera kontrole.

Fizičke: kamere, zaštitari, blindirana vrata,

Tehničke: kriptografija, vatrozidi, sustavi za detekciju napada,

Administrativne kontrole: politike, pravilnici, različiti propisi kojima definiramo što znači biti siguran, kako se ljudi moraju ponašati, kako uređaji moraju biti podešeni...

3. Navedite organizacijske faktore koji utječu na sigurnost informacijskog sustava.

Organizacijski faktori: Nedostatak budžeta, Kratki rokovi, Nedostatak podrške menadžmenta, Nedostatak odgovarajuće procjene rizika, Nepostojanje sigurnosnih procedura

4. Zašto su sistematski i operativni zapisi bitni te što sve treba učiniti kako bi bili sigurni i upotrebljivi?

Jer omogućavaju rekonstrukciju događaja i detekciju neočekivanih događaja. Nužno je držati ih na zasebnom mjestu radi prevencije neovlaštenih izmjena. CISO definira način upravljanja sistemskih i operativnih zapisima: vrši nadzor, te u manjim organizacijama moguće analizira logove te traži očitovanja. Današnji trend je da tvrtke sigurnost nadziru u Sigurnosno operativnim centrima (SOC), koji kontinuirano prate poboljšavaju sigurnosno stanje i sprečavaju, detektiraju sve sigurnosne incidente.

5. Koji je temeljni alat koji CISO koristi za svoj rad i zašto (što mu omogućava)?

Upravljanje rizicima (proces propisan internim aktima). Omogućava da se odrede rizici kojima je izložena organizacija. Tu spadaju procjena rizika, mogućnost prioritizacije rizika, te na temelju toga odluka pristupanja identificiranim rizicima (da li će se prihvatiti, ovladati ili prenijeti na treću stranu, no konačnu riječ u toj odluci ima uprava organizacije).

6. Korisnik `adminbp` kreirao je bazu podataka `nastavabp` u sustav PostgreSQL te je u navedenoj bazi kreirao sljedeće tablice: `student` i `ispit` (s nekim atributima). Korisnik `adminbp` ukinuo je korisniku PUBLIC dozvolu spajanja na bazu podataka `nastavabp` i sve dozvole za shemu public u `nastavabp`, a zatim je kreirao korisnika `novak`. Napiši naredbe kojima će `adminbp` omogućiti korisniku `novak` sljedeće:

- a) Spajanje na bazu `nastava` i korištenje sheme public i `nastavabp`:
GRANT CONNECT ON DATABASE nastavabp TO novak;
GRANT USAGE ON SCHEMA public TO novak;
GRANT USAGE ON SCHEMA public TO novak;
- b) Pregled svih podataka u tablici `student` osim adrese, s tim da `novak` može dodjeljivati tu dozvolu ostalim korisnicima:
GRANT SELECT(matBr, ime, prez, pbr) ON student TO novak WITH GRANT OPTION;
- c) Pregled, unos, izmjenu i brisanje svih podataka u tablici `ispit`:
GRANT SELECT, INSERT, UPDATE, DELETE ON ispit TO novak;
- d) Izmjenu svih podataka u tablici `student`, ali samo za one n-torce koje se odnose na studente iz Zadra (poštanski broj = 2300):
CREATE VIEW zadrani AS
SELECT * FROM student WHERE pbr = 2300 WITH CHECK OPTION;
GRANT UPDATE on zadrani TO novak;
- e) Korištenje već kreirane uloge `nastavnik`:
GRANT nastavnik TO novak;

7. Model Bell-la Padula (BLP) spada u koje upravljanje pristupom?:

- a) diskrecijsko upravljanje pristupom,
- b) mandatno upravljanje pristupom,**
- c) upravljanje pristupom temeljeno na ulogama

8. Što sadrži tipični zapis datoteke za pamćenje rada korisnika (auditing)?

SQL naredba koja se izvršava, mjesto s kojeg je upućen zahtjev (terminal, IP adresa računala), identifikator korisnika koji je pokrenuo operaciju, datum i vrijeme operacije, n-torce, atributi na koje se zahtjev odnosi, stara vrijednost n-torce, nova vrijednost n-torce

9. Što omogućuju pohranjene procedure u provođenju sigurnosne politike, a da se to ne može riješiti samo dozvolama nad tablicama i nad virtualnim tablicama? Napišite naredbu kojom će se korisniku `novak` omogućiti korištenje procedure `izracunaj`.

Omogućuje zaštitu podataka od neovlaštene uporabe na razini funkcija.

GRANT EXECUTE ON izracunaj TO novak

10. Objasnite princip strong-star-property kod mandatne politike pristupa u bazama podataka.

Korisnik može pisati isključivo na svojoj razini, nije moguće pisati u objekte koje mogu pročitati subjekti s nižom razinom
- spriječeno propuštanje informacija.

UVOD

SolarWinds

Ubačen maliciozni kod u programsku podršku Orion IT za nadzor i upravljanje mreža napad slučajno otkrila tvrtka FireEye

Primjer **napada na dobavni lanac (engl. supply chain attack)**

Colonial Pipeline

ucjenjivački napad

Tvrtka koja obavlja transport nafte i derivata uz jugoistočnu obalu SAD-a •

Ulaz u mrežu tvrtke napravljen pomoću **kompromitiranih vjerodajnica** •

Faktori koji utječu na sigurnost IS-a

- Ljudski faktori
 - Nedostatak edukacije u području sigurnosti
 - Nedostatak komunikacije po pitanju sigurnosti
 - Nedostatak svijesti
 - Nedostatak kulture
 - Neodgovarajuće ponašanje
- Organizacijski faktori
 - Nedostatak budžeta
 - Kratki rokovi
 - Nedostatak podrške menadžmenta
 - Nedostatak odgovarajuće procjene rizika
 - Nepostojanje sigurnosnih procedura
- Tehnološki faktor
 - Ranjivosti u IT imovini
 - Nedovoljni ili neodgovarajući sigurnosni mehanizmi

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

Kada su zahtjevi ispunjeni, kažemo da je sustav i/ili informacija sigurna. Ako neki od zahtjeva nije ispunjen, kažemo da se desio incident, odnosno, da je narušena sigurnost.

Tri temeljna zahtjeva

- **Tajnost/Povjerljivost**
- **Cjelovitost/Integritet**
- **Raspoloživost**

Dodatni zahtjevi

- **Autentičnost**
- **Neporecivost**

Da bi se desio incident moraju postojati dva preduvjeta: **ranjivost i prijetnja**

Prijetnja (engl. threat) je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu.

- Izvori prijetnji su ljudski (**namjerni ili slučajni**) ili prirodni

Načini postizanja sigurnosti

-Tako da uklonimo prijetnje i/ili ranjivosti

Kako djelovati na prijetnje?

- Djelovanje na motiv
- Podizanje cijene

Ranjivosti se mogu **ukloniti ili ublažiti kontrolama**

Kontrole su zaštite koje primjenjujemo u sustavu

Sve kontrole svrstavamo u tri velike grupe

- **Fizičke kontrole** – kamere, zaštitari, ograde, ... •
- **Tehničke kontrole** – vatrozidi, antivirus, ... •
- **Administrativne kontrole** – politike, procedure, pravilnici

Informacijski sustav je bilo koji organizirani sustav za prikupljanje, organizaciju, pohranu i razmjenu informacija

- Informacijski sustav ne uključuje nužno računala i/ili računalnu mrežu
- Iako su današnji informacijski sustavi nezamislivi bez njih
- Informacijski sustav uključuje i ljude i procese
- Informacijski sustav uključuje sve na čemu se nalaze informacije značajne za tvrtku
- Uz napomenu: koje nisu javno objavljene!

Informacijska tehnologija (IT) je primjena računala i telekomunikacijske opreme za pohranu, dohvata, prijenos i obradu podataka, često u poslovnom kontekstu.

U IT-ju temeljni zahtjev je tajnost •

Informacija ne smije biti poznata neovlaštenim osobama •

U Operational Technology OT-u temeljni zahtjev je raspoloživost

prvenstvena zadaća je upravljanje fizičkim procesima

Upravljanje sigurnošću

Voditelj sigurnosti informacijskog sustava – CISO

- osoba koja razumije sigurnost i ne bavi se operativnim detaljima
- pri vrhu organizacijske strukture - jedna od zahtjevnijih zadaća CISO-a je komunikacija s Upravom
- Voditelj sigurnosti zadužen je za cjelokupnu sigurnost (fizičku, informacijsku, prijevare)

Faza 1 (1990-te – 2000)

- uvjerenje da informacije u tvrtki nisu nikome interesantne
- ograničena sigurnost, naglasak na lozinkama i kontroli pristupa

Faza 2 (2000 – 2004)

- Pojava legislative za zaštitu privatnosti i podataka
- Prvi put se zahtjevalo da postoji netko zadužen za sigurnost

Faza 3 (2004 – 2008)

- Problem s ispunjavanjem regulative
- CISO orijentiran na rizike, naglasak na „mekim vještinama”, još uvijek dio IT-ja

Faza 4 (2008 – 2016)

- Sigurnost svjesna prijetnji, društvene mreže, mobilni uređaji, računarstvo u oblaku
- CISO treba marketing, politiku, tehnologiju

Faza 5 (2016 – 2020-te)

- Privatnost dobija na značenju (GDPR), „outsource”, dobavni lanac
- CISO svjestan privatnosti i podataka

SVRHA CISO-a

- Nadzire i koordinira aktivnosti vezane uz sigurnost informacijskog sustava.
- Inicira primjenu dobrih praksi i prihvaćenih standarda vezanih uz sigurnost informacijskog sustava.
- Ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

Zadaće CISO-a

- Izrada internih akata
- Provjera provođenja internih akata
- Upravljanje rizicima – temeljni alat u radu
- Upravljanje incidentima – postupak bi trebao biti definiran aktima
- Edukacija i osvještavanje
- Izvješćivanje uprave i nadzornog odbora
- Rad s vanjskim suradnicima
- Analiza sigurnosnih potreba
- Sudjelovanje u bitnim aktivnostima planiranja poslovanja i klasifikacije informacija
- Sudjelovanje u razvoju i održavanju IT-a
- definira način upravljanja sistemskih i operativnim zapisima (logovima)

Problemi (i izazovi) s kojima se CISO susreće

- Vrlo dinamična okolina koju je teško pratiti
- Evaluacija rizika raznih tehnologija
- Koordiniranje aktivnosti s organizacijskom jedinicom informacijske tehnologije i unutarnjom revizijom
- Operativni i strateški poslovi

Kompetencije CISO-a

- Upravljačke vještine
- Poslovne vještine
- Stalno usavršavanje
- „Soft skills”
- Vještine i znanja iz sigurnosti informacijskih sustava
- Planiranje oporavka od katastrofičnih događaja
- Sposobnost istraživanja sigurnosnih incidenata

Interni akti

Temeljni akt je **Politika sigurnosti informacijskog sustava**

krovni dokument koji definira što za informacijski sustav znači da je siguran
temelj za ostale akte

Vrste internih akata:

1. Politika
2. Pravilnik
3. Procedura

Sadržaj politike

- Pregled – o čemu je politika
- Svrha – zašto je politika potrebna
- Obuhvat – što sve politika obuhvaća
- Kome je namijenjena – tko je sve obvezan djelovati temeljem politike
- Politika – Temeljni dio dokumenta koji navodi što treba biti učinjeno
- Definicije – Pojmovi koji se upotrebljavaju u politici
- Verzioniranje – Vođenje evidencija o promjenama

Nadzor sigurnosti

Sigurnosno operativni centar - centralizirana funkcija unutar organizacije koja korištenjem ljudi, procesa i tehnologije kontinuirano prati i poboljšava sigurnosno stanje organizacije te sprečava, detektira, analizira i odgovara na sigurnosne incidente

Nadzor rada CISO-a

- Sprečavanje potencijalne štete zbog neodgovornog ili zlonamjernog ponašanja

Tu dužnost obavljaju: unutarnja i vanjska revizija, osoba/funkcija nadređena voditelju sigurnosti - CEO, CIO, CSO

Sigurnost programske podrške

- Inženjerstvo softvera koji će pri napadu nastaviti ispravno raditi

Sigurnosna programska podrška

- Računalni programi i knjižnice za potporu sigurnosti računala ili mreže

Osiguranje softvera

- Razina pouzdanosti da softver nema ranjivosti

Sigurnost aplikacije

Mjere poduzete tijekom životnog ciklusa aplikacije radi prevencije iznimki u odnosu na politiku sigurnosti aplikacije ili sustava uslijed pogrešaka u projektiranju, razvoju, ugradnji, nadogradnji ili održavanju aplikacije

Kada je sigurnost softverski problem ?

- zahtijeva promjenu implementacije ili dizajna (softvera)

Uzroci problema softverske sigurnosti

- nedostatak svijesti, značaja
- nedostatak znanja
- Sigurnost kao sekundarna briga

Sigurnosni ciljevi : CIA

1. Confidentiality (povjerljivost, tajnost)
2. Integrity (integritet, cjelovitost)
3. Availability (dostupnost)

Realizacija ciljeva: AAAA

- Autentifikacija (authentication)
- Autorizacija (authorization)
- Nadzor, praćenje (auditing)
- Djelovanje (action)

Životni ciklus sigurnog softvera

Analiza: sigurnosni zahtjevi, procjena rizika, ...

Dizajn: modeliranje prijetnji, analiza površine napada, ...

Implementacija: statička analiza, ...

Verifikacija: dinamička analiza, fuzz testiranje, ...

Isporuka: plan odgovora na incidente, finalni pregled

*ispitno pitanje

Prije početka rada:

- poduka svih članova da bi znali osnove i ostali u trendu
- barem jedan tečaj godišnje

1. Analiza

- rano postavljanje pouzdanih (trustworthiness) zahtjeva
- specifikacija minimalnih zahtjeva na sigurnost aplikacija
- uspostava minimalno prihvatljivih razina kvalitete sigurnosti i privatnosti
- tim dokazuje sukladnost kroz Final Security Review (FSR)
- procjena rizika

2. Dizajn

- što ranije uklanjanje problema sigurnosti i privatnosti
- izbjegavati „dodavanje“ sigurnosti na kraju razvoja
- opisati kako sigurno ugraditi funkcionalnost
- redukcija rizika smanjenjem prostora za napad
 - isključenjem ili restrikcijom pristupa na sistemske resurse
 - primjenom principa najmanjeg prava
 - uslojavanjem
- modeliranje prijetnje - **glavna aktivnost dizajna**

sigurne mogućnosti – opća funkcionalnost koju treba osigurati (npr. unos, robusnost)

sigurnosne mogućnosti – funkcionalnost koja se odnosi na sigurnost (npr. autentifikacija)

3. Implementacija

- odabir alata i okruženja
- analiza korištenih funkcija i API-ja s obzirom na sigurnost
- statička analiza - osigurava inspekciju programskog koda, ali ju ne može zamijeniti!!

4. Verifikacija

- dinamička analiza
- *fuzz testing* - nastoji se izazvati zastoj unosom neispravnih ili pseudoslučajnih podataka
- ponovni pregled modela prijetnji i mjerjenje površine napada

5. Isporuka

- definiranje plana odziva na incidente
- Final Security Review (FSR) - promišljena provjera svih sigurnosnih aktivnosti, prije objave
 - ishodi: passed FSR | passed FSR with exceptions | FSR with escalation
- **security advisor** potvrđuje (temeljem FSR i šire) da su zahtjevi zadovoljeni
- zasebno se potvrđuju komponente utjecaja na privatnost
- arhiviranje

Opcionalne aktivnosti

- Nadzor, ručna inspekcija koda (code review)
- Penetracijsko testiranje
- Analiza povredivosti sličnih aplikacija

RACI tablica

akronim (Responsable, Accountable, Consulted, Informed)

Sigurnosni zahtjevi

nefunkcionalni

- Procjene vrijednosti sustava – vrijednost sustava i podataka
- Zahtjevi za kontrolu pristupa – ograničenje na pristup podacima
- Zahtjevi za enkripcijom i autentifikacijom – kako, gdje i kada
- Zahtjevi za kontrolom virusa

Neki mogu *zahtijevati funkcionalnost*, npr.: duljina korisničkog unosa, validacija podataka

Izvori zahtjeva

- Korisnici
- Sigurnosna implikacija funkcionalnosti
- Regulatorna sukladnost

Alati za softversku sigurnost (ne mrežnu)

Microsoft SDL i derivati

- Attack Surface Analyzer – smanjenje površine napada
- Microsoft Threat Modeling Tool – modeliranje prijetnji
- MiniFuzz basic file fuzzing tool – fuzz testiranje
- Regular expression file fuzzing tool – testiranje potencijalnih DoS ranjivosti

Statička analiza

- StyleCop <https://stylecop.codeplex.com/> # slično, FxCop
- CodeSmart <http://www.axtools.com/>
- NDepend <http://www.ndepend.com/>
- PMD Java, Checkstyle, FindBugs+Find Security Bugs

SIGURNOST BAZA PODATAKA 1

Baza podataka - skup podataka koji su pohranjeni i organizirani tako da mogu zadovoljiti zahtjeve korisnika.

Sustav za upravljanje bazama podataka SUBP je programski sustav koji:

- može istovremeno upravljati s više baza podataka
- više korisnika/aplikacija uz osiguravanje sigurnosti i integriteta baze podataka
- temelji se na odabranom modelu podataka (hijerarhijski, mrežni, relacijski, objektno-relacijski, objektno-orientirani, ...)

Zadaće SUBP-a

- trajna pohrana podataka (persistent storage)
- osiguravanje programskog sučelja (programming interface)
 - DDL - Data Definition Language
 - DML - Data Manipulation Language
- optimiranje metoda pristupa podacima
- zaštita podataka
 - integritet podataka (integrity)
 - pristup podacima - autorizacija, sigurnost (security)
 - potpora za upravljanje transakcijama
 - upravljanje istodobnim pristupom (concurrency control)
 - obnova u slučaju razrušenja (recovery)

različite skupine korisnika:

- korisnici koji često koriste programirana sučelja (npr. službenici u banci)
- korisnici koji povremeno pristupaju bazi koristeći upitni jezik
- sofisticirani korisnici koriste je na složeniji način (npr. inženjeri, znanstvenici)
- Administratori
 - administrator poslužitelja baze podataka (database server administrator – DBSA)
 - instaliranje i nadogradnja SUBP-a; kreiranje novog korisnika; autorizacija na razini SUBP-a
 - administrator baze podataka (database administrator - DBA)
 - autorizacija na razini baze podataka (provodenje sigurnosne politike)
 - dodjeljivanje i ukidanje ovlasti korisniku baze podataka
 - dodjeljivanje sigurnosne klasifikacijske razine korisniku u višerazinskom sigurnosnom sustavu, u skladu s politikom organizacije

Oblici narušavanja sigurnosti baze podataka su:

- neovlašteno čitanje,
- izmjena
- uništavanje podataka

Posljedice:

- krađa ili prijevara
- gubitak tajnosti
- gubitak privatnosti
- gubitak raspoloživosti

sigurnost baze podataka se osigurava zaštitom na nekoliko razina:

- na razini SUBP
- na razini operacijskog sustava
 - spriječiti pristup radnoj memoriji računala ili datotekama u kojima SUBP pohranjuje podatke
- na razini računalne mreže
- fizička zaštita
- na razini korisnika

Defense-in-depth strategija

- zaštita u više slojeva
- probaj jednog sloja ne mora značiti i narušavanje sigurnosti podataka iz baze podataka
- nužna zaštita unutar baze podataka, čak i ako je implementiran poseban sustav zaštite baze podataka izvan baze podataka
- Svaki pokušaj neovlaštenog pristupa sustavu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, a ako je to moguće i mjestom s kojeg je takav pristup pokušan.

neki od postupaka kojima je bazu podataka moguće učiniti sigurnijom:

- ograničiti pristup važnim resursima - vatrozidi; upravljanje pristupom; antivirusna zaštita
 - patches
 - sustavi za otkrivanje i sprječavanje upada
- onemogućiti nepotrebne komponente i servise sustava za upravljanje bazama podataka
- ukloniti/onemogućiti nepotrebne korisničke račune i lozinke
- izvoditi procese baze podataka pod namjenskim, neprivilegiranim korisničkim računom

Aspekti zaštite podataka

- zakonski, socijalni i etički aspekt
 - ima li vlasnik baze podataka zakonsko pravo na prikupljanje i korištenje podataka
- strategijski aspekt
 - tko definira pravila pristupa
- operativni aspekt
 - kako osigurati poštivanje pravila

GDPR - General Data Protection Regulation

načelo najmanje ovlasti (least privilege)

- korisnik ima minimalan skup dozvola koje su neophodne za njegov trenutni zadatak
- pojedinac ima različite razine ovlasti u različito vrijeme, ovisno o zadaći ili funkciji koju obavlja

razdvajanje dužnosti (separation of duty - SoD)

- osjetljive zadatke u cijelosti ne može obaviti samo jedan korisnik

Mehanizmi zaštite na razini SUBP

- identifikacija i dokazivanje autentičnosti
- upravljanje pristupom
- šifriranje podataka
- praćenje pristupa podacima

- maskiranje podataka

Integritet baze podataka (database integrity) - operacije nad podacima koje korisnici obavljaju su ispravne (tj. uvijek rezultiraju konzistentnim stanjem baze podataka) • "podaci se štite od ovlaštenih korisnika,"

Sigurnost baze podataka (database security) - korisnici koji obavljaju operacije nad podacima su ovlašteni za obavljanje tih operacija • "podaci se štite od neovlaštenih korisnika"

U oba slučaja:

-

- moraju biti definirana pravila koja korisnici ne smiju narušiti •
- pravila se pohranjuju u rječnik podataka •
- SUBP nadgleda rad korisnika i osigurava poštivanje pravila

administrator sustava **omogućuje korisniku pristup sustavu** definiranjem jedinstvenog identifikatora korisnika (user name, user ID, login ID) i pripadne lozinke (password)

SQL-sjednica (SQL-session) je kontekst u kojem jedan korisnik obavlja niz SQL naredbi putem jedne veze (SQL-Connection) prema sustavu za upravljanje bazama podataka

- SQL-sjednica započinje kada korisnik ostvari vezu sa SUBP
- SQL-sjednica završava kada korisnik prekine vezu

```
CREATE USER name [ [ WITH ] option [ ... ] ]
where option can be:
    SUPERUSER | NOSUPERUSER
    | CREATEDB | NOCREATEDB
    | CREATEUSER | NOCREATEUSER
    | [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'
    | INHERIT | NOINHERIT
    | ...
```

Upravljanje pristupom - niz postupaka kojima se utvrđuje i evidentira pokušaj pristupa, te odobrava ili odbija pristup na temelju unaprijed utvrđenih pravila

sigurnosna politika - pravila pristupa na visokoj razini (zakonski, socijalni, etički aspekt)

- temeljena na načelu treba-znati (need-to-know), kompetentnosti, nadležnosti, sukobu interesa...
- na nju mogu utjecati zakonska i etička pitanja, politike na državnoj ili korporativnoj razini ...•
- dinamična - mijenja se u skladu s promjenama poslovnih faktora, regulativa i uvjeta u okruženju•
- problem preslikavanja nejasnih i dvomislenih zahtjeva u dobro definirana i jednoznačna pravila

sigurnosni model - formalni prikaz sigurnosne politike (strategijski aspekt)

sigurnosni mehanizam - (operativni aspekt) funkcije kojima je implementirano upravljanje pristupom

reference monitor - komponenta koja upravlja svakim pokušajem pristupa i utvrđuje je li u skladu sa sigurnosnom politikom

autorizacija - postupak evidentiranja pravila pristupa

Elementi sustava za upravljanje pristupom

- korisnik – entitet koji koristi računalni sustav (osoba, uređaj)
 - sjednica (session) - instanca dijaloga korisnika sa sustavom
- subjekt – aktivni entitet koji može inicirati zahtjev za obavljanje operacija na objektima
 - proces koji djeluje u ime korisnika
 - korisnik može imati više aktivnih subjekata
- objekt - entitet sustava na kojem može biti obavljena operacija
- operacija - aktivan proces pozvan od strane subjekta, koji nakon poziva izvršava funkcije
- dozvola (pravo pristupa, ovlast) određenog načina pristupa objektu u sustavu
 - kombinacija objekta i operacije
 - pozitivna dozvola - ako ne postoji, zatraženi pristup je odbijen
 - negativna dozvola (tj. zabrana) - ako postoji, zatraženi pristup je odbijen

klasični pristupi upravljanja pristupom:

- zatvorena politika - dozvoljen pristup za koji postoji (pozitivna) dozvola
- otvorena politika - uskraćen pristup za koji postoji zabrana (tj. "negativna dozvola")
 - ako zabrana ne postoji, pristup je dozvoljen

problemi kod kombiniranog korištenja pozitivnih i negativnih dozvola:

- nepotpunost - za pristup nije specificirana dozvola • može se izbjegići definiranjem prepostavljene politike
- nekonzistentnost - za pristup postoji i negativna i pozitivna dozvola • može se izbjegići definiranjem politike razrješavanja konflikata

Diskrecijsko upravljanje pristupom

- upravljanje pristupom na temelju:
 - identiteta korisnika koji zahtijeva pristup i
 - 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>
- podaci o dodijeljenim dozvolama pohranjuju se u rječnik podataka
- prije obavljanja svake operacije, SUBP provjerava ima li korisnik dozvolu za obavljanje operacije nad objektom (upravljanje pristupom)

Upravljanje pristupom u SQL-u

Mehanizmi upravljanja pristupom

- naredbe za dodjeljivanje (GRANT) i ukidanje dozvola (REVOKE)
- virtualne tablice (view)
- pohranjene procedure
- modifikacija upita

Objekti

- tablica (table) [2]
- atribut (stupac tablice, column) [2]
- virtualna tablica (pogled, view) [2]
- pohranjena procedura [2]
- baza podataka (neki sustavi, npr. IBM Informix)

Vlasnik objekta - implicitno dobiva dozvole za obavljanje svih vrsta operacija nad objektom

SHEME

PostgreSQL: [2]

- Baza podataka sadrži jednu ili više shema [2]
- Sheme sadrže tablice, virtualne tablice (, funkcije, ...) [2]
- Različite sheme mogu sadržavati istoimene tablice [2]
- Sheme analogue s:
 - Mapama u datotečnom sustavu (s tim da se ne mogu grijezditi) •
 - Imenskim područjima (namespaces) u programskim jezicima

♦ Stvaranje:

```
CREATE SCHEMA student;

CREATE TABLE student.postavke (
    username TEXT primary key,
    cm_skin TEXT not null
);
```

♦ Pristup:

```
-- schema.table
-- database.schema.table
SELECT * FROM student.postavke
```

♦ Brisanje:

```
DROP SCHEMA student;
-- cannot drop schema student because
-- other objects depend on it
DROP SCHEMA student CASCADE;
-- obrisani i sadržani objekti!!
```

Trenutne postavke za SSP se mogu dobiti sljedećom naredbom:

SHOW search_path;	search_path
	"\$user", public

- Kao trenutnu shemu PostgreSQL će odrediti shemu "\$user", ako takva postoji [2]
- Ako ne postoji, trenutna shema postaje public

Ako je CURRENT_USER npr. tibor, tada je "\$user" shema koja se zove tibor

Vrste dozvola u SQL-u na razini baze podataka - dbPrivilege

- CONNECT – spajanje na bazu
- CREATE – stvaranje shema

Vrste dozvola u SQL-u na razini sheme - (schemaPrivilege)

- USAGE - Nužan preduvjet za pristupanje objektima sadržanim u shemi.
- CREATE - Dozvoljava stvaranje novih objekata (tablice, funkcije, ...) u shemi.
- Korisnik nema dozvolu pristupa nijednom objektu sheme kojoj nije vlasnik

Vrste dozvola u SQL-u na razini [virtualne] tablice - (tablePrivilege)

- **SELECT, UPDATE, INSERT, DELETE, ALL PRIVILEGES(sve)**

SQL naredbe za dodjeljivanje i ukidanje dozvola

- **GRANT/REVOKE {privilegija} ON {db/schema/table} {ime} TO/FROM {korisnik}**

Zaštita i sigurnost informacijskih sustava

Uvod

prof. dr. sc. Krešimir Fertalj
izv. prof. dr. sc. Stjepan Groš
prof. dr. sc. Boris Vrdoljak

Motivacija

- Kontinuirani niz vijesti o napadima na organizacije
 - Mnogi incidenti se ni ne prijavljuju
- Stav je da nije pitanje **AKO** će se nekakav napad desiti već **KADA** će se desiti

Primjeri nekih značajnijih napada (1)

- SolarWinds
 - Prosinac 2020
 - Napadnuta tvrtka SolarWinds(!?)
 - Ubačen maliciozni kod u programsku podršku *Orion IT* za nadzor i upravljanje mreža
 - Mjeseci prošli prije nego je napad slučajno otkrila tvrtka **FireEye**
 - Primjer napada na dobavni lanac (engl. supply chain attack)
 - Ogroman broj žrtava, Microsoft, agencije američke Vlade, ...

Primjeri nekih značajnijih napada (2)

- *Colonial Pipeline* ucjenjivački napad
 - Svibanj 2021
 - Tvrtka koja obavlja transport nafte i derivata uz jugoistočnu obalu SAD-a
 - Vojne baze ovise o toj tvrtci
 - Tvrtka je dio kritične infrastrukture
 - Ulaz u mrežu tvrtke napravljen pomoću kompromitiranih vjerodajnica
 - Plaćena otkupnina, ali svejedno je oporavak potrajan
 - Dio otkupnine kasnije vraćen



Neki zaključci na temelju primjera

- Sve organizacije danas jako ovise o svojim informacijskim sustavima
 - Ako je narušena sigurnost informacijskog sustava tvrtka može pretrpjeti velike štete ili čak propasti.
 - To vrijedi čak i za industrijske sustave!
- Organizacije su međusobno ovisne
 - Napad na jednu organizaciju može imati katastrofalne posljedice po druge organizacije

I još neke činjenice o organizacijama

- Organizacije imaju kompleksne IT sustave
 - Teško je znati sve što se događa u tim sustavima
- Tehnologija se brzo mijenja i postaje sve kompleksnija
- Ljudi su bitna karika sustava
 - ... a ljudi grijše

O napadačima

- Jako ih je puno različitih sposobnosti, kompetencija i motivacija
- Vrlo brzo se prilagođavaju situaciji
- Teško ih je pronaći i uhvatiti
 - Najčešće nam je s druge strane nepoznata osoba ili grupa
- U pitanju je **inteligentni suparnik**

Problem s kojim se bavimo

- Kako zaštititi organizaciju od napada, u uvjetima
 - ... u kojima ne znamo što nam sve prijeti
 - ... imamo kompleksnu organizaciju gledajući tehnologiju i poslovne procese
 - ... ne poznajemo cijelu organizaciju, a možda nemamo ni kontrolu nad njom
 - ... napadači se stalno mijenjaju i poboljšavaju
 - ... tehnologija i poslovni zahtjevi idu naprijed jako brzo
 - ... imamo ograničene resurse na raspolaganju za obranu
- **OVO NIJE (SAMO) TEHNIČKO PITANJE**

Faktori koji utječu na sigurnost IS-a

- Možemo ih razvrstati u tri grupe
 - Ljudski faktori
 - Organizacijski faktori
 - Tehnološki faktor

Ljudski faktori

- Nedostatak edukacije i treninga u području sigurnosti
- Nedostatak komunikacije po pitanju sigurnosti
- Nedostatak kulture
 - Dijeljenje korisničkog računa, povlašteni pristup bez potrebe

Organizacijski faktori

- Nedostatak budžeta
- Kratki rokovi
- Nedostatak podrške menadžmenta
- Nedostatak odgovarajuće procjene rizika
- Nepostojanje sigurnosnih procedura

Tehnološki faktori

- Kompleksnost sustav
- Ranjivosti u IT imovini
- Nedovoljni ili neodgovarajući sigurnosni mehanizmi
 - primjerice vatrozidi, IDS-ovi, antivirusna podrška, lozinke, šifriranje, itd.

Teme predavanja

- Upravljanje sigurnošću informacijskog sustava
- Standardi sigurnosti informacijskog sustava
- Životni ciklus sigurnog razvoja sustava
- Analiza rizika i upravljanje rizikom informacijskog sustava
- Oblikovanje prijetnji
- Planiranje kontinuiteta poslovanja za nepredviđene slučajeve
- Sigurnost baza podataka
- Revizije informacijskog sustava
- Sigurnost elektroničkog poslovanja

Način polaganja ispita

- Kontinuirano praćenje nastave
 - Pohađanje nastave – 6 bodova
 - Međuispit – 47 bodova
 - Završni ispit – 47 bodova
 - Nema minimuma na svakoj od navedenih komponenti
- Ispitni rok
 - Pismeni ispit – 100 bodova
- **Napomena:** nema bodovnog praga na međuispitu, završnom ispitu ili pismenom ispitu

Ocjena	Bodova
Izvrstan	87,50
Vrlo dobar	75,00
Dobar	62,50
Dovoljan	50,00

Literatura

- Slajdovi će biti dostupni na stranicama predmeta
- Tijekom semestra, vezano uz specifične teme, dobijat ćete još literature

Neki izvori informacija (1)

- Stručne konferencije
 - BlackHat USA/EU/Asia/Israel [www.blackhat.com]
 - RSA Conference
- Znanstvene konferencije
 - ACM Conference on Computer and Communication Security
 - USENIX Security
 - IEEE Symposium on Security and Privacy

Neki izvori informacija (2)

- Blogovi
 - Krebs On Security, Schneier on Security, A Few Thoughts on Cryptographic Engineering
 - Symantec, Microsoft, FireEye, Kaspersky, ...
- Organizacije, udruge i certifikacije
 - SANS, ISACA, ISC2, MITRE
 - Honeynet organization
- Twitter

Osnovni pojmovi – ponavljanje

Ponavljanje – pojam sigurnosti

- Primjeri nekih izjava koje uključuju pojam „sigurnost”
 - Lozinke su sigurne
 - Web stranice tvrtke su sigurne
 - Poslužitelj je siguran
 - Tvrtka je sigurna
- Pojam „sigurnost” je složen i kontekstno osjetljiv

Ponavljanje – definicija sigurnosti

- Sigurnost (engl. security)
 - **Kontinuirani proces** čijim provođenjem se osigurava određeno stanje (sustava i/ili podataka/informacija). Željeno stanje je definirano određenim **zahtjevima**.
 - Kada su zahtjevi ispunjeni, kažemo da je sustav i/ili informacija sigurna. Ako neki od zahtjeva nije ispunjen, kažemo da se desio **incident**, odnosno, da je **narušena sigurnost**.
- U ovom predmetu zanima nas **sigurnost informacijskog sustava**
 - uključuje mnoga područja sigurnosti

Ponavljanje – osnovni sigurnosni zahtjevi

- Bez obzira o kojoj sigurnosti govorimo i dalje su bitni sigurnosni zahtjevi
- Tri temeljna zahtjeva
 - Tajnost/Povjerljivost (engl. secrecy, confidentiality)
 - Cjelovitost/Integritet (engl. integrity)
 - Raspoloživost (engl. availability)
- Dodatni zahtjevi
 - Autentičnost (engl. authenticity)
 - Neporecivost (engl. non-repudation)

Ponavljanje – Prijetnje

- Da bi se desio incident moraju postojati dva preduvjeta: ranjivost i **prijetnja**
- Prijetnja (engl. threat) je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu.
 - Izvori prijetnji su ljudski (napadači) ili prirodni (potres, nestanak struje);
 - Dodatno ljudski izvori mogu biti namjerni (napadači) ili slučajni (nepažnja osobe)

Ponavljanje – Ranjivosti

- Da bi se desio incident moraju postojati dva preduvjeta: **ranjivost** i prijetnja
- Ranjivost (engl. vulnerability) je pogreška ili slabost u dizajnu sustava, implementaciji, upotrebi ili upravljanju koja se može iskoristiti za narušavanje sigurnosti sustava ili informacije.
 - Pogreške u programskoj podršci (engl. bugs), propusti u protokolima, kriva upotreba programske podrške ili nekog sustava

Načini postizanja sigurnosti

- Tako da uklonimo prijetnje i/ili ranjivosti

Kako djelovati na prijetnje?

- Dva su osnovna pristupa
 - Djelovanje na motiv i podizanje cijene djelovanja
- Djelovanje na motiv
 - Ako imamo nešto što napadač želi, riješimo se toga
 - Nije uvijek primjenjivo
- Podizanje cijene
 - Otežavanje djelovanja napadaču – uvođenje zaštitnih mjera
 - Prijetnja visokim kaznama – teško je pronaći napadače

Djelovanje na ranjivosti

- Ranjivosti se mogu ukloniti ili ublažiti **kontrolama**
 - Kontrole su zaštite koje primjenjujemo u sustavu
 - Sve kontrole svrstavamo u tri velike grupe
 - Fizičke kontrole – kamere, zaštitari, ograde, ...
 - Tehničke kontrole – vatrozidi, antivirus, ...
 - Administrativne kontrole – politike, procedure, pravilnici

Pojam informacijskog sustava

- Što je informacijski sustav?
 - Odgovor na to pitanje nije lako dati, mnoštvo je mogućih definicija
- Za naše potrebe bit će sasvim dovoljna sljedeća definicija

Informacijski sustav je bilo koji organizirani sustav za prikupljanje, organizaciju, pohranu i razmjenu informacija

Neke posljedice/zanimljivosti definicije

- Informacijski sustav ne uključuje nužno računala i/ili računalnu mrežu
 - Iako su današnji informacijski sustavi nezamislivi bez njih
- **Informacijski sustav uključuje**
 - Ljude i procese
 - Sve na čemu se nalaze informacije značajne za tvrtku
 - Uz napomenu: koje nisu na javnim mjestima!

Informacijska (i komunikacijska) tehnologija

- Čest pojam (i skraćenica) u kontekstu informacijskih sustava
 - IT, ICT
- Nema općeprihvaćenih niti univerzalnih definicija navedenih pojmove
 - Svaka definicija ima svojih prednosti i nedostataka (a neke uopće nisu dobre!)
 - Ovisno o potrebi koristi se neka od raspoloživih definicija

Definicija IT/ICT pojma

- Jedna potencijalna definicija sasvim zadovoljavajuća za naše potrebe

Informacijska tehnologija (IT) je primjena računala i telekomunikacijske opreme za pohranu, dohvat, prijenos i obradu podataka, često u poslovnom kontekstu.

- Dakle, IT je sastavni dio (čak i temelj) IS-a
 - Slijedi da je sigurnost IS-a usko vezana uz sigurnost IT-a

Operativna tehnologija

- Engl. Operational Technology (OT)
- Koristi se u upravljačkim sustavima
 - Koristi iste tehnološke temelje kao IT, ali prvenstvena zadaća je upravljanje fizičkim procesima
- Sadrži elemente koji nisu uobičajeni u IT-ju
 - PLC, SCADA, RTU, ...
- Govorimo o industriji, različitim opskrbnim sustavima, ...

IT vs. OT

- U IT-ju temeljni zahtjev je *tajnost*
 - Informacija ne smije biti poznata neovlaštenim osobama
 - Svaka organizacija ima IT
- U OT-u temeljni zahtjev je *raspoloživost*
 - Prenose se mjerena i upravljačke naredbe
 - Samo neke organizacije imaju OT
 - Niz specifičnosti u odnosu na IT
- Iako ćemo govoriti u nastavku samo o IT-ju, ne zaboravite da postoji i OT

Zašto će sigurnost dugo biti problem?

- Sustavi postaju sve kompleksniji
- Paradoks je da je jeftinije izgraditi složen sustav nego jednostavan
 - Složen sustav se potom prilagođava da izvršava jednostavnu funkcionalnost
 - Primjer: CPU-ovi
- Zbog korištenja složenih sustava napadači mogu dobiti i drugačija ponašanja

Hvala!

Zaštita i sigurnost informacijskih sustava

Upravljanje sigurnošću

izv. prof. dr. sc. Stjepan Groš

Kako se zaštитiti od incidenata?

- U uvodu smo napravili pregled nekih incidenata.
 - Možemo nabrajati još mnoštvo drugih incidenata
- Incidenti su raznoliki
 - Ovise o prijetnji, onome što organizacija posjeduje, infrastrukturi koju koristi
 - Prilično složena situacija
- PITANJE JE KAKO SE ZAŠTITI?
 - Pretpostavimo da ste dobili zadaću zaštитiti neku organizaciju/tvrđtu od napada. Što učiniti? Kako krenuti?

Što organizacija može učiniti?

- Kupiti novi, veći, vatrozid?
 - Kako ga podesiti? I kako postojeći podesiti? Što dopustiti, što ne?
- Svuda instalirati antivirusni programski alat?
 - Koji? Kako znamo da nije onemogućen?
- Instalirati IDS sustave?
- Prikupljati sistemske i operativne zapise (logove)?
 - Koje? Kako? Koliko ih pohranjivati? Što s njima učiniti?
 - ...

Što organizacija može učiniti?

- Sve to, i više, moguće je...
 - Ali... to je isto kao da u rat idemo tako da samo pošaljemo jedinice u smjeru neprijatelja – s jedinom nadom da je to dovoljno...
 - Sigurnost **NIJE SAMO TEHNIČKO PITANJE**
- Zaštita organizacije zahtjeva ciljan, planiran i dugoročan pristup
 - Zaštitom (sigurnošću) organizacije **mora se upravljati**
 - Upravljanje sigurnošću mora biti sastavni dio upravljanja organizacijom!

Upravljanje u organizacijama

- Governance, Risks and Compliance, GRC
 - Temeljne zadaće visokog menadžmenta
- Sustav upravljanja
 - Sustav kako se upravlja
- Rizici
 - Upravljanje rizicima kako bi se smanjila izloženost
- Usklađenost
 - Usklađivanje sa zakonskom i drugom regulativom

UPRAVLJANJE SIGURNOŠĆU

Usklađenost (engl. compliance)

Pravni akti

- Usklađenost znači da organizacija poštuje sve pravne propise koji se odnose na nju
 - Zbog toga je bitno znati koji pravni propisi postoje!
- Vrste pravnih akata
 - Ustav; Međunarodni ugovor; Europske odredbe; Zakon; Uredba; Pravilnik, naredba, naputak; Sudski precedenti; Običajno pravo; **Akti društvenih organizacija**; Ukaz, presuda, rješenje.
- Pravni akti značajno utječu na organizacije

Zakoni

- Pravni akti koje donosi zakonodavno tijelo
 - U slučaju Hrvatske to je Sabor
- Zakoni su pravila koja zahtijevaju ili zabranjuju određena ponašanja u društvu
 - Proizlaze iz **etike** koja definira društveno prihvatljivo ponašanje
 - Etika je zasnovana na kulturi morala - čvrsti moralni stavovi ili običaji određene skupine.
 - Ključna razlika između zakona i etike - zakoni nose sankcije vlastim, a etika ne.

Podjela prava

- **Građansko i kazneno pravo**
 - Građansko pravo (civil law) – nacija ili država regulira odnos organizacija i ljudi
 - Kazneno pravo (criminal law) – aktivnosti štetne po društvo
- **Privatno i javno pravo**
 - Privatno pravo (private law) - obiteljsko pravo, radno pravo, ...
 - Javno pravo (public law) - ustavno, upravno, procesna, ...

EU regulativa

- Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)
- Uredba (EU) 2016/679 Europskog Parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (GDPR)
- The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554

Zakoni u području informacijske sigurnosti (1)

- **Zakon o informacijskoj sigurnosti (NN 79/07)**
 - Definira nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti (Ured Vijeća za nacionalnu sigurnost, ZSIS, NCERT).
 - Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

Zakoni u području informacijske sigurnosti (2)

- Kazneni zakon (NN 101/17)
 - Kaznena djela protiv računalnih sustava, programa i podataka (Glava XXV)
 - Kaznena djela protiv privatnosti (Glava XIV)
- Zakon o elektroničkoj trgovini (NN 173/03)
- Zakon o tajnosti podataka (NN 79/07)

Zakoni u području informacijske sigurnosti (3)

- Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018)

Uredbe u području informacijske sigurnosti

- Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/2018)

Upravljanje organizacijom

- U svim organizacijama postoji model upravljanja (engl. governance model)
 - Ovisan o vrsti organizacije i državi
- Model upravljanja podrazumijeva jasne odgovornosti i ovlasti

UPRAVLJANJE SIGURNOŠĆU

Upravljanje (engl. governance)

Sustav upravljanja (1)

- Temelj čine zakoni koji definiraju osnovni način upravljanja u organizacijama različitih tipova
 - Dionička društva, društva s ograničenom odgovornošću, udruge, ...
 - Ovisno o legislativnom području (EU, SAD, ...)
- Podrazumijeva jasno definirane ovlasti i odgovornosti

Sustav upravljanja (2)

- Sustav upravljanja kibernetičkom sigurnošću nije definiran u tim zakonskim aktima
 - Samo u pojedinim slučajevima definiran drugim zakonskim ili podzakonskim aktima
 - Posljedica su različiti sustavi upravljanja
- Ustalo se običaj da se funkcija za upravljanje sigurnošću naziva *Voditelj sigurnosti informacijskog sustava*
 - Chief Information Security Officer (CISO)

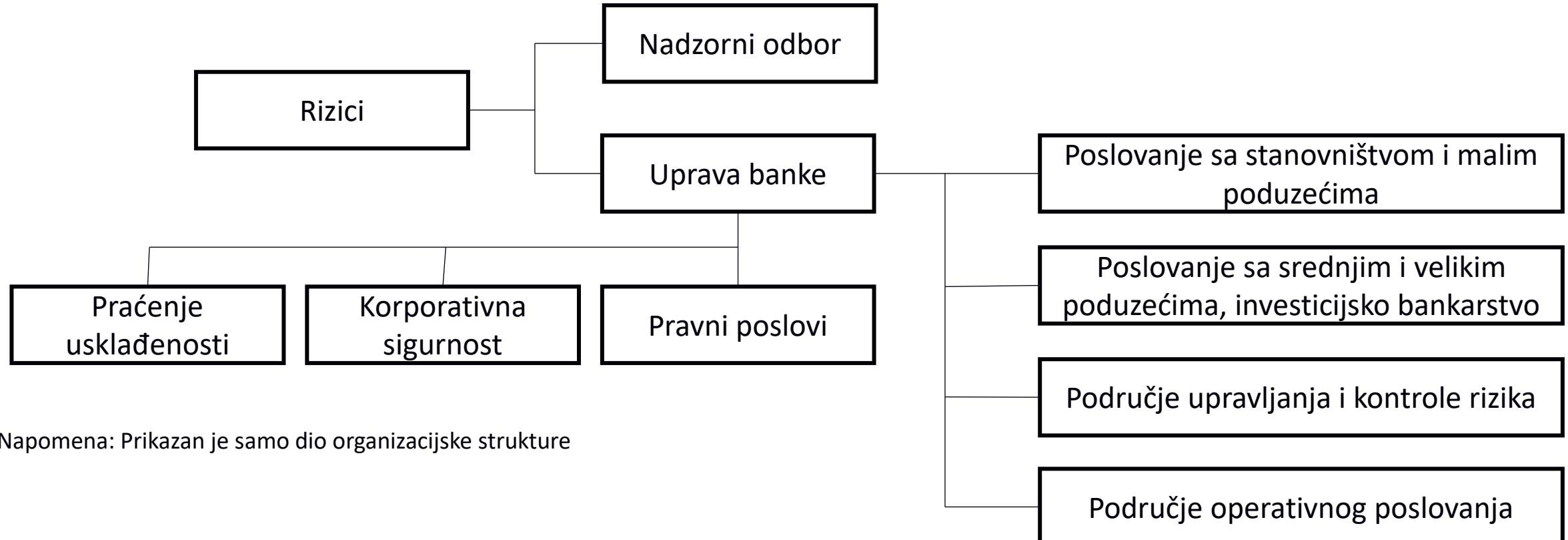
Voditelj sigurnosti informacijskog sustava

- Mora biti osoba koja razumije sigurnost
- Po mogućnosti ne smije se baviti operativnim detaljima
 - Različit od osoba koje se bave taktičkim detaljima
- Alternativna imena
 - Chief Information Security Officer, CISO
 - Chief Information System Security Officer, CISSO
 - I niz drugih imena...

Organizacijska struktura

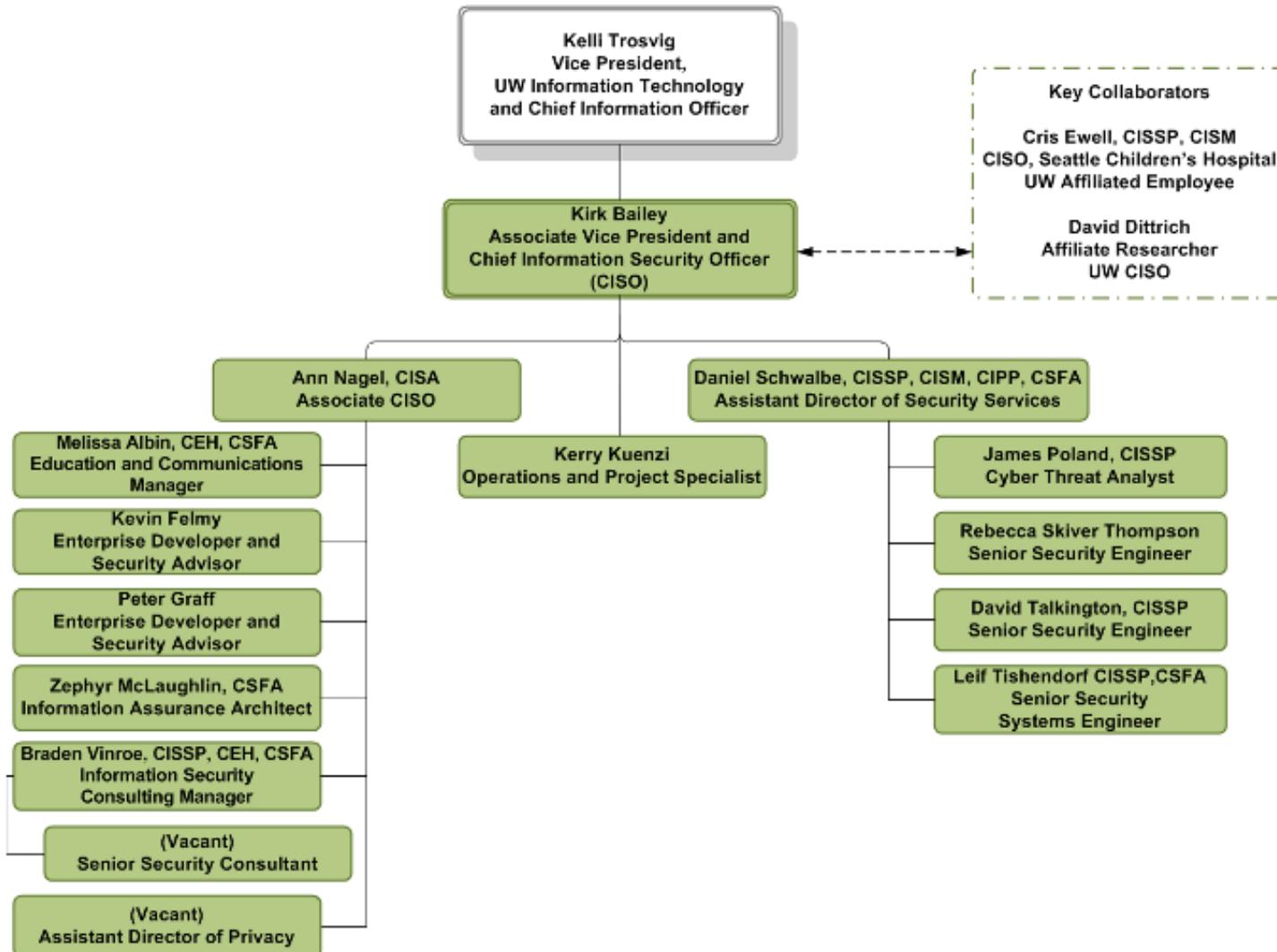
- CISO je pri vrhu organizacijske strukture
 - Direktno odgovara predsjedniku Uprave (CEO) ili nekog od članova Uprave (CFO, COO, head of legal council)
 - U slučaju potrebe može imati direktni pristup nadzornom odboru
- U slučaju većih organizacija radi se o uredu na čijem čelu se nalazi voditelj ureda
 - Tvrtka ima voditelja sigurnosti (CSO) kojemu CISO odgovara
 - Voditelj sigurnosti zadužen je za cjelokupnu sigurnost (fizičku, informacijsku, prijevare, ...)

Primjer organizacijske strukture (PBZ)



Napomena: Prikazan je samo dio organizacijske strukture

University of Washington – Office of CISO



Evolucija uloge voditelja sigurnosti (1)

- Od prvog CISO-a do danas uloga se mijenjala, a opseg širio
 - Posljedica je različite kompetencije osobe na toj poziciji
 - Uzrok je različito okruženje
- Faza 1 (1990-te – 2000)
 - Uvjerenje kako informacije u tvrtci nisu nikome interesantne
 - Ograničena sigurnost, naglasak na lozinkama i kontroli pristupa
 - Pojava Weba, osobna računala mijenjaju velika računala
 - Prvi imenovani CISO, Steve Katz, 1995
 - CISO je bio s tehničkom pozadinom i negdje u IT-ju

Evolucija uloge voditelja sigurnosti (2)

- Faza 2 (2000 – 2004)
 - Pojava legislative za zaštitu privatnosti i podataka
 - HIPAA, Gramm-Leach-Bliley, SOX
 - Prvi put se zahtijevalo da postoji netko zadužen za sigurnost
 - Usklađenost s regulativom
- Faza 3 (2004 – 2008)
 - Problem s ispunjavanjem regulative
 - CISO orijentiran na rizike, naglasak na „mekim vještinama”, još uvijek dio IT-ja

Evolucija uloge voditelja sigurnosti (3)

- Faza 4 (2008 – 2016)
 - Sigurnost svjesna prijetnji, društvene mreže, mobilni uređaji, računarstvo u oblaku
 - Treba li zabraniti FB? Hoće li to utjecati na zapošljavanje? LinkedIn? Što je s uređajima koji se donose u organizaciju?
 - CISO treba marketing, politiku, tehnologiju
 - Daljnje umrežavanje (tableti) zbog kojih su osjetljive informacije izloženije
- Faza 5 (2016 – 2020-te)
 - Privatnost dobija na značenju (GDPR), „outsource”, dobavni lanac
 - CISO svjestan privatnosti i podataka

Svrha CISO-a

- Nadzire i koordinira aktivnosti vezane uz sigurnost informacijskog sustava.
- Inicira primjenu dobrih praksi i prihvaćenih standarda vezanih uz sigurnost informacijskog sustava.
- Ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

Zadaće CISO-a – Izrada internih akata (1)

- Razvoj politike sigurnosti informacijskog sustava, standarda, smjernica i ostalih internih akata s ciljem postizanja i održavanja zadovoljavajuće razine sigurnosti
 - Uspostavljanje upravljačkog okvira.
- Temelji akt je **Politika sigurnosti informacijskog sustava**
 - krovni dokument koji definira što za informacijski sustav znači da je siguran.
 - Za sigurnost informacijskog sustava taj dokument je kao ustav koji je temeljni pravni akt države.
 - Temelj za ostale akte („Zakoni”)
- Bitan akt je i pravilnik o radu CISO-a, međutim on ne spada u skup internih akata koji definiraju sigurnost već je organizacijski

Zadaće CISO-a – Izrada internih akata (2)

- Može se postaviti pitanje čemu interni akti, tj. koja korist od njih?
 - Oni predstavljaju administrativne kontrole, nadopuna tehničkim kontrolama
 - Da svi dionici jasno i nedvosmisleno znaju što smiju (ili ne smiju), tko je za što zadužen, što se radi, kada i kako, ...

Zadaće CISO-a – Izrada internih akata (3)

- Vrste internih akata:
 - Politika
 - Piše ju Voditelj sigurnosti informacijskog sustava
 - Definira osnovna načela, smjernice... bez ikakvih konkretnih tehničkih detalja
 - Puna izraza tipa „Trebalo bi ...”, „Mora se...”, „Preporučljivo je...”, „Ako je moguće...”
 - Pravilnik (voditelj sigurnosti/IT)
 - Detaljnije razrađuje politiku, s konkretnijim detaljima no bez ulaska u veliku dubinu
 - Procedura (IT)
 - Detaljna razrada pojedinih dijelova pravilnika, jasno specificira korake

Zadaće CISO-a – Izrada internih akata (4)

- Primjeri internih akata
 - Politika sigurnosti informacijskog sustava
 - Po mogućnosti, što kraći dokument, no ima i vrlo dugih
 - Politika/pravilnik za izradu pričuvnih kopija
 - Politika/pravilnik za vođenje i bilježenje sistemskih i operativnih zapisa
 - Politika/pravilnik korištenja informacijskog sustava
 - Politika/pravilnik upravljanja sigurnosnim rizicima
- **Interni akti su živi dokumenti!**
- Interne akte odobrava i prihvata Uprava

Izazov pisanja politika

- Pisanje politika je složen posao
 - Mora biti efektivna te u skladu s ostalim organizacijskim politikama
- Neke preporuke za pisanje politika
 - Jasno i jednostavno napisana (ne koristiti komplikirane izraze)
 - Ne (pre)dugačka
 - U skladu s primjenjivim zakonima i regulativom
 - Razumna
 - Provediva

Sadržaj politike

- **Pregled** – o čemu je politika
- **Svrha** – zašto je politika potrebna
- **Obuhvat** – što sve politika obuhvaća
- **Kome je namijenjena** – tko je sve obvezan djelovati temeljem politike
- **Politika** – Temeljni dio dokumenta koji navodi što treba biti učinjeno
- **Definicije** – Pojmovi koji se upotrebljavaju u politici
- **Verzioniranje** – Vođenje evidencija o promjenama

Zadaće CISO-a – Provjera provođenja internih akata

- Kontroliranje provođenja politike sigurnosti informacijskog sustava i ostalih internih akata koji se odnose na sve aspekte sigurnosti informacijskog sustava
- Revizija internih sustava i pravilnika
- Po potrebi nadopuna, pojašnjenje ili izmjena pravilnika
 - Sustav se stalno mijenja te je potrebno i interne akte prilagođavati
 - Iskustvom se neke stvari ispostave teške, ili jednostavne, ili (ne)provedive

Zadaće CISO-a – Upravljanje rizicima (1)

- Temeljni alat u radu CISO-a
- Omogućava da se odrede rizici kojima je izložena organizacija
 - Procjena rizika (engl. risk assessment)
 - Potom je moguće napraviti prioritizaciju
 - Na temelju prioriteta odlučuje se što će se učiniti s identificiranim rizicima
 - Prihvati, ovladati (na neki način umanjiti), ili prenijeti na neku treću stranu
 - Uprava organizacije ima konačnu riječ po tom pitanju

Zadaće CISO-a – Upravljanje rizicima (2)

- Vrlo bitan element posla CISO-a koji se često radi na vrlo loš način
- Upravljanje rizicima je **proces** (kao i sigurnost)
 - Mora se uvijek provoditi jer se uvjeti stalno mijenjaju
- Propisan internim aktima

Zadaće CISO-a – Upravljanje incidentima (1)

- Danas nije pitanje AKO se desi incident već KADA će se desiti
- Postupak koji bi također **morao** biti definiran internim aktima
 - Tko/što/gdje/kada/kako, koga se zove, ovlasti i obaveze
 - Uključuje dijelove ili cijelu organizaciju, a CISO (možda i CEO) je koordinator
 - To recimo može ovisiti o incidentu (interni akt!)
 - Definira i što se podrazumijeva pod incidentom
 - Treba biti i uvježban, ili bar na neki način ispitan

Zadaće CISO-a – Upravljanje incidentima (2)

- Cilj upravljanja incidentima
 - Što prije detektirati incident
 - Utvrditi uzroke incidenta, posljedice i nastalu štetu te djelovati na otklanjanju incidenta i umanjivanju štete
 - Uvesti kontrole koje će spriječiti njegovo ponavljanje
- Nisu svi incidenti jednaki, a neki mogu dovesti i do krize u organizaciji

Zadaće CISO-a – Edukacija i osvještavanje

- Upozoravanje na potrebu za izobrazbom
- Davanje smjernica za izobrazbu svih osoba koje se koriste informacijskim sustavom banke, a u svezi sa sigurnosti informacijskog sustava
- Osvještavanje uključuje
 - Objašnjavati važnost sigurnosti organizacije.
 - Informiranje zaposlenika o njihovim ulogama i očekivanjima od uloge u sklopu sigurnosnih funkcija.
 - Davati smjernice u obavljanju pojedinih zadaća vezanih uz sigurnost ili rizike.
 - Edukacija korisnika.

Zadaće CISO-a – Potencijalne teme edukacije

- Politike sigurnosti i interni akti.
- Regulatorni zahtjevi.
- Socijalni inženjering.
- Kontinuitet poslovanja.
- Upravljanje katastrofalnim situacijama.
- Upravljanje sigurnosnim incidentima.
- Klasifikacija podataka, označavanje podataka i odgovarajuće rukovanje.
- Ponašanje zaposlenih.
- Fizička sigurnost.
- ...

Zadaće CISO-a – Metode provođenja edukacije

- Korištenjem sustava za e-učenje
 - Skalabilno
 - Neprilagođeno trenutnoj situaciji
- Direktnim predavanjem
 - Direktni kontakt s ljudima i mogućnosti demonstracija u tijeku predavanja
 - Ne skalira dobro
- Predavanjem putem Interneta (Skype i slično)

Zadaće CISO-a – Izvješćivanje

- CISO mora periodički izvješćivati upravu i nadzornom odboru
 - Odnosno, bilo koga koje je organizacijski odgovoran za svoj rad
 - Najčešće onaj koga CISO izvještava nije stručnjak za sigurnost
- Internim aktom o radu CISO-a ili nekim ekvivalentnim dokumentom propisani su detalji
 - Učestalost izvješćivanja
 - Sadržaj izvješća
 - Kome se izvješće sve podnosi

Zadaće CISO-a – Rad s vanjskim suradnicima

- Vanjski suradnici su
 - Revizori
 - Stručnjaci koji testiraju sigurnosti informacijskog sustava
- Rad s vanjskim suradnicima znači
 - Dogovaranje tipa i opsega poslova
 - Pružanje potrebnih informacija nužnih za provođenje ispitivanja
 - Analiza rezultata
 - Uključivanje rezultata u procjenu rizika
 - Iniciranje aktivnosti na temelju rezultata

Zadaće CISO-a – Analiza sigurnosnih potreba

- Analiziranje sigurnosnih potreba
- Na temelju analize predlaganje
 - Planiranja
 - implementacije
 - testiranja, i
 - nadziranja aktivnosti za poboljšanje sigurnosti informacijskog sustava
- Planiranje godišnjeg budžeta
 - Izlaganje upravi
 - Dio planiranih aktivnosti
- Planiranje i koordiniranje analize isplativosti preporučenih i postojećih sigurnosnih rješenja

Zadaće CISO-a – Sudjelovanje u bitnim aktivnostima

- Sudjelovanje u planiranje kontinuiteta poslovanja
 - Business Continuity Management, BCM
 - Sudjelovanje u procjeni adekvatnosti DR lokacije
- Klasifikacija informacija
 - Sve informacije u tvrtki moraju biti klasificirane na temelju tajnosti, integriteta i raspoloživosti
 - Izrađuje se pravilnik/politika te registar imovine
 - CISO može voditi navedenih postupak, ili samo sudjelovati u njemu

Zadaće CISO-a – Sudjelovanje u razvoju i održavanju IT-a (1)

- Sudjelovanje u značajnijim fazama u životnom ciklusu informacijskog sustava s aspekta sigurnosti
 - CISO je uključen kao savjetnik
 - Daje mišljenje o predloženim rješenjima
 - Po potrebi vrši analizu
 - Predlaže dodatna rješenja
- Primjeri
 - Odabir novog rješenja za udaljen pristup
 - Razvoj nove aplikacije
 - Arhitektura novog sustava

Zadaće CISO-a – Sudjelovanje u razvoju i održavanju IT-a (2)

- Praćenje raznih upozorenja i novog razvoja u računalnom kriminalu
 - Na temelju toga davanje smjernica IT-ju
 - Ažuriranje procjene rizika
- Procjena prijetnji
 - Analiza resursa, ciljeva, motiva
 - Primjer: Prijetnja DDoS napadom od anonimne skupine

Zadaće CISO-a – Sistemski i operativni zapisi

- Sistemski i operativni zapisi (logovi) vrlo su bitni sa sigurnost informacijskog sustava
 - Omogućavaju rekonstrukciju događaja
 - Omogućavaju detekciju neočekivanih događaja
- Nužno ih je držati na zasebnom mjestu
 - Kako bi se zaštitili od neovlaštenih izmjena
- Usklađeni satovi vrlo bitni za rekonstrukciju (!)
- CISO definira način upravljanja sistemskih i operativnim zapisima
 - Vrši nadzor
 - U manjim organizacijama moguće analizira logove te traži očitovanja

Nadzor sigurnosti

- Današnji trend je da tvrtke sigurnost nadziru u Sigurnosno operativnim centrima
 - Security Operations Center (SOC)
- SOC je centralizirana funkcija unutar organizacije koja korištenjem ljudi, procesa i tehnologije kontinuirano prati i poboljšava sigurnosno stanje organizacije te sprečava, detektira, analizira i odgovara na sigurnosne incidente
 - Nekada se pod tim smatrala fizička lokacija, ali danas ne treba biti
 - Trend je također iznajmljivanja usluge SOC-a
- SOC je evoluirao iz SIEM-a (security incident and event management), koji je evoluirao od centraliziranog bilježenja sistemskih i operativnih zapisa

SOC



Problemi (i izazovi) s kojima se CISO susreće (1)

- Vrlo dinamična okolina koju je teško pratiti
 - Prijetnje van organizacije se brzo mijenjaju i puno ih je
 - **Unutarnje prijetnje**
 - Informacijski sustav je vrlo dinamičan
 - Čak ni IT osoblje se ne pridržava pravila (!)
- Evaluacija rizika raznih tehnologija
 - „Cloud“ rješenja, BYOD, Mobilni uređaji, Specifične aplikacije

Problemi (i izazovi) s kojima se CISO susreće (2)

- Operativni i strateški poslovi
- Vanjski dobavljači
- Koordiniranje aktivnosti s organizacijskom jedinicom informacijske tehnologije i unutarnjom revizijom
 - Ponekad nisu na „istoj valnoj duljini“

Kompetencije CISO-a* (1)

- **Upravljačke vještine (engl. management skills)**
 - Odnosi se na one koje su neophodne da se postigne efektivna nabavka, alokacija, korištenje ljudskih resursa ili fizičkih resursa kako bi se postigao neki cilj
- **Poslovne vještine (engl. business skills)**
 - Povećati vrijednost organizacije i integrirati potrebu za sigurnošću s poslovnim ciljevima tvrtke
- **Stalno usavršavanje (engl. information systems security education)**
- **„Soft skills”**
 - Pisana i govorna komunikacija, efektivan prezentacija i slično.
 - Kritičko razmišljanje, rješavanje problema

* Whitten, Dwayne. "The chief information security officer: an analysis of the skills required for success." Journal of Computer Information Systems 48.3 (2008): 15.

Kompetencije CISO-a* (2)

- Vještine i znanja iz sigurnosti informacijskih sustava
- Planiranje oporavka od katastrofičnih događaja (engl. disaster recovery planning)
- Sposobnost istraživanja sigurnosnih incidenata (engl. security breach investigations)

* Whitten, Dwayne. "The chief information security officer: an analysis of the skills required for success." Journal of Computer Information Systems 48.3 (2008): 15.

Kako postati CISO

- Krenuti od dna prema vrhu
- Stjecanje tehničkih kompetencija
- Certifikati, dodatna edukacija
- Stjecanje upravljačkih kompetencija
- CISM, MBA, Specijalistički studij informacijske sigurnosti

Example CISO Career Patch



Nadzor rada CISO-a

- Postoji definiran sustav nadzora rada CISO-a
 - Sprečavanje potencijalne štete zbog neodgovornog ili zlonamjernog ponašanja
 - Poboljšanje rada CISO-a – povratna petlja
- Tu dužnost obavljaju
 - Revizije
 - Unutarnja i vanjska
 - Osoba/funkcija nadređena voditelju sigurnosti
 - CEO, CIO, CSO, ...

Hvala!



Zaštita i sigurnost informacijskih sustava

Sigurnost baza podataka

dr. sc. Jasenka Anzil
prof.dr.sc. Mirta Baranović
prof.dr.sc. Boris Vrdoljak

U ovoj prezentaciji koriste se i prilagođeni materijali iz predmeta Baze podataka (FER)

**Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva**

Sadržaj

- ◆ baze podataka i sustavi za upravljanje bazama podataka
- ◆ dokazivanje autentičnosti korisnika baze podataka
- ◆ upravljanje pristupom
 - diskrecijsko upravljanje pristupom
 - kontekstno ovisna zaštita podataka
 - mandatno upravljanje pristupom
 - baze podataka s višerazinskom zaštitom podataka
 - upravljanje pristupom temeljeno na ulogama
- ◆ šifriranje podataka
- ◆ nadgledanje rada korisnika



Baze podataka i sustavi za upravljanje bazama podataka

Baza podataka

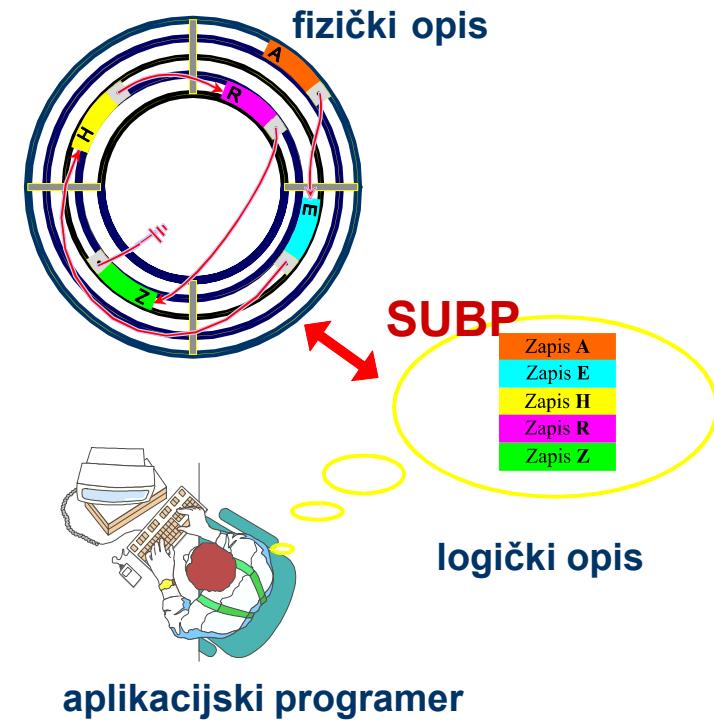
- skup podataka koji su pohranjeni i organizirani tako da mogu zadovoljiti zahtjeve korisnika. (M. Vetter)
- skup međusobno povezanih podataka, pohranjenih zajedno, uz isključenje bespotrebne zalihosti (redundancije), koji mogu zadovoljiti različite primjene. Podaci su pohranjeni na način neovisan o programima koji ih koriste. Prilikom dodavanja novih podataka, mijenjanja i pretraživanja postojećih podataka primjenjuje se zajednički i kontrolirani pristup. Podaci su strukturirani tako da služe kao osnova za razvoj budućih primjena. (J. Martin)

Sustav za upravljanje bazama podataka (SUBP)

- ◆ SUBP je programski sustav koji:
 - omogućava upravljanje podacima u bazi podataka
 - može istovremeno upravljati s više baza podataka
 - upravlja istovremenim pristupom bazi podataka od strane više korisnika/aplikacija uz osiguravanje sigurnosti i integriteta baze podataka
 - temelji se na odabranom modelu podataka (hijerarhijski, mrežni, **relacijski**, objektno-relacijski, objektno-orientirani, ...)

Zadaće SUBP-a

- ◆ trajna pohrana podataka (*persistent storage*)
 - ◆ skriva od korisnika detalje fizičke pohrane podataka
- ◆ osiguravanje programskog sučelja (*programming interface*)
 - ◆ omogućuje definiciju i rukovanje s podacima
 - ◆ DDL - Data Definition Language
 - ◆ DML - Data Manipulation Language
- ◆ optimiranje metoda pristupa podacima (*query optimization*)
- ◆ **zaštita podataka**
 - ◆ **integritet podataka (*integrity*)**
 - ◆ **pristup podacima - autorizacija, sigurnost (*security*)**
 - ◆ **potpora za upravljanje transakcijama**
 - ◆ **upravljanje istodobnim pristupom (*concurrency control*)**
 - ◆ **obnova u slučaju razrušenja (*recovery*)**



Korisnici

- pristupaju bazi tako da postavljaju upite, mijenjaju podatke i izrađuju izvještaje
- različite skupine korisnika:
 - korisnici koji često koriste bazu postavljajući standardne upite i radeći standardne promjene **koristeći programirana sučelja** (npr. službenici u banci, turističkim agencijama...)
 - korisnici koji povremeno pristupaju bazi **koristeći upitni jezik**
 - **sofisticirani korisnici** koji su dobro upoznati s bazom podataka i koriste je na složeniji način (npr. inženjeri, znanstvenici, poslovni analitičari)
 - **administratori**

Administratori

- ◆ organiziraju, nadziru i optimiziraju korištenje SUBP-a
- ◆ **odgovorni za sigurnost SUBP-a**

- ◆ administrator poslužitelja baze podataka (*database server administrator* – DBSA)
 - instaliranje i nadogradnja SUBP-a; kreiranje novog korisnika; autorizacija na razini SUBP-a

- ◆ administrator baze podataka (*database administrator* - DBA)
 - autorizacija na razini baze podataka (provođenje sigurnosne politike)
 - dodjeljivanje i ukidanje ovlasti korisniku baze podataka
 - dodjeljivanje sigurnosne klasifikacijske razine korisniku u višerazinskom sigurnosnom sustavu, u skladu s politikom organizacije



Sigurnost i zaštita baza podataka

Primjeri narušavanja sigurnosti podataka

- ◆ 2012 - Global Payments (posrednik između trgovina i kartičnih kuća) - pogodjeni MasterCard, Visa, American Express i Discover Financial Services, banke - ukradeni podaci o **1,5 milijuna računa** (neki izvori govore o 10 milijuna **kartica**)
- ◆ 2013-2014 – Yahoo – probijene lozinke – napadači došli do imena, email adresa, lozinki, telefonskih brojeva... **za 3 milijarde korisnika**
- ◆ 2018 – Marriott International – ukradeni osobni podaci oko **500 milijuna korisnika** (gostiju lanca hotela) u razdoblju od 2014. do 2018. godine

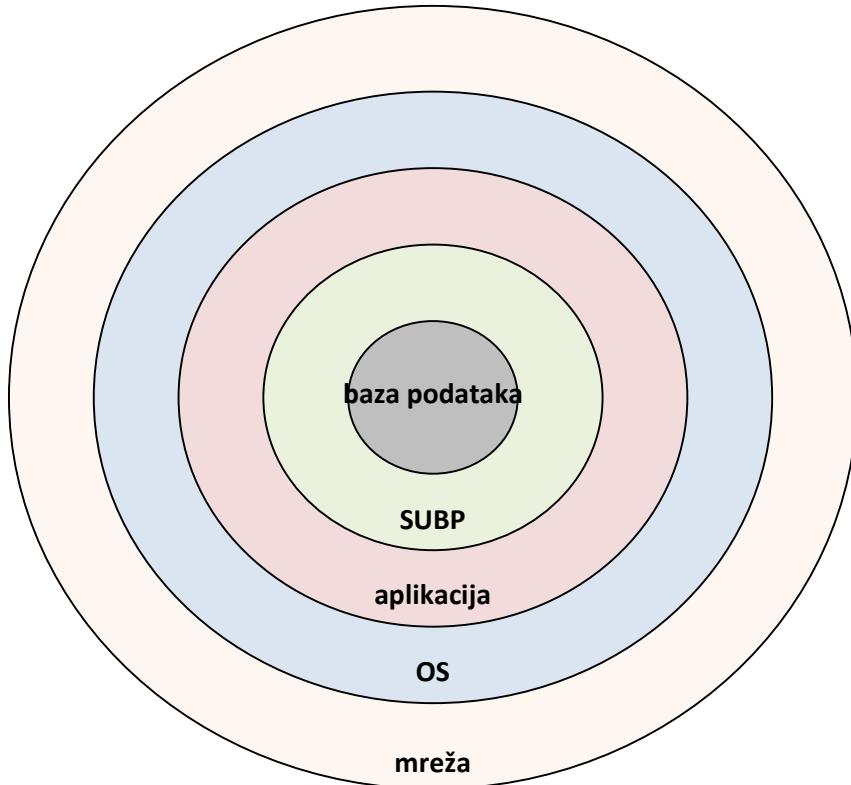
Narušavanje sigurnosti i moguće posljedice

- ◆ Oblici narušavanja sigurnosti baze podataka su:
 - neovlašteno čitanje, izmjena ili uništavanje podataka
- ◆ Moguće posljedice su:
 - krađa ili prijevara
 - gubitak tajnosti
 - odnosi se na podatke kritične za funkcioniranje organizacije
 - npr. krađa recepture - rezultira gubitkom konkurentnosti na tržištu
- ◆ gubitak privatnosti
 - odnosi se na osobne podatke
 - npr. krađa podataka o zdravstvenom stanju osobe – rezultira sudskim procesom protiv vlasnika baze podataka
- ◆ gubitak raspoloživosti
 - npr. uništenjem dijela podataka

Sigurnost baze podataka (1)

- ◆ sigurnost baze podataka se osigurava zaštitom na nekoliko razina
 - **na razini SUBP**
 - spriječiti pristup bazama podataka ili onim dijelovima baza podataka za koje korisnici nisu ovlašteni
 - **na razini operacijskog sustava**
 - spriječiti pristup radnoj memoriji računala ili datotekama u kojima SUBP pohranjuje podatke
 - **na razini računalne mreže**
 - spriječiti presretanje poruka
 - **fizička zaštita**
 - zaštita lokacije poslužitelja sustava za upravljanje bazama podataka
 - **na razini korisnika**
 - spriječiti da ovlašteni korisnici bilo nepažnjom bilo namjerno omoguće neovlaštenim osobama pristup podacima

Sigurnost baze podataka (2)



Defense-in-depth strategija

- ◆ zaštita u više slojeva
 - ne postoji savršeni zaštitni sloj, metoda ili proizvod
- ◆ probor jednog sloja ne mora značiti i narušavanje sigurnosti podataka iz baze podataka
- ◆ nužna zaštita unutar baze podataka, čak i ako je implementiran poseban sustav zaštite baze podataka izvan baze podataka

Svaki pokušaj neovlaštenog pristupa sustavu mora biti automatski zabilježen korisničkim imenom, datumom i vremenom, a ako je to moguće i mjestom s kojeg je takav pristup pokušan.

Sigurnost baze podataka (3)

- ◆ neki od postupaka kojima je bazu podataka moguće učiniti sigurnijom:
 - **ograničiti pristup važnim resursima** koji mogu biti pogrešno korišteni, zlonamjerno ili slučajno kao posljedica pogreške - vatrozidi; upravljanje pristupom; antivirusna zaštita...
 - upravljanje zakrpama (*patches*)
 - sustavi za otkrivanje i sprječavanje upada (*Intrusion prevention systems* - IPS , *Intrusion detection systems* - IDS)
 - onemogućiti nepotrebne komponente i servise sustava za upravljanje bazama podataka
 - ukloniti/onemogućiti nepotrebne korisničke račune i lozinke
 - izvoditi procese baze podataka pod namjenskim, neprivilegiranim korisničkim računom
 - ...

Aspekti zaštite podataka

- ◆ zakonski, socijalni i etički aspekt
 - ima li vlasnik baze podataka zakonsko pravo na prikupljanje i korištenje podataka
 - npr. smije li zdravstvena ustanova koja, u skladu sa zakonom prikuplja podatke o pacijentima, te iste podatke koristiti pri donošenju odluke hoće li svog bivšeg pacijenta zaposliti
- ◆ strategijski aspekt
 - tko definira pravila pristupa - tko određuje kakve ovlasti ima pojedini korisnik baze podataka, ...
- ◆ operativni aspekt
 - kako osigurati poštivanje pravila - kojim mehanizmima se osigurava poštivanje definiranih pravila, na koji način su lozinke zaštićene, koliko često se mijenjaju, ...

Pravni okvir

- ◆ **Ustav RH - Članak 37.**

Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.

Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u Republici.

Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.

- ◆ **Zakon o zaštiti osobnih podataka**

- ◆ **GDPR - General Data Protection Regulation**

Opća uredba o zaštiti osobnih podataka koja se primjenjuje od 25. svibnja 2018. godine.

Načelo najmanje ovlasti i razdvajanje dužnosti

- ◆ **načelo najmanje ovlasti (least privilege)**
 - korisnik ima **minimalan skup dozvola** koje su neophodne za njegov trenutni zadatak
 - pojedinac ima različite razine ovlasti u različito vrijeme, ovisno o zadaći ili funkciji koju obavlja
 - spriječeno obavljanje nepotrebnih i moguće štetnih akcija
- ◆ **razdvajanje dužnosti (separation of duty - SoD)**
 - osjetljive zadatke u cijelosti ne može obaviti samo jedan korisnik
 - smanjuje se mogućnost zloporabe (važno načelo u financijskim i vojnim okruženjima)

Mehanizmi zaštite na razini SUBP

- identifikacija i dokazivanje autentičnosti
- upravljanje pristupom
- šifriranje podataka
- praćenje pristupa podacima
- maskiranje podataka



Integritet i sigurnost baze podataka

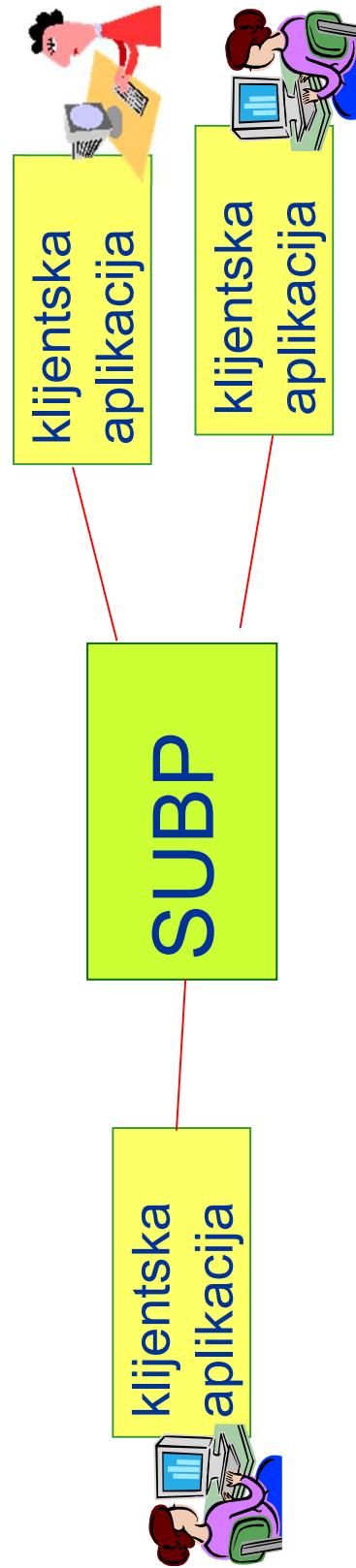
- ◆ Pojmovi *integritet* i *sigurnost* baze podataka se često spominju zajedno, međutim radi se o dva različita aspekta zaštite podataka
 - **Integritet baze podataka** (*database integrity*) - operacije nad podacima koje korisnici obavljaju **su ispravne** (tj. uvijek rezultiraju konzistentnim stanjem baze podataka)
 - "podaci se štite od ovlaštenih korisnika,"
 - **Sigurnost baze podataka** (*database security*) - korisnici koji obavljaju operacije nad podacima **su ovlašteni** za obavljanje tih operacija
 - "podaci se štite od neovlaštenih korisnika"
- Među ovim pojmovima postoje i sličnosti. U oba slučaja:
 - moraju biti definirana pravila koja korisnici ne smiju narušiti
 - pravila se pohranjuju u rječnik podataka
 - SUBP nadgleda rad korisnika i osigurava poštivanje pravila

Korisnici SUBP i ovjera autentičnosti

- ◆ administrator sustava (operacijskog sustava ili SUBP) omogućuje korisniku pristup sustavu (operacijskom sustavu ili SUBP) definiranjem jedinstvenog identifikatora korisnika (*user name*, *user ID*, *login ID*) i pripadne lozinke (*password*) koja je poznata samo dotičnom korisniku i sustavu
- ◆ korisnik koji pristupa sustavu (operacijskom sustavu ili SUBP) poznavanjem lozinke ovjerava svoju autentičnost (*authentication*)
- ◆ za ovjeru autentičnosti korisnika SUBP može koristiti
 - vlastite mehanizme
 - ili
 - vanjske mehanizme (npr. operacijski sustav)

SQL-sjednica

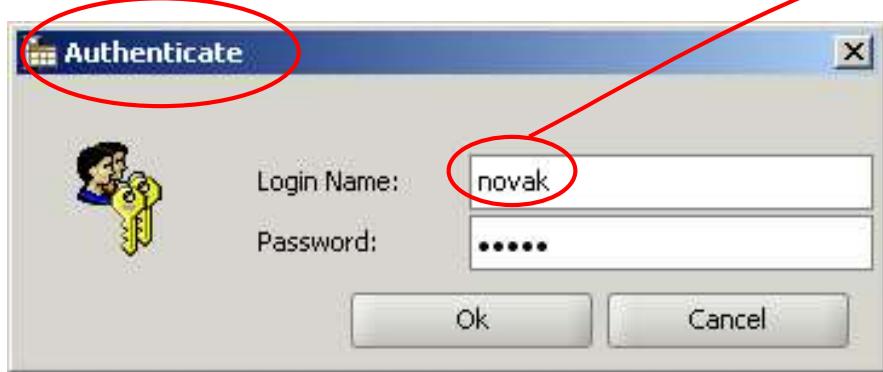
- SQL-sjednica (*SQL-session*) je kontekst u kojem jedan korisnik obavlja niz SQL naredbi putem jedne veze (*SQL-Connection*) prema sustavu za upravljanje bazama podataka
 - SQL-sjednica **započinje** u trenutku kada korisnik, upotrebom klijentske aplikacije, **ostvari vezu** (*connect*) sa sustavom za upravljanje bazama podataka
 - SQL-sjednica **završava** u trenutku kada korisnik **prekine vezu** (*disconnect*) prema sustavu za upravljanje bazama podataka



Korisnici u SQL-u

- ◆ autentificirani korisnik

- pri uspostavljanju SQL-sjednice korisnik se prijavljuje svojim identifikatorom korisnika, te lozinkom ovjerava svoju autentičnost
- funkcija CURRENT_USER vraća vrijednost identifikatora korisnika koji se koristi u dotičnoj SQL-sjednici



```
SELECT CURRENT_USER;
```

```
current_user  
novak
```

- bilo koji korisnik (PUBLIC)
 - dodjelom dozvole "korisniku" PUBLIC, dozvolu za obavljanje operacije dobivaju svi sadašnji i budući korisnici

Korisnici u PostgreSQL-u

```
CREATE USER name [ [ WITH ] option [ . . . ] ]
```

where option can be:

```
SUPERUSER | NOSUPERUSER  
| CREATEDB | NOCREATEDB  
| CREATEUSER | NOCREATEUSER  
| [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'  
| INHERIT | NOINHERIT  
| . . .
```

- Korisnici se i u PostgreSQL sustavu definiraju na razini SUBP-a, a ne na razini pojedinačne baze podataka
- Za SUPERUSER-a ne postoje ograničenja:

```
CREATE USER the_boss WITH SUPERUSER
```

```
PASSWORD 'superSecret' ;
```

„Superuser status is dangerous and should be used only when really needed.”

- CREATEDB - korisnik dobiva ovlast kreiranja baze podataka na PostgreSQL SUBP
- NOCREATEDB - preddefinirano ponašanje.

Korisnici u PostgreSQL-u

```
... | CREATEUSER | NOCREATEUSER
```

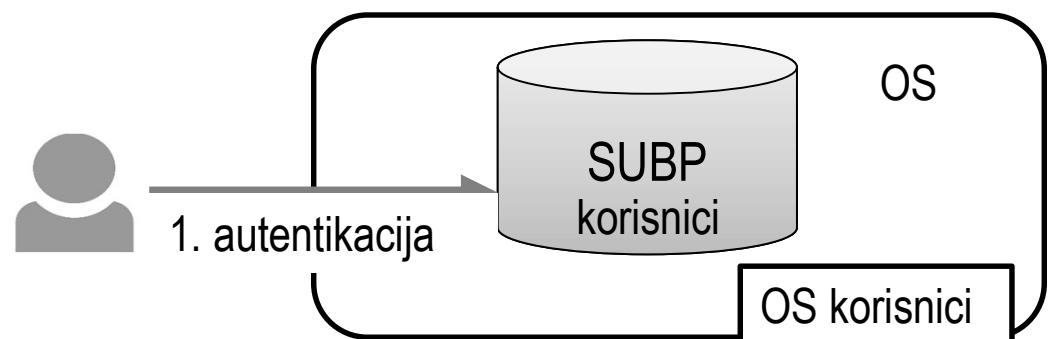
- CREATUSER - korisnik dobiva ovlast kreiranja drugih korisnika na PostgreSQL SUBP
- NOCREATEUSER - preddefinirano ponašanje.

```
CREATE USER badmin WITH CREATEDB CREATEUSER  
                      PASSWORD 'badminPwd' ;
```

Metode autentikacije

(PostgreSQL podržava čak 9):

- OS (trust auth)
- Vlastita (password auth)
- ...



IBM Informix: Dokazivanje autentičnosti

- ◆ interna autentikacija
 - ◆ lozinka pohranjena u poslužitelju baze podataka (tablica `sysIntAuthUsers` u bazi podataka `sysUser`) - šifrirana SHA-256 algoritmom (*Secure Hash Algorithm*)
- ◆ operacijski sustav
- ◆ posebni moduli (autentikacijski slojevi), npr:
 - Pluggable Authentication Modules (PAM)
 - za IBM Informix na UNIX i Linux OS
 - API za upravljanje autentikacijom, korisničkim računima, sjednicama i lozinkama
 - Lightweight Directory Access Protocol (LDAP) Authentication Support za Windows
 - za autentikaciju korisnika koristi se LDAP poslužitelj

Oracle: Zaštita lozinki (1)

- ◆ automatsko i transparentno **šifriranje lozinke** prije slanja preko mreže
- ◆ pohrana **sažetka (hash)** šifriranog SHA-512 algoritmom (*Secure Hash Algorithm*)
- ◆ provjera složenosti lozinke
- ◆ sprječavanje probijanja lozinke u slučaju višekratnih neuspjelih pokušaja prijave
 - ograničavanje broja neuspješnih pokušaja prijave
 - postepeno povećavanje vremena prije ponovnog pokušaja prijave - smanjenje broja pokušaja
 - isključivanje korisničkog računa

Oracle: Zaštita lozinki (2)

- ◆ definiranje sigurnosnih profila

```
CREATE PROFILE obicniKorisnik LIMIT  
    FAILED_LOGIN_ATTEMPTS 5  
    PASSWORD_LOCK_TIME 2;
```

- isključenje korisničkog računa na dva dana u slučaju pet neuspjelih pokušaja prijave

- DEFAULT profil

- ◆ povezivanje profila s korisnikom

```
CREATE USER u1 IDENTIFIED BY "pass11!1"  
    PROFILE obicniKorisnik;
```

- ◆ zaključavanje korisničkog računa

```
ALTER USER u1 ACCOUNT LOCK;
```

Parametar
FAILED_LOGIN_ATTEMPTS - broj neuspješnih pokušaja prijave prije zaključavanja korisničkog računa
PASSWORD_LIFE_TIME - trajanje lozinke (broj dana)
PASSWORD_LOCK_TIME - koliko je dana račun zaključan nakon određenog broja uzastopnih neuspjelih pokušaja prijave
PASSWORD_GRACE_TIME - broj dana do isteka lozinke (period odgode - dozvoljena prijava uz upozorenje)
PASSWORD_REUSE_TIME - mogućnost ponovnog korištenja iste lozinke (u danima)
PASSWORD_REUSE_MAX - potreban broj promjena lozinke prije ponovnog korištenja lozinke
PASSWORD_VERIFY_FUNCTION - funkcija za provjeru složenosti lozinke



Upravljanje pristupom

Upravljanje pristupom

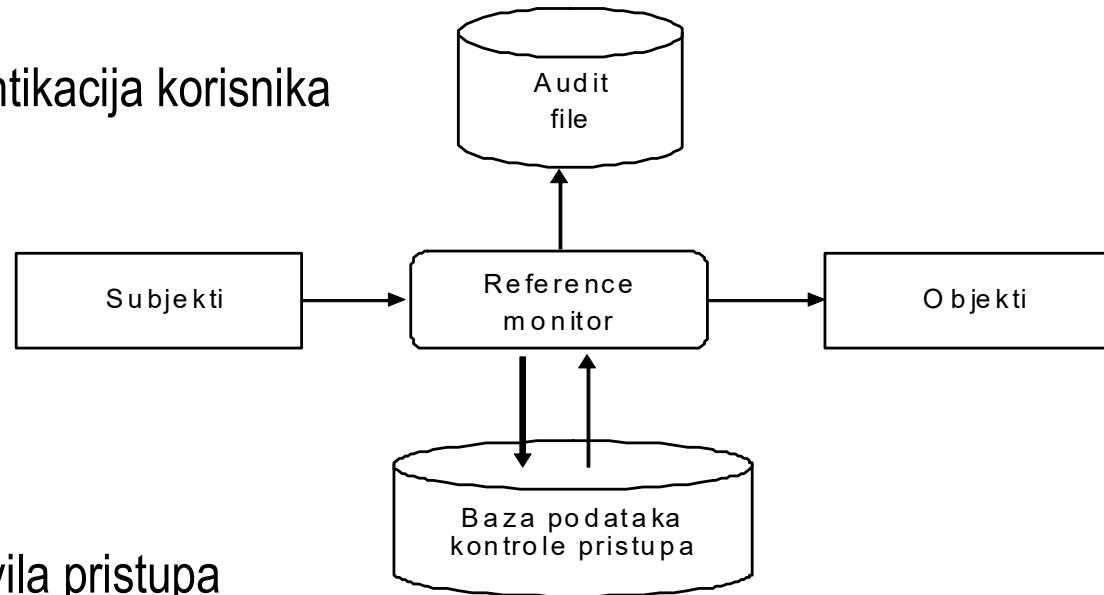
- ◆ niz postupaka kojima se utvrđuje i evidentira pokušaj pristupa, te odobrava ili odbija pristup na temelju unaprijed utvrđenih pravila
- ◆ razvoj sustava za upravljanje pristupom - višefazni proces
 - **sigurnosna politika** - pravila pristupa na visokoj razini (zakonski, socijalni, etički aspekt)
 - temeljena na načelu *treba-znati* (*need-to-know*), kompetentnosti, nadležnosti, sukobu interesa...
 - na nju mogu utjecati zakonska i etička pitanja, politike na državnoj ili korporativnoj razini ...
 - dinamična - mijenja se u skladu s promjenama poslovnih faktora, regulativa i uvjeta u okruženju
 - problem preslikavanja nejasnih i dvosmislenih zahtjeva u dobro definirana i jednoznačna pravila

Upravljanje pristupom

- ***sigurnosni model*** - formalni prikaz sigurnosne politike (strategijski aspekt)
 - ***diskrecijsko upravljanje pristupom*** (*discretionary access control* - **DAC**)
 - ***mandatno upravljanje pristupom*** (*mandatory access control* - **MAC**)
 - ***upravljanje pristupom temeljeno na ulogama*** (*role-based access control* - **RBAC**)
- ***sigurnosni mehanizam*** - (operativni aspekt) funkcije kojima je implementirano upravljanje pristupom

Mehanizmi upravljanja pristupom

- ◆ *reference monitor* - pouzdana komponenta koja upravlja svakim pokušajem pristupa objektu sustava i utvrđuje **je li taj pristup u skladu sa sigurnosnom politikom** utjelovljenom u bazi podataka upravljanja pristupom
 - uspoređuje sigurnosne atributе korisnika (npr. identifikator korisnika, grupa kojoj korisnik pripada, razina povjerenja iskazana korisniku) s onima koje imaju resursi (npr. oznaka osjetljivosti)
 - preduvjet: uspješna identifikacija i autentikacija korisnika



- ◆ **autorizacija** - postupak evidentiranja pravila pristupa
 - ◆ informacije koje opisuju prava pristupa moraju biti zaštićene od izmjene
 - ◆ sigurnosni mehanizmi implementirani kroz SQL

Elementi sustava za upravljanje pristupom

- ◆ **korisnik** – entitet koji koristi računalni sustav (osoba, uređaj)
 - **sjednica (session)** - instanca dijaloga korisnika sa sustavom
- ◆ **subjekt** – aktivni entitet koji može inicirati zahtjev za obavljanje operacija na objektima
 - proces koji djeluje u ime korisnika
 - korisnik može imati više aktivnih subjekata
- ◆ **objekt** - entitet sustava na kojem može biti obavljena operacija
- ◆ **operacija** - aktivan proces pozvan od strane subjekta, koji nakon poziva izvršava funkcije
- ◆ **dozvola (pravo pristupa, ovlast)** određenog načina pristupa objektu u sustavu
 - kombinacija objekta i operacije
 - za omogućavanje izvođenja iste operacije (npr. SELECT) na dva različita objekta (npr. tablice *student* i *predmet*) potrebne dvije dozvole
 - za omogućavanje obavljanja dviju različitih operacija (npr. UPDATE i SELECT) na istom objektu (npr. tablici *student*) potrebne su dvije dozvole

Elementi sustava za upravljanje pristupom - dozvola

- **pozitivna dozvola** - ako ne postoji, zatraženi pristup je odbijen
 - **negativna dozvola (tj. zabrana)** - ako postoji, zatraženi pristup je odbijen
-
- ◆ klasični pristupi upravljanja pristupom:
 - **zatvorena politika** - dozvoljen pristup za koji postoji (pozitivna) dozvola
 - **otvorena politika** - uskraćen pristup za koji postoji zabrana (tj. "negativna dozvola")
 - ako zabrana ne postoji, pristup je dozvoljen

Elementi sustava za upravljanje pristupom - dozvola

- ◆ problemi kod kombiniranog korištenja pozitivnih i negativnih dozvola:
 - *nepotpunost* - za pristup nije specificirana dozvola
 - može se izbjegići definiranjem prepostavljene politike
 - *nekonzistentnost* - za pristup postoji i negativna i pozitivna dozvola
 - može se izbjegići definiranjem politike razrješavanja konflikata
- ◆ politike razrješavanja konflikata:
 - *nepostojanje konflikata* – postojanje konflikta smatra se pogreškom
 - *prioritetne su negativne dozvole*
 - *prioritetne su pozitivne dozvole*
 - *ništa nema prioritet* – istovremeno postojanje konfliktnih dozvola poništava te dozvole (kao da nije specificirana nikakva dozvola)



Diskrečijsko upravljanje pristupom

Diskrečijsko upravljanje pristupom

- ◆ upravljanje pristupom na temelju:
 - **identiteta korisnika** koji zahtijeva pristup i
 - eksplicitnih **pravila pristupa** koja utvrđuju tko može izvesti koje akcije na kojim objektom sustava

Način ograničavanja pristupa objektima na temelju identiteta subjekata i/ili grupa kojoj oni pripadaju. Upravljanje je diskrečijsko u smislu da je subjekt s nekom dozvolom pristupa sposoban dati tu dozvolu (možda indirektno) nekom drugom subjektu (osim ako je to ograničeno MAC-om (Mandatory Access Control))

[US Department of Defense, Trusted Computer Security Evaluation Criteria (TCSEC),
DoD 5200.28-STD, 1985]

- ◆ koncept vlasništva nad objektom
 - **vlasnik objekta određuje kome se dozvoljava pristup**

Matrica autorizacijskih pravila (Matrica pristupa)

- ◆ Lampson (1974); Harrison, Ruzzo i Ullmann - HRU model (1976)
- ◆ stanje sustava - trojka (S, O, A)
- ◆ stanje autorizacije predstavljeno matricom pristupa A
 - stupci – **objekti** (o)
 - retci – **subjekti** (s)
 - element matrice – $A[s, o]$ - **ovlasti** subjekta s na objektu o
- ◆ zahtjev (s, o, a) - pristup dozvoljen ako a postoji u elementu matrice za s i o

KORISNICI	OBJEKTI		
	$Datoteka_1$	$Datoteka_2$	$Program_1$
k_1	read, write	read, write	execute
k_2	read		
k_3		read	execute

System R model

- ◆ 1970-e - IBM San Jose
- ◆ objekti - tablice i pogledi
- ◆ dozvole - *select, update, insert, delete, drop*
- ◆ subjekt koji kreira tablicu – vlasnik (ima sve ovlasti nad tablicom)
- ◆ dozvola s mogućnošću prenošenja (GRANT opcija)
 - subjekt kojemu je vlasnik dodijelio dozvolu može tu dozvolu dodijeliti drugim subjektima (bez GRANT opcije ili s GRANT opcijom)
- ◆ ukidanje dozvola
 - **kaskadno**, na temelju trenutka dodjeljivanja
 - ukidaju se sve dozvole koje je dodijelio korisnik kojem se ukida dozvola, a koje ne bi mogle biti dodijeljene bez postojanja dozvole koja se ukida
 - ukidanje dozvola se iterativno primjenjuje na sve korisnike koji su primili dozvole pristupa od svih korisnika s kojih je dozvola povučena
 - zahtijeva pamćenje povijesti i vremena dodjeljivanja dozvola

Diskrečijsko upravljanje pristupom u bazama podataka

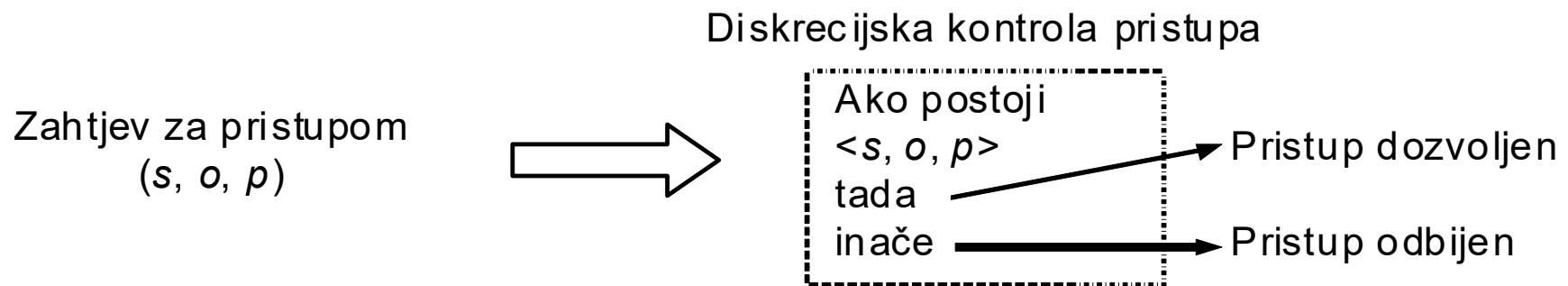
- ◆ podržano SQL standardom
- ◆ podržano u većini današnjih SUBP

- ◆ određenom korisniku potrebno je eksplicitno dodijeliti dozvolu za obavljanje određene operacije nad određenim objektom (autorizacija)
 - ◆ dozvole su opisane trojkama **<korisnik, objekt, vrsta operacije>**, npr:
 - <horvat, ispit, čitanje>
 - <horvat, ispit, izmjena>
 - <novak, predmet, čitanje>

 - ◆ podaci o dodijeljenim dozvolama pohranjuju se u rječnik podataka

Diskrečijsko upravljanje pristupom u bazama podataka

- ◆ prije obavljanja svake operacije, **SUBP provjerava ima li korisnik dozvolu za obavljanje operacije nad objektom** (upravljanje pristupom)
 - ◆ kada korisnik *novak* pokuša obaviti operaciju čitanja objekta (tablice) *predmet*, SUBP provjerava postoji li dozvola u obliku trojke *<novak, predmet, čitanje>*



Upravljanje pristupom u SQL-u

- ◆ **Mehanizmi upravljanja pristupom**
 - naredbe za dodjeljivanje (**GRANT**) i ukidanje dozvola (**REVOKE**)
 - virtualne tablice (view)
 - pohranjene procedure
 - modifikacija upita
- ◆ **Objekti**
 - tablica (table)
 - atribut (stupac tablice, column)
 - virtualna tablica (pogled, view)
 - pohranjena procedura
 - baza podataka (neki sustavi, npr. IBM Informix)
- ◆ **Vlasnik objekta** - korisnik koji je kreirao objekt
 - implicitno dobiva dozvole za obavljanje svih vrsta operacija nad objektom, uključujući
 - dozvole za dodjeljivanje svih vrsta dozvola nad tim objektom drugim korisnicima i
 - uništavanje objekta

SUBP i baze podataka

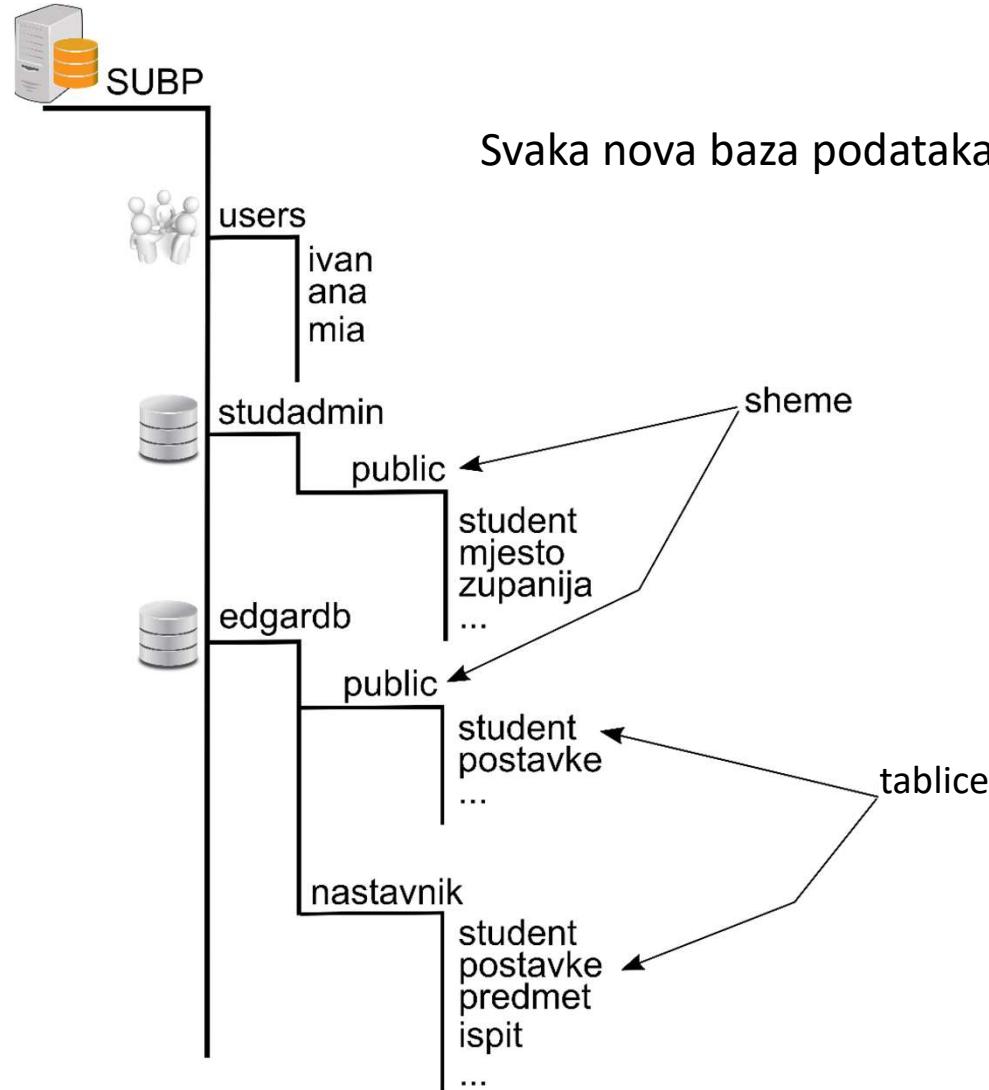
- ◆ SUBP općenito sadrži više (N) baza podataka
 - Korisnici su dijeljeni, na razini cijelog SUBP-a
 - To ne znači da imaju pravo pristupa svim bazama podataka
 - Ne mogu postojati dva korisnika „ivan”
 - Korisnik se pri spajanju na SUBP zapravo spaja na odabranu bazu podataka (npr. *studadmin*)

Sheme (eng. schemas)

- ◆ PostgreSQL:

- Baza podataka sadrži jednu ili više **shema**
- Sheme sadrže tablice, virtualne tablice (, funkcije, ...)
- Različite sheme mogu sadržavati istoimene tablice
- Sheme analogne s:
 - Mapama u datotečnom sustavu (s tim da se ne mogu gnijezditi)
 - Imenskim područjima (*namespaces*) u programskim jezicima

SUBP/BP/Shema



Zašto sheme?

- ◆ Omogućiti višekorisnički pristup bazi podataka, pri čemu želimo razdijeliti korisnike, odnosno pristup objektima baze podatka (tablice, funkcije, ...)
- ◆ Organizirati tablice u logičke grupe, kako bi s njima lakše upravljali (npr. javno, interno, admin, ...)
- ◆ Uspostaviti sustav dozvola (objašnjeno kasnije)

Sheme - SQL

- ◆ Stvaranje:

```
CREATE SCHEMA student;

CREATE TABLE student.postavke (
    username TEXT primary key,
    cm_skin TEXT not null
);
```

- ◆ Pristup:

```
-- schema.table
-- database.schema.table
SELECT * FROM student.postavke
```

- ◆ Brisanje:

```
DROP SCHEMA student;
-- cannot drop schema student because
-- other objects depend on it
DROP SCHEMA student CASCADE;
-- obrisani i sadržani objekti!!
```

Shema *public* je opcionalna, može se obrisati.

Određivanje sheme (SSP - schema search path)

- ◆ Ako se u SQL naredbi ne upotrijebi puno ime tablice, SUBP pretražuje SSP i pokušava ga odrediti:
 - Koristi se **prva** pronađena tablica
 - Ako se ne pronađe, javlja se greška (to ne znači da tablica tog imena ne postoji!)
- ◆ Prva **postojeća** shema u SSP se zove **trenutna shema**
- ◆ Trenutna shema se koristi za stvaranje novih objekata (tablica, ...)
- ◆ Trenutne postavke za SSP se mogu dobiti sljedećom naredbom:

```
SHOW search_path;
```

search_path
"\$user", public

- Kao trenutnu shemu PostgreSQL će odrediti shemu "\$user", ako takva postoji
 - Ako ne postoji, trenutna shema postaje *public*
-
- ◆ Ako je CURRENT_USER npr. *tibor*, tada je "\$user" shema koja se zove *tibor*

Određivanje sheme - Primjer

Vlasnik baze podataka kreirao je korisnika *tibor* i sljedeće dvije sheme:

```
CREATE USER tibor WITH PASSWORD 'tiborPwd';
CREATE SCHEMA student;
CREATE SCHEMA nastavnik;
```

Nakon uspostavljanja korisničke sjednice s bazom podataka, *tibor* obavlja sljedeću naredbu:

```
CREATE TABLE ocjena
(sifOcjena int PRIMARY KEY,
 opisOcjena CHAR(2) NOT NULL,)
```

U kojoj shemi će biti kreirana tablica ocjena?

U shemi *public* jer shema *tibor* ne postoji.

Gornja naredba je ekvivalentna naredbi:

```
CREATE TABLE public.ocjena
(sifOcjena int PRIMARY KEY,
 opisOcjena CHAR(2) NOT NULL,)
```

Vrste dozvola u SQL-u na razini baze podataka (dbPrivilege)

- ◆ Različiti SUBP imaju različita rješenja za dodjeljivanje dozvola na razini baze podataka.
- ◆ PostgreSQL:
 - CONNECT
 - Dozvoljava spajanje (uspostavljanje SQL-sjednice) na bazu podataka
 - Spojeni korisnik može obavljati operacije nad objektima za koje je dobio dozvolu od vlasnika objekta ili je njihov vlasnik
 - Preddefinirano ponašanje je da korisnik PUBLIC (pa i **tibor**) ima CONNECT dozvolu na bazu podataka u PostgreSQL SUBP
 - CREATE
 - Dozvoljava stvaranje novih shema u bazi podataka

- ◆ PostgreSQL:

- **USAGE**

- Nužan preduvjet za pristupanje objektima sadržanim u shemi. Ne podrazumijeva nikakve daljnje dozvole za konkretnе objekte u shemi.

- **CREATE**

- Dozvoljava stvaranje novih objekata (tablice, funkcije, ...) u shemi.

- Preddefinirano ponašanje:

- Korisnik nema dozvolu pristupa nijednom objektu sheme kojoj nije vlasnik.
 - Za pristup mu vlasnik sheme treba dodijeliti dozvolu USAGE
 - Za kreiranje objekata u shemi, dodatno mora dobiti CREATE
 - PUBLIC ima **CREATE** i **USAGE** dozvole **za shemu public**

Vrste dozvola u SQL-u na razini [virtualne] tablice (*tablePrivilege*)

- ◆ **SELECT [(*columnList*)]**
 - čitanje n-torki (ili vrijednosti navedenih atributa) [virtualne] tablice
- ◆ **UPDATE [(*columnList*)]**
 - Izmjena n-torki (ili vrijednosti navedenih atributa) [virtualne] tablice
- ◆ **INSERT**
 - unos n-torki [virtualne] tablice
- ◆ **DELETE**
 - brisanje n-torki [virtualne] tablice
- ◆ **ALL PRIVILEGES**
 - sve do sada navedene vrste operacija nad [virtualnom] tablicom
- ◆ itd. gore je naveden samo dio dozvola

SQL naredbe za dodjeljivanje i ukidanje dozvola

- ◆ **GRANT** *dbPrivilege* ON DATABASE name TO { PUBLIC | *userList* }
 - ◆ **REVOKE** *dbPrivilege* ON DATABASE name FROM { PUBLIC | *userList* }
-
- ◆ **GRANT** *schemaPrivilege* ON SCHEMA name TO { PUBLIC | *userList* }
 - ◆ **REVOKE** *schemaPrivilege* ON SCHEMA name FROM { PUBLIC | *userList* }
-
- ◆ **GRANT** *tablePrivilegeList* ON { *tableName* | *viewName* }
 TO { PUBLIC | *userList* }
 [WITH GRANT OPTION]
 - ◆ **REVOKE** *tablePrivilegeList* ON { *tableName* | *viewName* }
 FROM { PUBLIC | *userList* }
 [CASCADE | RESTRICT]

```
GRANT { { CREATE | USAGE } [ , ... ] | ALL  
GRANT { { CREATE | USAGE } [ , ... ] | ALL
```

PostgreSQL - preddefinirane dozvole korisnika PUBLIC

- ◆ Ključna riječ PUBLIC (<> shema *public*!)
 - Označava sve korisnike, čak i one koji će tek nastati
- ◆ PgSQL - preddefinirane dozvole korisnika PUBLIC:
 - Dozvola uspostavljanja konekcije sa svim bazama na PgSQL SUBP

```
GRANT CONNECT ON DATABASE * TO PUBLIC;
```
 - Dozvole USAGE i CREATE za sve sheme public u svim bazama na PgSQL SUBP

```
GRANT ALL ON SCHEMA public TO PUBLIC;
```


(kao da smo napisali i GRANT USAGE i GRANT CREATE)
 - Primijetite da PUBLIC nema nikakvu dozvolu na razini tablica u shemi **public**

Primjer

Mnogi koriste ovakav sustav (u produkciji), za nešto strože inicijalne postavke sigurnosti:

```
--ACCESS DB
REVOKE CONNECT ON DATABASE dbName FROM PUBLIC;
GRANT CONNECT ON DATABASE dbName TO user;

--ACCESS SCHEMA
REVOKE ALL      ON SCHEMA public FROM PUBLIC;
GRANT USAGE      ON SCHEMA public  TO user;

--ACCESS TABLES (pretpostavka je da postoje dolje navedene uloge)
GRANT SELECT          ON ALL TABLES IN SCHEMA public TO read_only;
GRANT SELECT, INSERT,
       UPDATE, DELETE   ON ALL TABLES IN SCHEMA public TO read_write;
GRANT ALL             ON ALL TABLES IN SCHEMA public TO admin;
```

Primjer 1 (PostgreSQL):

student	matBr	ime	prez	pbr	adresa
---------	-------	-----	------	-----	--------

ispit	matBr	nazPred	datIsp	ocj
-------	-------	---------	--------	-----

Korisnik badmin treba

- kreirati bazu podataka studBaza
- korisniku PUBLIC ukinuti dozvolu spajanja na studBaza
- korisniku PUBLIC ukinuti sve dozvole za shemu *public* u studBaza
- kreirati tablice student i ispit
- kreirati korisnike *horvat*, *novak* i *kolar* i omogućiti im spajanje na studBaza i korištenje *public* sheme u studBaza
- ◆ korisnik *horvat* treba dobiti dozvole:
 - pregled svih podataka u tablicama student i ispit
 - unos, izmjena, brisanje svih podataka u tablici ispit
- ◆ korisnik *novak* treba dobiti dozvole:
 - pregled svih podataka u tablici student
 - izmjena poštanskog broja i adrese u tablici student
- ◆ korisnik *kolar* treba dobiti dozvolu:
 - pregled svih podataka u tablici student, osim adrese

Primjer 1 (nastavak, PostgreSQL):

postgres ← naredbu obavlja korisnik **postgres** (**SUPERUSER**)

```
CREATE USER badmin WITH CREATEDB CREATEROLE  
                      PASSWORD 'badminPwd';
```

korisnik badmin dobiva dozvolu kreiranja baza podataka i korisnika.

badmin ← naredbe obavlja korisnik **badmin**

```
CREATE DATABASE studbaza;  
  
REVOKE CONNECT ON DATABASE studBaza  
    FROM PUBLIC;
```

korisnik badmin je vlasnik baze podataka studBaza. Može ukinuti preddefiniranu dozvolu CONNECT korisniku PUBLIC.

postgres

```
REVOKE ALL ON SCHEMA public FROM PUBLIC;
```

vlasnik sheme *public* u svakoj bazi podataka je korisnik **postgres** (specifičnost PgSQL). Korisnik **badmin** nema ovlasti za ovu naredbu.

badmin

```
CREATE TABLE student (...);  
CREATE TABLE ispit (...);  
  
CREATE USER horvat;  
CREATE USER kolar;  
CREATE USER novak;
```

kreiranje novih objekata u bazi.
tablice će biti kreirane u shemi public.

kreiranje korisnika s mogućnošću uspostavljanja SQL-sjednice na razini SUBP

Primjer 1 (nastavak, PostgreSQL):

badmin

```
GRANT CONNECT ON DATABASE studbaza TO horvat;
GRANT CONNECT ON DATABASE studbaza TO novak;
GRANT CONNECT ON DATABASE studbaza TO kolar;

GRANT USAGE ON SCHEMA public TO horvat;
GRANT USAGE ON SCHEMA public TO novak;
GRANT USAGE ON SCHEMA public TO kolar;
```

```
GRANT SELECT ON student TO horvat;

GRANT SELECT, INSERT
    , UPDATE, DELETE ON ispit
TO horvat;

GRANT SELECT ON student TO novak;

GRANT UPDATE(pbr, adresa)
ON student TO novak;

GRANT SELECT(matBr, ime
            , prez, pbr)
ON student TO kolar;
```

- dozvole spajanja na studBaza.
Treba jer je ukinuta CONNECT
dozvola za PUBLIC.
- dozvola korištenja sheme *public*.
Treba jer je ukinut USAGE i
CREATE za PUBLIC.
- dozvola korisniku *horvat* za pregled
podataka u tablici student
- dozvole korisniku *horvat* za pregled,
unos, izmjenu i brisanje podataka u
tablici ispit
- dozvola korisniku *novak* za pregled
podataka u tablici student
- dozvola korisniku *novak* za izmjenu
vrijednosti atributa u tablici student
- dozvola korisniku *kolar* za pregled svih
podataka u tablici student, osim adrese

Primjer 2 (PostgreSQL):

badmin

```
CREATE DATABASE studBaza;
CREATE SCHEMA student;

CREATE TABLE student.postavke (
    username text primary key, ...);
CREATE TABLE postavkePub(
    username text primary key, ...);
```

korisnik badmin kreira bazu podataka studBaza, te dvije tablice, jednu u shemi student, drugu u PUBLIC shemi

Sjetimo se: PostgreSQL (*default*) daje CONNECT dozvolu korisniku PUBLIC!

tibor

```
CREATE TABLE postavkeTib (...)

INSERT INTO postavkeTib VALUES (...);
```

Može, jer :

- ima CONNECT (bez CONNECT ne bi mogao uspostaviti SQL-sjednicu),
- ima USAGE i CREATE za shemu public u kojoj se stvara *postavketib*
- je vlasnik *postavketib* pa može obaviti INSERT

tibor

```
SELECT * FROM postavkePub;
INSERT INTO postavkePub VALUES (...);

SELECT * FROM student.postavke;
INSERT INTO student.postavke ...;

CREATE TABLE student.T2(...);

CREATE SCHEMA moja;
```

NE može, jer:

- USAGE na shemu *public* ne uključuje dozvole za operacije nad tablicama
- Nije mu dana dozvola za student.postavke
- Nema dozvole (USAGE) za shemu student
- Nema dozvole za stvaranje sheme

Primjer 2 (nastavak):

tibor

```
DROP TABLE postavkePub;
```

→ ne može jer nije vlasnik objekta (niti je SUPERUSER)

kolar

```
SELECT * FROM postavkePub;
```

→ NE može, jer nema dozvole za operacije nad postavkePub

tibor

```
GRANT CONNECT ON DATABASE  
studBaza TO kolar;
```

→ ne može jer nije SUPERUSER

tibor

```
GRANT SELECT  
ON postavkeTib TO kolar;
```

→ Može, jer je **vlasnik** tablice postavkeTib

Primjer 2 (nastavak):

postgres

```
GRANT CREATE ON DATABASE  
studBaza TO tibor;
```

Može, jer je SUPERUSER

tibor

```
CREATE SCHEMA tibor;
```

Može, jer sad ima dozvolu

tibor

```
CREATE TABLE tibor.postavke( . . . );  
GRANT SELECT ON tibor.postavke TO kolar;
```

Može, jer je vlasnik sheme

kolar

```
SELECT * FROM tibor.postavke;
```

Ne može, jer nema dozvolu na
shemu (ima samo na tablicu)

tibor

```
GRANT USAGE ON SCHEMA tibor TO kolar;
```

Može, jer je vlasnik sheme

kolar

```
SELECT * FROM tibor.postavke;
```

Može

Dodjeljivanje prenosivih dozvola

- ◆ Ako se korisniku dozvola dodijeli uz navođenje opcije WITH GRANT OPTION, korisnik će moći dodjeljivati tu istu dozvolu ostalim korisnicima (unatoč tome što nije vlasnik objekta)

Primjer:

korisnik1

```
CREATE TABLE ispit (...);  
GRANT SELECT ON ispit TO korisnik2 WITH GRANT OPTION;  
GRANT SELECT ON ispit TO korisnik3 WITH GRANT OPTION;
```

korisnik2

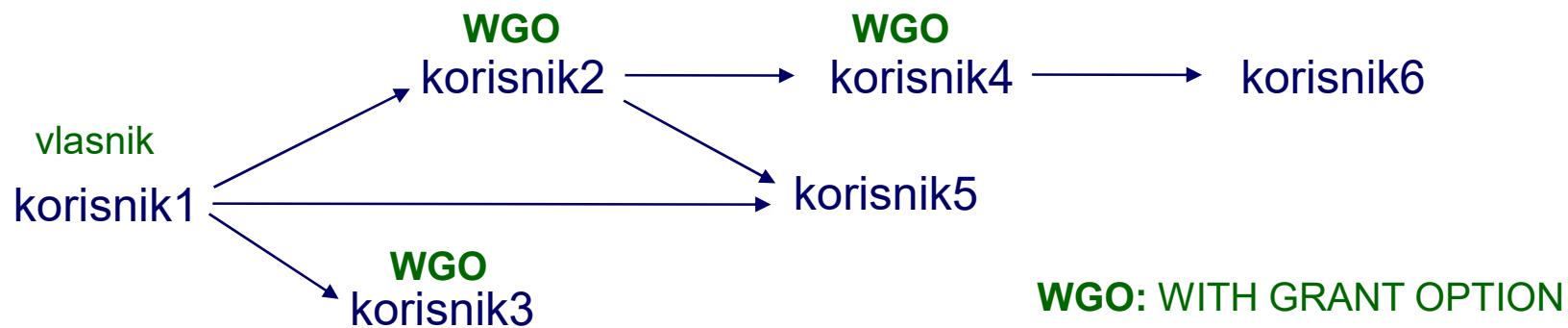
```
GRANT SELECT ON ispit TO korisnik4 WITH GRANT OPTION;  
GRANT SELECT ON ispit TO korisnik5;
```

korisnik4

```
GRANT SELECT ON ispit TO korisnik6;
```

korisnik1

```
GRANT SELECT ON ispit TO korisnik5;
```



Ukidanje dozvola

- korisnik koji je dozvolu dodijelio, tu istu dozvolu može ukinuti naredbom REVOKE

Primjer:

- vlasnik baze podataka studBaza je korisnik badmin
- vlasnik tablice mjesto je korisnik horvat

horvat

```
GRANT SELECT, UPDATE ON mjesto TO novak WITH GRANT OPTION;
```

novak

```
GRANT SELECT, UPDATE ON mjesto TO kolar;
```

- npr. naredbu:

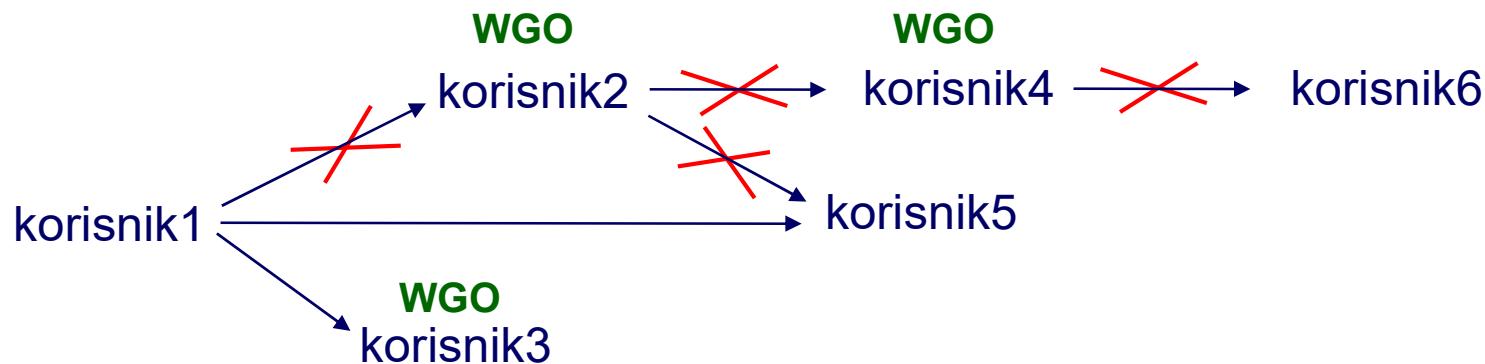
```
REVOKE UPDATE ON mjesto FROM kolar;
```
- može obaviti korisnik novak jer je novak korisnik koji je dozvolu dodijelio

Ukidanje dozvola dodijeljenih temeljem WITH GRANT OPTION

- ukidanjem dozvole korisniku x (koji je dozvole dalje dodjeljivao temeljem ovlasti stečene pomoću WITH GRANT OPTION) **uz primjenu opcije CASCADE**, dozvola se ukida i svim ostalim korisnicima koji su dotičnu dozvolu stekli od korisnika x (neposredno ili posredno)

Primjer: **korisnik1**

```
REVOKE SELECT ON ispit FROM korisnik2 CASCADE;
```



- obavljanjem naredbe dozvolu gube korisnik2, korisnik4 i korisnik6
- korisnik5 će izgubiti dozvolu koju je dobio od korisnika2, ali će zadržati dozvolu koju je dobio od korisnika1
- **ukoliko se opcija CASCADE ne navede**, naredba REVOKE neće uspjeti ako postoji dodatne neposredne dozvole

IBM Informix: Dodjeljivanje i ukidanje dozvola

- ◆ na razini baze podataka:

```
GRANT dbPrivilege TO { PUBLIC | userList }
```

```
REVOKE dbPrivilege FROM { PUBLIC | userList }
```

- ◆ na razini [virtualne] tablice:

```
GRANT tablePrivilegeList ON { tableName | viewName }  
    TO { PUBLIC | userList | roleList }  
    [ WITH GRANT OPTION ]
```

```
REVOKE tablePrivilegeList ON { tableName | viewName }  
    FROM { PUBLIC | userList | roleList }  
    [ CASCADE | RESTRICT ]
```

IBM Informix: Vrste dozvola na razini baze podataka

CONNECT	<ul style="list-style-type: none">uspostavljanje SQL-sjednice i obavljanje operacija nad objektima za koje je korisnik dobio dozvolu od vlasnika objekta ili je njihov vlasnik, kreiranje virtualnih i privremenih tablica
RESOURCE	<ul style="list-style-type: none">CONNECT + kreiranje novih objekata u bazi podataka (tablica, indeksa, ograničenja, pohranjenih procedura ...)
DBA	<ul style="list-style-type: none">RESOURCE + neovisno o vlasništvu i dozvolama nad objektima u bazi podataka: sve vrste operacija nad svim objektima, uništavanje svih objekata (uključujući i bazu podataka)korisnik koji kreira bazu podataka je vlasnik te baze podataka i implicitno dobiva DBA (<i>Database administrator</i>) dozvolu

Primjer:

DBA

```
GRANT DBA TO u1;  
GRANT RESOURCE TO u1;
```

- nema učinka dodjeljivanje RESOURCE dozvole korisniku koji već ima DBA dozvolu - korisnik *u₁*, i dalje ima DBA dozvolu
- ukidanjem DBA dozvole, korisnik i dalje ima CONNECT dozvolu
- za sprečavanje uspostavljanja SQL-sjednice potrebno je ukinuti i CONNECT dozvolu

```
REVOKE DBA FROM u1;  
REVOKE CONNECT FROM u1;
```

IBM Informix: Vrste dozvola na razini [virtualne] tablice

SELECT [(columnList)]	◆ čitanje n-torki (ili vrijednosti navedenih atributa) [virtualne] tablice
UPDATE [(columnList)]	◆ izmjena n-torki (ili vrijednosti navedenih atributa) [virtualne] tablice
INSERT[(columnList)]	◆ unos n-torki (ili vrijednosti navedenih atributa) [virtualne] tablice
DELETE	◆ brisanje n-torki [virtualne] tablice
REFERENCES [(columnList)]	◆ korištenje tablice (ili samo navedenih atributa) kao pozivane tablice pri definiranju stranog ključa)
INDEX	◆ kreiranje indeksa nad tablicom
ALTER	◆ izmjena strukture tablice i definiranje integritetskih ograničenja
ALL PRIVILEGES	◆ sve vrste operacija nad [virtualnom] tablicom

Primjer:

```
UPDATE nastavnik SET koef = 0.9*koef
WHERE NOT EXISTS
  (SELECT * FROM predmetGrupa
   WHERE predmetGrupa.sifNastavnik = nastavnik.sifNastavnik
     AND predmetGrupa.akGodina = 2022);
```

Potrebne dozvole:

- ◆ pristup bazi podataka
- ◆ SELECT: *nastavnik.sifNastavnik, nastavnik.koef , predmetGrupa.sifNastavnik, predmetGrupa.akGodina*
- ◆ UPDATE: *nastavnik.koef*

ORACLE: kategorije dozvola

- ◆ ORACLE: dozvole se mogu svrstati u dvije općenite kategorije:

- sistemske dozvole

- omogućavaju izvršavanje različitih tipova naredbi
 - ne odnose se na neki konkretni objekt baze podataka, već na određenu operaciju ili klasu operacija nad tipom objekta
 - neke od sistemskih dozvola su: CREATE USER; ALTER USER; DROP USER; CREATE SESSION; CREATE ANY INDEX; ALTER ANY INDEX; DROP ANY INDEX; CREATE TABLE; CREATE ANY TABLE; ALTER ANY TABLE; DELETE ANY TABLE; DROP ANY TABLE; INSERT ANY TABLE; SELECT ANY TABLE; UPDATE ANY TABLE; CREATE VIEW; CREATE ANY VIEW; DROP ANY VIEW; CREATE PROCEDURE; CREATE ANY PROCEDURE; EXECUTE ANY PROCEDURE ...

```
GRANT CREATE SESSION TO u1;
```

- korisniku *u1* dozvoljeno je uspostavljanje SQL-sjednice

- dozvole nad objektima

- omogućavaju obavljanje određenih operacija na određenom objektu baze podataka
 - npr. SELECT, UPDATE, INSERT i DELETE operacije na tablicama, ALTER, REFERENCES, INDEX i ALL na tablicama, EXECUTE na pohranjenim procedurama

SQL Server: kategorije dozvola

- ◆ administrator korisniku treba omogućiti pristup instanci SQL Server poslužitelja (CREATE LOGIN naredbom) te pristup bazi podataka (CREATE USER naredbom), npr:

```
CREATE LOGIN loginNameU1 WITH PASSWORD = 'ABCxyz' MUST_CHANGE;
USE stuSluBaza;
CREATE USER u1 FOR LOGIN loginNameU1;
```

- dozvole se mogu svrstati u dvije općenite kategorije:
 - dozvole obavljanja naredbi – upravljaju obavljanjem naredbi kao što su CREATE TABLE, CREATE VIEW, CREATE FUNCTION, CREATE PROCEDURE, itd.
 - dozvole nad objektima baze podataka – upravljaju obavljanjem operacije na postojećem objektu baze podataka, npr. DELETE, INSERT, SELECT, UPDATE, EXECUTE, REFERENCES ...

SQL Server: negativne dozvole (tj. zabrane)

- **SQL Server:** osim dodjeljivanja dozvole pristupa (GRANT), omogućeno je postavljanje zabrane, odnosno dodjeljivanje negativne dozvole (DENY)
- REVOKE ukida dozvole dodijeljene GRANT i DENY naredbama

```
DENY CREATE TABLE TO u1;
```

- korisniku *u1* zabranjuje se izvođenje CREATE TABLE naredbe

```
REVOKE CREATE TABLE FROM u1;
```

- korisniku *u1* ukida se zabrana izvođenja CREATE TABLE naredbe

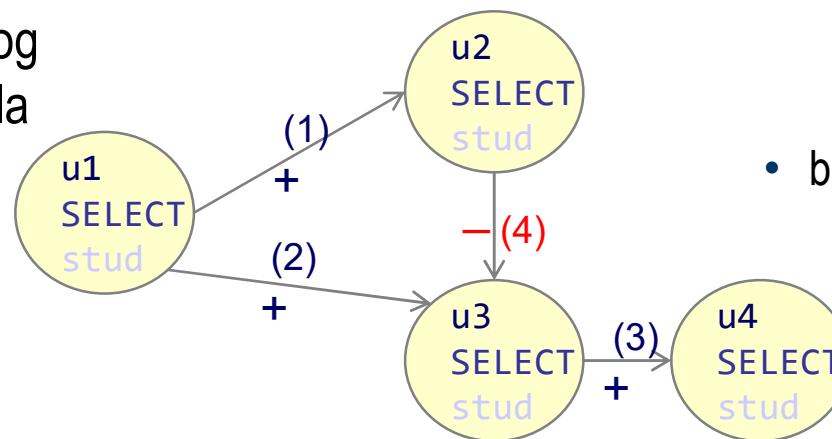
```
DENY SELECT (jmbg) ON student TO u1;
```

- korisniku *u1* zabranjuje se izvođenje SELECT naredbe nad atributom *student.jmbg*

```
REVOKE SELECT (jmbg) ON student TO u1;
```

- korisniku *u1* ukida se zabrana izvođenja SELECT naredbe nad atributom *student.jmbg*

- konflikti koji se pojavljuju zbog postojanja negativnih dozvola razrješavaju se u skladu s politikom: ***prioritetne su negativne dozvole:***



- blokirane su (nisu uklonjene):
 - pozitivna dozvola koju je *u1* dodijelio korisniku *u3*
 - pozitivna dozvola koju je *u3* dodijelio korisniku *u4*

Zaštita i sigurnost informacijskih sustava

Sigurnost baza podataka, 2. dio

Upravljanje pristupom ovisno o sadržaju i kontekstu

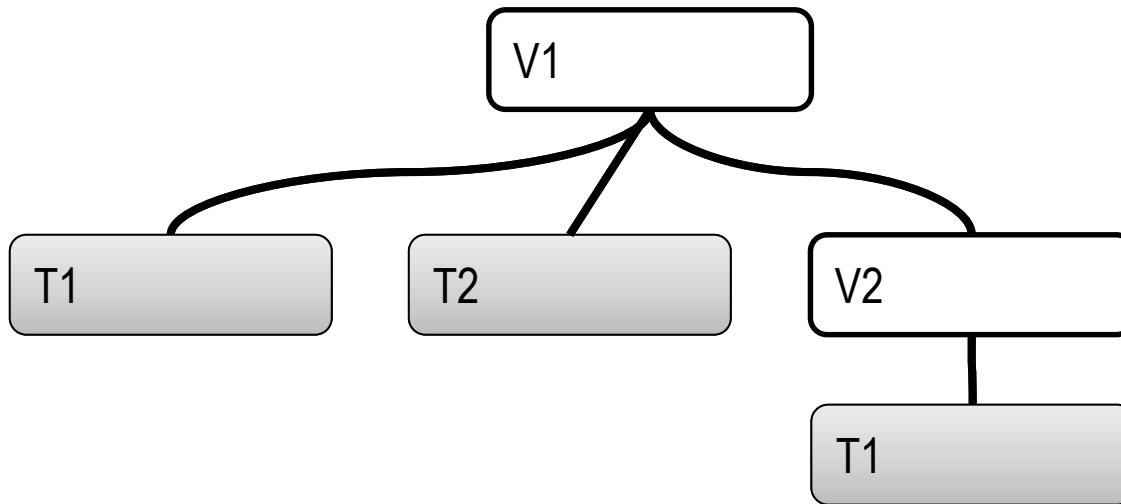
- ◆ upravljanje pristupom ovisno o **sadržaju** (*content-dependent, value-dependent, data-dependent*)
 - pristup objektu na temelju sadržaja jedne ili više njegovih komponenata
- ◆ upravljanje pristupom ovisno o **kontekstu** (*context-dependent, system-dependent*)
 - pristup objektu ovisi o trenutnom kontekstu - u obzir uzima predikate sustava (vrijeme, lokacija ...), trenutnog korisnika

Upravljanje pristupom ovisno o sadržaju i kontekstu

- ◆ dva načina implementacije upravljanja pristupom ovisnog o sadržaju i kontekstu:
 - **definiranje virtualnih tablica** koje odabiru objekt čiji sadržaj zadovoljava dani uvjet te dodjeljivanje dozvola na virtualne tablice, umjesto na temeljne tablice
 - podržano u svim komercijalnim SUBP- ovima
 - **povezivanje predikata** (ili logičke kombinacije predikata) s autorizacijama
 - predikat izražava uvjet nad sadržajem objekta koji mora biti zadovoljen kako bi pristup bio dozvoljen
 - podržan u Oracle SUBP-u

Virtualne tablice

- ◆ Tablica kojoj su shema i sadržaj definirani izrazom relacijske algebre čiji su operandi temeljne ili virtualne tablice.
 - u praksi, shema i sadržaj virtualne tablice opisuju se u obliku SQL upita



- ◆ Sadržaj virtualne tablice dinamički se određuje u trenutku obavljanja operacije nad virtualnom tablicom: ovisi o trenutačnom stanju temeljnih tablica

Virtualna tablica (primjer)

polozeniIspit		
mbr	sifPred	ocj
100	1001	5
101	1001	4
102	1001	3
100	1002	2
101	1002	5
100	1003	3
101	1003	3

```
CREATE VIEW projek (sifPred  
, prosOcj) AS  
SELECT sifPred, AVG(ocj)  
FROM polozeniIspit  
GROUP BY sifPred;
```

projek	
sifPred	prosOcj
?	?

- Tek u trenutku obavljanja upita, SUBP dinamički određuje sadržaj virtualne tablice *projek*

```
SELECT MIN(prosOcj) AS minPros  
, MAX(prosOcj) AS maksPros  
FROM projek;
```

projek	
sifPred	prosOcj
1001	4.00
1002	3.50
1003	3.00

minPros	maksPros
3.00	4.00

Primjer (nastavak)

- ◆ Sadržaj virtualne tablice se ponovno određuje pri izvršavanju svakog upita koji koristi tu virtualnu tablicu

```
INSERT INTO polozeniIspit VALUES(102, 1003, 2);
```

```
SELECT MIN(prosOcj) AS minPros  
      , MAX(prosOcj) AS maksPros  
FROM prosjek;
```

polozeniIspit

mbr	sifPred	ocj
100	1001	5
101	1001	4
102	1001	3
100	1002	2
101	1002	5
100	1003	3
101	1003	3
102	1003	2

prosjek

sifPred	prosOcj
1001	4.00
1002	3.50
1003	2.67

minPros	maksPros
2.67	4.00

Svojstva virtualne tablice

- ◆ Obavljanjem naredbe CREATE VIEW u rječnik podataka se pohranjuje samo definicija virtualne tablice
 - sadržaj virtualne tablice se određuje tek za vrijeme izvršavanja upita koji koristi virtualnu tablicu
 - odnosno, sadržaj virtualne tablice uvijek odražava sadržaj temeljnih tablica u trenutku izvršavanja upita u kojem se virtualna tablica koristi
- ◆ virtualne tablice se u upitima mogu koristiti na svim mjestima gdje se mogu koristiti temeljne tablice
 - između ostalog i za kreiranje novih virtualnih tablica
- ◆ definicija virtualne tablice je trajno pohranjena u bazi podataka
- ◆ virtualna tablica je u dosegu ("vidljiva je") u svim SQL-sjednicama

Atributi virtualne tablice

- ◆ Ako se nazivi atributa u definiciji virtualne tablice ne navedu, nazivi atributa virtualne tablice određeni su nazivima atributa u SELECT naredbi kojom se definira sadržaj virtualne tablice
- ◆ tipovi podataka za atrubute virtualne tablice proizlaze iz tipova podataka atributa temeljnih tablica koje se koriste u definiciji virtualne tablice

```
CREATE VIEW zadrani1 AS
    SELECT mbr, ime, prez
        FROM osoba
       WHERE pbrStan = 23000;
SELECT * FROM zadrani1;
```

mbr	ime	prez
101	Ana	Kolar
103	Tea	Ban

```
CREATE VIEW zadrani2 (matBr
                      , imeSt
                      , prezSt) AS
    SELECT mbr, ime, prez
        FROM osoba
       WHERE pbrStan = 23000;
SELECT * FROM zadrani2;
```

osoba

mbr	ime	prez	pbrStan
101	Ana	Kolar	23000
102	Tomo	Novak	21000
103	Tea	Ban	23000

matBr	imeSt	prezSt
101	Ana	Kolar
103	Tea	Ban

Atributi virtualne tablice

- ◆ Ako se u listi za selekciju pri definiciji virtualne tablice koriste izrazi, nazine atributa virtualne tablice treba eksplicitno navesti

polozeniIspit		
mbr	sifPred	ocj
100	1001	2
101	1001	4
102	1001	3
100	1002	2
101	1002	5
100	1003	3
101	1003	3

```
CREATE VIEW projek (sifPred  
, prosOcj) AS  
SELECT sifPred, AVG(ocj)  
FROM polozeniIspit  
GROUP BY sifPred;
```

ispravno

```
CREATE VIEW projek AS  
SELECT sifPred  
, AVG(ocj)  
FROM polozeniIspit  
GROUP BY sifPred;
```

neispravno

Dopušteno, ali **besmisleno**
U PostgreSQLu, atribut će se zvati „?column?”.
Ako se navedu dva izraza, onda dolazi do greške.

Materijalizirane virtualne tablice

- Materijalizirane virtualne tablice: SUBP fizički pohranjuje sadržaj virtualne tablice. Kada se promijeni sadržaj neke od temeljnih tablica pomoću kojih je virtualna tablica definirana, SUBP automatski mijenja i sadržaj materijalizirane virtualne tablice
 - prednost: virtualne tablice koje se vrlo često koriste, a čiji se sadržaj određuje složenim upitima, ne moraju se svaki puta kada neki korisnik koristi tu virtualnu tablicu ponovno izračunavati
 - nedostatak: ako se temeljne tablice pomoću kojih je virtualna tablica definirana često mijenjaju, pri svakoj izmjeni temeljnih tablica troši se dodatno vrijeme radi izmjene sadržaja virtualne tablice
- Podržavaju riječki, Oracle prvi, SQL Server (*Indexed views*)
- PostgreSQL ne održava automatski podatke u materijaliziranoj virtualnoj tablici ažurnim, tj. potrebno je ručno osvježiti podatke

Implementacija virtualnih tablica

- ◆ Kako sustavi za upravljanje bazama podataka izvršavaju upite koji sadrže virtualne tablice (ako se **ne** radi o materijaliziranim virtualnim tablicama)?

Modifikacijom upita

- SUBP ugrađuje elemente definicije virtualne tablice u originalni SQL upit koji koristi virtualnu tablicu - umjesto originalnog SQL upita izvršava se modificirani SQL upit

Izvršavanje modifikacijom upita

- ◆ Primjer:

ispit		
mbr	predmet	ocj
100	Elektronika	3
100	Fizika	2
101	Elektronika	5
101	Fizika	2
102	Fizika	1
103	Fizika	5

stud			
mbr	ime	prez	pbrStan
100	Ivan	Kolar	52100
101	Ana	Horvat	42230
102	Jura	Novak	52100
103	Ana	Ban	52100

mjesto	
pbr	nazMjesto
42000	Varaždin
52100	Pula
42230	Ludbreg

studenti koji su položili predmet Fizika

```
CREATE VIEW polFiz AS
    SELECT stud.* , ocj
        FROM ispit, stud
       WHERE ispit.mbr = stud.mbr
         AND predmet = 'Fizika'
         AND ocj > 1;
```

korisnik obavlja:

```
SELECT * FROM polFiz;
```

↓ SUBP modificira upit

```
SELECT stud.* , ocj
    FROM ispit, stud
   WHERE ispit.mbr = stud.mbr
     AND predmet = 'Fizika'
     AND ocj > 1;
```



mbr	ime	prez	pbrStan	ocj
100	Ivan	Kolar	52100	2
101	Ana	Horvat	42230	2
103	Ana	Ban	52100	5

Primjer (nastavak)

- Ispisati prezime, ime i dobivenu ocjenu iz Fizike za studente koji su položili Fiziku, a stanuju u Puli

korisnik obavlja:

```
SELECT polFiz.prez, polFiz.ime, polFiz.ocj
  FROM polFiz, mjesto
 WHERE polFiz.pbrStan = mjesto.pbr
   AND nazMjesto = 'Pula';
```

```
CREATE VIEW polFiz AS
  SELECT stud.*, ocj
    FROM ispit, stud
   WHERE ispit.mbr = stud.mbr
     AND predmet = 'Fizika'
     AND ocj > 1;
```

↓ SUBP modificira upit

```
SELECT stud.prez, stud.ime, ispit.ocj
  FROM ispit, stud, mjesto
 WHERE ispit.mbr = stud.mbr
   AND predmet = 'Fizika'
   AND ocj > 1
   AND stud.pbrStan = mjesto.pbr
   AND nazMjesto = 'Pula';
```

prez	ime	ocj
Kolar	Ivan	2
Ban	Ana	5

Virtualna tablica: INSERT, UPDATE, DELETE

- virtualne tablice se također mogu koristiti u naredbama INSERT, UPDATE i DELETE

```
CREATE VIEW splitStud AS  
    SELECT mbr, ime, prez, pbrStan  
        FROM stud  
    WHERE pbrStan = 21000;
```

stud			
mbr	ime	prez	pbrStan
100	Ivan	Kolar	31000
101	Ana	Horvat	21000

```
INSERT INTO splitStud  
VALUES (102, 'Jure', 'Novak', 21000);  
  
SELECT * FROM splitStud;
```

mbr	ime	prez	pbrStan
101	Ana	Horvat	21000
102	Jure	Novak	21000

```
INSERT INTO splitStud  
VALUES (103, 'Tea', 'Ban', 10000);  
  
SELECT * FROM splitStud;
```

mbr	ime	prez	pbrStan
101	Ana	Horvat	21000
102	Jure	Novak	21000

n-torka jest unesena u temeljnu tablicu,
ali se "ne vidi" u virtualnoj tablici

```
SELECT * FROM stud;
```

mbr	ime	prez	pbrStan
100	Ivan	Kolar	31000
101	Ana	Horvat	21000
102	Jure	Novak	21000
103	Tea	Ban	10000

Virtualna tablica: INSERT, UPDATE, DELETE

- ◆ SUBP ne može promijeniti "sadržaj virtualne tablice" - umjesto toga mora promijeniti sadržaj temeljnih tablica koje se koriste u definiciji te virtualne tablice

ispit

mbr	predmet	ocj
100	Elektronika	1
100	Fizika	5
101	Elektronika	1
101	Fizika	3

```
CREATE VIEW prosli AS  
SELECT * FROM ispit  
WHERE ocj > 1;
```

```
CREATE VIEW pali AS  
SELECT * FROM ispit  
WHERE ocj = 1;
```

korisnik
obavlja:

```
UPDATE prosli SET ocj = 4  
WHERE mbr = 100  
AND predmet = 'Fizika';
```



SUBP modificira upit

```
UPDATE ispit SET ocj = 4  
WHERE ocj > 1  
AND mbr = 100  
AND predmet = 'Fizika';
```

Virtualna tablica: problem migrirajućih n-torki

- ♦ n-torka se pojavljuje u virtualnoj tablici onda kada zadovoljava uvjet iz definicije virtualne tablice
 - n-torka unesena u virtualnu tablicu ili izmijenjena u virtualnoj tablici može "nestati" iz te virtualne tablice (i eventualno se "pojaviti" u nekoj drugoj virtualnoj tablici)

ispit

	mbr	predmet	ocj
t ₁	100	Elektronika	1
t ₂	100	Fizika	5
t ₃	101	Elektronika	1
t ₄	101	Fizika	3

```
CREATE VIEW prosli AS  
SELECT * FROM ispit  
WHERE ocj > 1;
```

```
CREATE VIEW pali AS  
SELECT * FROM ispit  
WHERE ocj = 1;
```

korisnik
obavlja:

```
UPDATE prosli SET ocj = 1  
WHERE mbr = 100  
AND predmet = 'Fizika';  
INSERT INTO prosli  
VALUES (102, 'Elektronika', 1);
```

- n-torka t_2 je "nestala" iz *prosli* i "pojavila" se u *pali*
- nova n-torka $<102, \text{Elektronika}, 1>$ unesena preko *prosli* se "pojavila" u *pali*

Virtualna tablica: problem migrirajućih n-torki

- ◆ **Rješenje:** virtualne tablice koje se koriste u naredbama koje mijenjaju podatke obavezno se kreiraju uz opciju **WITH CHECK OPTION**
 - SUBP tada ne dopušta izmjenu ili unos n-torke putem virtualne tablice ukoliko n-torka nakon obavljanja operacije više ne bi pripadala virtualnoj tablici putem koje je izmijenjena ili unesena

ispit	mbr	predmet	ocj
	100	Elektronika	1
	100	Fizika	5
	101	Elektronika	1
	101	Fizika	3

```
CREATE VIEW prosli AS  
SELECT * FROM ispit  
WHERE ocj > 1  
WITH CHECK OPTION;
```

```
CREATE VIEW pali AS  
SELECT * FROM ispit  
WHERE ocj = 1  
WITH CHECK OPTION;
```

```
UPDATE prosli SET ocj = 1  
WHERE mbr = 100          pogreška  
AND predmet = 'Fizika';
```

```
UPDATE prosli SET ocj = 4  
WHERE mbr = 100          O.K.  
AND predmet = 'Fizika';
```

```
INSERT INTO prosli      pogreška  
VALUES (102, 'Fizika', 1);
```

```
INSERT INTO prosli      O.K.  
VALUES (102, 'Fizika', 3);
```

```
INSERT INTO pali        pogreška  
VALUES (102, 'Fizika', 3);
```

Neizmjenjive virtualne tablice

- ◆ SUBP ne može promijeniti "sadržaj virtualne tablice" - umjesto toga mora promijeniti sadržaj temeljnih tablica koje se koriste u definiciji te virtualne tablice
 - ako je virtualna tablica definirana tako da SUBP nije u stanju **jednoznačno** odrediti koje operacije treba obaviti na temeljnim tablicama, tada je virtualna tablica **neizmjenjiva (non-updatable)**

polozeniIspit

mbr	sifPred	ocj
100	1001	5
101	1001	4
102	1001	3
100	1002	2
101	1002	5
100	1003	3
101	1003	3

```
CREATE VIEW projek (sifPred  
, prosOcj) AS  
SELECT sifPred, AVG(ocj)  
FROM polozeniIspit  
GROUP BY sifPred;
```

SELECT * FROM projek;

sifPred	prosOcj
1001	4.00
1002	3.50
1003	3.00

```
UPDATE projek SET prosOcj = 4.5  
WHERE sifPred = 1001;
```

?

```
INSERT INTO projek VALUES (1004, 2.5);
```

?

Izmjenjive virtualne tablice

- ◆ Virtualna tablica je izmjenjiva ako u glavnom SELECT dijelu definicije virtualne tablice koristi atributе iz samo jedne temeljne tablice r(R) i pri tome:
 - ne sadrži eliminaciju duplikata pomoću DISTINCT
 - ne sadrži izraze u listi za selekciju (osim trivijalnih izraza koji sadrže samo ime atributa)
 - izostavljeni atributi ne smiju imati NOT NULL ograničenje ili moraju imati prepostavljenu (*default*) vrijednost
 - ne sadrži spajanje ili uniju
 - ne sadrži grupiranje i postavljanje uvjeta nad grupom (GROUP BY i HAVING)
- ◆ Prethodno navedena ograničenja se ne odnose na eventualne podupite koji se koriste unutar WHERE dijela SELECT naredbe koja se koristi za definiciju virtualne tablice

Primjeri izmjenjivih virtualnih tablica

ispit	matBr	sifPred	datIsp	ocj	sifNas
	1111	1001	29.01.2011	1	101
	1111	1001	05.02.2011	3	101
	1111	1003	28.06.2011	2	303
	1111	1002	27.06.2011	4	202
	1234	1001	29.01.2011	3	202

stud	matBr	prez	ime	pbrSt
	1111	Novak	Ivan	10000
	4444	Ban	Marko	51000
	1234	Kolar	Petar	23000

```
CREATE VIEW poloziliNista AS
    SELECT * FROM stud
    WHERE NOT EXISTS
        (SELECT * FROM ispit
            WHERE ispit.matBr = stud.matBr
            AND ocj > 1)
    WITH CHECK OPTION;
```

```
CREATE VIEW ispitizadranal AS
    SELECT matBr
        , sifPred
        , datIsp
        , ocj
    FROM ispit
    WHERE matBr IN (
        SELECT matBr FROM stud
        WHERE pbrSt = 23000)
    WITH CHECK OPTION;
```

Primjeri neizmjenjivih virtualnih tablica

ispit	matBr	sifPred	datIsp	ocj	sifNas
	1111	1001	29.01.2011	1	1111
	1111	1001	05.02.2011	3	1111
	1111	1003	28.06.2011	2	3333
	1111	1002	27.06.2011	4	2222
	1234	1001	29.01.2011	3	2222

```
CREATE VIEW ispitiZadrana2 AS
    SELECT ispit.matBr
        , sifPred
        , datIsp
        , ocj
    FROM ispit, stud
    WHERE ispit.matBr = stud.matBr
        AND pbrSt = 23000;
```

stud	matBr	prez	ime	pbrSt
	1111	Novak	Ivan	10000
	1234	Kolar	Petar	21000

```
CREATE VIEW projek
    (matBr, prosOcj) AS
    SELECT matBr, AVG(ocj)
    FROM ispit
    GROUP BY matBr;
```

```
CREATE VIEW stud1 (ime_pres) AS
    SELECT ime || prez
    FROM stud;
```

```
CREATE VIEW poloziliNesto AS
    SELECT DISTINCT matBr
    FROM ispit
    WHERE ocj > 1;
```

usporediti s izmjenjivom virtualnom
tablicom **ispitiZadrana1** s
prethodne stranice!



Primjena virtualnih tablica u provođenju sigurnosne politike

- ◆ omogućavaju **prikaz samo onih informacija koje su korisniku potrebne:**
 - **zbirne informacije i/ili samo neki atributi tablice i/ili samo neke n-torce iz tablice**
 - korisniku se dodjeljuju ovlasti nad virtualnom tablicom

Primjena virtualnih tablica u kontekstu dozvola

ispit

mbrSt	nazPred	datlsp	ocj
100	Fizika	1.5.2010	3
102	Matematika	7.9.2009	1
102	Matematika	9.2.2010	5
107	Fizika	5.4.2012	4

- ◆ vlasnik tablice ispit je korisnik horvat
- ◆ korisniku novak treba omogućiti pregled samo prosječnih ocjena po predmetima
- ◆ korisniku kolar treba omogućiti pregled, unos, izmjenu i brisanje samo za ispite iz predmeta Fizika

horvat

```
CREATE VIEW prosjek (nazPred, prosOcj) AS
    SELECT nazPred, AVG(ocj)
        FROM ispit
    GROUP BY nazPred;
GRANT SELECT ON prosjek TO novak;

CREATE VIEW ispitFizika AS
    SELECT * FROM ispit
        WHERE nazPred = 'Fizika'
    WITH CHECK OPTION;
GRANT SELECT, INSERT, UPDATE, DELETE
    ON ispitFizika TO kolar;
```

zašto je nužno virtualnu tablicu
ispitFizika kreirati uz opciju
WITH CHECK OPTION?

Dodjeljivanje kontekstno ovisnih dozvola

ispit

mbrSt	sifPred	datIsp	ocj
100	100	1.5.2010	3
102	200	7.9.2009	1
102	200	9.2.2010	5
107	300	5.4.2012	4

nast

sifNast	imeN	prezN	userId
1001	Slavko	Kolar	kolar
1002	Ivo	Ban	ban
1003	Ana	Novak	novak

predaje

sifNast	sifPred
1001	100
1001	200
1002	200
1003	200
1003	300

- ◆ vlasnik tablica je korisnik horvat
- ◆ svakom nastavniku (korisnicima kolar, ban, novak) omogućiti pregled i izmjenu ispita samo iz predmeta koje predaju

horvat

LOŠE RJEŠENJE!

```
CREATE VIEW kolarIspiti AS
    SELECT * FROM ispit
    WHERE sifPred IN (
        SELECT sifPred FROM predaje
        WHERE sifNast = 1001) WITH CHECK OPTION;
GRANT SELECT, UPDATE ON kolarIspiti TO kolar;
```

- ponoviti za svakog nastavnika: banIspiti, novakIspiti, ...
- nova virtualna tablica za svakog novog nastavnika (≈ 150 na FER-u)
- svaki nastavnik upit nad tablicom ispit mora pisati na drugačiji način

Dodjeljivanje kontekstno ovisnih dozvola

ispit

mbrSt	sifPred	datIsp	ocj
100	100	1.5.2010	3
102	200	7.9.2009	1
102	200	9.2.2010	5
107	300	5.4.2012	4

nast

sifNast	imeN	prezN	userId
1001	Slavko	Kolar	kolar
1002	Ivo	Ban	ban
1003	Ana	Novak	novak

predaje

sifNast	sifPred
1001	100
1001	200
1002	200
1003	200
1003	300

horvat

```
CREATE VIEW ispitiZaNastavnike AS
    SELECT * FROM ispit
    WHERE sifPred IN (
        SELECT sifPred FROM predaje, nast
        WHERE predaje.sifNast = nast.sifNast
        AND userId = CURRENT_USER) WITH CHECK OPTION;
GRANT SELECT, UPDATE ON ispitiZaNastavnike TO kolar;
GRANT SELECT, UPDATE ON ispitiZaNastavnike TO ban;
GRANT SELECT, UPDATE ON ispitiZaNastavnike TO novak;
```

ISPRAVNO
RJEŠENJE!

- "sadržaj" virtualne tablice ovisit će o identifikatoru nastavnika koji je ostvario SQL-sjednicu

Pohranjene procedure/funkcije (1)

- ◆ pohranjena **procedura/funkcija** je potprogram koji je pohranjen u rječniku podataka i koji se izvršava u kontekstu sustava za upravljanje bazama podataka
 - procedura je potprogram koji u pozivajući program ne vraća rezultat
 - funkcija je potprogram koji u pozivajući program vraća rezultat
 - koristi se i termin *pohranjena rutina (stored routine)*
- ◆ može biti implementirana kao:
 - SQL procedura - napisana u SQL-u
 - (napomena: u nastavku se pod pojmom *procedura* misli na *SQL proceduru*)
 - vanjska procedura (*external routine*)
 - napisana u eksternom programskom jeziku (npr. Java, C++)
 - poziva se na isti način kao SQL procedura

Pohranjene procedure/funkcije (2)

- ◆ pohranjena je kao objekt u rječniku baze podataka
- ◆ proizvođači SUBP koriste vlastite inačice jezika za definiranje pohranjenih procedura (standard postoji, ali je rijetko gdje implementiran)
 - PostgreSQL: PL/pgSQL
 - IBM Informix: SPL (Stored Procedure Language)
 - Oracle: PL/SQL (Procedural Language/Structured Query Language)
 - Microsoft SQL Server: Transact-SQL
- ◆ Navedeni jezici proširuju mogućnosti SQL jezika proceduralnim elementima koji se koriste u strukturiranim jezicima (C, Java, ...). Osim SQL naredbi, moguće je korištenje varijabli, naredbi za upravljanje tokom programa (*if, for, while, ...*), naredbi za rukovanje iznimkama (*exception handling*)
...
- ◆ postiže se veća produktivnost programera i smanjuje mogućnost pogreške
 - programski kôd potreban za obavljanje nekog postupka koji čini logičku cjelinu implementira se i testira na samo jednom mjestu

Primjena pohranjenih procedura u provođenju sigurnosne politike

- ◆ **SQL** omogućuje zaštitu podataka od neovlaštene uporabe **na razini objekata** (tablice, atributi, virtualne tablice)
 - korisniku se može ograničiti pristup do pojedinih objekata i vrsta operacije koju nad tim objektima može obaviti (brisanje, izmjena, unos, dohvati)
 - **nije moguće ograničiti način** na koji će korisnik obavljati operacije za koje je dobio dozvolu
- ◆ **pohranjena procedura** omogućuje zaštitu podataka od neovlaštene uporabe **na razini funkcija**
 - korisniku se pridijeli **dozvola za obavljanje definirane procedure**, umjesto dozvole za pristup podacima
 - time je **precizno određen način** na koji korisnik smije obaviti operacije nad podacima
 - primjena dozvola u skladu s poslovnim pravilima ugrađenim u proceduru
 - princip najmanje ovlasti

```
CREATE PROCEDURE prijaviIspit (JMBAG CHAR(12), sifPred INTEGER, datumRok DATE)
EXECUTE PROCEDURE obaviProvjereUzPrijavu (JMBAG, sifPred, datumRok);
EXECUTE PROCEDURE odrediRbrIzlaz (JMBAG, sifPred, datumRok) INTO rbrIzlaz;
INSERT INTO ispit VALUES (JMBAG, sifPred, datumRok, rbrIzlaz);
END PROCEDURE;
```

Dozvole za pohranjene procedure/funkcije

- ◆ SQL naredbe za dodjeljivanje i ukidanje dozvola za izvršavanje procedura

```
GRANT EXECUTE ON {procName | funName}  
    TO {PUBLIC | userList | roleList}  
    [WITH GRANT OPTION]
```

```
REVOKE EXECUTE ON {procName | funName}  
    FROM {PUBLIC | userList | roleList}  
    [ CASCADE | RESTRICT ]
```

Primjer

- ♦ Korisnik *novak* je službenik u banci kojem je potrebno omogućiti obavljanje **isključivo** jedne vrste bankovne transakcije: prebacivanje iznosa s jednog na drugi račun

racun	brRacun	stanje
	1001	1250.15
	1002	-300.00
	1003	10.25

- zadatak se ne može riješiti dodjelom dozvole za obavljanje operacije UPDATE nad tablicom *racun* korisniku *novak* (zašto?)

novak

```
UPDATE racun  
SET stanje = stanje - 60.30  
WHERE brRacun = 1001;
```

[Error] ERROR: permission denied for relation racun

```
CREATE FUNCTION prebaci(sRacunaBr racun.brRacun%TYPE  
, naRacunBr racun.brRacun%TYPE  
, iznos racun.stanje%TYPE) RETURNS VOID AS
```

...

PostgreSQL: PL/pgSQL

```
GRANT EXECUTE ON prebaci TO novak;
```

Mandatno upravljanje pristupom

(*Mandatory Access Control – MAC*)

Mandatno upravljanje pristupom

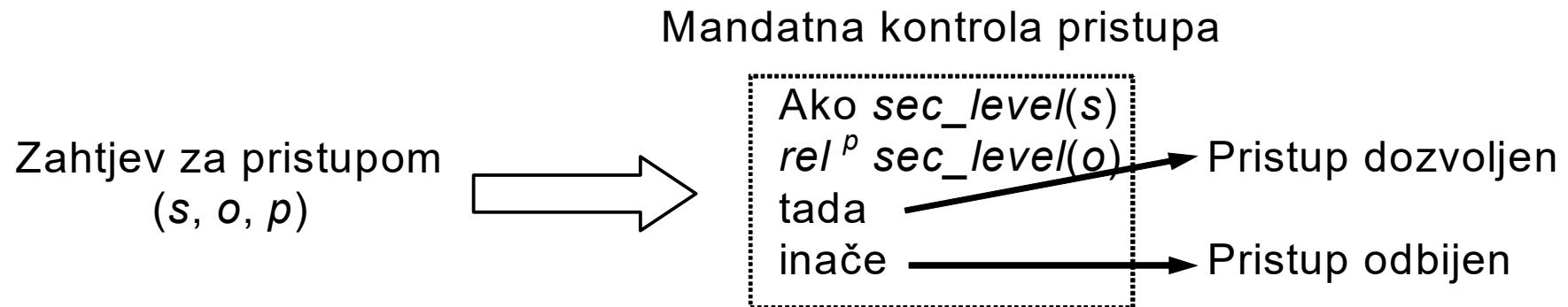
- ◆ *obavezno upravljanje pristupom (upravljanje pristupom na osnovi mandata)* - sigurnosna politika na razini sustava određuje tko ima pravo pristupa, a ne vlasnik objekata
- ◆ primjenjiva u sustavima u kojima se dozvole dodjeljuju ovisno o poziciji korisnika u hijerarhiji neke organizacije (vojska, državna uprava, ...)

“Način ograničavanja pristupa objektima temeljen je na osjetljivosti (predstavljenom oznakom (*label*)) informacija sadržanih u objektu i formalne autorizacije (tj. razine ovlasti) subjekata za informacije takve osjetljivosti.“

[US Department of Defense, Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, 1985]

Mandatno upravljanje pristupom

- ◆ svaki **objekt** dobiva oznaku **klasifikacijske razine** (*classification level*), npr. **povjerljivo, tajno, ...**
 - 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:

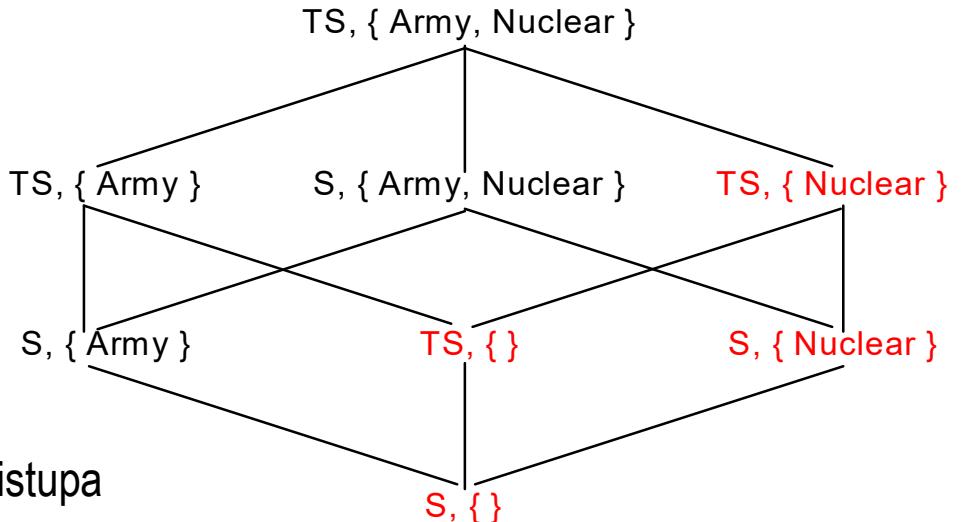


Višerazinska mandatna politika pristupa

- ◆ višerazinska politika pristupa (*multilevel security policy*) - najčešći oblik mandatne politike pristupa
- ◆ administrator sustava svakom objektu i subjektu pridružuje **klasu pristupa**
- ◆ **klasa pristupa** se sastoji od dvije komponente:
 - ◆ **sigurnosna razina** – element hijerarhijski uređenog skupa, npr. **TS > S > C > U** (*Top Secret, Secret, Confidential, Unclassified*)
 - ◆ **skup kategorija** – podskup neuređenog skupa elemenata (**funkcionalna područja ili područja kompetentnosti**), npr: { *Nuclear, Army* }

Višerazinska mandatna politika pristupa

- ◆ klasa pristupa c_1 **dominantna** je klasi pristupa c_2 , tj. $c_1 \geq c_2$ ako je
 - sigurnosna razina klase pristupa $c_1 \geq$ sigurnosne razine klase pristupa c_2
 - kategorije klase pristupa c_1 uključuju one od c_2
- klase pristupa c_1 i c_2 su neusporedive ako niti $c_1 \geq c_2$ niti $c_2 \geq c_1$



- ◆ korisnik se može prijaviti na sustav u svakoj klasi pristupa kojoj je njegova klasa pristupa dominantna
 - ◆ nakon spajanja korisnika na sustav stvara se subjekt u toj klasi pristupa
 - primjer: klase pristupa s kojima se na sustav može spojiti korisnik ovlašten za (TS, {Nuclear}):

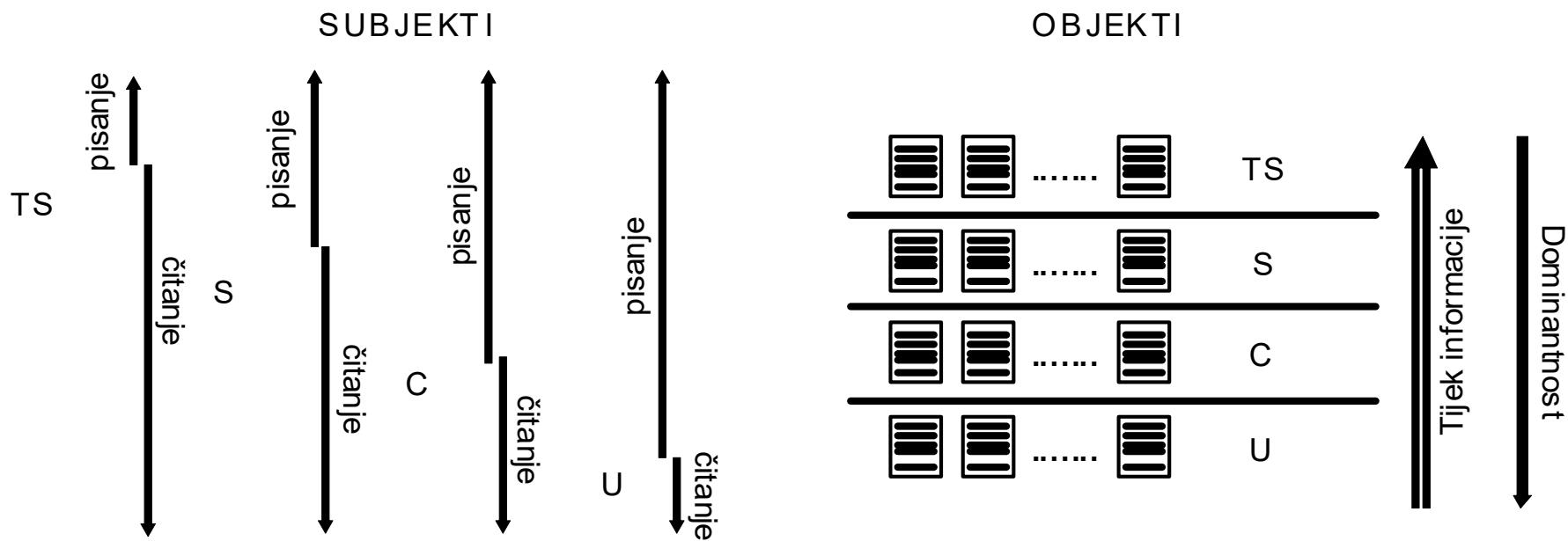
$$C = \{ \text{Nuclear, Army} \}$$
$$\text{TS} > \text{S}$$

BLP model (1)

- ◆ **Bell – La Padula Security Model** (1973)
- ◆ cilj: spriječiti tijek informacije od subjekata/objekata više razine prema subjektima/objektima nižih (ili neusporedivih) razina

BLP model (2)

- ◆ načela koja osiguravaju očuvanje tajnosti:
 - **simple property (no-read-up)** - subjektu je dozvoljeno čitanje iz objekta samo ako je klasa pristupa subjekta dominantna klasi pristupa objekta (tj. može čitati iz onih objekata kojima je njegova klasa pristupa dominantna)
 - ***-property (star-property, no-write-down)**: subjektu je dozvoljeno pisanje u objekt samo ako je klasa pristupa objekta dominantna klasi pristupa subjekta
 - nije moguće pisati u objekte koje mogu pročitati subjekti s nižom razine - spriječeno propuštanje informacija



BLP model (3)

Primjer: koriste se tri klase pristupa sastavljene od sigurnosnih razina (S, C, U)

- ◆ relacija ***ispit*** ima sigurnosnu razinu S
- ◆ korisnik u_1 ima razinu ovlasti U:
 - na sustav se može spojiti samo na razini U
 - može kreirati i čitati samo objekte razine U
 - kreira relaciju ***xyz*** koja ima sigurnosnu razinu U
- ◆ korisnik u_2 ima razinu ovlasti S:
 - na sustav se može spojiti na razini S, C ili U
 - ako radi kao S subjekt:
 - može čitati iz relacije ***ispit***
 - ne može pisati u relaciju ***xyz*** koja ima razinu U (*no-write-down*)
 - ako radi kao U subjekt:
 - ne može čitati iz relacije ***ispit*** (*no-read-up*)

Zajednička primjena DAC i MAC politike

- ◆ DAC i MAC politike nisu međusobno isključive i mogu biti primijenjene zajedno
 - diskrecijska politika djeluje unutar granica mandatne politike i može samo sprječiti neki pristup koji bi uz primjenu samo MAC politike bio dozvoljen

Mandatna politika pristupa u bazama podataka

- ◆ klasifikacija na razini: relacije; atributa; n-torke (zаписа); podatka
- ◆ primjenjuju se osnovni principi MAC-a:
 - ***simple property (no-read-up)***
 - ***strong-star-property*** (umjesto **-property*): korisnik može pisati **isključivo na svojoj razini** (radi sprječavanja uništenja npr. S-podataka od strane U-korisnika)
- ◆ subjekti na različitim razinama imaju različite poglede na relaciju
 - pogled je sastavljen samo od elemenata čijom klasifikacijom dominiraju
 - nerazlikovanje NULL vrijednosti – neprikazani podatak može biti posljedica njegove NULL vrijednosti u bazi podataka **ili posljedica tajnosti (klasifikacije) podatka**
- ◆ implementacija u komercijalnim SUBP-ovima:
 - IBM Informix - Label Based Access Control (LBAC)
 - Oracle Label Security

Upravljanje pristupom temeljeno na ulogama

(Role-Based Access Control - RBAC)

Dodjeljivanje istih dozvola velikom broju korisnika

PROBLEM:

- ◆ svakom nastavniku treba dodijeliti dozvole za
 - pregled, unos i izmjenu podataka o ispitima za predmete koje predaje, pregled podataka iz relacije *nast*, iz relacije *predaje*, itd.
 - 150 nastavnika \Rightarrow 150 puta treba obaviti niz naredbi za dodjelu dozvola:

```
GRANT SELECT, INSERT, UPDATE ON ispitizaNastavnike TO kolar;
GRANT SELECT ON predmet TO kolar;
GRANT SELECT ON nast TO kolar;
...
-- ponoviti za svakog od 150 nastavnika
```

- ◆ za svakog novog zaposlenog nastavnika ponoviti postupak
- ◆ kada nastavnik ode u mirovinu, mora se obaviti niz REVOKE naredbi
- ◆ ako se promijene pravila pristupa (npr. odluči se da nastavnici mogu brisati "svoje" ispite), promjena se mora provesti za svakog nastavnika posebno:

```
GRANT DELETE ON ispitizaNastavnike TO kolar;
-- ponoviti za svakog od 150 nastavnika
```

Upravljanje pristupom temeljeno na ulogama

- ◆ Osnovne postavke
 - podaci vlasništvo poduzeća
 - korisnicima nije dozvoljeno donošenje odluka o pristupu
 - za upravljanje dozvolama zadužen je administrator za sigurnost
 - odluke o pristupu temeljene na ulogama korisnika kao dijela organizacije
 - bolnica: liječnik i medicinska sestra
 - banka: blagajnik i računovođa
 - Korisnici ne mogu svoje ovlasti prosljeđivati drugim korisnicima
liječnik ne smije dopustiti medicinskoj sestri prepisivanje lijekova

Upravljanje pristupom temeljeno na ulogama

- ◆ glavna osobina RBAC modela:
 - svaki pristup podatkovnim objektima i resursima, potreban korisniku za obavljanje njegova zadatka, obavlja se **kroz uloge**
 - uloga predstavlja poslovnu funkciju unutar organizacije
 - ovlasti nad podatkovnim objektima i resursima potrebnim za obavljanje zadatka dodijeljene su ulogama umjesto pojedinim korisnicima
 - korisnik je ovlašten za obavljanje odgovarajuće uloge

RBAC u relacijskim bazama podataka - SQL standard

- ◆ kreiranje uloge:

```
CREATE ROLE roleName [ WITH ADMIN <grantor> ]  
<grantor> ::= CURRENT_USER | CURRENT_ROLE
```

- ◆ uništavanje uloge:

```
DROP ROLE roleName
```

- ◆ dodjeljivanje uloge korisniku:

```
GRANT roleName [ {, roleName } ... ]  
TO <grantee> [ {, <grantee>} ... ]  
[ WITH ADMIN OPTION ][ GRANTED BY <grantor> ]  
  
<grantee> ::= PUBLIC | <roleName> | <userIdentifier>
```

- ◆ ukidanje uloge korisniku:

```
REVOKE [ ADMIN OPTION FOR ] uloga [ {, uloga} ... ]  
FROM <grantee> [ {, <grantee>} ... ]  
[ GRANTED BY <grantor> ] <drop behavior>  
  
<drop behavior> ::= CASCADE | RESTRICT
```

- ◆ aktivacija i deaktivacija uloge:

```
SET ROLE 'roleName'  
SET ROLE NONE
```

- ◆ uloga koja je aktivna u SQL sjednici: CURRENT_ROLE

PostgreSQL uloge

- definira se uloga (*role*), npr. *nastavnik*
- dozvole se, umjesto direktno korisnicima, dodjeljuju novoj ulozi
- uloga može predstavljati jednog ili više korisnika
- uloge se, kao i korisnici, definiraju na razini cijelog SUBP-a

```
CREATE ROLE name [ [ WITH ] option [ . . . ] ]
```

where option can be:

```
| CREATEDB | NOCREATEDB  
| CREATEROLE | NOCREATEROLE  
| [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'  
| INHERIT | NOINHERIT  
| LOGIN | NOLOGIN
```

...

Nalik opcijama CREATE USER naredbe

INHERIT znači da uloga (automatski) nasljeđuje dozvole eventualnih dodatnih uloga koje su joj dodijeljene. INHERIT je preddefinirano ponašanje.

Dodjeljivanje istih dozvola velikom broju korisnika

```
CREATE ROLE nastavnik;
GRANT SELECT, INSERT, UPDATE ON ispitiZaNastavnike TO nastavnik;
GRANT SELECT ON nast TO nastavnik;
GRANT SELECT ON predaje TO nastavnik;
...
...
```

- svakom nastavniku, umjesto cijelog niza dozvola, dovoljno je dodijeliti dozvolu za korištenje uloge nastavnik

```
GRANT nastavnik TO kolar;
GRANT nastavnik TO ban;
...
...
```

Dodjeljivanje istih dozvola velikom broju korisnika

- ◆ uloga/korisnik aktivira drugu ulogu uz pomoć naredbe SET ROLE
- ◆ Ako je korisnik kreiran s preddefiniranom opcijom INHERIT (to je slučaj u našem primjeru) nije potrebno aktivirati ulogu jer ionako automatski ima sve njene dozvole.

ban: `SET ROLE nastavnik;`

- ako nastavnik s identifikatorom korisnika ban ode u mirovinu

`REVOKE nastavnik FROM ban;`

- ako nastavnici trebaju dobiti dozvolu za brisanje "svojih" ispita

`GRANT DELETE ON ispitiZaNastavnike TO nastavnik;`

IBM informix: RBAC implementacija

- ◆ svakom nastavniku treba dodijeliti dozvole za pregled, unos i izmjenu podataka o ispitima za predmete koje predaje, pregled podataka iz relacija *nast*, *predaje*, itd.
 - definira se uloga *nastavnik* i dozvole se dodijele toj ulozi
 - svakom nastavniku se dodijeli dozvola za korištenje uloge *nastavnik*

```
CREATE ROLE nastavnik;
GRANT SELECT, INSERT, UPDATE ON ispitiZaNastavnike TO nastavnik;
GRANT SELECT ON nast TO nastavnik;
GRANT SELECT ON predaje TO nastavnik;    ...
```

```
GRANT nastavnik TO kolar;
GRANT nastavnik TO novak;
...
```

- ako nastavnik s identifikatorom korisnika *novak* ode u mirovinu:
- ako nastavnici trebaju dobiti dozvolu i za brisanje "svojih" ispita:

```
REVOKE nastavnik FROM novak;
```

```
GRANT DELETE ON ispitiZaNastavnike TO nastavnik;
```

- ◆ nakon uspostavljanja SQL-sjednice, korisnik posjeduje sljedeće dozvole:
 - sve dozvole dodijeljene PUBLIC "korisniku"
 - sve dozvole dodijeljene izravno dotičnom korisniku
 - sve dozvole nad objektima kojima je dotični korisnik vlasnik
 - dozvole korisnika na razini baze podataka
 - ako namjerava koristiti i dozvole dodijeljene ulozi *nastavnik*, mora obaviti naredbu:

```
SET ROLE nastavnik;
```

Šifriranje podataka

Šifriranje podataka

- ◆ dodatna razina zaštite ako neovlašteni korisnik uspije doći do podataka iz baze podataka
 - prисluškivanjem komunikacijskih linija ili
 - zaobilaznjem sustava za upravljanje bazama podataka (npr. krađom datoteke ili diska)
- ◆ mjere:
 - prijenos šifriranih podataka (*data-in-transit*) i/ili
 - pohrana šifriranih podataka (*data-at-rest*)
- šifriranje se može koristiti kao zadnji sloj obrane radi zaštite osjetljivih i vrlo povjerljivih informacija
 - nije zamjena za ostale tehnike zaštite podataka, npr. za upravljanje pristupom

Prijenos šifriranih podataka

- ◆ **šifriranje/dešifriranje podataka u prijenosu** događa se u krajnjim točkama komunikacije između klijenta i poslužitelja
 - podaci pohranjeni u bazi podataka i podaci koje koristi klijentska aplikacija nisu šifrirani
- ◆ implementacijske mogućnosti šifriranja podataka u prijenosu:
 - **specifične mogućnosti određenog SUBP-a** (npr. Oracle Advanced Security)
 - *Connection-based methods* (npr. korištenje Secure Sockets Layer [SSL])
 - *Secure tunnels* (npr. korištenje Secure Shell [SSH] tunela)
 - mogućnosti koje podržava operacijski sustav (npr. IPSec)
- ◆ u svim, osim u prvoj kategoriji, prijenos šifriranih podataka temelji se **na industrijskim standardima** i ne ovisi o proizvođaču baze podataka
- ◆ većina metoda šifrira cijeli komunikacijski tok

Pohrana šifriranih podataka (1)

- ◆ **šifriranje vrijednosti koje su pohranjene u bazi podataka**
- ◆ šifriranje/dešifriranje moguće je obaviti na razini:
 - **aplikacije**
 - biblioteke za šifriranje/dešifriranje podataka (npr. Java Cryptographic Extensions - JCE)
 - bazi podataka se pristupa s već šifriranim podatkom - transparentno za bazu podataka
 - šifriranje/dešifriranje je možda potrebno obaviti na više mesta
 - npr. pohranjena procedura koristi podatke šifrirane u Java kôdu aplikacije
 - korištenje podataka samo iz aplikacije - ograničeno je korištenje interaktivnog alata za rad s bazom podataka, čak i uz potrebne ovlasti
 - **datotečnog sustava**
 - korištenje mogućnosti naprednog datotečnog sustava za pohranu podataka u šifriranom obliku
 - npr. Windows - Encrypted File System (EFS)
 - šifrirano je sve, a ne samo osjetljivi podaci - lošije performance
 - **sustava za upravljanje bazama podataka**

Pohrana šifriranih podataka (2)

- ◆ **šifriranje/dešifriranje na razini sustava za upravljanje bazama podataka:**
 - ugrađene rutine baza podataka (npr. T-SQL: DB_ENCRYPT i DB_DECRYPT funkcije)
 - proširenja SUBP-a (dodatni paketi) (npr. Oracle - DBMS_CRYPTO paket)
- ◆ podaci su neupotrebljivi dok se ne dešifriraju
 - SUBP ne može obaviti učinkovita uspoređivanja vrijednosti i temeljne operacije nad šifratima

Pohrana šifriranih podataka (2)

- ◆ neizbježan **pad performansi**, ovisno o opsegu šifriranja i korištenim algoritmima
 - ispitivanje Database Server Technologies Group: Oracle 9.2.0.1 - uzorak od 1,6 milijuna šifriranih brojeva socijalnog osiguranja
 - SELECT koji vraća sve zapise: uz korištenje DES algoritma - **200 puta sporiji**
 - UPDATE zapisa: uz korištenje DES algoritma - četiri puta sporiji, uz triple DES - osam puta sporiji
- ◆ šifrirani podaci zauzimaju više prostora od originalnog teksta
- ◆ **smjernice:**
 - **šifrirati selektivno - samo iznimno osjetljive informacije**
 - **ne šifrirati atributе koji se koriste kao ključevi ili indeksi**

Upravljanje ključevima za šifriranje

- kompromitirani ključevi - mogućnost otkrivanja informacije
- izgubljeni ključevi - gubitak informacija

Upravljanje ključevima:

- ◆ generiranje ključeva
 - npr. Oracle funkcija RANDOMBYTES paketa DBMS_CRYPTO
- ◆ prijenos ključeva
 - prijenos šifriranog ključa od aplikacije do baze podataka
- ◆ pohrana ključeva
 - u bazi podataka, u operacijskom sustavu
 - alati koji nude cjelovita rješenja vezana uz upravljanje ključem
 - korisnici upravljaju vlastitim ključevima za šifriranje
 - korištenje transparentnog šifriranja baze podataka
- ◆ promjena ključa
 - obaviti dok se podacima ne pristupa

Transparentno šifriranje podataka

- ◆ **šifriranje/dešifriranje** podataka **obavlja SUBP** prilikom pohrane/dohvata podatka
 - nije potrebno koristiti posebne funkcije
 - transparentno za korisnike baze podataka
 - nije potrebna izmjena aplikacija radi rukovanja šifriranim podacima
- ◆ poslovi **upravljanja ključem** su **automatizirani**
 - korisnik ili aplikacija ne mora upravljati ključem za šifriranje
- ◆ implementirano u nekim sustavima za upravljanje bazama podataka:
 - Oracle - *Transparent Data Encryption* (TDE)
 - SQL Server - *Extensible Key Management* (EKM)

Praćenje rada korisnika

Praćenje rada korisnika (auditing)

- ◆ praćenje različitih kategorija pristupa:
 - prijava/odjava za rad s bazom podataka
 - neuspjeli pokušaji prijave
 - obavljanje DDL naredbi
 - pogreške koje dojavljuje sustav za upravljanje bazama podataka
 - promjene definicija pohranjenih procedura i okidača
 - promjene podataka o korisnicima, njihovim dozvolama i ostalih sigurnosnih atributa
 - promjene osjetljivih podataka
 - dohvati osjetljivih podataka
 - izmjene definicija snimanja traga i snimljenih podataka

Praćenje rada korisnika (auditing)

- ◆ evidentirati svaki pristup osjetljivim podacima u posebnoj datoteci za praćenje rada korisnika (*Audit Trail*)
- ◆ tipičan zapis datoteke sadrži sljedeće informacije:
 - SQL naredba koja se izvršava (*statement source*)
 - mjesto s kojeg je upućen zahtjev (terminal, IP adresa računala)
 - identifikator korisnika koji je pokrenuo operaciju
 - datum i vrijeme operacije
 - n-torce, atributi na koje se zahtjev odnosi
 - stara vrijednost n-torke
 - nova vrijednost n-torke
- ◆ sama činjenica da se prati "trag" obavljenih operacija nad podacima, često je dovoljna za sprečavanje zloporabe

Praćenje rada korisnika

- ◆ analizom prikupljenih podataka moguće je saznati:
 - postoje li odstupanja od sigurnosne politike koju bi trebalo provoditi
 - postoje li aktivnosti "korisnika" za koje nije ovlašten
 - tko je i kako izmijenio podatke
 - što rade ovlašteni korisnici; što rade privilegirani korisnici
 - je li bilo pokušaja napada npr. SQL injekcijom, ubacivanja zlonamjernog programskog koda u pohranjene procedure ...

Selektivno praćenje

- ◆ nužnost **selektivnog** praćenja DML aktivnosti zbog mogućnosti stvaranja **goleme količine** podataka - praćenje aktivnosti na podskupu tablica baze podataka
- ◆ u slučaju promjena ovlasti i ostalih sigurnosnih atributa nužno implementirati obavještavanje o promjenama u stvarnom vremenu

Implementacija

- mehanizmi sustava za upravljanje baze podataka
 - **okidači** - implementacija vlastitih rješenja praćenja rada korisnika
 - **proširenja funkcionalnosti**: praćenje tragova - *trace functions*
 - potrebno je izdvajanje informacija i stvaranje izvješća
- **vanjski sustavi** za praćenje rada korisnika (*third-party* rješenja)
 - prikupljanje podataka, izvještavanje i slanje upozorenja
 - podržavaju veći broj sustava za upravljanje bazama podataka (Oracle, SQL Server, Sybase, DB2, IBM Informix ...)
 - Imperva - Database Activity Monitoring
 - DAS-DBAuditor: Database Auditor
 - Ambeo - Activity Tracker, Usage Tracker, NetServer
 - nisu pod nadzorom DBA (princip razdvajanja dužnosti)
- **usporedba shema** (*snapshots*)
 - periodičko prikupljanje sheme (obično jednom dnevno) i usporedba s prethodnom shemom (*diff*)

Dodatna razmatranja

- ◆ mjesto **pohrane** prikupljenih podataka
 - goleme količine podataka
 - izbjegavati fizički medij na kojem su pohranjeni podaci produkcijskog sustava baze podataka
- ◆ mogućnost **arhiviranja** prikupljenih podataka
 - propisi mogu zahtijevati čuvanje prikupljenih podataka više godina
 - postizanje razumnog vremena odziva prilikom analize podataka
 - utvrđivanje dinamike arhiviranja
 - arhiviranje napravljenih izvješća na temelju prikupljenih podataka
- ◆ zaštita od **neovlaštenog pristupa**:
 - prikupljenim podacima tijekom praćenja
 - napravljenim arhivama tijekom prijenosa i na mjestu pohrane

Zaštita i privatnost podataka

- ◆ **Opća uredba o zaštiti podataka EU**
(GDPR - General Data Protection Regulation)
 - Primjenjuje se od **25.5.2018.**
 - Uredbom se utvrđuju **pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka** i pravila povezana sa **slobodnim kretanjem osobnih podataka**.

Zaštita i privatnost podataka

- ◆ Opća uredba o zaštiti podataka EU - **obaveze:**
 - Klijent mora moći dati izričit pristanak na korištenje svojih podataka,
 - Mora moći biti obaviješten kada, u kojem obliku (izvorno, anonimizirani, ili pseudo-anonimizirani) i od strane koga se koriste njegovi podaci, za koju namjenu, i koliko dugo će biti pohranjeni;
 - Omogućiti klijentima uvid u njihove osobne podatke i omogućiti ispravak nepravilnosti;
 - Jamčiti da nema prijenosa podataka u zemlji izvan EU-a koji ima nedovoljnu zaštitu podataka;
 - Ispuniti "pravo na zaborav" – obrisati osobne podatke klijenta na njegov zahtjev, ako su ispunjeni propisani uvjeti.
 - ◆ Za kršenje odredbi mogu se izreći upravne novčane kazne u iznosu do 20 000 000 EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu finansijsku godinu, ovisno o tome što je veće.
-



Zaštita i sigurnost informacijskih sustava

Sigurnost u sustavima za elektroničko poslovanje

prof. dr. sc. Boris Vrdoljak

dr. sc. Luka Humski

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Zaštićeno licencijom <http://creativecommons.org/licenses/by-nc-sa/2.5/hr/>



Creative Commons



□ slobodno smijete:

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo

□ pod sljedećim uvjetima:

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencem koja je ista ili slična ovoj.

U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.

Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s <http://creativecommons.org/>.

Elektroničko poslovanje

Primjeri elektroničkog poslovanja

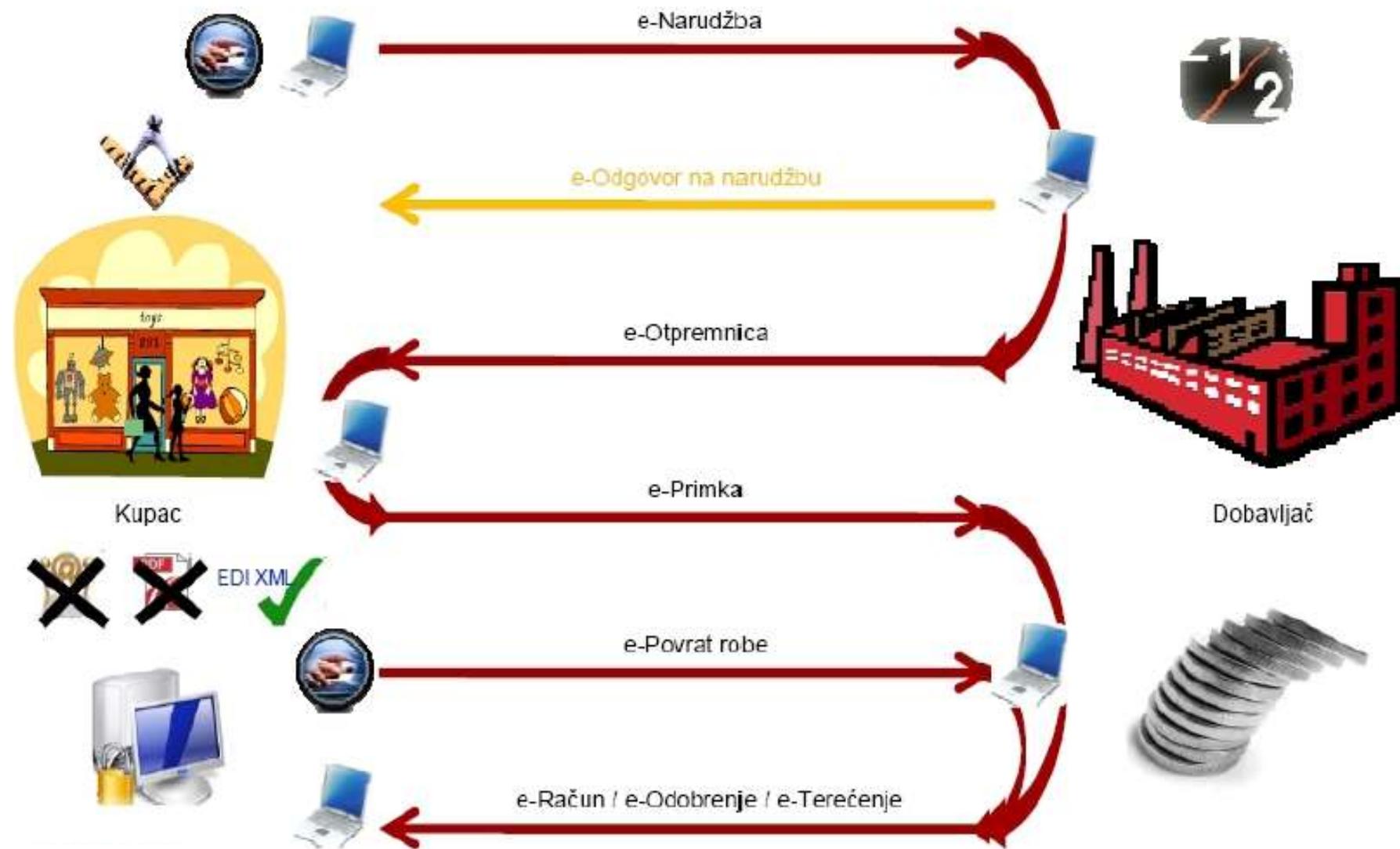
- ◆ elektroničko komuniciranje s drugim poduzećima radi narudžbe proizvoda i usluga te njihovo elektroničko plaćanje
 - poslovanje medu tvrtkama – B2B (Business-to-Business)
- ◆ prodavanje proizvoda i usluga preko Web sjedišta
 - e-trgovina, poslovanje tvrtke s krajnjim potrošačem – B2C (Business-to-Consumer)

Elektroničko poslovanje B2B - razmjena poslovnih dokumenata

Osnovni poslovni procesi u dobavnom lancu i elektronički dokumenti koji se razmjenjuju:

- ◆ Katalog *e-katalog*
- ◆ Naručivanje *e-narudžbenica*
- ◆ Otpremanje *e-otpremnica*
- ◆ Primanje *e-primka*
- ◆ Fakturiranje *e-račun*
- ◆ Plaćanje *e-nalog za plaćanje*

Primjer razmjene e-dokumenata



Dobavni lanac – osnovni poslovni procesi i dokumenti

- ◆ Suvremenih električki dokumenti koji se razmjenjuju u električkom poslovanju većinom su u formatu XML.
- ◆ Postoje i starije norme EDI (*Electronic Data Interchange*), od kojih je najvažnija norma EDIFACT (*Electronic Data Interchange For Administration, Commerce and Transport*).
- ◆ razmjena suvremenih poslovnih električkih dokumenata – tehnologije: XML i usluge Weba
- ◆ SIGURNOST?

Sigurnost elektroničkog poslovanja

- ◆ B2B - razmjena XML dokumenata i korištenje Web usluga
- ◆ Osiguravanje autentičnosti (deklarirani pošiljatelj je stvarni pošiljatelj) i integriteta (nemogućnost izmjene poruke)
 - [E-potpis](#)
- ◆ Kad istekne digitalni certifikat, kako dokazati da je u doba potpisivanja dokumenta certifikat vrijedio?
 - [Vremenska ovjera, vremenski žig \(timestamp\)](#)
- ◆ Potpisivanje i šifriranje u formatu XML
 - [XML Signature](#) i [XML Encryption](#)
- ◆ Sigurnost Web usluga
 - [Web Services Security \(WSS\)](#) i druge norme (WS-Extensions)
 - [WS-I Basic Security Profile](#)
 - [Sigurnost RESTful Web usluga](#)

Sigurnost pri razmjeni elektroničkih dokumenata

- ◆ **e-račun** je najrašireniji elektronički poslovni dokument
- ◆ sve zemlje članice EU trebaju omogućiti primanje **e-Računa** za porezne svrhe (PDV) ako su ispunjena dva uvjeta:
 - 1) **primatelj se mora složiti** s primanjem računa u elektroničkom formatu;
 - 2) **integritet** (nemogućnost izmjene) i **autentičnost** (deklarirani pošiljatelj je stvarni pošiljatelj) moraju biti osigurani pri prijenosu i arhiviranju.

Ovaj drugi zahtjev može se ispuniti bilo **naprednim elektroničkim potpisom** ili kroz elektroničku razmjenu podataka (EDI) s ugovorenim sigurnosnim mjerama.

Elektronički (digitalni) potpis

- U poslovnom i ICT-svijetu često susrećemo pojam digitalni potpis, elektronički potpis, e-potpis ili engleski naziv *e-signature*.
- Elektronički potpis je uredbom eIDAS (koju je donijela EU) definiran na sljedeći način: „*podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje*“.
- U sklopu ovog predmeta:
 - pojmove elektronički potpis i digitalni potpis koristit ćemo kao sinonime,
 - pojam elektronički potpis neće uključivati i sliku ručnog potpisa (iako se i ona u širem smislu može smatrati vrstom elektroničkog potpisa).

Asimetrična kriptografija

Za digitalno potpisivanje koristi se **asimetrična kriptografija**.

- jedan algoritam i **par ključeva**: jedan ključ za šifriranje, drugi za dešifriranje
- ◆ Šifriranje: transformira se **otvoreni tekst** (*plaintext*) koristeći unaprijed dogovoren ključ
- ◆ Rezultat šifriranja naziva se **šifrat** (*ciphertext*) ili **kriptogram**
- ◆ matematički algoritam određuje kako se šifrira otvoreni tekst
- ◆ složenost ovisi o duljini ključa (broj bitova)
- ◆ **snaga** sustava za šifriranje **počiva na ključu**
 - napadač može imati šifrirane tekstove i znati algoritme, ranjivost sustava ovisi o snazi ključa
 - dulje ključeve teže je probiti (vrijeme, novac)
 - duljina ključa: 128, 192 ili 256 bita

Asimetrična kriptografija

- u asimetričnoj kriptografiji ključevi su međusobno vezani
- neizvedivo je poznavajući algoritam i jedan ključ otkriti drugi
- često: svejedno je kojim ključem se šifrira, a kojim dešifrira
 - rade isključivo u paru
- **jedan od dva ključa mora ostati tajan**

Svaki korisnik ima par ključeva:

- **privatni** (tajni) ključ
 - Dostupan isključivo korisniku, ne smije se distribuirati
- **javni** ključ
 - Dostupan svima, mora se distribuirati

Asimetrična kriptografija

- ono što se šifrira javnim ključem, može se dešifrirati samo privatnim
- ono što se šifrira privatnim ključem, može se dešifrirati samo javnim
- poznavanjem javnog ključa ne može se izračunati tajni ključ u nekom razumnoj vremenu
- vrijeme potrebno za izračunavanje tajnog ključa iz poznatog javnog ključa, tj. razbijanje šifre, mjeri se milijunima godina na danas najjačim raspoloživim računalima
- Asimetrična kriptografija naziva se i **kriptografijom javnog ključa**.

Algoritmi za asimetričnu kriptografiju

- ◆ RSA (Rivest-Shamir-Adleman) - MIT
 - najpopularniji algoritam, razvijen 1977.
- ◆ Diffie-Hellman
 - razvijen 1976.
- ◆ Elliptic Curve Cryptosystem (**ECC**)
- ◆ ostali:
 - ElGamal, Rabin, Knapsack, McEliece, NTRU, Braid Groups, Lucas

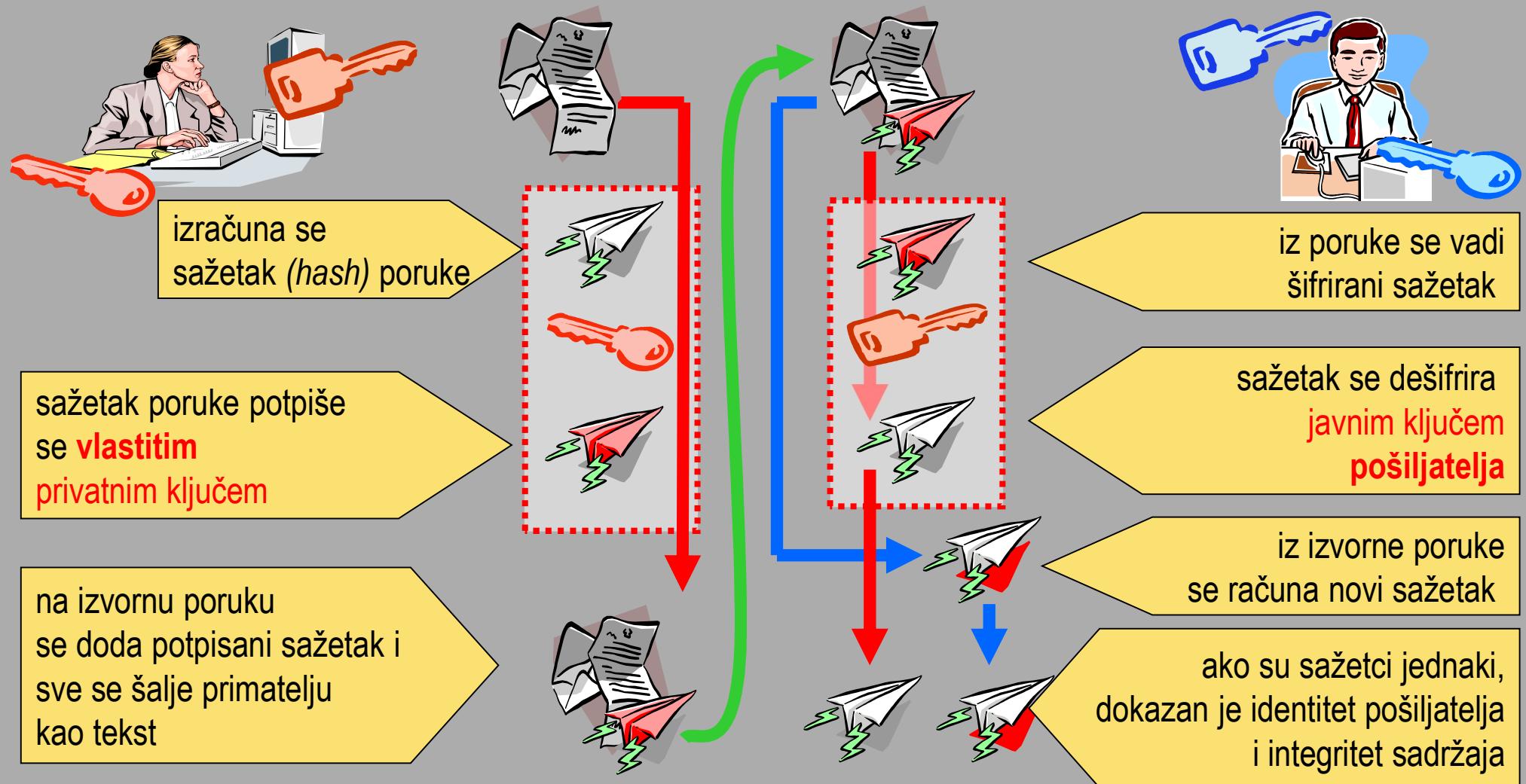
Hash funkcija i digitalno potpisivanje

- ◆ prije **digitalnog potpisivanja** treba **generirati sažetak** (hash, digest) poruke
- ◆ hash funkcija
 - ulaz: niz znakova proizvoljne duljine
 - izlaz: niz znakova fiksne duljine (npr. 256 bita)
- ◆ osnovna svojstva hash funkcije:
 - *hash* je jednosmjerna funkcija
 - nije moguće na osnovu izlaza regenerirati ulaznu poruku
 - nije moguće odrediti ulaznu poruku koja bi imala zadani hash
 - „primjena” i „promjena” će dati potpuno drugačiji sažetak (*hash*)
 - promjenom jednog bita ulaza dobiva se potpuno drugačiji izlaz

Hash-algoritmi

- ◆ Secure Hash Algorithm (SHA-1) – ne preporučuje se koristiti
 - algoritam američke vlade (NSA)
 - daje *hash* vrijednost duljine 160 bita iz niza znakova bilo koje duljine
 - **kolizija** otkrivena u 2^{69} hasheva, 2005. godine
- ◆ **SHA-2** (varijante SHA2-224, SHA2-256, SHA2-384, SHA2-512)
- ◆ **SHA-3** (varijante SHA3-224, SHA3-256, SHA3-384, SHA3-512)
- ◆ Message Digest Algorithm 5 (MD5) – ne preporučuje se koristiti
 - daje *hash* duljine 128 bita
 - MD5 probijen 2008. godine

Postupak digitalnog potpisivanja



Digitalni certifikat

- ◆ Digitalni certifikat skup je podataka u elektroničkom obliku koji predstavlja elektronički identitet u raznim elektroničkim interakcijama.
- ◆ Skup podataka koji identificira korisnika i davatelja usluge certificiranja
- ◆ Rješava problem dokazivanja identiteta
- ◆ Povezuje **identitet korisnika** s njegovim **javnim ključem** - **potvrđuje da je određeni korisnik vlasnik određenog javnog ključa**

Digitalni certifikat

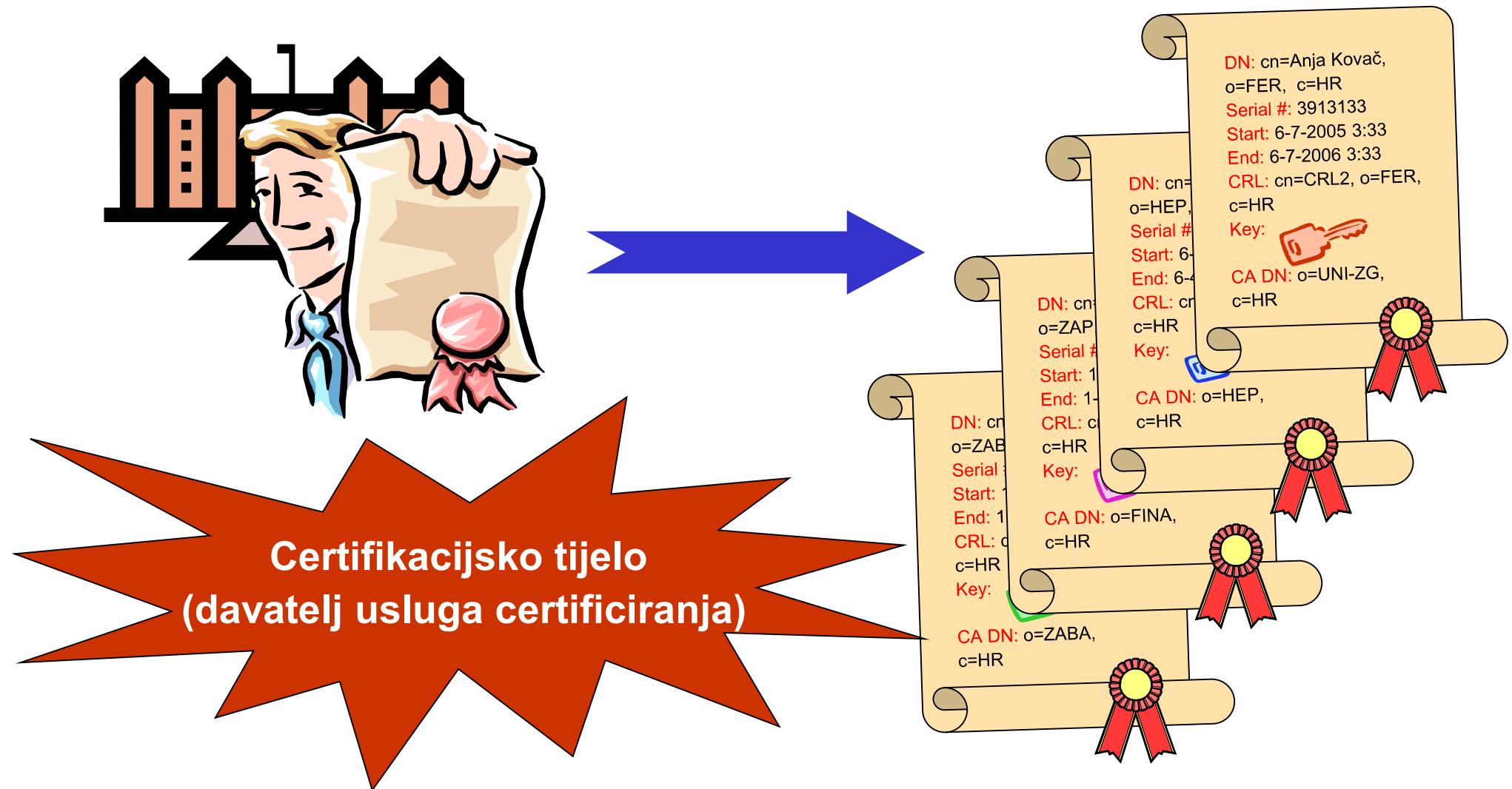
- ◆ Za točnost podataka jamči tijelo koje je certifikat izdalo, a koje je prije izdavanja certifikata provelo procese identifikacije i autentifikacije kako bi moglo jamčiti povezanost između nekog korisnika i njegova javnog ključa. To tijelo potpisuje svaki izdani certifikat svojim **privatnim ključem**.
 - ◆ Certifikate u pravilu izdaju organizacije specijalizirane za izdavanje certifikata.
-
- ◆ Norma:
 - za digitalne certifikate koristi se norma **X.509**
 - imena su u certifikatima prikazana kao parovi: ime – vrijednost

Sadržaj certifikata



Izdavanje certifikata

Certifikacijsko tijelo (CA – Certificate Authority)



Digitalni certifikat

- ◆ Ako pošiljatelj potpiše poruku svojim privatnim ključem, primatelj može **znati da se radi upravo o tom pošiljatelju**:
 - ako može **dešifrirati** digitalni potpis **javnim ključem pošiljatelja**
 - ako **digitalni certifikat potvrđuje** da je korišteni javni ključ upravo **javni ključ tog pošiljatelja**
 - ako digitalni certifikat **nije istekao ili opozvan**
- ◆ Pretpostavka za ovaj postupak je da korisnici imaju **povjerenje u certifikacijsko tijelo** (tj. davatelja usluga certificiranja) koje je izdalo certifikat i potpisalo ga svojim privatnim ključem ili u certifikacijsko tijelo koje je certificiralo certifikacijsko tijelo koje je izdalo certifikat.

Infrastruktura javnog ključa

◆ PKI - Public Key Infrastructure

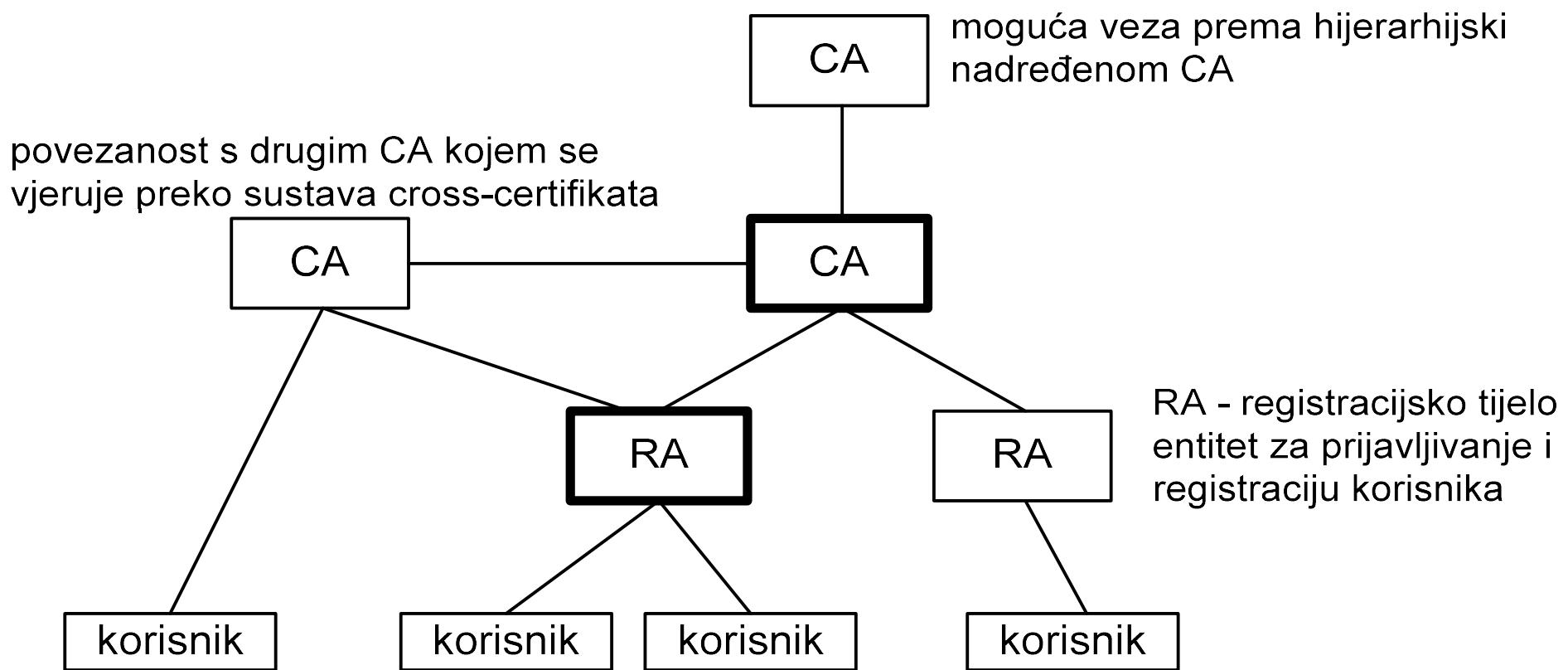
- skup sklopolja, programske podrške, ljudi, politika i procedura potrebnih za stvaranje, upravljanje, izdavanje, korištenje, pohranjivanje i opozivanje digitalnih certifikata
- osnova za stvaranje sigurne i povjerljive razmjene podataka između sudionika u sustavu
- osigurava:
 - **cjelovitost** elektroničke komunikacije onemogućavajući izmjene podataka tijekom njihovog prenošenja mrežom
 - **potvrđivanje identiteta** strana koje sudjeluju u komunikaciji
 - **neporecivost** sudjelovanja bilo koje strane u komunikaciji

Dijelovi PKI

- ◆ **certifikacijsko tijelo (CA – Certificate Authority)**
 - obavlja izdavanje i povlačenje certifikata, održavanje informacija o stanju certifikata, objava važećih certifikata...
- ◆ **registracijsko tijelo (RA – Registration Authority)**
 - obavlja registraciju korisnika (provjerava sadržaj certifikata za CA, obavlja identifikaciju i autentifikaciju strana koje se prijavljuju za dobivanje certifikata)
- ◆ **repozitorij**
 - sadrži bazu izdanih certifikata i bazu opozvanih certifikata (CRL – engl. *Certification Revocation List*)
- ◆ **klijenti (aplikacije)**
 - provjeravaju digitalne potpise i certifikate kod CA
- ◆ **korisnici sustava PKI**
 - vlasnici certifikata
- ◆ **centar za pouzdano vremensko označavanje (TSA – engl. *Timestamp Authority*)**
 - stvara vremenske žigove

Odnos RA i CA

- ◆ jedan CA može imati više RA za različite skupine korisnika
- ◆ jedan RA može biti povezan s više CA



Hijerarhija certifikacijskih tijela

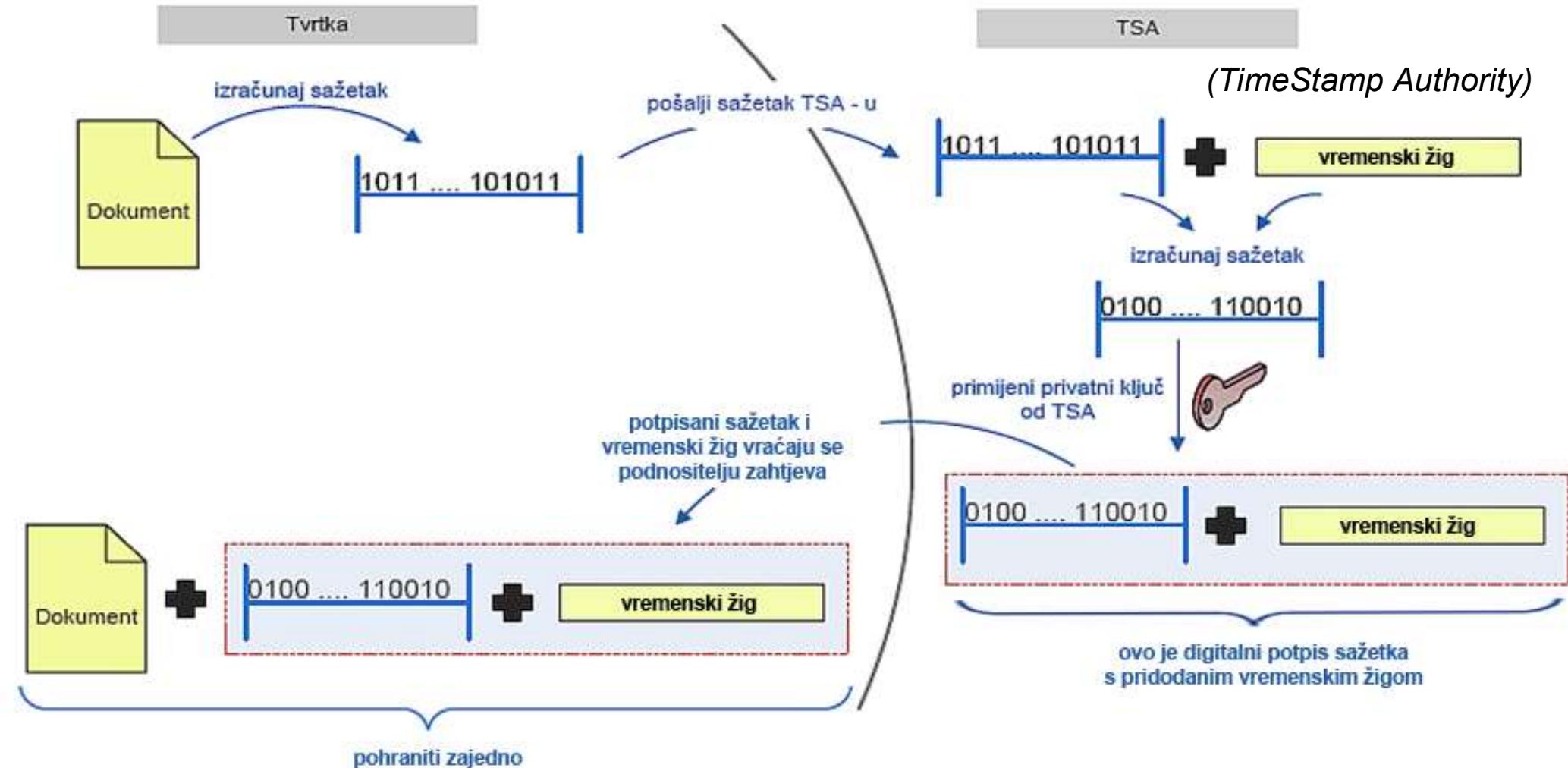
- ◆ Jedan CA može potpisati certifikat drugog CA
- ◆ Može se napraviti **hijerarhija certifikacijskih tijela (CA)**
- ◆ Ako nemamo povjerenja u neki CA, možda imamo povjerenja u CA koji je u hijerarhiji iznad njega. Time stječemo povjerenje i u CA na nižoj razini hijerarhije
- ◆ CA na najvišoj razini sam potpisuje svoj certifikat – to je onda samopotpisani certifikat. CA sa samopotpisanim certifikatom je korijenski CA

Centar za pouzdano vremensko označavanje (TSA)

- ◆ Stvara vremenske žigove kako bi se dokazalo da su određeni podaci postojali prije određenog vremena
- ◆ **VREMENSKI ŽIG**
 - Vremenski žig, vremenski pečat, vremenska oznaka, vremenska ovjera, engl. *timestamp*
 - **Osigurava pouzdanost digitalnog potpisa i poslije isteka valjanosti ili opoziva certifikata potpisnika**
 - Pomoću vremenskog žiga može se dokazati da je potpis napravljen prije isteka valjanosti certifikata

Postupak dodjeljivanja vremenskog žiga

podnositelj zahtjeva za vremenskim žigom

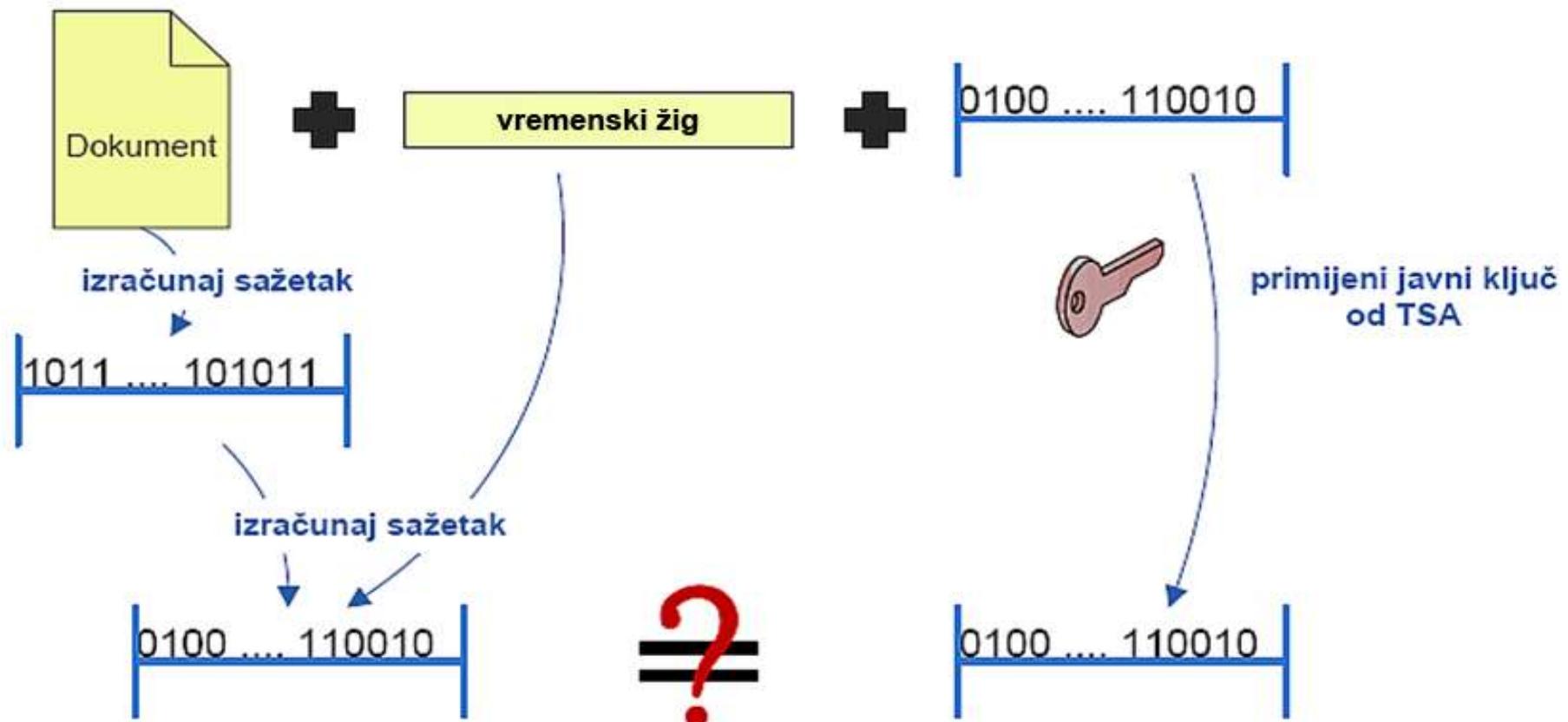


- TSA ne prima originalne podatke od podnositelja zahtjeva već uvijek barata sažetcima

Postupak dodjeljivanja vremenskog žiga

- ◆ Proces stvaranja vremenske oznake zasniva se na funkcijama sažimanja i digitalnom potpisu. Prvo, podnositac zahtjeva za vremenskom oznakom izračuna sažetak dokumenta na kojega želi staviti vremensku oznaku. Zatim se taj sažetak šalje centru za vremensko označavanje.
- ◆ TSA prima poslani sažetak, kreira vremensku oznaku te na temelju ta dva objekta stvara novi sažetak. Novi sažetak TSA potpisuje svojim privatnim ključem i šalje nazad podnositelju zahtjeva za vremenskom oznakom. Podnositelj zahtjeva dokument posprema zajedno s vremenskom oznakom i sažetkom.
- ◆ TSA ne prima originalne podatke od podnositelja zahtjeva već uvijek barata sažetcima podataka.

Postupak provjere vremenskog žiga



Postupak provjere vremenskog žiga

- ◆ Podnositelj zahtjeva prvo izračunava sažetak originalnih podataka, nakon toga tom sažetku nadodaje vremensku oznaku koju je dobio od TSA i ponovo izračunava sažetak.
- ◆ Nakon toga, pošiljatelj dohvaća certifikat TSA koji sadrži javni ključ i njime dešifririra poruku dobivenu od TSA. Time postupkom dokazuje se da je TSA zaista šifrirao (potpisao) tu poruku svojim privatnim ključem. Nakon toga dešifriranu poruku od TSA usporedimo sa sažetkom koji smo prije izračunali.
- ◆ **Ako su sažetci jednaki, dokazano je da su i vremenska oznaka i dokument nepromijenjeni te da je TSA izdao vremensku oznaku**

Postupak provjere vremenskog žiga

- ◆ **Ne može se poreći da je podnositelj zahtjeva za vremenskom oznakom bio u posjedu originalnog dokumenta u vremenu naznačenom vremenskom oznakom.**
- ◆ Ako sažetci nisu jednaki, to znači
 - da su vremenska oznaka ili dokument promijenjeni
 - ili da vremensku oznaku nije izdao navedeni TSA

Davatelji usluga certificiranja (CA) u RH

1. Financijska agencija (FINA)

- Datum upisa u evidenciju: 16. 7. 2008.
- Usluge: *kvalificirani certifikat za e-potpis, kvalificirani certifikat za e-pečat, kvalificirani certifikat za autentifikaciju mrežnih stranica, kvalificirani vremenski žig, certifikat za elektronički potpis (prepoznat na nacionalnoj razini)*
- Izdaje certifikate fizičkim i pravnim osobama za opću namjenu

2. Agencija za komercijalnu djelatnost (AKD)

- Datum upisa u evidenciju: 29. 5. 2015.
- Usluge: *kvalificirani certifikat za e-potpis, kvalificirani certifikat za e-pečat, kvalificirani vremenski žig*
- Certifikati za eOI – pametna osobna iskaznica

Evidenciju davatelja usluga certificiranja u RH vodi Ministarstvo gospodarstva i održivog razvoja

3. Zagrebačka banka (ZABA)

- Datum upisa u evidenciju: 7. 6. 2016.
- Usluge: *kvalificirani certifikat za e-potpis, kvalificirani vremenski žig*
- Certifikati primarno za bankarske usluge

Vremenska ovjera u RH

FINA TSA – davatelj usluga javne vremenske ovjere

- ◆ FINA (kao **TSA**) pružatelj je usluge **ovjere elektroničkog potpisa**
- ◆ FINA TSA vremenskim žigom ovjerava potpis potpisnika
- ◆ potvrđuje se da su **podaci i elektronički potpis postojali prije stavljanja vremenskog žiga**

Digitalni potpis u EU (i RH) – tri vrste potpisa

■ Elektronički potpis

- podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje

■ Napredni elektronički potpis mora ispunjavati sljedeće zahtjeve:

- na nedvojben način je povezan s potpisnikom
- omogućava identificiranje potpisnika
- izrađen je korištenjem podataka za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom
- povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka

■ Kvalificirani elektronički potpis

- napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i **temelji se na kvalificiranom certifikatu za elektroničke potpise**

Problemi s primjenom e-potpisa u EU

- ◆ zemlje članice prihvatile su kvalificirane elektroničke potpise kao pravno ekvivalentne ručnim potpisima te ih prihvaćaju kao dokaz u pravnim postupcima
– **pravna osnova za korištenje digitalnih potpisa postoji**
- ◆ neke zemlje još uvijek imaju formalne prepreke širem uvođenju digitalnog potpisivanja (npr. zahtjevi za pisanim potpisom na dva primjerka na posebnom obrascu)
- ◆ korištenje digitalnog potpisa u zemljama EU još nije doseglo svoj vrhunac, ali se dogodio porast korištenja za vrijeme *lockdowna* izazvanog pandemijom COVID-a

Uredba eIDAS

- ◆ eIDAS – *Electronic Identification and Signature* (hrv. električna identifikacija i potpis)
- ◆ Uredba Europskog parlamenta i Vijeća o električkoj identifikaciji i uslugama povjerenja za električke transakcije na unutarnjem tržištu – donesena 23. 7. 2014.
 - Obvezujući zakonodavni akt za sve države članice
- ◆ Donesena zbog neusklađenosti nacionalnih zakonodavstava
 - Razlike u provedbi normi i pravila u praksi
 - **Kako pouzdano validirati e-potpis potpisnika iz druge države?**
 - Nedostatak pouzdanih informacija potrebnih za potpunu validaciju e-potpisa
- ◆ **Cilj: uspostava povjerenja i uzajamnog priznavanja e-potpisa i e-pečata unutar EU**

Digitalni potpis u EU (i RH)

- ◆ Do **7. 7. 2017.** u RH Zakon o elektroničkom potpisu (iz 2002. godine)
- ◆ **23. 7. 2014.** Europski parlament i vijeće donose uredbu eIDAS
- ◆ **Od 1. 7. 2016.** Zakon o elektroničkom potpisu prestaje vrijediti u dijelu koji je u suprotnosti s uredbom eIDAS
- ◆ **19. 6. 2017.** Hrvatski sabor donosi Zakon o provedbi Uredbe (...)

Elektronički pečat

◆ Tri vrste pečata:

Uvodi se
uredbom eIDAS

■ Elektronički pečat

- podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka

■ Napredni elektronički pečat mora ispunjavati sljedeće zahtjeve:

- na nedvojben način je povezan s autorom pečata
- omogućava identificiranje autora pečata
- izrađen je korištenjem podataka za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata
- povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka

■ Kvalificirani elektronički pečat

- napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat

Elektronički potpis i pečat

Elektronički potpis	Elektronički pečat
Potpisnik: fizička osoba koja izrađuje elektronički potpis	Autor pečata: pravna osoba koja izrađuje elektronički pečat
Elektronički potpis: podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje	Elektronički pečat: podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka
Sredstvo za izradu elektroničkog potpisa	Sredstvo za izradu elektroničkog pečata
Certifikat za elektronički potpis	Certifikat za elektronički pečat

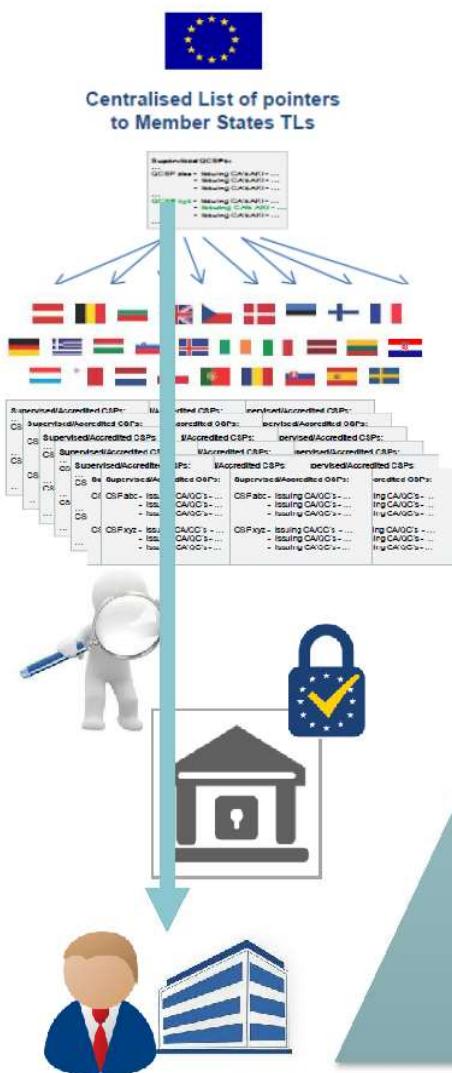
preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, travanj 2015.

Elektronički potpis i pečat (2)

Elektronički potpis	Elektronički pečat
Napredan elektronički potpis <ul style="list-style-type: none">• Na nedvojben način je povezan s potpisnikom• Omogućava identificiranje potpisnika• Izrađen je korištenjem podacima za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom• Povezan je s njime potpisanim podacima na način da se može se otkriti bilo koja naknadna izmjena podataka	Napredan elektronički pečat <ul style="list-style-type: none">• Na nedvojben način je povezan s autorom pečata• Omogućava identificiranje autora pečata• Izrađen je korištenjem podacima za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata• Povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka
Kvalificirani certifikat za elektronički potpis Izdaje ga kvalificirani pružatelj usluga povjerenja i ispunjava posebne uvjete	Kvalificirani certifikat za elektronički pečat Izdaje ga kvalificirani pružatelj usluga povjerenja i ispunjava posebne uvjete
Kvalificirano sredstvo za izradu elektroničkog potpisa Dodatno ispunjava zahtjeve za povjerljivost i sigurnost podataka za izradu e-potpisa, zaštićuju e-potpis od krivotvorenja i sl.	Kvalificirano sredstvo za izradu elektroničkog pečata Dodatno ispunjava zahtjeve za povjerljivost i sigurnost podataka za izradu e-pečata, zaštićuju e-pečat od krivotvorenja i sl.

preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, travanj 2015.

Sustav povjerenja prema uredbi eIDAS



preuzeto iz: Perinčić, M., eIDAS uredba – Povjerenje i uzajamno priznavanje e-potpisa i e-pečata u EU, stručni skup e-biz 2015., Zagreb, 2015.

Sigurnost XML-dokumenata

- ◆ Elektroničko poslovanje uglavnom se temelji na razmjeni **XML dokumenata**.
- ◆ Sigurnosne norme ugrađene u XML:
 - ***XML-Encryption*** i ***XML-Signature***
 - dodaju se dokumentu bez kršenja pravila XML-a
 - takvi dokumenti mogu se pregledavati korištenjem standardnih alata za XML
- ◆ sigurnost XML-dokumenata može biti implementirana i korištenjem standardnih sigurnosnih protokola
 - ti algoritmi koriste binarne datoteke koje onda mogu biti interpretirane samo korištenjem posebnih alata

Sigurnost XML-dokumenata

- ◆ za siguran prijenos dokumenata kroz mrežu može se koristiti protokol TLS
 - time se **štiti samo prijenos** podataka kroz mrežu, a **ne i pohrana**
 - dokument prestaje biti siguran onog trenutka kada stigne na odredište
- ◆ primjenom sigurnosnih mjera nad samim dokumentom korištenjem standarda za sigurnost XML-a, dokument se osigurava i u prijenosu i u kasnijoj pohrani jer se ne osigurava veza nego sami dokument
- ◆ norma ***XML Digital Signature*** koristi se za pohranu digitalnog potpisa u XML-dokument
- ◆ norma ***XML Encryption*** koristi se za pohranu kriptiranog sadržaja u formatu XML

Kanonikalizacija

- ◆ dva logički jednaka XML-dokumenta mogu biti različito zapisana
- ◆ primjerice, u jednom se nalazi **razmak viška ili prazan red viška**
- ◆ dva dokumenta logički jednaka, ali sažetak ta dva dokumenta dobiven *hash*-algoritmom nije jednak!
 - kod digitalnog potpisivanja to za **posljedicu ima neuspješnu verifikaciju potpisa**, iako dokument logički nije promijenjen, tj. očekivalo bi se da bi verifikacija trebala biti uspješna
- ◆ kako bi se takvi problemi izbjegli, **XML-dokumente treba kanonikalizirati** tj. **svesti se na jednak (kanonički) oblik** (normiranje razmaka i sl.)

XML-Signature (XML-DSig)

- ◆ **XML-DSig** je W3C norma
 - ◆ W3C = World Wide Web Consortium
- ◆ definira kako ugraditi digitalni potpis u XML dokument (tako da su zadovoljena pravila XML-a)
- ◆ nije algoritam za digitalno potpisivanje
- ◆ jednim potpisom moguće je potpisati više dokumenata
- ◆ moguće je potpisati i dokumente koji nisu u formatu XML
- ◆ moguće je potpisati samo dio XML dokumenta (na taj se način omogućuje da različite dijelove jednog XML-dokumenta potpisuju različiti ljudi)

XML Signature Syntax and Processing Version 1.1

(W3C preporuka, 11.4.2013.)

<http://www.w3.org/TR/xmldsig-core/>

XML-Signature (XML-DSig)

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI?>
      (<Transforms>) ?
      <DigestMethod>
        <DigestValue>
      </Reference>)+)
    </SignedInfo>
    <SignatureValue>
      (<KeyInfo>) ?
      (<Object ID?>) *
    </Signature>
```

- ◆ XML potpis se u XML dokumentu realizira preko elementa ***signature***
- ◆ ? - predstavlja nula ili jedno pojavljivanje,
- ◆ + - jedno ili više pojavljivanja,
- ◆ * - nula ili više pojavljivanja

XML-Signature (XML-DSig)

```
<Signature ID?>
    <SignedInfo>
        <CanonicalizationMethod/>
        ...
    </SignedInfo>
    ...
</Signature>
```

- ◆ Element *SignedInfo* – unutar svojih podelemenata **identificira podatke koji se potpisuju te različite algoritme** koji će se koristiti
- ◆ *CanonicalizationMethod* - sadrži ime **algoritma kojim se radi kanonikalizacija podataka**

XML-Signature (XML-DSig)

- ◆ *SignatureMethod* - definira **algoritam za generiranje potpisa**
- ◆ *SignatureValue* - sadrži vrijednost potpisa elementa *SignedInfo*

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
      (<Reference URI?>
        (<Transforms>) ?
        <DigestMethod>
          <DigestValue>
        </Reference>) +
      </SignedInfo>
    <SignatureValue>
    ...
  </Signature>
```

XML-Signature (XML-DSig)

- ◆ **Reference** - identificira resurse koji će biti potpisani i sve algoritme koji će se koristiti za pretprocesiranje podataka.
- ◆ Ti algoritmi su ispisani u elementu **Transforms** i uključuju operacije kao što su šifriranje/dešifriranje, kompresija/inflacija ili **XPath** transformacija (XPath omogućuje potpisivanje dijela dokumenta).

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI?>
      (<Transforms>)?)
    <DigestMethod>
    <DigestValue>
  </Reference>) +
  </SignedInfo>
  <SignatureValue>
...
</Signature>
```

XML-Signature (XML-DSig)

- ◆ Element **Reference** ima atribut **URI** koji je neobavezan, ali ako potpis sadrži **više elemenata Reference** onda je URI neobavezan samo za jedan element, a ostali ga moraju imati.
- ◆ Ako je sadržaj URI-ja "", tj. prazan znakovni niz, to znači da se potpisuje dokument u kojem se nalazi element

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI?>
      (<Transforms>) ?
    <DigestMethod>
      <DigestValue>
    </Reference>) +
  </SignedInfo>
  <SignatureValue>
...
</Signature>
```

XML-Signature (XML-DSig)

Svaki *Reference* uključuje :

- ◆ **DigestMethod** - sadrži informaciju o algoritmu koji se koristi za računanje sažetka dokumenta
- ◆ **DigestValue** - sadrži sažetak dokumenta izračunat algoritmom navedenim u *DigestMethod*

KeyInfo - sadrži informacije o ključu i o certifikatu

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI?>
      (<Transforms>) ?
      <DigestMethod>
      <DigestValue>
    </Reference>) +
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>) ?
...
</Signature>
```

XML-Signature (XML-DSig)

```
<SignedInfo>
  <CanonicalizationMethod
    Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
  <SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <Reference URI="">
    <Transforms>
      <Transform
        Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <DigestValue>tVicGh6V+8cHbVVFIU91o5+L3OQ=</DigestValue>
  </Reference>
</SignedInfo>
```

XML-Signature (XML-DSig)

```
<SignatureValue>
dJDHiGQMaKN8iPuWApAL57eVnxz2BQtyujwfPSgE7HyKoxYtoRB97ocxZ
8ZU440wHtE39ZwRGIjvwor3WfURxnIgnI1CChMXXwoGpHH//Zc0z4ejaz
DuCNEq4Mm4OUVTiEVuwcvAOMkfDHaM82awYQiOGcvMbZe38UX0oPJ2DOE=
</SignatureValue>
<KeyInfo>
<X509Data>
<X509SubjectName>
CN=My Name,O=Test Certificates Inc.,C=US
</X509SubjectName>
<X509Certificate>
MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhkiG9v0BAQUFADBAMQswCQYD
VQQGEwJVUzEfMB0GA1UEChMWVGVzdCBDZXJ0aWZpY2F0ZXNgbSW5jLjEQ
MA4GA1UEAxMHTXkgTmFtZTAeFw0wNzAxMDMyMTE4MTFaFw0zMTA4MjUy
...
</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</PurchaseOrder>
```

XML-Signature (XML-DSig)

- ◆ XML potpis može se pojaviti u tri osnovna oblika:
 - Omotani potpis (**Enveloped**) – potpis se nalazi unutar dokumenta.
 - Omotavajući potpis (**Enveloping**) – potpis omeđuje dokument koji potpisuje.
 - Odvojeni potpis (**Detached**) – potpis se nalazi u zasebnom dokumentu, a URI (*Universal Resource Identifier*) određuje koji dokument potpisuje.
- moguće je kombinacijama ta tri oblika dobiti nove
- jedna od mogućih kombinacija: omotavajući potpis umetnuti u dokument tako da on potpisuje neke točno određene podatke

XML-Signature (XML-DSig)

```
<Igrac xmlns="http://www.hou.hr/">
  <Ime>Antea</Ime>
  <Prezime>Tadic</Prezime>
  <Pozicija>Tehnicar</Pozicija>

  <Signature xmlns='http://www.w3.org/2000/09/xmldsig#'\>

    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/07/xmldsig#rsa-sha1" />
      <Reference URI="">
        <Transforms Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710" />
        <DigestMethod Algorithm="http://www.w3.org/2000/07/xmldsig#sha1" />
        <DigestValue>jkhKJHHIhkklADKHj=dfs34'FDE'?sds</DigestValue>
      </Reference>
    </SignedInfo>

    <SignatureValue>DFSLK89sdf?sdasHK</SignatureValue>

    <KeyInfo>
      <X509Data>
```

- ◆ Primjer omotanog potpisa - potpisuje se dokument u kojem se nalazi <Signature>

XML-Signature (XML-DSig)

- ◆ U slučaju omotavajućeg potpisa, potpisuje se sadržaj elementa *Object*

```
<Signature ID?>
  <SignedInfo>
    ...
  </SignedInfo>
  <SignatureValue>
    (<KeyInfo>) ?
    (<Object ID?>)*
  </Signature>
```

XML-Signature (XML-DSig)

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <ds:SignatureMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#obj">
            <ds:DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue/>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue/>
    <ds:Object Id="obj">Hello, World!</ds:Object>
</ds:Signature>
```

- ◆ Primjer omotavajućeg potpisa - potpisuje se sadržaj elementa <Object>

XML-Signature (XML-DSig)

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <ds:SignatureMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="http://www.w3.org/TR/xml-stylesheet">
            <ds:DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue/>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue/>
</ds:Signature>
```

- ◆ Primjer odvojenog potpisa – potpis se nalazi u zasebnoj XML-datoteci, a ono što se potpisuje identificira se URI-jem u elementima <Reference>

XML-Signature (XML-DSig)

```
<Igrac xmlns="http://www.hou.hr/">
  <Ime>Antea</Ime>
  <Prezime>Tadic</Prezime>
  <Pozicija>Tehnicar</Pozicija>
  <Signature xmlns='http://www.w3.org/2000/09/xmldsig#'%gt;
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/07/xmldsig#rsa-sha1" />
      <Reference URI=""> ovaj dokument
        <Transforms Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710" />
        <DigestMethod Algorithm="http://www.w3.org/2000/07/xmldsig#sha1" />
        <DigestValue>jkhKJHHihkk1ADKHj=dfsf34'FDE'?sdsa</DigestValue>
      </Reference>
      <Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
      </Reference> neki drugi dokument identificiran URI-jem
    </SignedInfo>
    <SignatureValue>DFSLK89sdf?sdashK</SignatureValue>
    <KeyInfo>...</KeyInfo>
    <Object>...</Object>
  </Signature>
</Igrac>
```

Primjer hibridnog potpisa – kombinacija omotanog i odvojenog potpisa

XAdES (*XML Advanced Electronic Signatures*)

- ◆ **Skup proširenja preporuke XML-Dsig**

(samo prijavljen za W3C preporuku)

ETSI (*European Telecommunications Standards Institute*) norma

TS 101 733

- ◆ Definira šest profila koji se razlikuju po razini zaštite koju nude:

- XAdES - napredni el. potpis u skladu s Direktivom 1999/93/EC
- XAdES-T - uključuje i vremensku oznaku
- XAdES-C - dodaje na XAdES-T poveznice na certifikate i listu opozvanih certifikata
- XAdES-X - dodaje na XAdES-C vremenske oznake na uvedene poveznice
- XAdES-X-L - u potpisani dokument dodaje certifikate i listu opozvanih certifikata
- XAdES-A - zahtijeva slijed vremenskih oznaka za dugoročno arhiviranje

XML Encryption (XML-Enc)

- ◆ **XML-Enc** opisuje kako šifrirani sadržaj **ugraditi u XML**
- ◆ **Nije** algoritam šifriranja

- ◆ Mogu se šifrirati i neXML-ovski dokumenti
- ◆ Moguće je šifrirati samo dio XML-dokumenta
- ◆ Različite dijelove XML-dokumenta moguće je šifrirati različitim ključevima – kontrola pristupa

- ◆ **XML Encryption Syntax and Processing** Version 1.1. (11.4.2013.)
<http://www.w3.org/TR/xmlenc-core/>

XML Encryption

Šifriranje se može izvesti na tri načina:

- ◆ korištenjem **simetrične kriptografije** – podatci se šifriraju simetričnim ključem koji su ranije sudionici komunikacije na neki (siguran) način razmijenili
- ◆ korištenjem **asimetrične kriptografije** – podatci se šifriraju javnim ključem primatelja
- ◆ korištenjem **hibridnog pristupa** – podatci se šifriraju simetričnim ključem, a taj simetrični ključ šifrira se javnim ključem primatelja; šifrirani simetrični ključ i sadržaj šifriran tim simetričnim ključem ugrađuju se u XML-dokument; ovaj je pristup najučestaliji

XML Encryption – struktura

```
<EncryptedData Id? Type?MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey?>
    <AgreementMethod?>
    <ds:KeyName?>
    <ds:RetrievalMethod?>
    <ds:*?>
  </ds:KeyInfo?>
  <CipherData> ←
    <CipherValue?>
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties?> ←
</EncryptedData>
```

Algoritam kojim se podatci šifriraju

Informacije o ključu kojim je sadržaj šifriran

Šifrirani podatci

Dodatne informacije

XML-Encryption (XML-Enc)

- ◆ Specifikaciju ***XML Encryption Syntax and Processing*** izdao je **W3C XML Encryption Working Group** s ciljem da uspostavi proces šifriranja/dešifriranja digitalnih sadržaja (uključujući XML dokumente kao i njihove dijelove) i sintaksu, kako bi se prikazali:
 - **šifrirani sadržaj** i
 - **informacija koja omogućava** određenom primatelju **dešifriranje** primljenog sadržaja.
- ◆ Rezultat šifriranja je podatkovni element koji sadrži (preko jednog od svojih podelemenata) ili identificira (preko URI reference) **šifrirane podatke**.
- ◆ Kad šifriramo XML element ili sadržaj elementa, **šifrirani podaci** (*element EncryptedData*) **zamjenjuju element odnosno sadržaj** u šifriranoj verziji XML dokumenta.

XML Encryption – primjer

```
<?xml version="1.0" standalone="no"?>
<igrac>
    <ime>Antea</ime>
    <prezime>Tadic</prezime>
    <EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
        xmlns="http://www.w3.org/2001/04/xmlenc#">
        <EncryptionMethod algoritam za šifriranje saržaja
            Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                <EncryptionMethod algoritam šifriranja simetričnog ključa
                    Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <KeyName>session</KeyName>
                </KeyInfo>
                <CipherData> Šifrirani simetrični ključ
                    <CipherValue>r4f7SI1aZKSvibbfsd5345</CipherValue>
                </CipherData>
            </EncryptedKey>
        </KeyInfo>
        <CipherData> podatci šifrirani simetričnim ključem
            <CipherValue>sGNhKqcSovipJdOFCFKYEEMRFsdaZIUh</CipherValue>
        </CipherData>
    </EncryptedData>
</igrac>
```

- šifrira se sadržaj elementa <pozicija>
- koristi se hibridni pristup

Šifrirani sadržaj

algoritam za šifriranje saržaja

Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />

algoritam šifriranja simetričnog ključa

Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />

simetrični ključ

<CipherValue>r4f7SI1aZKSvibbfsd5345</CipherValue>

podatci šifrirani simetričnim ključem

<CipherValue>sGNhKqcSovipJdOFCFKYEEMRFsdaZIUh</CipherValue>

- simetrični ključ
šifrira se javnim
ključem
primatelja
(algoritam RSA)
i zajedno sa
šifriranim
sadržajem šalje
na odredište

XML Encryption – primjer

Objašnjenje primjera:

- ◆ šifriran je sadržaj elementa <pozicija>
- ◆ hibridni pristup - podatci se šifriraju simetričnim ključem, a onda se taj simetrični ključ šifrira javnim ključem primatelja i takav se zajedno sa šifriranim sadržajem šalje na odredište
- ◆ na slici je plavom bojom označen algoritam kojim se šifrira simetrični ključ - asimetrični algoritam RSA
- ◆ zelenom je bojom prikazan šifrirani ključ
- ◆ sadržaj XML-dokumenta koji je potrebno sakriti šifrira se simetričnim algoritmom AES što je na slici prikazano narančastom bojom. Tako se dobije šifrirani sadržaj koji je na slici označen sivom bojom.
- ◆ element <EncryptedData> (crveno na slici) nalazi upravo na mjestu na kojem se prethodno nalazio element koji se šifrira

Pitanja

1. Koji je redoslijed razmjene sljedećih dokumenata?

- ◆ *e-otpremnica*
- ◆ *e-račun*
- ◆ *e-primka*
- ◆ *e-narudžbenica*

2. Koji je drugi naziv za asimetričnu kriptografiju?

3. Koji je najpoznatiji algoritam za asimetričnu kriptografiju?

4. Koji hash-algoritmi se koriste?

-
5. Što se može dokazati digitalnim potpisom?
 6. Što se može potvrditi digitalnim certifikatom?
 7. Što se može dokazati vremenskim žigom (što se tiče pouzdanosti digitalnog potpisa)?

1. redoslijed razmjene dokumenata:

- ◆ *e-narudžbenica*
- ◆ *e-otpremnica*
- ◆ *e-primka*
- ◆ *e-račun*

2. Koji je drugi naziv za asimetričnu kriptografiju?

Kriptografija javnog ključa.

3. Koji je najpoznatiji algoritam za asimetričnu kriptografiju?

RSA

4. Koji hash-algoritmi se koriste?

SHA-2 i SHA-3

5. Što se može dokazati digitalnim potpisom?

Identitet pošiljatelja i integritet (cjelovitost) sadržaja.

6. Što se može potvrditi digitalnim certifikatom?

Da je određeni korisnik vlasnik određenog javnog ključa.

7. Što se može dokazati vremenskim žigom (što se tiče pouzdanosti digitalnog potpisa)?

Da je potpis napravljen prije isteka valjanosti certifikata.

Sigurnost u elektroničkoj trgovini



Sigurnosni zahtjevi kod *online* plaćanja

- ◆ **Autentifikacija** - u transakciji online plaćanja se zna tko sudjeluje u transakciji i zna se da je osoba upravo ta za koju tvrdi da jest.
- ◆ **Integritet** - podaci iz transakcije se neće mijenjati
- ◆ **Jedinstvenost zahtjeva za plaćanjem** - omogućava trgovcu da prepozna ponovni zahtjev za istom transakcijom
- ◆ **Neporecivost transakcije** - nakon izvršavanja transakcije kupac ne može poreći da je izvršio transakciju, odnosno trgovac ne može poreći da je primio transakciju
- ◆ **Povjerljivost** – podacima o transakciji se ne može neovlašteno pristupiti
- ◆ **Privatnost i anonimnost kupca** - trgovac može vidjeti samo pseudonim ili korisničko ime kupca, ali ne i njegove privatne podatke
- ◆ **Pouzdanost sustava** - preventivne radnje u slučaju pada sustava te kod greški prilikom izvršavanja transakcije

Kartična naplata u elektroničkoj trgovini

- ◆ Primjer: **PayPal** – jedan od najraširenijih i najpoznatijih sustava za online plaćanje na svijetu
- ◆ pri transakciji se trgovcu **ne daje broj kreditne kartice**
 - trgovcu se proslijeđuje **samo e-mail adresa kupca**
 - trgovac prima *online* uplatu bez mogućnosti da vidi financijske podatke kupca
 - nakon svake transakcije korisnik na svoju e-mail adresu dobiva e-mail poruku s informacijama o izvršenoj transakciji
- ◆ svi podaci (osobni i financijski) koji se šalju s klijentskog računala na *PayPal* poslužitelj su šifrirani.
 - prilikom registracije ili prijave na *PayPal* web stranice koristi se TLS 1.2 (ili viši)
 - za SSL certifikate koristi se algoritam SHA-256
- ◆ poslužitelji s osjetljivim financijskim podacima **nisu direktno povezani na Internet**

Kartična naplata u elektroničkoj trgovini

Sigurnost *PayPal* transakcija (nastavak)

- ◆ Provjera:
- ◆ ***Address Verification Service (AVS)*** je sustav koji se koristi za **verifikaciju adrese osobe** koja tvrdi da posjeduje određenu kreditnu karticu. Sustav će usporediti adresu koju daje korisnik kreditne kartice kod izvršavanja transakcije online plaćanja (ili kod povezivanja kreditne kartice s *PayPal* računom) s adresom koja je zapisana kod izdavatelja kartice. AVS provjerava samo brojčani dio adrese (poštanski broj, kućni broj).
- ◆ ***Card Security Code (CSC)*** ili ***Card Code Verification (CCV)*** - troznamenkasti ili četveroznamenkasti sigurnosni kod koji se obično nalazi na stražnjoj strani kreditne kartice napisan obrnuto nakošeno.
 - Taj kod koristi se kao sigurnosna provjera kad ne postoji mogućnost korištenja PIN-a.
 - Trgovci koji zahtijevaju CVV2 kod pri transakcijama tipa ***card-not-present*** ne smiju taj kod **pohraniti**.
 - Ta sigurnosna mjera je jedna od sigurnosnih mjer sigurnosnog standarda **PCI DSS** (*Payment Card Industry Data Security Standard*).



Kartična naplata u elektroničkoj trgovini

- ◆ O sigurnosti...
... s web-stranica
pružatelja usluga online
naplate

- **3D Secure zaštita za sve trgovce i kupce**
 - WSpay™ sustav koristi najviše standarde zaštite i privatnosti podataka.
 - Svi trgovci koji koriste WSpay™ su uključeni u 3D secure zaštitu, čime se jamči korisnicima shopa da je kupnja sigurna.
 - Brojevi kreditnih kartica kupaca se ne čuvaju na sustavu a sami upis se štiti SSL enkripcijom podataka
- **Certifikacija po PCI DSS standardima**
 - WSpay™ sustav radi kontinuirano na povećanju sigurnosti i potvrđivanju toga. Od ove godine će biti potvrđeno da posluje po najvišim standardima koji kartičar propisuje.
 - PCI Data Security Standard (PCI DSS) je norma koja definira sigurnosne mjere za obradu, spremanje i prenošenja (komunikaciju) kartičnih podataka.



Sigurnost

Od 1.siječnja 2008. godine počeo se primjenjivati novi sigurnosni standard (PCI DSS) u CEMEA regiji. Sigurnosni standard vrijedi za sve trgovce, procesore i banke koji sudjeluju u kartičnom poslovanju. PCI DSS vrijedi i za proizvođače opreme, aplikacija kako i na tvrtke koje nude hosting usluge.

VISA, MasterCard, American Express, Diners, Discover Card i JCB su zajedno stvorili industrijski standard za sigurnost podataka kako bi zaštitili svoje korisnike. Ovaj standard za industriju kartičnog poslovanja osigurava svim trgovcima, bankama i pružateljima usluga zaštitu podataka vlasnika kartica.

Svi pružatelji usluga moraju se certificirati od strane kvalificiranih revizora sigurnosti za VISA-u i akreditiranog pružatelja usluga skeniranja za MasterCard kako bi zadržali pravo procesiranja kartičnog plaćanja.

PCI DSS - *Payment Card Industry Data Security Standard*

- sigurnosni standard za kartično poslovanje
- definira minimalne sigurnosne mjere i procese
- ◆ Definirao ga je *Payment Card Industry Security Standards Council*
 - **Visa, MasterCard, American Express, Discover Card i JCB** su zajedno stvorili industrijski standard za sigurnost podataka kako bi zaštitili svoje korisnike.
 - osigurava trgovcima, kartičnim kućama, bankama i ostalim poslovnim subjektima koji se bave kartičnim poslovanjem **zaštitu podataka vlasnika kartica**
- ◆ Prva verzija standarda PCI DSS izdana je 2004. godine
- ◆ Verzija 3.2.1 izdana je u svibnju 2018. godine

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

PCI DSS

- ◆ **Banke i pružatelji usluga** moraju se **certificirati kod kvalificiranih revizora sigurnosti**, a trgovci su dužni se pridržavati PCI DSS standarda i obavljati kartično poslovanje samo s certificiranim pružateljima usluga.
- ◆ PCI DSS 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.
 - ◆ 12 osnovnih zahtjeva i oko 270 podzahtjeva

PCI DSS – načela i zahtjevi

Neki od zahtjeva iz PCI DSS:

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

- Promijeniti početne zaporce postavljene od strane dobavljača

Zahtjev 3: Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štititi.

- **sigurnosni kodovi kartica** (troznamenkasti ili četveroznamenkasti broj obično ispisan na stražnjoj strani kartice) koji se koriste za potvrđivanje (verifikaciju) transakcije i **PIN brojevi ne smiju se pohranjivati.**

PCI DSS – načela i zahtjevi

Neki od zahtjeva iz PCI DSS (nastavak):

Zahtjev 4: Tijekom prijenosa putem otvorenih, javnih mreža svi podatci o vlasniku kartice moraju se štititi šifriranjem (enkripcijom).

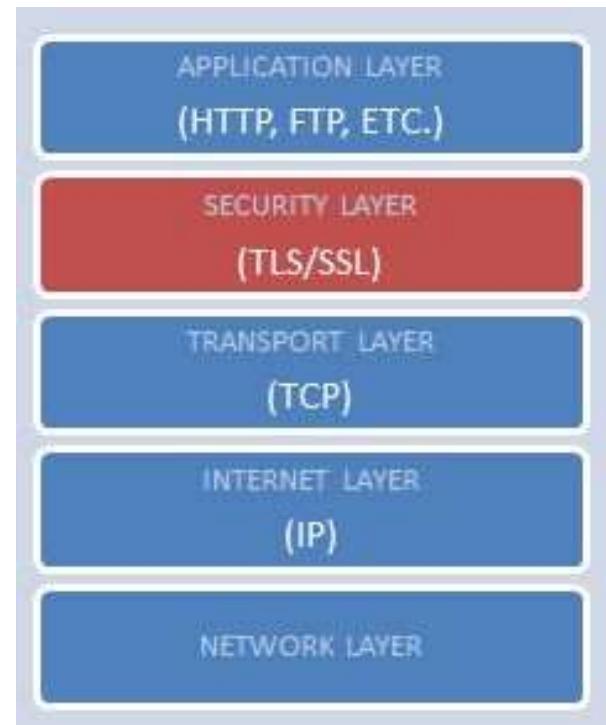
- Koristiti snažne kriptografske metode i sigurnosne protokole (primjerice SSL/TLS, IPSEC, SSH) za **zaštitu osjetljivih kartičnih (korisničkih) podataka tijekom prijenosa** kroz otvorene, javne mreže (Internet, bežični prijenos, GSM i GPRS).

Zahtjev 5: Nužno je koristiti i redovito osvježavati softver za zaštitu od zlonamjernog koda, odnosno antivirusni softver

...

TLS / SSL

- ◆ Broj kreditne kartice upisuje se preko web preglednika i putuje do web poslužitelja on-line trgovine
- ◆ **kod električkog plaćanja** potrebno je između transportnog protokola TCP i aplikacijskog protokola HTTP koristiti i **sigurnosni protokol TLS / SSL**
- ◆ **TLS / SSL** osigurava **šifriranje** cijelokupne komunikacije iznad transportnog sloja.



TLS / SSL

- ◆ **protokol SSL** (eng. *Secure Socket Layer*) razvila je tvrtke Netscape Communications – verzija SSL 3.0 izašla je 1996. godine
- ◆ **protokol TLS** (eng. *Transport Layer Security*) objavljen je 1999. godine - nadogradnja na SSL 3.0
 - 2006. godine TLS 1.1
 - 2008. godine **TLS 1.2** - koristi *hash-funkciju SHA-256* (iz SHA-2)
 - 2018. godine **TLS 1.3**
- ◆ **TLS / SSL**
 - koristi se za ostvarivanje sigurnije razmjene povjerljivih podataka, poput korisničkog imena i zaporce, broja kreditne kartice i sl.
 - temelji se na upotrebi kriptografije te infrastrukture javnih ključeva (engl. *Public key infrastructure - PKI*)
 - privatni i javni ključevi

TLS / SSL

- ◆ Za **kartično plaćanje** preko mreže preporučuje se korištenje **TLS 1.2** ili **TLS 1.3** (objavljen u kolovozu 2018. godine)
 - ◆ Ne koristiti SSL.
-
- ◆ Pri korištenju SSL/TLS-a
 - adresa počinje oznakom **https : //**
 - sva komunikacija između preglednika i web poslužitelja se šifrira
-
- ◆ **HTTPS** (*Hypertext Transfer Protocol Secure*) - kombinacija protokola HTTP i SSL/TLS (*Secure Sockets Layer / Transport Layer Security*)

TLS / SSL

- ◆ Služi za zaštitu od napada:
 - prislушкиvanje (eng. *eavesdropping*)
 - čovjek-u-sredini (eng. *man-in-the-middle*)
- ◆ onemogućuje se presretanje i neovlašteno prislушкиvanje komunikacije te eventualna krađa broja kreditne kartice
- ◆ međutim, ne rješava se problem **pohrane** brojeva kreditne kartice na samom poslužitelju

TLS / SSL

- ◆ Kad je uspostavljena sigurna veza (certifikat zaprimljen i provjerен od strane CA), pojavljuje se ikona lokota u pregledniku i adresa počinje oznakom `https://`



- ◆ Prilikom unosa povjerljivih podataka na web stranice provjeriti je li web stranica trenutno zaštićena (`https://`)
- ◆ preglednik obično ima ugrađene sigurnosne mehanizme koji javljaju ako web sjedište nije sigurno

TLS / SSL

- ◆ neki CA su uveli SSL certifikate tipa “samo provjera domene” (*domain validation only*) za koje se radi **minimalna provjera** detalja u certifikatu
 - za svaku uspješnu SSL konekciju – pojavljuje se ikona lokota
- ◆ **mnogi preglednici nisu jasno razlikovali certifikate s blažom validacijom od onih koji rade rigoroznu provjeru**
 - korisnici nisu svjesni je li web sjedište dovoljno provjereno ili nije
 - mogućnost *phishinga* – web sjedišta napravljena da bi služila za *phishing* mogu koristiti TLS/SSL da bi dobili dodatni kredibilitet
- ◆ **Extended Validation Certificate (EV)** propisuje **strože kriterije** za provjeru identiteta
 - Prikazuje se ime CA koji je izdao EV certifikat
 - Boja (obično zelena) ukazuje na to na je EV certifikat valjan
- ◆ Današnji web-preglednici prikazuju status EV.



Phishing

- ◆ **Phishing** - napadači pokušavaju saznati povjerljive podatke (najčešće zaporce, podatke o kreditnoj kartici ili PIN) lažno se predstavljajući kao vjerodostojan subjekt u komunikaciji.
- ◆ **lažnom porukom** elektroničke pošte ili porukom preko sustava za trenutno poručivanje korisnika se pokušava namamiti **na lažnu web stranicu**, kako bi na njoj upisao svoje korisničko ime i zaporku, PIN, broj kreditne kartice i sl.
- ◆ Npr. “*Radi provjere da Vaš račun nije neovlašteno korišten, molimo kliknite na poveznicu dolje i potvrdite svoj identitet*”
- ◆ lažne Web stranice banaka ili *online* trgovina koje vizualno izgledaju identično stvarnim stranicama
- ◆ Ako lažna stranica mimicira internetsko bankarstvo, u trenutku kada se korisnik prijavi na sustav, u pozadini ga skripta može automatski prijaviti na pravu stranicu banke, dok još vrijedi generirani OTP (one-time password). Nakon toga skripta, skriveno od korisnika, započinje prijenos novca...

TLS / SSL

- ◆ Tvrta koja je razvila određeni web preglednik odlučuje kojim certifikacijskim tijelima (CA – *certification authority*) će vjerovati.
- ◆ **Korisnik treba vjerovati HTTPS konekciji samo ako:**
 - Korisnik vjeruje da preglednik ispravno implementira HTTPS s ispravno unaprijed instaliranim provjerama certifikata poznatih i pouzdanih CA
 - Sjedište weba ima valjani certifikat (kojeg je potpisao CA)
 - Korisnik ima povjerenje u tog CA

TLS / SSL

- ◆ **TLS/SSL certifikati**
 - posjetiteljima Web sjedišta potvrđuju identitet web sjedišta,
 - garantiraju sigurnu i povjerljivu razmjenu podataka
- ◆ Kao rezultat raste povjerenje posjetitelja Web sjedišta.
- ◆ Najpoznatije tvrtke koje izdaju SSL certifikate:
VeriSign, Thawte, GeoTrust, RapidSSL, GlobalSign, GoDaddy, Entrust, ...
- ◆ korijenski CA – može ovlastiti druga certifikacijska tijela da potpisuju i provjeravaju certifikate u njihovo ime (hijerarhija CA)
- ◆ **Povjerenje u sustav certificiranja?**
 - povjerenje u CA niže u hijerarhiji koji su dobili ovlasti od korijenskih CA?
 - donošenje normi za provjeru CA (kao PCI norme u kartičnom poslovanju)?





Zaštita i sigurnost informacijskih sustava

Sigurnost u sustavima za elektroničko poslovanje 2. dio

prof. dr. sc. Boris Vrdoljak

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Zaštićeno licencijom <http://creativecommons.org/licenses/by-nc-sa/2.5/hr/>



Creative Commons



□ **slobodno smijete:**

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo

□ **pod sljedećim uvjetima:**

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.

Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s <http://creativecommons.org/>.

Sigurnost usluga Weba

Tehnologija usluga weba se u elektroničkom poslovanju počela primjenjivati **pojavom sigurnosnih normi za usluge weba**.

Usluge weba

Osnovne norme za usluge weba:

- ◆ **SOAP** (engl. *Simple Object Access Protocol*)
 - protokol koji **definira strukturu paketa kojima se razmjenjuju strukturirani podaci** između dva udaljena programska entiteta
 - zasniva se na XML-u
 - osnovna norma ne uključuje sigurnosne mehanizme
- ◆ **WSDL** (engl. *Web Service Description Language*)
 - omogućuje **normizirani opis sučelja** usluge weba
- ◆ **UDDI** (engl. *Universal Description, Discovery and Integration*)
 - registar **za objavu i pretragu** postojećih usluga weba

SOAP

- ◆ SOAP poruke se sastoje od **tri glavna elementa**:
 - **omotnica (envelope)** - korijenski element koji definira početak i kraj SOAP poruke
 - **zaglavlje (header)** - nije obavezan element, a može sadržavati jedan ili više blokova metapodataka o samoj poruci
 - **tijelo (body)** - sadrži podatke namijenjene primatelju poruke



Usluge weba i normizacijske organizacije

W3C (World Wide Web Consortium) je specificirao norme :

- XML, XML Schema, XSLT
- specifikacije za implementaciju usluga weba – norme SOAP i WSDL

OASIS (Organization for Advancement of Structured Information Standards)

- ◆ normizacija jedne od najvažnijih komponenti specifikacija proširenja usluga weba – okvira **WS-Security** zaduženog **za sigurnosne mehanizme**

WS-I (Web Services Interoperability Organization) izdao je 2007. godine **Osnovni sigurnosni profil** (engl. **Basic Security Profile**) - verzija 1.1 je iz 2010.

- skup najvažnijih tehnologija vezanih uz **sigurnost XML-a i usluga weba**

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>

Sigurnost usluga weba

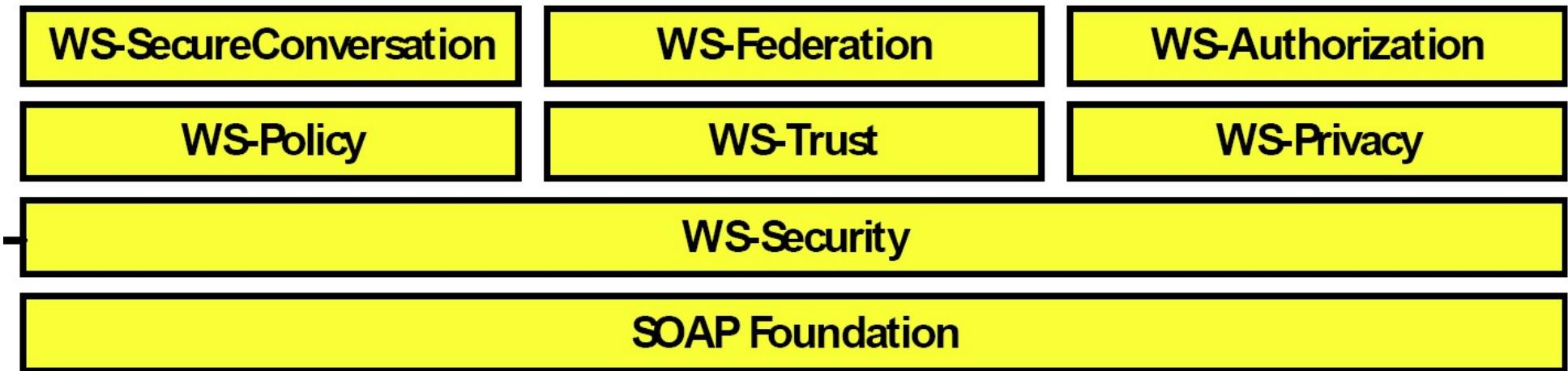
- ◆ **jezgra normi za web usluge - SOAP, WSDL i UDDI - nije dovoljna za uspješno ispunjavanje svih aspekata infrastrukture za e-Poslovanje.**
- ◆ zahtjevi uslužno orijentiranih arhitektura nadilaze ono što skup specifikacija **SOAP+WSDL+UDDI** može pružiti
- ◆ potrebno je uvesti dodatne tehnologije kako bi se ti zahtjevi mogli uspješno zadovoljiti
- ◆ proširenja specifikacija Web usluga: **WS-Extensions**
 - prepoznaju se po prefiksnu "**WS-**"

WS-Extensions

- ◆ Neka od važnijih proširenja - **WS-Extensions** (1):
 - **WS-Security** – grupa specifikacija za uvođenje **sigurnosnih mehanizama** koji se mogu koristiti za konstruiranje niza sigurnosnih protokola.
 - » **Integritet poruka** pruža **XML Signature**, a za **osiguravanje povjerljivosti** se koristi **XML Encryption**.

WS-Security (WSS)

- ◆ Razvoj sigurnosne arhitekture se nastavio pa su nad specifikacijom WS-Security razvijene dodatne specifikacije



WS-Extensions

- ◆ Neka od važnijih proširenja - *WS-Extensions* (2):
 - **WS-Policy** – omogućuje definiciju **pravila i ograničenja** vezanih uz **sigurnost** poruke, način obrade ili sam sadržaj
 - **WS-Trust** – specificira kako se sigurnosne značke (tokeni) izdaju, obnavljaju i validiraju
 - **WS-Privacy** – objašnjava kako web-usluge mogu provesti pravila vezana za **privatnost**

WS-Extensions

- ◆ Neka od važnijih proširenja - *WS-Extensions* (3):
 - **WS-SecureConversation** – za sigurnu konverzaciju - među ostalim, specificira kako se kreiraju i razmjenjuju ključevi
 - **WS-Federation** – bavi se upravljanjem sigurnosnim identitetima u heterogenom sigurnosnom okruženju
 - **WS-Authorization** – pokriva upravljanje podacima za autorizaciju kao što su sigurnosne značke (*token*) i politikama za davanje pristupa resursima

WS-Extensions

- ◆ Neka od važnijih proširenja - **WS-Extensions** (4):
 - **WS-ReliableMessaging** – za sigurnu dostavu SOAP poruka
 - **WS-Addressing** – za imenovanje i prepoznavanje krajnjih točaka u asinkronoj komunikaciji
 - **WS-MetadataExchange** – omogućuje ugradnju dodatnih metapodataka o usluzi koji bi stavili uslugu u semantički kontekst te pružali dodatne informacije kao što su kvaliteta usluge i sl.

Sigurnost usluga weba

WS-SecureConversation

WS-Federation

WS-Authorization

WS-Policy

WS-Trust

WS-Privacy

WS-Security

SOAP Foundation

WS-Security (WSS)

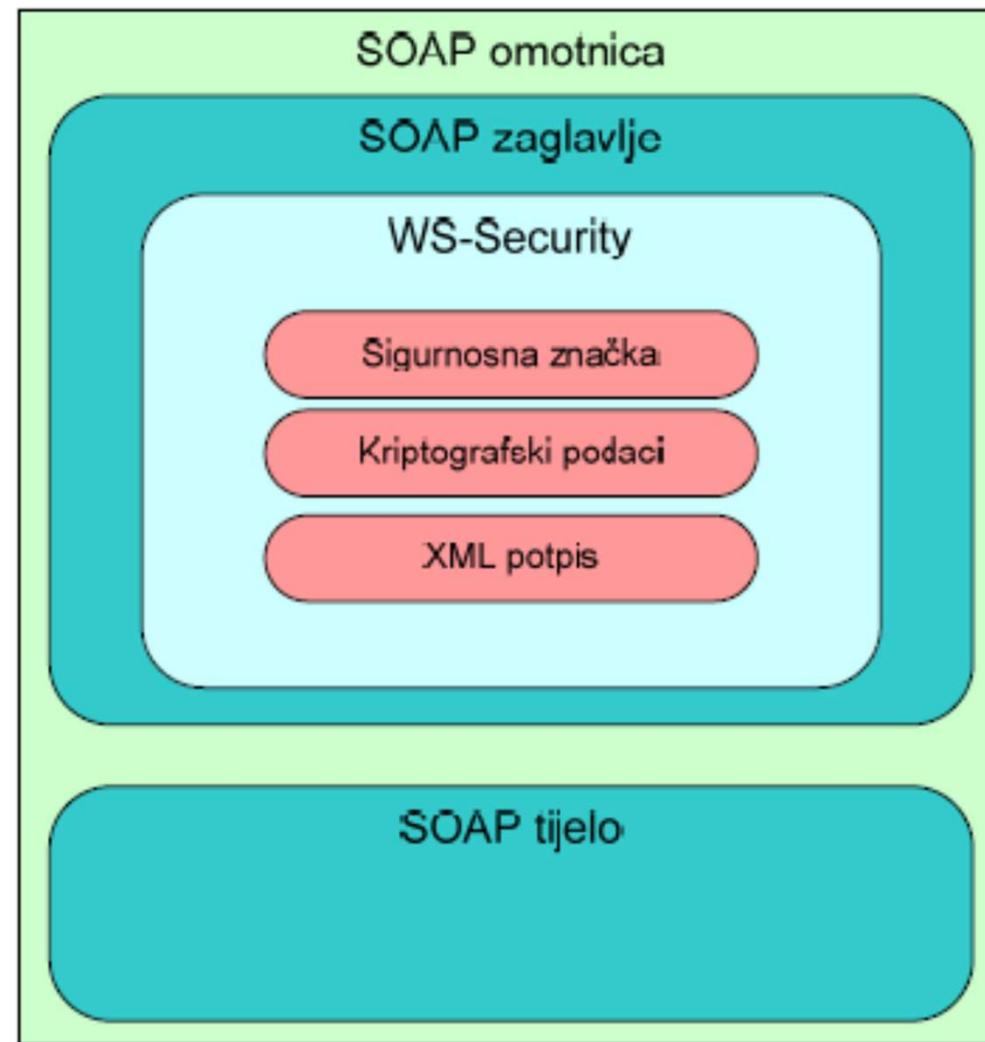
- ◆ **WSS** (**WS-Security**, *Web Services Security*) je komunikacijski protokol koji osigurava sigurnost primjene usluga Weba.
- ◆ razvili su ga IBM, Microsoft i VeriSign, a **OASIS** ga je objavio kao normu **WS-Security 1.1**.
- ◆ Prva verzija (1.0) izdana je 2004. godine, a verzija 1.1. izdana je 2006. godine
- ◆ cilj je postizanje **sigurnosti s kraja na kraj komunikacije**, a ne samo na razini prijenosa.

WS-Security (WSS)

- ◆ WS-Security definira **element SOAP zaglavlja** koji nosi podatke vezane uz **sigurnost**.
- ◆ **zaglavlje** može sadržavati informacije definirane normom **XML-Signature** koje opisuju način potpisivanja poruke, korišteni ključ i rezultat potpisa.
- ◆ kod šifriranja (kriptiranja) elemenata unutar poruke, element SOAP zaglavlja koji se odnosi na WS-Security sadrži informacije definirane normom **XML-Encryption**.
- ◆ WS-Security **ne definira** format potpisa ili šifriranja. Umjesto toga, specificira **način kako će se format**, definiran drugom specifikacijom, **ugraditi u SOAP poruku**.

WS-Security (WSS)

- ◆ Sigurnosne informacije u SOAP poruci prema normi WS-Security



WS-Security (WSS)

- ◆ **WS-Security 1.1** čine sljedeći dokumenti i specifikacije:
 - *SOAP Message Security 1.1* - glavna specifikacija
<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>
 - *Username Token Profile 1.1*
 - *X.509 Token profile 1.1*
 - *SAML Token profile 1.1*
 - *Kerberos Token Profile 1.1*
 - *Rights Expression Language (REL) Token profile 1.1*
 - *SOAP with Attachments (SwA) profile 1.1*
- ◆ pet sigurnosnih *tokena* (oznaka, značaka) koje su definirane u različitim profilima

WS-Security (WSS)

- ◆ WSS protokol uključuje detalje o korištenju
 - **digitalnih certifikata** kao što su **X.509** certifikati koji se koriste u primjeni PKI infrastrukture,
 - jezika **SAML** (*Security Assertion Markup Language*),
 - **Kerberosa** (protokol za autentifikaciju).
- ◆ prikazuje kako pripojiti sigurnosne tokene na poruke u izvršavanju Web servisa
- ◆ Kerberos, SAML i X.509 rješavaju problem autentifikacije

WS-Security (WSS)

- ◆ ***UsernameToken profile*** - specificira na koji način koristiti UsernameToken kao način identifikacije podnositelja zahtjeva putem korisničkog imena
- ◆ ***X.509 Certificate Token Profile*** - definira na koji način u SOAP poruku dodati X.509 certifikat (za validaciju javnih ključeva)
- ◆ ***The SAML Token Profile*** - definira na koji način možemo dodavati SAML izraze u sigurnosna zaglavlja te na koji način se referencirati na te izraze iz tijela SOAP poruke.
- ◆ ***The Kerberos Token Profile*** - propisuje način implementacije Kerberos AP-REQ poruke koja korisniku omogućuje autentikaciju usluge.
- ◆ ***The Rights Expression Language (REL) Token Profile*** – definira se uključivanje ISO/IEX 21000-5 prava u SOAP poruke. REL oznaka je definirana u obliku licence koja vlasniku garantira određena prava, a koju potpisuje nadležno tijelo.

WS-Security (WSS)

```
<SOAP:Envelope xmlns:SOAP="...">
  <SOAP:Header>
    <wsse:Security SOAP:role="..." SOAP:mustUnderstand="...">
      <wsse:UsernameToken>
        ...
        </wsse:UsernameToken>
        ...
      </wsse:Security>
    </SOAP:Header>
    <SOAP:Body Id="MsgBody">
      <!-- SOAP Body data -->
    </SOAP:Body>
  </SOAP:Envelope>
```

Primjer dijela zaglavlja SOAP poruke koji se odnosi na WS-Security

REST arhitektura

- ◆ REST je kratica za *Representational State Transfer*
 - Stil arhitekture za izgradnju raspodijeljenih sustava
 - Komunikacija između klijenta i poslužitelja odvija se bez očuvanja stanja na poslužitelju.
 - Pojedini resurs dostupan je korištenjem URI-ja.
- ◆ Postoje još i arhitekture GraphQL, oData itd.

RESTful usluge

- ◆ Web usluge koje se temelje na arhitekturi REST nazivaju se **RESTful** web usluge.
 - ◆ Daju mogućnost prijenosa podataka u XML i JSON formatu
 - ◆ RESTful web usluge jednostavnije su za implementaciju i fleksibilnije od klasičnih Web usluga gdje se koriste SOAP poruke.
-
- ◆ RESTful web usluge se u potpunosti oslanjaju na protokol HTTP i **nemaju ugrađene sigurnosne mehanizme**.
 - ◆ Veća je **sigurnosna ranjivost** nego kod klasičnih Web usluga.
 - ◆ **Ranjivosti koje vrijede općenito** za protokol HTTP i web aplikacije, vrijede i u ovom slučaju.

Primjeri elektroničkog poslovanja

- ◆ elektroničko komuniciranje s drugim poduzećima radi narudžbe proizvoda i usluga te njihovo elektroničko plaćanje
 - poslovanje medu tvrtkama – B2B (Business-to-Business)
- ◆ prodavanje proizvoda i usluga preko Web sjedišta
 - e-trgovina, poslovanje tvrtke s krajnjim potrošačem – B2C (Business-to-Consumer)

Sigurnost u elektroničkoj trgovini



Sigurnosni zahtjevi kod *online* plaćanja

- ◆ **Autentifikacija** - u transakciji online plaćanja se zna tko sudjeluje u transakciji i zna se da je osoba upravo ta za koju tvrdi da jest.
- ◆ **Integritet** - podaci iz transakcije se neće mijenjati
- ◆ **Jedinstvenost zahtjeva za plaćanjem** - omogućava trgovcu da prepozna ponovni zahtjev za istom transakcijom
- ◆ **Neporecivost transakcije** - nakon izvršavanja transakcije kupac ne može poreći da je izvršio transakciju, odnosno trgovac ne može poreći da je primio transakciju
- ◆ **Povjerljivost** – podacima o transakciji se ne može neovlašteno pristupiti
- ◆ **Privatnost i anonimnost kupca** - trgovac može vidjeti samo pseudonim ili korisničko ime kupca, ali ne i njegove privatne podatke
- ◆ **Pouzdanost sustava** - preventivne radnje u slučaju pada sustava te kod greški prilikom izvršavanja transakcije

Kartična naplata u elektroničkoj trgovini

- ◆ Primjer: **PayPal** – jedan od najraširenijih i najpoznatijih sustava za online plaćanje na svijetu
- ◆ pri transakciji se trgovcu **ne daje broj kreditne kartice**
- ◆ za slanje novca potrebno je znati samo **e-mail adresu** *PayPal* računa osobe/tvrtke kojoj se želi poslati novac
 - trgovac prima *online* uplatu bez mogućnosti da vidi financijske podatke kupca
 - nakon svake transakcije korisnik na svoju e-mail adresu dobiva e-mail poruku s informacijama o izvršenoj transakciji
- ◆ svi podaci (osobni i financijski) koji se šalju s klijentskog računala na *PayPal* poslužitelj su **šifrirani**.
 - prilikom registracije ili prijave na *PayPal* web stranice koristi se **TLS 1.2** (za SSL certifikate koristi se algoritam SHA-256)
- ◆ poslužitelji s osjetljivim financijskim podacima **nisu direktno povezani na Internet**

Kartična naplata u elektroničkoj trgovini

Provjera:

- ◆ **AVS (Address Verification Service)** je sustav koji se koristi za **verifikaciju adrese osobe** koja tvrdi da posjeduje određenu kreditnu karticu. Sustav će usporediti adresu koju daje korisnik kreditne kartice kod izvršavanja transakcije online plaćanja (ili kod povezivanja kreditne kartice s *PayPal* računom) s adresom koja je zapisana kod izdavatelja kartice. AVS provjerava samo brojčani dio adrese (poštanski broj, kućni broj).
- ◆ **Card Verification Code (CVC)** ili **Card Verification Value (CVV)** ili **Card Security Code (CSC)** - troznamenkasti ili četveroznamenkasti sigurnosni kod koji se obično nalazi na stražnjoj strani kreditne kartice napisan obrnuto nakošeno.
 - Taj kod koristi se kao sigurnosna provjera kad ne postoji mogućnost korištenja PIN-a.
 - Trgovci koji zahtijevaju CVV2 kod pri transakcijama tipa **card-not-present** ne smiju taj kod **pohraniti**.
 - Ta sigurnosna mjera je jedna od sigurnosnih mjer sigurnosnog standarda **PCI DSS** (*Payment Card Industry Data Security Standard*).



Zaštita podataka u kartičnom poslovanju

- ◆ O sigurnosti...
... s web-stranica
pružatelja usluga online
naplate

- **3D Secure zaštita za sve trgovce i kupce**
 - WSpay™ sustav koristi najviše standarde zaštite i privatnosti podataka.
 - Svi trgovci koji koriste WSpay™ su uključeni u 3D secure zaštitu, čime se jamči korisnicima shopa da je kupnja sigurna.
 - ~~Brojevi kreditnih kartica kupaca se ne čuvaju na sustavu a sami upis se štiti SSL enkripcijom podataka~~
- **Certifikacija po PCI DSS standardima**
 - WSpay™ sustav radi kontinuirano na povećanju sigurnosti i potvrđivanju toga. Od ove godine će biti potvrđeno da posluje po najvišim standardima koji kartičar propisuje.
 - ~~PCI Data Security Standard (PCI DSS) je norma koja definira sigurnosne mјere za obradu, spremanje i prenošenja (komunikaciju) kartičnih podataka.~~



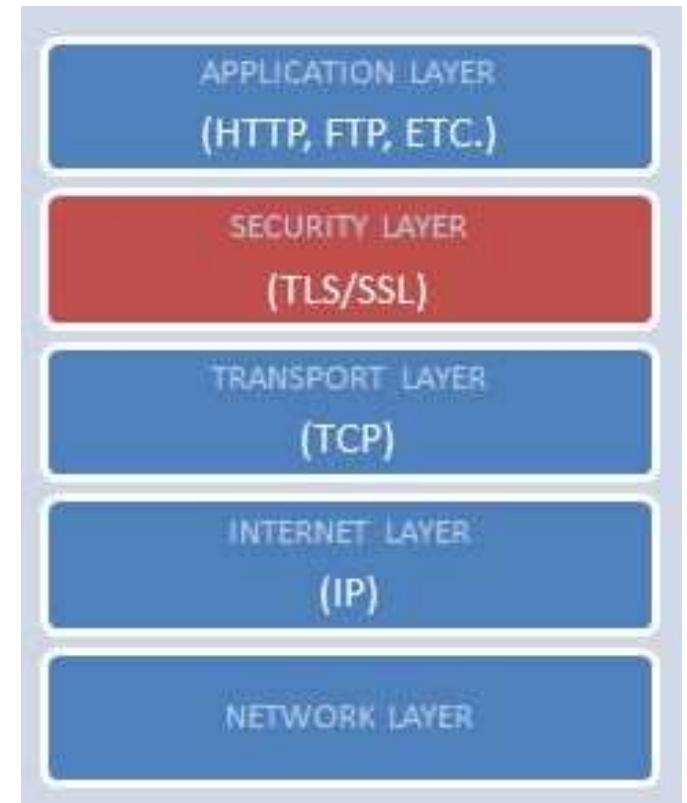
PCI DSS - *Payment Card Industry Data Security Standard*

- sigurnosni standard za kartično poslovanje
- definira minimalne sigurnosne mjere i procese
- ◆ Definirao ga je *Payment Card Industry Security Standards Council*
 - **Visa, MasterCard, American Express, Discover Card i JCB** su zajedno stvorili industrijski standard za sigurnost podataka kako bi zaštitili svoje korisnike.
 - osigurava trgovcima, kartičnim kućama, bankama i ostalim poslovnim subjektima koji se bave kartičnim poslovanjem **zaštitu podataka vlasnika kartica**

O PCI DSS-u detaljnije kasnije u ovom predavanju te u predavanju
Revizija sigurnosti informacijskih sustava

TLS / SSL

- ◆ Broj kreditne kartice upisuje se preko web preglednika i putuje do web poslužitelja on-line trgovine
- ◆ **kod elektroničkog plaćanja** potrebno je između transportnog protokola TCP i aplikacijskog protokola HTTP koristiti i **sigurnosni protokol TLS / SSL**
- ◆ **TLS / SSL** osigurava **šifriranje** cijelokupne komunikacije iznad transportnog sloja.



TLS / SSL

- koristi se za ostvarivanje sigurnije razmjene povjerljivih podataka, poput korisničkog imena i zaporke, broja kreditne kartice i sl.
- temelji se na upotrebi kriptografije te infrastrukture javnih ključeva (engl. *Public key infrastructure - PKI*)
 - privatni i javni ključevi

TLS / SSL

- ◆ Za **kartično plaćanje** preko mreže preporučuje se korištenje **TLS 1.2** ili **TLS 1.3** (objavljen 2018. godine)
 - ◆ Ne koristiti SSL.
-
- ◆ Pri korištenju SSL/TLS-a
 - adresa počinje oznakom **https : //**
 - sva komunikacija između preglednika i web poslužitelja se šifrira
-
- ◆ **HTTPS** (*Hypertext Transfer Protocol Secure*) - kombinacija protokola HTTP i SSL/TLS (*Secure Sockets Layer / Transport Layer Security*)

TLS / SSL

- ◆ Služi za zaštitu od napada:
 - prislушкиvanje (eng. *eavesdropping*)
 - čovjek-u-sredini (eng. *man-in-the-middle*)
- ◆ onemogućuje se presretanje i neovlašteno prislушкиvanje komunikacije te eventualna krađa broja kreditne kartice
- ◆ međutim, ne rješava se problem **pohrane** brojeva kreditne kartice na samom poslužitelju

TLS / SSL

- ◆ **TLS/SSL certifikati**
 - posjetiteljima Web sjedišta **potvrđuju identitet web sjedišta**,
 - garantiraju **sigurnu i povjerljivu razmjenu podataka**
- ◆ Kao rezultat raste povjerenje posjetitelja Web sjedišta.
- ◆ Najpoznatije tvrtke koje izdaju SSL certifikate:
GlobalSign, DigiCert, GoDaddy, Entrust, ...

TLS / SSL

- ◆ neki CA (*Certificate Authority*) su uveli SSL certifikate tipa “samo provjera domene” (*domain validation only*) za koje se radi **minimalna provjera** detalja u certifikatu
 - za svaku uspješnu SSL konekciju – pojavljuje se ikona lokota
- ◆ **mnogi preglednici nisu jasno razlikovali certifikate s blažom validacijom od onih koji rade rigoroznu provjeru**
 - mogućnost *phishinga* – web sjedišta napravljena da bi služila za *phishing* mogu koristiti TLS/SSL da bi dobili dodatni kredibilitet
- ◆ **Extended Validation Certificate (EV)** propisuje **strože kriterije** za provjeru identiteta
 - Prikazuje se ime CA koji je izdao EV certifikat
 - Boja (obično zelena) ukazuje na to na je EV certifikat valjan
- ◆ Današnji web-preglednici prikazuju status EV.



Phishing

- ◆ **Phishing** - napadači pokušavaju saznati povjerljive podatke (najčešće zaporce, podatke o kreditnoj kartici ili PIN) lažno se predstavljajući kao vjerodostojan subjekt u komunikaciji.
- ◆ **lažnom porukom** elektroničke pošte ili porukom preko sustava za trenutno poručivanje korisnika se pokušava namamiti **na lažnu web stranicu**, kako bi na njoj upisao svoje korisničko ime i zaporku, PIN, broj kreditne kartice i sl.
- ◆ Npr. “*Radi provjere da Vaš račun nije neovlašteno korišten, molimo kliknite na poveznicu dolje i potvrdite svoj identitet*”
- ◆ lažne Web stranice banaka ili *online* trgovina koje vizualno izgledaju identično stvarnim stranicama
- ◆ U trenutku kada se korisnik prijavi na sustav, u pozadini ga skripta može automatski prijaviti na pravu stranicu banke, dok još vrijedi generirani OTP (one-time password). Nakon toga skripta, skriveno od korisnika, započinje prijenos novca...

Sigurnost kartičnog poslovanja

Trustwave - Global Security Report



www.trustwave.com

- ◆ **Trustwave SpiderLabs** – istrage diljem svijeta
- ◆ Istraga se pokreće na temelju sumnje da je izvršen neovlašteni upad u informacijski sustav
- ◆ Cilj: ustanoviti kako se napad dogodio i kolika je šteta
- ◆ U većini slučajeva napad je potvrđen i došlo je do krađe osjetljivih podataka

Trustwave - Global Security Report



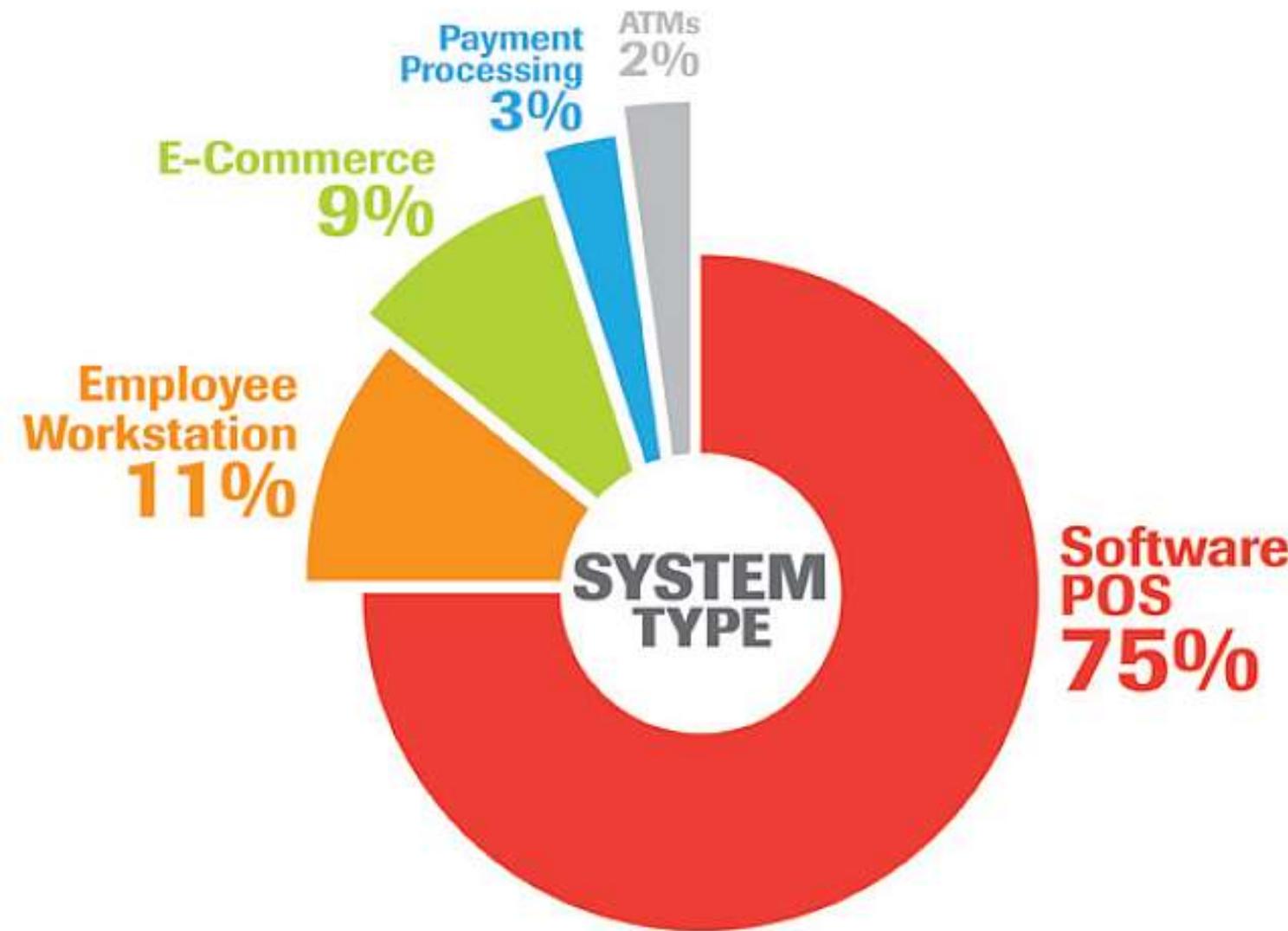
- ◆ U većini incidenata cilj su bili podaci vezani za kartično poslovanje
 - ◆ Napomena: jedan od razloga je i to što je SpiderLabs jedan od rijetkih timova koje su najveći kartičari ovlastili da provodi **istrage vezane za napade na podatke o karticama**

Trustwave - Global Security Report 2011

- ◆ 2011. godine programski sustavi za **prodajna mjesta (POS - point-of-sale)** – najčešće mjesto napada - iz POS sustava najlakše doći do podataka
 - ◆ ranjivost: **kartice s magnetskom trakom**
- ◆ **Payment Application Data Security Standard (PA-DSS)** – nalaže da programska podrška POS sustava mora proći striktno definiran skup sigurnosnih provjera - te provjere rijetko se u potpunosti provode.
- ◆ Istrage otkrile probleme već kod osnovnih sigurnosnih provjera, npr. korištenje *default* lozinke.
- ◆ Malim tvrtkama često informatičke tvrtke koje nemaju dovoljno znanja i vještina što se tiče sigurnosti sustava, uvedu i održavaju sustav za POS.



Trustwave - Global Security Report 2011

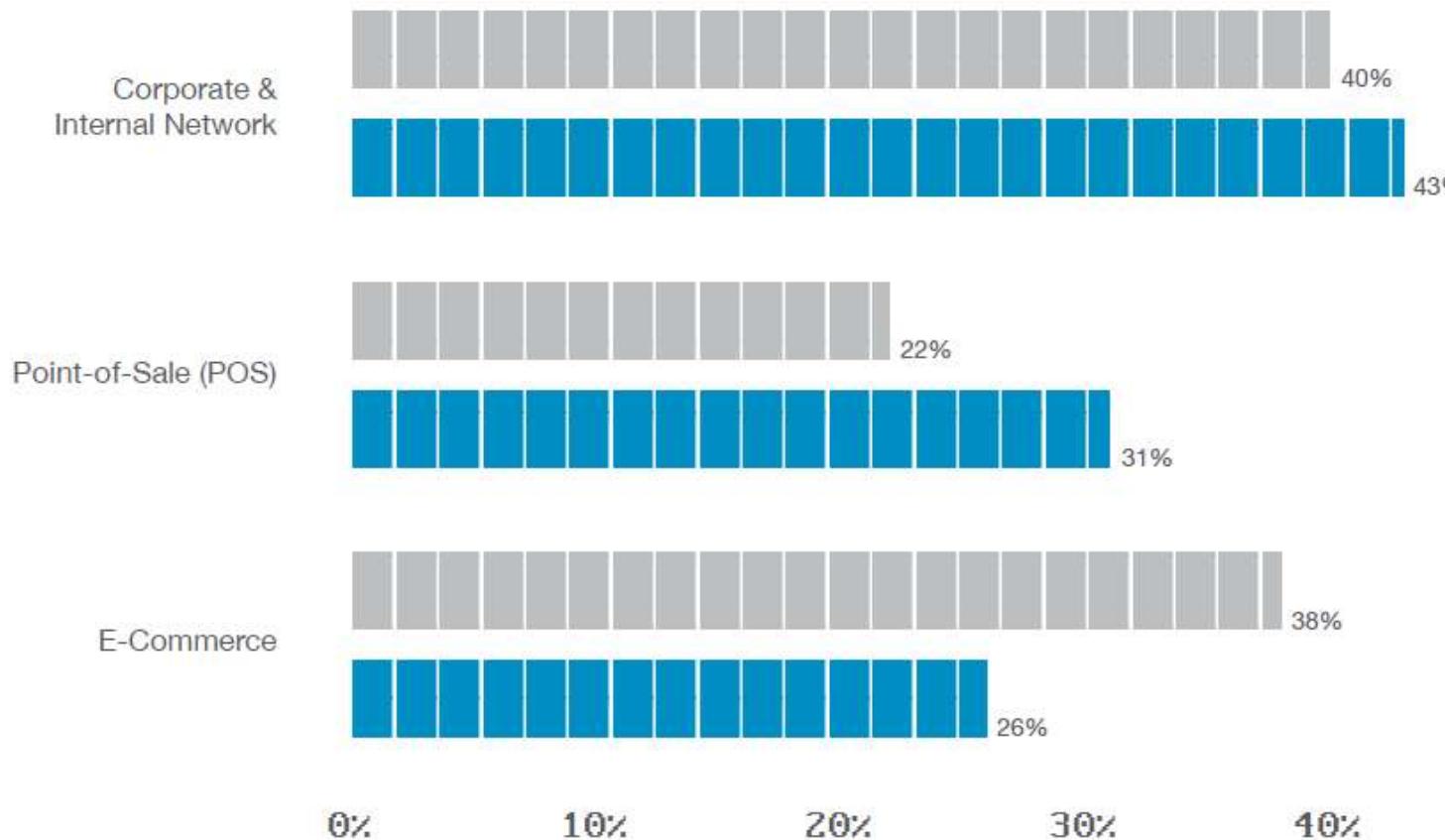


izvor:
Trustwave
Global Security Report
2011

Trustwave - Global Security Report 2017

izvor:
Trustwave
Global Security Report
2017

COMPROMISES BY ENVIRONMENT

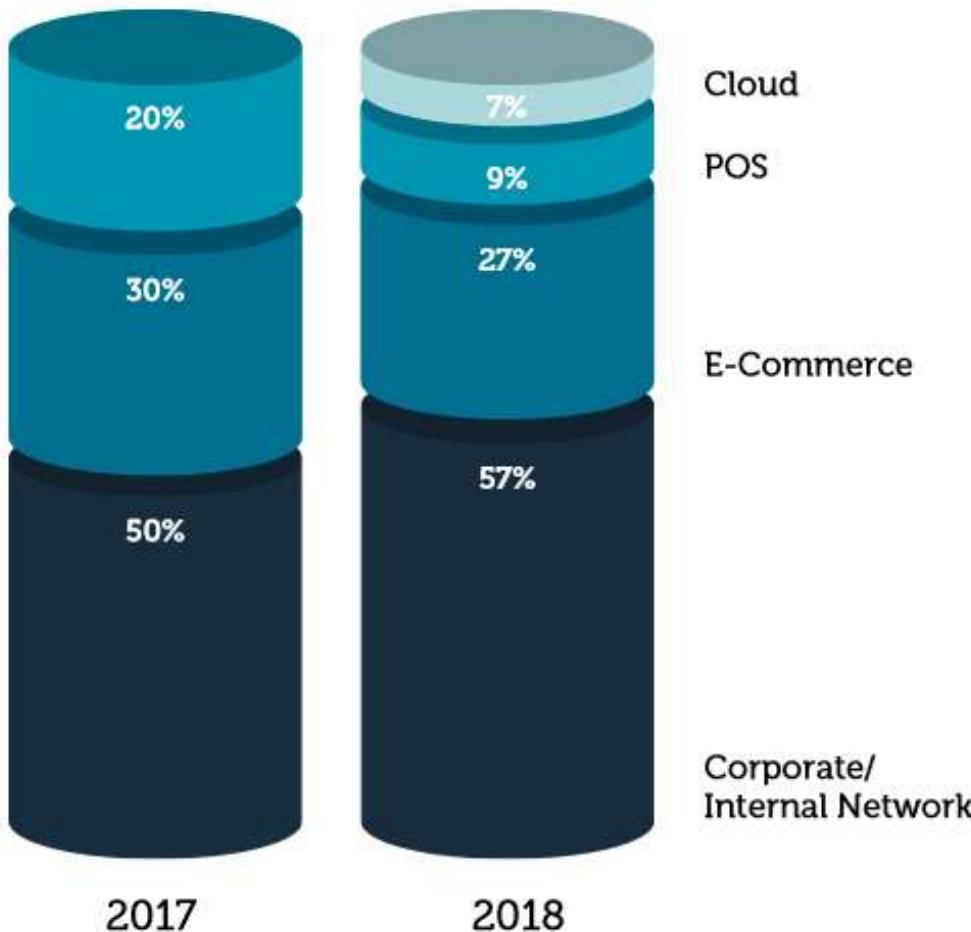


2015
2016

Trustwave - Global Security Report 2017

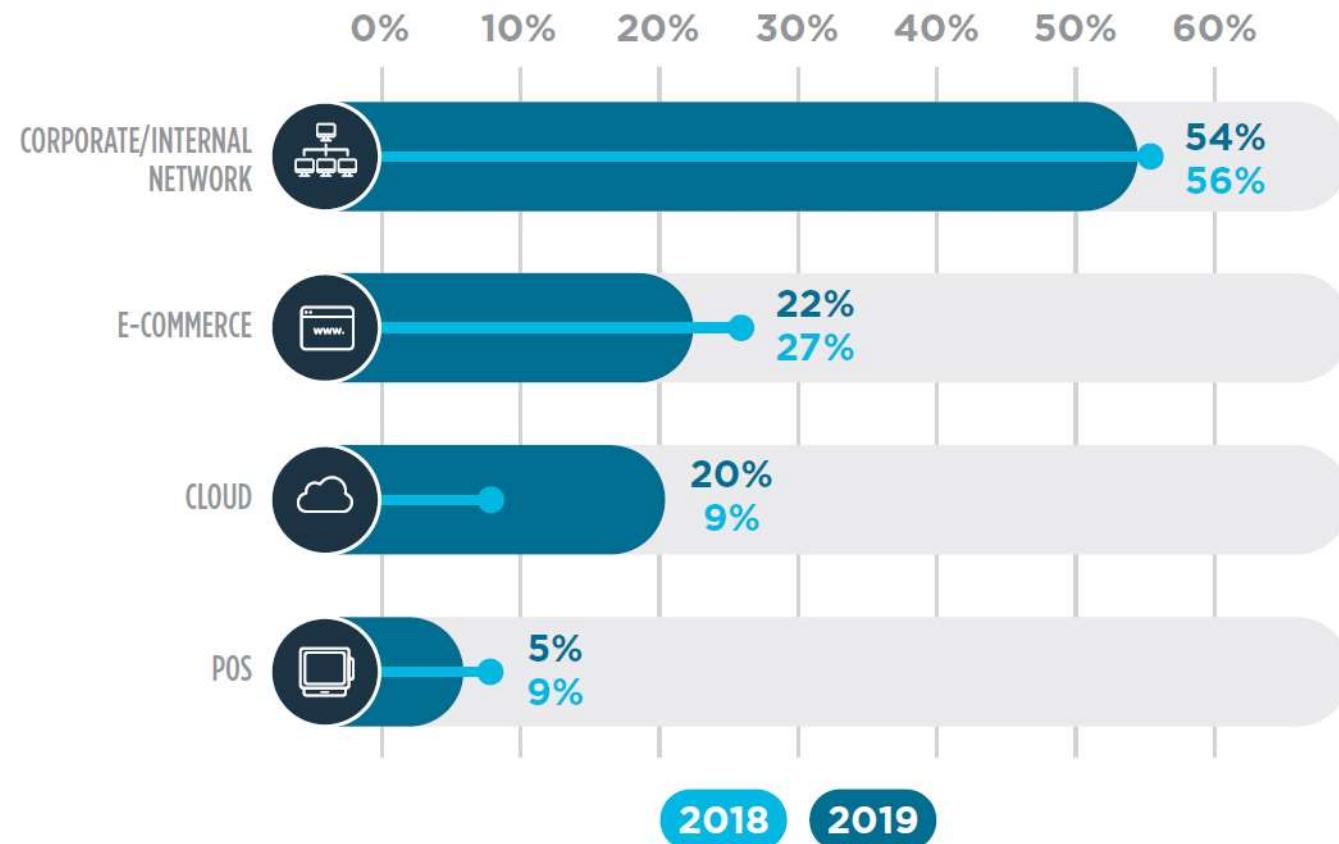
- ◆ Manje napada u e-trgovini u 2016. u odnosu na 2015.
 - ◆ Implementacija sigurnije infrastrukture
 - ◆ U nekim slučajevima banke diktiraju promjene u području sigurnosti

Trustwave - Global Security Report 2019

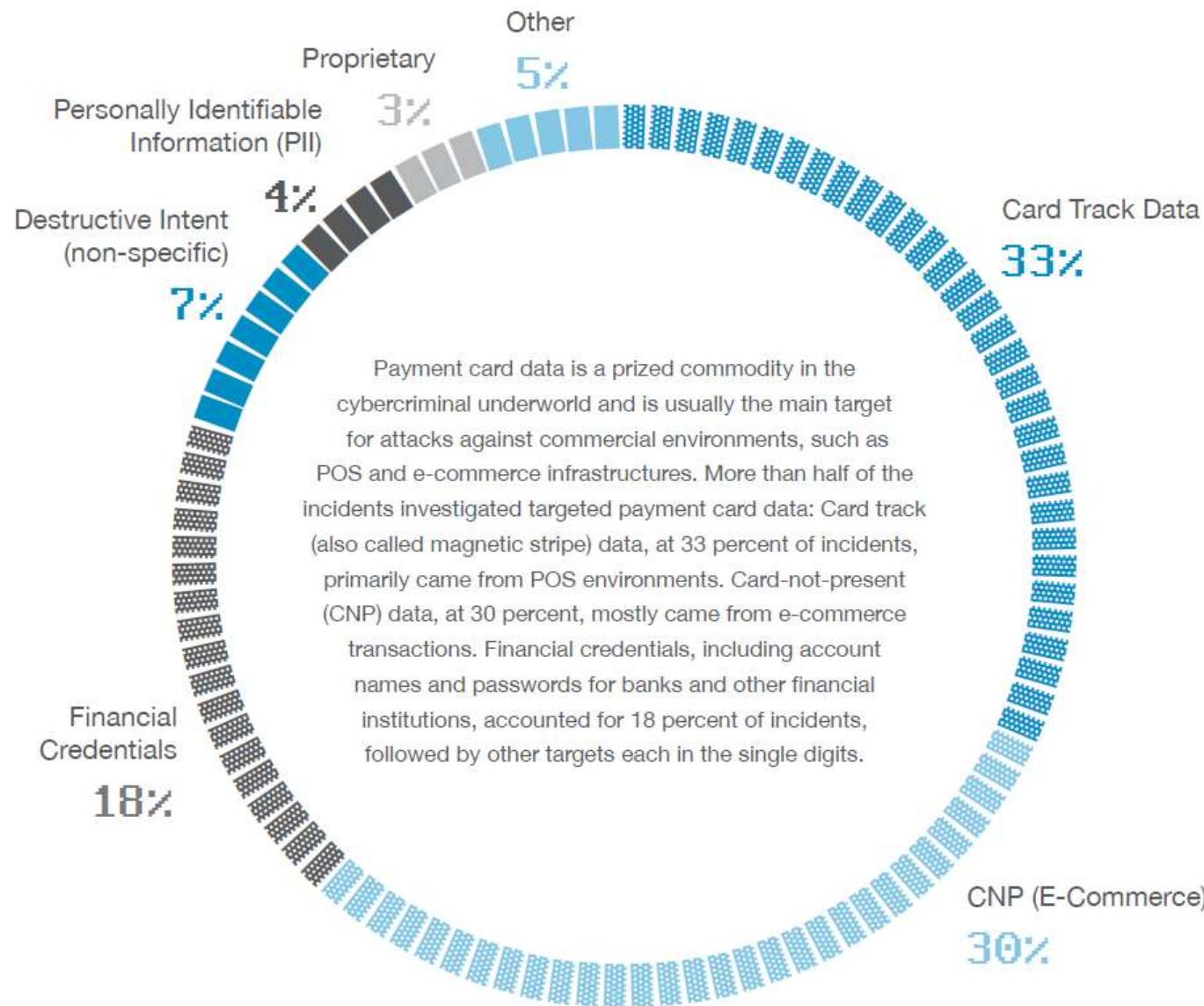


Trustwave - Global Security Report 2020

COMPROMISES BY ENVIRONMENT



Trustwave - Global Security Report 2017

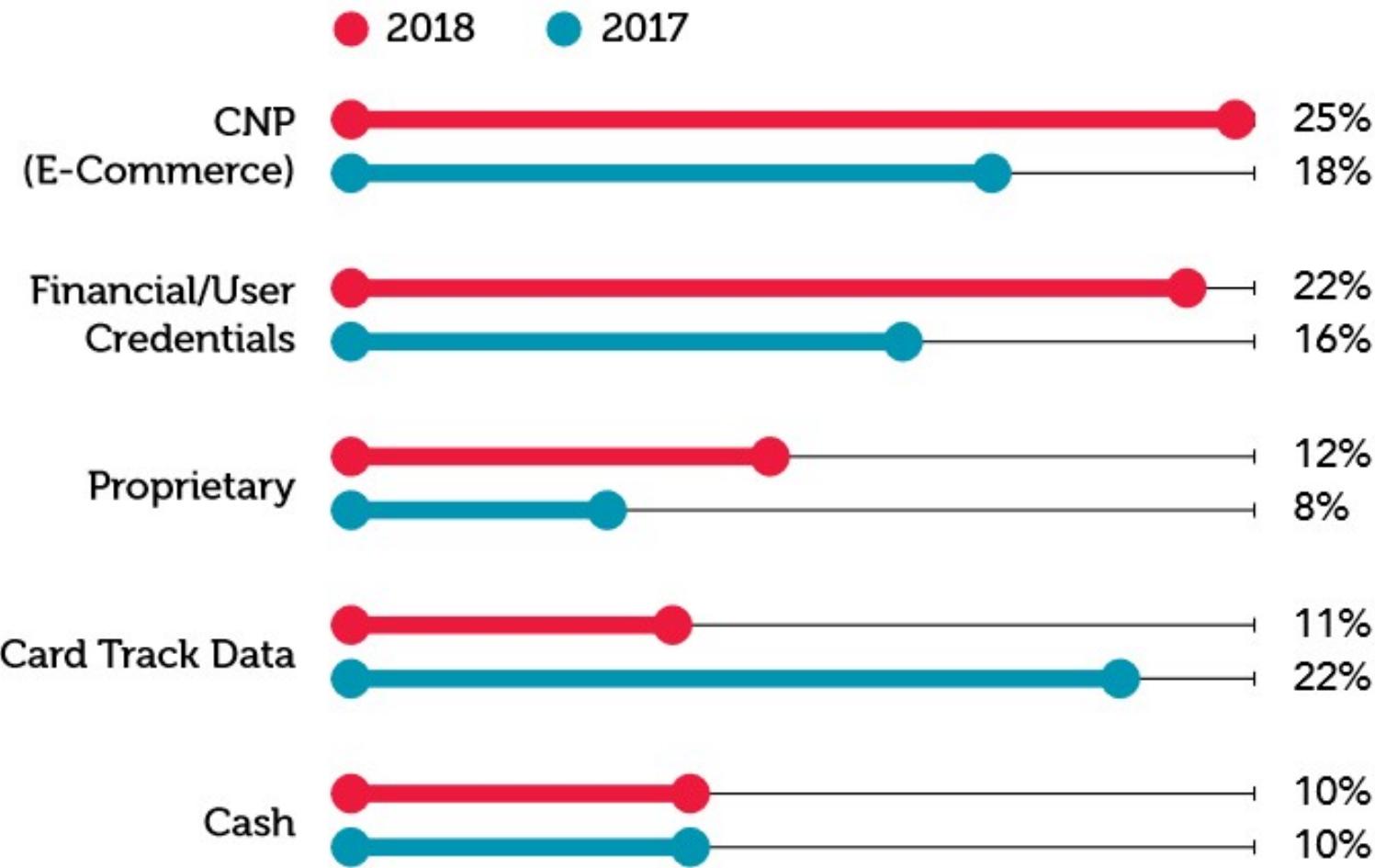


izvor:
Trustwave
Global Security Report
2017

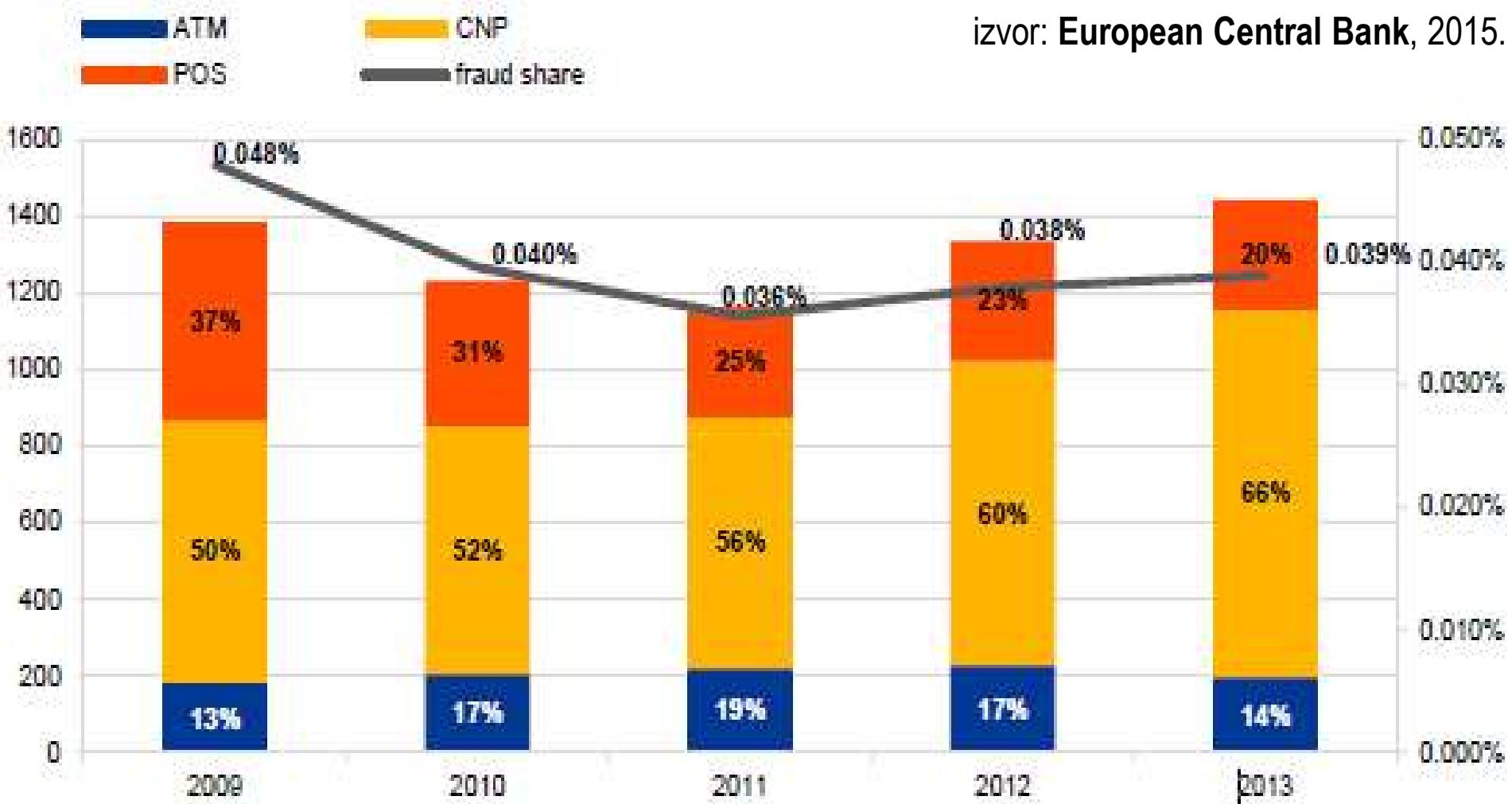
Card track
- magnetske trake

CNP = Card not
present
(e-trgovina)

Trustwave - Global Security Report 2019

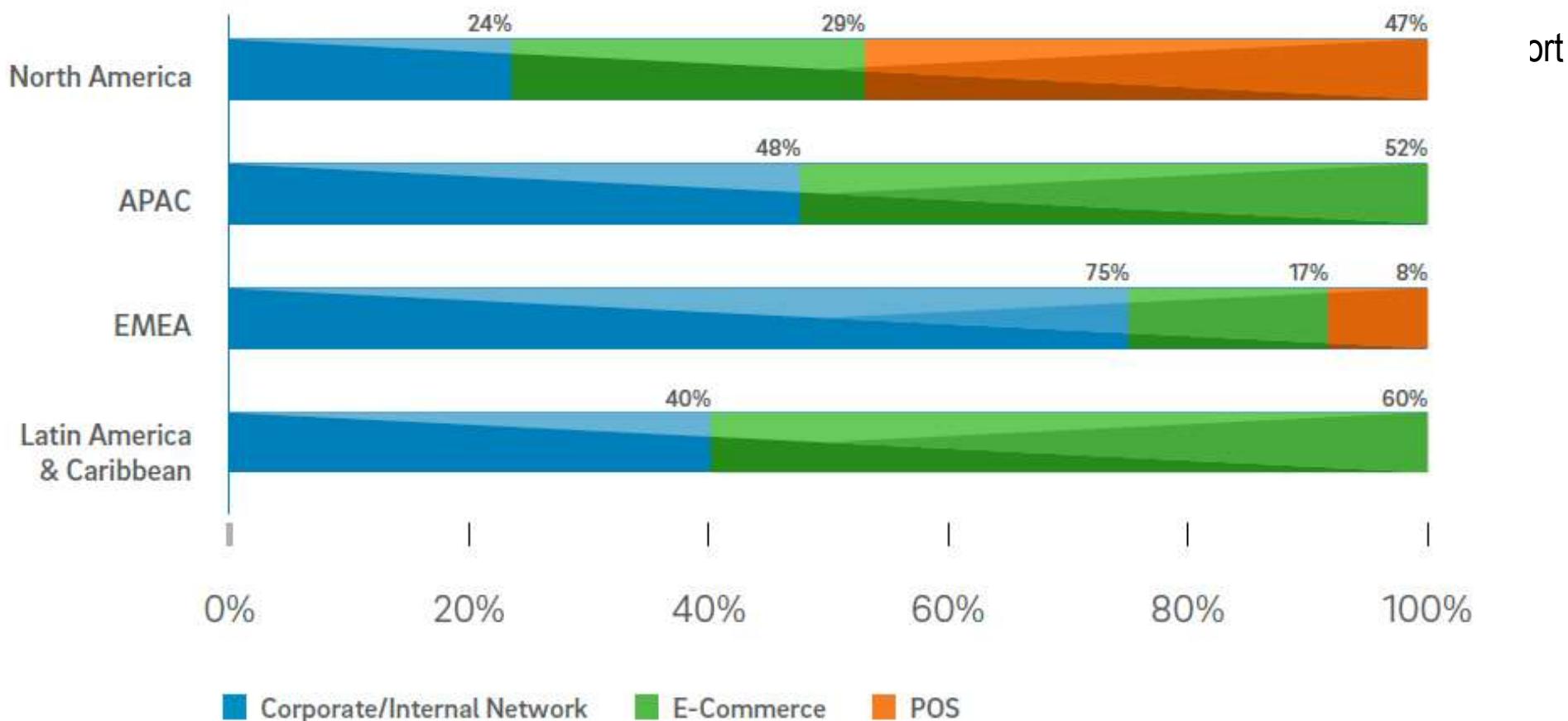


Distribucija kartične prijevare u milijunima eura



Trustwave - Global Security Report 2016

ENVIRONMENTS COMPROMISED BY REGION

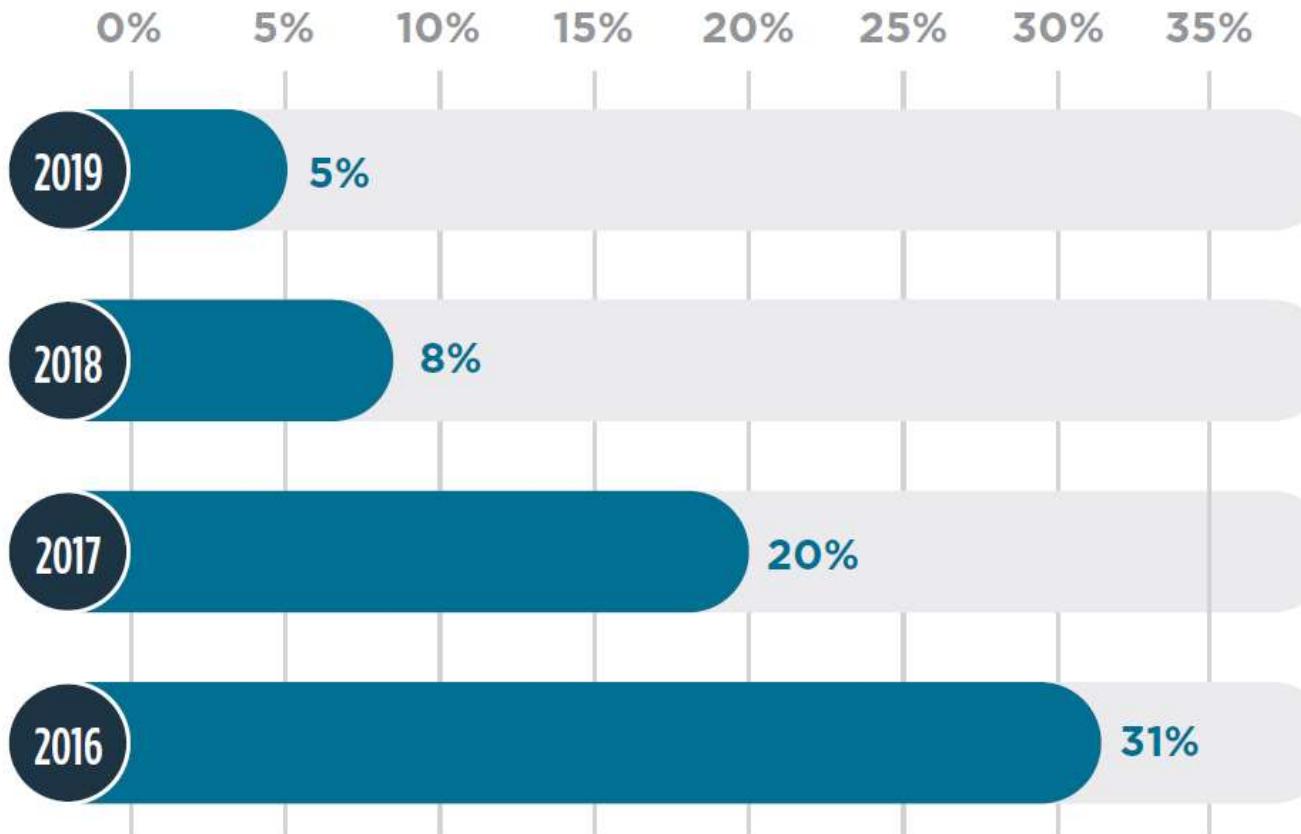


Trustwave - Global Security Report 2016

- ◆ SAD je kasnio u primjeni norme **EMV** (koja se često naziva **chip-and-PIN**)
- ◆ Zbog toga je u SAD broj napada na blagajnama (POS Point-Of-Sale), koji se odnose na korištenje kartica s magnetskim trakama prilično velik.
- ◆ U listopadu 2015. bio je rok u SAD za instalaciju opreme koja je EMV-kompatibilna

Trustwave - Global Security Report 2020

POS COMPROMISES BY YEAR



EMV

EMV = Europay, MasterCard and Visa

- globalno prihvaćeni protokol za pametne kartice (engl. *smart cards*) koje se koriste za plaćanja
- **definira interakciju između pametne kartice i uređaja za obradu kartica** za financijske transakcije na fizičkoj, podatkovnoj i aplikacijskoj razini.
- Donesene su i specifikacije za beskontaktno plaćanje.

Ciljevi:

- prihvatanje pametnih kreditnih i debitnih kartica diljem svijeta
- **sigurnost i konzistentnost platnih transakcija na mjestu prodaje**
- definiranje minimuma funkcionalnosti koji je potreban za internacionalnu interoperabilnost

- Svaki izdavač može postaviti vlastita pravila koja se odnose na:
 - Sigurnost
 - Upravljanje rizikom
 - Implementaciju
- Svaki prihvativelj kartica također može postaviti svoja pravila
- Norma EMV opisana je u 4 knjige:

Knjiga	U upotrebi od:	Verzija	Opis
Knjiga 1	Lipanj 2008.	4.2	Sučelje između integriranog čipa i terminala neovisno o aplikaciji
Knjiga 2	Lipanj 2008.	4.2	Sigurnost i upravljanje ključevima
Knjiga 3	Lipanj 2008.	4.2	Specifikacija aplikacije
Knjiga 4	Lipanj 2008.	4.2	Zahtjevi za sučelje prihvativelja, posjednika kartice i rukovatelja terminalom

- ◆ kupac autorizira transakciju kreditnom ili debitnom karticom **umetanjem kartice i unosom PIN-a** u POS terminal
- ◆ **verifikacija PIN-a** obično se provodi **u čipu** pametne kartice, koji se autentificira na terminalu digitalnim certifikatom.
 - PIN se šalje kartici koja ga uspoređuje sa pohranjenim PIN-om
 - Ako se podudaraju, **kartica vraća 0x9000**, a ako to ne prođe kartica vraća 0x63C x, gdje je x broj preostalih pokušaja unosa PIN-a do zaključavanja kartice.
- ◆ detalji transakcije također se autentificiraju kriptografskim kodom za ovjeru poruke **MAC** (*Message Authentication Code*), primjenom simetričnog ključa koji se dijeli između kartice i banke koja je izdala karticu (izdavatelj)

EMV naredbe

- ◆ Naredbe koje **terminal** šalje kartici:
 - vanjska autentikacija
 - generiranje aplikacijskog kriptograma
 - dohvati podataka
 - dohvati opciju obrade
 - interna autentikacija
 - čitanje zapisa
 - odabir aplikacije ili datoteke
 - potvrda (usporedba PIN-a)

- ◆ Naredbe koje **izdavač** šalje kartici:
 - blokiranje aplikacije
 - odblokiranje aplikacije
 - blokiranje kartice
 - promjena/deblokiranje PIN-a

EMV faze

EMV protokol može se podijeliti u **tri faze**:

- ◆ **Autentifikacija kartice**
 - Osigurava terminalu podatke o banci koja je izdala karticu i to da podaci na kartici nisu mijenjani
- ◆ **Provjera vlasnika kartice**
 - Usporedba upisanog PIN-a i onog na kartici
- ◆ **Autorizacija transakcije**
 - Uvjerava terminal da je banka izdavatelj kartice autorizirala transakciju

Beskontaktno plaćanje - NFC tehnologija

- posljednjih godina NFC tehnologija (eng. Near Field Communication) se koristi za beskontaktno plaćanje kreditnom karticom ili mobilnim uređajem
 - kratkodometna bežična tehnologija

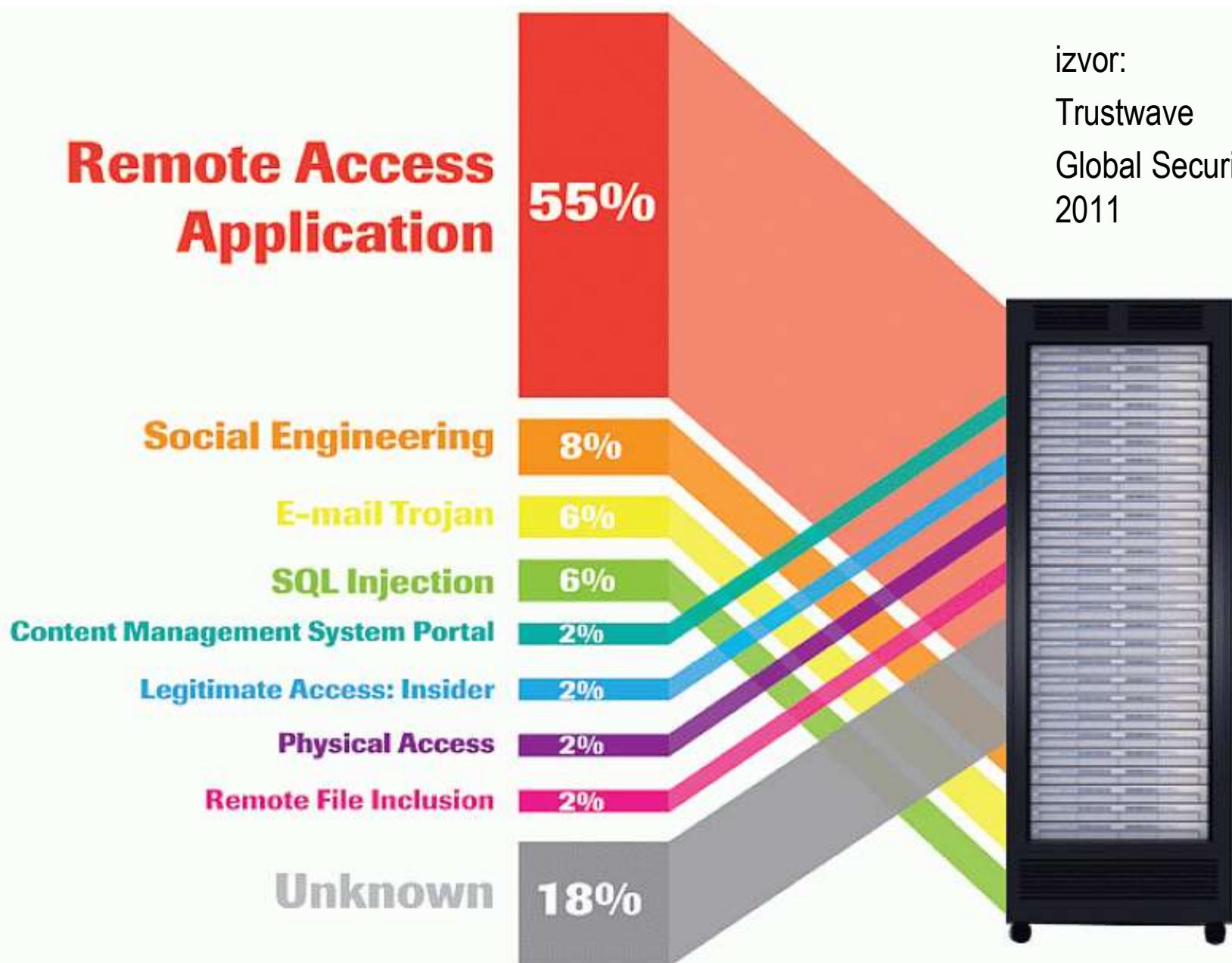


- postoji skup specifikacija EMV Contactless:
<https://www.emvco.com/emv-technologies/contactless/>

Trustwave - Global Security Report 2011

- ◆ Metode napada
- ◆ 2011. godine u većini slučajeva napadač je koristio **dostupnu aplikaciju za daljinski pristup** (remote access application). Ako su se pri tome u sustavu još koristile **default lozinke** koje je dao proizvođač, izvedba napada je trivijalna.
- ◆ Primjer: mala tvrtka ni ne zna da je aplikacija za daljinski pristup na Internetu, a informatička tvrtka koja je instalirala sustav koristi aplikaciju za njegovo održavanje.

Metode napada



izvor:

Trustwave

Global Security Report
2011

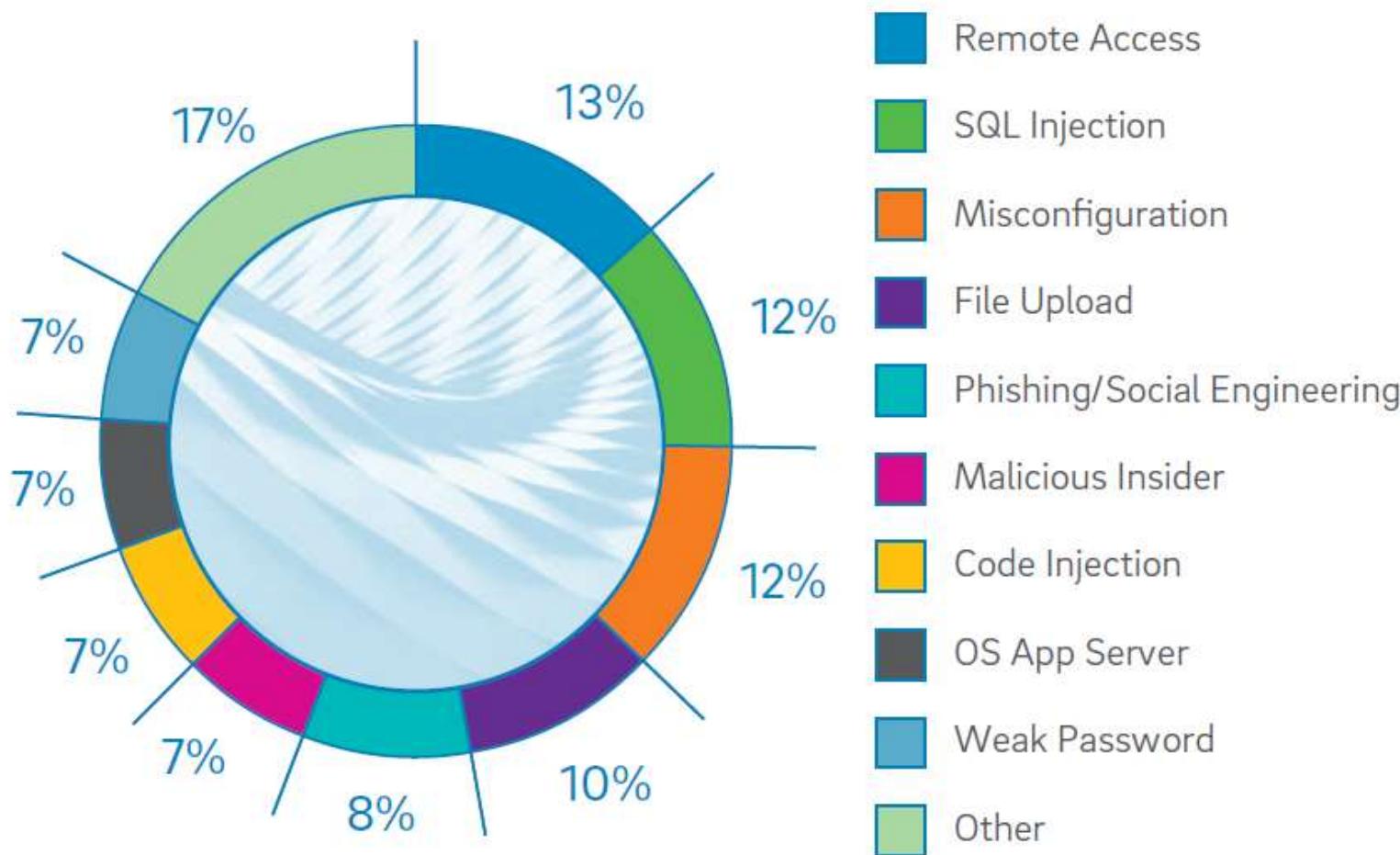
Trustwave - Global Security Report 2011

Metode napada:

- ◆ Društveni inženjering – različite metode
- ◆ Napadač se preko telefona predstavlja kao da je iz IT tvrtke koja održava sustav i uvjeri zaposlenika da instalira aplikaciju za daljinski pristup na ciljanom sustavu
- ◆ E-mailovi s malicioznim PDF dokumentima
- ◆ Umetanje SQL-a (SQL injection) – najpopularnija metoda upada za Web-aplikacije
 - ◆ referenca -The Open Web Application Security Project (OWASP) :
http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

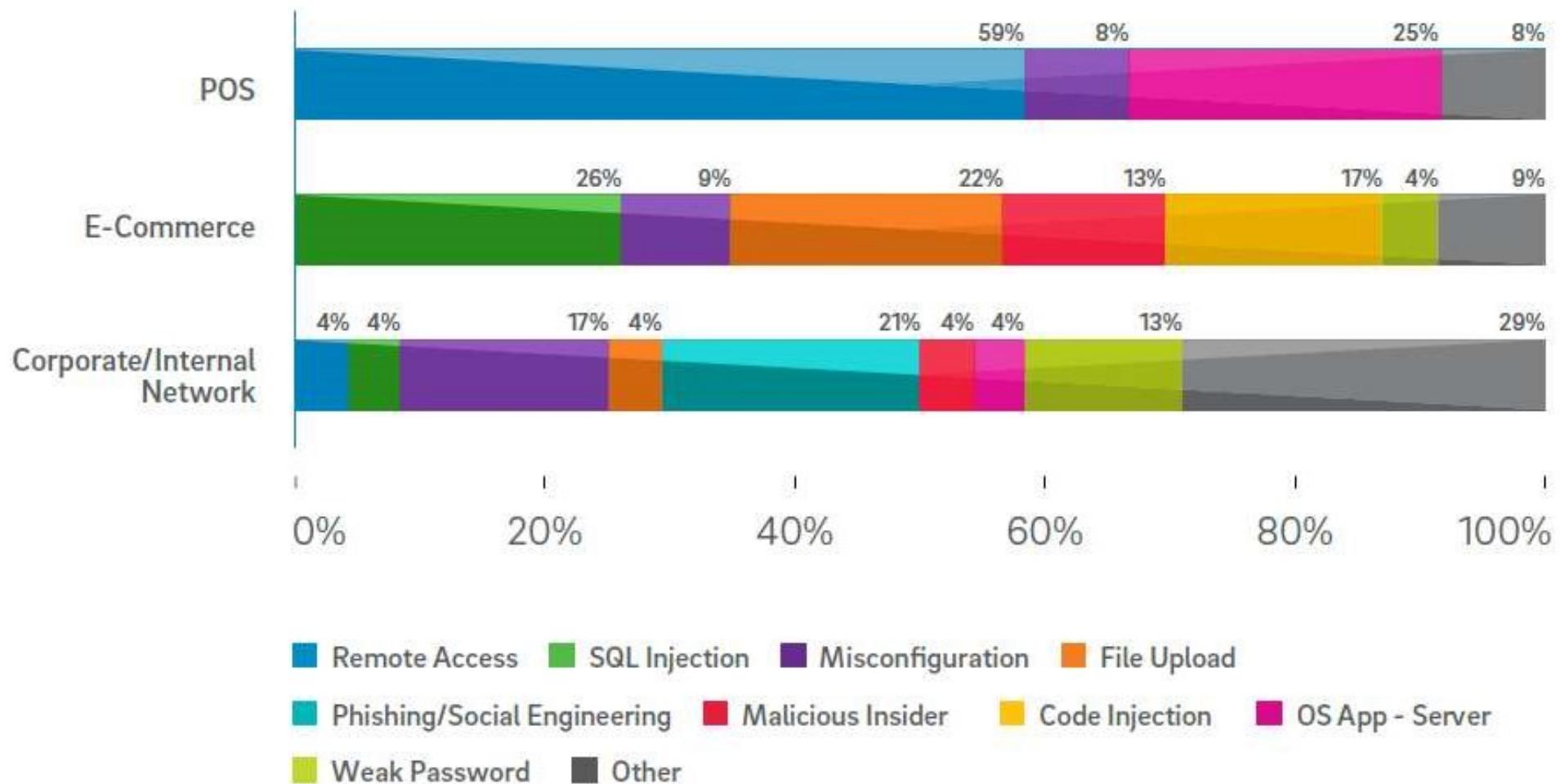
Trustwave - Global Security Report 2016

FACTORS CONTRIBUTING TO COMPROMISE



izvor:
Trustwave
Global
Security
Report 2016

Trustwave - Global Security Report 2016



Neispunjavanje zahtjeva PCI DSS



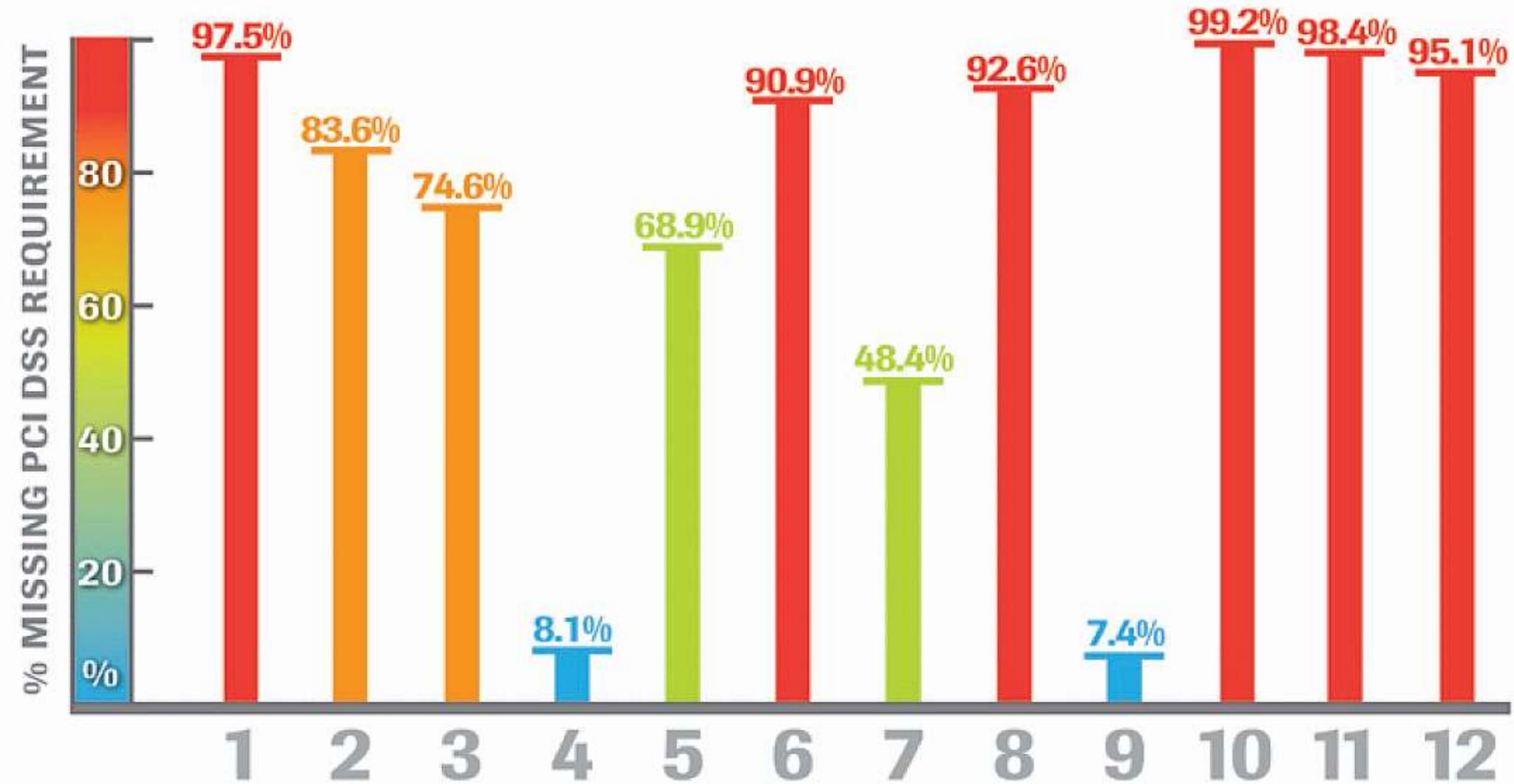
- ◆ U većini napada evidentiranih u **Global Security Report 2011**, kojima su cilj bili podaci o karticama, u sustavima koji su napadnuti nisu bili zadovoljeni svi zahtjevi koje propisuje PCI DSS.
- ◆ Mnoge napadnute tvrtke su vjerovale da su kupile sustav koji zadovoljava **PCI DSS** zahtjeve. Nažalost, prodavači sustava znaju tvrditi da sustav zadovoljava sve zahtjeve, a to se pokaže neistinitim ili **se sustavi ne konfiguriraju i ne održavaju na ispravan način**.
- ◆ 2011. godine napadnute organizacije u 97.5% slučajeva **nisu imale dobro konfiguiriran vatrozid** koji će u potpunosti zaštititi proces plaćanja. Od tih organizacija, **84% nije uopće imalo vatrozid**.

Zahtjevi PCI DSS

- ◆ **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 podatci o vlasniku kartice moraju se štititi šifriranjem (enkripcijom).**
- ◆ **Zahtjev 5: Nužno je koristiti i redovito osvježavati (ažurirati) softver za zaštitu od zlonamjernog koda, odnosno antivirusni softver**
- ◆ **Zahtjev 6: Razvijati i održavati sigurne sustave i aplikacije**

PCI DSS – neispunjavanje zahtjeva

izvor: Trustwave 2011



Zahtjevi PCI DSS

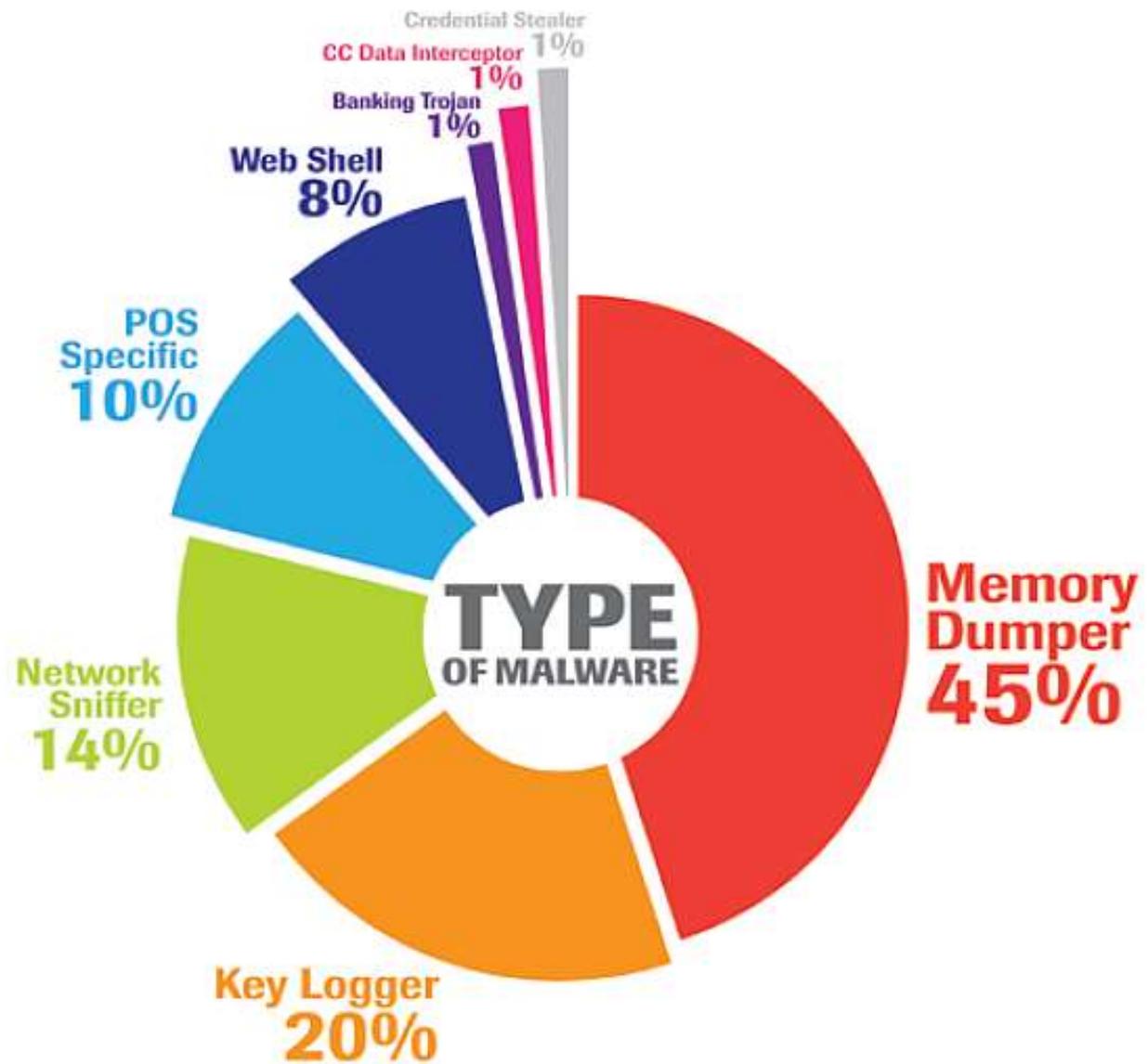
- ◆ **Zahtjev 7: Pristup podatcima o vlasniku kartice nužno je ograničiti na minimum onoga što se o njemu u konkretnoj transakciji treba znati.**
- ◆ **Zahtjev 8: Svakoj osobi koja ima pristupa računalnom sustavu treba pridijeliti jedinstvenu identifikaciju (ID).**
- ◆ **Zahtjev 9: Maksimalno ograničiti fizički pristup podatcima o vlasniku kartice.**
- ◆ **Zahtjev 10: Pratiti i nadzirati svaki pristup mrežnim resursima i podatcima o vlasniku kartice.**
- ◆ **Zahtjev 11: Redovito provjeravati sigurnost sustava i procesa.**
- ◆ **Zahtjev 12: Razviti i održavati odgovarajuću politiku informacijske sigurnosti.**

Neovlašteno izvlačenje podataka



- ◆ **Zlonamjerni programi** često izvlače podatke koristeći “normalne” legitimne operacije slične onima koje bi i informatičarsko osoblje koristilo.
- ◆ Primjer: ***sniffing*** – to isto rade administratori koji žele razumjeti što se događa u lokalnoj mreži.
 - Napadači koriste *sniffing* za **presretanje podataka** na putu od POS (point-of-sale) terminala do poslužitelja za obradu podataka.
- ◆ Primjer: ***memory dumping*** – **snimanje stanja radne memorije**, obično se legitimno obavlja kad se neki program sruši da bi administrator mogao analizirati uzrok rušenja programa
 - Ako zlonamjerni program radi snimanje stanja radne memorije, **antivirusni program ga ne može na jednostavan način detektirati**

Trustwave - Global Security Report 2011



izvor:
Trustwave
Global Security Report
2011

Neovlašteno izvlačenje
podataka

Primjer: Heartland Payment Systems 2008.

- ◆ **Heartland Payment Systems**
 - tvrtka za obradu plaćanja, šesta po veličini u SAD
 - obrađuje 100 milijuna transakcija mjesечно
 - pokriva 250 000 trgovaca
- ◆ Sustavi za obradu kartičnog poslovanja napadnuti 2008. godine
 - Najveća krađa podataka o karticama u povijesti
 - 130 milijuna kreditnih i debitnih kartica
 - Heartland prijavio da je izgubio 12.6 milijuna dolara

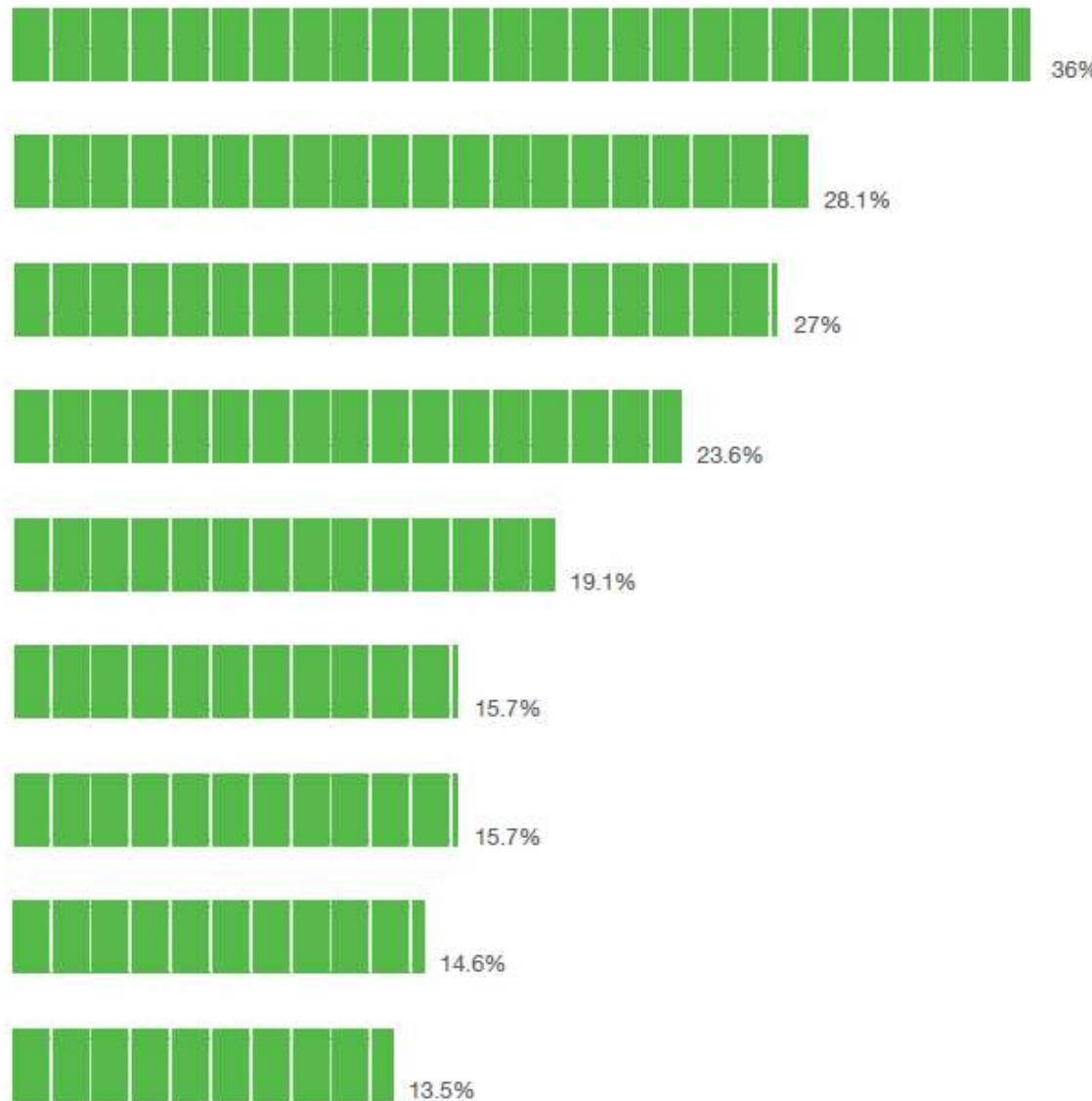
Primjer: Heartland Payment Systems 2008.

- ◆ Napadači uspjeli ubaciti ***key logging*** program kroz vatrozid
- ◆ ***sniffing*** - nadgledali su mrežni promet, hvatali podatke o karticama
- ◆ Podaci su uključivali informacije upisane u **magnetske trake** na karticama. S tim podacima, **napadači su mogli upisati ukradene informacije u nove kartice.**
- ◆ Jedan od napadača uhvaćen je i osuđen je na 20 godina zatvora.
- ◆ U svibnju 2009. godine objavljeno je da je Heartland Payment Systems certificiran da radi u skladu s PCI DSS normom.

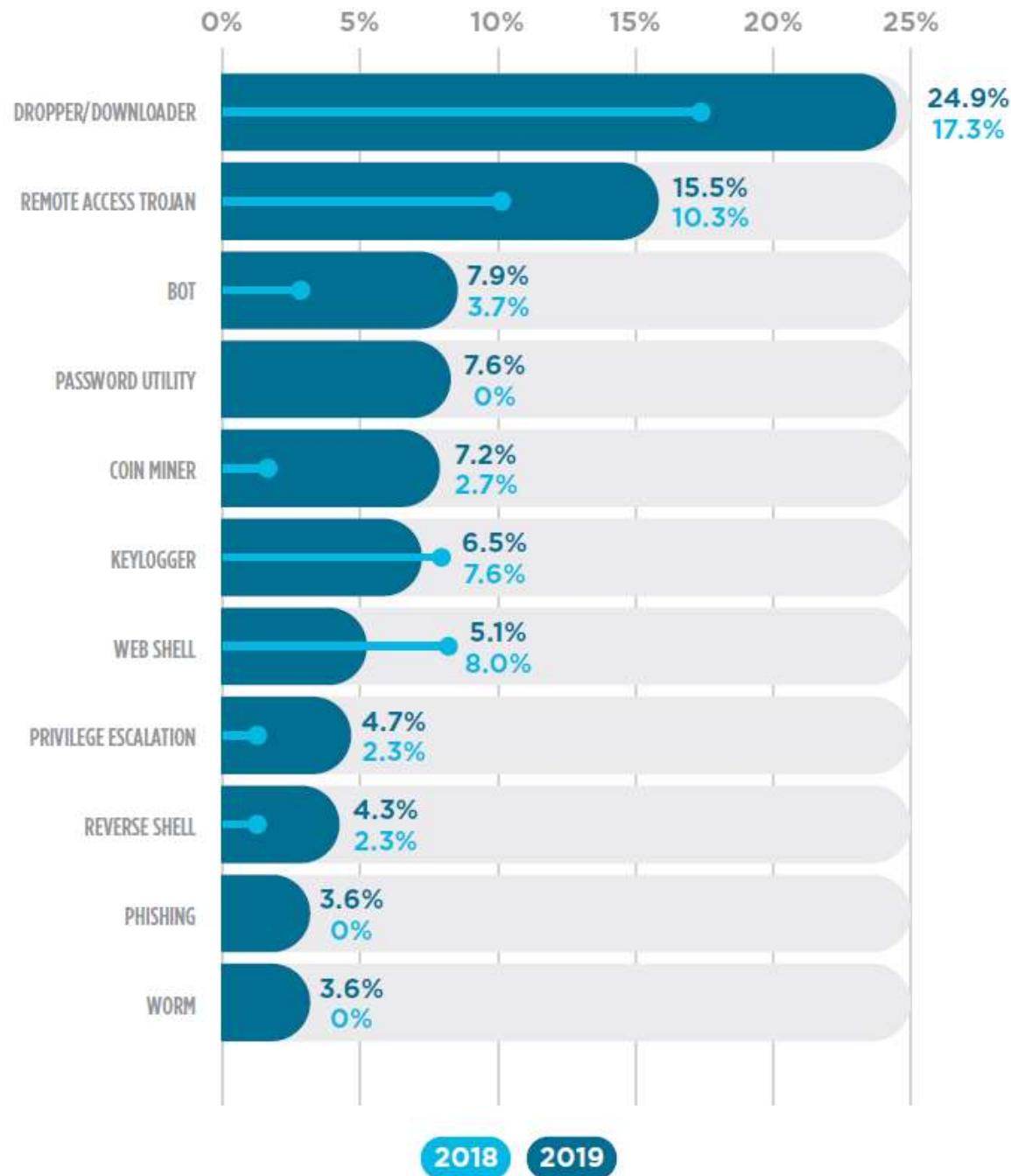
Trustwave - Global Security Report 2017

izvor:
Trustwave
Global
Security
Report 2017

TOP FEATURES OF MALWARE ENCOUNTERED DURING INVESTIGATIONS



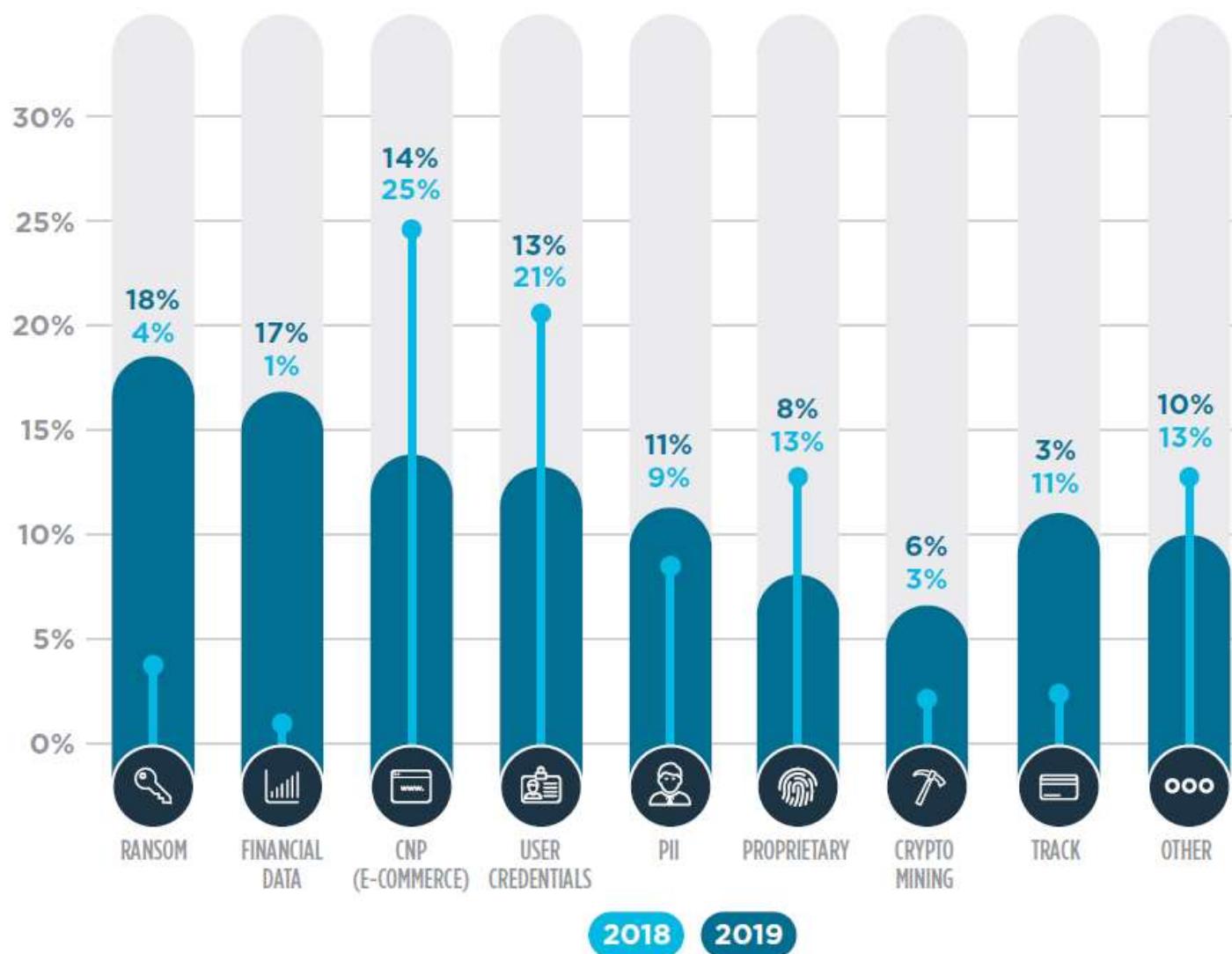
TYPES OF MALWARE ENCOUNTERED DURING INVESTIGATIONS



izvor:
Trustwave
Global
Security
Report 2020

Trustwave - Global Security Report 2020

COMPROMISES BY TYPE OF DATA TARGETED



izvor:
Trustwave
Global
Security
Report 2020

Neovlašteno izvlačenje podataka



- ◆ Kako se sve više pazi na zahtjeve određene sigurnosnim normama (PCI DSS, PA-DSS, OWASP...), poboljšala se situacija što se tiče **pohrane** podataka na siguran način.
 - Arhivirani podaci su **manje dostupni** napadačima nego ranije.
- ◆ **Fokus** je sve više na **neovlaštenom izvlačenju podataka** pri njihovom **prijenosu**.
- ◆ Podaci o karticama vrijede samo u određenom vremenskom periodu (kartica vrijedi do određenog datuma).
 - Kad se **pri prijenosu** podataka izvlače podaci, za očekivati je da se radi o **vrijedećim** karticama
 - kod arhiviranih podataka to ne mora biti slučaj - tada je potrebno provjeravati vrijede li još uvijek brojevi kartica.

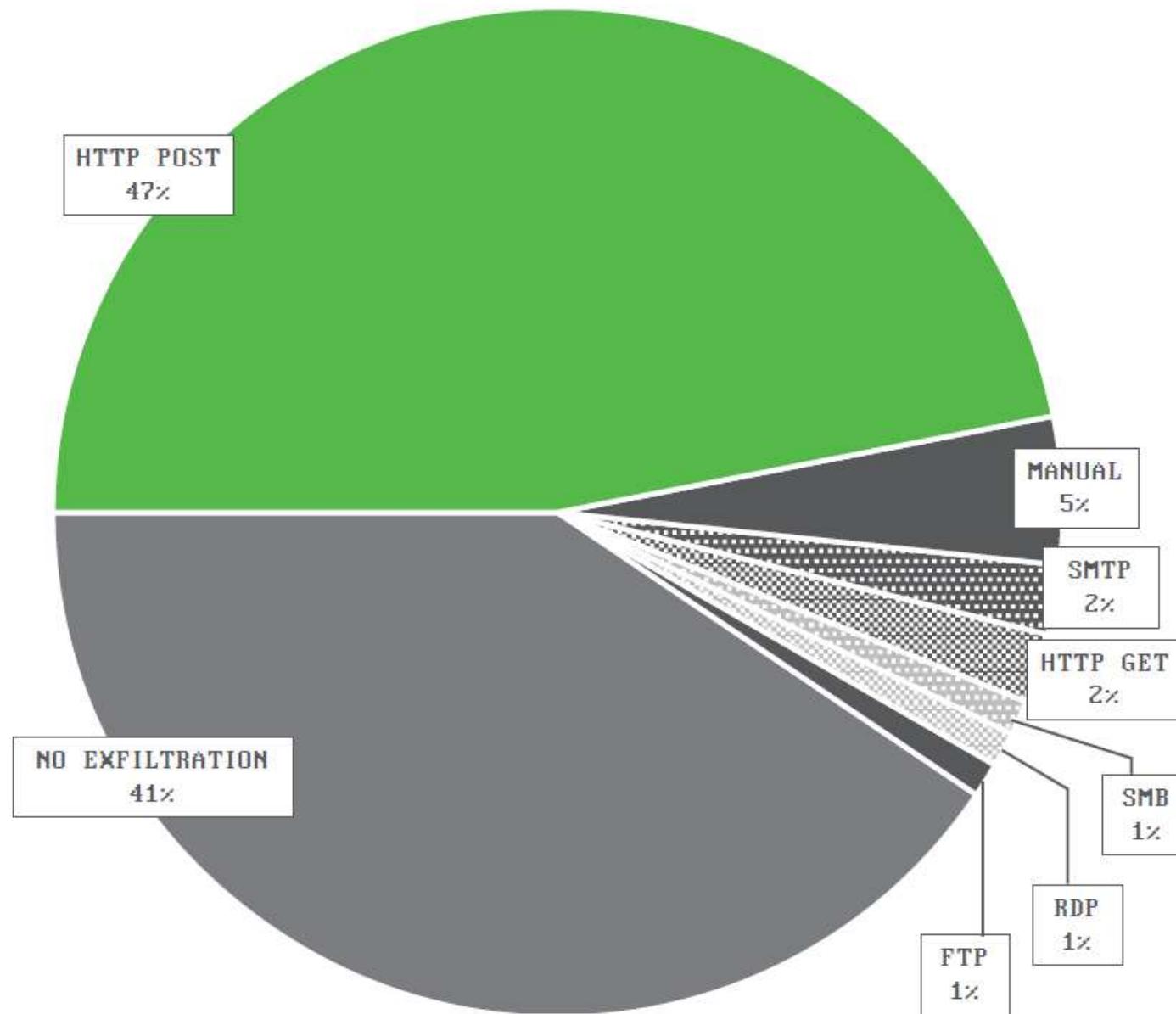
Neovlašteno izvlačenje podataka



- ◆ Datoteka u koju zlonamjerni program pohrani izvučene podatke se obično šalje koristeći **HTTP**.
- ◆ Preporučuje se:
 - napraviti **restrikciju toka informacija iz lokalne mreže** prema Internetu - *network egress filtering*
 - TCP/IP paketi koji se šalju iz lokalne mreže se **ispituju na usmjeritelju (router) ili vatrozidu**. Paketima koji ne zadovoljavaju sigurnosne zahtjeve ne dopušta se da napuste mrežu.
 - implementirati sustave **DLP (Data Loss Prevention)**.

MALWARE EXFILTRATION

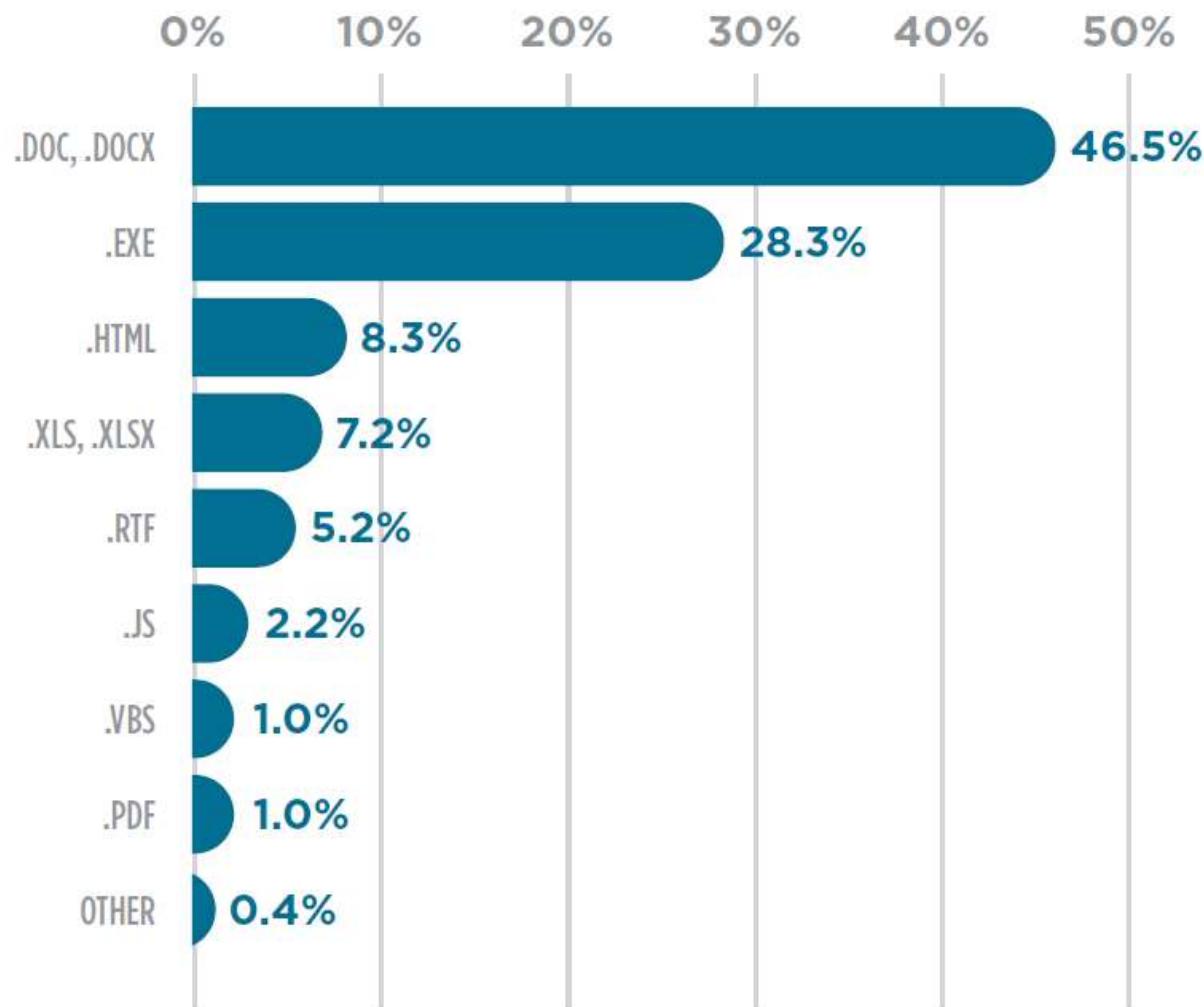
METHODS OF EXFILTRATION



izvor:
Trustwave
Global Security Report
2017

Trustwave - Global Security Report 2020

EMAILED MALWARE FILE TYPES, 2019



izvor:
Trustwave
Global Security Report
2020



Zaštita i sigurnost informacijskih sustava

Revizija sigurnosti informacijskih sustava

prof. dr. sc. Boris Vrdoljak

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

Zaštićeno licencijom <http://creativecommons.org/licenses/by-nc-sa/2.5/hr/>



Creative Commons



□ slobodno smijete:

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo

□ pod sljedećim uvjetima:

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencem koja je ista ili slična ovoj.

U slučaju daljnog korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu.

Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava.

Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s <http://creativecommons.org/>.

- ◆ Pojedinu zaštitu koju primjenjujemo kako bismo postigli sigurnost nazivamo **kontrola** (engl. *control*)
- ◆ Sve kontrole su razvrstane u tri velike grupe:
 - Fizičke kontrole
 - Kamere, zaštitari, blindirana vrata, ...
 - Tehničke kontrole
 - Kriptografija, vatrozidi, sustavi za detekciju napada, ...
 - Administrativne kontrole
 - Politike, pravilnici, itd.
 - Različiti propisi kojima definiramo što znači biti siguran, kako se ljudi moraju ponašati, kako uređaji moraju biti podešeni, ...

Revizija sigurnosti informacijskih sustava

- ◆ Dobro oblikovanim i provedenim kontrolama smanjuje se ranjivost sustava, odnosno rizik da će zlonamjerni napadači ili neki prirodni izvor sigurnosne prijetnje prouzročiti štetu.
- ◆ **Revizijom sigurnosti informacijskog sustava**
 - provjerava se postoji li određene **kontrole**,
 - testira se njihova učinkovitost,
 - prikupljaju se podaci i dokazi pomoću kojih je moguće procijeniti sigurnosne **rizike**,
 - daju se upravi **preporuke** koje mjeru poduzeti kako bi se negativni učinak uočenih rizika smanjio ili uklonio.

Provjeda revizije sigurnosti informacijskih sustava

1. Određivanje **područja** revizije (Što revidirati?)
 - Određivanje ciljeva za svako područje revizije
 2. Određivanje **načina** testiranja (Koje kontrole provjeravamo? Kako provjeravamo njihovu učinkovitost?)
 3. **Provjeda** testiranja
 - Analiza dokumentacije
 - Prikupljanje revizijskih dokaza
 - Ankete, intervjuji
 - Analiza ranjivosti, analiza aktualnih sigurnosnih prijetnji
 - Tehničko testiranje sustava, probni napadi
 - Analiza revizijskih dokaza
 4. Procjena **rizika**
 5. Priprema revizijskog **izvješća** koje uključuje preporuke za poboljšanje
 6. Predstavljanje revizijskog izvješća upravi
-

Tehničke kontrole pri reviziji sigurnosti informacijskih sustava

Što se tiče tehničkih kontrola, provedba revizije uključuje:

- ◆ provjeru korisničkih računa (računi koji se već dugo ne koriste, slabe lozinke, korištenje uloga...)
- ◆ provjeru mreže (pristup izvana, otvoreni portovi...)
- ◆ zaštitu podataka pri prijenosu (šifriranje) i pri pohrani (postavke sustava za upravljanje bazama podataka, šifriranje važnih podataka)
- ◆ nadzor mrežnog prometa
- ◆ antivirusni softver (ažuriranje, korištenje)
- ◆ zaštita ključnih uređaja (npr. POS – sustavi prodajnih mjesta)
- ◆ uspostavljene procedure i odgovornosti u slučaju napada
- ◆ podizanje svijesti zaposlenika o sigurnosnim prijetnjama
- ◆ ...

Okviri upravljanja sigurnošću informacijskih sustava

Za provođenje revizije sigurnosti informacijskih sustava mogu se koristiti okviri:

- ◆ ISO/IEC **27001**
- ◆ **CobiT** (ISACA)
- ◆ **PCI DSS**
- ◆ US National Institute of Standards and Technology (**NIST**) Cybersecurity Framework
<http://www.nist.gov/cyberframework/>
- ◆ **SANS** Institute CIS Controls (ranije: Critical Security Controls)
<https://www.sans.org/blog/cis-controls-v8/>
- ◆ Uredba o zaštiti podataka - **GDPR** (General Data Protection Regulation)

ISO/IEC 27001, CobiT i PCI DSS pomažu pri odabiru područja revizije i određivanju kontrolnih ciljeva.

ISO/IEC 27001

ISO/IEC 27001 – norma za upravljanje informacijskom sigurnošću

- ◆ Zajednički su je objavili Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC)
- ◆ sadrži zahtjeve za uspostavljanje, provedbu, održavanje i kontinuirano poboljšanje **sustava upravljanja informacijskom sigurnošću (ISMS)**
- ◆ ISMS je skup politika i procedura za sustavno upravljanje osjetljivim podacima organizacije.
- ◆ ISO/IEC 27001 osigurava da se organizacija brani ne samo od rizika temeljenih na tehnologiji, već i drugih prijetnji, kao što su slabo informirani zaposlenici ili neučinkoviti postupci.

<https://www.iso.org/standard/27001>

- ◆ mogućnost dobivanja certifikata nakon revizije

ISO/IEC 27001

Norma ISO/IEC 27001 zahtijeva da menadžment:

- ◆ sustavno **ispituje rizike** informacijske sigurnosti organizacije,
- ◆ oblikuje i implementira sveobuhvatan **paket kontrola** kako bi se riješili oni rizici koji se smatraju neprihvatljivima,
- ◆ usvoji sveobuhvatni **postupak upravljanja** kako bi se osiguralo da kontrole sigurnosti i dalje udovoljavaju potrebama organizacije u pogledu informacijske sigurnosti.

Obitelj normi ISO/IEC 27000

ISO/IEC 27001 je dio obitelji normi **ISO/IEC 27000**

- ◆ ISO/IEC **27002** *Code of practice for information security management*
 - preporuča **najbolju praksu** u korištenju sigurnosnih kontrola
 - daje preporuke za upravljanje informacijskom sigurnošću za one osobe koje su odgovorne za iniciranje, implementiranje ili održavanje sigurnosti u svojim organizacijama
- ◆ ISO/IEC **27001** *Information Security Management System Specification*
 - formalan i sveobuhvatan pristup implementaciji kontrolnih struktura prema 27002

Obitelj normi ISO/IEC 27000

- ◆ ISO/IEC 27003, *Information security management system implementation guidance*
- ◆ ISO/IEC 27004, *Information security management — Measurement*
- ◆ ISO/IEC 27005, *Information security risk management*
- ◆ ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*
- ◆ ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ◆ ISO/IEC TR 27008, *Guidelines for auditors on information security controls*
- ◆ ...

ISO/IEC 27001

Normom **ISO/IEC 27001** reguliraju se sljedeća područja (1):

- 1. Politike informacijske sigurnosti**
- 2. Organizacija informacijske sigurnosti**
- 3. Upravljanje imovinom**
- 4. Sigurnost vezana za ljudske resurse**
- 5. Kriptografija**
- 6. Fizička sigurnost i zaštita od utjecaja okoline**
- 7. Sigurnost informatičkih resursa i poslovnih operacija**
 - ◆ sigurni rad uređaja za obradu informacija, zaštita od zlonamjernog koda, pričuvna pohrana,...

ISO/IEC 27001

Normom ISO/IEC 27001 reguliraju se sljedeća područja (2):

8. Sigurnost komunikacijske infrastrukture

- sigurnost računalnih mreža, zaštita podataka pri prijenosu unutar ili izvan organizacije,...

9. Kontrola pristupa

10. Razvoj i održavanje informacijskih sustava

- sigurnost u procesima razvoja i podrške, upravljanje ranjivostima...

11. Upravljanje incidentima informacijske sigurnosti

12. Upravljanje odnosom s dobavljačima

13. Upravljanje kontinuitetom poslovanja

14. Sukladnost

- sa zakonima i regulativom, sa sigurnosnim politikama i normama, tehnička sukladnost, revizija sustava

CobiT (ISACA)

CoBiT (*Control Objective for Information and related Technology*)

- ◆ autor: ISACA (eng. *Information System Audit and Control Association*)
- ◆ CobiT daje smjernice za analizu, mjerjenje i kontrolu primjene informacijskih sustava u poslovanju
- ◆ detaljno opisuje informatičke procese svrstane u 37 područja, među kojima su i sljedeća područja:
 - **upravljanje sigurnošću**
 - **upravljanje rizikom**
 - **upravljanje zahtjevima usluga i incidentima**
 - **upravljanje kontinuitetom poslovanja**
 - ...
- ◆ **određuje obveze i područja odgovornosti**
- ◆ **određuje ciljeve nadzora i sigurnosne kontrole**

PCI DSS - *Payment Card Industry Data Security Standard*

- sigurnosni standard za kartično poslovanje
- definira minimalne sigurnosne mjere i procese
- ◆ Definirao ga je *Payment Card Industry Security Standards Council*
 - **Visa, MasterCard, American Express, Discover Card i JCB** su zajedno stvorili industrijski standard za sigurnost podataka
 - osigurava trgovcima, kartičnim kućama, bankama i ostalim poslovnim subjektima koji se bave kartičnim poslovanjem **zaštitu podataka vlasnika kartica**
- ◆ Prva verzija standarda PCI DSS izdana je 2004. godine
- ◆ Verzija 2.0 izdana je u listopadu 2010. godine
- ◆ **Verzija 3.2 izdana 2016. godine**

<https://www.pcisecuritystandards.org/>

PCI DSS

- ◆ **Banke i pružatelji usluga** moraju se **certificirati** kod kvalificiranih revizora sigurnosti, a trgovci su dužni se pridržavati PCI DSS standarda i obavljati kartično poslovanje samo s certificiranim pružateljima usluga.
- ◆ PCI DSS 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.
 - ◆ 12 osnovnih zahtjeva i oko 270 podzahtjeva

PCI DSS – načela i zahtjevi

Izgradnja i održavanje sigurne mreže

Zahtjev 1: Instalirati i održavati odgovarajuću konfiguraciju vatrozida (eng. *firewall*) radi zaštite podataka o vlasnicima kartica.

- **Zabraniti izravan vanjski pristup** s Interneta prema bilo kojoj komponenti sustava koja podržava rad okruženja u kojem se nalaze **kartični (korisnički) podaci**.
- **Neprekidno uklanjati maliciozni promet**
- Uvesti **fizičku razdiobu mreže** (segmentaciju) kako bi se odijelili sustavi i mreže koji su okrenuti javnoj uporabi (čime postaju nepouzdani), od sustava na kojima se nalaze kartični (korisnički) podatci
- Uvesti vatrozidove koje odbijaju ili kontroliraju cjelokupni **promet s bežičnih mreža** u sustave na kojima se nalaze kartični podaci
- Uvesti **zaštitu za mrežne aplikacije, baze podataka...**

PCI DSS – načela i zahtjevi

Izgradnja i održavanje sigurne mreže

Zahtjev 2: Ne koristiti lozinke i druge sigurnosne parametre dobivene od dobavljača softverskog sigurnosnog rješenja

- **Promijeniti početne zaporce** postavljene od strane dobavljača
- Sustave za koje je potrebna visoka sigurnost nije dozvoljeno smještati na isti poslužitelj
- Administratorski nekonzolni pristup (npr. putem web sučelja) potrebno je **zaštititi snažnim kriptografskim metodama**, koristeći tehnologije kao što su SSH (Secure Shell) ili SSL/TLS
- Koristiti **sigurne upravljačke protokole i nadzor nad mrežnim prometom** kako bi se spriječila uporaba nedozvoljenih protokola.

PCI DSS – načela i zahtjevi

Zaštita podataka o vlasniku kartice

Zahtjev 3: Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štititi.

- Često nadograđivati sustav za upravljanje sigurnošću. Povjerljivi podaci potrebni za autentikaciju ne smiju se pohranjivati nakon autorizacije, čak i ako su kriptirani.
- **sigurnosni kodovi kartica CVC2** (troznamenkasti ili četveroznamenkasti broj obično ispisan na stražnjoj strani kartice) koji se koriste za potvrđivanje (verifikaciju) transakcije ne smiju se pohranjivati, kao niti PIN (personal identification number) brojevi i kriptirani PIN blokovi.

PCI DSS – načela i zahtjevi

Zaštita podataka o vlasniku kartice

Zahtjev 4: Tijekom prijenosa putem otvorenih, javnih mreža svi podatci o vlasniku kartice moraju se štititi šifriranjem (enkripcijom).

- Koristiti **snažne kriptografske metode i sigurnosne protokole** (primjerice SSL/TLS, IPSEC, SSH) za **zaštitu osjetljivih kartičnih (korisničkih) podataka tijekom prijenosa** kroz otvorene, javne mreže (Internet, bežični prijenos, GSM, GPRS, bluetooth...).
- Uvesti zaštitu od prijenosa nešifriranih podataka
 - moguće je ugraditi filter koji omogućava **sustavu za zaštitu od neovlaštenog pristupa (Intrusion Prevention System – IPS)** otkrivanje o kojoj se aplikaciji i vrsti podataka radi

PCI DSS – načela i zahtjevi

Razvoj i održavanje programa upravljanja ranjivostima sustava

Zahtjev 5: Nužno je koristiti i redovito osvježavati (ažurirati) softver za zaštitu od zlonamjernog koda, odnosno antivirusni softver

- Postaviti **antivirusno programsko rješenje** na sve sustave na koje može djelovati zlonamjerni kod (s naglaskom na osobna računala i poslužitelje)
- Osigurati da sva antivirusna programska rješenja imaju mogućnost prepoznati, ukloniti i štititi od svih poznatih vrsta zlonamjernog koda
- Osigurati da su svi mehanizmi **antivirusne zaštite ažurirani i pokrenuti** te da stvaraju **zapise o korištenju (audit logs)**

PCI DSS – načela i zahtjevi

Razvoj i održavanje programa upravljanja ranjivostima sustava

Zahtjev 6: Razvijati i održavati sigurne sustave i aplikacije

- Osigurati da su sve komponente sustava i softver zaštićeni od poznatih ranjivosti na način da su u produkcijski rad uvedene sve **posljednje sigurnosne zakrpe**.
- Potrebno je razviti ili pribaviti aplikaciju koja pruža brzu, točnu i pouzdanu **zaštitu od unutarnjih i vanjskih cyber napada**.

PCI DSS – načela i zahtjevi

Implementacija strogih mjera kontrole pristupa

Zahtjev 7: Pristup podatcima o vlasniku kartice nužno je ograničiti na minimum onoga što se o njemu u konkretnoj transakciji treba znati.

- Ograničiti pristup sastavnicama sustava i kartičnim (korisničkim) podacima na **samo one pojedince koji imaju poslovnu potrebu** za takvom vrstom pristupa.
- Uspostaviti sustav kontrole pristupa po principu autoriziranja pojedinog korisnika za **pristup najmanjoj količini podataka potrebnoj za rad**.

PCI DSS – načela i zahtjevi

Implementacija strogih mjera kontrole pristupa

Zahtjev 8: Svakoj osobi koja ima pristupa računalnom sustavu treba pridijeliti jedinstvenu identifikaciju (ID).

- Dodijeliti svim **korisnicima jedinstveni identifikator (ID)** prije nego što im se autorizira pristup sastavnicama sustava ili kartičnim (korisničkim) podacima.
- Uvesti **dvosmjernu provjeru identiteta** udaljeni pristup mreži za zaposlenike, administratore (zahtjev za pristup mrežnoj razini koji dolazi izvana)
- Potrebno je osigurati prikladnu provjeru identiteta korisnika i **upravljanje provjerom identiteta za korisnike i administratore** na svim sastavnicama sustava – nadzirati dodavanje, promjenu i brisanje korisničkih ID-a, provjeravati lozinke, zahtijevati “jake” lozinke...

PCI DSS – načela i zahtjevi

Implementacija strogih mjera kontrole pristupa

Zahtjev 9: Maksimalno ograničiti fizički pristup podatcima o vlasniku kartice.

- Koristiti prikladne **kontrole pristupa objektu** kako bi se **ograničio pristup i olakšao nadzor fizičkog pristupa** sustavima smještenim u okruženju koje pohranjuje kartične (korisničke) podatke.
- Razviti procedure za **osiguravanje različitih razina fizičkog pristupa** između zaposlenika i posjetitelja, posebice u štićenim područjima gdje su smješteni kartični (korisnički) podaci.
- Zbog mogućeg utjecaja neovlaštenog fizičkog pristupa, moguće je da su potrebne dodatne autentikacijske kontrole, kao i dodatni nadzor fizičkog pristupa. Primjerice, može se zahtijevati dvofaktorska autentifikacija i nadzirani posjet za sve oblike fizičkog pristupa podatkovnom centru.

PCI DSS – načela i zahtjevi

Redoviti nadzor i ispitivanje mreže

Zahtjev 10: Pratiti i nadzirati svaki pristup mrežnim resursima i podacima o vlasniku kartice.

- Uspostaviti proces povezivanja svih vrsta pristupa sastavnicama sustava (pogotovo ako se radi o administratorskom pristupu) sa pojedinim korisnikom.

- Zapise o korištenju sustava trebalo bi **pregledavati najmanje na dnevnoj razini**. Pregled zapisa trebao bi uključivati poslužitelje koji se koriste za uspostavu sigurnosti, kao što su poslužitelji **IDS (Intrusion Detection System)**.

PCI DSS – načela i zahtjevi

Redoviti nadzor i ispitivanje mreže

Zahtjev 11: Redovito provjeravati sigurnost sustava i procesa.

- Barem jednom kvartalno provjeravati postoje li **točke za bežični pristup**, pogotovo ako se radi o bežičnoj mreži bez jakih sigurnosnih postavki.
- Jednom kvartalno i nakon značajne promjene na mrežnom okruženju potrebno je provesti **testiranje mreže** na unutarnje i vanjske prijetnje i slabosti.
- Koristiti **IDS (Intrusion Detection System)** i/ili **IPS (Intrusion Prevention System)** kako bi se nadzirao sav mrežni promet prema i van okruženja koje pohranjuje kartične (korisničke) podatke. Dodatno, potrebno je nadzirati i mrežni promet koji se odvija unutar samog okruženja.
- IDS i IPS sustave potrebno je **redovito ažurirati**.

PCI DSS – načela i zahtjevi

Razvoj i održavanje informacijske sigurnosne politike

Zahtjev 12: Razviti i održavati odgovarajuću politiku informacijske sigurnosti.

- Razviti **operativne sigurnosne procedure** koje su usklađene za zahtjevima PCI DSS norme (primjerice, procedure održavanja korisničkih računa, procedure pregleda zapisa o korištenju).
- Razviti **politike korištenja za kritične tehnologije** (primjerice, tehnologije za udaljeni pristup, bežične tehnologije, prijenosne medije, prijenosna računala, korištenje elektroničke pošte, korištenje Interneta), kroz koje je potrebno definirati prikladnu uporabu tih tehnologija.
- Napraviti **plan za incidentne situacije** (uloge, odgovornosti, komunikacija, procedure, ...)

