HTTPS-Analyse

Wireshark unterstützt die Entschlüsselung von SSL/TLS Sessions, wenn man das Master-Secret berechnen kann.Bei Cipher Suites, welche das RSA-Kryptosystem verwenden, kann der private RSA-Schlüssel zum Entschlüsseln des pre-master secret verwendet werden. Wenn jedoch die Diffie-Hellman cipher-suites verwendet werden, wird der private RSA-Key nur zum Signieren der Diffie-Hellman Parameter verwendet.

Wenn man nun Wireshark verwendet gibt es mehrere Methoden SSL/TLS zu entschlüsseln. Die erste Möglichkeit ist das Entschlüsseln des Pre-Master-Secret mit dem privaten RSA-Key, jedoch funktioniert dies nur nur bei RSA-Kryptosystemen. Die andere Möglichkeit ist eine SSL Keylogfile festzulegen, welche das Master-Secret speichert.

In den folgenden Schritten zeige ich wie man nun ein SSL Keylog File generiert und anschließend per Wireshark mitgeschnitten Traffic entschlüsselt.

Unter Windows

Systemeigenschaften

1. Unter Systemeigenschaften, klickt man auf Erweitert dann auf Umgebungsvariable.

 \times

Computername	Hardware	Erweitert	Computerschutz	Remote	
Sie müssen als Administrator angemeldet sein, um diese Änderungen durchführen zu können. Leistung					
Visuelle Effekte, Prozessorzeitplanung, Speichemutzung und virtueller Speicher					
				<u>E</u> instellungen	
Benutzerprof	le				
Desktopeins	tellungen be	züglich der	Anmeldung		
				Einstellungen	
Starten und	Niederherste	llen			
Systemstart,	Systemstart, Systemfehler und Debuginformationen				
				Ei <u>n</u> stellungen	
			<u>U</u> mge	ebungsvariablen	
		(OK Abbred	Chen Ü <u>b</u> ernehmen	

Anlegen einer neuen Systemvariable indem man auf Neu klickt. 2.

Umgebungsvariablen

Variable	Wert	^	
JD2_HOME	D:\Users\larsm\AppData\Local\JDownloader 2.0		
MOZ_PLUGIN_PATH	IN_PATH C:\Program Files (x86)\Foxit Software\Foxit Reader\plugins\ C:\OneDrive C:\Users\larsm\AppData\Local\Microsoft\WindowsApps;		
OneDrive			
Path			
QT_DEVICE_PIXEL_RATIO	auto	ľ	
SSLKEYLOGFILE	D:\data\ssl\sslkeylog.log		
TEMP	C:\Users\larsm\AppData\Local\Temp	•	
	Neu Bearbeiten Löschen		
stemvariablen			
stemvariablen Variable	Wert		
stemvariablen Variable asl.log	Wert Destination=file		
stemvariablen Variable asl.log ComSpec	Wert Destination=file C:\Windows\system32\cmd.exe		
stemvariablen Variable asl.log ComSpec DriverData	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData	•	
stemvariablen Variable asl.log ComSpec DriverData JAVA_HOME	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData C:\Program Files\Java\jdk-11.0.1	,	
stemvariablen Variable asl.log ComSpec DriverData JAVA_HOME JC_CLASSIC_HOME	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData C:\Program Files\Java\jdk-11.0.1 C:\Program Files (x86)\Oracle\Java Card Development Kit 3.0.5u3\		
stemvariablen Variable asl.log ComSpec DriverData JAVA_HOME JC_CLASSIC_HOME NUMBER_OF_PROCESSORS	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData C:\Program Files\Java\jdk-11.0.1 C:\Program Files (x86)\Oracle\Java Card Development Kit 3.0.5u3\ 8		
stemvariablen Variable asl.log ComSpec DriverData JAVA_HOME JC_CLASSIC_HOME NUMBER_OF_PROCESSORS OS	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData C:\Program Files\Java\jdk-11.0.1 C:\Program Files (x86)\Oracle\Java Card Development Kit 3.0.5u3\ 8 Windows NT		
stemvariablen Variable asl.log ComSpec DriverData JAVA_HOME JC_CLASSIC_HOME NUMBER_OF_PROCESSORS OS	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData C:\Program Files\Java\jdk-11.0.1 C:\Program Files (x86)\Oracle\Java Card Development Kit 3.0.5u3\ 8 Windows NT		
rstemvariablen Variable asl.log ComSpec DriverData JAVA_HOME JC_CLASSIC_HOME NUMBER_OF_PROCESSORS OS	Wert Destination=file C:\Windows\system32\cmd.exe C:\Windows\System32\Drivers\DriverData C:\Program Files\Java\jdk-11.0.1 C:\Program Files (x86)\Oracle\Java Card Development Kit 3.0.5u3\ 8 Windows NT Neu Bearbeiten Löschen		

Unter Name der Variable gibt man "SSLKEYLOGFILE" ein und verweist unter Wert 3. der Variable auf einen selbstgewählten Ort wo man die Protokolldatei speichern möchte. \times

Neue Systemvariable

<u>N</u> ame der Variablen:	SSLKEYLOGFILE			
<u>W</u> ert der Variablen:	C:\Data\sslkeylog.log			
Verzeichnis durchsuch	nen Datei d <u>u</u> rchsuchen	OK Abbrechen		

 \times

Unter Linux

Man verwendet den export Befehl um eine zu exportierende Umgebungsvariable zu definieren. Der Befehl für SSLKEYLOGFILE ist:

export SSLKEYLOGFILE="VALUE"

VALUE ersetzt man durch einen selbstgewählten Ort wo man die Datei speichern möchte. Ein Beispiel wäre ~/Desktop/sessionkey.log

Einrichtung von Wireshark

Wenn man Firefox 63, Chromium 68 oder Chrome 66 verwendet, wird der symmetrische Sitzungsschlüssel auf jeden Fall mitgeschnitten. Jedoch muss man auch noch Wireshark einrichten damit der mitgeschnitte Datenverkehr entschlüsselt werden kann.

Edit	t View Go Capture A	nalyze Statistics Tele	phony Wireless Tools Help		
	Сору	•			
Q	Find Packet	Strg+F	🔁 🗸 Ex	pression	
	Find Next	Strg+N			
	Find Previous	Strg+B			
	Mark/Unmark Packet	Strg+M			
	Mark All Displayed	Strg+Umschalt+M			
	Unmark All Displayed	Strg+Alt+M	✓ All interfaces shown ▼		
	Next Mark	Strg+Umschalt+N			
	Previous Mark	Strg+Umschalt+B			
	Ignore/Unignore Packet	Strg+D	-		
	Ignore All Displayed	Strg+Umschalt+D			
	Unignore All Displayed	Strg+Alt+D			
	Set/Unset Time Reference	Strg+T			
	Unset All Time References	Strg+Alt+T			
	Next Time Reference	Strg+Alt+N			
	Previous Time Reference	Strg+Alt+B			
	Time Shift	Strg+Umschalt+T			
	Packet Comment	Strg+Alt+C			
	Delete All Packet Comment	s			
	Configuration Profiles	Strg+Umschalt+A			
	Prefere zes	Strg+Umschalt+P			

1. In Wireshark klickt man auf Bearbeiten und dann auf Einstellungen.

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.6.4 (v2.6.4-0-g29d48ec8). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default

2. Wenn man das Tab Protokolle erweitert und dann auf SSL geht, setzt man im Feld von (*Pre*)-*Master-Secret log Filename* den Speicherort von SSLKEYLOGFILE ein.

Wireshark · Preference	ces	?	\times
Wireshark - Preference Snort Socks SolarEdge SoulSeek SoupBinTCP SPDY Spice SPRT SRVLOC SSCOP SSDP SSH SSL STANAG 506i STANAG 500 STANAG 500	Secure Sockets Layer RSA keys list Edit SSL debug file Reassemble SSL records spanning multiple TCP segments Reassemble SSL Application Data spanning multiple SSL records Reassemble SSL Application Code (MAC), ignore "mac failed" Pre-Shared-Key (Pre)-Master-Secret log filename D:\data\ssl\sslkeylog.log Browse	?	×
SUA SV SYNC SVNCHROPH			
< >	ОК	Abbrechen Hilf	ė

3. Wenn man nun per Wireshark den Internetverkehr mitschneidet, und diesen anschließend analysiert, gibt es nun einen neuen Tab "Decrypted SSL Tab"

Wireshark · Packet 1301 · Ethernet	_	\Box \times
 > Ethernet II, Src: Avm_71:b7:9a (34:31:c4:71:b7:9a), Dst: WistronC_bb:a6:07 (30:65:ec:bb:a6:07) > Internet Protocol Version 4, Src: 93.184.220.70, Dst: 192.168.178.27 > Transmission Control Protocol, Src Port: 443, Dst Port: 51463, Seq: 4001, Ack: 598, Len: 271 > Secure Sockets Layer > TLSv1.3 Record Layer: Handshake Protocol: New Session Ticket 		د لاک
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$		
Frame (325 bytes) Decrypted SSL (249 bytes)	Schließen	Hilfe

Eine Erklärung der Einträge in der SSL Keylogfile kann man unter folgendem Link nachlesen:

https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/Key_Log_Format