SZAKDOLGOZAT

Koós Gábor

Debrecen

2010

Debreceni Egyetem
Informatikai Kar

Biztonságos Elektronikus Kereskedelem
(Secure Electronic Commerce)

Témavezető: Dr. Huszti Andrea
Egyetemi Adjunktus

Készítette: Koós Gábor
Mérnök Informatikus

Debrecen
2010

1 Tartalomjegyzék

2 Bevezetés

Az első biztonságos, interneten keresztül zajló kiskereskedelmi tranzakciót 16 évvel ezelőtt hajtották végre. Ennek során egy Sting albumot vásárolt valaki hitelkártyával a Net Market –en.
Az amerikai NetMarket.com alapítója, Daniel Kohn visszaemlékezései szerint a tranzakció során egy főiskolai csoporttársa vásárolta meg Sting Ten Summoner's Tales című albumát CD-n. Az album 12,48 dollárba került, amely összeg a kiszállítás költségeivel egészült ki. A megrendelő hitelkártyával fizette ki a számla ellenértékét, s a tranzakció során felhasznált adatokat titkosítva továbbították a világhálón.
A jeles eseményről a New York Times is beszámolt, s a társaság vezetője ennek kapcsán több országos rádió- és tévéadó műsorában is szerepelt meghívott vendégként.

A Net Market elsősége nem tartott sokáig, a számítógép-alkatrészek online értékesítésével foglalkozó, szintén 1994-ben indult Internet Shopping Network az első e-tranzakció végrehajtása után egy hónappal leköröz te a céget az eladások számában. Az e-kereskedelem későbbi globális népszerűvé válását eleinte több tényező is gátolta: kezdetben a Nemzeti Kutatási Alapítvány szabályzata értelmében mindennemű kereskedelmi tevékenység tilos volt az interneten. Emellett az is nehezítette a biztonságos e-kereskedelmi tranzakciók lebonyolítását, hogy az amerikai kormányzat exporttilalmat rendelt el az erős titkosítást tartalmazó szoftverekre, így azokat az Egyesült Államokon kívül nem lehetett használni

3 Az e-kereskedelem (e-business) folyamata

Elektronikus kereskedelemnek (üzletelésnek) nevezzük mindazon eszközök és eljárások összességét, amelyekkel megvalósítható az áruk, termékek, szolgáltatások és ellenértékük cseréje és az ehhez kapcsolódó adminisztrációt a világhálón keresztül.
Az e-kereskedelem részei:

- az interneten lebonyolított árucsere-tranzakció.
- az áruk ellenértékének interneten történő kiegyesítése
- az eladó és a vevő közötti kommunikáció a tranzakcióhoz kapcsolódóan.

Árucsere-tranzakció: egy adott áru, termék vagy szolgáltatás kiválasztása és megrendelése. Ez az internetes áruházakban bonyolódik, melyekben nyilvántartják az áruk egyedi jellemzőit, a megrendeléseiket és a vevő információkat (tájékoztatás).
Az árucsere-tranzakciót a pénzügyi teljesítés követi (ki kell fizetni).
Módjai:

- hagyományos (kp, átutalás, utánvétel)
- internetes fizetés (hitelkártyás)

(engedély az eladónak, hogy megterhelje a bankszámlánkat; az átutalás a bankok elektronikus rendszerein keresztül történik)

Az e-kereskedelem rendszerek tipikus funkciói:

- a vevő (felhasználó) azonosítása,
- a termék vagy szolgáltatás kiválasztása,
- megrendelés.

A vevő azonosítása:
Regisztráció az ügyfél-nyilvántartásban, a számlázáshoz és kiszállításhoz szükséges adatokkal.
Autentikáció: felhasználónév, jelszó helyességének, érvényességének ellenőrzése.
A felhasználó hozzáférjen saját adataihoz és módosíthassa azokat.

A termék kiválasztása:
Kell egy termék adatbázis a termékek jellemzőinek nyilvántartásához (szövegek, kép, video, audió anyagok tárolása).
Strukturált keresési lehetőség.
Megrendelés előkészítése, kiválasztási (kívánság) lista: kosár

Megrendelés:
A megrendelés ellenőrzése: azt rendelte-e az ügyfél, amit akart.
Szállítási és fizetési mód kiválasztása.
Megrendelés jóváhagyása.
Visszaigazolás például e-mail-ben

Egy egyszerűsített modell elemei:

- web szerver, a webes felület kezelésére. A felhasználó közvetlenül ehhez csatlakozik.
- alkalmazás szerver (tranzakciós), a felhasználó által indított műveleteket elvégzésére.
- adatbázis szerver, az alkalmazás szervert adatokkal látja el, illetve tőle adatokat fogad.

Az e-kereskedelmi rendszer kapcsolatai.
Nem önmagában áll, integrálni kell a vállalat informatikai rendszerébe. A vállalat készlet-nyilvántartási, pénzügyi-számviteli és logisztikai rendszerébe kell főként bekapcsolódnia.
Meg kell oldani a visszáru kezelés mellett, a reklamációk kezelését.

Az e-kereskedelem fajtái
B2C, Business to Consumer: kiskereskedelmi értékesítés.
A legismertebb és leglátványosabb kapcsolati forma a B2C, mely a vállalkozások és fogyasztók közötti online kapcsolatot jelenti. Térhódítása a ’90-es években kezdődött, az internet széleskörű elterjedésével. Bár az elektronikus értékesítés bevétele lényegesen alacsonyabb, mint a B2B esetén, az üzletkötések száma jelentősen meghaladja azt. A B2C kereskedelmet legtöbbször az online kiskereskedelemmel azonosítják, ennek fő oka, hogy a

tranzakciók nyílt hálózaton, az interneten keresztül jönnek létre, így mára ez a kereskedelmi forma a hétköznapi élet részévé vált.

Jellemzője:

- egy eladó – sok egyedi vevő,
- nagy mennyiségű, de egyenként kisösszegű tranzakció,
- viszonylag homogén árukészlet,
- a megrendelések termékben, időben rosszul becsülhetőek,
- egy ügyfél regisztráció egy személyt jelent.

B2B, Business to Business: vállalatközi kereskedelem

A B2B a vállalatok, vállalkozások közötti online kapcsolatot jelenti. Az interneten történő kereskedelem kb. 80%-át a B2B kereskedelem teszi ki. A vállalatok között a teljes értékesítési lánc, amely akár az alapanyag megrendelésétől kezdve az üzleti kommunikációkon keresztül a teljesítésig terjed, elektronizálva lehet.(Nagykereskedő – kiskereskedő, vállalat – vállalat)

Jellemzője:

- a rendelések nagy volumenűek, több áruféleséget tartalmaz,
- egy regisztrációhoz több személy tartozhat,
- egy ügyfélnek több regisztrációja is lehet,
- a rendelések elég jól becsülhetőek.

Az e-piactér, e-beszerzés (B2B Marketplace)

Vagy egy téma köré szerveződnek: pl. gyógyszeripari gépek gyógyszeripari cégeknek.

Vagy tetszőleges beszállítói kör – tetszőleges vevőkör.

Customer-driven: vásárlói oldalról meghatározott, vendor-driven beszállítói oldalról meghatározott.

Nemcsak kereskedelmi, hanem információs szolgáltatásokat is kínálnak (iparági hírek, tenderfigyelés)

C2C Customer to Customer

Napjainkban a fogyasztók közötti online kapcsolat ugyancsak óriási népszerűségnek örvend. Az online portálokon történő aukciókon (www.vatera.hu, www.ebay.com), valamint az

apróhirdetéseken (www.express.hu) keresztül hatalmas mennyiségű áru cserél gazdát a teljes termékskálát lefedve. Az virtuális közösségek, fórumok teret adnak a hasonló érdeklődési körűek számára, hogy megvitassák tapasztalataikat, ötleteiket (http://www.sg.hu/forum.php).

Két természetes személy közötti kereskedés megvalósulása. Hazai példákat említve a teljesség igénye nélkül bolhapiac, pl. www.ebay.com, www.vatera.hu.
A szolgáltató csak az informatikai és jogi hátteret biztosítja, bizonyos ellenértékért cserébe. Úgy, mint web szerverek, adatvédelem és ezek megfelelő védelme, melyekből a felhasználó csak a webes felületet látja.
A kereskedő felek egyike sem a szolgáltató üzletkötője.

B2A Business to Administration

Az elektronikus kereskedelem egyik típusa, amikor az elektronikus úton létrejött üzlet az üzleti élet egyik szereplője és a kormányzat között történik, a közigazgatás és az üzleti szektor közötti ügyleteket foglalja magában. A B2B részterülete is lehet, ahol az egyik fél mindig valamilyen közigazgatási szerv.

C2A Consumer to Administration

A közigazgatás és magánszemélyek közötti elektronikus ügyletek elnevezése. A lakosság és a helyi vagy központi hivatalok közötti online ügyintézést jelenti. Ide tartozik az egészségügyi szolgáltatás, az oktatás, igazolások, engedélyek igénylése, pályázati űrlapok elérése vagy akár az online választás lehetősége is.
Példaként említve, mára a megfelelő infrastruktúra kiépítettségének köszönhetően bármely állampolgár számára elérhetővé vált, hogy elektronikus formában nyújtsa be adóbevallását az APEH-nak. Ezzel lényegesen felgyorsítva a folyamatot.
Vagy egy másik nem minden napos tevékenység végrehajtása. Földhivatali tulajdonlap megtekintése a www.takarnet.hu weblapon. Mindkét művelet végrehajtásához rendelkezni kell a hazánkban egyre inkább terjedő ügyfélkapu nevezetű hitelesítéssel. Ügyfélkapu regisztrációjának elengedhetetlen feltétele a személyazonosság igazolása. Ehhez – amennyiben nem rendelkezik a leendő ügyfél minősített elektronikus aláírással – személyesen meg kell jelennie valamelyik Okmányirodában.

Egyéb e-kereskedelmi formák

Internetes banki rendszerek.

Speciális megoldásokat igényel:

- biztonság,
- az e-banki műveleteket át kell fordítani a back-Office (háttér) számára érthető tranzakciókká.

Főbb részei:

- web szerver: a prezentációs réteget szolgáltatja
- tranzakciós szerver: a felhasználóktól kapott utasításokat végrehajtja (pl. átutalás)
- adatbázis szerver: autentikáció, személyes adatok, korábbi banki műveletek nyilvántartása, szolgáltatása a tranzakciós szervernek
- back-Office előtétrendszer: segítségével a tranzakciós szerver átadja a felhasználó által indított tranzakciókat a bank háttérrendszerének, illetve a banki üzenetek továbbítása az e-bank adatbázisába illetve a tranzakciós szerverhez.

A tranzakciós szerver illetve a back-Office előtét általában egyedi fejlesztés.

Az e-kereskedelem biztonsága

Jogi oldalról ide tartoznak:

- személyes adatok védelme,
- információs önrendelkezési jog,
- az ajánlattétel és szerződéskötés jogi vonzatai (területi hatály)

Üzleti oldalról:

- szerződésben vállalt kötelezettségek.
- technikai okokra visszavezethető nem teljesítési.
- termékazonossági kérdések.

Műszaki oldalról:

Az e-kereskedelmi rendszert műszaki oldalról úgy kell kialakítani, hogy az a hatályos törvényekben, jogszabályokban és szerződésekben vállalt kötelezettségeknek eleget tudjon tenni. A hardveres eszközök a fent említett szabályzásoknak maximálisan eleget tegyen.

Illetéktelen fizikai behatolások és természeti csapások ellen védve legyen a rendszer. Néhány példa: Tűz-víz biztos helyiség, megfelelő nagyságú szünetmentes tápegység.
Adatbiztonság: Szoftveres technikai-műszaki fogalom – a tárolt adatok sérülés, véletlen vagy jogosulatlan módosítás, jogosulatlan hozzáférés (adatlopás) ellen védve legyenek: autentikáció, archiválás, vírusok elleni védekezés, titkosítási eljárások.
A két leggyakoribb veszély:
Feltörés: (Hardveres) pl. hitelkártya adatok megszerzése: kártyaszám, név, PIN kód
DoS attack (Denial of Service)(Szoftveres) a web szerverre hirtelen több kérés érkezik célzottan ártó szándékkal, mint amit az fel tud dolgozni. Ennek következménye teljes rendszer leállás vagy akár adatvesztés is lehet.

Az üzleti értelemben vett megbízhatóság kérdései:
Hitelesség: Kiszolgáló hitelesítése az ügyfélbiztonság érdekében. Ezzel elnyerhető az ügyfelek abszolút bizalma anélkül, hogy személyesen találkoznának a szolgáltatóval vagy egymással.
Sértetlenség: A tranzakcióhoz tartozó adatok megmásíthatatlansága.
Letagadhatatlanság: Tranzakciók nyomon követhetősége.

E három probléma megoldása:
PKI (Public Key Infrastructure) alapú elektronikus aláírás.
A titkosítás, digitális hitelesítés és azonosítás meghatározó architektúrája a PKI (Public Key Infrastructure - nyilvános kulcsú infrastruktúra). Ennek központi komponense a CA (Certificate Authority - Hitelesítő Hatóság), és az e köré csoportosuló feladatokat (directory szolgáltatás, tanúsítvány-kibocsátás és visszavonás stb.) megvalósító rendszerek.
A PKI rendszer kiterjedt feladatkörre nyújt megoldást egy komplex szoftvercsomag keretében, mely a védelem olyan széles spektrumát lefedi, amit még néhány éve több gyártó több szoftvere tudott csak megoldani. A teljes lefedettségű PKI kiépítési projekt keretében olyan rendszerintegrátori és tanácsadói szolgáltatásokat nyújtunk, mint a szabályozás kialakítása, rendszertervezés, szerverkörnyezet kialakítása, hálózati integráció, széles körű biztonsági megoldások, projektmenedzsment.

Az elektronikus aláírás olyan kriptográfiai eljárás, amelynek segítségével joghatás kiváltására alkalmas, akár a kézzel írott aláírással vagy a közjegyző előtt tett aláírással egyenértékű bizonyító erejű dokumentum hozható létre a hatályos jogszabályok, elsősorban az elektronikus aláírásról szóló 2001. évi XXXV. törvény szerint.

Három kategóriába sorolható:

- A **minősített elektronikus aláírás** a legmagasabb biztonsági szintű elektronikus aláírás. A minősített aláírás olyan fokozott biztonságú elektronikus aláírás, amely minősített tanúsítványra épül, és amelyet biztonságos aláírás-létrehozó eszköz (pl. egy speciális minősítésű intelligens kártya, avagy chipkártya) segítségével hoztak létre. A minősített elektronikus aláírás mindenképpen kriptográfiai technológiákra - jellemzően PKI-re és X.509 tanúsítványokra - épül, a Nemzeti Hírközlési Hatóság által meghatározott kriptográfiai algoritmuskészletek alapján.
- A **fokozott biztonságú elektronikus aláírás** a minősítettnél alacsonyabb biztonsági szintet képvisel, sokkal kevesebb szabály vonatkozik rá. A fokozott biztonságú aláírás is kriptográfiai megoldásokra épül, de nem feltétlenül PKI alapú, a szükséges követelmények akár PGP segítségével is teljesíthetőek. Például, egy fokozott biztonságú elektronikus aláírás esetén:
    - nem feltétlenül történt személyes azonosítás,
    - az aláírás-létrehozó adatot nem feltétlenül védi intelligens kártya,
    - a hitelesítés szolgáltató nem feltétlenül vállal felelősséget a tanúsítványért stb.
- **Fokozott biztonságúnak nem minősülő elektronikus aláírás**. Az elektronikus aláírásról szóló törvény (Eat) szerint létezhet olyan elektronikus aláírás is, amely nem felel meg a fokozott biztonságú aláírás követelményeinek sem. (Ilyen például, ha valaki odaírja a nevét egy e-mail végére.) Az ilyen aláírásról az Eat. mindössze annyit állít, hogy a bíróság nem utasíthatja el önmagában azért, mert elektronikusan létezik. Az Eat. a 2004. évi módosítás előtt "egyszerű" elektronikus aláírásnak nevezte az ilyen aláírást. A most hatályos törvényben már nem szerepel ez a kifejezés, de néhol még ma is találkozhatunk vele.

Design

A vásárlókat elegáns design-nal, a termékek világos bemutatásával és könnyű kezelhetőséggel kell magunkhoz csábítani. Az igazi hatékonysághoz a kreativitás és a technikai tudás kényes egyensúlyát kell megtalálni:

- ha csak a design-nal törődünk, elveszítjük a funkcionalitást.
- ha csak a programozással törődünk, akkor veszélyeztetjük a látványt.

Bár az eladás a végső cél, de ha a site nem hagy emléket és nem tartja fenn a potenciális vásárlók érdeklődését, akkor az áruház nem lesz sikeres.

E-kereskedelmi site fejlesztési irányelvei:

1. A site frissen tartása: a soha sem változó site nem csábítja a vásárlókat és nem sugallja a visszatérést, nem ébreszt érdeklődést a nézelődőben.
2. Legyen professzionális kinézetű: a site-nak nem csak a terméket, hanem a társaságot is el kell adni. Egy elhanyagolt, hibákkal tűzdelt site, rossz benyomást kelt és az emberek gyorsan elhagyják azt.
3. Legyen a site egyszerű: a vásárló találja meg könnyen, amit akar. Vezesse végig az online vásárlás fázisain az ügyfeleket lehetőleg anélkül, hogy akadályba ütköznének.
4. Megfontoltnak kell leni a technikai újítások bevezetése kapcsán: nem minden potenciális vásárló képes használni a technikai vívmányait site-ot.
5. Átláthatóság szemelőt tartása: a gyengén tervezett web site rengeteg gombbal és linkekkel zavaros útvesztővé válik, amivel sok vásárló nem akar megküzdeni és egy kattintással elhagyja az oldalt.
6. Sablonok használata: célszerű egy rugalmas sablont használni az egész site-on. Ezzel nem csak fejlesztési időt takaríthatunk meg, hanem az egyöntetűség a látogatókra is kedvező benyomást tesz.
7. Kritikus a szervezés: a háttér adatbázist úgy kell elkészíteni, hogy a termékek gyorsan és könnyen előhívhatóak legyenek. Ne célszerű halmozni a választási lehetőségeket és ezzel várakoztatni a vásárlókat.
8. Tisztán tartás: legyenek a lapok egyszerűek és nem zsúfoltak. A túlzottan sok információzavaró és irritáló lehet. A szöveg legyen könnyen olvasható és jól tagolt.
9. Korlátozni kell a grafikus tartalmat: gyorsan kell site-nak betöltődnie. Érdemes tömöríteni a képeket, mellyel meggyorsítható a betöltés és így a kisebb sebességű

internetet használóknak sem okoz majd problémát. Továbbá tartózkodjunk az előugró ablakoktól.

10. Vásárlók elkötelezetté tétele: a haszon egy részét célszerű a megújulásba fektetni. Akkor is erősíteni kell az ügyfél bizalmát, ha nem vásárolt. Online tippekkel is érdemes a szakértelmet bizonyítani. Manapság elterjedt a hírlevél küldése is bizonyos időközönként, mellyel felszínen tartható az érdeklődés.
11. Kommunikációs lehetőség megteremtése: a web-en vásárlók könnyen elcsábulnak. Friss tippek, információk, online kérdőívek, felmérések, társalgási fórumok, gyakori kérdések.

Az E-commerce alkotó elemei

Az E-commerce pénz online átutalása az interneten eladott termékek és szolgáltatások szállítása fejében. Bár ez egyszerűen hangzik, mégis gyakran nehéz meghatározni, hogy mi szükséges az E-commerce folytatásához.

Feladat

- Termék és/vagy szolgáltatás online eladása.
- Megrendelés fogadása, vásárlók nyomon követése.
- Hitelkártya elfogadása fizető eszközként.
- Hitelkártya online/offline feldolgozása.
- Online csekk elfogadás és fedezet ellenőrzés.

Feltétel

- Website, web host, bevásárló kocsi.
- A web site-tal integrált adatbázis.
- Kereskedelmi account.
- Fizetési processzor.
- Automatikus csekkhitelesítés.

A web site-on, a bevásárló kocsin és egy relációs adatbázison kívül még alapvetően 4 dolog szükséges az e-áruház működtetéséhez:

- Web host,
- site biztonság,
- kereskedelmi account,
- fizetési processzor.

A Web host:

Kiválasztása legyen alaposan megfontolt, mivel az áthelyezés költséges, kockázatos és megbontja a korábbi gyakorlatot. Számtalan szolgáltató elérhető, de célravezető a választás előtt alaposan áttekinteni a kínálatot

1. Tervezz:

   Meg kell becsülni a tárigényt, a forgalmat, milyen lehetőségeket kell installálni a szerverre, milyen támogatást igényel majdan.
2. Igények benyújtása:

   Az igények összegyűjtését követően, a listát el kell jutatni a számba vehető szolgáltatókhoz (pl.: biztonságos NT szerver, korlátlan e-mail, 24 órás FTP elérés, tárigény, a használt adatbázis és a web site céljainak körvonalai.

   Egyúttal célszerű ajánlatot kérni ár, rejtett díjak, technikai támogatás, programok installálásának lehetőségének
3. A válaszok kiértékelése:

   A választ nem adók, vagy elérhetetlenek, akikkel a későbbiek folyamán is lehetnek problémák vagy túlterheltek, ami szintén nehezíti a közös munkát
4. Tartsuk szem előtt a tapasztalatot, a specializációt, kapacitást:

   A web site elhelyezéséhez technikai jártasság és megfelelő háttér szükséges: legoptimálisabb szoftver, gyors, megbízható gépek. Biztonság, áramkimaradás áthidalásának megoldása, garantált visszaállás. Ajánlatosabb csak web hostinggal foglalkozót választani.
5. A technikai támogatás elérése:

   Fontos az ügyfélszolgálat, technikai támogatók gyors és könnyű elérhetősége. Az e-mail önmagában kevés.
6. Kapcsolati sebesség:

Nem csak a 24 órás elérhetőség, hanem a gyors elérhetőség is fontos. Fontos lehet a Multi-Home host (Egynél több hálózati interfésszel rendelkező gazdagép) elérése melyet nem minden szolgáltató tud biztosítani. (Tűzfal)

7. Korlátlan felügyeleti hozzáférés:
   Vannak olyan szolgáltatók, akik korlátozzák a karbantartás számát, vagy időszakát. Napi 24 órában szükséges a site tartalmának és az e-mail accountoknak a menedzselése.

Site biztonság

A web áruházad legnagyobb akadálya a vásárlók félelme. A biztonság megalapozza, vagy hiánya tönkre teszi az üzletet. A Netscape 1995-ben vezette be az SSL-t (Secure-Socket-Layer). Az SSL bevezetése (ajándék az e-commerce közösségnek) drámaian csökkentette a tranzakciók kockázatát és növelte a vásárlók bizalmát. Az SSL-lel a vásárló információi csak a kiválasztott kereskedők által használhatóak. Használatához szükséges egy hitelesített tanúsítvány egy megbízható harmadik féltől. Ez egy olyan azonosítási forma, amivel bizonyítható, hogy az vagy, akinek mondod magad. A bizonyítvány (dig. ID) egy elfogadott szervezettől vagy cégtől szerezhető be.
1997.-ben mutatta be a VISA és a MASTERCARD a nagyközönségnek SET-et. (Secure Electronic Transaction). Hosszú évek óta egyik legjobb biztonságos elektronikus tranzakciót nyújtó protokollja. Megjelenését követően hamar az elektronikus fizetések szabványává vált. A SET rendszerkövetelménye igencsak magas a jelentős számításigényű műveletek végrehajtása miatt. Ez egy hitelkártyát használó, online fizetési rendszer, ahol a tranzakciót használó összes résztvevő azonosítva van.

A Kereskedelmi account

A hitelkártya vagy online csekk elfogadása fizetőeszközként nagyon ajánlott, hiszen az internet egy azonnali médium. Ehhez egy kereskedelmi accountra van szükség egy kereskedelmi banktól, mely nem feltétlenül a saját bankunk, hanem egy kereskedelmi accountszolgáltató. Ilyen az OTP-is
Nem érdemes elfogadni az ajánlott szolgáltató eszközöket, gyakran 4-5-ször drágábbak a piaci árnál. Érdemes az interneten kereskedelmi account szolgáltatót keresni.

A fizetési processzor (Payment Processor)

Minden tranzakcióban a következő csoportok vesznek részt:

- az online kereskedő,
- a vásárló,
- a bankod,
- a hitelkártya kibocsátó bankja,
- online processzor, ami az egészet menedzseli.

A tranzakció lépései

1. Authentication (hitelesítés):
   Ellenőrzi, hogy a hitelkártyának érvényes száma van, hivatalosan lett kiadva, nem jelentették ellopottnak.
2. Authorization (érvényesség, jogosultság)
   Van-e elegendő fedezet a vásárláshoz, ha igen, zárolja a megfelelő összeget.
3. Kiegyenlítés
   Teljesítés után, értesíteni kell a bankot, hogy a lefoglalt összeg átutalható a bolt bankszámlájára.

A kereskedelmi account szolgál, a hitelkártyák elfogadására. A fizetéshez szükség van fizetés processzre vagy tranzakció szolgáltatásra:

- kézi feldolgozás (kis volumen)
- automatikus feldolgozás (Real-Time CreditCard Verification)

A kézi feldolgozást akkor választjuk, ha a fizetési processzor nehezen integrálható a web site-hoz.

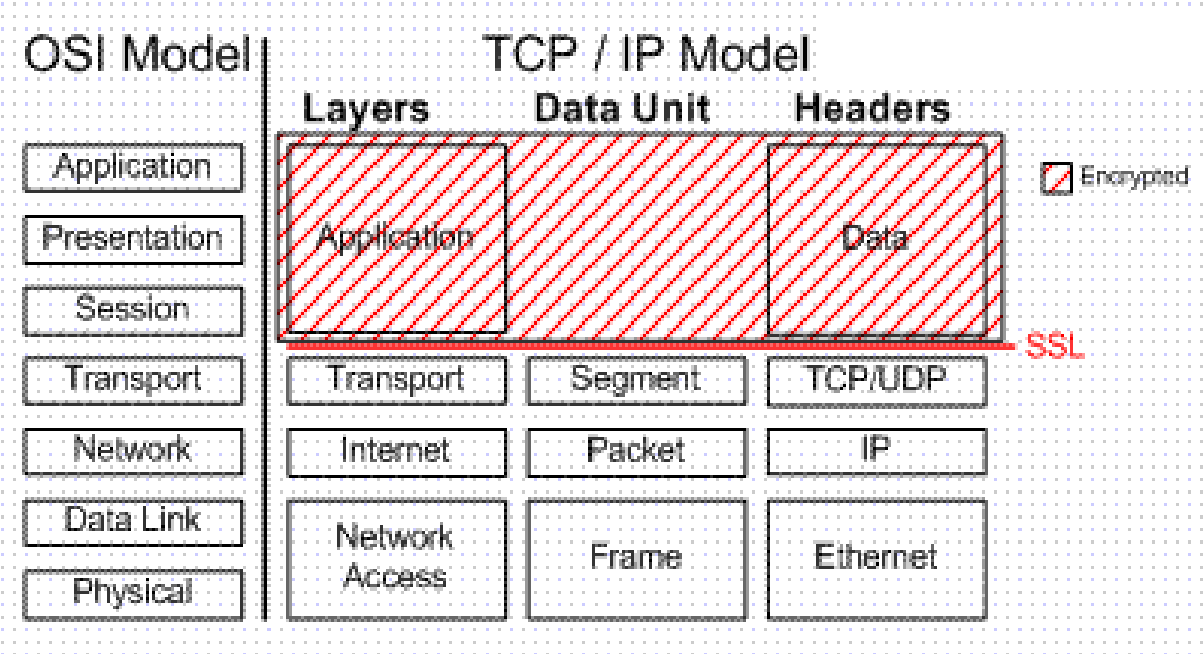
Az automatikus processzorral sok idő takarítható meg. Automatikus feldolgozás esetén a web site együttműködik a fizetési processzel, hogy ellenőrizze a kártyát és végrehajtsa a tranzakciót. Csak a sikeres megrendelésekről kap tájékoztatást.

Amikor a vásárló kitölt egy megrendelőt és megadja hitelkártya adatait, az információk SSL kapcsolaton keresztül küldődnek a fizetési processzorhoz. A PP biztonságos üzenetet küld a hitelkártya kibocsátó bankhoz, ellenőrzi a fedezetet (a kártya aktív, nem letiltott).

Ha a tranzakció érvényes, a bankértesítést küld és zárolja a pénzt. A web site értesítést kap a jóváhagyásról, így a megrendelés elfogadható és feldolgozható. Ezután igazolás küldhető vagy elutasítás a vásárlónak a megrendelésről.

4 Az SSL bemutatása

Az SSL (Secure Socket Layer; Biztonsági Alréteg) egy protokoll réteg, amely a hálózati (Network layer) és az alkalmazási rétegek (Application layer) között van. Mint neve is sugallja, az SSL mindenféle forgalom titkosítására használható - LDAP, POP, IMAP és legfőképp HTTP.



SSL helye az OSI modellben

Az SSL algoritmusok

Háromféle titkosítási technológiát használnak az SSL-el: "nyilvános-titkos kulcs" (Public-Private Key), "szimmetrikus kulcs" (Symmetric Key), és "digitális aláírás" (Digital Signature).

SSL kapcsolat indítása

Ebben az algoritmusban a titkosítás és a visszafejtés nyilvános-titkos kulcspárral történik. A web szerveré a titkos kulcs, a nyilvános kulcsot pedig a tanúsítványban küldi el a kliensnek.

1. A kliens kéri a HTTPS-t használó Web szervertől a tartalmat.
2. A web szerver válaszol egy Digitális Tanúsítvánnyal (Digital Certificate), amiben benne van a szerver nyilvános kulcsa.
3. A kliens ellenőrzi, hogy lejárt-e a tanúsítvány.
4. Ezután a kliens ellenőrzi, hogy a tanúsítványhatóság (Certificate Authority; továbbiakban CA), amely aláírta a tanúsítványt, megbízott hatóság-e a böngésző listáján. Ez a magyarázata annak, miért van szükségünk egy megbízott CA-tól kapott tanúsítványra.
5. A kliens ellenőrzi, hogy a web szerver teljes domain neve (Fully Qualified Domain Name) megegyezik-e a tanúsítványon lévő közönséges névvel (Common Name).
6. Ha minden megfelelő, létrejön az SSL kapcsolat.

Bármelyik kulcs használható titkosításra és visszafejtésre egyaránt (ha annak párját használják visszafejtésre és titkosításra - dacas). Végül is, ha az egyik kulcsot használták titkosításra, a másikat kell használni a visszafejtésre stb. Egy üzenet nem titkosítható és visszafejthető kizárólag a nyilvános kulcs használatával.

A titkos kulccsal történő titkosítás és a nyilvános kulccsal történő visszafejtés biztosíték a címzetteknek arról, hogy a küldeményt a küldő (a titkos kulcs tulajdonosa) adta fel (mivel a titkos kulcs használatához szükséges jelmondatot csak Ő ismeri - dacas). A nyilvános kulccsal történő titkosítás és titkos kulccsal visszafejtés biztosítja azt, hogy a küldeményt csak a meghatározott címzett (a titkos kulcs tulajdonosa) képes visszafejteni.

Szimmetrikus titkosítás - az adatok tulajdonképpeni átvitele: Miután az SSL kapcsolat létrejött, szimmetrikus titkosítást használ az adatok titkosítására, kevesebb CPU ciklust felhasználva. Szimmetrikus titkosításkor az adat ugyanazzal a kulccsal titkosítható és visszafejthető. A szimmetrikus titkosítás kulcsa a kapcsolat indításakor kerül átadásra, a nyilvános-titkos kulcspárral történő titkosítás alatt.

Üzenet ellenőrzés A szerver kivonatot készít az üzenetről valamilyen algoritmus szerint, mint például HMAC, SHA, MD5, majd ezek alapján ellenőrzi az adatok sértetlenségét.

A hitelesség és sértetlenség ellenőrzése

Titkosítási folyamat

- 1. lépés: az eredeti "sima szöveg" titkosítása a feladó titkos kulcsának használatával, ennek eredménye a "titkosított szöveg 1". Ez biztosítja a feladó hitelességét.
- 2. lépés: a "titkosított szöveg 1" titkosítása a címzett nyilvános kulcsával, ennek eredménye a "titkosított szöveg 2". Ez biztosítja a címzett hitelességét (értsd: csak a címzett tudja visszafejteni a szöveget a saját titkos kulcsával).
- 3. lépés: az SHA1 üzenet kivonat (ellenőrző összeg - dacas) készítése a "sima szöveg" alapján.
- 4. lépés: SHA1 üzenet kivonat titkosítása a feladó titkos kulcsával, ennek eredménye a "sima szöveg" digitális aláírása. Ezt a digitális aláírást a címzett felhasználhatja az üzenet sértetlenségének és a feladó hitelességének ellenőrzésére.
- 5. lépés: a "digitális aláírás" és a "titkosított szöveg 2" elküldése a címzettnek.

Visszafejtési folyamat

- 1. lépés: a "titkosított szöveg 2" visszafejtése a címzett titkos kulcsának használatával, ennek eredménye a "titkosított szöveg 1".
- 2. lépés: a "titkosított szöveg 1" visszafejtése a feladó nyilvános kulcsának használatával, ennek eredménye a "sima szöveg".
- 3. lépés: SHA1 üzenet kivonat (ellenőrző összeg - dacas) elkészítése, az előző 2 lépés eredményeként kapott "sima szöveg" alapján.
- 4. lépés: a "digitális aláírás" visszafejtése a feladó nyilvános kulcsának használatával, ennek eredménye az "SHA1 üzenet kivonat".
- 5. lépés: az "SHA üzenet kivonat #1" és "SHA üzenet kivonat #2" összehasonlítása. Amennyiben a kettő egyezik, úgy az üzenet nem módosult az átvitel alatt, így az

Teszt tanúsítványok

Az Apache fordítása közben létrehoztunk egy teszt tanúsítványt. A mod-ssl csomagban lévő makefile programot használtuk az egyéni Tanúsítvány létrehozásához. Erre a

```
# make certificate TYPE=custom
```

parancsot használtuk.
Ezt a tanúsítványt tesztelési célokra használhatjuk.

Tanúsítványok "üzemi" használatra

"Üzemi" használathoz szükségünk lesz egy tanúsítványra valamely Certificate Authority-tól (tanúsítványhatóság) (ezentúl CA). A CA-k a tanúsítványt áruba bocsátók, akik egy megbízható CA listán vannak a felhasználó böngésző kliensében. Ha a CA nincs a megbízott hatóságok listáján, a felhasználó figyelmeztető üzenetet kap, amikor megpróbál kapcsolódni egy biztosított/biztonságos helyhez.
Hasonlóan a teszt tanúsítványokhoz, ez is küld egy figyelmeztető üzenetet a felhasználó böngészőjének.

Hogyan generálhatunk a CSR-t?

A CSR (TAK) vagy Certificate Signing Request-et (tanúsítvány aláírási kérelem) el kell küldeni egy megbízott CA-nak aláírásra. Ez a rész foglalkozik azzal, hogyan generálhatunk CSR-t és küldhetünk el egy általunk kiválasztott CA-nak. Az # openssl req parancs használható erre, az alábbiak szerint:

```
# cd /usr/local/apache/conf/
# /usr/local/ssl/bin/openssl req -new -nodes -keyout private.key -out public.csr
Generating a 1024 bit RSA private key
.....++++++
....++++++
writing new private key to 'private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Seagate
Organizational Unit Name (eg, section) []:Global Client Server
Common Name (eg, YOUR name) []:xml.seagate.com
Email Address []:saqib@seagate.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:badpassword
An optional company name []:
```

"PRNG not seeded" üzenet

Ha nincs /dev/random könyvtár a rendszerünkön, "PRNG not seeded" hibaüzenetet kapsz. Ebben az esetben ki kell adni a következő parancsot:

```
# /usr/local/ssl/bin/openssl req -rand some_file.ext -new -nodes -keyout private.key -out public.csr
```

A "some_file.ext" részt cseréljük ki egy rendszerünkön létező fájl nevére. Bármilyen fájlt megadhatunk. Az Openssl ezt fogja véletlen szám generáláshoz használni.

A Solaris 9 rendszer részeként adnak /dev/random fájlt. Amennyiben Solaris rendszert használunk, elképzelhető, hogy telepítenünk kell a 112438 foltot a /dev/random fájl használatához.

Ezen a ponton pár kérdést tesz fel a szerver helyéről, hogy generálhassa a Certificate Signing Request-et.

Megjegyzés: A közönség béli nevünk (Common Name) a teljes DNS neve (Fully Qualified DNS) a webszerverünknek, például dav.server.com. Ha mást írunk oda, akkor NEM fog működni. A jövőbeli használat érdekében a jelszó megjegyzése nagyon fontos.

Mihelyst befejeződött a folyamat, lesz egy private.key és egy public.csr fájlunk. Szükséges lesz a public.csr fájlt bemutatnunk a CA-nak. Ekkor a public.key fájl még nem titkosított. A titkosításhoz használnunk kell az alábbi parancsokat.

```
# mv private.key private.key.unecrpyted
# /usr/local/ssl/bin/openssl rsa -in private.key.unecrpyted -des3 -out private.key
```

A szerver titkos kulcsának és tanúsítványának telepítése.
Miután a CA feldolgozta a kérésed, visszaküldenek egy kódolt tanúsítványt. A Digitális Tanúsítvány formátumát az X.509 v3 szabvány határozza meg. A következőkben látható egy tipikus, X509 v3 szabvány szerinti Digitális Tanúsítvány felépítése:

- Certificate
  - Version
  - Serial Number
  - Algorithm ID
  - Issuer
  - Validity
  -
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
  -
    - Public Key Algorithm
    - RSA Public Key
  - Extensions
- Certificate Signature Algorithm
- Certificate Signature

Egy Digitális Tanúsítvány ellenőrzése
Egy X.509 Tanúsítvány ellenőrzésére a következő parancsot kell használnunk, ahol a server.crt a Digitális Tanúsítványt tartalmazó fájl neve.

```
# openssl verify server.crt
server.crt: OK
```

A httpd.conf fájl módosítása a tanúsítványok telepítéséhez

Ezt kell elhelyeznünk a szerveren, és beállítanunk az Apache-ban ennek helyét.

Például a titkos kulcsot az /usr/local/apache2/conf/ssl.key/ könyvtárba, a tanúsítványt pedig az /usr/local/apache2/conf/ssl.crt/ könyvtárba.

Be kell másolni a tanúsítványt egy server.crt nevű fájlba, az /usr/local/apache2/conf/ssl.crt/ könyvtárba.

Az előző lépésben generált private.key fájlt helyezük az /usr/local/apache2/conf/ssl.key/ könyvtárba.

Ezután módosítjuk az /usr/local/apache2/conf/ssl.conf fájlt, hogy a megfelelő titkos kulcsra és tanúsítványra mutasson:

```
#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile /usr/local/apache2/conf/ssl.crt/server.crt
#SSLCertificateFile /usr/local/apache2/conf/ssl.crt/server-dsa.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/private.key
#SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/server-dsa.key
```

A jelmondat (passphrase) eltávolítása az RSA titkos kulcsból

A webszerveren tárolt RSA titkos kulcs általában titkosított, ezért szükségünk van egy jelmondatra a használatához. Ezért kér jelmondatot, mikor az Apache-ot modssl-el indítjuk.

```
# apachectl startssl
Apache/1.3.23 mod_ssl/2.8.6 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide us with the pass phrases.
Server your.server.dom:443 (RSA)
Enter pass phrase:
```

Az RSA titkos kulcs titkosítása nagyon fontos. Ha valaki megkaparintja a "titkosítatlan RSA titkos kulcsot", akkor könnyen eltulajdoníthatja a webszervert. Ha a kulcs titkosított, az illető nem tud semmit tenni a jelmondat nélkül, hacsak "nyers erővel" (brute force) fel nem töri. Használjunk erős (értsd: hosszú és értelmetlen, abc kis és nagy betűi számjegyekkel kombinálva) jelmondatot erre a célra.

A kulcs titkosítása néha kellemetlenség forrása is lehet, mivel a webszerver minden indításakor kéri a jelmondatot. Különösen ha rc szkripteket használunk, a webszerver rendszerindításkor történő betöltéséhez. A jelmondat bekérése problémát okozhat, mivel megállítja a folyamatot, bemenetre vár.

Könnyen megszabadulhatunk a jelmondattól, ha visszafejtjük (decrypt) a kulcsot. Bizonyosodjunk meg arról, hogy senki se szerezheti meg a kulcsot. Vegyük figyelembe a biztonsági és védelmi ajánlásokat, mielőtt visszafejtjük a kulcsot a webszerveren.

A kulcs visszafejtésének módja:

Először készítsünk másolatot a titkosított kulcsról.

```
# cp server.key server.key.cryp
```

aztán írjuk újra a kulcsot titkosítással. Kérni fogja az eredeti titkosított kulcs jelmondatát:

```
# /usr/local/ssl/bin/openssl rsa -in server.key.cryp -out server.key
read RSA key
```

```
Enter PEM pass phrase:
writing RSA key
```

Íme egy módja annak, miként biztosíthatjuk a visszafejtett titkos kulcsot. Így csak a root felhasználó olvashatja:

```
# chmod 400 server.key
```

Munkafolyamatok közötti SSL részfolyamat-gyorstár (Inter Process SSL Session Cache)

Az Apache többfolyamatos modellt használ, amelyben NEM ugyanaz a munkafolyamat foglalkozik az összes kéréssel. Ennek eredményeként az SSL részfolyamat adatai (Session Information) elvesznek, mikor a kliens többszörös kéréssel fordul a szerverhez. A többszörös kapcsolódás nagy többletterhelést jelent a webszervernek és a kliensnek. Ennek elkerülésére az SSL részfolyamatok adatai egy munkafolyamatok közötti részfolyamat-tárban tárolódnak, ez lehetővé teszi a munkafolyamatok számára a kapcsolódási adatokhoz való hozzáférést. Az SSLSessionCache kapcsoló az /usr/local/apache2/conf/ssl.conf fájlban van, itt határozhatjuk meg az SSL részfolyamat-gyorstár helyét:

```
SSLSessionCache        shmht:logs/ssl_scache(512000)
#SSLSessionCache        shmcb:logs/ssl_scache(512000)
#SSLSessionCache         dbm:logs/ssl_scache
SSLSessionCacheTimeout  300
```

A dbm használata: a logs/ssl_scache DBF hash-fájlt készít gyorstárként a helyi lemezeden.
A shmht használata: a logs/ssl_scache(512000) a gyorstárat a megosztott memóriában hozza létre.

shmht vs shmcb

shmht: egy hash táblát használ az SSL kapcsolódási adatok gyorstárazására a megosztott memóriában.

shmcb: egy ciklikus buffert használ az SSL kapcsolódási adatok gyorstárazására a megosztott memóriában.

Az SSLSession gyorstár ellenőrzése

Az SSLSessionCache megfelelő működésének ellenőrzésére az openssl segédprogramot használhatjuk a -reconnect kapcsolóval, mint azt a következőkben láthatjuk:

```
# openssl s_client -connect your.server.dom:443 -state  -reconnect

CONNECTED(00000003)
.......
.......
Reused, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
SSL-Session:
.....
Reused, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
SSL-Session:
.....
Reused, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
SSL-Session:
.....
Reused, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
SSL-Session:
.....
Reused, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
SSL-Session:
.....
```

A -reconnect kapcsoló kényszeríti az "s_client"-et arra, hogy ötször ugyanazzal a SSL munkafolyamat-azonosítóval (SSL session ID) kapcsolódjon a szerverhez. Ötször ugyanannak az SSL munkafolyamat-azonosítónak az újra használatát kell látnunk, mint a fenti példában.

5 Az SSL megvalósítása és használata a HTTP forgalom biztonságossá tételére

Az Internet kezdeti kialakításánál sajnos nem volt szempont a rosszindulatú szereplők ellen védelmet nyújtó biztonságos hálózati megoldás alkalmazása. Emiatt a biztonsági szolgáltatásokat (titkosság, hitelesség, kommunikáló felek azonosítása) utólag kellett – kiegészítésként – a már elterjedt internetes protokollokhoz illeszteni. Rendkívül sok egyedi megoldás született, amelyek közül a robosztus, de mégis könnyen alkalmazható SSL vált de-facto szabvánnyá, amely TLS néven az IETF által elfogadott Internet szabvány szintre emelkedett. Az SSL, a TLS – illetve a mobil környezetre adaptált változat –, a WTLS mind titkos és hiteles adatátvitelt, mind a kommunikáló felek nyilvános kulcsú rejtjelezésen alapuló azonosítását szolgálja.

SSL-TLS-WTLS

Az első széles körben elterjedt biztonságos kommunikációs csatornát megvalósító protokoll a Netscape által 1994-95-ben kifejlesztett SSL (Secure Socket Layer) volt, amelynek azóta a harmadik verziójánál tartunk. Ez a protokoll de-facto szabvánnyá vált és a Netscape böngészőn kívül számos egyéb területen kezdék alkalmazni. 1999-ben az IETF (Internet Engineering Task Force) elfogadott szabvány szintre emelte az SSL-t azzal, hogy kiadott egy RFC-t 2246-os számmal, így az SSL-re kísértetiesen hasonlító TLS-t (Transport Layer Security) internetes szabvánnyá is tette. Ezzel párhuzamosan 1998-ban a WAP Forum által készített specifikációban megjelent a WTLS protokoll (Wireless Transport Layer Security) tervezete is, amely a drótnélküli kommunikáció (WAP, Wireless Application Protocoll) biztonsági rétegét tartalmazta és amely szintén kísértetiesen hasonlít a két előbb említett protokollhoz. (A WTLS gyakorlatilag a TLS mobil környezetre adoptált változata.) A három protokoll funkciója és felépítése annyira hasonló, hogy egyszerre tárgyaljuk őket, külön megemlítve az esetleges különbségeket. (Később látni fogjuk, hogy van lényeges különbség is a WTLS és az SSL-TLS páros között. (Az előbbi ugyanis a megbízható kapcsolatot garantáló

szállítási réteg (a TCP-nek megfelelő WTP) alatt specifikálja a biztonsági réteget, míg a másik a TCP fölött.)

Alapvető tulajdonságok

Az SSL készítői titkos és megbízható kommunikációs csatorna létrehozását tűzték ki célul maguk elé, amely egyrészről támaszkodik egy tőle függetlenül létező megbízható szálltási protokollra (pl. a TCP-re), másrészt kiszolgálja a felettes protokollokat (tipikusan a HTTP-t). A fejlesztés során a következő lényeges tulajdonságokat kívánták megvalósítani:

- A létrejövő kapcsolatnak titkosnak kell lennie. A kapcsolatfelvételkor megtörténő szimmetrikus kulcs csereje után a kommunikáció rejtjelezett formában zajlik (a kicserélt szimmetrikus kulcs felhasználásával).
- A felépült kommunikációs csatorna hitelesített, azaz az üzenetek sértetlenségét (illetve ennek ellenőrzését) ellenőrző-kód (MAC, Message Authentication Code) garantálja.

Ezeket a tulajdonságokat a következő célokban foglalták össze (a fontosság sorrendjében):

1. Titkosság (secrecy): A protokoll titkos kapcsolatot valósít meg két kommunikáló fél között.
2. Együttműködési képesség (interoperability): Független programozók által létrehozott programoknak képesnek kell lenniük egymással sikeresen kommunikálni a protokoll használatával. (Eltekintve speciális, opcionális esetektől.)
3. Továbbfejleszthetőség (extensibility): A protokoll egy olyan keretrendszer legyen, ami lehetőséget ad újabb kulcscsere, rejtjelező és ellenörző-kód készítő algoritmusok felvételére. (Ezzel megakadályozható, hogy egy rejtjel-algoritmus törése/elévülése miatt később újabb protokollt kelljen kifejleszteni.)
4. Relatív hatékonyság (relative efficiency): Mivel a kriptográfiai eljárások általában CPU-igényesek (főleg a nyilvános kulcsú rejtjelezés esetén) ezért a már sikeresen felépített kapcsolatok fontos adatait, szimmetrikus kulcsait valamilyen később is használható formában tárolni kell.

Az SSL-TLS-WTLS protokollokban gyakran előforduló kriptográfiai kifejezések definíciót a protokollok működésének megértéséhez szükséges tisztázni.

Pre-master secret

A pre-master secret gyakorlatilag egy 384 bites (48 byte) véletlen szám. A kliens hozza létre. Ezt rejtjelezi a szerver nyilvános kulcsával, majd elküldi neki. Ha a szerver képes dekódolni a számára kódolt üzenetet a saját titkos kulcsával (tehát valóban az, akinek állítja magát, mert rendelkezik a titkos kulccsal) és így meg tudja ismerni a pre-master secret-et, akkor ebből elkészíti a master secret-et.

Master Secret

Egy 48 byte hosszú titkos adatcsomag, amit a kliens és a szerver ugyanazzal a módszerrel hoz létre. Ebből készül a szimmetrikus rejtjelezés közös szimmetrikus kulcsaként használt session key.

Session Key

A kapcsolat során titkosítás, illetve a MAC aláírására használt szimmetrikus kulcs. A master secretből készíti egymással párhuzamosan a kliens és a szerver. **MAC - Message Authentication Code** (üzenethitelesítő kód): Olyan Kulcstól függő kontrollösszeg, amely a vevőoldalon az adatok véletlen és szándékos módosítását egyaránt képes detektálni.

Session Identifier

A session identifier (session ID) a szerver által véletlenszerűen kisorsolt szám, amely az adott kapcsolatot és a hozzá tartozó szimmetrikus kulcsot azonosítja.

Sequence Number (üzenet-sorszám)

Mindkét kommunikáló fél nyilvántartja a küldött és fogadott üzenetek sorszámait. Amikor a change cipher spec üzenetet kicserélik, akkor a sequence number értéke nullázódik, és újra inkrementálódni kezd.

Bulk data algorithm

A szimmetrikus rejtjelezéshez használt rejtjel-algoritmus és annak paraméterei.

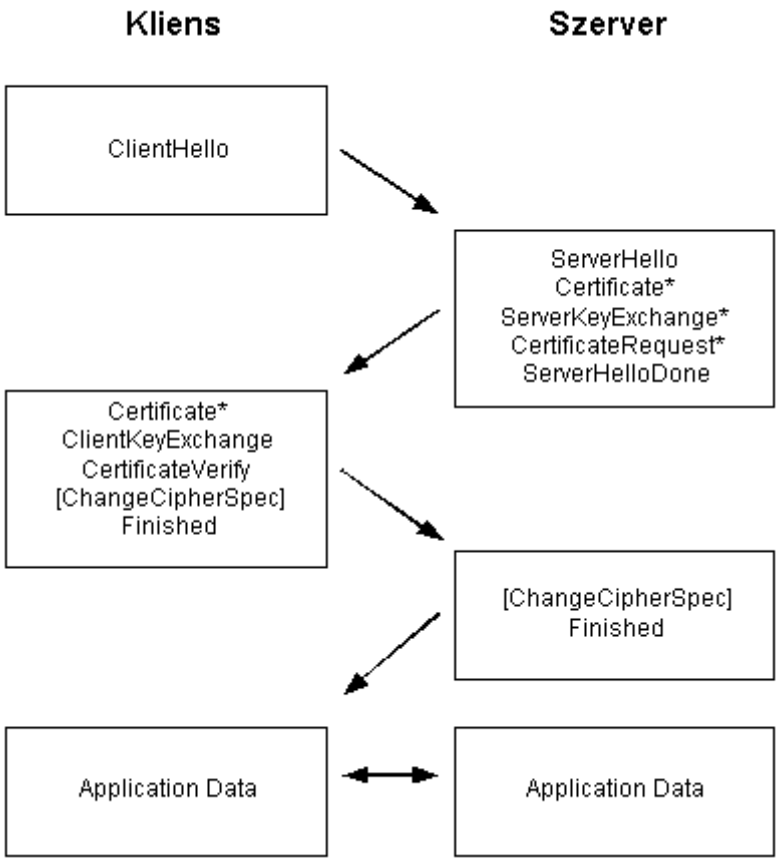
Cipher Spec

A cipher spec egy adatstruktúra, amely tartalmazza a rejtjelezett kommunikáció során használt rejtjelező-metódust (bulk data algorithm) és az ellenőrző-kód algoritmusát (MAC algorithm), az egyeztetett ideiglenes szimmetrikus kulcsot (session key) valamint néhány a kommunikáció során használt egyéb kriptográfiai jellemzőt.

Az SSL-TLS-WTLS teljes kapcsolatfelvétel

A kapcsolatfelvétel során a felek opcionálisan azonosítják egymást, megállapodnak egy közös kulcscsere, kódoló és MAC algoritmusban, majd a kiválasztott kulcscsere eljárással titkosan egyeztetnek egy ideiglenes szimmetrikus kulcsot a rejtjelezéshez és a MAC kódoláshoz. Ezt az egyeztetési lépést nevezik kapcsolatfelvételnek (kézfogás, handshake process).

Maga a kapcsolatfelvétel számos üzenetcseréből áll:



Teljes kapcsolatfelvétel

A fenti üzenethalmazt nevezik teljes kapcsolatfelvételnek (full handshake), mivel az összes üzenetet tartalmazza, ami egy ilyen akció során ezen protokollokban felmerülhet. A *-gal jelölt üzenetek opcionálisak. Használatukra csak szükséges esetekben kerül sor.

Az üzenetek

Client Hello

Ezt az üzenetet küldi a kliens a kapcsolatfelvétel elején a szervernek. Az üzenet tartalmazza a már esetlegesen régebbről meglévő session ID-t, a kliens által ismert rejtjel-algoritmusokat, és egy véletlen byte-sorozatot (client random), amit később a szimmetrikus kulcs előállításához kell majd.

Server Hello

Ezzel az üzenettel válaszol a szerver a ClientHello üzenetre. Tartalmazza a kapcsolat szerver által meghatározott session ID-ját, a szerver által kiválasztott rejtjel-algoritmust és a szerver által készített véletlen byte-sorozatot, ami úgyszintén szükséges lesz majd a szimmetrikus kulcs készítéséhez.

Certificate

A kliens és a szerver is elküldi elektronikus tanúsítványát, ha a másik fél ezt igényli, azonosítás céljából. A kliens számára opcionális.

Server Key Exchange

Ezt az üzenetet akkor küldi a szerver, ha nincs saját cetificate-je; van, de az csak aláírásra (signing) haszálható; vagy Fortezza kulcscsere metódust használ a két fél. Az üzenet egy nyilvános kulcsot tartalmaz, ami az előbb leírt művelet végrehajtását lehetővé teszi.

Certificate Request

Ezt az üzenetet a szerver küldi a kliensnek, ha kliens autentikációt akar végrehajtani és ezért elkéri a kliens tanúsítványát. Az üzenetben a szerver felsorolja, hogy milyen módszerrel és milyen CA-k által aláírt tanúsítványokat fogad csak el.

Server Hello Done

Ezt az üzenetet akkor küldi a szerver, amikor befejezte a ServerHello-t követő üzenetek küldését és készen áll az új kulccsal való rejtjelezett kommunikációra. Erre az egyébként üres üzenetre az opcionális üzenetek miatt van szükség.

Client Key Exchange

Ezt az üzenetet a kliens küldi saját tanúsítványa után (ha egyáltalán a szerver kérte azt), vagy rögtön a ServerHelloDone után. Az üzenet tartalmazza a a szerver nyilvános kulcsával rejtjelezett pre-master secret-et, amit a kliens hoz létre. Amennyiben a szerver képes azt dekódolni és az alapján a master secret-et és az ideiglenes kulcsot kiszámolni, akkor ezzel indirekten bizonyítja szeméyazonosságát.

Certificate Verify

Az üzenetet a kliens küldi közvetlen bizonyítékaként a saját személyazonosságának. Maga az üzenet a kapcsolatfelvétel során – a kliens és a szerver által – küldött üzenetek egy része, a master secret és konstans adatok felhasználásával készült adatsorozat digitálisan aláírását tartalmazza áltozata, amit a szerver a kliens nyilvános kulcsával tud ellenőrizni.

Change Cipher Spec

Az üzenet egy jelzés arra a kommunikációs parter felé, hogy a következő elküldött üzenet már az új megállapodás szerinti rejtjel-algoritmussal lesz kódolva.

Finished

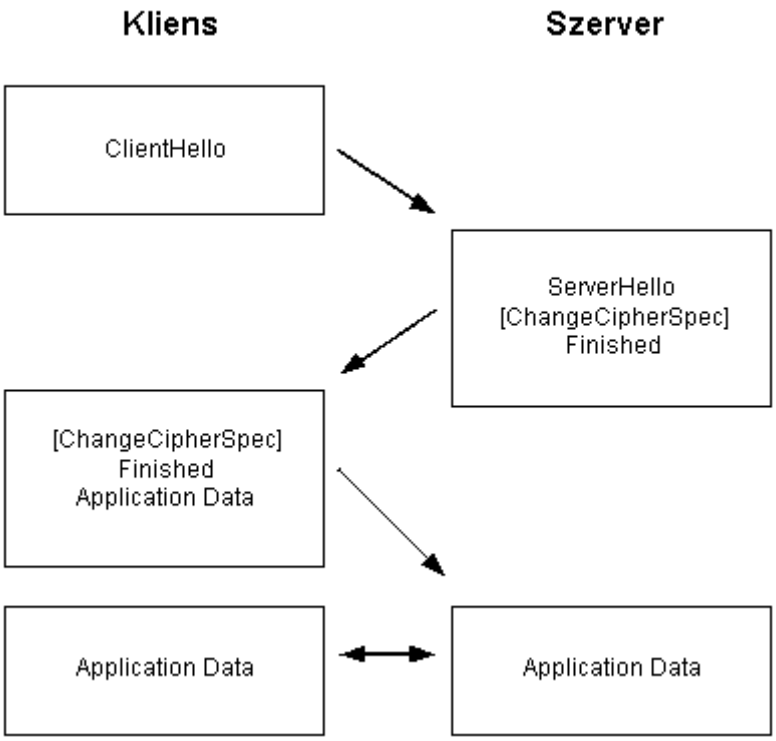
Ez az első üzenet, ami már az új algoritmusokkal lett kódolva. Az üzenet jelentése az, hogy a kulcscsere és partner-azonosítás sikeresen lezajlott. Az eddigi üzenetek SHA 2 vagy MD5 algoritmussal készített aláírását tartalmazza. Ha bármi manipuláció történt volna a kapcsolat-felépítés során, az legkésőbb ekkor kiderül.

Egyéb SSL-TLS-WTLS kapcsolat felvételi módok

A teljes kapcsolatfelvételen kívül a partnereknek lehetőségük van rövidített (abbreviated) vagy optimalizált (optimized) kapcsolatfelvételre is. Ezek a módok a teljes kapcsolatfelvételi mód már ismertetett üzeneteinek egy szűkebb részét használják.

Rövidített kapcsolatfelvétel

Ha a kliens már kapcsolatban volt korábban a szerverrel és megőrizte a session ID-t, akkor lehetősége van a már egyeztetett rejtjel paraméterek (rejtjel algoritmusok, szimmetrikus kulcs stb.) ismételt használatára. Ezt úgy kezdeményezheti, hogy a ClientHello üzenetben kitölti a session ID mezőt a korábban használt session ID-val. Ha a szerver elfogadja az elküldött ID-t (pl. nem túl régi a kulcs és még „emlékszik rá"), akkor a ServerHello üzenetben ugyanezt, a korábban használt session ID-t küldi vissza (ellenkező esetben új session ID-t sorsol) majd a ChangeCipherSpec üzenetet követően a rejtjelezett kommunikáció azonnal kezdődhet.

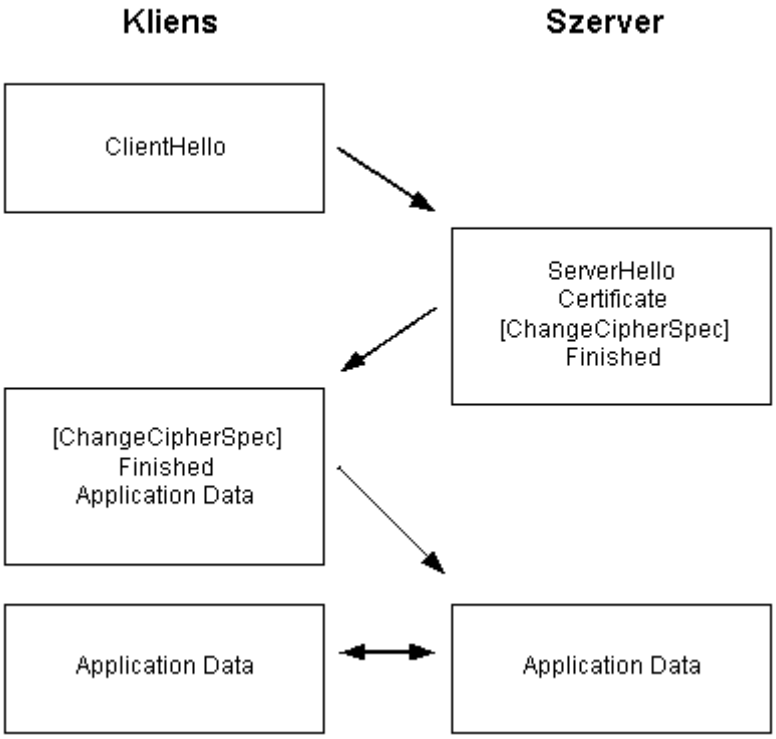


Rövidített kapcsolatfelvétel – a korábbi kapcsolat újrahasznosítása

Optimalizált kapcsolatfelvétel

Ha a kommunikáló felek elliptikus görbén értelmezett (EC) Diffie-Hellmann típusú kulcscsere algoritmust (ECDH) használnak, akkor a szervernek lehetősége lehet lerövidíteni a kapcsolatfelvétel folyamatát, amennyiben meg tudja szerezni a kliens tanusítványát valamilyen saját forrásból (pl. LDAP használatával). Ekkor a ClientHello beérkezése után a szerver a kliens tanúsítványa segítségével saját maga elkészítheti a pre-master secret-et, a master secret-et és belőle a szimmetrikus kulcsot. A kliensnek már csak saját tanúsítványát és

a ChangeCipherSpec üzenetet küldi el, amire a kliens szintén ChangeCipherSpec üzenettel válaszol, és azonnal rátérhetnek a rejtjelezett kommunikációra.



Optimalizált handshake

Manapság a fájlszerveren tárolt adatok biztonsága nagyon fontos. A kompromittált adatok több ezer dollárba is kerülhetnek egy társaságnak. Az utolsó részben LDAP hitelesítési modult fordítottunk az Apache-ba, hogy biztosítsuk a hitelesítési mechanizmust. Bár a HTTP forgalom nem igazán biztonságos, és minden adat tiszta szövegként jelenik meg - ez azt jelenti, hogy az LDAP hitelesítés (userid/passwd) ugyancsak tiszta szövegként megy át. Ez problémát okozhat. Bárki kutathat ezen userid/passwd párosok után és hozzáférhet a DAV állományhoz. Ennek megelőzéséhez titkosítanunk kell a HTTP forgalmat, valójában a HTTP+SSL vagy HTTPS segítségével. Bármi, ami átmegy a HTTPS-en, titkosított lesz. A HTTPS a 443-as porton fut. Az előző rész fordítási folyamatának eredményeként az Apache mindkét porton, a 80-ason (normál HTTP) és 443-ason (HTTPS) is fut. Ha csak a DAV-hoz használjuk majd a szervert, akkor nagyon ajánlott bezárni a 80-as portot.

6 TLS (Transport Layer Security)

TLS és az elődje a Secure Sockets Layer, (SSL), olyan kriptográfiai protokollok, amik gondoskodnak, hálózatok fölötti kommunikációknak, mint például az Internetnek, a biztonságos használatáról. A protokollok több verziója elterjedt, használatban vannak több alkalmazásban (internetes böngészés, elektronikus posta, Internet fax, VoIP) .

A TLS egy IETF a standard protokollt követ, minek utolsó frissítése az RFC 5246 amit a korábbi SSL részletes leírások alapján fejlesztet a Netscape Corporation .

Internet protokoll
Alkalmazási réteg
BGP · DHCP · DNS · FTP · HTTP · IMAP· IRC · LDAP · MGCP · NNTP · NTP ·POP · RIP · RPC · RTP · SIP · SMTP ·SNMP · SSH · Telnet · TLS/SSL · XMPP
Szállítási réteg
TCP · UDP · DCCP · SCTP · RSVP ·ECN
Internet réteg
IP (IPv4 , IPv6) · ICMP · ICMPv6 · IGMP· IPsec
Adatkapcsolati réteg
ARP/InARP · NDP · OSPF · alagutat ás(L2TP) · PPP · médiahozzáférés-szabályozás (Ethernet , DSL , ISDN ,FDDI)

A TLS protokoll megengedi az ügyfél/kiszolgáló alkalmazásnak, hogy kommunikáljanak egy hálózaton keresztül, de megakadályozza, hogy illetéktelenek hallgatózzanak vagy beavatkozzanak.

TLS végpontot nyújt hitelesítés és kommunikációs bizalmasság, amik az interneten kriptográfiát használnak. A TLS, RSA 1024 és 2048 bit-es védelmet keppes nyújtani.

Tipikus vég-felhasználó a TLS hitelesítés egyoldalú: csak a szervert hitelesítik (az ügyfél tudja, hogy a szerver hitelesített), de fordítva ez nem teljesül, (az ügyfél nem hitelesített vagy névtelen).

TLS szintén támogatja a biztosabb kétoldalú kapcsolatmódot (jellemzően vállalati alkalmazásokban használt). Ezekben a kommunikáló felek biztosak lehetnek egymás kilétében (feltéve, hogy szorgalmasan ellenőrzik az azonosító adatokat, egymás tanúsítványait). Ezt a kölcsönös hitelesítést, vagy 2SSL. Kölcsönös hitelesítéshez szükséges, hogy a kliens oldal is rendelkezzen TLS tanúsítvánnyal. Hacsak, TLS-PSK-t, Secure Remote Password (SRP) protokollt, vagy valamilyen más protokollt használnak, amely biztosíthatja az erős, kölcsönös hitelesítést a bizonyítványok hiányában.

Jellemzően a fő információkat és okleveleket, amik nélkülözhetetlenek TLS-hez, valamilyen X.509 oklevélben vannak, ami a szükséges mezőket és adatformátumokat határoz meg.

Cipher Suite(titkosító csomag)

Mikor egy TLS vagy a SSL kapcsolat létrejön, az ügyfél és a szerver megtárgyalnak egy Cipher Suite-et miközben Cipher Suite kódokat váltanak (ügyfélben, szia és szerver, szia üzenetek), mely meghatározza a használandó titkosító algoritmusok egy kombinációját a kapcsolatban, és létrehoz egyfajta ’ udvariasságot ’ ügyfél és szerver között, ez minden interaktív szerverbevetés egy szükséges összetevője.

A fő csere és hitelesítési algoritmusok jellemzően nyilvános kulcsú algoritmusok, vagy TLS-PSK kulcsok. Az üzenet hitelesítési kódk a kriptográfiai hash-függvények segítségével hozzák létre egy HMAC konstrukciót a TLS-nél, és egy nem szabványos ál véletlen függvényt az SSL-nél.

Története

Biztonságos Hálózati Programozás API

A szállítási réteg-biztonságért végzett korai kutató munkák, tartalmazták a Secure Network Programming-et (SNP), mely feltárta annak a megközelítését, hogy van a szállítási rétegnek egy olyan API-ja, amit közelről hasonlító Berkeley foglalatba helyez, hogy meg könnyítse utólagos alkalmazását, korábban meglévő hálózati alkalmazások biztonsági intézkedésekkel való ellátását. Az SNP projekt megkapta a 2004-es ACM szoftverrendszer-díját.

TLS version 1.0

TLS 1.0 először feljavításként jelent meg 1999 januárjában, RFC 2246 SSL Version 3.0-hoz. Ahogy megjelent az RFC-ben, ez a protokoll és az SSL 3.0 közti különbségek nem drámaiak, de elég jelentősek ahhoz, hogy a TLS 1.0 és SSL 3.0 ne működjenek együtt. TLS 1.0 tartalmaz egy eszközt, ami által egy TLS implementáció visszaminősítheti a kapcsolatot SSL 3.0-vá.

TLS verzion 1.1

TLS 1.1 2006 áprilisában megjelent RFC 4346 frissítés a TLS 1.0-hoz

Jelentős különbségek ebben a verzióban:

- A hozzáadott védelem Cipher block chaining (CBC) támadások ellen.
- Inplicit Initialization Vector (IV) felváltása egy Explicit IV-re.
- Változz a padding hiba kezelésében.
- A paraméterek IANA regisztrációjának nyújtott támogatás.

TLS version 1.2

TLS 1.2 2008 augusztusában jelent meg mint RFC 5246. Ez a korábbi TLS 1.1 részletes leírásán alapul. Főbb különbségek a következők

- A MD5 / SHA-1 pseudorandom funkciót (PRF) felváltották Cipher-suite -re SHA-256.
- A MD5 / SHA-1 Finished üzenet módosítása SHA-256-ra, Cipher-suite specifikus hash algoritmus használatának lehetőségével
- Hitelesített titkosításnak nyújtott támogatás bővítése.
- TLS Extensions definíció és Advanced Encryption Standard (az AES) Cipher Suites hozzáadása.

Standardok

TLS aktuális jóváhagyott verziója version 1.2, melyet az alábbiak jellemzik:

- RFC 5246 : a szállítási rétegbiztonság (TLS) protokoll-verzió 1.2.

Korábbi verziók:

- RFC 2246 : a TLS protokoll-verzió 1.0.
- RFC 4346 : a szállítási rétegbiztonság (TLS) protokoll-verzió 1.1.
- A másik RFC-k azután beleértve kiterjesztették TLS-t:
- RFC 2595 : „Using TLS with IMAP, POP3 and ACAP" . Részletezi az IMAP, POP3 és olyan ACAP szolgáltatásoknak egy kiterjesztését, amik megengedik a szervernek és ügyfélnek, hogy arra használják a TLS-t, hogy az interneten privát, hitelesített kommunikációt hajtsanak végre.
- RFC 2712 : "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)" 40 bites Cipher Suites-ek, amiket meghatároztak ebben , csak a célból jelentek meg, hogy dokumentálják a már felhasznált Cipher Suite kódokat .
- RFC 2817 : „Upgrading to TLS Within HTTP/1.1", megmagyarázza, hogy hogyan lehet arra használni az Upgrade szerkezetet HTTP/1.1-ban, hogy a TLS kezdeményezze, több mint egy létező TCP kapcsolatot. Ez megengedi a nem biztosított és biztosított HTTP-forgalomnak, hogy ugyanazt a jól ismert végpontot ossza meg.
- RFC 2818 : „HTTP Over TLS", A különböző szerverportok használatával megkülönbözteti a biztonságos forgalmat a nem biztonságostól.
- RFC 3207 : „SMTP Service Extension for Secure SMTP over Transport Layer Security". Részletez egy kiterjesztést a SMTP szolgáltatásra az megengedi egy SMTP szervernek és ügyfélnek, hogy arra használják a SMTP-t, hogy az interneten privát, hitelesített kommunikációt hajtson végre.
- RFC 3268 : „AES Ciphersuites for TLS". Az AES Cipher Suitesek alkalmazása a korábban létező szimmetrikus számjegyeknél.
- RFC 3546 : „Transport Layer Security (TLS) Extensions", Hozzáad egy arra szolgáló technikát, hogy gyűlésinicializálás alatt tárgyal meg protokoll-kiterjesztéseket, és meghatároz néhány kiterjesztést. Ez az elékszűlt RFC 4366 által elavult .
- RFC 3749 : „Transport Layer Security Protocol Compression Methods", Részletezi a szerkezetet a kompressziós módszerek és a DEFLATE kompressziós módszer számára.

- RFC 3943 : „Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)”
- RFC 4132 : „Addition of Camellia Cipher Suites to Transport Layer Security (TLS)”
- RFC 4162: „Addition of SEED Cipher Suites to Transport Layer Security (TLS)”
- RFC 4217 : „Securing FTP with TLS”
- RFC 4279 : „Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)”. Hozzáad három új Cipher Suites kollekciót a TLS-hez. Ezzel támogatja a hitelesítés alapú előre kiosztott kulcsok használatát.
- RFC 4347 : "Datagram Transport Layer Security ". Részletez egy olyan TLS változatot, ami datagram protokollok fölött működik, (pl.: UDP).
- RFC 4366 : „Transport Layer Security (TLS) Extensions”. Leír egy készlet speciális kiterjesztést, és egy általános kiterjesztés szerkezetet is.
- RFC 4492 : „Elliptic Curve Cryptography”.
- RFC 4507 : Transport Layer Security (TLS) Session Resumption without Server-Side State”
- RFC 4680 : „TLS Handshake Message for Supplemental Data”.
- RFC 4681 : „TLS User Mapping Extension”.
- RFC 4785 : „Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)”.
- RFC 5054 : „Using the Secure Remote Password (SRP) Protocol for TLS Authentication”..
- RFC 5746 : „Transport Layer Security (TLS) Renegotiation Indication Extension”.

7 Kormány által jegyzett protokoll-korlátozások

SSL néhány korai implementációja a kriptográfiai technológia exportjának az amerikai kormányzati korlátozásai miatt 40 bites szimmetrikus kulcsokat használt. A nyilvános vita több éves perek sorozata után, és hosszabb kulcsfontosságú méretekkel rendelkező kriptográfiai termékek végső amerikai kormányzati felismerése külsőt, az USA-t, termelt, a hatóságok enyhítették az exportmegszorítások néhány szempontját.

Implementációk

SSL-et és TLS-t széles körben több nyitott forrás szoftverprojektben valósították meg. A programozók SSL/TLS funkcionalitásokat használhatnak az Open SSL-t, NSS-ot vagy a GnuTLS könyvtárakat. A Microsoft Windows a Secure Channel csomagja részeként tartalmazza az SSL és a TLS egy implementációját.

A Delphi programozók egy Indy könyvtárat használhatnak.

Böngészők implementációja:

A legújabb web böngészők közül mindegyik támogatja TLS-t:

- Apple Safari-ja támogatja a TLS-t.
- Mozilla Firefox , version 2 és a feletti verziói, támogatják a TLS 1.0 2010 áprilisa , Firefox nem támogatja TLS 1.1 vagy 1.2-őt
- Internet Explorer 8 Windows 7 és Windows Server 2008 R2 támogatja TLS 1.2-őt.
- Presto 2.2 és az Opera támogatja a TLS 1.2-őt.

8 Befejezés

Az e-kereskedelem oly módon forradalmasította a 21. századot, mint kevés más iparág és közben egy teljes, önálló iparággá fejlődött. Míg korábban szinte csak B2B tranzakcióra használták fel, addig manapság már szinte mindenki, aki aktív internet felhasználónak számít, legalább egyszer életében kapcsolatba kerül az e-kereskedelem valamilyen formájával. Az e-kereskedelem fejlődési irányát jelentősen befolyásolja a technológia változása. Az egyre növekvő sávszélesség és nagyobb teljesítményű számítógépek megengedik az erőforrás igényesebb technológiák használatát, ami növeli a felhasználói és vásárlási élményt, ugyanakkor az internetes vevő egyre türelmetlenebb, egyre kevésbé hajlandó várakozni. Emiatt a következő évek két kulcsszava a gyorsulás és egyszerűsödés lehet, amivel kielégítik a felhasználók növekvő igényét az egyszerűség és gyorsaság iránt. Ezzel együtt kiszorulnak az öncélú „flashes" megoldások és törekednek majd a kompatibilis sztenderd rendszerekre. A kiskereskedelemre gyakorolt hatása által egyre szervesebb kapcsolódás lesz az offline és online üzletmenet között, mert rájöttek a cégek, hogy az online és az offline bolt egymást erősíti, nem egymástól vonnak el vásárlókat. A cél, hogy egyre gördülékenyebb együttműködés legyen a katalógus, a boltok és a web áruházak között. Idővel akár megfordulhat a trend, és az online boltok fognak offline, hagyományos áruházakat nyitni (például notebook.com). Az internetes boltok térhódításának hála nagymértékben megnő a vásárlók számára elérhető termékpaletta, ennek hatására, a vásárlási döntés megkönnyítésére nőni fog az aggregátor; áru-összehasonlító/árukereső oldalak száma. Világosabbá, egyszerűbbé fogják tenni a fizetési folyamatokat, nőni fog az online pénztárca jellegű megoldások száma.

A piac felosztását tekintve letisztuló folyamat veszi kezdetét, csökkeni fognak a közepes méretű web áruházak, egybeolvadnak vagy beolvadnak a piacvezető oldalakba, akik a piac még nagyobb százalékát fogják uralni. Várhatóan növekedni fog a longtail szereplők száma, akik réspiacokat céloznak majd meg.

Jelenleg is nagy problémát okoz az immateriális tulajdonsága a webnek, ami megnehezíti a termékek ismertetését. Erre jelentenek megoldást az egyre modernebb 3D-s interaktív termék animációk, valamint a videók növekvő használata.

Szintén a hatékonyabb vevőkiszolgálást és vásárlást könnyítést szolgálja a kontakt-pontok létrehozása, ezáltal több helyen átvehetőek és visszaadhatóak a termékek. Egyre

elterjedtebbek a valós idejű ügyfélszolgálati chat megoldások, mellyel a vásárlói bizalom is könnyen növelhető. Fontos irány a személyre szabhatóság, mely keretében a teljes marketing kommunikációra jellemzőek lesznek az egyre személyre szabottabb megoldások. A közösségi oldalak hihetetlen népszerűségének hatására a szakemberek felismerték a közösség összetartó és generáló erejét, ezáltal az ilyen csoportok hatalma egyre inkább érvényesülni fog az e-kereskedelemben is, melynek hatására a közösség portálok és a web áruházak közötti határok egyre inkább elmosódnak. Új vásárlási felületek jelennek meg, növekszik a mobiltelefonos vásárlások aránya, ami rámutat, hogy a jövőben számítani lehet több eltérő fejlődési irányra az e-kereskedelmen belül.

Az e-kereskedelem nagy népszerűségre és terjeszkedésre számíthat a jövőben a következő egyszerű okok miatt:

- Ez a legkényelmesebb módja a vásárlásnak.
- Nem igényel semmilyen mértékű helyváltoztatást.
- A „világ legnagyobb hipermarketje” az internet, szinte minden gyártó kínálata megtalálható rajta.
- Non-stop, 24 órás nyitva tartás.
- A web áruházakban jóval nagyobb és gyakoribb akciókkal találkozhatunk, a gyártók és forgalmazók kisebb költsége miatt.
- Könnyű összehasonlítani a különböző termékeket.

Látható, hogy egy átlagos vásárló számára minden szempontból előnyös lehet az online vásárlás, és ha ezeket az előnyöket mind többen megismerik, akkor csak tovább növekszik az e-kereskedelem.

Azonban nemcsak a végfelhasználók, hanem a gyártók és kiskereskedők számára is rendkívül hasznos lehet ha a jövőben online szervezik az üzleti tranzakcióikat. A technológiai fejlesztések által nemcsak olcsóbb hanem hatékonyabb logisztikai megoldásokkal élhet, az internet nyújtotta hatalmas vevőbázis pedig határtalan marketing lehetőségeket nyújt számára. A hangsúly pedig a határtalanon van, hiszen az e-kereskedelemben tényleg nincsenek határok, sem földrészek, az e-kereskedelem maga a megtestesült globalizáció.

9 Köszönetnyilvánítás

A következőkben szeretnék köszönetet mondani mindazoknak, akik segítettek a diplomamunkám elkészítésében.

Dr. Huszti Andrea egyetemi adjunktus konzulensemnek munkám lelkiismeretes vezetéséért, szakmai tanácsaiért és segítségért szeretném hálás köszönetem kifejezni.

10 Források

Könyv:

- Szemere Brigitta: E-business (2008) Dunaújvárosi Főiskolai Kiadó
- Vezérvonal (2001.november)Kiskapu KFT
- Eric Rescorla: SSL and TLS: Designing and Building Secure Systems (2001) Addison-Wesley,
- SNP: An Interface for Secure Network Programming The University of Texas at Austin

WEB:

- http://www.origo.hu
- http://www.wikipedia.com
- http://tldp.fsf.hu/HOWTO/Apache-WebDAV-LDAP-HOWTO-hu/index.html
- http://www.biztostu.hu
- http://www.emenedzser.hu/eker.htm
- http://www.linuxvilag.hu
- http://www.ietf.org/rfc/rfc2246.txt
- http://www.netlock.hu