SHARKFEST '12

Wireshark Developer and User Conference

Hands-On LAB: SSL Troubleshooting with Wireshark and Tshark

Sake Blok

Application Delivery Networking Consultant and Troubleshooter

sake.blok@SYN-bit.nl

About you?

- Who…
  - …thinks SSL is just about encryption?
  - …troubleshooted SSL traffic before?
  - …knows the purpose of each handshake message?
  - …tried to decrypt SSL traffic before?
  - …and ran into problems decrypting?
  - …troubleshooted client authentication problems?

About me?

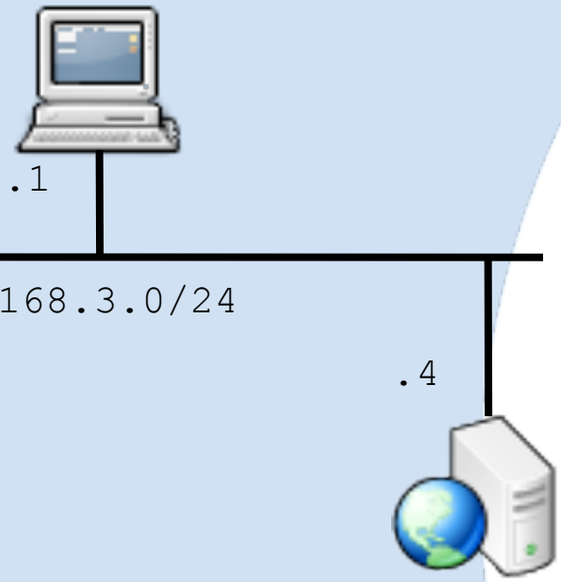
- Started SYN-bit in 2009
- Application Delivery Networking Consultant & Troubleshooter (F5 Networks, Cisco ACE, Alteon)
- Have used SSL extensively in customer projects
- Using Ethereal since 1999, developing since 2006, member core-developers since 2007
- Enjoy scuba diving and art-house movies

Sake Blok sake.blok@SYN-bit.nl

Lab setup

Client
WinXP - Firefox

Client-cert 1: Neo
Client-cert 2: Trinity



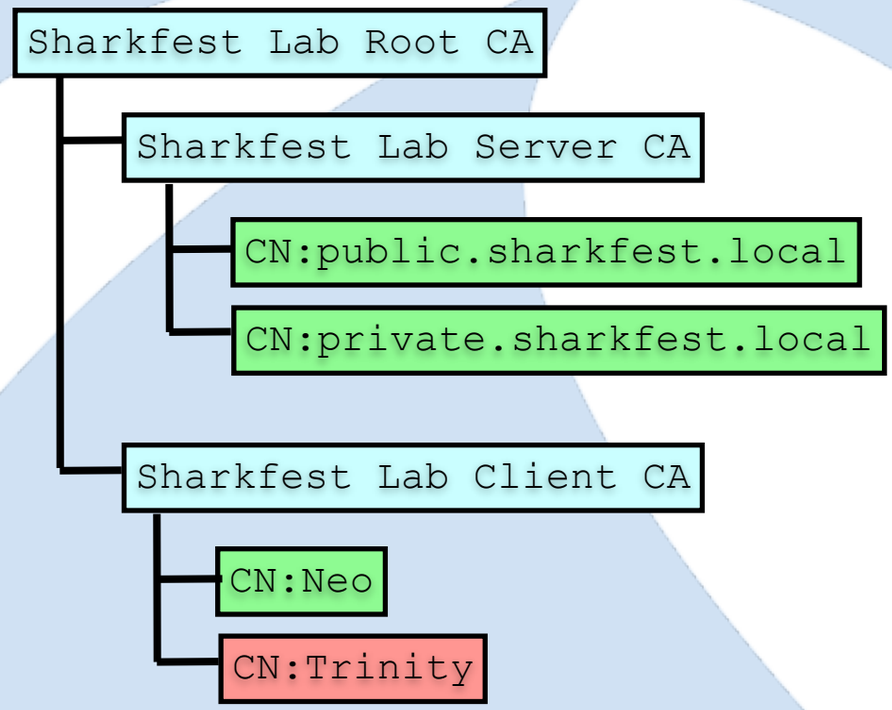
(virtual) Server 1
Ubuntu - Apache

Server-cert:
public.sharkfest.local

(virtual) Server 2
Ubuntu - Apache

Server-cert:
private.sharkfest.local

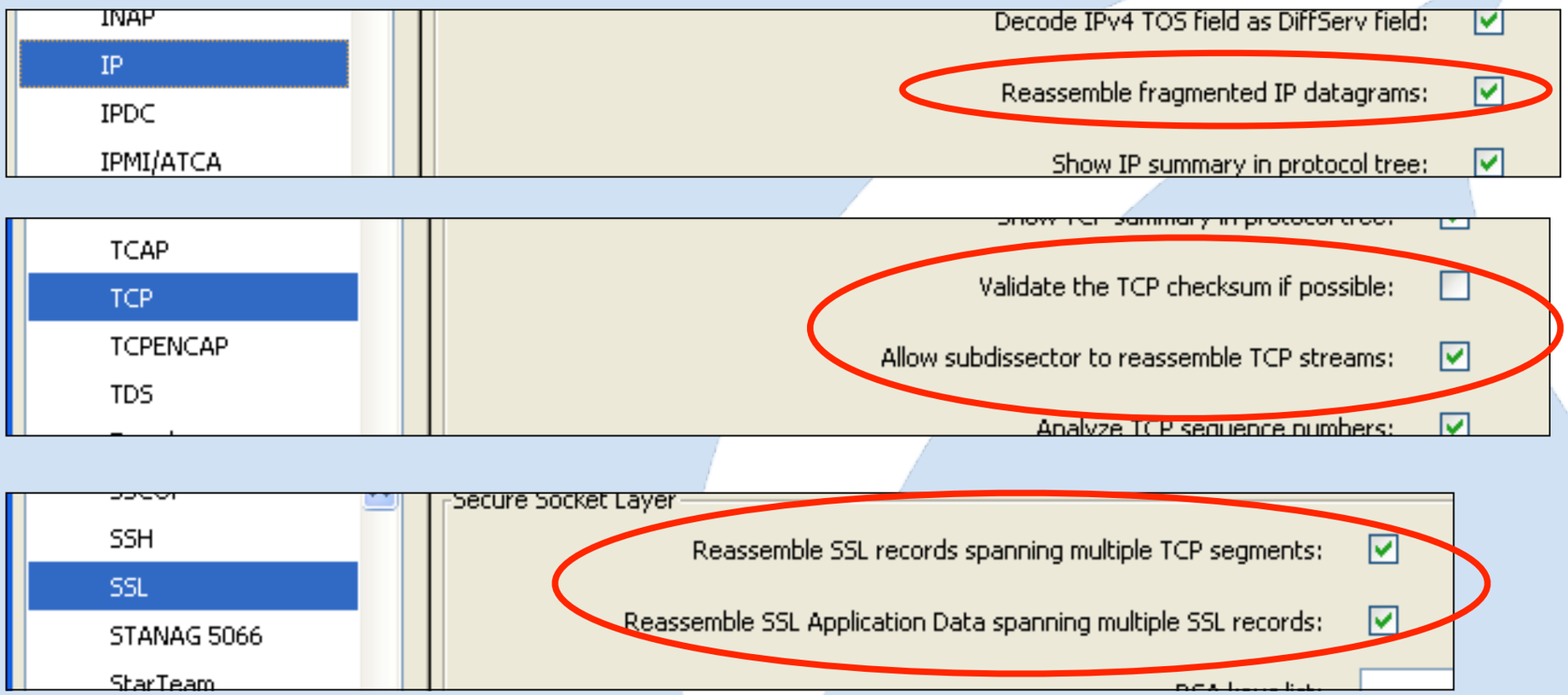
Require Client-Certificate



Getting the labguide & files

- Use my AP to connect to my Linux-VM
- SSID: SYN-bit-wrt54g
  Password: wpa2@linksys
- Goto http://192.168.10.2/sharkfest
- Download&view labguide.pdf

Choosing the right settings




```
ip.defragment: TRUE
tcp.check_checksum: FALSE
tcp.desegment_tcp_streams: TRUE
ssl.desegment_ssl_records: TRUE
ssl.desegment_ssl_application_data: TRUE
```

Exercises

1. Exploring a normal SSL session
2. Extracting a certificate from a trace file
3. SSL decryption
4. Exporting and importing SSL session keys (to provide to a 3rd party)
5. (optional) Changing Firefox SSL Settings to make decryption work

1) Exploring a normal SSL session

Tracefile : ssl.cap

a) Which cipher suites does the client support?
b) Which cipher suite was chosen by the server?
c) Which CA has signed the server certificate?
d) What is the common name of the server certificate?
e) How many SSL negotiations are present in the file?
f) How many of them are full handshakes?
g) Were the clocks of the client and the server in sync?

2) Extracting a certificate from a trace file

Tracefile : ssl.cap

a) Select the first frame with a certificate, which frame have you selected?

b) How many certificates were sent by the server?

c) What does the certificate chain look like?

d) Select the Intermediate CA certificate and export it to file. Be careful that you just export one certificate and that you do not include the length field in the export.

e) If you exported the correct bytes, you can open the saved certificate in your browser. Can you?

3) SSL decryption

Tracefile : ssl.cap
Keyfile : ssl.pem

a) Add the private key to the SSL settings to enable decryption. Can you see http traffic in Wireshark now?
(hint: you need to use 192.168.3.3, 443, http, <file-location>)

b) Does the Host: header match the common name in the certificate? Would the user have noticed this?

c) Are all SSL sessions decrypted?

d) Do a "Follow TCP stream" and "Follow SSL stream" on the first session. What's the difference?

e) Save frame 23-37 in a separate file and open it. Is decryption still working? If not, why not? Keep the file for the next exercise.

4) Exporting and importing SSL session keys (to provide to a 3rd party)

Tracefile : ssl.cap
Keyfile : ssl.pem

a) If removed, reconfigure the private key in the SSL protocol preferences. Make sure all sessions are decrypted.

b) Export the SSL session keys to a file with "File -> Export SSL session keys". Open the file in a text editor and remove the line where Session-ID starts with "fbcf"

c) Now remove the private key from the SSL protocol preferences and point "(Pre)-Master Secret..." to the file with the exported keys.

d) Which SSL sessions are now decrypted?

e) Are you able to decrypt the session in the file from exercise 3d? Was it using the deleted SSL-id?

5) Changing Firefox SSL Settings to make decryption work

Live capture of traffic to https://192.168.10.2/sharkfest

a) Use wireshark to capture the following traffic

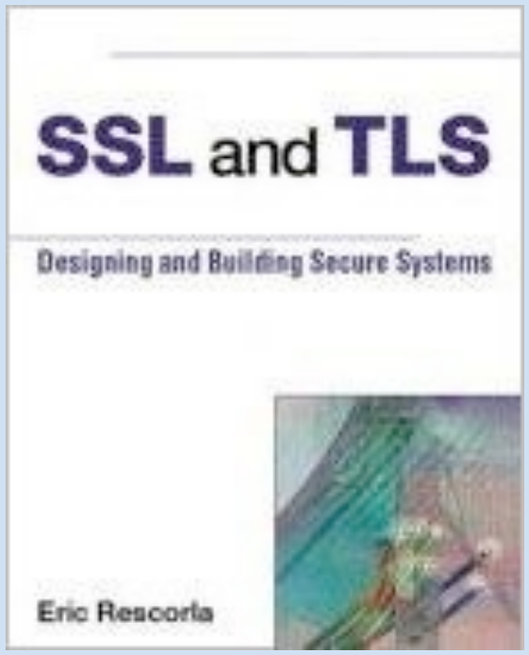
b) Use firefox to go to https://192.168.10.2/sharkfest/ and reload the page a few times. Use the previously downloaded key to decrypt the session. Does it work? Which cipher suite is used?

c) Use the url about:config in Firefox to change some settings. Filter on *"security.ssl3*dh*"* and make sure they are all disabled (false).

d) Perform *a)* again, what differences do you see in the SSL packets?

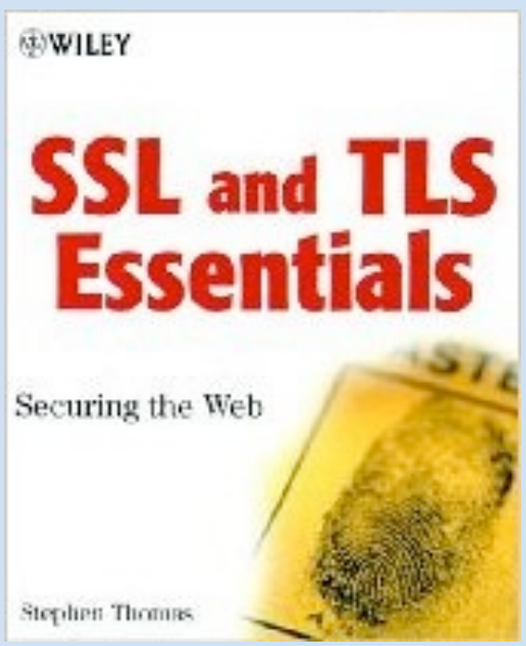
e) In the same manner change *security.enable_tls_session_tickets* to false. Now look at the differences in the tracefile and whether packets are decypted or not. What differences do you see?

Further Reading about SSL



SSL and TLS: Designing and Building Secure Systems

by Eric Rescorla



SSL and TLS Essentials: Securing the Web

by Stephen A. Thomas

Questions & Discussion

FIN/ACK, ACK, FIN/ACK, ACK!

Thank You!

Sake Blok

sake.blok@SYN-bit.nl