technische universität
dortmund

Fakultät für Informatik
Lehrstuhl 4

M. Sc.-Inf. Dimitri Scheftelowitsch
M. Sc.-Math. Alexander Frank

Wintersemester 2016/17

Rechnernetze und verteilte Systeme
Übungsblatt 14

Ausgabe: 30. Januar, **Besprechung:** 7. – 10. Februar, **keine Abgabepflicht**

Quizfragen

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

Aufgabe 14.1

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 14.2

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?

Aufgabe 14.3

(a) SNMP-Nachrichten werden über UDP (und insbesondere nicht über TCP) verschickt. Warum?

(b) Es gibt zwei Arten von Kommunikation in SNMP: Request-Response und Traps. Was sind die Vor- und Nachteile dieser Kommunikationsarten bezüglich Overhead, Benachrichtigungszeit bei Ausnahmeereignissen, Robustheit hinsichtlich verlorener Nachrichten?