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. Dann prüfen wir noch, ob wir Webserver „überreden“ können, nicht mehr aktuelle Verfahren einzusetzen.

1 Hausaufgabe: Vorbereitende Fragen beantworten

Nachstehende Fragen sind vor dem Praktikumstermin zu beantworten!

Die Fragen stellen sicher, dass Sie sich mit dem Thema auseinander gesetzt haben.

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_RSA_WITH_AES_256_GCM_SHA384**

Was bedeutet welcher Eintrag?

Eintrag	Bedeutung bzw. Einsatzzweck
ECDHE	
RSA	
AES_256	
SHA384	
GCM	

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 Im Praktikum: Analyse von Zertifikaten

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 folgende Daten an:

	HS	PB	CB
Anzahl Zertifikate im Zertifizierungspfad			
Gültigkeitsdauer des Serverzertifikats			
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 Prüfung des Antragsstellers

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

Öffnen Sie im Browser das Digicert CPS. Den Link finden Sie unter *Zertifikatsregeln* (OID 1.3.6.1.5.5.7.2.1) im Postbank Zertifikat.

Wofür steht die Abk. CPS? _____

Im CPS stehen in Abschnitt 3.2.5 *Validation of Authority* in der Tabelle Querverweise auf die für DV, OV und EV erforderlichen Berechtigungsprüfungen. Notieren Sie hier kurz zu den Querverweisen die Abschnittsnummer und den jeweiligen Dokumentennamen.

DV	
OV	
EC	

In Abschnitt 1.1 des CPS finden sich in der Tabelle die Links zu den beiden Dokumenten. Öffnen Sie die aktuellen Versionen der beiden Dokumente. Wer ist der Herausgeber/Autor der Dokumente?

Wie lauten die vollständigen Titel der Dokumente? Bitte vervollständigen:

Baseline Requirements …
Guidelines for …

Werfen Sie einen Blick in die oben notierten Querverweise und beschreiben Sie kurz mit eigenen Worten, was jeweils geprüft wird. (In den ersten beiden Fällen können Sie das dem ersten Satz des jeweiligen Abschnitts entnehmen.)

DV	
OV	
EV	

Um einen Eindruck der Komplexität der EV Prüfungen zu gewinnen: Wie viele Seiten umfasst Kap. 11 *Verification Requirements* der EV Guidelines? _____

Welche 3 „*Existences*“ des Antragstellers sind neben anderen Dingen nachzuweisen?

2.3 Zertifikatsprüfung: Online Certificate Status Protocol und Sperrlisten

Wenn ein Zertifikat vor dem in ihm angegebenen Gültigkeitsende ungültig gemacht werden sollen, kann das Zertifikat zurückgerufen / gesperrt werden – wie eine Kreditkarte.

Ob ein Zertifikat gesperrt ist, kann durch eine OCSP-Abfrage oder einen Blick in die Sperrliste der CA ermittelt werden.

2.3.1 OCSP-Abfrage

Mit OCSP kann man die Gültigkeit von Zertifikaten abfragen, um zu verifizieren, dass das Zertifikat nicht zwischenzeitlich gesperrt wurde.

Lassen Sie sich im Browser die Zertifikate zu www.hs-osnabrueck.de anzeigen und speichern Sie

- das Serverzertifikat in der Datei `hscert.crt`

- das CA-Zertifikat (NICHT das Root-Zertifikat!) in der Datei `cacert.crt`

Starten Sie openssl und kontrollieren Sie die Zertifikate mit dem Kommando

```
x509 –in <Zertifikatsdatei> -noout –text
```

Ermitteln Sie aus den Zertifikats-Extensions die URL des OCSP-Dienstes der CA.

OSCP-URL:

Starten Sie eine OCSP-Abfrage in openssl:

```
ocsp -issuer cacert.crt -cert hscert.crt -url <OCSP-URL> -CAfile
cacert.crt -partial_chain
```

(Die Option `-partial_chain` verwenden wir, da wir zur Prüfung nicht das Root-Zertifikat mit bereitgestellt haben.)

OCSP-Request und -Reply werden in HTTP übertragen. Zeichnen Sie die OCSP-Abfrage mit Wireshark (LAN Verbindung 1 = Internet) mit dem Capture-Filter `tcp port 80` auf.

Beantworten Sie folgende Fragen mit der Wireshark-Aufzeichnung:

Ist der OCSP-Request signiert? _____

Im OCSP-Request wird das zu prüfende Zertifikat nicht übertragen! Durch welche 3 Angaben ist das Zertifikat im Request eindeutig referenziert?

Identifizieren Sie im OCSP Response den certStatus: good (0) check O

Wie lange ist das Ergebnis der OCSP-Abfrage maximal gültig? _____

2.3.2 Sperrlistenabruf, -anzeige und -prüfung

Ermitteln Sie aus den Zertifikats-Extensions die URL der Sperrliste der DFN-CA, kopieren sie die URL in den Browser und speichern Sie die Sperrliste in der Datei `cacrl.crl`

Lassen Sie sich die Inhalte der Sperrliste in openssl anzeigen:

```
crl -in cacrl.crl -inform DER -text -noout
```

Wie lange ist die Sperrliste der DFN-CA gültig? _____

Die CRL ist signiert. Um die CRL-Signatur zu prüfen, benötigen Sie das Zertifikat des Herausgebers (issuer) der CLR. Der Issuer und der Authority Key Identifier werden bei der CRL-Anzeige mit angezeigt. Speichern Sie aus dem Browser heraus das zugehörige CA-Zertifikat in der Datei `dfnca2.crt`.

Prüfen Sie, dass der *Authority Key Identifier* der Sperrliste
mit dem *Subject Key Identifier* des Zertifikats übereinstimmt. check O

Anschließend verifizieren Sie die Sperrlisten-Signatur in openssl mit dem Kommando

```
crl -in cacrl.crl -inform DER -CAfile dfnca2.crt -noout
```

Falls das nicht zur Ausgabe `verify OK` führt, suchen und beheben Sie den Fehler.

Die URL der Sperrliste der Digicert-CA ist im Postbank-Zertifikat angegeben. Speichern Sie die Sperrliste in der Datei `digi.crl` und lassen Sie sich die Sperrliste in openssl anzeigen. Da hier viele Zertifikate gesperrt sind, brechen Sie die Ausgabe zeitnah ab.

Wie lange ist die Sperrliste der Digicert-CA gültig?

_____

Welche Informationen sind für jedes gesperrte Zertifikat in der Sperrliste angegeben?

Hinweis: Zur Prüfung, ob ein Zertifikat in der Liste angegeben ist, könnte man die openssl Ausgabe auf grep umleiten:

```
openssl crl -in digi.crl -inform DER -text -noout | grep
<Seriennummer des zu prüfenden Zertifikats>
```

3 TLS 1.3 Analyse mit Whireshark

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

Öffnen Sie Wireshark und geben Sie als Capture-Filter **`tcp port 443`** ein.

Öffnen Sie dann im Firefox die Seite **`www.computerbase.de`**

Stoppen Sie nach dem Laden der Seite die Wireshark-Aufzeichnung.

3.1 Analyse der Client Hello PDU

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

Wie viele verschiedene CipherSuites
schlägt der Client 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?

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?

3.2 Analyse der Server Hello PDU

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

Welche Kurve wird vom Server für den Schlüsselaustausch gewählt? _____

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

Wie bei TLS 1.2 authentifiziert sich auch bei TLS 1.3 der Server per Zertifikat und digitaler Signatur seines öffentlichen DH-Server-Schlüsselanteils.

Wo wird in den Daten das Zertifikat und die Signatur verschickt?

4 TLS 1.2 Analyse mit Wireshark

Jetzt zwingen wir den Server dazu, TLS 1.2 zu verwenden. Starten Sie eine neue Wireshark-Aufzeichnung. Die alte Aufzeichnung können Sie löschen.

Öffnen Sie openssl und starten Sie dort einen Verbindungsaufbau, der TLS1.2 erzwingt, mit dem Befehl

```
s_client -connect www.computerbase.de:443 -tls1_2
```

Prüfen Sie im Client Hello, dass der Client ausschließlich TLS 1.2 Ciphersuites anbietet. check O

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

Prüfen Sie im Client Hello und Server Hello, dass keine DH-Schlüsselanteile mitgesendet werden. check O

4.1 Weitere TLS 1.2 PDUs

4.1.1 Übertragene Zertifikate

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

Das müssten weniger Zertifikate sein, als im Zertifizierungspfad im Browser angezeigt wurden (Aufgabenteil 1.1). Welches Zertifikat fehlt? _____

Woher kennt der Client das fehlende Zertifikat? _____

Auf Basis welcher 2 Informationen im Zertifikat kann der Client das fehlende Zertifikat zuordnen?

Unter den Zertifikatserweiterungen (Extensions) gibt es kritische und unkritische. Kritische Erweiterungen sind bei der Prüfung des Zertifikats zu berücksichtigen.

Welche 2 Erweiterungen sind in den übertragenen Zertifikaten kritisch? _____

Welche Key-Usages hat

… das Serverzertifikat? _____

… das CA-Zertifikat? _____

Wieso ist es wichtig, dass diese beiden Erweiterungen kritisch sind, also mit geprüft werden?

4.1.2 Schlüsselaustausch PDUs

In der Server Key Exchange PDU schickt der Server seinen Schlüsselanteil inkl. einer Signatur.

Zu welchen Schlüsselaustausch-Verfahren über welcher elliptischen Kurve gehört der Schlüsselanteil des Servers und wie lang ist der Schlüsselanteil (Bytes)

Mit welchem Signaturalgorithmus über welcher elliptischen Kurve ist der Schlüsselanteil vom Server signiert?

Mit welchem öffentlichen Schlüssel prüft der Client die Signatur?

Wie heißt das entsprechende Feld im Zertifikat, in dem der öffentliche Schlüssel gespeichert ist? _____

Prüfen Sie, ob der öffentliche Schlüssel zu dem angegebenen Signierverfahren und der angegebenen elliptischen Kurve passt. check O

Lokalisieren Sie in Client Key Exchange PDU den DH-Schlüsselanteil des Clients.

Prüfen Sie, ob der Client-Schlüsselanteil zum selben Algorithmus gehört, wie der DH-Schlüsselanteil des Servers check O

und beide Schlüsselanteile die gleiche Länge in Bytes ausweisen. check O

5 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

Ermitteln Sie in openssl per **`s_client –help`** die Funktion folgender Optionen:

`-tls1`	
`-tls1_1`	

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

`s_client –connect <servername> -tls1  bzw. –tls1_1`

ob ein Verbindungsaufbau mit einer älteren TLS Version möglich ist.

	www.computerbase.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 Optoion –cipher RSA für das openssl s_client Kommando

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

Ist eine TLS-Verbindung mit RSA-Schlüsselaustausch möglich?

Zu www.computerbase.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> –cipher ADH`

Ist eine TLS-Verbindung ohne Serverauthentisierung möglich?

Zu www.computerbase.de:

Zu www.hs-osnabrueck.de: