Protocolul HSTS impotriva atacurilor MITM

Rodica BULAI, Eugeniu CUCU
Technical University of Moldova
rodica.bulai@mail.utm.md, eugeniu.cucu@ati.utm.md

***Abstract* — Un atac man-in-the-middle (MITM) este un tip de atac cibernetic care permite unui actor rău intenționat să facă interceptarea, trimiterea și primirea datelor destinate pentru altcineva. Un atac MITM exploatează procesarea în timp real al tranzacțiilor, conversațiilor sau transferul altor date.**

HTTP Strict Transport Security (HSTS), este un protocol de securitate care forțează browser-ele Web, să folosească doar conexiuni HTTPS, pentru securizarea datelor.

***Index Terms* — MITM, HTTPS, HSTS, certificare SSL, SSLStrip.**

I. INTRODUCERE

Într-o rețea de calculatoare este foarte important ca informațiile transmise să nu poată fi accesate sau interceptate de către persoane neautorizate.

Acest aspect este esențial în condițiile în care rețelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea de operațiuni bancare.

Serverele Web, nu sunt conectate direct intre ele și datele transmise trebuie să treacă prin diverse routere de rețea. Aceste routere, sunt situate intre servere și au acces complet la cererile trimise prin HTTP.

Datele trimise prin HTTP, sunt transferate ca text simplu, necriptate și routerele pot acționa ca un MITM, care pot citi sau chiar redirecționa datele respective. Un atac de tip MITM (omul de la mijloc), este un atac destul de complicat în care atacatorul se interpune ca „unealta de tranzit", între două sisteme, respectiv server și router. Persoana care face transferul de date este convinsa că datele transmise ajung la sursa, însă în realitate, atacatorul controlează toate datele și, în special, sunt urmărite tranzacțiile financiare.

II. HTTP STRICT TRANSPORT SECURITY (HSTS)

HSTS este o opțiune de imbunătățire a securiții care este specificată de aplicația web prin utilizarea unui antet HTTP special indicat în răspuns.

Odată ce un browser acceptat primește acest antet, browserul va împiedica transmiterea oricăror comunicări prin HTTP către domen-ul specificat și va trimite în schimb toate comunicările prin HTTPS, fig.1.

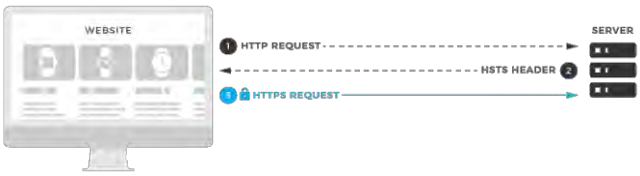

Fig.1 – Comunicații HSTS

Specificația a fost lansată și publicată la sfârșitul lui 2012 ca RFC 6797 (HTTP Strict Transport Security (HSTS)) de către IETF [1].

HSTS abordează următoarele amenințări:

1. User-ul salvează site-urile sau introduce manual http://example.com și este supus unui atac de tip man-in-the-middle
   - HSTS redirecționează automat cererile HTTP către HTTPS pentru domen-ul cerut
2. Aplicația Web care este destinată de a utiliza doar conexiune HTTPS conține în mod neadecvat legături HTTP sau servește conținut prin HTTP.
   - HSTS redirecționează automat cererile HTTP către HTTPS pentru domen-ul cerut.
3. Un atacator "man-in-the-middle" încearcă să intercepteze traficul de la un utilizator victima folosind un certificat nevalid și speră că utilizatorul va accepta certificatul.
   - HSTS nu permite unui utilizator să suprascrie certificatul nevalid.

După cum s-a menționat mai sus, unul dintre atacurile prin care se poate intercepta traficul dintre două calculatoare din aceeași rețea este MAN-IN-THE-MIDDLE-ATTACK. Din păcate este greu detectabil și ușor de folosit în rețelele locale actuale.

Un atac MITM poate fi ușor efectuat cu asa instrumente ca SSLStrip [2].

SSLStrip este un instrument care deturnează transparent traficul HTTP într-o rețea, urmărește link-urile HTTPS și redirecționările, iar apoi redirecționează aceste link-uri în link-uri HTTP.

În SSL Strip, tot traficul de la dispozitivul victimei este direcționat printr-un proxy creat de atacator și poate fi gândit ca atac Man-in-the-middle.

Un scenariu în care există o victimă (A), un atacator (B) și un server (C), fig. 2 arată cum SSL Strip rulează pe mașina atacator, care este un server proxy; prin urmare, nu există nici o legătură directă între victimă și server.

Prin urmare traficul este redirecționat, captat, modificat și prezintă o amenințare pentru victima.

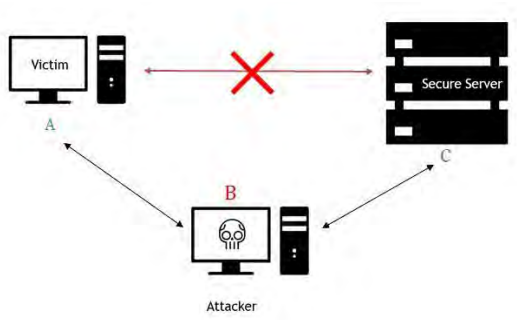

Fig. 2 – Atac MITM

Deci lipsa implementării HSTS, poate duce la preluarea datelor sau utilizatorul poate sa fie redirecționat către pagini clonate, folosite de atacator pentru a copia date personale, parole de logare în diverse conturi sau date despre carduri de credit.

Politica HSTS forțează toate răspunsurile sa treacă prin conexiuni HTTPS (certificare SSL). Acest lucru ne asigura faptul ca întregul canal este criptat înainte ca datele sa fie trimise. Implementarea HSTS face imposibila modificarea datelor în tranzit de către atacatori.

Trecerea de la http://, la conexiuni https://, (cu SSL), ofera cea mai buna aparare impotriva atacatorilor. HSTS, asigură că toate conexiunile sunt criptate și se folosește doar https://.

III. UTILIZARE HSTS

Implementarea HSTS se poate face în mai multe moduri și diferă în funcție de serverul de hosting.

Pentru început trebuie de adaugat antetul HSTS în toate răspunsurile venite de la server.

Activarea HSTS pe un server implică adăugarea următorului antet de răspuns HSTS într-un răspuns HTTPS:

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

De exmplu, *Strict-Transport-Security: max-age=16070400; includeSubDomains*

Parametrul care trebuie inclus obligatoriu este durata maximă în secunde *max-age*.

Acest parametru specifică timpul în care browserul trebuie să se conecteze la server folosind conexiunea HTTPS.

Chiar daca parametrul include și *SubDomains*, el nu este obligatoriu. Totuși este recomandat de inclus, astfel încât browserul să utilizeze conexiunea HTTPS pentru subdomen-uri existente și viitoare.

Atunci când browser-ul accesează resursa web, serverul răspunde cu antetul HSTS.

Aceast lucru instruiește browserul să se conecteze la server și la întregul domen prin HTTPS. Browserul va reține apoi că va folosi conexiunea HTTPS pentru durata specificată în parametrul max-age.

Chiar dacă un utilizator va introduce http://www.domain.com, sau introduce numele de domen fără http, utilizează un marcaj sau o legătură HTTP utilizată de server, browserul va redirecționa automat cererea în HTTPS.

Odată ce durata maximă expiră, browserul începe să acceseze serverul prin HTTP, cu excepția cazului în care utilizatorul specifică HTTPS.

După primirea antetului HSTS, browserul trimite o solicitare HTTPS.

HSTS este acceptat de majoritatea browserelor. Chrome și Mozilla Firefox mențin o listă de preîncărcări HSTS care informează automat browserul că site-ul web poate fi accesat numai prin HTTPS.

Un inginer web poate adăuga un site web în lista HSTS preîncărcată adăugând parametrul "preload" în antetul răspunsului de pe server.

De exemplu, *Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.*

IV. CONCLUZII

Un atac MITM poate fi realizat foarte ușor doar cu câteva utilitare gratuite sslstrip, arpspoof, iptables care sunt prezente în sistemul de operare Kali Linux. Unica problemă ar fi accesarea rețelei locale. Într-o rețea Wi-Fi necunoscută, avem nevoie, cel puțin, de parola de acces, pe când într-o rețea deschisa, este foarte simplu de utlizat aceste unelte știind doar gateway-ul serverului.

Avantajul principal al instrumentului SSLStrip este că browser-ul dvs. nu va afișa orice eroare de certificat SSL, iar victimele nu au nici un indiciu că un astfel de atac are loc, deci trebuie prevenit.

HTTP Strict Transport Security este o politică de securitate web simplă, dar puternică, care asigură site-urile HTTPS împotriva atacurilor MITM.

Cauzează browserele compatibile să impună regulile de securitate prin redirecționarea automată a tuturor legăturilor HTTP în legături HTTPS.

Trecerea de la HTTP la conexiunile securizate HTTPS (cu SSL) oferă cea mai bună apărare împotriva atacurilor de redirecționare.

Chiar și atunci când într-o rețea nesigura, un atacator nu poate forța browserul să utilizeze conexiunea nesecurizată HTTP.

HSTS asigură că toate comunicările vor fi criptate și toate răspunsurile trimise și primite sunt livrate către - și primite de la - serverul autentificat.

BIBLIOGRAFIE

[1] [Resursă electronică] - Regim de access: https://tools.ietf.org/html/rfc6797.

[2] [Resursă electronică] - Regim de access: https://tools.kali.org/information-gathering/sslstrip.

[3] [Resursă electronică] - Regim de access: https://github.com/moxie0/sslstrip.

[4] [Resursă electronică] - Regim de access: http://www.paladion.net/ssl-stripping-revisiting-http-downgrading-attacks/.

[5] [Resursă electronică] - Regim de access: http://www.veracode.com/security/man-middle-attack.