1 b)

TLS_AES_256_GCM_SHA384 (Enabled by default)TLS_CHACHA20_POLY1305_SHA256 (Enabled by default)

TLS_AES_128_GCM_SHA256 (Enabled by default)

TLS_AES_128_CCM_8_SHA256

TLS_AES_128_CCM_SHA256

1 a) Hauptunterschied zwischen TLS1.3 [RFC8446] und TLS 1.2 [RFC5246]: Unsichere v

Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

d) This is completely new to TLS 1.3 — the client and the server can establisha key offline and omit the key-share portion of the handshake entirely (in theory, anyway). In practice, this pre-shared-key is negotiated after a "normal" (EC)DHE key establishment and takes the place of what prior revisions of TLS called session resumption.

Security
SoSe 23
LV 4120, 7240

Übungsblatt 10

Digital Signature (Authentication) algorithms:

Aufgabe 10.1 (TLS):

a) Nennen Sie die wichtigsten Unterschiede zwischen TLS1.2 und TLS1.3.

b) Versuchen Sie herauszufinden, welche fünf Cipher Suites in TLS1.3 nur noch unterstützt werden und implementiert sein müssen. *Tipp: TLS.1.3 ist im RFC8446 der Internet Engineering Task Force (IETF) spezifiziert.*

c) Enthalten die Cipher Suites in TLS1.3 irgendwelche Signaturverfahren, wenn ja welche?

d) Welche Algorithmen für Key Share werden in TLS1.3 unterstützt?

e) In der Vorlesung zur sicheren Kommunikation ist auf Folie 20 das Handshake für TLS mit einer Cipher Suite aufgezeigt. Skizzieren Sie zusammen mit dem Handshake Protokollablauf auf Folie 23 der Vorlesung das Handshake Protokoll für TLS1.3 mit den kryptographischen Algorithmen DHE, ECDSA und der Cipher Suite TLS_AES_128_GCM_SHA256.

Aufgabe 10.2 (Aufgabe: Sichere Kommunikation in Architekturen):

a) Welches Kommunikationsabsicherung oder Protokolle sollten für folgende Szenarios verwendet werden, um beste Sicherheit zu gewährleisten? Begründen Sie ihre Aussage.

a1) Sicheres Speichern von Daten in einem Cloudspeicher. Via einem Client- Programm können können Daten auf dem Cloudspeicher mit einer Server-Applikation sicher gespeichert und ausgetauscht werden.

a2) Sicheres Versenden von Emails zwischen verschiedene Firmenservern, welche selber gehostet werden.

a3) Nennen Sie ein Anwendungsbeispiel für eine Transportabsicherung auf der IP-Schicht. Mit welchem Protokoll kann es umgesetzt werden. Begründen Sie warum diese Absicherung in dem Beispiel ausreicht.

a4) Nennen Sie ein Beispiel bei dem eine Absicherung auf MAC-Ebene benötigt wird.

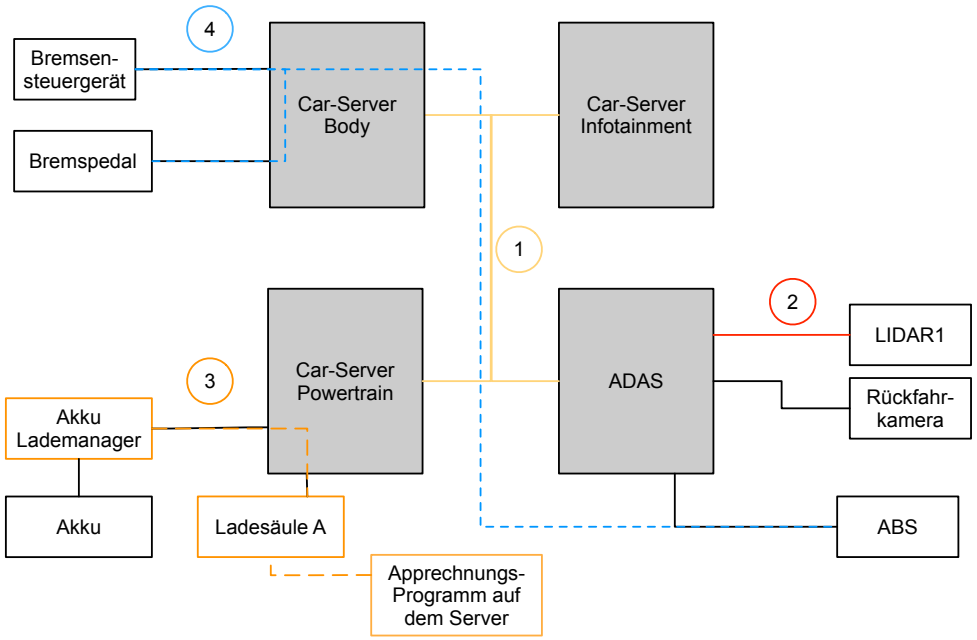
b) Gegeben sei folgende Automotive-Architektur. Bestimmen Sie für die vier folgenden Kommunikationsszenarien, auf welcher Ebene die Kommunikation abgesichert werden muss. Geben Sie beispielsweise Protokolle an. Zur Visualisierung ist die Architektur unten skizziert und die Kommunikationsszenerien entsprechend Ihrer Nummer eingezeichnet.

1 Car-Server Kommunikation: Eine schnelle Kommunikation zwischen den Car-Servern wird benötigt. Jeder Car-Server ist einer Zone zugeordnet und fungiert wie ein Gateway zu der zugewiesenen Zone. Diese Kommunikation muss gegen direkte physikalische Abgriffe zum Mitlesen abgesichert sein. Diese Kommunikation stellt das Backbone des Fahrzeugs dar.

2 Kommunikation der ADAS-Komponeten: Eine sichere Kommunikation zwischen einem LIDAR und dem Advance Drving Assitant Service (ADAS) Server muss abgesichert werden. Die beiden Komponenten kommunizieren über Automotive-Ethernet und stellen sich gegenseitig verschiedene Services und Schnittstellen für Applikationen zur Verfügung.

3 Sicheres Laden und Abrechnen mit der Ladekosten: Zwischen dem Akkumanager und dem Abrechnungsprogramm auf dem Server wird Über die Ladesäule eine sichere Verbindung etabliert, um die Daten (Konto- und Zahlungsdaten) zur Abrechnung sicher auszutauschen.

4 Auf dem Bremsensteuergerät gibt es die Funktion *Notbremsung* diese kann durch Nachrichten von dem Bremspedalkontroller oder dem Antiblockiersystem (ABS) gesendet werden. Der Bremsenkontroller hat eine Applikation, welche die Beschleunigung des Bremspedals misst und daraus ableitet, ob der Fahrer eine Vollbremsung machen möchte. Diese Applikation kann dem Bremsensteuergerät eine Notbremsnachricht schicken. Ebenso kann das ABS der Bremse eine Notbremsnachricht zum Einleiten einer Notbremsung schicken.



Aufgabe 10.3 (Aufgabe: OAuth 2.0):

a) Lesen Sie sich den Artikel unter [Link] zum Thema OAuth 2.0 durch. Versuchen Sie den Anmeldeprozess, der im Artikel unter dem Rich-Client-Szenario beschrieben wird, auf die Anwendung zur Anmeldung bei der B2D-App anzuwenden. In diesem Szenario wird angenommen, dass ein App-Benutzer sich über seinen Google-Account mithilfe von OAuth 2.0 online auf der Webseite eines B2D-Servers in sein Benutzerkonto einloggen kann. Die Anmeldeseite kann entweder über einen Browser aufgerufen werden oder direkt aus der B2D-App über einen Webservice. In diesem Beispiel dient Google als Identitätsanbieter. Zeichnen Sie ein Diagramm, das diesen Anmeldeprozess veranschaulicht