Fakulteta za računalništvo

Seminarska naloga

Ali je kupovanje preko interneta varno - www.eon.si?

november, 2000

Marko Hrastovec

UVOD

Trgovine, ki imajo svoje prodajalne tudi na internetu, morajo svojim kupcem zagotoviti varno trgovanje. Če bodo uporabniki mnenja, da trgovina ni dovolj varna, ne bodo v njej ničesar kupili. Trgovanje preko interneta pa po mnenju trgovcev postaja zelo pomembno v boju s konkurenco. Analitiki ocenjujejo da naj bi bilo čez 10 let okoli 10% prometa opravljenega z nakupi preko interneta. To pa ni zanemarljiva številka. Kdor torej ne bo imel trgovine tudi na internetu, ali pa le ta ne bo omogočala varnih transakcij, bo v hudem zaostanku.

Kaj pa pomeni varnost transakcij v internetu? Problemi so isti kot v običajni trgovini. To pomeni, da se v transakcijo ne sme vriniti tretja oseba, ki bi na kakršenkoli način prišla do zaupnih podatkov. Ljudje se najbolj bojijo, da bi nekdo lahko prisluškoval njihovemu »pogovoru« s trgovino in bi jim ukradel številko kreditne kartice, s katero bi potem kupoval na njihov račun.

Če internet trgovine uporabljajo dovolj dobre varnostne ukrepe proti napadom, je možnost zlorabe precej majhna. Problem nastane, če trgovina ne uporablja šifriranja pri trgovanju preko omrežij. V tem primeru lahko vsak prisluškovalec ve, kakšni podatki se prenašajo po mreži. Nobena resna trgovina pa si tega ne upa privoščiti. Ker kupci ne znajo oceniti, kdaj je trgovanje preko interneta varni in kdaj ne, mora trgovina zagotoviti varne prenose podatkov.

V začetku trgovine varnih prenosov niso zagotavljale. Zaradi tega so bile zlorabe preproste in to je nagnalo ljudem strah v kosti. Izvedel sem, da se je neki slovenski trgovini zelo povečal promet, ko so med svoje storitve dodali tudi dostavo po povzetju. Dokler so imeli le možnost plačevanja s plačilnimi karticami, so prodali zelo malo. Verjetno sta za to dva poglavitna razloga:

- pri nas plačevanje s karticami še ni tako razširjeno;
- ljudje se bojijo zlorab in nočejo vpisovati številk svojih kreditnih kartic.

V nalogi sem preučil, kakšne vrste zaščite uporablja zaenkrat edini slovenski ponudnik storitev transakcij za trgovine v internetu.

Najprej bom opisal, kaj se sploh dogaja pri nakupu preko interneta. Kam potujejo podatki in kdo je vpleten pri poteku nakupa.

Potem pa si bomo pogledali, kako je pri posameznih delih transakcije in na strežnikih poskrbljeno za varnost.

Na koncu bom opisal še, kakšne vrste napadov so možne na take trgovine in kakšne so njihove posledice.

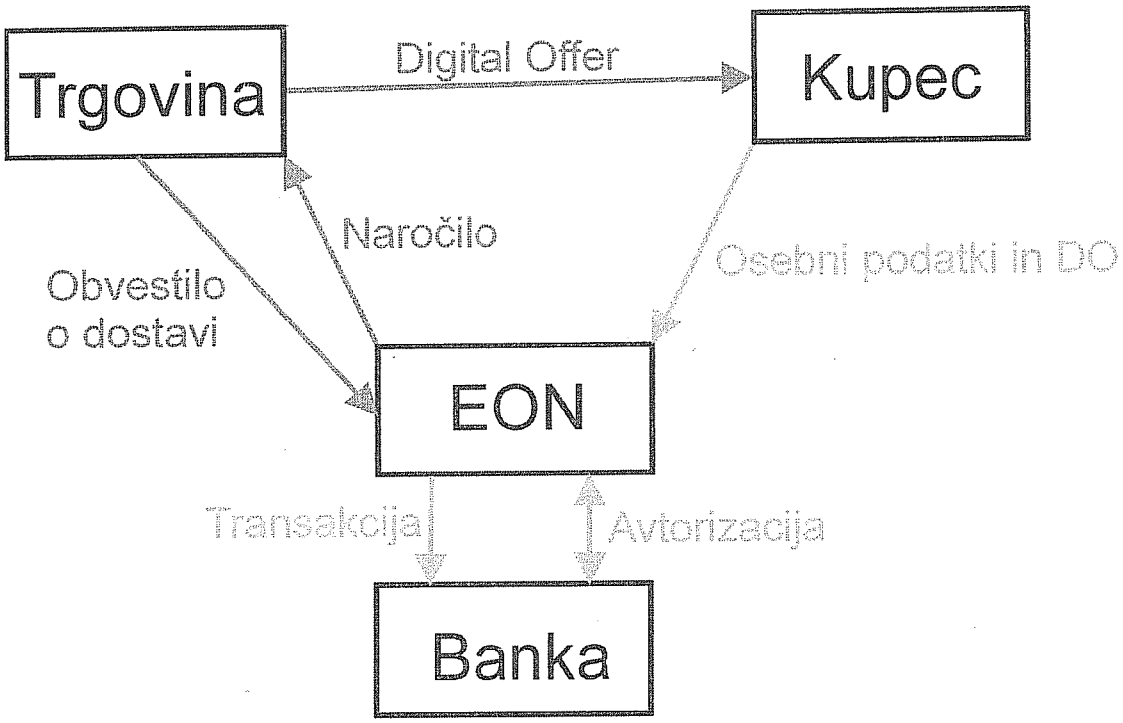
Kako poteka nakup preko interneta

V našem primeru so pri nakupu vpleteni štirje igralci:

- trgovina,
- kupec,
- EON,
- banka.

Trgovina ima podatke o svojih artiklih, ki si jih kupec preko interneta prenese k sebi. Ti podatki so javni in vsebujejo med drugim tudi informacijo o ceni in stopnji davka. Te podatke kupec pošlje na Eon, ko želi izbrani artikel kupiti.

Kupec bi lahko spremenil ceno in poslal spremenjene podatke Eonu, ki ne ve, kolikšna je prava cena artikla. Zato je poleg vsega pri vsakem artiklu še 128 bitni rezultat zgoščevalne funkcije MD5. S tem je zagotovljeno, da se da spremembe podatkov o artiklih hitro ugotoviti, če se rezultati zgoščevalnih funkcij ne ujemajo. Ključe za zgoščevalne ključe si morata strežnika izmenjati vsaj enkrat mesečno.



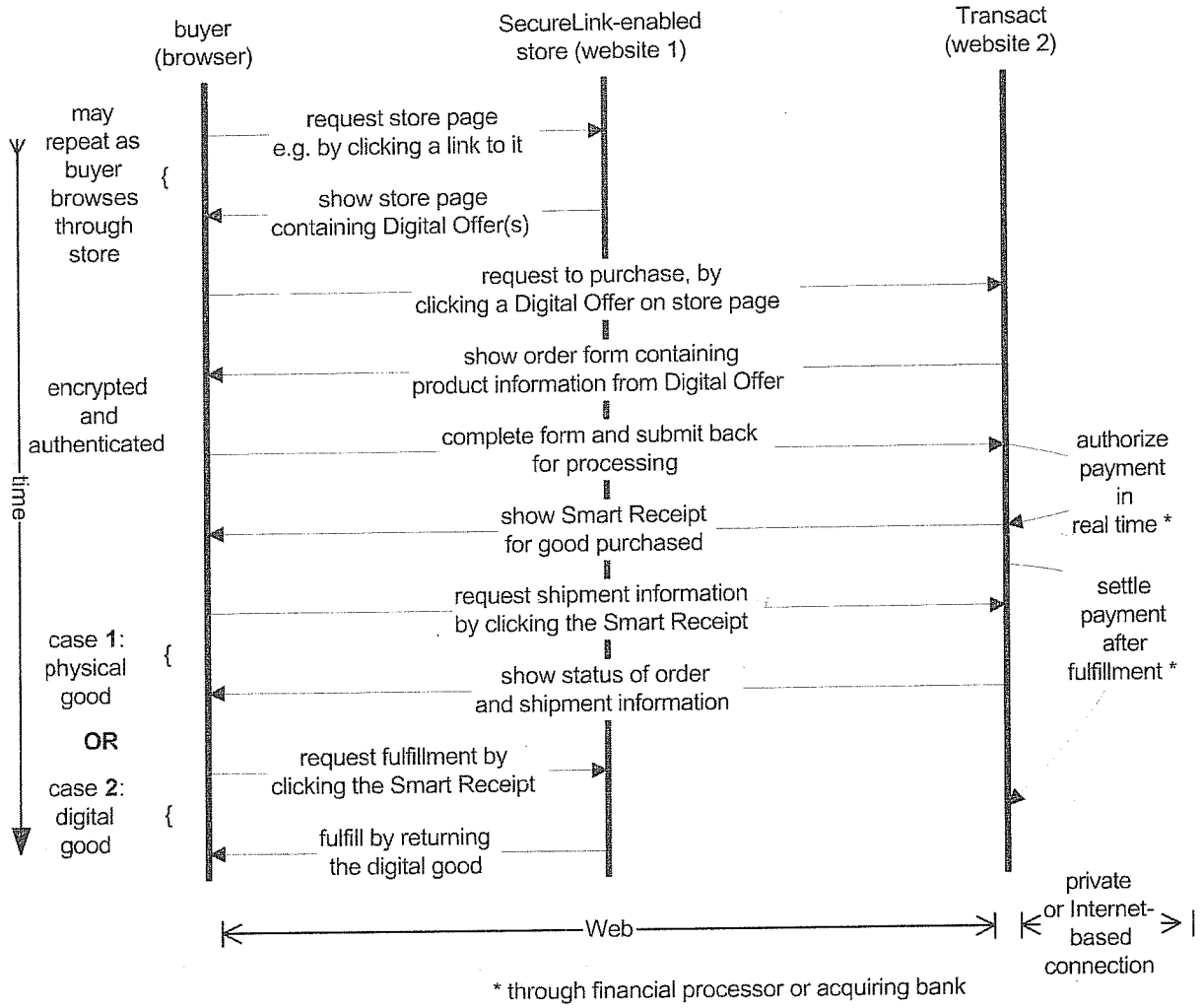
Slika 1: Potek nakupa preko interneta

Strežnik za izvajanje transakcij in avtorizacijo kartic (Transact strežnik) sproti preverja vse podatke o artiklih, ki jih kupci pošiljajo tja. Ko se odločimo za nakup, moramo vpisati številko svoje kreditne kartice in ostale podatke. Od tega trenutka naprej komuniciramo le s Transact strežnikom preko SSL kanala s 128 bitnim ključem. Zato strežnik s podatki o artiklih, ki ga ima trgovina, ne potrebuje varnega SSL prenosa. Vse kar dobimo s strežnika trgovine (vsebinskega strežnika), so javne informacije.

Transact strežnik izvede avtorizacijo kartice. To je možno izvesti na več načinov. Lahko se izvede preko kakšne posebne povezave do banke ali pa spet kar s http protokolom preko SSL kanala. V primeru Eonovega strežnika je vzpostavljena posebna povezava do avtorizacijskega strežnika. To je še posebej ugodno zato, ker sta oba strežnika postavljena v istem prostoru in je kabel dolg le nekaj metrov, kar močno zmanjša možnost prisluškovanja.

Ko je avtorizacija izvedena se kupcu pošlje račun, ki si ga lahko izpiše na papir. Trgovina pa dobi obvestilo o kupljenih artiklih z vsemi potrebnimi podatki, da lahko izda naročeno blago.

Ko trgovina blago zares pošlje naročniku obvesti Transact strežnik, da je bilo blago poslano. Šele takrat se izvede tudi bančna transakcija, ki prenese denar s kupčevega računa na prodajalčev.



Slika 2: Natančna shema poteka nakupa

Na sliki 2 je potek nakupa orisan podrobneje. Na vrhu so napisani vsi vpleteni v proces:

- buyer (kupec),
- SecureLink-enabled store (vsebinski strežnik - trgovina z artikli),
- Transact (strežnik za opravljanje plačilnega prometa).

Z vodoravnimi puščicami so označene komunikacije, ki si sledijo časovno od zgoraj navzdol. Spodaj lahko vidimo, da obstajata dve vrsti dobrin, ki jih lahko ponudimo:

- fizične dobrine in
- digitalne dobrine.

Fizične dobrine mora prodajalec dostaviti na nek način do kupca (pošta, kurirska služba,...). Digitalne dobrine pa si lahko uporabnik po uspešnem nakupu sam presname z vsebinskega strežnika.

Varnost

Za varnost so pomembni predvsem trije elementi. Najpomembnejša sta oba strežnika. Nanju naj bi bilo čim težje vdreti. Tretja šibka točka pa je izmenjava podatkov med tema dvema strežnikoma. Verjetnost prisluškovanja ali nepooblaščene izmenjave podatkov naj bi bila čim manjša.

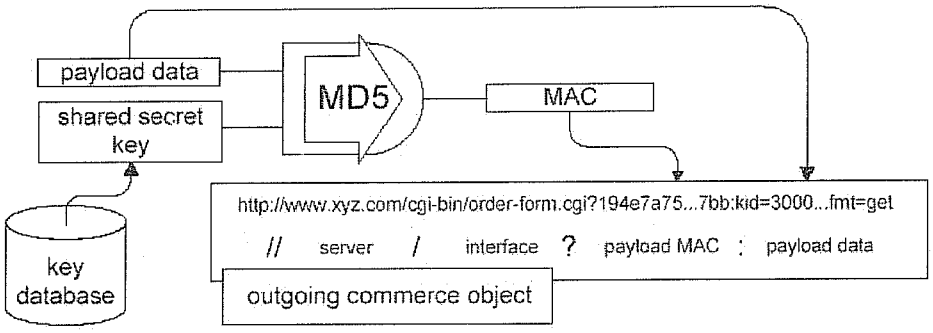
Vsebinski strežnik

Varnost vsebinskega strežnika je odgovornost administratorja tega strežnika. Skrbniki Transact strežnika se z varnostjo vsebinskega strežnika ne ukvarjajo. Informacije na tem strežniku so v glavnem javne. Kritična informacija so ključi za generiranje digitalnih ponudb (Digital Offers). Z ukradenim veljavnim ključem z vsebinskega strežnika si lahko sami naredimo digitalno ponudbo. To pomeni, da si lahko tudi sami izberemo ceno artikla in še marsikaj. Do številk kreditnih kartic ali kakšnih podobnih zaupnih podatkov pa na ta način nikakor ne moremo priti.

Ko sem sam delal trgovino, mi z Eona niso mogli dostaviti programskega paketa za generiranje ključev, ki bi deloval na operacijskem sistemu Linux. Sama trgovina je namreč narejena na takem strežniku. Zato sem se moral odločiti, da se bodo simetrični ključi generirali drugje. Izbral sem računalnik z operacijskim sistemom Windows NT, na katerem ta programski paket deluje. Na tem računalniku se tudi generirajo digitalne ponudbe, ki se potem avtomatsko prenašajo na pravi strežnik.

Ta rešitev je bolj okorna in zapletena. Zaradi nje izgubimo tudi nekaj pomembne funkcionalnosti. Je pa tudi precej bolj varna. Windows NT strežnik je postavljen za požarnim zidom in ni vseskozi dostopen na internetu. Dejaven je le takrat, ko se enkrat mesečno generira nov simetrični ključ in takrat, ko pošilja zgenerirane podatke (digitalne ponudbe) o artiklih na strežnik s trgovino (vsebinski strežnik). Vdiralec ima torej na voljo le zelo kratek

omejen čas, ko je računalnik s ključi prisoten v internetu.



Slika 3: Struktura digitalne ponudbe

Tole je primer digitalne ponudbe, ki se nahaja na vsebinskem strežniku:

```
http://kastor.eon.si:80/tms-ts/bin/orderform.cgi?H2b4663a7
05c9e1e3b7d4d17ce37c5e56:kid=400561.11&valid=962549885&Vat
Flag=0&goodstype=h&desc=LokomotivaZb20sZb20strojevodjoZb20
-Zb20TomyZbac&domain=5011666065673&weight=440&amt=2172.90&
objtype=do&version=4.0&curl=httpZb3aZb2fZb2fwww.dom.siZb2f
cgi-binZb2figrace_detail.plZb3fEANZb3d5011666065673&VatRat
e=0.19&ss=env
```

Vidijo se vsi glavni podatki o artiklu, ki pa jih kljub temu ne moremo kar tako spreminjati, saj je na začetku shranjen tudi rezultat zgoščevalne funkcije. Dobra stvar take digitalne ponudbe je v tem, da jo lahko damo komurkoli, ki jo želi objaviti.

Transact Server

Transact strežnik je po mojem mnenju najbolj zaželena tarča vdiralcev. Zato mora biti tudi najbolje zaščiten. Najbolj pomembni podatki pa so ključi in podatki o kupcih z njihovimi številkami kreditnih kartic.

Varovanje ključev

Transact strežnik hrani več vrst ključev.

Prvi so ključi, s katerimi šifrira podatke, ki jih zapisuje v relacijske podatkovne baze. Ta par privatnega in javnega ključe je namenjen izključno interni uporabi in zato ni potrebe, da bi ta ključ potrjevali pri kakšni agenciji.

Ti ključi so shranjeni v posebni datoteki, do katere imata dostop le »superuser« in »Transact user«. Šifrirani so z geslom, ki ga poda operator, ki upravlja s strežnikom.

Drugi so simetrični ključi za MD5. Ti so tudi shranjeni v posebni bazi. Iz dokumentacije se ni dalo razbrati, če so v bazi šifrirani ali ne. Sklepam, da niso, ker jih strežnik zelo veliko uporablja in bi mu dešifriranje vzelo preveč časa. Mislim pa tudi, da bi bilo posebno poudarjeno v dokumentaciji, če bi bili šifrirani.

Tretji pa so ključi za vzpostavitev varnega SSL prenosa. To vrsto prenosa strežnik uporablja za več namenov:

- za komunikacijo z uporabnikom, ko ta vpisuje svoje osebne podatke in
- z vsebinskim strežnikom, kadar si izmenjujeta ključe.

Hranjenje podatkov o plačilnih karticah

Prva zelo pomembna zaščita je ta, da se nikoli na noben račun, dobavnico, naročilo,... ne izpiše celotna številke kartice. S tem se izognemo skušnjavam, ki bi lahko zapeljale zaposlene, ki imajo opravka s temi dokumenti. Ni pa tudi tako nevarno, če kdo te dokumente ukrade. Seveda dokumenti vsebujejo vse ostale potrebne podatke, ki so potrebni, da lahko kupljeno blago dostavijo, izstavijo račun,...

Na disk pa se podatki o kreditni kartici zapišejo v posebni obliki, ki je opisana tule.

- Vsi podatki o kartici (številka, tip, rok trajanja,...) so združeni v en niz.

- Generirajo se štirje naključni biti in se vstavijo na vnaprej določeno mesto ("soljenje[1]").
- Šifriranje z radix64[2].
- Generira se naključni DES ključ.
- Zašifrira se informacija o kartici z DESom.
- DES ključ se zašifrira z javnim delom nesimetričnega ključa "data security key".
- Združi se šifrirana informacija o kartici in DES ključ v en niz.
- Vse skupaj se še enkrat zašifrira v radix64 in v taki obliki shrani na disk.

Ko strežnik potrebuje podatke o kartici izvede opisan postopek v obratnem vrstnem redu z ustreznimi ključi.

Naključni biti za »soljenje« se dodajo za otežitev napada s slovarjem.

Radix64 se uporablja zato, da ni problemov pri shranjevanju v relacijsko bazo podatkov ali pri uporabi s kakšnim drugim programom, ki bi ga kakšni nestandardni ASCII znaki uspeli zmesti.

Izmenjave ključev

Izmenjava ključev poteka po naslednjem postopku:

1. Vsebinski in transakcijski strežnik zgenerirata vsak svoj par privatnega in javnega ključa. Oba strežnika morata imeti vsak svoj certifikat za varni SSL prenos. Vsebinski strežnik nato uporabi program, ki ga dobi od lastnika Transact strežnika. S tem programom se pošlje certifikat, uporabniško ime in geslo do transakcijskega strežnika. Ta odgovori s svojim certifikatom. Oba uporabita javne ključe, da preverita digitalne podpise in se prepričata o identiteti strežnika na drugi strani. S tem vzpostavita varni SSL kanal preko katerega lahko komunicirata.
2. Vsebinski strežnik zgenerira simetrični ključ za generiranje MAC za objekte prodaje ("Commerce Objects").

---

[1] Vstavljanje naključnih bitov v informacijo na vnaprej določena mesta. S tem se oteži napad s slovarjem, ker ne moremo vedeti, kakšen bi moral biti čistopis.

[2] To je bijektivna preslikava, ki en byte pretvori v dva in obratno. V obliki z dvema bytoma so pomembni torej le štirje biti. Ostali pa so izbrani tako, da je znak možno natisniti. V taki obliki se informacija nikoli ne popači pri raznih prenosih.

3. Vsebinski strežnik digitalno podpiše simetrični ključ, ga zašifrira z javnim ključem Transact strežnika in ga pošlje k njemu preko SSL kanala.
4. Transact strežnik odšifrira ključ in preveri digitalni podpis. Če se vse ujema, imata oba nov simetrični ključ.

Simetrični ključ tako potuje preko mreže dvakrat šifriran. Prvič je digitalno podpisan in šifriran z nesimetričnim algoritmom. Potem pa se še dodatno zašifrira pri prenosu preko SSL kanala.

Izmenjava simetričnega ključa mora biti narejena vsaj enkrat mesečno. Zamenjava certifikata (javnega/privatnega ključa) pa vsaj enkrat letno.

Napadi

Spreminanje podatkov o artiklih

Ta vrsta vdora bi nam utegnila koristiti, če želimo popravljati podatke o artiklih. Treba je ukrasti le simetrični ključ. Ker je simetrični ključ tudi na vsebinskem strežniku, je to najlažji vdor. Za vsebinski strežnik skrbi sam prodajalec, ki nima toliko izkušenj z vdori, kot lastnik Transact strežnika.

Na ta način lahko kupujemo artikle s »popustom«, ki si ga sami določimo. Ta način vdora pa nam ne prinese dosti koristi:

- Čez mesec dni je treba ključ ponovno ukrasti, ker mu poteče veljavnost.
- Prodajalec nas lahko hitro odkrije, saj bo verjetno odkril, da nekatere artikle prodaja prepoceni. Potem pa lahko hitro ugotovi, kam jih je dostavil.

Ko bi enkrat imeli dostop do tega strežnika in bi lahko ukradli še certifikat za SSL in še nekatera gesla. V tem primeru pa bi lahko izvedli izmenjavo simetričnih ključev s Transact strežnikom. S tem bi stari simetrični ključ prave trgovine postal neveljaven in se v njej ne bi dalo več kupovati. To vrsto vdora pa bi odkrili verjetno še prej, ker bi trgovina nehala deovati.

Če se lahko izognemo dinamičnemu kreiranju MAC, lahko vse zgeneriramo vnaprej na računalniku, ki je bolje zaščiten. Ob taki konfiguraciji, pa vdiralec na strežniku ne bo našel nobenih pomembnih informacij. Največ kar lahko stori, je, da poskuša doseči ustavitev strežnika.

Kraja zaupnih podatkov

Zaupni podatki se hranijo le na Transact strežniku. Za ta strežnik naj bi skrbeli strokovnjaki s področja računalniške varnosti. Če uspe vdor na ta računalnik, dobi hacker podatke o vseh kupcih iz vseh trgovin, ki jih vodi ta strežnik.

Ta vrsta vdora pa je malo verjetna. Poleg vdora bi si moral vdiralec dobiti še marsikateri privilegij na računalniku preden bi imel dostop do vseh ključev in podatkov. Podatki so namreč razmetani na več mestih.

Če pa bi prišel do vseh ključev in podatkov, pa kraja številk kreditnih kartic ne bi bila noben problem več.

Zaključek

Moje mnenje je, da je kupovanje preko interneta na ta način dovolj varno. Če bodo trgovine uporabljale takšno stopnjo zaščite in varnosti, kot je opisana v tej nalogi, mislim, da bo število zlorab ne bo dosti večje, kot v običajnem poslovanju s kreditnimi karticami. Podatke in prenose bi se dalo tudi še bolje zaščititi, vendar mislim, da za to trenutno še ni velike potrebe. Kljub temu pa je treba biti zelo pazljiv. Večina vdorov se zgodi zato, ker administratorji ne poskrbijo za varnost tako kot bi lahko.

Literatura

1. EON, d.o.o.: Zakaj je kupovati v internetu varno?, http://www.eon.si/prispevki/nakup/poglavje2.asp, 1999-2000
2. Open Market: Security Considerations in Transact, http://www.openmarket.com/, 1999
3. Open Market: The Transact 4 Architecture, http://www.openmarket.com/, 1998
4. Open Market: Internet Commerce: The Open Market Transact Solution, http://www.openmarket.com/, 1998
5. VeriSign: White Paper - Securing Your WebSite for Business, http://www.verisign.com/rsc/gd/srv/secure-bus/secure_web_site_guide.html
6. Netscape: How SSL Works, http://developer.netscape.com/tech/security/ssl/howitworks.html