Spletne tehnologije, UL, FRI (VSP)
ST 11 – Varnost

doc.dr. Mira Trebar

http://dilbert.com/strip/2005-08-12

http://dilbert.com/strip/2014-05-19

Varnost spletnih aplikacij

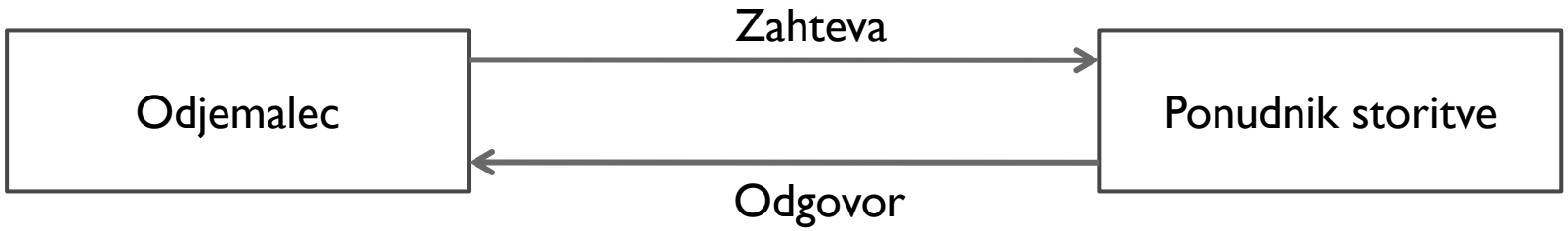
- Uvod
- Vidiki varnosti
- Šifriranje, Digitalni podpisi, Certifikati
- Varna interakcija: Odjemalec-Ponudnik storitve
- Varnost – Odjemalec
- Varnost – Ponudnik storitve

- Kappel, G., Proll, B., Reich, S., Retschitzegger., Web Engineering, John Wiley, 2006, (Poglavje 13, 265-292)

  Ucilnica: Web security.pdf

Uvod

- Spletne aplikacije - varnost



Varnost računalnika
Varnost osebnih podatkov

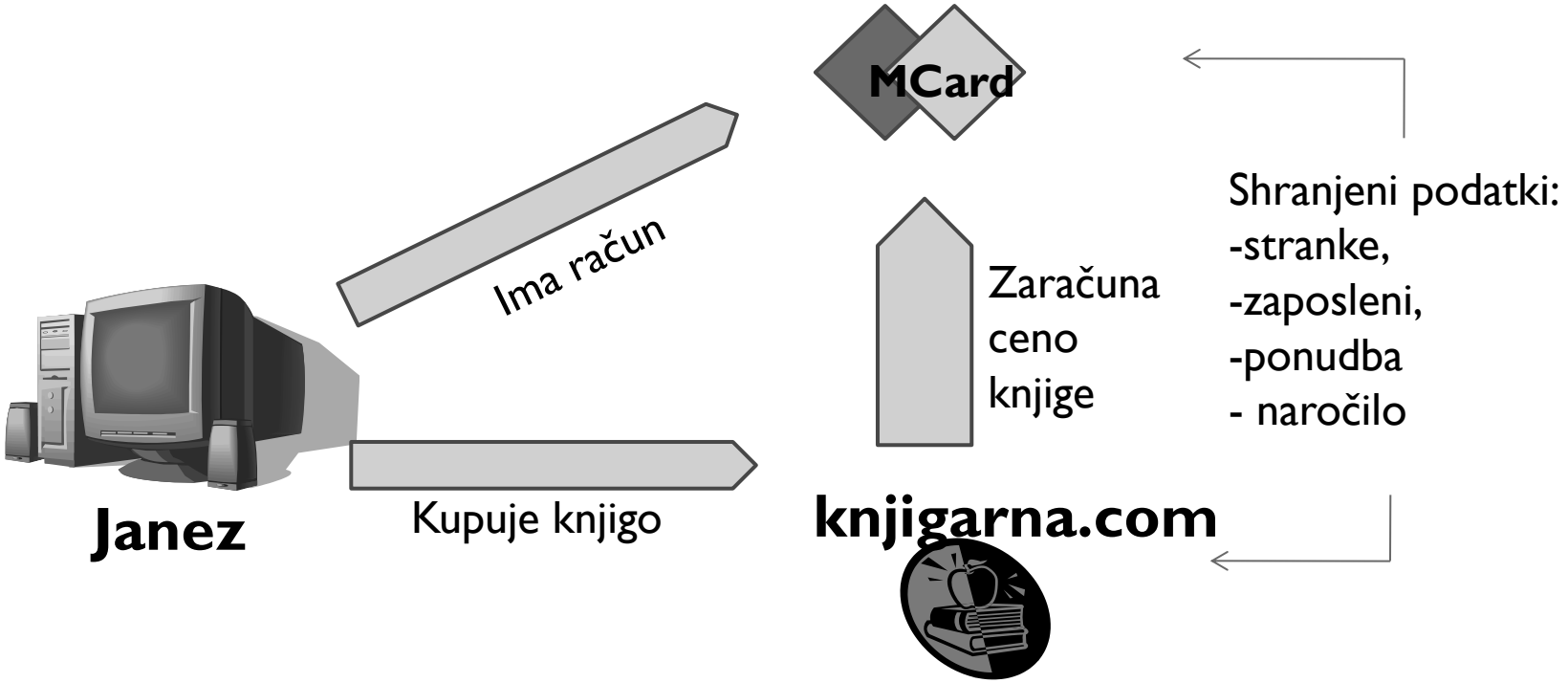
Omrežna varnost
Varna izmenjava sporočil
Ni možna zavrnitev

Varnost gostitelja
Razpoložljivost storitve

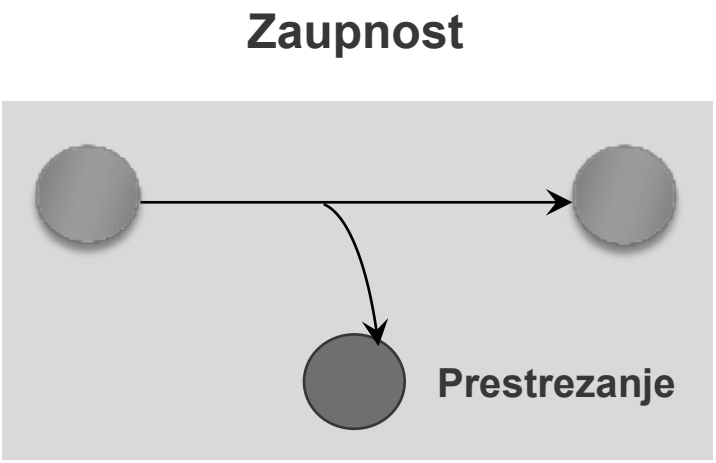
- Uporabnikov računalnik: Zavarovati odjemalca in njegove osebne podatke
- Internet: Varovanje podatkov ob prenosu
- Ponudnik storitve: Varovanje strežnika in tam shranjenih podatkov

Vidiki varnosti

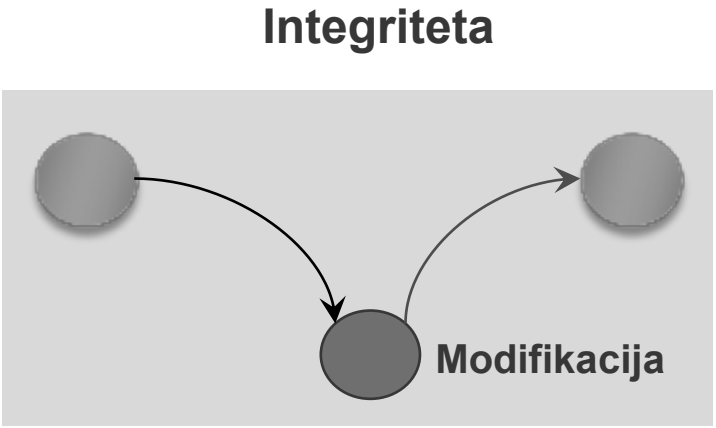
- Transakcija za izvedbo naročila knjige – e-poslovanje:
  - Janez kupuje knjigo v spletni trgovini.
  - Plačilo se izvede z uporabo plačilne kartice.
- Varnost spletnih aplikacij



- Zaupnost ('Confidentiality') – podatki, ki si jih izmenjujeta odjemalec in ponudnik, ne smejo biti dostopni tretji osebi (šifriranje, zasebni kanali, VPN-'virtual private network').

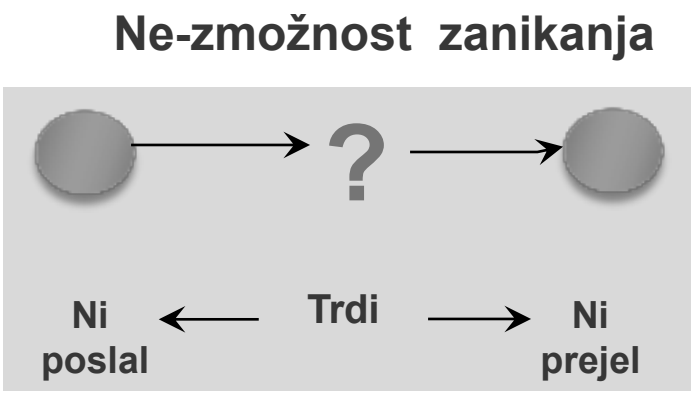


- Integriteta ('Integrity') – neokrnjenost podatkov, nihče ne sme imeti možnosti spreminjanja podatkov, ki se izmenjujejo.



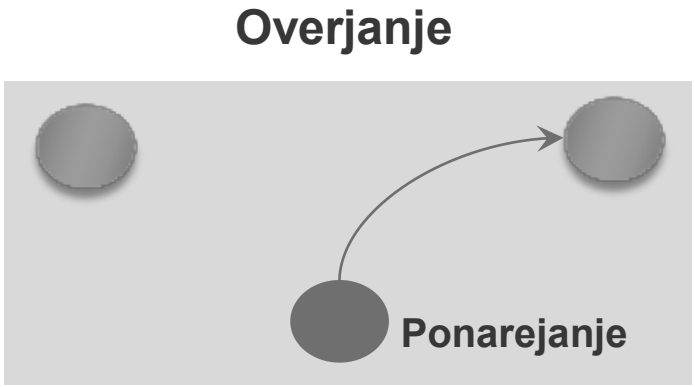
- Ni možno ovreči/zanikati (ni ovrgljiv) ('Non-repudiation') – stranka, ki je izvedla naročilo, nima možnosti zavrnitve ali zanikanja tega naročila.

  Kdo je kaj poslal in kdaj?



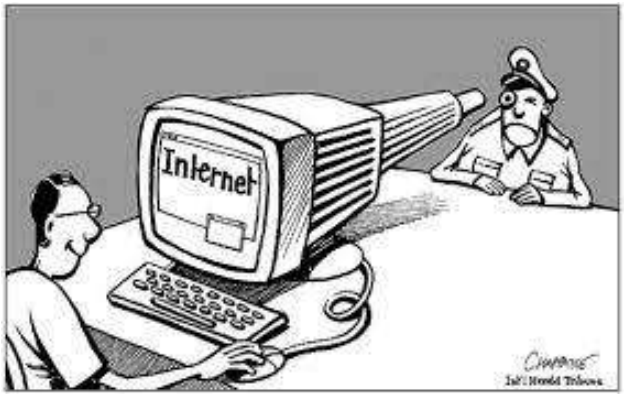
- Overjanje ('Authentication') – dokazovanje identitete osebe ali glavnega subjekta (prijava/geslo).

  Kdo si?



- Avtorizacija ('authorization') – uporabljena za izvajanje pravic overjenih, verodostojnih uporabnikov, ki so jim odobrene.
  - Dostopna kontrolna lista pravic
  - Kontrola dostopa na osnovi vlog

    Kaj lahko narediš?
- Razpoložljivost ('availability') – zagotavlja neomejeno dostopnost spletnih aplikacij – ekonomski pomen.
- Zasebnost ('privacy') – zahteva zaupanja vredno obdelavo podatkov, kot so:
  - osebni podatki (kontaktni podatki, številka kreditne kartice),
  - v lokalnem sistemu shranjene datoteke.

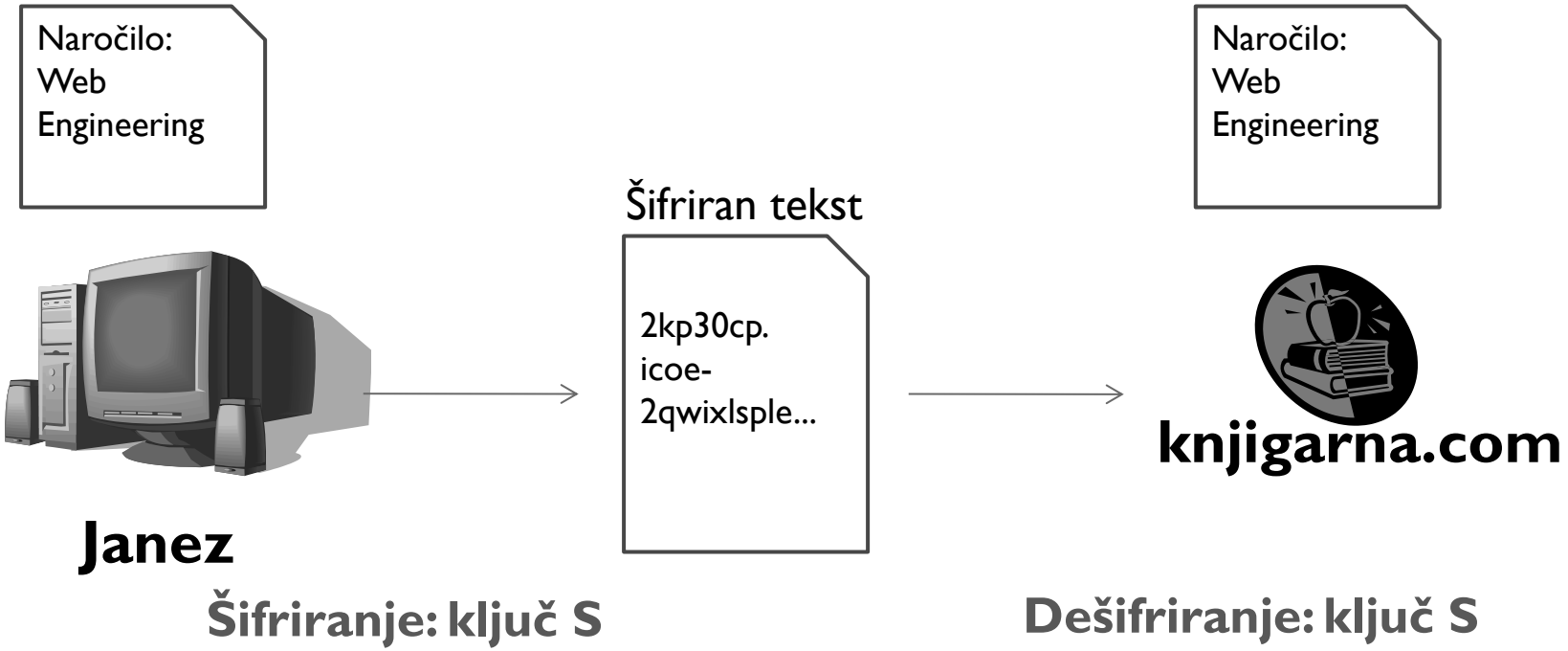


http://beebom.com/5-tools-protect-your-privacy-online/

Šifriranje/Dešifriranje

- Šifriranje ('encryption') -
  - osnovna tehnologija za omogočanje varnega sporočanja.
  - z uporabo matematične funkcije se navaden tekst pretvori v šifriran tekst.
- Dešifriranje ('decryption') - pretvorba šifriranega teksta nazaj v navaden tekst.
- Kriptografski algoritmi - ključi kot tajnost za šifriranje/dešifriranje.
- Brez poznavanja individualnih (zasebnih) ključev dešifriranje praktično ni možno, čeprav so vsi šifrirni algoritmi javno dostopni.
- Algoritem je dober, če je edini možen način napada iskanje vseh možnih ključev.
- Simetrična in asimetrična kriptografija (tajnopis)

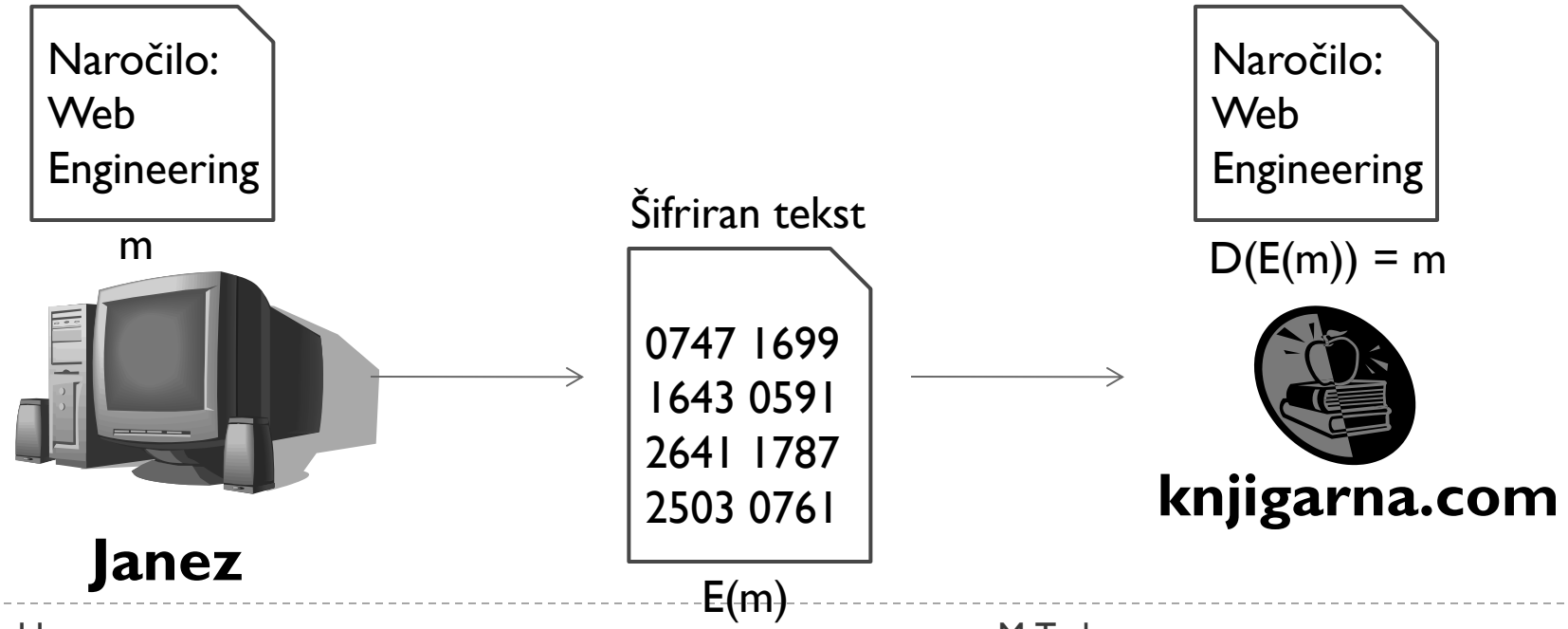
Simetrična kriptografija



- Spreminjanje (šifriranje) podatkov:
  - Skriti ključ S (skrivnost), izmenjava ključa pred izvedbo prenosa
  - Simetrični algoritem:
    - DES (Data Encryption Standarad), 64bitov (vsak 8 bit je pariteta)
    - AES (Advanced Encryption Standard), algoritem Rijndael, 128, 192, 256 bitov

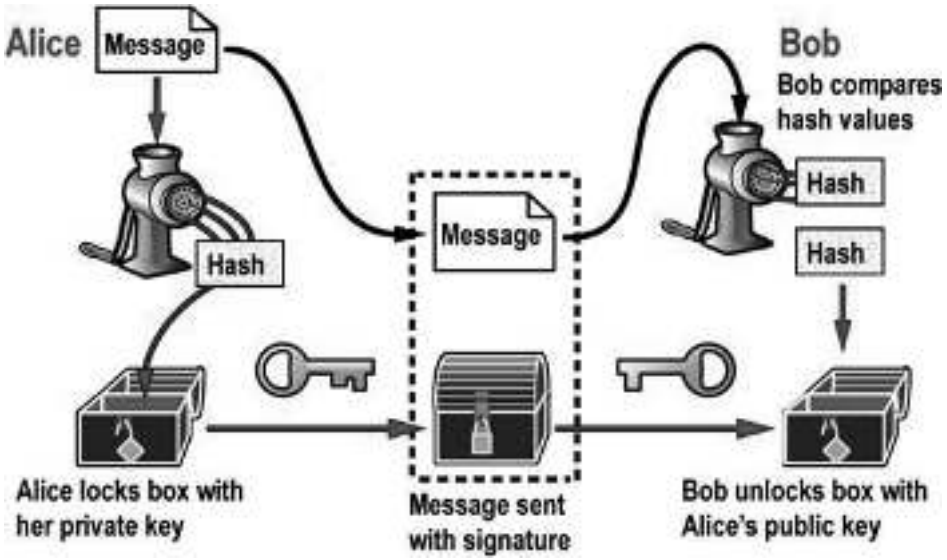
Asimetrična kriptografija

- Uporabljeni so različni ključi (par ključev):
  - Privatni ključ (D) in javni ključ (E), ki je splošno dostopen
  - Janez uporabi za šifriranje sporočila m javni ključ E
  - Knjigarna uporabi javni in privatni ključ za dešifriranje (E,D)
- Asimetrični algoritem šifriranja/dešifriranja (RSA algoritem), razvit na MIT, avtorji so: **R**ivest, **S**hamir, **A**dleman



Digitalni podpisi

- Mehanizem, ki
  - preprečuje spremembo podatkov pri prenosu (integriteta)
  - zagotavlja preprečevanje zavrnitev (ne da se ga zanikati)
  - omogoča dokaz istovetnosti (overjanje)
- Sklicujejo se na:
  - razpršitvene (hash) algoritme – računanje z majhnimi količinami podatkov
    1. MD5-Message Digest algorithm 5,
    2. SHA-1 –Secure hash algorithm
  - Asimetrično šifriranje.



http://www.hill2dot0.com/wiki/index.php?title=Digital_signature

Certifikati in javni ključi

- Certifikati vsebujejo naslednej komponente:
  - Javni ključ
  - Informacijo o certifikatu (lastnik, veljavnost)
  - Digitalni podpis
- Certifikate podeljuje overitelj (CA-Certification Authority)
- Identiteto lastnikov certifikatov preverja agencija za registracijo (RA – Registration Authority).
- X.509 digitalni certifikati so:
  - tehnologija za zagotavljanje zanesljive razdelitve ključev za spletne aplikacije.
  - uporabljeni za vzpostavitev varne SSL povezave.
  - uporabljeni zato, da se poveže javni ključ z identiteto lastnika privatnega ključa.
- Obdobje veljavnosti

Varna interakcija (Odjemalec/Strežnik)

- Varnost 'Point-to-Point' – uporaba protokolov:
  - SSL (Secure Sockets Layer)
  - TLS (Transport Level Security)
- Varnost 'End-to-End' - 'online' transakcije, ki vključujejo več kot dve stranki

  Primer nakupa knjige:, kjer ima knjigarna:
  - posredniško vlogo
  - ne zahteva podatkov o kreditni kartici kot navadni tekst
  - komunikacija med Janezom in knjigarno je navaden TLS (Transport Layer Security)
  - komunikacija med Janezom in Mcard je 'End-to-End'
  - varnost na nivoju sporočila – informacija je varna v sporočilu
- Overjanje uporabnika (identiteta): prijava/geslo, digitalni certifikat
- Avtorizacija uporabnika (pravice): identita in drugi parametri

Varnost – Odjemalec

- Transakcija – izmenjava osebnih podatkov.
- Vspostavitev zaupanja s ponudnikom storitve - vprašanji:
  - Kako so podatki shranjeni pri ponudniku storitev?
  - Zakaj ponudnik storitve uporabi podatke?
- Ohraniti zasebnost:
  - P3P (Platform for Privacy Preferences) - standard za varovanje podatkov v XML.
  - P3P agenti (brskalniki, vtičniki) – stran se prikaže, če ni konflikta v zasebnosti
- Varnost kode, ki se izvaja/interpretira v brskalniku:
  - dinamične spletne strani: JavaScript, Java applet, ActiveX ogrodje
  - E-trgovina (prikaz posamezne strani za izvedbo nakupa)
- Ribarjenje (phishing) in lažno predstavljanje (web Spoofing)
- Namizna varnost: Oglaševalsko programje (Adware), Vohunsko programje (Spyware),, Virusi (Viruses), Črvi (Worms), Trojanski konji (Trojan horses)

Varnost – Ponudnik storitve

- Napadi na spletne aplikacije - razvijalci:
  - dobijo natančno predstavo o izvedbi varnih storitev,
  - Imajo informacije o preprečevanju tipičnih varnostnih pomanjkljivosti.
- Cross-Site scripting (XSS napad)
- SQL injection – napad na spletno aplikacijo
- Dostopnost storitve:
  - Zavrnitev storitve – uporabniku je onemogočen dostop zaradi preobremenitve (CPE, pomnilnik)
  - Prekoračitev vmesnega pomnilnika pri vnosnih poljih – program se sesuje
- Varnost gostitelja
  - Konstantno posodabljanje sistema
  - Nadzor in pregledovanje varnostnih pomanjkljivosti

- Kako zavarovati spletne aplikacije:
  - http://www.it.northwestern.edu/policies/webapps.html
  - **OWASP Guide Project,** https://www.owasp.org/index.php/OWASP_Guide_Project