Challenge 2 — Padding Oracle
NKP4, SS23

Aufgabenstellung

Du hast ein Wireshark-Capture vorliegen, in dem eine verschlüsselte Nachricht enthalten ist.

Teilaufgabe 1

Bei den vorliegenden Daten handelt es sich offensichtlich um ein proprietäres Nachrichtenformat für verschlüsselten Traffic. Um welche Art von Verschlüsselung handelt es sich? Was antwortet der Server, wenn du ihm die Nachricht nochmal schickst?

Nach dieser Teilaufgabe

- kennst du den verwendeten Verschlüsselungsalgorithmus samt verwendeten Betriebsmodus - und kannst dich an die dafür verwendeten Block- und Schlüssellängen erinnern.
- kennst du das Format der Antworten des Servers.
- hast du interessante Informationen zum Erreichen des Badges vorliegen.

Teilaufgabe 2

Was antwortet der Server, wenn du eines der ersten Bytes des Chiffrats änderst? Was antwortet der Server, wenn du eines der letzten Bytes des Chiffrats änderst? Die Antworten fallen unterschiedlich aus.[1] Du vermutest, dass der Server als Padding Oracle fungiert - also abhängig davon, ob das Padding im Klartext korrekt ist oder nicht, unterschiedlich antwortet.

Nach dieser Teilaufgabe weißt du,

- welche Antwort der Server schickt, wenn die Klartextnachricht ein korrektes Padding enthält.
- welche Antwort der Server schickt, wenn die Klartextnachricht kein korrektes Padding enthält.

Teilaufgabe 3

Mache dich schlau über das PKCS#7-Padding-Format. Wie wird eine Nachricht gepaddet, deren Länge kein Vielfaches der Blocklänge der Blockchiffre ist? Wie wird eine Nachricht gepaddet, deren Länge ein Vielfaches der Blocklänge der Blockchiffre ist?

Nach dieser Teilaufgabe kannst du in Kenntnis der Blocklänge

- an eine gegebene Nachricht ein korrektes PKCS#7-Padding anbringen.
- feststellen, ob eine gegebene Nachricht ein korrektes PKCS#7-Padding enthält.

[1] Tun sie das nicht, hast du vielleicht einen Fehler im Nachrichtenformat. Bedenke, dass das Chiffrat hexadezimal notiert ist.

Teilaufgabe 4

Mache dich schlau über die Komplexität des Padding-Oracle-Angriffs. Wie viele Anfragen an das Padding Oracle sind zur Entschlüsselung der vorliegenden Nachricht in etwa notwendig? Ist der Angriff in der vorliegenden Zeit und mit den vorliegenden Ressourcen möglich?

Nach dieser Teilaufgabe kannst du für eine gegebene Chiffratlänge

- berechnen, wie viele Anfragen zur Ermittlung des Klartextes mittels Padding-Oracle-Angriff in etwa notwendig sind.
- berechnen, wie lange ein Padding-Oracle-Angriff maximal dauert, wenn die Antwortzeit des Servers maximal 1 Sekunde beträgt.

Teilaufgabe 5

Implementiere den Padding-Oracle-Angriff und ermittle den Klartext.

5.1 Ermittle die Padding-Bytes

Mache dich schlau, wie die Entschlüsselung im CBC-Modus funktioniert und richte deine Augen auf das allerletzte XOR. Hier wirst du ansetzen. Welches Byte im Chiffrat musst du ändern, um (irgend)eine Änderung im allerletzten Byte des Klartexts (und NICHT im Byte davor) zu erreichen?

Mit diesem Wissen kannst du nun testweise jedes einzelne Byte im letzten Klartextblock verändern. Triffst du dabei ein Padding-Byte, hast du das Padding kaputtgemacht. Triffst du ein Inhalts-Byte, ist das Padding noch intakt. Nun kennst du also die Position aller Padding-Bytes. Und du kennst auch die Länge des Paddings. Und daher kennst du auch den Inhalt der Padding-Bytes.

Nach dieser Teilaufgabe weißt du

- welches Byte im Chiffrat du manipulieren musst, um genau ein Klartext-Byte an einer gewünschten Position zu manipulieren.
- wie du mit Hilfe des Padding Oracles die Padding-Bytes ermitteln kannst.

Nach dieser Teilaufgabe kennst du

- die letzten Bytes des Klartextes (die Padding-Bytes).

5.2 Ermittle das letzte Byte des Nachrichteninhalts

Richte deine Augen nun auf das allerletzte Klartext-Byte: Du kennst schon dessen Inhalt und du weißt, welches Chiffrat-Byte du manipulieren musst, um dessen Inhalt zu ändern. Wie kannst du also den Inhalt des Klartext-Bytes auf einen von dir gewählten Wert ändern?

Mit diesem Wissen kannst du das Chiffrat so ändern, dass sich alle Padding-Bytes im Klartext auf den nächsthöheren Wert ändern. Aus Teilaufgabe 3 weißt du nun, dass dieses Padding nur korrekt ist, wenn du es schaffst, dass auch das Klartext-Byte davor zum Padding-Byte wird. Dabei hilft dir nun wieder das Padding Oracle.

Du weißt, welches Chiffrat-Byte du ändern musst, um (irgend)eine Änderung in genau diesem Klartext-Byte zu erreichen. Ändere nun das Chiffrat-Byte so lange auf verschiedene Werte, bis dir das Padding Oracle sagt, dass das Padding korrekt ist. Geschafft!

Du kennst nun also das modifizierte Chiffrat-Byte und das zugehörige modifizierte Klartext-Byte. Richte deine Augen wieder auf das allerletzte XOR der CBC-Entschlüsselung. Was kannst du dir mit deinem Wissen also ausrechnen? Und wie kannst du mit dem Ergebnis deiner Berechnung das originale Klartext-Byte ermitteln?

Nach dieser Teilaufgabe kannst du

- bei Kenntnis eines Klartext-Bytes durch Manipulation des Chiffrats dieses Klartext-Byte auf einen gewünschten Wert ändern.
- mit Hilfe des Padding Oracles durch Manipulation des Chiffrats aus dem letzten Inhalts-Byte der Klartextnachricht ein Padding-Byte mit bekanntem Inhalt machen.
- aus dem modifizierten Chiffrat-Byte, dem bekannten modifizierten Klartext-Byte (das neue Padding-Byte) und dem originalen Chiffrat-Byte das originale Klartext-Byte berechnen.

Nach dieser Teilaufgabe kennst du

- das letzte Byte des Nachrichteninhalts.

5.3 Ermittle den gesamten letzten Klartextblock

Die Vorgehensweise aus Abschnitt 5.2 lässt sich nun Schritt für Schritt auch auf alle anderen Bytes des letzten Klartextblocks anwenden. Ermittle so den gesamten letzten Block.

Nach dieser Teilaufgabe kennst du

- den letzten Block der Klartextnachricht.

5.4 Ermittle den vorletzten Klartextblock

Entferne nun den kompletten letzten Chiffratblock. Der zugehörige Klartext wird nun vermutlich kein korrektes Padding haben. Das ist aber kein Problem, denn du weißt ja aus Teilaufgabe 3, dass das kürzeste Padding nur ein Byte lang ist und auch was dessen Inhalt sein muss.

Es gilt also analog zu Abschnitt 5.2. das entsprechende Chiffrat-Byte so lange zu ändern, bis das Padding Oracle ein korrektes Padding meldet. Anschließend kannst du analog zu Abschnitt 5.2. das originale Klartext-Byte ermitteln. Für den Rest des Blockes gehe wie in Abschnitt 5.3 vor.

Nach dieser Teilaufgabe kennst du

- den vorletzten Block der Klartextnachricht.

5.5 Ermittle alle Klartextblöcke

Analog zu Abschnitt 5.4 kannst du nun den gesamten Klartext ermitteln.

Nach dieser Teilaufgabe kennst du

- die gesamte Klartextnachricht.

5.6 Reflexion

Abschließend überlegst du, ob der Angriff durch eine der folgenden Maßnahmen verhinderbar wäre:

- Durch eine größere Schlüssellänge?
- Durch Austausch des Verschlüsselungsalgorithmus auf eine andere Blockchiffre?
- Durch Verwendung einer Stromchiffre statt einer Blockchiffre?
- Durch Verwendung (welcher?) zusätzlicher kryptographischer Mechanismen?

Und jetzt hol dir den Badge ...

Verwende die Informationen aus Teilaufgabe 1 und Teilaufgabe 5, um dich in den gesicherten Bereich einzuloggen.