SSL sertifikati

Sadržaj

Uvod

Svedoci smo da internet postaje vodeće sredstvo komunikacije, poslovanja i trgovine. Podaci koji se tom prilikom razmenjuju, često i vrlo osetljivi podaci, lako mogu postati predmet zloupotrebe. Krađa identiteta, neovlašćeno skidanje novca sa bankovnih računa, phishing prevare, zatrpavanje neželjenim, nekad i malicioznim email-ovima, na žalost, postali su svakodnevica ljudi koji koriste internet. Veliki broj korisnika ustručava se od ostavljanja svojih podataka na sajtovima i upuštanja u online kupovinu. Zbog svega toga, online bezbednosti treba da se pristupa sa jednakom ozbiljnošću kao fizičkoj bezbednosti lica, kuće ili posla.

Kako bi se u potpunosti iskoristili potencijali interneta kao medija komunikacije i poslovanja, bilo je neophodno uspostaviti stadarde koje web sajtovi moraju ispuniti, kako bi izgradili odnos poverenja sa korisnicima. Veliki broj kompanija koje posluju online, kao standard i okvir bezbednog poslovanja i bezbedne komunikacije na internetu, prihvatili su SSL sertifikate.

Šta je SSL?

Secure Socket Layer (SSL) je digitalni fajl ili kod koji se koristi kao pomoć pri zaštiti i autentifikaciji komunikacije kako na internetu tako i na intranetu u okviru organizacija. SSL protokol stvara kriptovanu vezu između web servera i web browsera, koja osigurava da podaci koji se razmenjuju između servera i browsera ostanu tajni i bezbedni, a korisnici ga prepoznaju po katancu koji se pojavljuje u njihovim browser-ima.

SSL protokol razvio je Netscape 1995. i vrlo brzo postao je primarni metod zaštite prenosa podataka putem interneta.

SSL je ugrađen u svaki veći web server i web browser i koristi tehnike enkripcije javnih-privatnih ključeva. Tako se stvara tajni kanal komunikacije. Da bi se uspostavila SSL veza, web server mora imati instaliran digitalni sertifikat; ovaj sertifikat koristi javne i tajne ključeve koji se koriste za enkripciju i sertifikat jedinstveno i pozitivno identifikuje server. Digitalne sertifikate možete zamisliti kao elektronske identifikacione karte, nešto kao vozačke dozvole ili lične karte, koje potvrđuju autentičnost servera pre nego što se uspostavi šifrovani kanal za komunikaciju.

Kao što nećete svoje lične podatke ili podatke svog bankovnog računa napisati na poleđini razglednice, tako ne želite ni da ti podaci budu vidljivi svima na internetu.

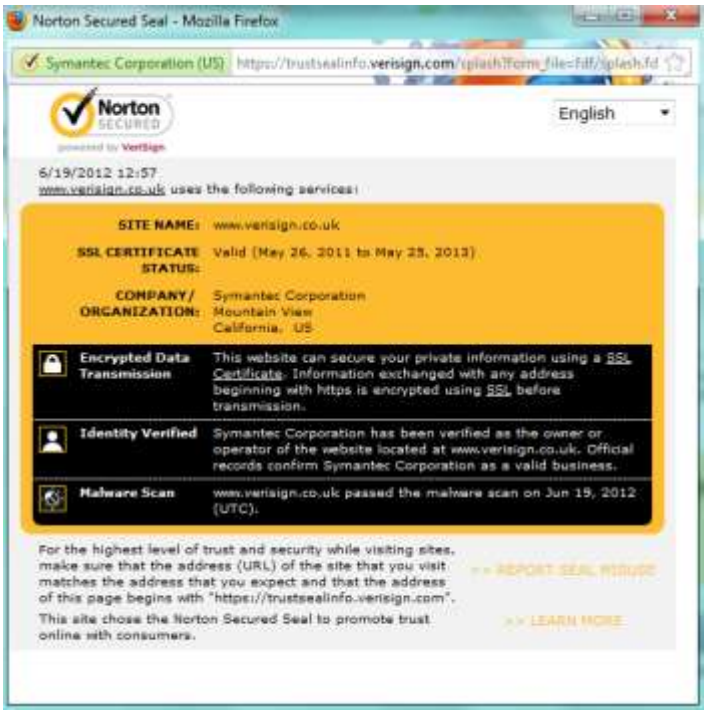
Uobičajeno je da digitalne sertifikate izdaje treća strana koja je nezavisna i od poverenja, čime se osigurava verodostojnost i široko prihvatanje. Izdavalac sertifikata poznat je još i kao Certification Authority (CA). Poznati globalni CA su na primer VeriSign, Thawte i GeoTrust.

Svaki SSL sertifikat izdaje se za poseban server i poseban domen (adresu web sajta) i CA verifikuje svaki entitet za čiji server i domen se sertifikat izdaje. Kada u browser ukucate adresu sajta koji ima SSL sertifikat, browser i server se prepoznaju. Uspostavlja se sigurna veza, kreira se jedinstveni ključ za tu sesiju i može se početi sa bezbednom komunikacijom i razmenom podataka.

Kako ćete znati da je neki sajt zaštićen SSL sertifikatom?

1. Tako što će ispred adrese sajta u address bar-u browsera stajati https://, što znači „Secure HTTP“.
2. Videćete simbol katanca, koji se može nalaziti na vrhu ili dnu strane, zavisno od browsera koji koristite.
3. Često možete videti „trust mark“ na samom sajtu. Ako kliknete na znak videćete detalje vezane za sertifikat, zajedno sa podacima kompanije.

4. Klikom na zaključan katanac u prozoru browsera ili na „trust mark“ prikazaće vam se naziv autentifikovane organizacije, ako postoji SSL sertifikat adresa će postati zelena, ako se podaci ne poklapaju (npr. adresa sajta i ime organizacije) ili je sertifikat istekao browser će prikazati grešku ili upozorenje.



Karakteristike SSL-a

Ljudi često povezuju SSL sa enkripcijom, dok zapravo SSL sertifikat podrazumeva četiri posebne karakteristike koje su ključne za obezbeđivanje privatnosti i bezbednosti koju zahtevaju kupci i korisnici: enkripcija, integritet, autentifikacija i neporecivost.

ENKRIPCIJA

Enkripcija koristi matematičke algoritme za transformisanje podataka tako da ih mogu pročitati samo strane kojima su ti podaci namenjeni. U slučaju SSL-a, tajni i javni ključevi koji su deo digitalnog sertifikata servera igraju važnu ulogu u obezbeđivanju podataka poslatih na i sa web browser-a.

INTEGRITET

Enkripcijom podataka, tako što ih mogu pročitati samo strane kojima su ti podaci namenjeni, SSL sertifikati takođe obezbeđuju integritet tih podataka. Drugim rečima, ako niko drugi ne može uspešno da pročita podatke, ti podaci ne mogu biti izmenjeni u toku prenosa. Modifikovanje kriptovanih podataka učinilo bi ih neupotrebljivim i strane kojima su podaci namenjeni bi znale da je neko pokušao da otvori podatke.

AUTENTIFIKACIJA

Jedna od glavnih uloga CA u izdavanju digitalnih seritfikata je da identifikuju organizaciju, ili osobu, koja traži sertifikat. SSL sertifikati su vezani za internet domensko ime i verifikacijom vlasništva tog imena, CA osigurava da korisnici znaju sa kim imaju posla na osnovnom nivou.

NEPORECIVOST

Enkripcija, integritet i autentifikacija zajedno čine neporecivost, što znači da ni jedna strana u sigurnoj transakciji ne može s pravom da tvrdi da je u njihovoj komunikaciji učestvovao iko drugi, do oni sami. Ova karakteristika otklanja mogućnost poricanja jedne strane, ili povlačenje informacija koje su poslate online.

Vrste SSL sertifikata

Postoji nekoliko vrsta SSL sertifikata, koji se međusobno razlikuju po nivou zaštite koju pružaju.

1. Prvi tip SSL sertifikata su **samopotpisani sertifikati (self-signed certificate).** Ove sertifikate ne izdaje CA, nego vlasnik sajta i samim tim nemaju istu težinu kao sertifikati koje izdaje CA.
2. Kao početni nivo SSL sertifikacije uzima se **sertifikat za validaciju domena (Domain Validated Certificate)**. Jedino što ovaj sertifikat garantuje je da je onaj koji traži sertifikat vlasnik domena za koji taj sertifikat traži. Ne vrše se dodatne provere kojima bi se utvrdilo da li je vlasnik domena i stvarni privredni subjekat.
3. **SSL sertifikat potpune autentifikacije (fully authenticated SSL Certificate)** je prvi korak stvarne online bezbednosti i sticanja poverenja. Ovi sertifikati se izdaju tek kada organizacija koja traži sertifikat prođe niz procedura za validaciju i potvrdi da je privredni subjekat, vlasnik domena i da ima autoritet da zatraži sertifikat.
4. **Džoker sertifikati (Wildcard Certificate)** koriste se kada na jednom domenskom imenu imamo više različitih host sufiksa. Ovaj sertifikat omogućava punu SSL bezbednost bilo kom

hostu na domenu - na primer host.vas_domen.com, gde se „host“ menja, dok ime domena ostaje konstantno.

5. Sličan džoker sertifikatu je **SAN sertifikat (Subject Alternative Name)** koji omogućava da se više od jednog domena doda na jedan SSL serifikat.
6. **Code Signing sertifikati** garantuju da softver koji ste preuzeli nije neovlašćeno izmenjen usput, odnosno da na njih nije zakačen neki maliciozni softver.
7. **Sertifikati sa proširenom validacijom (Extended Validation – EV)** obezbeđuje najviši nivo autentifikacije i poverenja kupaca. Kada kupac poseti sajt koji ima EV sertifikat, adresna traka postaje zelena i pojavljuje se polje sa imenom legitimnog vlasnika web sajta, zajedno sa imenom provajdera koji je izdao EV sertifikat. Takođe prikazaće se i ime vlasnika sertifikata i CA.

Zaključak

Poverenje – ključna reč za e-business. 70% online kupaca odbija da učestvuje u online kupovini jer nemaju osećaj sigurnosti u plaćanju. Ono što garantuje sigurnost transakcije i podataka i što obezbeđuje poverenje korisnika, to jest kupaca, jesu SSL sertifikati. Studije slučaja pokazuju povećanje prodaje za 10% samo nedelju dana nakon isticanja „sigurnosnog pečata“ na sajtu. [1]

SSL sertifikati nisu potrebni samo sajtovima koji se bave online prodajom. Svaki sajt koji prikuplja ili obrađuje informacije koje treba zaštititi od uljeza i hakera (bilo da su to brojevi kreditnih kartica, matični brojevi, brojevi telefona ili samo email adrese), trebalo bi da ima SSL sertifikat.

SSL sertifikat je mala cena koju treba platiti za kupovinu poverenja i lojalnosti korisnika.

[1] http://www.verisign.co.uk/static/Opodo-Case-Study.pdf

Reference:

1. Beginner's Guide to Digital SSL Certificates http://www.verisign.co.uk/ssl/ssl-information-center/ssl-resources/guide-ssl-beginner.pdf
2. Extended Validation SSL Certificates: A Standard for Trust
3. Licensing VeriSign Certificates Securing Multiple Web Server and Domain Configurations