Praktikum 3 zur Vorlesung IT-Sicherheit

Thema Zertifikate und SSL/TLS

In diesem Praktikum analysieren wir Public-Key Zertifikate. Anschließend schauen wir uns für TLS als meistgenutztes Sicherungsprotokoll den Verbindungsaufbau an. Wenn Sie möchten, können Sie abschließend noch prüfen, ob es gelingt Webserver zu „überreden“, nicht mehr aktuelle Verfahren einzusetzen.

Versuchsteile 1 und 2 sind VOR dem Praktikumstermin zu Hause zu bearbeiten.

1 Hausaufgabe: Vorbereitende Fragen beantworten

1.1 Allgemeine Fragen zu Zertifikaten

Wozu dient ein Zertifikat? Welche Zuordnung wird beglaubigt?

Serverzertifikate sind signiert. Mit welchem Schlüssel kann die Signatur geprüft werden?

Gemäß welchem Standard sind aktuelle Zertifikate aufgebaut? _____

Wofür steht die Abkürzung CRL? _____

1.2 Analyse einer TLS CipherSuite

Analysieren Sie die CipherSuite **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**

Was bedeutet welcher Eintrag?

Eintrag	Bedeutung bzw. Einsatzzweck
ECDHE	
ECDSA	
AES_256_GCM	
SHA384	

Wie prüft der Client die Authentizität des Servers?

Beim RSA-Schlüsselaustausch wählt der Client einen zufälligen Session Key und überträgt diesen, verschlüsselt mit dem öffentlichen RSA-Schlüssel des Servers aus dem Serverzertifikat, an den Server.

Erläutern Sie, welchen Nachteil der RSA-Schlüsselaustausch gegenüber der Schlüsselvereinbarung mittels Diffie-Hellman hat:

Wie lautet die zugehörige Sicherheitseigenschaft, die bei Diffie-Hellman erfüllt ist?

2 Hausaufgabe: Webseiten Zertifikate analysieren

2.1 Allgemeine Informationen in den Zertifikaten

Öffnen Sie mit Firefox folgende Seiten in verschiedenen Tabs:

www.hs-osnabrueck.de (kurz HS)

www.postbank.de (kurz PB)

www.computerbase.de (kurz CB)

Welches Protokoll wird bei den Seiten zum Seitenabruf verwendet? _____

Gehen Sie bei den Seiten auf das Schloss-Symbol und lassen Sie sich Daten zur Verschlüsselung der Verbindung anzeigen. Welche TLS Version kommt zum Einsatz, und welche CipherSuite wird verwendet?

	TLS Version	CipherSuite
HS		
PB		
CB		

Lassen Sie sich zu den Seiten die Serverzertifikate anzeigen und geben Sie in der nachstehenden Tabelle die entsprechenden Daten an:

	HS	PB	CB
Anzahl Zertifikate im Zertifizierungspfad			
Gültigkeits**dauer** des Serverzertifikats (nicht nur Ablaufdatum!)			
Von welcher Organisation ist die CA?			
Kryptoalgorithmus und Schlüssellänge (Bits) des öffentlichen Schlüssels			
Mit welchen Verfahren (Hashfkt./Public-Key-Alg.) ist das Zertifikat signiert?			
Validierungsart gemäß der Zertifizierungsregeln OID 2.23.140.1. …			

2.2 Validierungsarten = Art der Prüfung des Antragsstellers

Die Prüfungen/Validierungen, die vor der Zertifikatsausstellung zum Antragsteller erfolgen, bestimmen letztlich den eigentlichen Wert eines Zertifikats. Daher sollen Sie sich diese Prüfungen noch etwas genauer anschauen.

Im Internet werden gemäß der notwendigen Überprüfung des Antragstellers (Validierung) DV, OV, EV und IV Zertifikate unterschieden.

Von welcher Validierungsart ein gegebenes Zertifikat ist, sowie ein Verweis auf die zugehörigen Zertifizierungsregeln (CPS), ist i.d.R. in den Zertifikats-Extensions angegeben. Das sollten Sie in der letzten Zeile der obigen Tabelle für die 3 Zertifikate angeben.

Ermitteln Sie durch eine Internet-Recherche, was sich hinter den verschiedenen Validierungsarten verbirgt und fassen Sie die zugehörigen Prüfungen kurz mit eigenen Worten zusammen.

DV	
OV	
EV	
IV	

Welche Validierungsart ist am „lockersten“? _____

Bei welcher Validierungsart erfolgen die strengsten Prüfungen? _____

Die genauen Validierungsanforderungen werden übrigens vom CA/Browser Forum (cabforum.org) spezifiziert.

3 TLS 1.2 Analyse mit Wireshark

Als erstes analysieren wir einen TLS-Sitzungsaufbau für TLS 1.2.

Hierzu liegt eine Wireshark-Aufzeichnung für einen TLS1.2 geschützten Aufruf der Seite www.hs.-osnabrueck.de vor. Öffnen Sie die Datei **`hs-osnabrueck-tls-12.pcapng`** durch einen Doppelklick mit Wireshark. Geben Sie als Displayfilter **`tls`** ein.

3.1 Analyse von Client Hello und Server Hello

Wie lang ist der Random, den der Client dem Server mitteilt? _____

Prüfen Sie, dass der Random, den der Server dem Client schickt, dieselbe Länge hat. check O

Wie viele verschiedene CipherSuites schlägt der Client dem Server zur Auswahl vor? _____

Welche CipherSuite wird vom Server gewählt (Server Hello)? _____

3.2 Übertragene Zertifikate

Lokalisieren Sie die übertragenen Zertifikate.
Wie viele Zertifikate werden übertragen? _____

Welches dieser Zertifikate sollte bereits im Browser gespeichert sein? _____

Was passiert, wenn der Client das entsprechende Zertifikat im Browser nicht findet?

Unter den Zertifikatserweiterungen gibt es kritische und unkritische. Kritische Erweiterungen sind bei der Prüfung des Zertifikats zu berücksichtigen. Insbesondere die Erweiterung *KeyUsage* ist kritisch.

Welche Key-Usages hat

… das Serverzertifikat? _____

… das CA-Zertifikat? _____

Was könnten Sie mit einem Serverzertifikat (inkl. private Key) unbefugter Weise machen, wenn die Key-Usage nicht überprüft würde?

3.3 Schlüsselaustausch PDUs

In der Ciphersuite ist das Schlüsselaustausch-Verfahren mit angegeben. Welches Schlüsselaustausch-Verfahren wird hier verwendet? _____

Der Schlüsselaustausch erfolgt in den beiden Key Exchange PDUs.

In der Server Key Exchange PDU schickt der Server seinen DH-Schlüsselanteil inkl. einer Signatur an den Client. Nach Verifikation der Signatur weiß der Client, dass der öffentliche DH-Server-Schlüsselanteil nur von dem durch das Serverzertifikat ausgewiesenen Server kommen kann.

Welche elliptische Kurve wird für den DH-Schlüsselaustausch verwendet? _____

Wie lang ist der DH-Schlüsselanteil (Bytes) des Servers? _____

Prüfen Sie, dass die DH-Schlüsselanteile von Client und Server die gleiche Länge in Bytes aufweisen. check O

Geben Sie die ersten 2 Byte (4-Hex Ziffern) der DH-Schlüsselanteils des Clients an: _____

Mit welchem Signaturalgorithmus gemäß welchem Standard ist der Schlüsselanteil vom Server signiert (*Signature Algorithm*)?

Mit welchem öffentlichen Schlüssel prüft der Client die Signatur des DH-Schlüsselanteils des Servers?

Wie heißt das entsprechende Feld im Zertifikat, in dem der öffentliche Schlüssel inkl. Algorithmen-Angaben gespeichert ist?

In dem Feld finden Sie auch den verwendeten Modulus.
Geben Sie die ersten 3 Byte (6 Hex Ziffern) des Modulus an: _____ _____ _____

4 TLS 1.3 Analyse mit Whireshark

Als nächstes analysieren wir einen TLS-Sitzungsaufbau für TLS 1.3.

Hierzu liegt eine Wireshark-Aufzeichnung für einen TLS1.3 geschützten Aufruf der Seite www.computerbase.de vor. Öffnen Sie die Datei **`computerbase-tls-13.pcapng`** durch einen Doppelklick mit Wireshark. Geben Sie als Displayfilter **`tls`** ein.

4.1 Analyse der Client Hello PDU

Wie viele verschiedene CipherSuites schlägt der Client diesmal dem Server zur Auswahl vor? _____

Im Client Hello sind CipherSuites der TLS Versionen 1.2 und 1.3. enthalten.

Woran können Sie diese unterscheiden?

Geben Sie beispielhaft eine Ciphersuite für TLS 1.2 und eine für TLS 1.3 an:

TLS 1.2	
TLS 1.3	

Wie viele DH-Gruppen unterstützt der Client? (Klicken Sie sich zur Beantwortung bis auf die Namen der „Supported Groups“ durch.) _____

Wie heißt die Extension, in der der Client seine DH-Schlüsselanteile mitsendet: _____

Zu wie vielen und welchen elliptischen Kurven liefert der Client DH-Schlüsselanteile (mit welchen Bytelängen) mit?

4.2 Analyse der Server Hello PDU

Welche der vom Client vorgeschlagenen CipherSuite wird vom Server ausgewählt? _____

Welche DH-Gruppe/Kurve wird vom Server für den Schlüsselaustausch gewählt? _____

Verifizieren Sie, dass der DH-Server-Schlüsselanteil genauso lang ist, wie der vom Client. check O

Jetzt haben Server und Client DH-Schlüsselanteile getauscht und erzeugen damit einen gemeinsamen Schlüssel für die Absicherung. Der Server signalisiert dem Client mit seiner anschließenden *Change Cipher Spec* PDU, dass er ab jetzt abgesichert (verschlüsselt und authentisiert) sendet.

Wie bei TLS 1.2 authentifiziert sich auch bei TLS 1.3 der Server per Zertifikat und digitaler Signatur. Signiert werden bei TLS 1.3 die bisher ausgetauschten Handshake-Nachrichten.

Die zugehörigen PDUs werden vom Server allerdings bereits verschlüsselt verschickt.

4.3 Entschlüsseln der weiteren TLS 1.3 PDUs

Damit Wireshark Zertifikate und Signatur anzeigen kann, muss Wireshark die zugehörigen PDUs entschlüsseln können. Damit das möglich ist, wurde der Browser beim Aufruf der Seite so konfiguriert, dass er die verwendeten TLS-Schlüssel speichert. Diese stehen in der Datei **`\ITS\ITS_P3\tlskeys.txt`** auf dem Desktop und im Lernraum.

Um die unverschlüsselte und verschlüsselte Version vergleichen zu können, öffnen Sie ein zweites Mal durch Doppelklick die Datei **`computerbase-tls-13.pcapng`** in Wireshark.

Geben Sie in einem Wireshark-Fenster den kompletten Pfad zur Datei **`tlskeys.txt`** unter „Bearbeiten => Einstellungen => Protocols => TLS“ im Feld „"(Pre)Master-Secret log file name" ein.

In dem Wireshark-Fenster sollten jetzt die TLS 1.3 PDUs **`Certificate`** und **`Certificate Verify`** sichtbar sein.

Wie waren die entsprechenden PDUs im verschlüsselten Original-Netzverkehr bezeichnet? _____

4.4 Untersuchung der Certificate-PDU und des OCSP Status

Wie viele Zertifikate werden in der Certificate PDU an den Client übertragen? _____

Zu welchem der Zertifikate liefert der Server einen OCSP Status (status-request) mit? _____

Klicken Sie sich in der OSCP Response bis nach unten durch.

Von wem stammt die Response (*responderID*)? _____

Verifizieren Sie, dass die *responseID* mit dem Inhaber *(subject)* des CA-Zertifikats (weiter unten) übereinstimmt. check O

Welchen Status (*certStatus*) hat das Serverzertifikat gemäß der OCSP-Antwort, und wie lange ist der Status gültig?

Status:	Gültigkeitsdauer:

Der OCSP Response ist vom Responder signiert, mit welchem Algorithmus? _____

Mit welchem Schlüssel prüft der Client die Signatur des OCSP Responses?

Suchen Sie den Schlüssel im Zertifikat und verifizieren Sie, dass der Schlüssel (subjectPublicKeyInfo) für den Signieralgorithmus vorgesehen ist. check O

Geben Sie die ersten beiden Bytes (4 Hex Ziffern) des Modulus an: ____ ____

Prüfen Sie auch, dass der Schlüssel zur Signierung eingesetzt werden darf (Key-Usage). check O

4.5 Analyse der Certificate Verify PDU

Abschließend schickt der Server dem Client eine Signatur über die bereits ausgetauschten Nachrichten. Erst mit dieser Signatur weist er nach, dass er im Besitz des privaten Schlüssels ist, der zum öffentlichen Schlüssel aus seinem Zertifikat passt, und dass sein DH-Schlüsselanteil tatsächlich von ihm kommt.

Welcher Signaturalgorithmus über welcher elliptischen Kurve wird verwendet? _____

Welches Hash-Verfahren wird verwendet? _____

Wofür steht die Abkürzung ECDSA?

Mit welchem Schlüssel prüft der Client die Signatur?

Suchen Sie den Schlüssel im betreffenden Zertifikat und verifizieren Sie, dass der Schlüssel (subjectPublicKeyInfo) für die elliptische Kurve vorgesehen ist. check O

Wie lauten die ersten beiden Bytes des öffentlichen Schlüssels? ____ ____

5 Optional: Server Versions- / Cipher Fallbacks testen

Der Client schickt dem Server Ciphersuites zur Auswahl. Was ist, wenn der Client versucht, eine Verbindung mit schwachen Verfahren aufzubauen? Lässt sich der Server darauf ein?

5.1 Verhalten für ältere TLS Versionen testen

In openssl können Sie mit dem Befehl **`s_client`** eine SSL/TLS-Verbindung zu einem angegebenen Server aufbauen.

Starten Sie openssl und ermitteln per **`s_client -help`** die Funktion folgender Optionen:

`-tls1`	
`-tls1_1`	

Prüfen Sie für banking.postbank.de und www.hs-osnabrueck.de mit dem Befehl

`s_client -connect <servername>:443 -tls1  bzw. -tls1_1`

ob ein Verbindungsaufbau mit einer älteren TLS Version möglich ist.

	banking.postbank.de	www.hs-osnabrueck.de
TLS 1.0		
TLS 1.1		

5.2 TLS ohne Perfect Forward Secrecy

Testen wir, ob die Server TLS-Verbindungen ohne PFS erlauben, also neben Diffie-Hellman auch einen Schlüsselaustausch per RSA zulassen.

Hierzu nutzen wir die Option –cipher RSA für das openssl s_client Kommando

```
s_client –connect <servername>:443 -tls1_2 –cipher RSA
```

Ist eine TLS-Verbindung mit RSA-Schlüsselaustausch möglich?

Zu banking.postbank.de: _____

Zu www.hs-osnabrueck.de: _____

Falls eine Verbindung möglich ist, zeichnen Sie den TLS Handschake mit Wireshark auf und schauen Sie, welche CipherSuites der Client anbietet und der Server wählt. Die vom Server gewählte sollte mit TLS_RSA_WITH starten

Servername:

Vom Server gewählte CipherSuite: _____

5.3 TLS ohne Serverauthentifizierung

Mit CipherSuites TLS_ADH_WITH … kann ein anonymer DH-Schlüsselaustausch erfolgen, d.h. ohne Serverauthentisierung. Testen Sie mit der Option –cipher ADH ob die Webserver eine TLS Verbindung ohne Authentisierung zulassen.

```
s_client –connect <servername>:443 –cipher ADH
```

Ist eine TLS-Verbindung ohne Serverauthentisierung möglich?

Zu www.computerbase.de:

Zu www.hs-osnabrueck.de: