

# Scenariji ogrožanja e-bančnih storitev in primeri zaščitnih ukrepov

mag. Lucija Zupan, CISM,  
Nova ljubljanska banka d.d.

Tadej Vodopivec, CISA, CISSP, CBCP,  
ComTrade d.o.o.

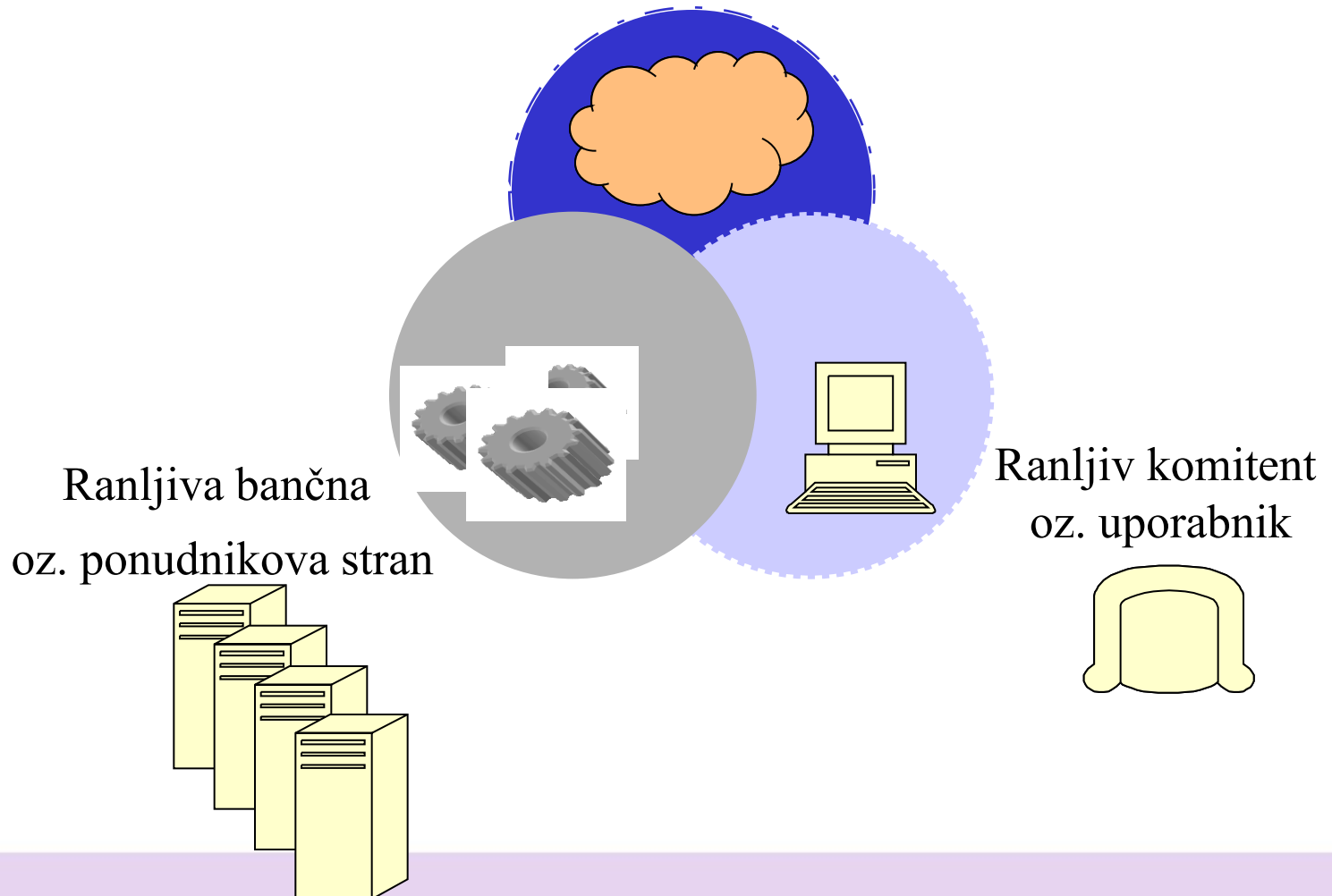
- **Scenariji ogrožanja**
  - Ranljivo okolje e-bančništva
  - Ranljiva bančna oz. ponudnikova stran
  - Ranljiv komitent oz. uporabnik
- **Primeri zaščitnih ukrepov**
  - kjer je možno, jih bomo navezali na scenarij ogrožanja

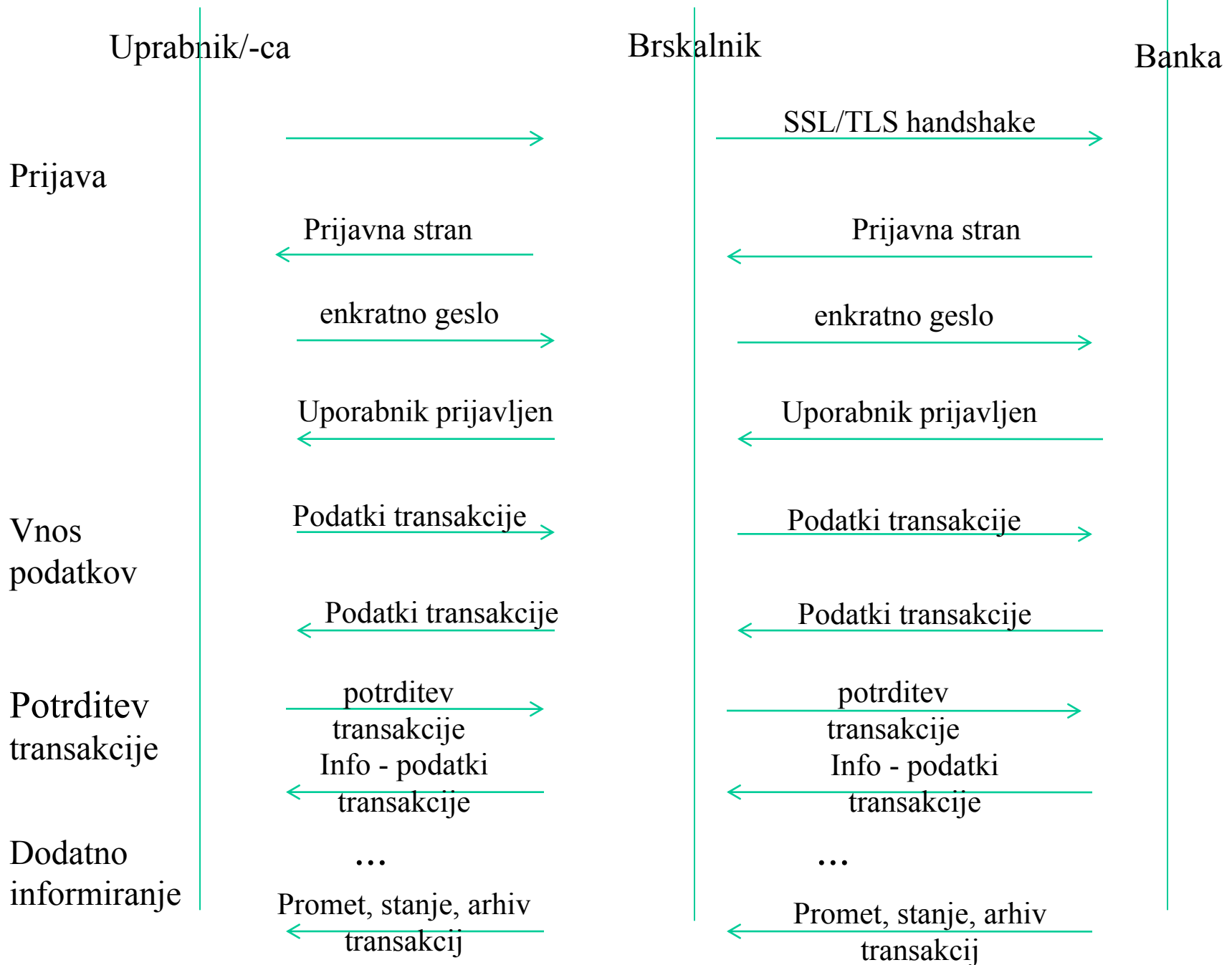


# Scenariji ogrožanja



Ranljivo okolje e-bančništva  
(v grobem internet)



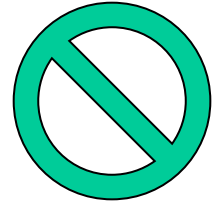


- Scenariji ogrožanja
  - **Ranljivo okolje e-bančništva**
  - Ranljiva bančna oz. ponudnikova stran
  - Ranljiv komitent oz. uporabnik
- Primeri zaščitnih ukrepov
  - kjer je možno, jih bomo navezali na scenarij ogrožanja





- **DoS in DDoS**
- Pharming, Phishing
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil





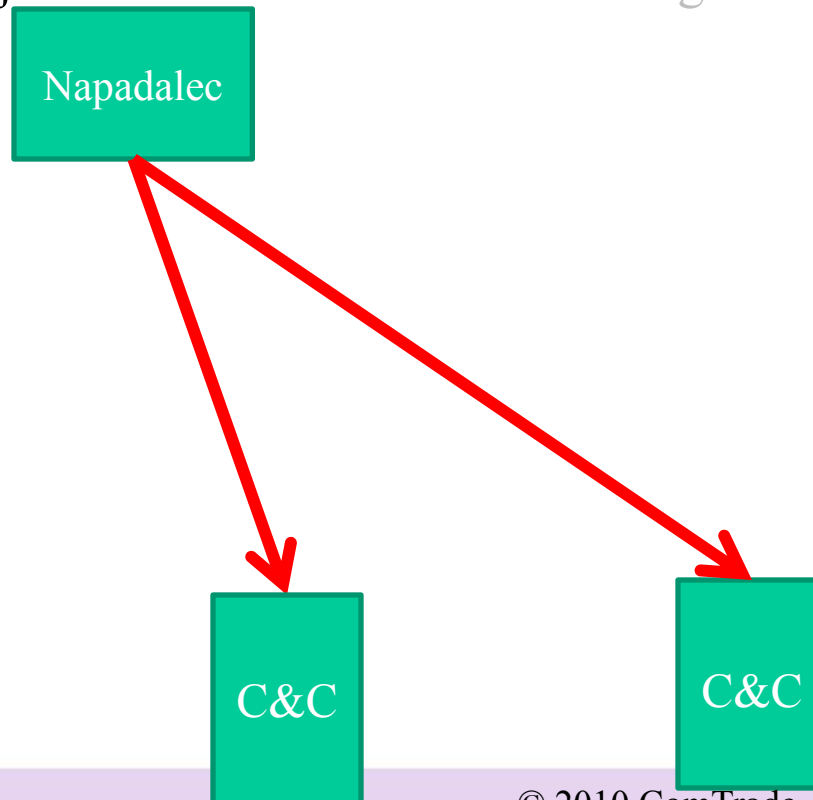
- DoS – denial of service
  - [http://malerisch.net/docs/defending\\_against\\_application\\_level\\_dos/Roberto\\_Suggi\\_Liverani\\_OWASPNZDAY2010-Defending\\_against\\_application\\_DoS.pdf](http://malerisch.net/docs/defending_against_application_level_dos/Roberto_Suggi_Liverani_OWASPNZDAY2010-Defending_against_application_DoS.pdf)
- DDoS – distributed DoS
  - “ojačitev” DoS napada s pomočjo botnetov



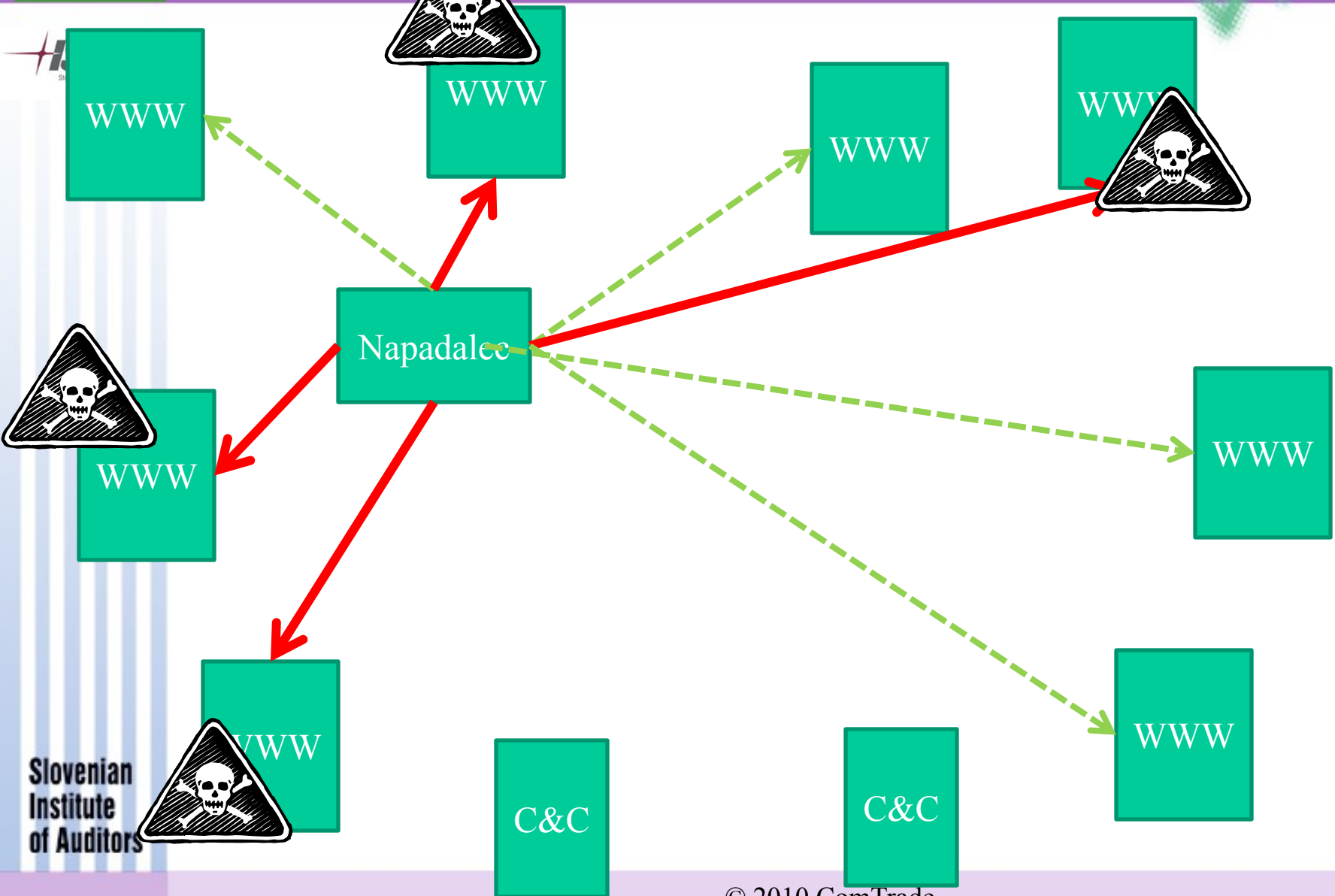
**botnet** (*angl. botnet, robot network*)

1. preko spleta v mrežo povezani boti (roboti) ali avtomatizirani programi npr IRC boti
2. prikrito omrežje računalnikov, okuženih z zlonamerno kodo, ki ga lahko upravljamo z oddaljene lokacije, največkrat za ilegalno početje

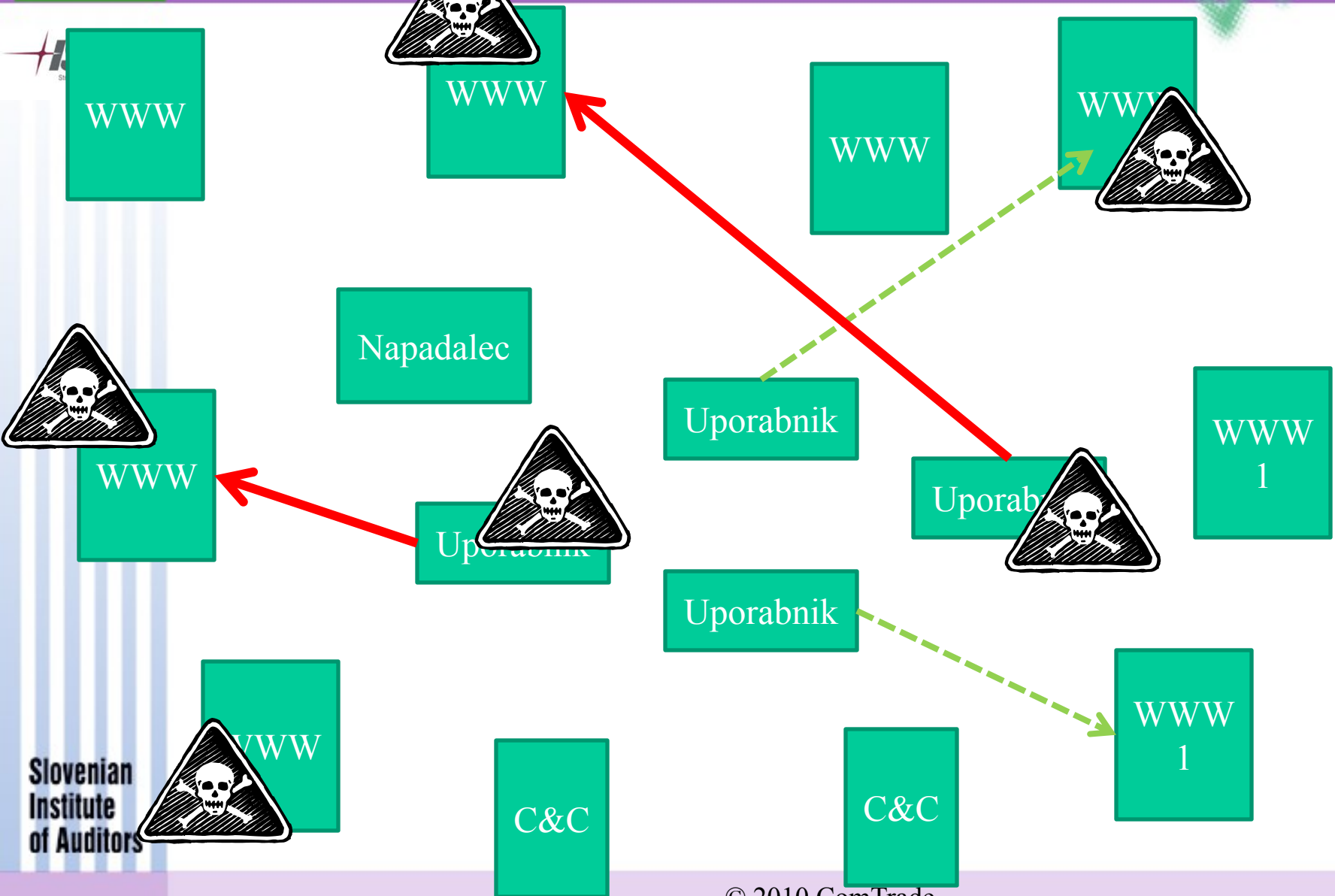
vir: [www.islovar.org](http://www.islovar.org)

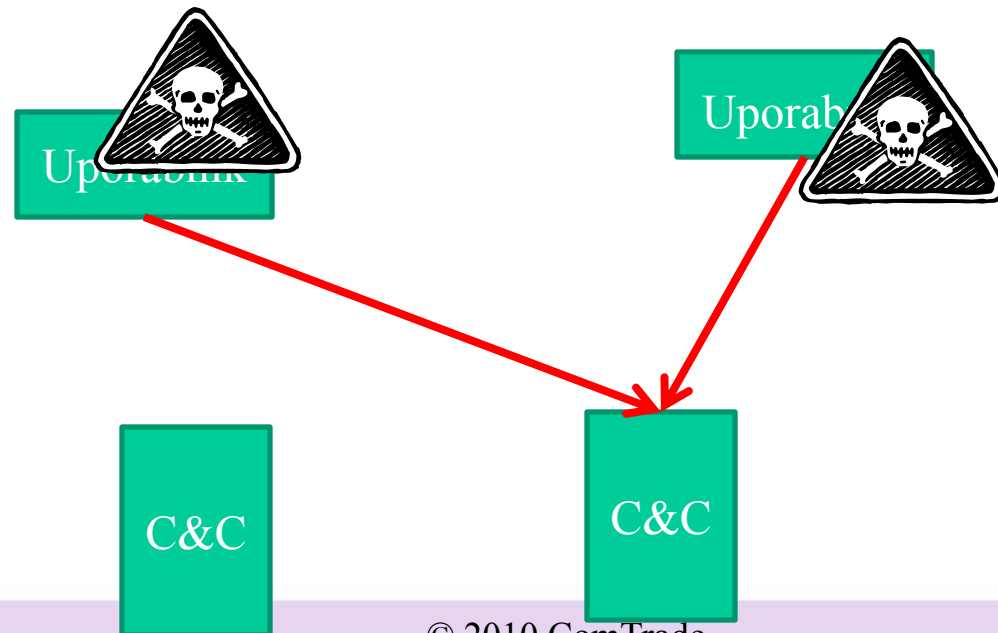


# Botneti

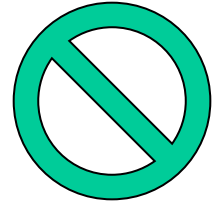


# Botneti





- DoS in DDoS
- **Pharming, Phishing**
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil





- Phishing
  - nepooblaščno pridobivanje skrivnih podatkov
  - e-bančništvo: uporabniška imena, gesla, zasebni ključi
  - e-pošta + naiven uporabnik -> lažna spletna stran
- Pharming
  - “zastrupljen” DNS pri uporabniku

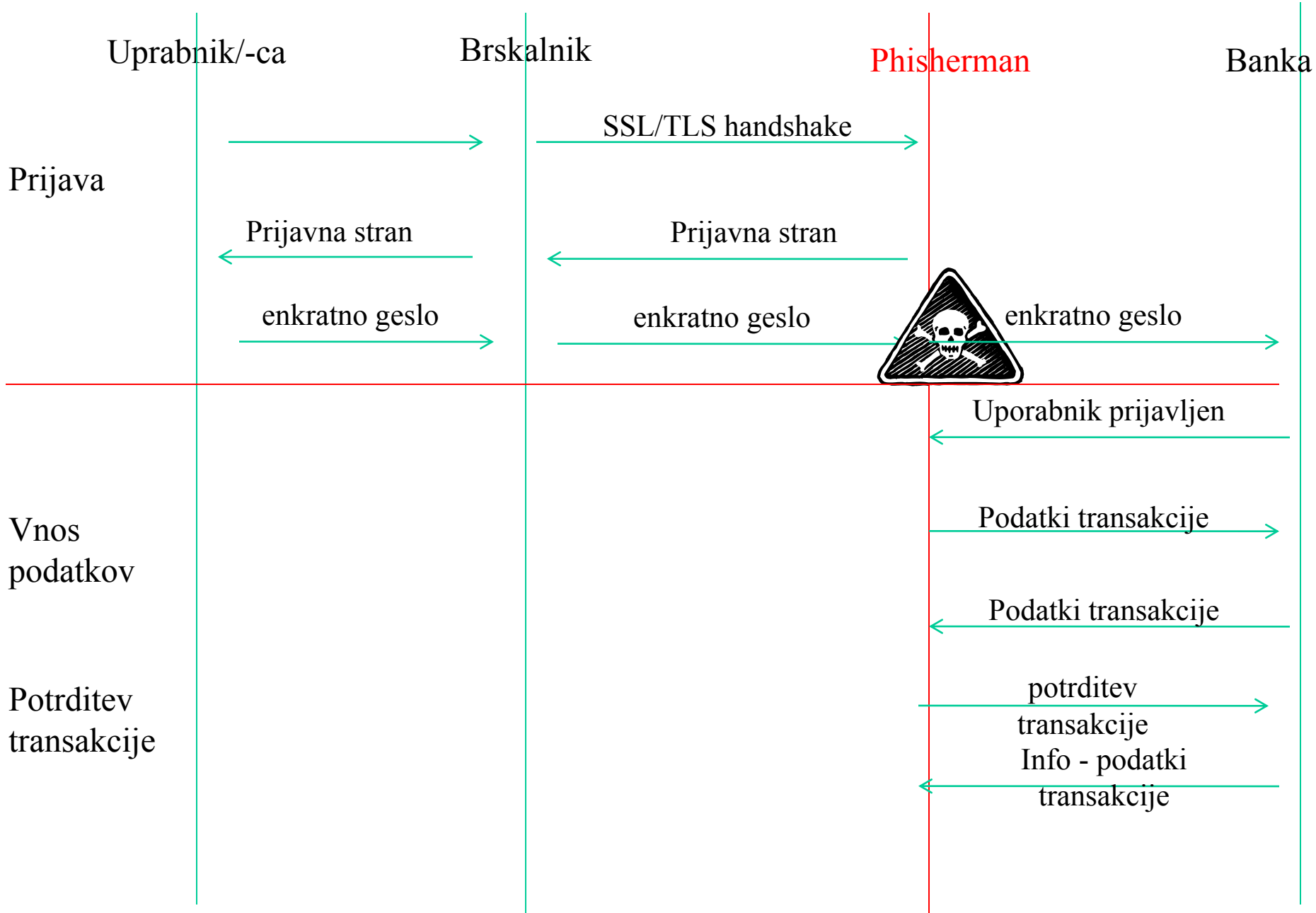


- UNIX: /etc/hosts
- Windows:  
C:\WINDOWS\system32\drivers\etc\hosts
- Hišni usmerjevalnik

127.0.0.1      localhost

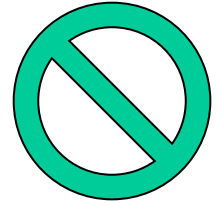
194.87.13.6      www.moja-banka.si

194.87.13.6      www.glavna-banka.si



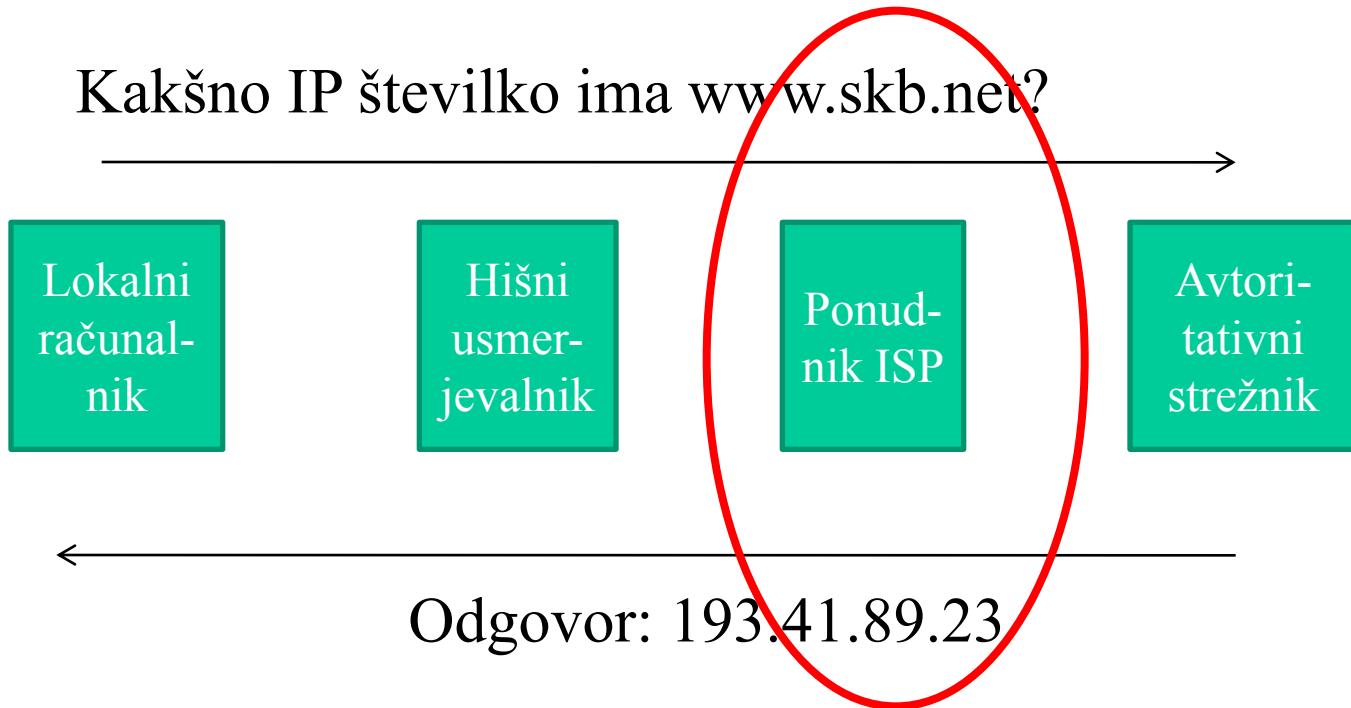
# DNS cache poisoning

- DoS in DDoS
- Pharming, Phishing
- **DNS cache poisoning v omrežju**
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil





Kakšno IP številko ima **www.skb.net**?



Lokalni računalnik

Hišni usmerjevalnik

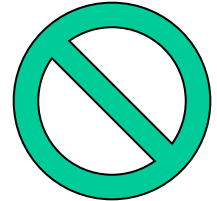
Ponudnik ISP

Avtoritativni strežnik

Odgovor: 193.41.89.23

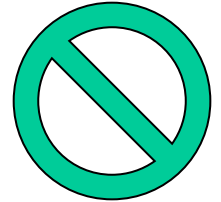
# Zlonamerno pre-usmerjanje

- DoS in DDoS
- Pharming, Phishing
- DNS cache poisoning v omrežju
- **Zlonamerno pre-usmerjanje IP prometa**
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil



# Ponarejena ali zavajajoča potrdila

- DoS in DDoS
- Pharming, Phishing
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- **Ponarejena ali zavajajoča strežniška digitalna potrdila**
- MITM napad
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil



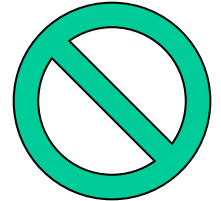
# Ponarejena ali zavajajoča potrdila

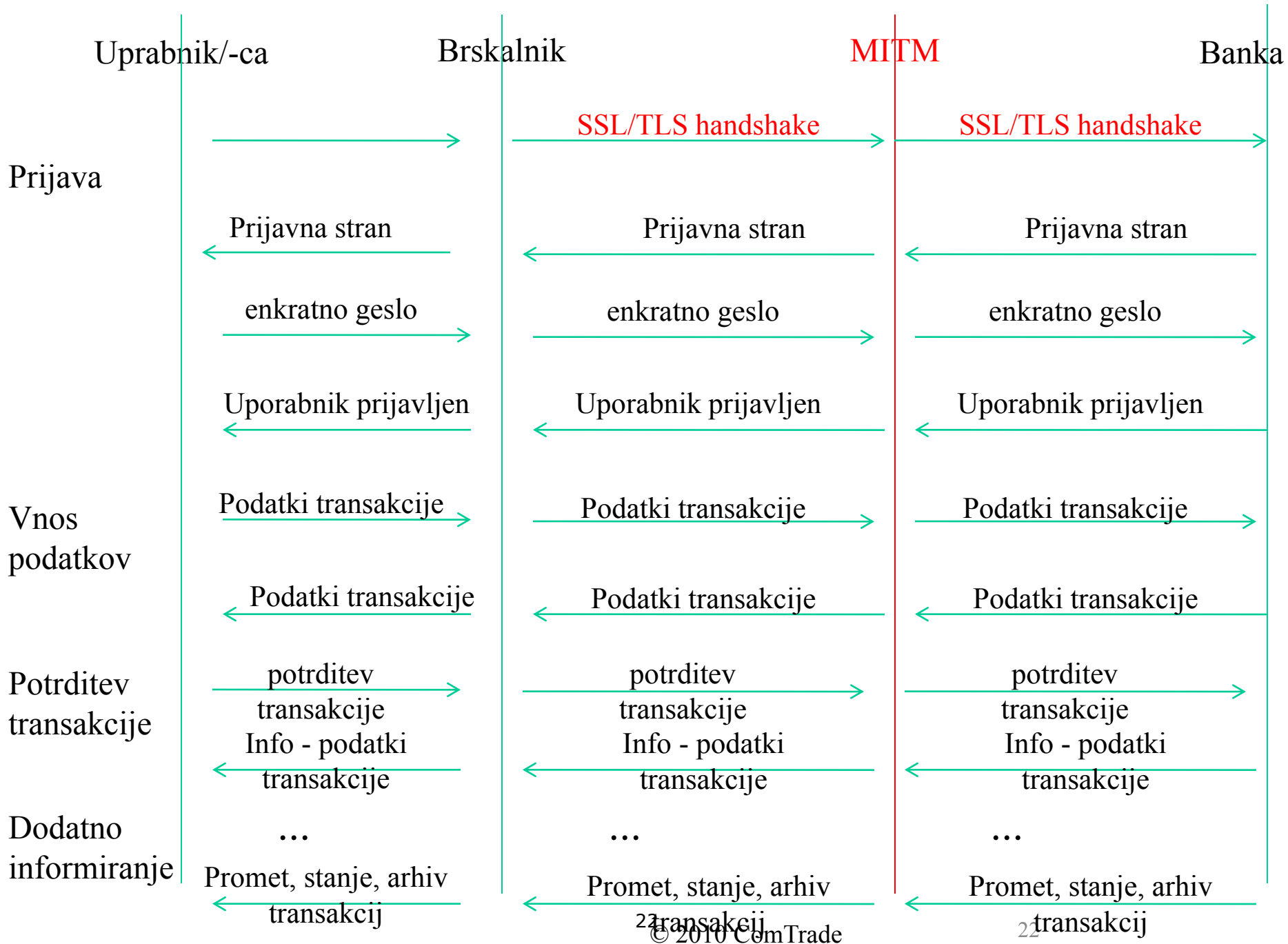
- izkoriščanje odsotnosti polja X.509 End Entity v digitalnih potrdilih
- uporaba mednarodnih domenskih imen s podobnimi znaki (npr. č in ć) ali znaki, ki jih brskalniki ne pokažejo
- uporaba ničtih znakov (ASCII kod 0), ki v nekaterih okoljih označujejo konec niza (npr. certifikat za `https://moja.banka.si[\x00].napadalec.org`) so v preteklosti overitelji izdajali vsakomur, ki je dokazal lastništvo domene `napadalec.org`, brskalniki pa so ga obravnavali in prikazali kot `moja.banka.si`
- ustvarjanje vtisa HTTPS strani s prikazom ključavnice v ikoni spletnega mesta in podobno (angl. visual spoofing)

Glej tudi <http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>



- DoS in DDoS
- Pharming, Phishing
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- **MITM napad**
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil





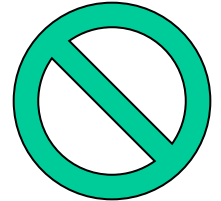
# SSL Renegotiation MITM

<http://www.phonefactor.com/sslgap/ssl-tls-authentication-patches>

Protokol je popravljen od 7.1.2010 (RFC 5746)

Microsoft je izdal popravke v avgustu 2010

- DoS in DDoS
- Pharming, Phishing
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- **Mule**
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil



V policiji ugotavljamo, da se neznani storilci v večini primerov **izdajajo za podjetja**, kot so Lesprom, Dia-group, Contici-travel ipd. ter **po elektronski pošti pošiljajo ponudbe za lažno poslovno sodelovanje** naključnim osebam.

Vsem, ki se javijo in izrazijo interes za sodelovanje, v podpis pošiljajo pogodbe, iz katerih je razvidno, da bodo na svoje transakcijske račune prejeli denar, ki ga morajo nato poslati na drug račun, večinoma prek plačilnega sistema Western Union in Moneygram. Za to opravilo jim obljubijo plačilo, ki je lahko izraženo v odstotkih od posamezne transakcije ali kot mesečno plačilo. Računi, kamor se prenaša tako pridobljen denar, so večinoma v Ukrajini in Rusiji, kjer se izgubljajo koristne sledi za izsleditev storilcev.

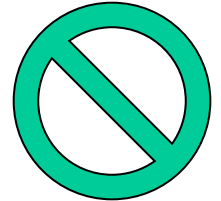
**Denarna sredstva, ki jih ljudje v takšnih primerih prejemajo na svoje transakcijske račune, izvirajo iz kaznivih dejanj. Vse, ki pridejo v stik z izmišljenimi podjetji, zato pozivamo, da se na tovrstne oglase in poskuse nezakonitega sodelovanja ne odzoveje!**

V nasprotnem primeru bi neznanim storilcem omogočili izvršitev **kaznivega dejanja velike tatvine ter napada na informacijski sistem**, zaradi česar bi bili **tudi sami kazensko odgovorni**. Zoper vse, ki bodo v Sloveniji na takšen način prejemali denar, bo policija ukrepala in podala kazensko ovadbo na pristojno državno tožilstvo.

vir: <http://www.policija.si/index.php/preventiva/preventiva/7411-zlorabe-elektronskega-bannitva-opozorilo-uporabnikom-elektronskih-bannih-storitev>

# Napad na A5/1 šifriranje

- DoS in DDoS
- Pharming, Phishing
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- Mule
- **Mobilna telefonija - napad na A5/1 šifriranje**
- **Mobilna telefonija – MITM napad med bazno postajo in uporabnikom**
- Mobilna telefonija – SMishing in potvarjanje SMS sporočil

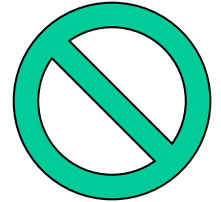


# Napad na A5/1 šifriranje

- Kriptoanaliza A5/1 šifriranja
  - kljub večkratnim dokazom o ranljivosti javno objavljen uspešno izveden praktičen koncept napada (s strani raziskovalcev) šele konec 2009 praktično demonstrirano – uporaba t.i. mavričnih tabel
  - <http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html>
- MITM napad na komunikacijo GSM bazna postaja – GSM aparat
  - standard GSM ne predvideva avtentikacije bazne postaje aparatu
  - obveščevalne službe (in baje kriminalne združbe) uporabljajo že dlje časa – t.i. IMSI catcher
  - možna realizacija tudi s cenovno dostopno opremo
- Obe varianti zahtevata fizično bližino žrtvi napada (ista bazna postaja)
- UMTS / 3G sta odporna na ta napad, če telefon ne preklopi na GSM
- Vpliv na e-bančništvo:
  - Prestrežanje enkratnih SMS OTP kod
  - Modificiranje (MITM) SMS OTP potrditvenih sporočil (npr. vsebina transakcije)
  - prizadeto SMS bančništvo brez dodatnega šifriranja



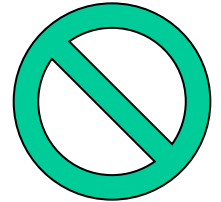
- DoS in DDoS
- Pharming, Phishing
- DNS cache poisoning v omrežju
- Zlonamerno pre-usmerjanje IP prometa
- Ponarejena ali zavajajoča strežniška digitalna potrdila
- MITM napad
- Mule
- Mobilna telefonija - napad na A5/1 šifriranje
- Mobilna telefonija – MITM napad med bazno postajo in uporabnikom
- **Mobilna telefonija – SMishing in potvarjanje SMS sporočil**



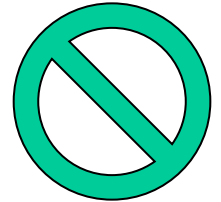
- Scenariji ogrožanja
  - Ranljivo okolje e-bančništva
  - **Ranljiva bančna oz. ponudnikova stran**
  - Ranljiv komitent oz. uporabnik
- Primeri zaščitnih ukrepov
  - kjer je možno, jih bomo navezali na scenarij ogrožanja

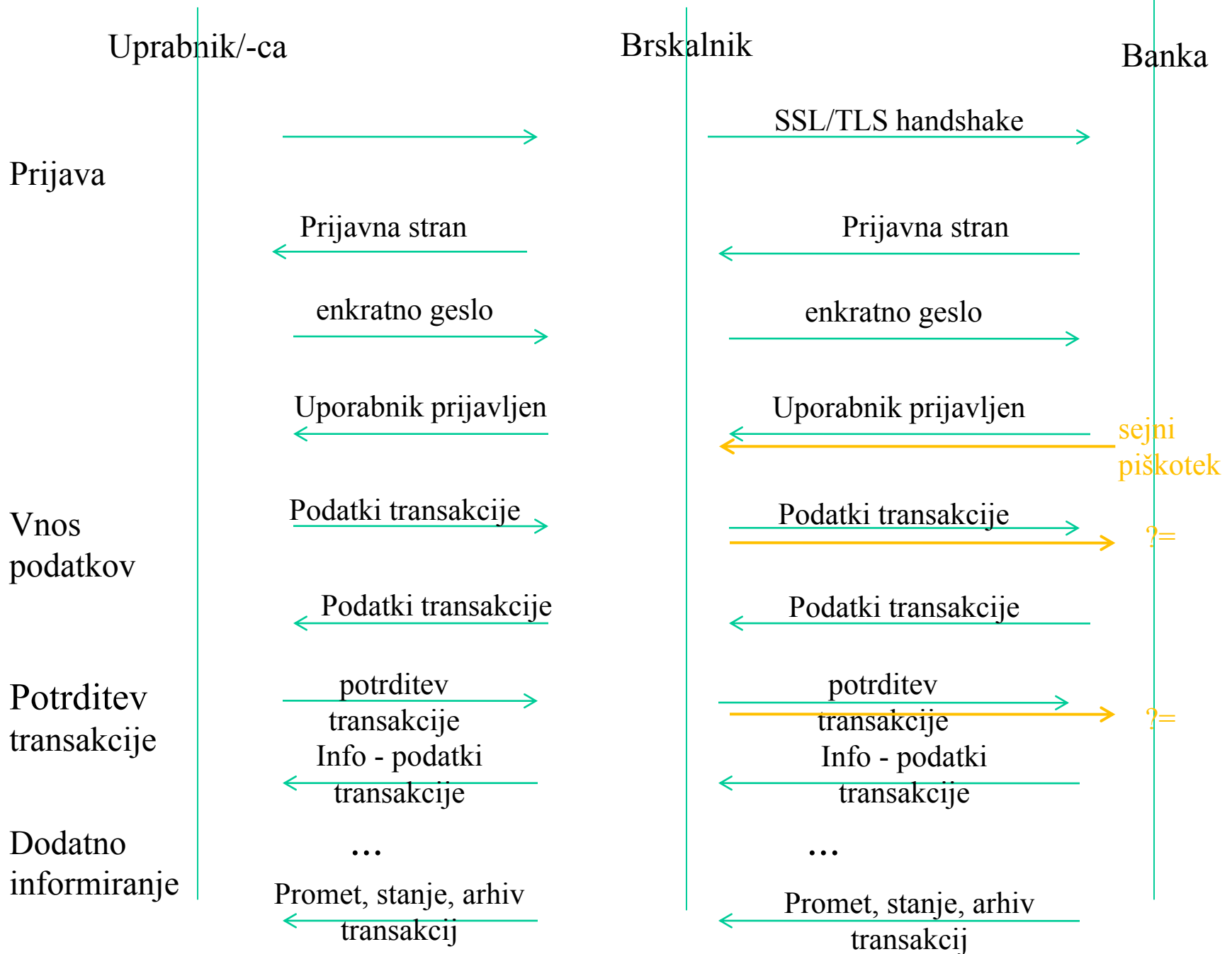


- **Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata**
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

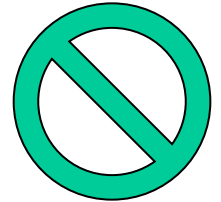


- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- **XSS - Cross site scripting**
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

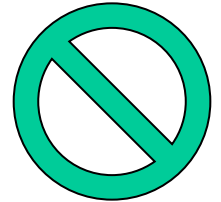




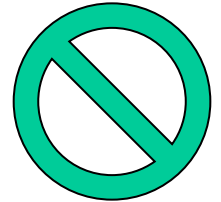
- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- **SQL injection in druga vrivanja**
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

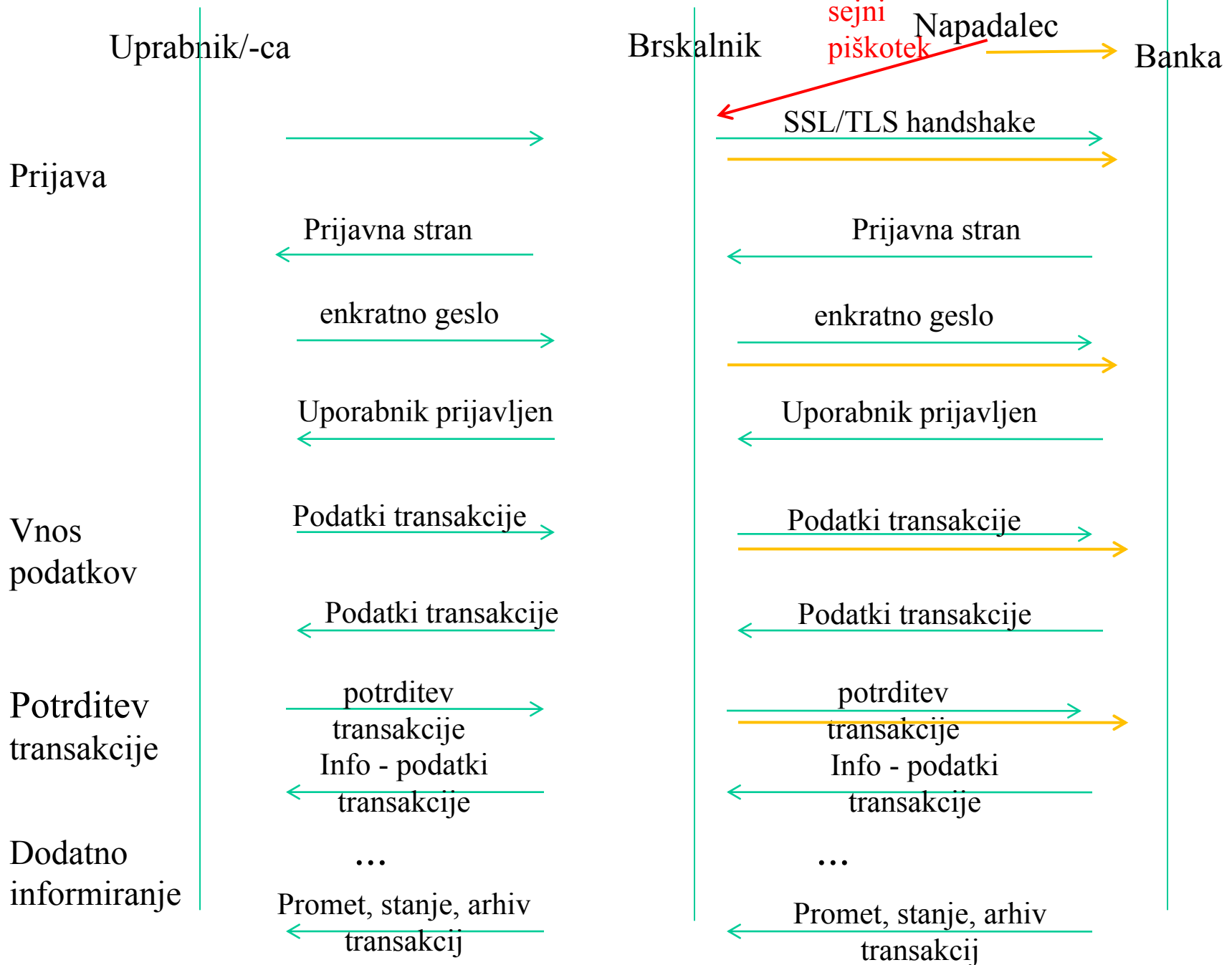


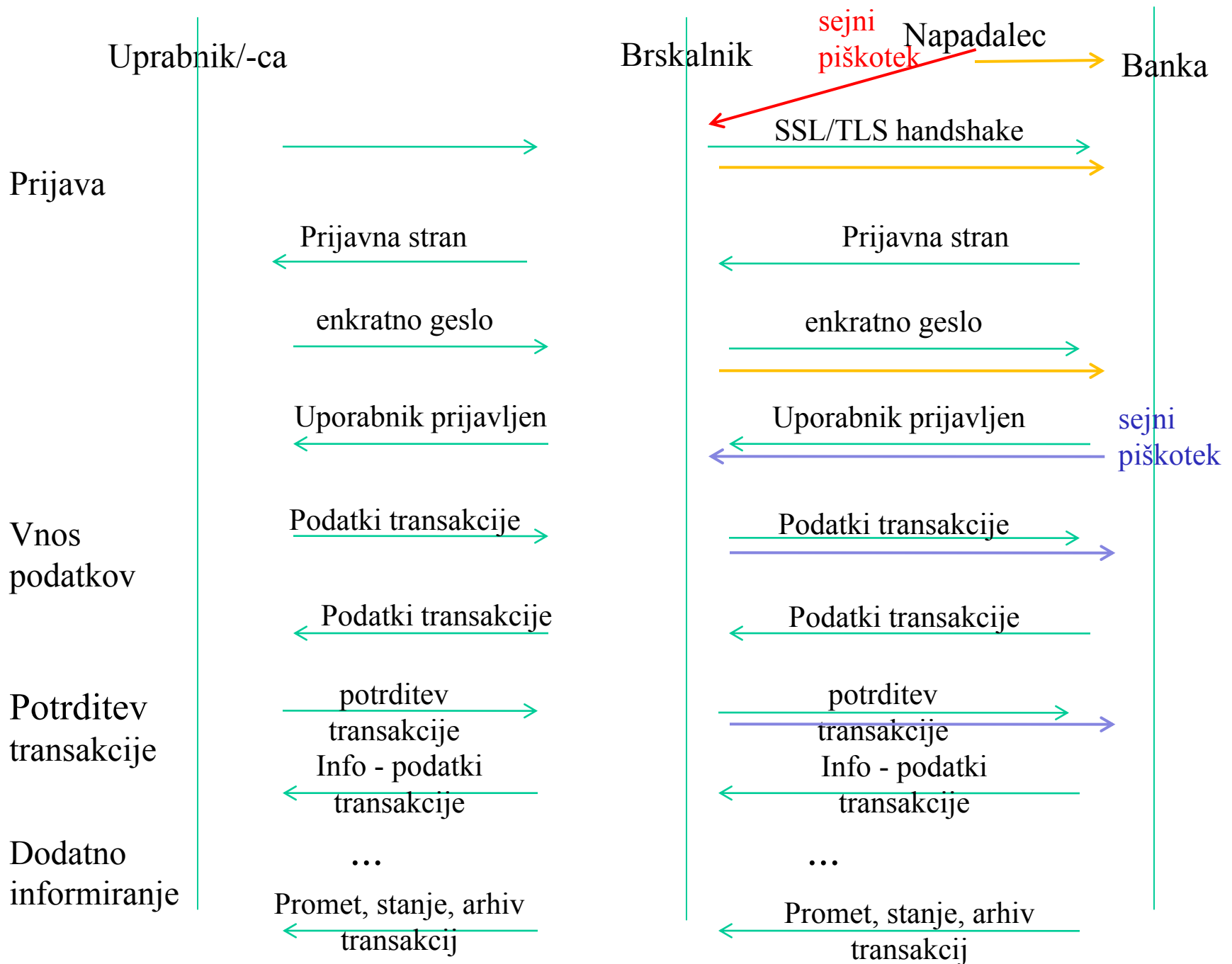
- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- **Cross Site Request Forgery (XSRF ali CSRF)**
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve



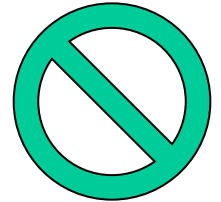
- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- **Session fixation**
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve



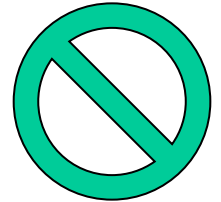




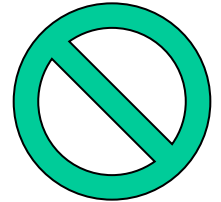
- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- **Kripto analiza**
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve



- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- **Izkoriščanje prekoračitve med-pomnilnika**
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

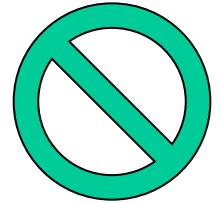


- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- **DoS (lokaliziran)**
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

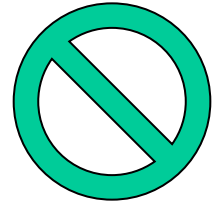


# Prirejanje parametrov

- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- **Prirejanje parametrov**
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

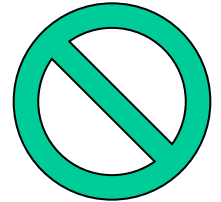


- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- **Napad z grobo silo**
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve



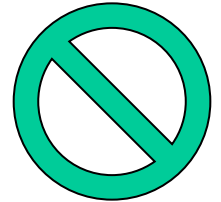
# Napake, ki povedo preveč

- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- **Pridobivanje podatkov iz sporočil o napakah**
- Brisanje sledi napada
- Napad na skrbniški del ali nastavitve

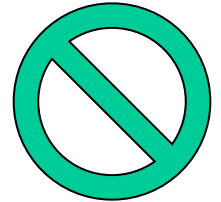


# Brisanje sledi napada

- Nepooblaščen pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- **Brisanje sledi napada**
- Napad na skrbniški del ali nastavitve



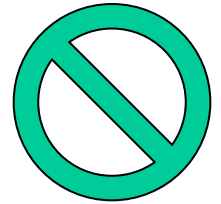
- Nepooblašena pridobitev zasebnega ključa strežniškega certifikata
- XSS - Cross site scripting
- SQL injection in druga vrivanja
- Cross Site Request Forgery (XSRF ali CSRF)
- Session fixation
- Kripto analiza
- Izkoriščanje prekoračitve med-pomnilnika
- DoS (lokaliziran)
- Prirejanje parametrov
- Napad z grobo silo
- Pridobivanje podatkov iz sporočil o napakah
- Brisanje sledi napada
- **Napad na skrbniški del ali nastavitve**



- Scenariji ogrožanja
  - Ranljivo okolje e-bančništva
  - Ranljiva bančna oz. ponudnikova stran
  - **Ranljiv komitent oz. uporabnik**
- Primeri zaščitnih ukrepov
  - kjer je možno, jih bomo navezali na scenarij ogrožanja

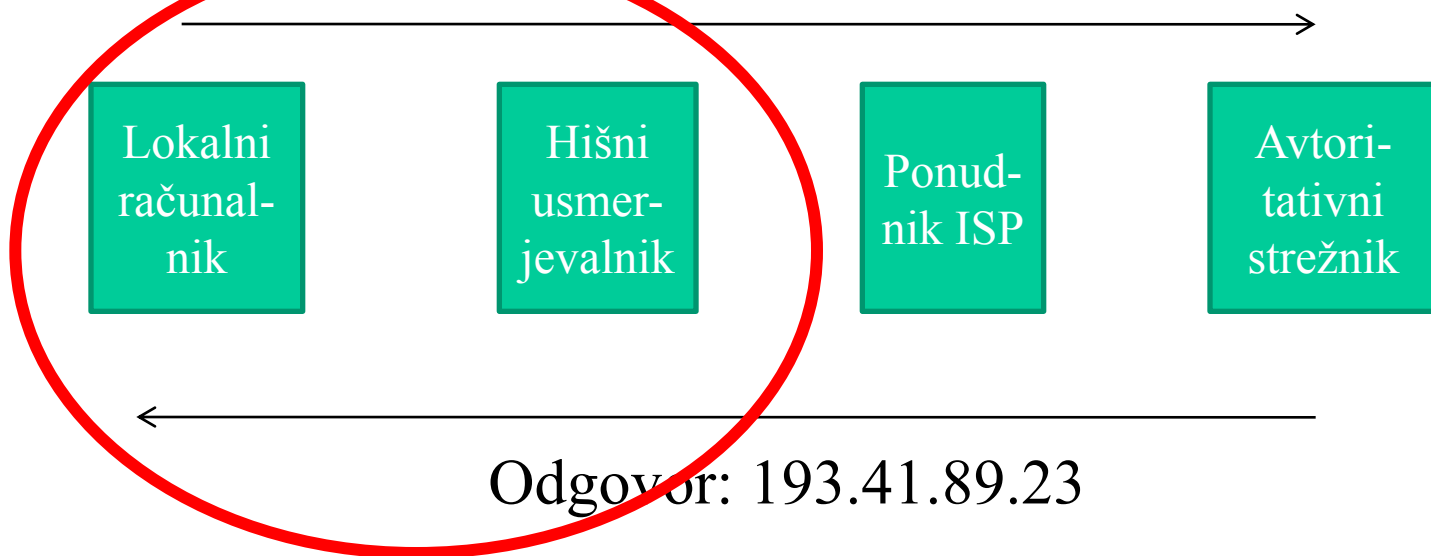


- **Manipulacija DNS pri uporabniku**
- kraja zasebnega ključa PKI
- prestrazanje gesel
- MITB napad
- Trojanski konji in botneti
- Socialni inženiring
- Kraja seje
- Izkoriščanje varnostnih pomanjkljivosti pri integraciji internega sistema za obdelavo plačil (ERP) v organizaciji z B2B kanalom e-banke



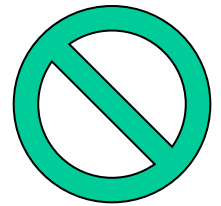


Kakšno IP številko ima www.skb.net?

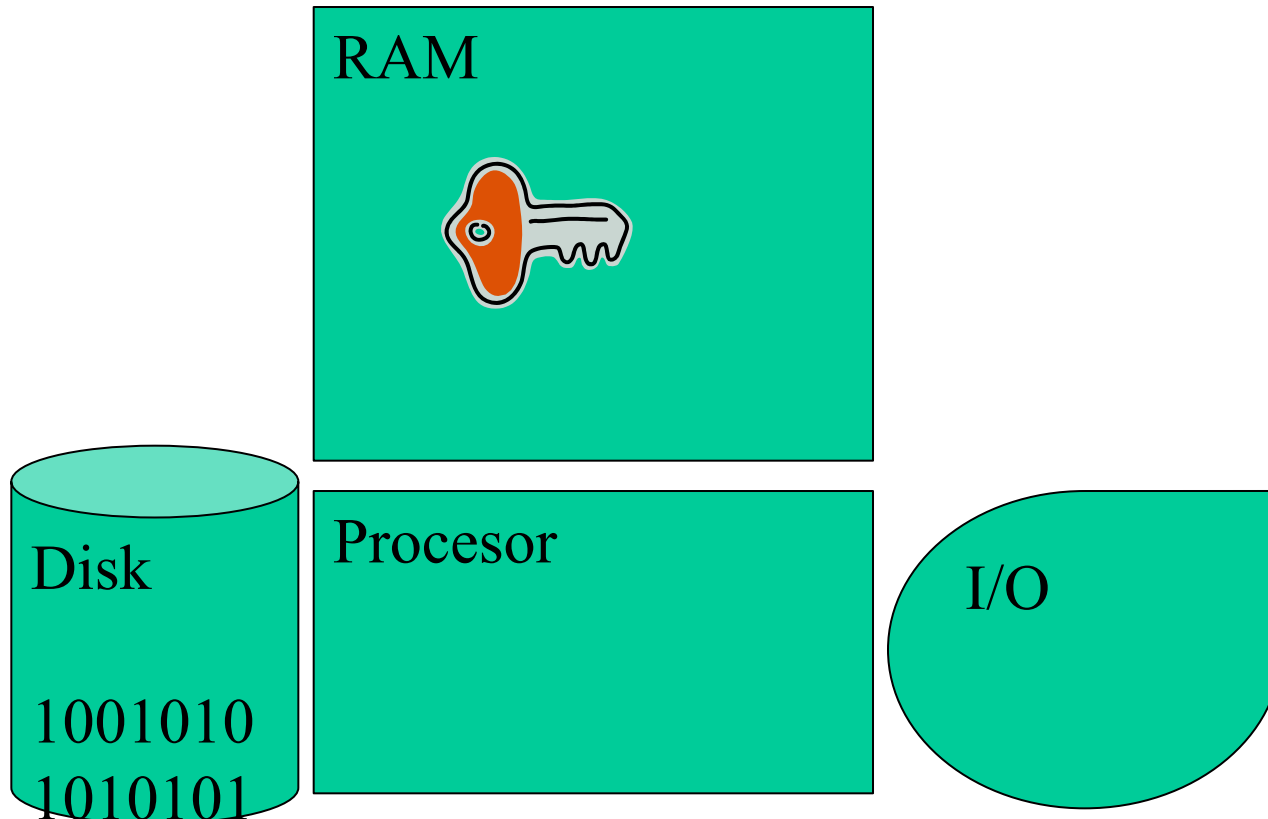


# Kraja zasebnega ključa PKI

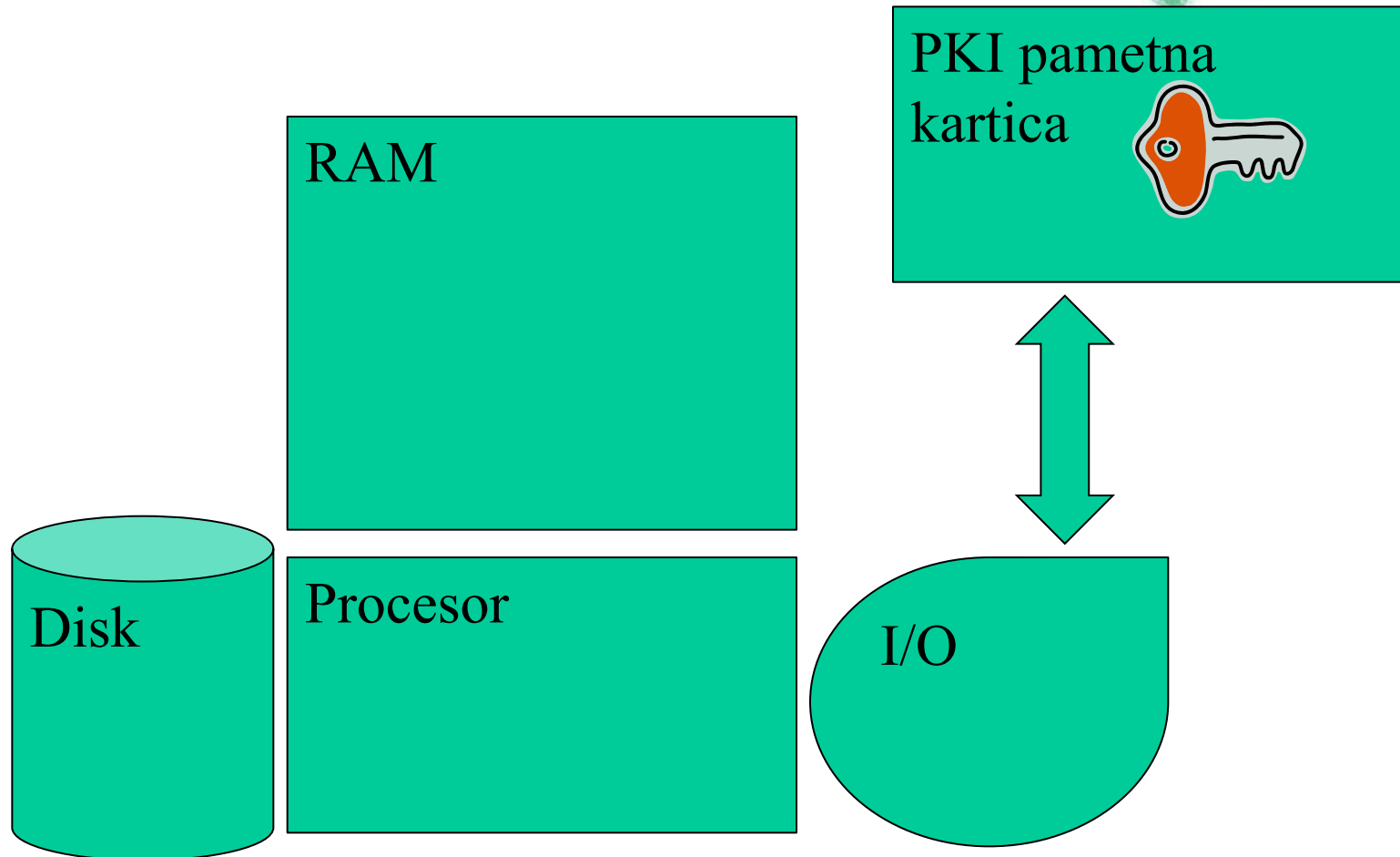
- Manipulacija DNS pri uporabniku
- **kraja zasebnega ključa PKI**
- prestrežanje gesel
- MITB napad
- Trojanski konji in botneti
- Socialni inženiring
- Kraja seje
- Izkoriščanje varnostnih pomanjkljivosti pri integraciji internega sistema za obdelavo plačil (ERP) v organizaciji z B2B kanalom e-banke



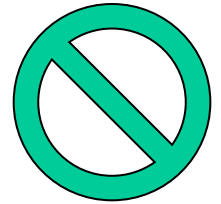
# Nešifriran ključ v pomnilniku



# Pametna kartica

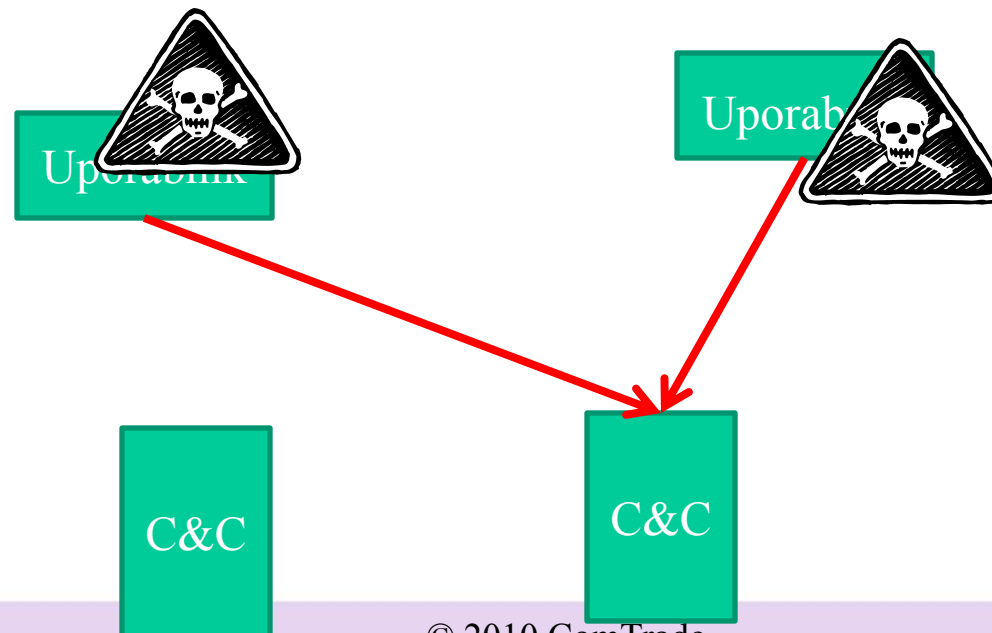


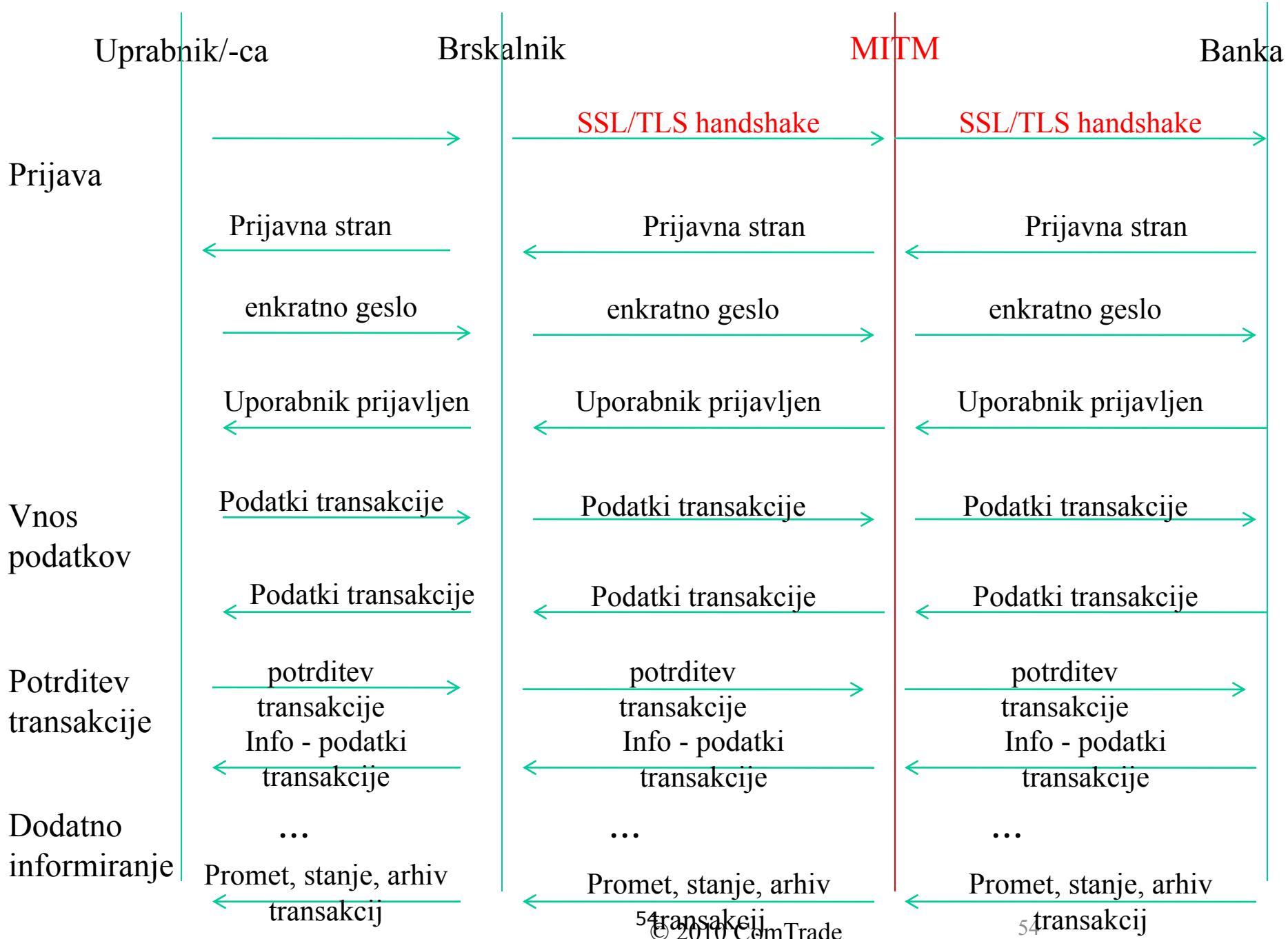
- Manipulacija DNS pri uporabniku
- kraja zasebnega ključa PKI
- **prestrezanje gesel**
- **MITB napad**
- **Trojanski konji in botneti**
- Socialni inženiring
- Kraja seje
- Izkoriščanje varnostnih pomanjkljivosti pri integraciji internega sistema za obdelavo plačil (ERP) v organizaciji z B2B kanalom e-banke

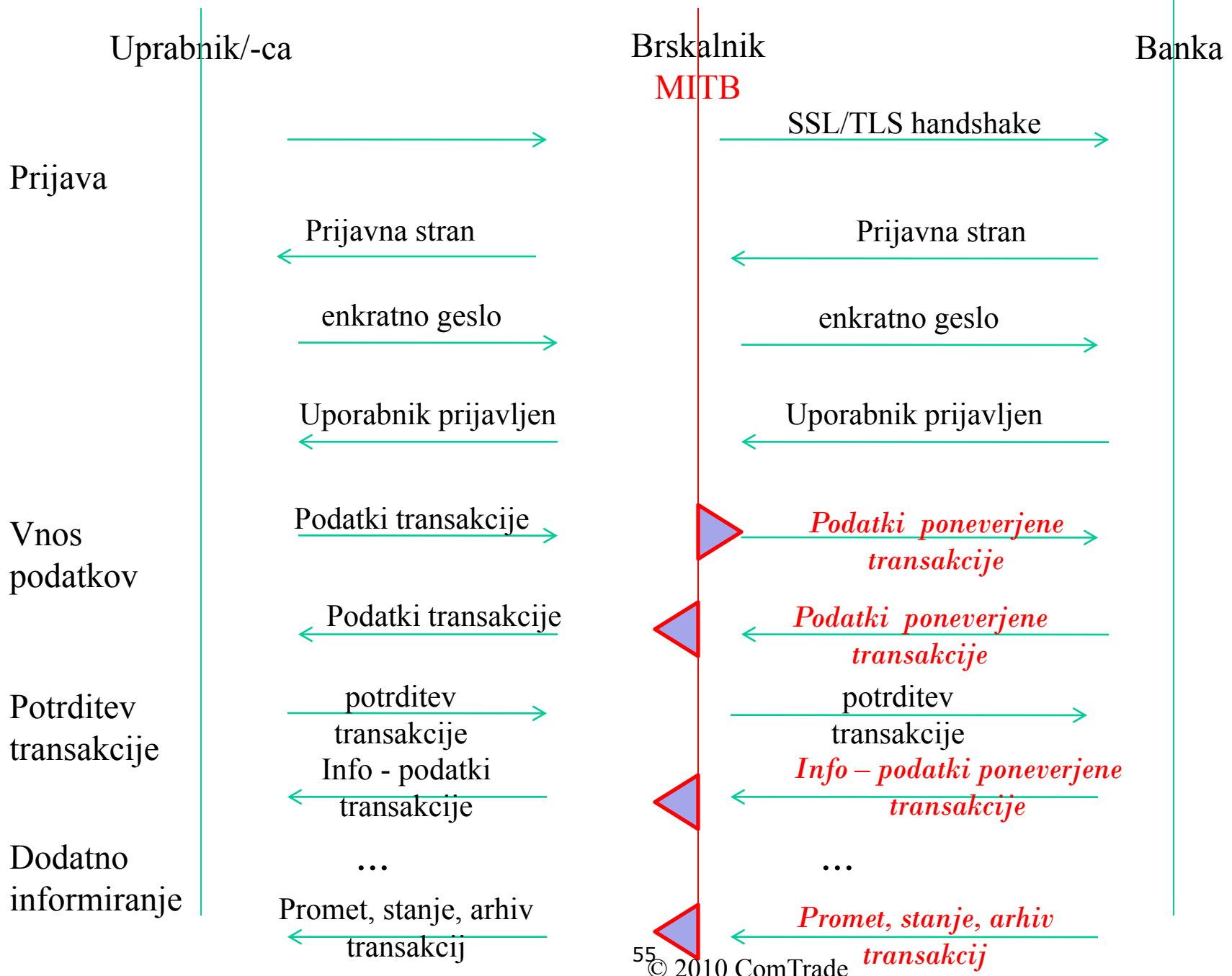


Zlonameren program lokalno na uporabnikovem računalniku prestreže geslo, enkratno kodo, ... in jo pošlje napadalcu

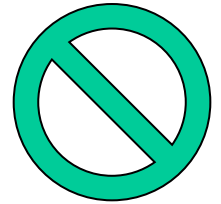
predpogoj je “okužen” računalnik



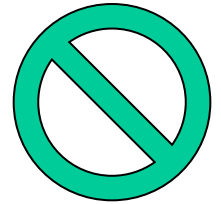


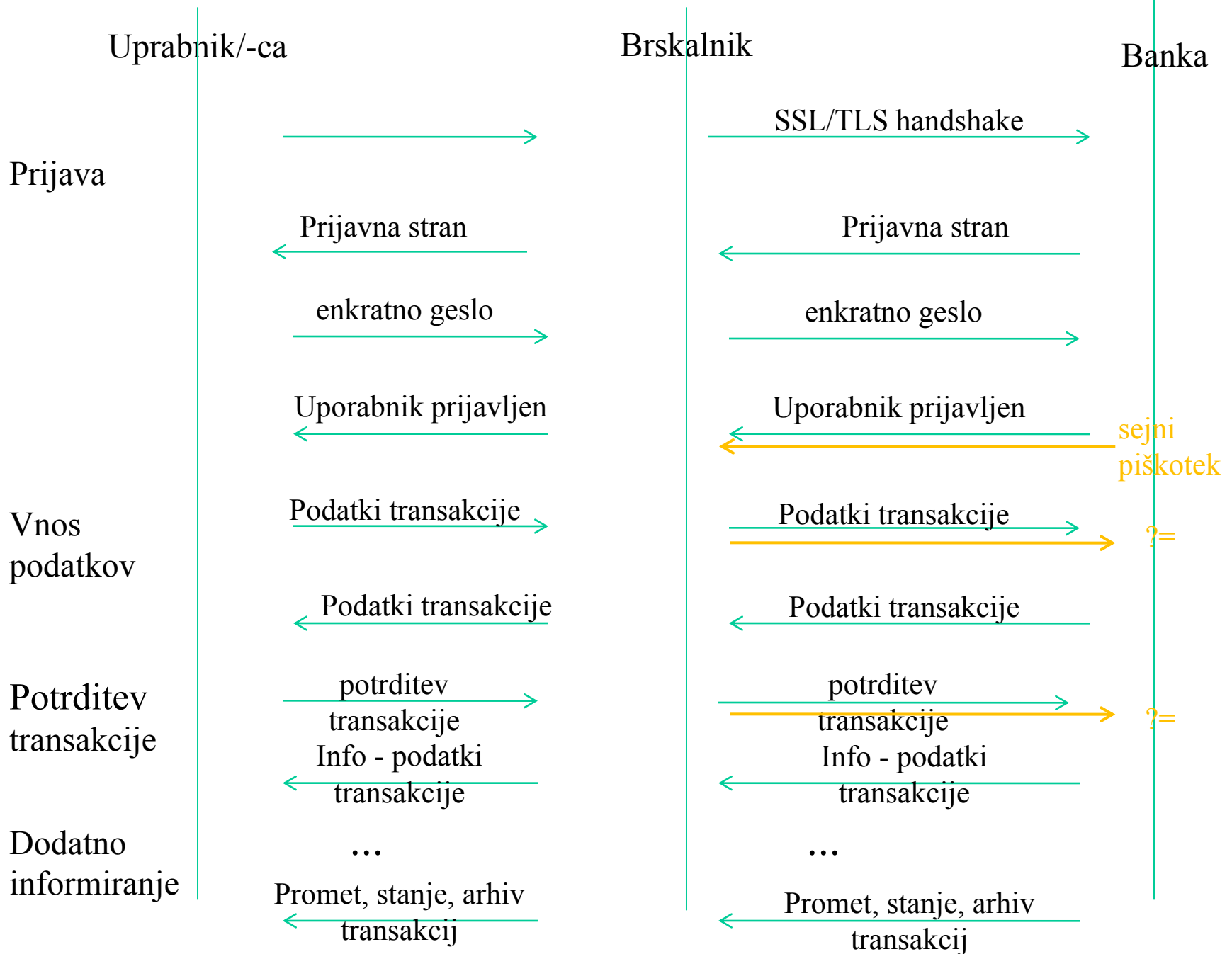


- Manipulacija DNS pri uporabniku
- kraja zasebnega ključa PKI
- prestrezanje gesel
- MITB napad
- Trojanski konji in botneti
- **Socialni inženiring**
- Kraja seje
- Izkoriščanje varnostnih pomanjkljivosti pri integraciji internega sistema za obdelavo plačil (ERP) v organizaciji z B2B kanalom e-banke



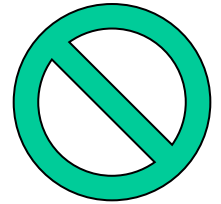
- Manipulacija DNS pri uporabniku
- kraja zasebnega ključa PKI
- prestrežanje gesel
- MITB napad
- Trojanski konji in botneti
- Socialni inženiring
- **Kraja seje**
- Izkoriščanje varnostnih pomanjkljivosti pri integraciji internega sistema za obdelavo plačil (ERP) v organizaciji z B2B kanalom e-banke

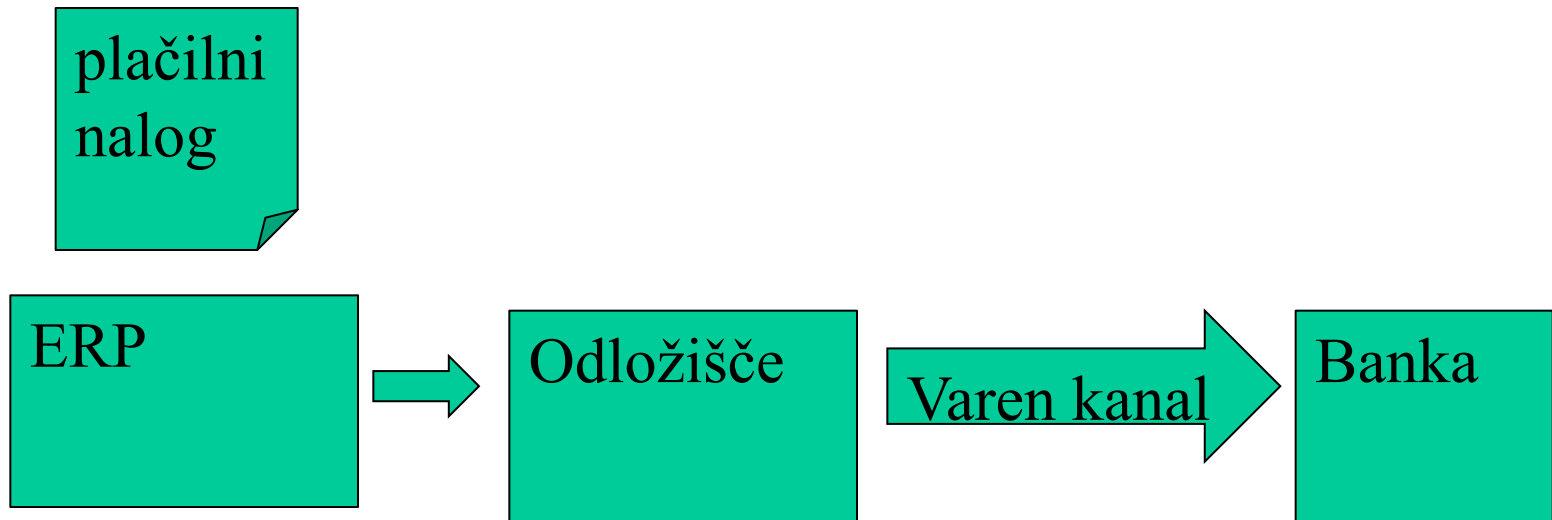




# Izkoriščanje ranljivosti integracije

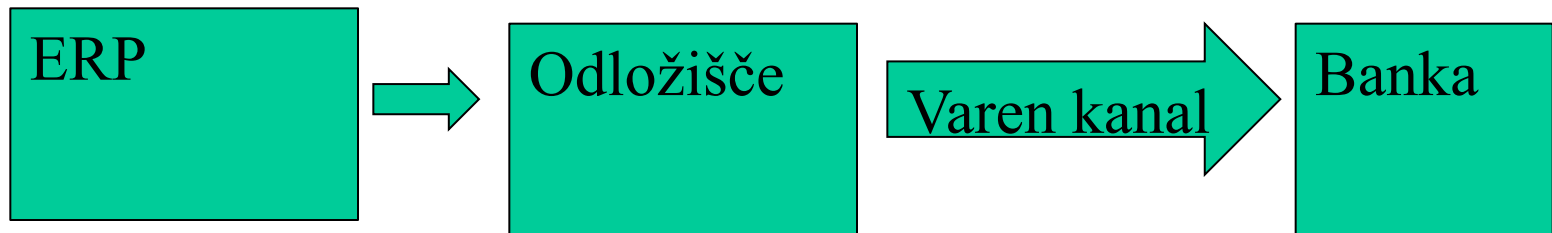
- Manipulacija DNS pri uporabniku
- kraja zasebnega ključa PKI
- prestrezanje gesel
- MITB napad
- Trojanski konji in botneti
- Socialni inženiring
- Kraja seje
- **Izkoriščanje varnostnih pomanjkljivosti pri integraciji internega sistema za obdelavo plačil (ERP) v organizaciji z B2B kanalom e-banke**





Napadalec

plačilni  
nalog



# Primeri zaščitnih ukrepov

- Scenariji ogrožanja
  - Ranljivo okolje e-bančništva
  - Ranljiva bančna oz. ponudnikova stran
  - Ranljiv komitent oz. uporabnik
- **Primeri zaščitnih ukrepov**
  - kjer je možno, jih bomo navezali na scenarij ogrožanja



# Odnosi s podizvajalci/dobavitelji

- pravica pregleda izvorne kode
- pravica revidiranja vsega (SaaS primer)
- izrecno pogodbeno ureditev varstva osebnih podatkov v primeru SaaS

- glej standard A7700;  
[http://www.a7700.org/index\\_e.html](http://www.a7700.org/index_e.html) za spletne aplikacije
- OWASP – [www.owasp.org](http://www.owasp.org)
- OSSTM - <http://www.isecom.org/osstmm/>
- Microsoft predlog za varnost v agilnih življ. ciklih:
  - [http://www.blackhat.com/presentations/bh-dc-10/Sullivan\\_Bryan/BlackHat-DC-2010-Sullivan-SDL-Agile-slides.pdf](http://www.blackhat.com/presentations/bh-dc-10/Sullivan_Bryan/BlackHat-DC-2010-Sullivan-SDL-Agile-slides.pdf)

# OOB distribution of passwords

- banke navadno ne pošiljajo gesel po internetu

- ali obstaja proces v e-banki?
  - povezanost z zunanjimi akterji
  - realno je pričakovati, da imajo banke z več incidenti boljši proces
- kdaj je dosegljiva podpora uporabnikom?
- ali uporabniki vedo, kako postopati v primeru suma zlorabe?
- kakšen je odnos podpornikov do uporabnika, ki želi prijaviti sum zlorabe ali ranljivosti – ga poskuša »odpraviti« po liniji najmanjšega odpora ali resno obravnava njegove sume?
- geslo za blokiranje uporabniškega računa



- Gartner group - Magic Quadrant for Web Fraud Detection, <http://www.entrust.com/resources/download.cfm/23683/>
- Entrust - <http://www.entrust.com/fraud-detection/>
- Norkom Technologies - <http://www.norkom.com/>
- RSA Fraud Action & Transaction Monitoring-  
<http://www.rsa.com/node.aspx?id=3020>,  
<http://www.rsa.com/node.aspx?id=3069>
- Oracle Adaptive Access Manager -  
<http://www.oracle.com/products/middleware/identity-management/adaptive-access-manager.html>
- Rešitve, ki so sestavni del specifične aplikacije, se lahko prožijo ob bolj subtilnih dejanjih – npr. poskus SQL injectiona, tamperinga...
- Interakcija z drugimi procesi (npr. clearing točka)

# Revizijska sled



- revizijska sled – beleženje IP v času prijave in času transakcije (ali je enak?),
- pošiljanje revizijske sledi na neodvisen strežnik



- revizijska sled – beleženje IP v času prijave in času transakcije (ali je enak?),
- ali blokada uporabnika prepreči nadaljnje transakcije v že vzpostavljeni seji?
- digitalna potrdila – ali je digitalno potrdilo konsistentno preverjano skozi spletno sejo, predvsem ob plačilnih transakcijah in podobno občutljivih dejanjih



- »all input is evil«
- setting cookies secure and HTTPOnly
- SSL for password (v slo dosledno srečamo)
- XSRF countermeasures
  - [http://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery\\_\(CSRF\)\\_Prevention\\_Cheat\\_Sheet](http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)
- Pravilna uporaba SSL
  - <http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>



- PCI DSS – Payment Card Industry Data Security Standard, kjer so plačilne/kreditne kartice in PAN (primary account number) številke - <https://www.pcisecuritystandards.org/index.shtml>
- Uporaba t.i. shared secret na različnih komunikacijskih kanalih za avtenetikacijo banke odjemalcu (npr. WWW/SSL, SMS)



- HSM (angl. Hardware Security Module) in TLS/SSL akceleratorji
- IPV6 združljivost/dosegljivost,
- Uporaba DNSSEC za domeno strežnika,
- Pošiljanje revizijske sledi na neodvisen strežnik,
- Ali imajo e-banking na dveh oddaljenih lokacijah in koliko časa je potrebno za aktiviranje druge lokacije,
- Secure piškotki (angl. cookies), izogibanje mešanja SSL in ne-SSL delov spletne strani strani

- Avtentikacija uporabnika, potrjevanje in verifikacija transakcij
  - deljena odgovornost za potrjevanje transakcij (pride v poštev za organizacije)
  - digitalni podpisi transakcij
  - avtentikacija odjemalca z SSL
  - pametne kartice / USB ključki
  - WPKI – Wireless PKI
  - Passwindow – [www.passwindow.com](http://www.passwindow.com)

- Avtentikacija uporabnika, potrjevanje in verifikacija transakcij
  - ZTIC – IBM <http://www.zurich.ibm.com/ztic/>
  - EMV CAP card + reader
  - SMS OTP transaction verification
    - uporabnik dobi SMS s podrobnostmi transakcije in s potrditveno kodo za to specifično transakcijo
  - Preverjanje transakcije po glasovnem kanalu s klicem na znano telefonsko številko uporabnika (angl. Out of band - voice channel transaction verification)
  - Digitalni podpis s tipkovnico in prikazom na čitalniku pametnih kartic

- Obveščanje uporabnikov – večine tega banka ne more zagotavljati kot sistematičen ukrep
- Trusteer Rapport -  
<http://www.trusteer.com/solutions/home-users/online-security>
- Ironkey in podobne (drage?) rešitve, ki vzpostavijo bolj varno okolje za brskanje
- Anti-☠ware
- Posodobitve
- Za techno-freake:
  - Live CD – read only OS na CD, s katerega uporabnik dostopa do e-banke
  - Virtual machine reverting to initial state – similar as Live CD

- menjava privzetih gesel na hišnem usmerjevalniku
- uporaba pametnih kartic, kot varnega medija za hrambo digitalnih potrdil
- zaščita elektronskih identifikacijskih elementov v primeru hrambe na disku (servis, služba, ...)
- Uporaba uporabniških profilov ki onemogočajo nameščanje programske opreme in spremembe sistemskih nastavitev računalnika
- Uporaba zadnjih različic požarne pregrade, brskalnika, operacijskega sistema.
- Odpornost na lažne strani spletne banke z nastavitvijo osebnih sporočil, dodatnimi gesli in ignoriranju nepreverjene elektronske pošte.

# Vprašanja, razprava...

- Scenariji ogrožanja
  - Ranljivo okolje e-bančništva
  - Ranljiva bančna oz. ponudnikova stran
  - Ranljiv komitent oz. uporabnik
- Primeri zaščitnih ukrepov
  - kjer je možno, jih bomo navezali na scenarij ogrožanja

