NS2 – Präsenzwochenende

Bleichenbacher

Auf dem Server cloud.nds.rub.de laufen 2 TLS Server (mit HTTPS) welche unterschiedliche konfiguriert sind:

cloud.nds.rub.de:40064

cloud.nds.rub.de:40157

Beide Server sind mit demselben Zertifikat ausgestattet. Es ist ihnen gelungen die verschlüsselte Kommunikation eines Login Versuchs auf den Server cloud.nds.rub.de:40157 aufzuzeichnen.

Die Aufzeichnung finden Sie im angehängten PCAP-File.

Frage 1

Welche Cipher Suite wurde in der Verbindung ausgehandelt?

Frage 2

Kann die ausgehandelte Cipher Suite potenziell mit dem Bleichenbacher Angriff entschlüsselt werden?

Frage 3

Wie lauten die Nonces von Client und Server?

Frage 4

Wie lautet das verschlüsselte Premastersecret das der Client an den Server überträgt?

Wir haben das Tool Attacks.jar bereitgestellt. Bei dem Tool handelt es sich um einen Teil des TLS-Analyse Frameworks TLS-Attacker, welches vom Lehrstuhl für Netz- und Datensicherheit entwickelt wird. Um das Tool benutzen zu

können, benötigen sie Java 8 / 11. Sie können das Tool mit 'java -jar Attacks.jar' starten

Frage 5

Analysieren sie die beiden Server auf ihre Verwundbarkeit für den Bleichenbacher-Angriff. Welcher Server ist verwundbar?

Hinweis 1: Sie können einen Server mit dem folgenden Befehl testen:

java -jar Attacks.jar bleichenbacher -connect [server]:[port]

Hinweis 2: Achten sie bei dem Test auf eine stabile Internetverbindung

Frage 6

Beobachten sie während des Tests den Handshake zu dem verwundbaren Server. Welchen Verhaltensunterschied zeigt der Server bei korrekt oder falsch gepaddeten ClientKeyExchange Nachrichten?

Frage 7

Eine interessante Eigenschaft des Bleichenbacher-Angriffs ist, dass ein Server der nicht direkt Verwundbar ist, aber dasselbe Zertifikat benutzt wie ein Verwundbarer Server ebenfalls attackiert werden kann (vgl. DROWN). Führen Sie nun den Bleichenbacher-Angriff auf den verwundbaren Server durch, und entschlüsseln Sie die ClientKeyExchange Nachricht! Wie lautet das entschlüsselte Premaster Secret?

Hinweis: Sie können den vollständigen Bleichenbacher-Angriff durch Hinzufügen der folgenden Parameter starten:

-executeAttack -encrypted_premaster_secret [verschlüsseltes pms]

Hinweis 2: Das Tool ist in manchen Fällen nicht so stabil. Achten Sie darauf, dass Sie während des ganzen Angriffs eine stabile Internetverbindung haben (am besten kein W-LAN!). Der Angriff kann je nach Verbindung einige Zeit dauern (idR ca 30 min).

Hinweis 3: Falls der erste Versuch fehlschlägt, wiederholen Sie den Angriff ;)

Hinweis 4: Achtung, es ist abschließend nur nach dem Premaster Secret gefragt.

Frage 8

Nutzen Sie nun ihr Wissen und die Tools aus vorherigen Übungen, um das Mastersecret der Verbindung des PCAP-Files zu berechnen. Wie lautet dieses?

Hinweis: Wenn Sie alles richtig gemacht haben, beginnt Ihr Mastersecret mit 0xb67cc1

Frage 9

Nutzen sie nun Wireshark und das Mastersecret, um die komplette Verbindung zu entschlüsseln. Wie lauten Benutzername und Passwort der BasicAuthentication?

Schauen Sie sich damit das Video an :)