12.-Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 02.07.2015
Abgabe 09.07.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1. RFC7525 SSL/TLS dient der Absicherung von Internetdiensten, die beispielsweise über HTTP angeboten werden. In jüngerer Zeit wurden einige Schwachstellen von SSL/TLS entdeckt, daher hat die IETF in RFC7525 Richtlinien (`https://www.rfc-editor.org/rfc/rfc7525.txt`) zur sicheren Verwendung von SSL/TLS verabschiedet.

1. Welche anderen Internetdienste werden ebenfalls häufig über SSL/TLS abgesichert?
2. Welche Versionen von SSL/TLS werden in RFC7525 verboten, welche erlaubt und welche werden empfohlen?
3. Was ist HSTS und warum wird es empfohlen?

Aufgabe 2. SSL-Client Machen Sie sich mit einem SSL-Client Ihrer Wahl vertraut, beispielsweise `openssl` unter Ubuntu.

1. Welche Cipher Suits unterstützt Ihr SSL-Client?[1]

Bauen Sie eine SSL-Verbindung zu `fu-berlin.de:443` auf.

2. Wie groß ist der öffentliche Schlüssel von `fu-berlin.de:443`?
3. Welcher Cipher wird verwendet? Erklären Sie **kurz** die einzelnen Bestandteile.

[1] Falls Sie Ihre Abgabe handschriftlich anfertigen: Mit welchem Befehl können Sie alle unterstützten Cipher Suits auflisten?

Aufgabe 3. POODLE-Angriff Im Oktober 2014 wurde der POODLE-Angriff auf SSL Version 3 entdeckt. Eine Zusammenfassung finden Sie unter `https://www.imperialviolet.org/2014/10/14/poodle.html`.

1. Erklären Sie kurz, wozu Padding in Block Ciphers verwendet wird.
2. Welche Schwäche von SSL Version 3 wird bei POODLE genutzt?
3. Unter welchen Voraussetzungen kann ein Angreifer POODLE durchführen?
4. Welche SSL/TLS-Versionen unterstützt `fu-berlin.de:443`?
5. Wie viele HTTP-Requests benötigt ein Angreifer, um das 112 Byte lange Session-Cookie von `fu-berlin.de:443` zu entschlüsseln?
6. Verwenden Sie einen Browser, der SSL Version 3 verwendet?

Aufgabe 4. Logjam-Angriff Am 20. Mai diesen Jahres wurde der Logjam-Angriff veröffentlicht[2]. Er basiert auf einem Downgrade-Angriff, der beim Diffie-Hellman-Schlüsselaustausch die Größe der zugrunde liegenden Gruppe auf 512bit reduzieren kann, sowie auf einem Algorithmus, der nach einer etwa einwöchtenlichen Vorberechnung diskrete Logarithmen in dieser Gruppe in wenigen Minuten berechnen kann.

1. Erklären Sie, unter welchen Voraussetzungen ein Downgrade-Angriff auf TLS-Verbindungen durchgeführt werden kann.
2. Warum können die Ergebnisse der Vorberechnung auf so viele verschiedene Verbindungen angewendet werden?
3. Wie lässt sich der Angriff verhindern?
4. Erklären Sie kurz, ob `fu-berlin:443` mit Logjam angegriffen werden kann.

[2]Siehe `https://weakdh.org/`