NS2 – Präsenzwochenende

Record Encryption

Gegeben seien die folgenden Client Keys für die Session aus handshake.pcapng:

Key 1:

67d545b020c46aef2da4c1220380cde0

Key 2:

5f6fa4951a65884ab239d9af9b481874f6324df63bdca909a4bacdfe9c62f9ba

Frage 1

Welcher der beiden Schlüssel ist der Client Write Key, welcher Client Write Mac Key?

Frage 2

Sie sollen nun selbst einen Record erzeugen und eine ApplicationData Nachricht verschlüsseln, die vom Client and den Server (nach der Finished Nachricht) gesendet werden soll.

Die Nachricht, die Sie verschlüsseln sollen, lautet:
4576656e2074686520736d616c6c65737420706572736f6e2063616e20636861
6e6765207468652063 6f75727365206f662074686520667574572652e

TLS in der ausgehandelten Version folgt dem "MAC-then-Pad-then-Encrypt"-Paradigma. Daher müssen Sie zunächst die HMAC berechnen. Diese wird wie folgt berechnet:

HMAC[key] (Sequenznummer | Content Type des Records | Versionsbytes der TLS-Version | Länge der zu verschlüsselnden Nachricht (2 Bytes) | Nachricht)

Sie sollen nun selbst einen Record erzeugen und eine ApplicationData Nachricht verschlüsseln, die vom Client and den Server (nach der Finished Nachricht) gesendet werden soll.

Die Sequenznummer ist eine 64-Bit Zahl, welche die Anzahl der bisher gesendeten Records (unter dem aktuellen Schlüssel) wiedergibt. Da Sie den zweiten verschlüsselten Record (des Clients) dieser Verbindung senden wollen, müssen Sie die Sequenznummer 0x0000000000000001 verwenden. Der Content Type ist 0x17 (Application Data).

Über welche Bytes wird der HMAC gebildet?

Frage 3

Wie lautet der HMAC? Verwenden Sie tls_ hmac.py

Frage 4

Wie viele Padding Bytes werden mindestens benötigt, um den Record zu verschlüsseln?

Frage 5

Wie lautet das minimale Padding für den Record?

Frage 6

Sie haben nun alle benötigten Informationen, um den Record zu verschlüsseln. Nutzen sie den IV 443020de1cad09bfd6381ffb94daafbb. Wie lautet der Inhalt des verschlüsselten Records (ohne IV)? Verwenden Sie aes_encrypt.py
Hinweise: Die ersten acht Bytes lauten 06557245f3a1e9b0

Frage 7

Wie lautet der vollständige Record?

Hinweis: der vollständige Record sollte 117 Bytes umfassen