

2019-Winter_GA2

- 2.3 Per HTTPS soll eine sichere Verbindung zum Server gewährleistet werden. Erläutern Sie die drei Kriterien für eine sichere Verbindung: Authentizität, Integrität und Vertraulichkeit. Geben Sie dabei an, durch welche Maßnahme das jeweilige Kriterium bei einer HTTPS Verbindung erfüllt wird.
- 2.4 HTTPS nutzt bei der Verbindung die Hybridverschlüsselung. Geben Sie alle Schritte an, die von Server und Client ausgeführt werden müssen, damit ein Datenaustausch per Hybridverschlüsselung zu Stande kommen kann.
- 2.5 Die Sportler melden sich auf dem Server mit Benutzername und Passwort an. Beschreiben Sie eine Möglichkeit, wie diese Anmeldedaten sicher auf dem Server gespeichert werden können.

2018-Winter_GA2

- 1.3.3 Beim SSH-Protokoll kommt eine hybride Verschlüsselung zum Einsatz. Beschreiben Sie in Stichworten den Ablauf einer hybriden Verschlüsselung.
- 1.3.4 Die Authentifizierung beim SSL-Protokoll erfolgt mittels Zertifikat. Nennen Sie drei Angaben, die ein solches Zertifikat enthalten muss.

2018-Winter_FA228-FIAE

Aufgabe 2 IT-Systemtechnik

- 2.1 Ihr Auftraggeber bittet Sie um eine Erklärung verschiedener Verschlüsselungsverfahren.
- 2.1.1 Person A möchte an Person B eine verschlüsselte Nachricht versenden. Erklären Sie den Ablauf der asymmetrischen Verschlüsselung. Gehen Sie dabei auch auf die verwendeten Schlüssel ein.



- 2.1.2 Erklären Sie, wie das asymmetrische Verfahren zur Signatur von digitalen Inhalten eingesetzt werden kann.
- 2.1.3 Nennen Sie je einen Vor- und Nachteil der asymmetrischen gegenüber der symmetrischen Verschlüsselung und begründen Sie, welches Verfahren für die Verschlüsselung eines umfangreichen Datenträgers besser geeignet ist.
- 2.1.4 Beim SSL- bzw. TLS-Protokoll werden symmetrische und asymmetrische Verschlüsselungsverfahren miteinander kombiniert. Erklären Sie das SSL/TLS-Verfahren mit Hilfe der Begriffe „Public Key“, „Private Key“ und „Session Key“.

Projektbeschreibung

Die Firma Aircraft AW AG fertigt und modifiziert Bauteile für die Flugzeugindustrie. An ihrem Fertigungsstandort in Deutschland befinden sich die allgemeine Verwaltung, die Finanzbuchhaltung, der Einkauf, Wareneingang und -ausgang sowie die Fertigung und Entwicklung. Ferner betreibt Aircraft AW ein Verkaufsbüro in Seattle, Washington.

- 1.4 Die Außenstelle in Seattle ist über eine VPN-Lösung an das Firmennetz angebunden. Dabei erfüllt VPN die Forderungen nach Authentizität, Vertraulichkeit und Integrität.
 - 1.4.1 Erklären Sie kurz jede der drei oben genannten Forderungen.
 - 1.4.2 Erläutern Sie, womit bei einer VPN-Verbindung die oben genannten Forderungen erfüllt werden.
- 1.5 Für einen sicheren Email-Austausch mit dem Standort in Seattle wird der S/MIME Standard verwendet. S/MIME verwendet ein hybrides Verschlüsselungsverfahren.
 - 1.5.1 Stellen Sie das symmetrische und asymmetrische Verschlüsselungsverfahren gegenüber und erläutern Sie dabei die Unterschiede.
 - 1.5.2 Erläutern Sie die Vor- und Nachteile der beiden Verfahren.
 - 1.5.3 Beschreiben Sie, wie ein hybrides Verschlüsselungsverfahren arbeitet. Gehen Sie dabei auf Schlüsselerzeugung, Schlüsselübergabe und Verschlüsselung ein.
 - 1.5.4 Warum wird bei der E-Mailverschlüsselung das Hybridverfahren verwendet? Begründen Sie Ihre Antwort.

Projektbeschreibung

Das WW-Systemhaus ist ein mittelständisches Unternehmen, das u.a. PCs in Eigenfertigung herstellt. Im Systemhaus sind ca. 500 Mitarbeiter beschäftigt.

Aufgabe 1 Firmennetzwerk

- 1.4 Die Firmenleitung beschließt, im Zuge der NSA-Veröffentlichungen auf eine „sichere“ weltweite Emailkommunikation, unter Einsatz von digitalen Zertifikaten, umzustellen.
 - 1.4.1 Beschreiben Sie, wie das Unternehmen ein entsprechendes Zertifikat erhalten kann.
 - 1.4.2 Erläutern Sie den Vorgang der Verifizierung eines Zertifikates.