technische universität
dortmund

Fakultät für Informatik
Lehrstühle 4, 12

Dimitri Scheftelowitsch, Daniel Friesel
Benedikt Maus, Christian Gemke, Thomas Krieg, Felix Homa, Rico van Endern

Wintersemester 2017/18

Rechnernetze und verteilte Systeme
Übungsblatt 13

Ausgabe: 15. Januar 2018, **Besprechung:** 23. Januar – 26. Januar 2018, **keine Abgabepflicht**

Quizfragen

1. Beschreiben Sie die verschiedenen Parteien und ihre Ziele in einem typischen Sicherheits-Szenario.
2. Differenzieren Sie zwischen symmetrischer und asymmetrischer Verschlüsselung.
3. Differenzieren Sie zwischen Authentizität und Integrität einer Nachricht. Kann man Authentizität ohne Integrität erlangen? Kann man Integrität ohne Authentizität erlangen?
4. Beschreiben Sie den Zweck einer digitalen Signatur.

Aufgabe 13.1

Wir betrachten potenzielle Angriffe auf Kommunikation und die sich daraus ergebenden Anforderungen an ein Sicherheitsprotokoll.

(a) Beschreiben Sie den Known-Ciphertext-Angriff. Welche Eigenschaften sollte ein Verschlüsselungsprotokoll erfüllen, damit dieser Angriff nicht funktioniert?

(b) Beschreiben Sie den Man-In-The-Middle-Angriff. Wie kann man ein Authentifizierungsprotokoll gestalten, damit MitM nicht möglich ist?

(c) Beschreiben Sie den Chosen-Plaintext-Angriff. Wie soll ein Verschlüsselungsprotokoll gestaltet werden, damit dieser nicht (so einfach) möglich ist?

Aufgabe 13.2

Eine Computer überträgt permanent Daten mit 10 kB/s und erzeugt alle zehn Sekunden einen einsekündigen Burst-Transfer mit einer durchschnittlichen Datenrate von 1 MB/s (die Wartezeit zwischen zwei aufeinander folgenden Bursts beträgt also neun Sekunden). Zur Einhaltung von Quality of Service-Garantien nutzt der ihm vorgeschaltete Router das *Leaky Bucket*-Verfahren mit einer fest eingestellten Senderate von 90 kB/s und einer 500 kB großen Warteschlange.

Beantworten Sie die folgenden Fragen zu diesem Szenario. Verwenden Sie dabei die Konvention 1 MB = 1000 kB = 1000000 Byte.

(a) Besteht die Gefahr, dass Pakete verworfen werden?

(b) Falls ja: Lässt sich dies durch Anpassung der Warteschlangengröße verhindern?
Falls nein: Unterhalb welcher Warteschlangengröße besteht dieses Risiko?

(c) Wir betrachten nun nur noch den Burst-Transfer und gehen davon aus, dass keine weiteren Datenübertragungen stattfinden. Ab welcher im Bucket eingestellten Senderate würden bei einer Warteschlangengröße von 1000 kB mit Sicherheit keine Pakete verworfen werden?

Aufgabe 13.3 (optional)

Wir wollen die Funktionalität einer Firewall genau betrachten.

(a) Auf welcher Schicht bzw. auf welchen Schichten operiert eine Firewall?

(b) Beschreiben Sie die Funktionsweise und die Filtertypen einer Firewall.

(c) Wie kann man von außen erkennen, ob eine Firewall vorgeschaltet ist?