CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nove sigurnosne mjere web preglednika

NCERT-PUBDOC-2011-08-330

Nacionalni CERT

Nacionalni CERT

Sadržaj

1 Uvod

U svijetu računalne sigurnosti, najčešći su sigurnosni problemi vezani uz web stranice. Svaka organizacija koja imalo drži do sebe, posjeduje web stranicu kojom se prezentira na Internetu. Međutim, upravo ta web stranica može biti „rupa“ koju napadač može iskoristiti za dobivanje pristupa informacijskom sustavu organizacije. Web ranjivosti su opasne najviše zbog činjenice da se njihovim korištenjem zaobilaze mrežne zaštite kao što su vatrozidovi jer ih oni ne mogu otkriti.

Kao što je svima poznato, web stranicama se pristupa putem web preglednika. Upravo su oni mjesto na kojem se mogu uvesti određene sigurnosne provjere, odnosno implementirati tehnologije koje mogu spriječiti dio napada. Zajedno s izlaskom novih inačica najpopularnijih web preglednika, Mozille Firefox (inačice 4) i Microsoftovog Internet Explorera (inačice 9), predstavljeno je i nekoliko značajnih sigurnosnih mogućnosti.

Content Security Policy (CSP) je dodatni sloj sigurnosti koji pomaže otkrivanju i sprječavanju određenih vrsti napada kao što su XSS (Cross Site Scripting) i napad ubacivanjem podataka (data injection) [1]. Takvi se napadi koriste za krađu podataka, distribuciju malvera i narušavanje izgleda početnih web stranica („defacement“). HTTP Strict Transport Security je sigurnosna mjera koja web stranicama omogućuje da preglednicima nalažu korištenje isključivo protokola HTTPS, umjesto HTTP. Tako se izbjegavaju „man-in-the-middle“ napadi ili slučajevi kod kojih je korisnik nemaran i zanemaruje poruku o neprovjerenom SSL certifikatu te posjećuje malicioznu web stranicu. Tu je još i, „X-Frame-Options“ opcija HTTP zaglavlja kojom se može onemogućiti prikazivanje web stranice unutar okvira (<frame> ili <iframe> elementa). Tracking Protection zajedno s listama, služi kako bi korisnici mogli izabrati koje web stranice smiju pratiti njihove online aktivnosti, sve u svrhu zaštite privatnosti. Tu je još i podsjetnik na postojanje protokola Online Certificate Status Protocol koji je namijenjen provjeri valjanosti SSL certifikata, odnosno je li certifikat povučen.

2 Tehnologije

2.1 Content Security Policy

Content Security Policy se omogućuje na strani poslužitelja koji se konfigurira tako da vraća HTTP zaglavlje X-Content-Security-Policy. CSP je u potpunosti kompatibilan i s web preglednicima koji ga ne podržavaju. Kad takav web preglednik naiđe na stranicu s uključenim CSP-om, jednostavno će navedeno zaglavlje ignorirati. Zasad tehnologiju podržava Mozilla Firefox 4.
Glavna uloga CSP-a je onemogućivanje i logiranje XSS napada. Takvi napadi koriste povjerenje koje web preglednik ima u sadržaj primljen s web stranice. Zaštitu od malicioznog sadržaja CSP postiže tako da administratorima poslužitelja nudi mogućnost definiranja domena u koje klijentov web preglednik može imati povjerenja, odnosno s kojih se smije izvršavati određeni sadržaj. Druga važna uloga je zaštita od tzv. „clickjacking" napada kod kojih maliciozna stranica zavara posjetitelja da mišem klikne na neki objekt koji se nalazi na drugoj web stranici. To se tipično izvodi postavljanjem sadržaja druge stranice unutar <iframe> elementa. Primjer za to bilo je širenje malicioznog sadržaja putem društvene mreže Facebook, točnije njenog „Like" gumba na kojeg su korisnici klikali ne znajući da to rade (tzv. „likejacking"). Pomoću CSP-a mogu se definirati i protokoli koji su dopušteni (npr. samo HTTPS). Društvena mreža Twitter već je počela koristiti CSP [3], a početak njegovog korištenja objavili su i mnogi drugi servisi. Također postoje programski dodaci, koji omogućuju njegovu jednostavnu implementaciju, namijenjeni poznatim sustavima za upravljanje web stranicama (CMS-ovima) kao što su WordPress, Django i Drupal.
U narednom dijelu poglavlja, opisan je način korištenja CSP-a sa stajališta klijenta i poslužitelja, odnosno administratora ili programera.

2.1.1 Inicijalne postavke

Dok je CSP uključen, na snazi je skup zabrana. Inicijalno je riječ o sljedećim zabranama:

1) inline JavaScript skripte - programski kod unutar HTML <script> elemenata se ignorira osim ako je atributom src definiran izvor s liste dopuštenih (white list)
2) kod iza javascript: URI-a se ignorira
3) ignorira se kod koji bi se trebao izvršiti nakon određenih događaja (event) poput onog definiranog atributom „onclick"
4) blokirana je JavaScript funkcija eval()
5) pozivi funkcijama windows.setTimeout() i window.setInterval() s parametrima tipa string (kao koda koji se treba izvršiti) se ignoriraju
6) blokirano je korištenje konstruktora Function() za definiranje funkcija iz koda u string (tekstualnom) formatu
7) blokirani su svi URI-ji koji sadrže podatke (data URI)
8) XBL binding je moguć jedino koristeći chrome: ili resource: URI-je
9) CSP atributi „policy-uri" i „report-uri" moraju upućivati na isti poslužitelj kao i dokument koji štite

Prve tri zabrane štite od XSS napada čineći ih vrlo teškim za izvesti. Kako bi XSS napad uspio, napadač mora imati pristup skriptnoj datoteci s bijele liste te istu referencirati unutar <script> atributa. Zabrane 4-6 onemogućuju ubacivanje malicioznog koda kroz tip podataka string, odnosno niz znakova. Znakovi mogu doći iz nesigurnih izvora, prenositi

se pomoću nesigurnih protokola ili ih napadači mogu ubaciti. Dvije pretposljednje zabrane onemogućuju ubacivanje malicioznog koda pomoću URI-ja, dok posljednja zabrana sprječava napadače da pomoću CSP zaglavlja izvrše napad na stranice koje nemaju uključenu CSP zaštitu.

2.1.2 Korištenje CSP-a

Sigurnosna politika CSP-a definira se spomenutim HTTP zaglavljem X-Content-Security-Policy i predstavlja skup direktiva (odvojenih točka-zarezom) koje opisuju kako će se CSP primjenjivati. Direktiva „allow" opisuje s kojih domena je dopušteno učitavati sadržaj i ona je jedina obvezna direktiva.
Na primjer, ukoliko administrator želi da se sadržaj učitava samo s domene web stranice, isključujući čak i poddomene, to će definirati na sljedeći način:

```
X-Content-Security-Policy: allow 'self'
```

Ako se želi korisnicima dozvoliti učitavanje slika s bilo kojih domena, ali ograničiti učitavanje video i audio datoteka s dva provjerena izvora te skripti s jednog izvora, to se radi ovako:

```
X-Content-Security-Policy: allow 'self'; img-src *; media-src media1.com
media2.com; script-src skripte.primjer.com
```

Zvjezdica (*) je specijalni znak koji označava bilo koju domenu. Ukoliko se želi osigurati da se sadržaj prenosi isključivo protokolom SSL s točno jedne domene, to se čini ovako:

```
X-Content-Security-Policy: allow https://banking.banka.com
```

2.1.3 Parametri pri definiranju sigurnosnih pravila

Za definiranje sigurnosnih pravila poput onih prethodno spomenutih, koristi se nekoliko parametara. Većina direktiva zahtjeva navođenje izvora sadržaja (u obliku skupa znakova) s kojeg se sadržaj smije učitati.
Poslužitelji se označavaju putem domena ili IP adresa. Pomoću zvjezdice (*) moguće je označiti skup domena, a moguće je i specificirati port (iza dvotočke nakon oznake za poslužitelja). Ako se navodi više poslužitelja ili skupova poslužitelja, između njih se stavlja razmak.
Neki od parametara (sekcija) kojima se definiraju sigurnosna pravila su:

- **allow** - najvažnija sekcija, ujedno i jedina koja je nužna; definira da je zabranjen sav sadržaj osim onog koji je eksplicitno dopušten
- **options** - omogućuje proširenje skupa dopuštenog sadržaja (inicijalno zabranjenog), a to su: inline-script (omogućuje korištenje javascript: URI-ji) i eval-script (eval() i slične metode)
- **img-src** - specificira s kojih izvora se smiju učitavati slike i fav-ikone
- **media-src** - specificira s kojih izvora se smije učitavati sadržaj unutar <audio> i <video> elemenata nove HTML inačice 5
- **script-src** - definira izvore s kojih je dopušteno učitavati JavaScript kod
- **object-src** - definira izvora za elemente <object>, <embed> i <applet>
- **frame-src** - definira otkud se smije učitati sadržaj <frame> i <iframe> elemenata

- **frame-ancestors** - definira listu poslužitelja kojima je dopušteno staviti našu web stranicu unutar <frame> ili <iframe> elemenata; treća stranica koja (pomoću tih elemenata ulančano) učitava drugu koja onda učitava našu stranicu također mora biti navedena u listi. Drugim riječima, ako web stranica 1 postavlja web stranicu 2 unutar iframe elementa, dok ona postavlja web stranicu 3 unutar iframe-a, web stranica 3 mora unutar frame-ancestors liste uključiti web stranice 1 i 2.
- **style-src** - definira iz kojih se izvora smiju učitavati datoteke stilova (stylesheet), to uključuje i eksterno i „inline" učitavanje
- **policy-uri** - pokazuje lokaciju vanjske datoteke koja sadrži sigurnosnu politiku (umjesto da se ona definira unutar HTTP zaglavlja); datoteka mora biti na istom poslužitelju kao i web stranica koju štiti

Osim parametara, postoje i dvije ključne riječi se koriste za opis posebnih klasa izvora sadržaja. To su:

- **'self'** - označava poslužitelj na kojem se nalazi web stranica
- '**none**' - označava prazan skup, odnosno zabranjuje sve poslužitelje

2.1.4 Izvještaji o pokušajima napada

Jedna od važnih značajki CSP-a je mogućnost generiranja i dostavljanja izvještaja o zabilježenim napadima. Administratori mogu definirati format izvještaja, a dostavljaju se putem HTTP POST metode na poslužitelje navedene parametrom „**report-uri**". Inicijalno je ova mogućnost isključena. Kako bi se spriječilo napadače u otimanju navedenih izvještaja u svrhu prikupljanja informacija o meti, poslužitelj ne šalje izvještaje u slučaju primanja zahtjeva za preusmjeravanjem.

Primjer definicije pravila koje uključuje slanje izvještaja na poslužitelj izvjestaji.primjer.com:

```
X-Content-Security-Policy: allow self; report-uri
http://izvjestaji.primjer.com/skripta.cgi
```

JSON objekt izvještaja sadrži sljedeće podatke:

- **request** - HTTP zahtjev koji je doveo do zlouporabe, uključuje metodu, put do traženog sadržaja i HTTP verziju
- **request-headers** - HTTP zaglavlja koja su poslana tijekom povrede CSP-a
- **blocked-uri** - URI sadržaja koji je blokiran
- **violated-directive** - parametar prekršenog pravila
- **original-policy** - definicija prekršenog pravila

2.2 HTTP Strict Transport Security

HTTP Strict Transport Security je sigurnosna mjera koja web stranicama omogućuje da web preglednicima nalažu korištenje isključivo protokola HTTPS, umjesto HTTP. Naime, u slučaju kad web stranica prima vezu prvo putem HTTP-a, a tek onda preusmjerava na HTTPS, postoji opasnost od „man-in-the-middle" napada. Napadač može provesti takav napad preusmjeravajući korisnika na malicioznu web stranicu umjesto na sigurnu inačicu legitimne web stranice. Uz Strict Transport Security, takva vrsta napada je onemogućena jer nakon što korisnik pristupi web stranici putem HTTPS-a koja koristi navedenu zaštitu, ona prisiljava web preglednik da se odsad spaja isključivo putem HTTPS-a.

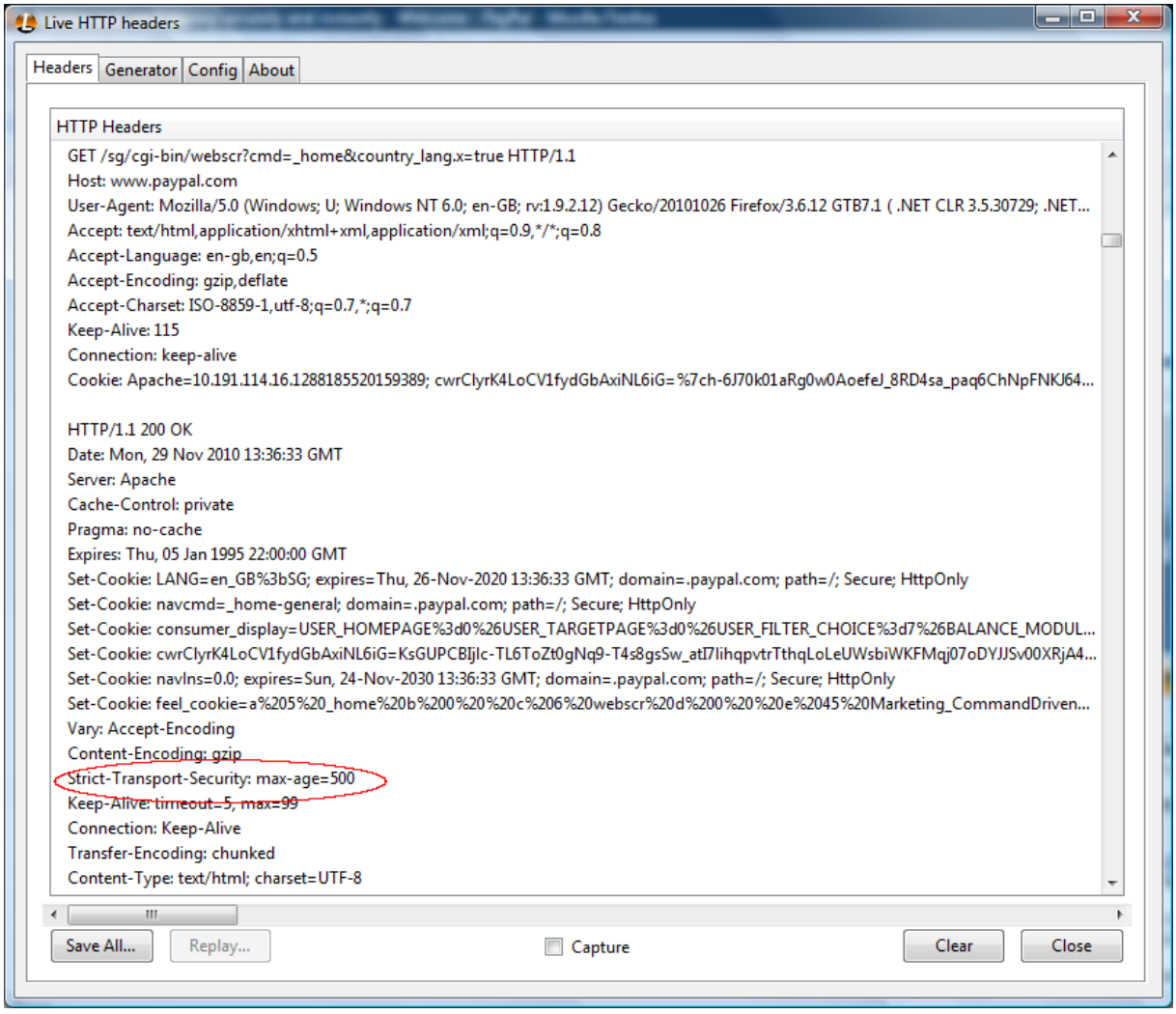
Strict Transport Security se uključuje putem HTTP zaglavlja stranice koja se štiti:

```
Strict-Transport-Security: max-age:expireTime [; includeSubdomains]
```

parametri su definirani kako slijedi:

- **expireTime** - predstavlja vrijeme u sekundama u kojem web preglednik pamti da se štićenoj stranici može pristupati samo putem HTTPS-a
- **includeSubdomains** (opcionalan) - ako je prisutan, primjenjuje se i na sve navedene poddomene

Kad web preglednik pristupi stranici koju štiti Strict Transport Security, on preuzima Strict-Transport-Security zaglavlje i sve buduće zahtjeve za učitanjem stranice preko HTTP-a obrađuje koristeći HTTPS protokol dok ne istekne definirani vremenski interval (expireTime). Svakim preuzimanjem navedenog zaglavlja, preglednik osvježava vrijednost vremenskog intervala.
Jedan od poznatih web servisa koji koristi STS je PayPal (slika). Upisivanjem URL-a http://www.paypal.com (ili samo www.paypal.com), preglednik nas automatski preusmjerava na zaštićenu stranicu https://www.paypal.com.



2.1: HTTP zaglavlje servisa PayPal u kojem je vidljiva upotreba STS

2.3 X-Frame-Options

HTTP zaglavlje odgovora, „X-Frame-Options“ definira smije li web preglednik prikazati web stranicu unutar <frame> ili <iframe> elementa. Cilj ove mjere je zaštita od potencijalnih clickjacking napada koji koriste prikaz sadržaja neke legitimne web stranice unutar spomenutih elemenata. Ova sigurnosna mjera premijerno je predstavljena u web pregledniku Internet Explorer 8, a tablica ispod daje uvid od kojih inačica najpopularnijih web preglednika je mjera podržana.

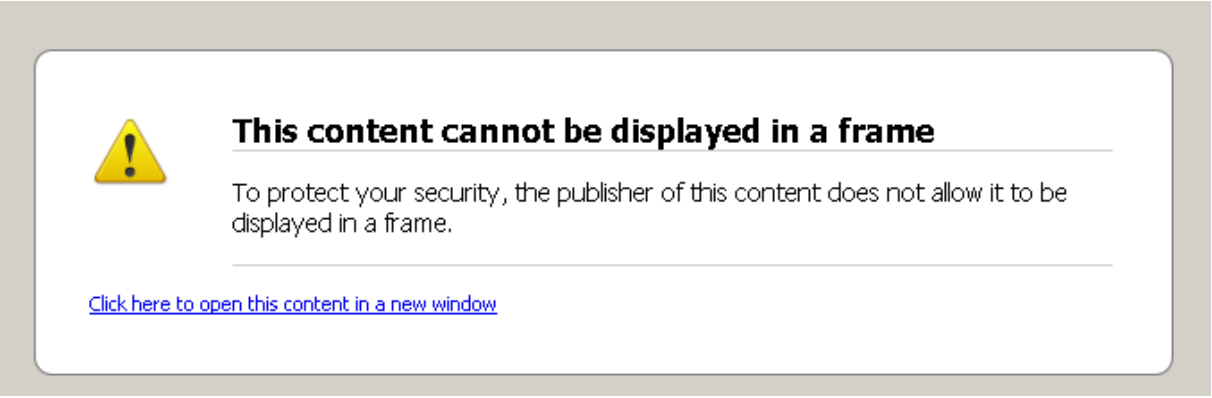
2.1: inačice preglednika od kojih je podržana opcija X-Frame-Options

web preglednik	najniža inačica koja podržava X-Frame-Options
Internet Explorer	8.0
Firefox	3.6.9
Opera	10.50
Safari	4.0
Chrome	4.1.249.1042

Zaglavlje ima dvije opcije kod konfiguriranja:

- **DENY** - uz postavljenu ovu opciju, općenito je zabranjeno da se web stranica prikazuje u okviru
- **SAMEORIGIN** - uz ovu opciju, web stranica se smije prikazati u okviru jedino ako se okvir nalazi na istoj domeni

U slučaju zabrane učitavanja web stranice u okvir, na ovaj način, u okvir se postavlja prazna web stranica (u slučaju Firefoxa, prazan okvir je označen sa about:blank), a nakon toga se na to mjesto postavlja poruka o pogrešci (prikazana na slici, kod preglednika Firefox)



2.2: poruka o pogrešci radi X-Frame-Options zaštite kod Firefoxa

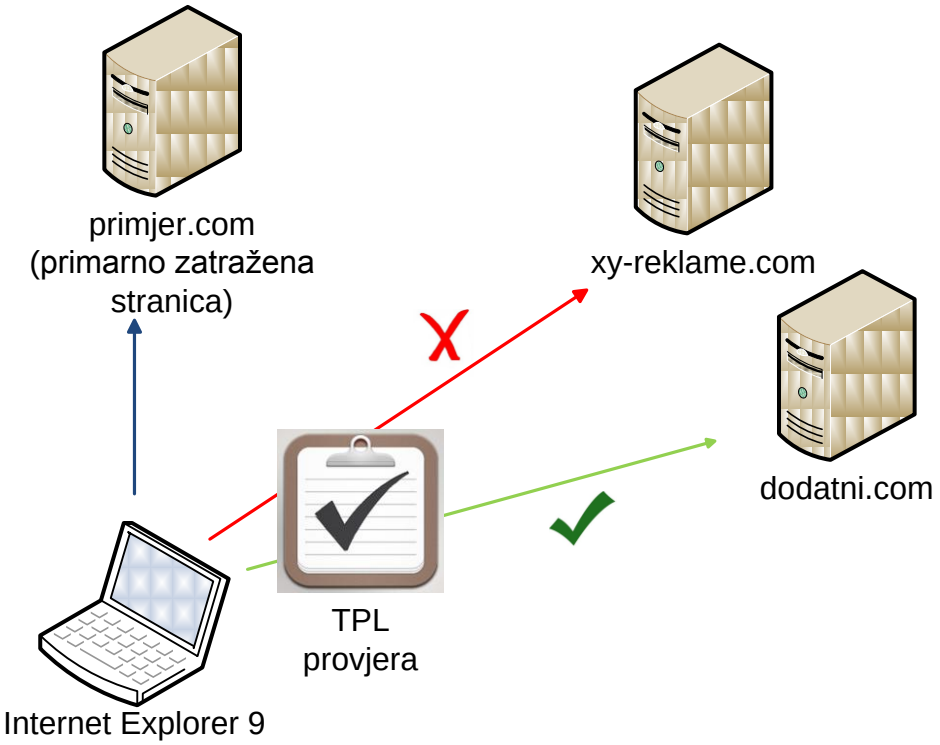
2.4 Tracking Protection i Tracking Protection Lists

Danas korisnici dijele mnoštvo informacija širom Interneta, a da toga često nisu ni svjesni. Web stranice tako mogu putem korisnikovog web preglednika doći u posjed podataka kao što su web stranice koje je posjetio, a to se obično koristi u svrhu personaliziranog

oglašavanja. Međutim, izlaganje takvih podataka može imati i neželjene posljedice, kao što su uvijek prisutni razni oblici zlouporabe i povrede privatnosti.
Zajedno s novom inačicom svojeg web preglednika Internet Explorera 9, Microsoft je predstavio i dvije tehnologije koje bi korisnicima trebale omogućiti kontrolu nad podacima o svojim online aktivnostima. Drugim riječima, korisnici tako dobivaju mogućnost definiranja koje web stranice smiju pratiti njihovu aktivnost.
Riječ je o:

- **Tracking Protection** - mehanizam putem kojeg korisnik može identificirati i blokirati praćenje svojih aktivnosti (mehanizam je „opt-in“, odnosno korisnik ga mora eksplicitno uključiti kako bi ga mogao koristiti)
- **Tracking Protection Lists (TPL)** - liste pomoću kojih korisnici mogu definirati koji sadržaj s web stranica smije pratiti njihove aktivnosti

TPL je lista URL-ova (poput google.com) koje će preglednik posjetiti jedino u slučaju ako ih korisnik posjećuje direktno klikom na link ili upisom u adresno polje. Prije slanja HTTP zahtjeva, IE9 provjerava TPL listu, odnosno je li zatraženi URL odobren. Limitiranjem zahtjeva prema web stranicama i sadržaja koji dolazi s drugih stranica (indirektno), ovo ograničava količinu korisničkih informacija koja se može prikupiti. Inicijalno, ova lista je prazna te je korisnik postepeno popunjava ovisno o svojim izborima, odnosno potrebama. Korisnik može koristiti više listi koje može preuzeti na Internetu od trećih strana, odnosno različitih organizacija koje se bave očuvanjem privatnosti.
Korištenje TPL-a blokira mnoge reklamne sadržaje koje se pojavljuju na web stranicama, te se ta mogućnost često uspoređuje s popularnim dodatkom za preglednik Firefox, AdBlock.

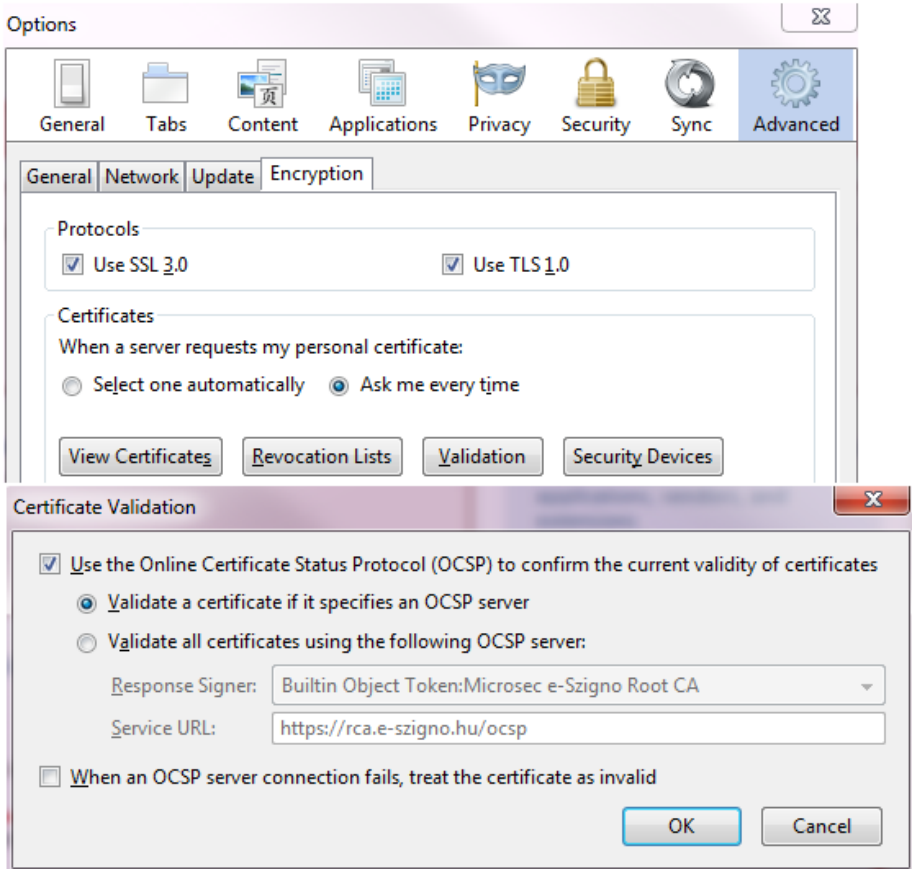


2.3: način rada Tracking Protection listi

2.5 Online Certificate Status Protocol

Kako bi infrastruktura javnih ključeva (PKI) radila pouzdano, nužno je da provjera i povlačenje certifikata rade pouzdano. Napadači često koriste neispravne, pa čak i ukradene SSL certifikate na svojim malicioznim stranicama radi uvjerljivosti, stoga je od vrlo velike važnosti na vrijeme blokirati takve certifikate.

Za razliku od ranije opisanih sigurnosnih mjera, protokol OCSP postoji već duži niz godina, a o vrsti i inačici web preglednika ovisi o tome je li inicijalno uključen. Konkretno, podržan je od inačice Internet Explorera 7 za Windows Vistu, od prve inačice Firefoxa, dok je Firefox 3 prva inačica koja ga inicijalno uključuje. Također je podržan od prve inačice Chromea i Opere 8.0. U web pregledniku Safari na Apple Mac OS X operacijskom sustavu, on se mora ručno uključiti u aplikaciji Keychain Access.



2.4: uključivanje OCSP-a u web pregledniku Mozilla Firefox

Online Certificate Status Protocol (OCSP) je Internet protokol koji se koristi za dohvaćanje liste povučenih X.509 certifikata, a stvoren je kao alternativa CRL (Certificate Revocation List) listama s kojima su zabilježeni određeni problemi. Naime, CRL liste su se pokazale neefikasnima u smislu prevelike potrošnje prostora i opterećenja mreže. Upravo radi rješenja tog problema se razvio OCSP koji koristi optimizirane poruke koje se obično prenose protokolom HTTP. Poruke se prenose na način zahtjeva i odgovora, a OCSP poslužitelji se nazivaju responderi. OCSP responder na zahtjev klijenta vraća odgovor koji može biti da je certifikat dobar, povučen ili nepoznat. Protokol može biti realiziran i hijerarhijski, tako da nekoliko respondera odgovara višem tijelu te da pri tome međusobno provjeravaju svoje odgovore i uspoređuju ih s odgovorom višeg tijela.

3 Zaključak

Koncentriranjem na sve veći razvoj sigurnosnih zaštita, proizvođači web preglednika, pokazali su da je im je jasan utjecaj kojeg ima sigurnost običnih korisnika. Takvi korisnici su najranjiviji te im je potrebno pružiti što sigurniju okolinu. Web preglednici postali su vektori napada u velikom broju slučaja. Postoji cijeli niz različitih vrsti napada na dinamičke web stranice, a ove mjere su korak u pravom smjeru jer ih u većini slučajeva mogu spriječiti. Privatnost korisnika i posljedice koje mogu nastati izlaganjem neželjenih podataka često su zanemarene. Upitan je i način na koji različiti servisi za reklamiranje koriste te podatke. Stoga je predstavljanje tehnologija kao što je Tracking Protection također važan korak unaprijed.

Kod razvoja i primjene sigurnosnih poboljšanja, uvijek je potrebno tražiti ravnotežu između ostvarenog stupnja sigurnosti i lakoće korištenja. Nove sigurnosne mjere u web preglednicima pružaju dobar odnos jer je njihova implementacija vrlo jednostavna. Međutim, uvijek treba imati na umu da ni jedna zaštita ne može biti potpuna te da napadači uvijek pronalaze nove metode za uspješno izvođenje svojih zlonamjernih aktivnosti.

4 Literatura i reference

1. Content Security Policy, https://developer.mozilla.org/en/Security/CSP, Mozilla Developer Network , listopad 2010.
2. Firefox 4 With Content Security Policy Due Tuesday, http://threatpost.com/en_us/blogs/firefox-4-content-security-policy-due-tuesday-032211, ThreatPost , 22.3.2011.
3. Twitter integrates Firefox 4 security feature, http://www.zdnet.co.uk/blogs/security-bullet-in-10000166/twitter-integrates-firefox-4-security-feature-10022060/, ZDNet, 24.3.2011.
4. IE9 with do-not-track option released, http://www.scmagazineus.com/ie9-with-do-not-track-option-released/article/198392/ , SC Magazine US, 15.3.2011.
5. Firefox 4 final to shipped with HTTP Strict Transport Security (Force HTTPS) Support, http://techdows.com/2010/08/firefox-4-final-to-shipped-with-http-strict-transport-security-force-https-support.html, 28.8.2010.
6. IE9 and Privacy: Introducing Tracking Protection, http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx , MSDN Blogs, 7.12.2010.