

1) Authentifizierung: Vertrauen in die Richtigkeit von Nachrichten, welche Entscheidungen bezüglich der Sicherheit betreffen.

- Datenintegrität: Daten nicht verändert werden von einer unbefugten Partei

- Datenvertraulichkeit: Unautorisierte Inhalt von Nachrichten nicht lesen

- Erkennen von Fehlverhalten + Vidermaß: Erkennen von Zertifikatsmissbrauch + Fehlverhalten, sowie die Fähigkeit diesen Fahrzeugen das Recht zu nehmen Nachrichten zu versenden, welche andere vertrauen werden.

2) Individuals, loosely coordinated groups, ^{Gegner/Konkurrierende} ^{Ausländische} Adversary organisations, Foreign Governments, Government agencies

3) Senden falscher Sicherheitsnachrichten: Erzeugen unnötige Warnungen bei anderen Fahrzeugen.

- Unschuldige Fahrzeuge beschuldigen sich falsch zu Verhalten \rightarrow Erschwert das Finden von Fahrzeugen die sich tatsächlich falschverhalten

- Imitieren von Fahrzeugen/Network entitäten: Andere Fahrzeugen vorgehen es wären mehr Autos in der Nähe als es tatsächlich sind \rightarrow z.B. Dreck vor einem am Bremsen

- Denial of Service (DoS): Deaktivieren/stören der Kommunikationsfähigkeit anderer Fahrzeuge

4) Kryptographische Algorithmen/protokolle, Sicherheitsunterstützende Mechanismen

5) Daten in Geheimtext umwandeln um seine Bedeutung zu verheimlichen

6) Sym: Ver-/Entschlüsseln mit dem selben Schlüssel

Asym: Versch. mit Pub. Key, Entsch. mit Priv. Key

7) Hash des Klartext berechnen \rightarrow Versch. mit Pub. Key \rightarrow Mit Nachricht versenden \rightarrow Hash entsch. \rightarrow Vergleichen mit Hash empf. Nachricht

8) Sichert das Zertifikat eines Fahrzeugs ab, da man dieser Zertifizierungsstelle vertrauen kann \rightarrow Pub. Key ^{bereits} vorinstalliert, Signierung mit Priv. Key

9) Enthält min. Name + Pub. Key des Besitzers

+ Protocol Version, Seriennummer Zertifikat, Gültigkeitszeitraum, Zertifikat Zertifizierungsstelle

10) Verteilen von Zertifikaten an alle Teilnehmer

11) 1) Root Zertifizierungsstelle ^(RCA) \rightarrow Zertifizieren sich gegenseitig CA = Zertifizierung Autorität (Zertifizierungsstelle)

2) lang Zeit ^(LTCA) " + Pseudonym ^(PCA) \rightarrow Vertrauenspfad zu den RCA

3) ITS Centre/Roadside/Vehicle Station \rightarrow erhalten Zert. von LTCA/PCA

12) RCA: Definieren einheitliche Richtlinien auf alle LTCA's + PCA's

LTCA: Ausgabe LTC's an ITS Stationen

PCA: Autorisiert von RCA, Ausgabe PC's an ITS Stationen

13) Gleichmäßiges Vertrauen + Kosteneffizient der RCA

- Flexibilität bei Prozessintegration \rightarrow Neue Hersteller führen eigene LTCA unter Europäischen RCA + Organisation Geford PCA für alle Hersteller

- Flache Struktur \rightarrow nur ein Zert. pro Nachricht

14) Privatsphäre der Position/Interessen/Sozialer Status/Privatleben

15) Identitäten sind an Fahrzeuge gebunden

16) Durch Benutzung mehrerer Identitäten anstatt einer \rightarrow Verfolgen schwierig, immer andere Ident

17) 1. PCA weisen Basisidentitäten Automobilindustrie zu

2. Diese weisen eine " pro neuen Fahrzeug zu

3. Fahrzeuge erstellen selbst pool von p versch. Pseudonymen in Form von Zertifikatsanfragen

4. " Fragen bei PCA signierung jedes Pseudonyms an über internet

5. PCA überprüft Anfrage \rightarrow falls korrekt, sende signiertes Pseudonym zurück

18) Komplette Zufällig, Periodisch, Geographisch, Fahrzeugwerte/Kommunikationsqualität, Silent Periods

19) Overhead \rightarrow Jedes CAM müsste 150-160 Byte zusätzlich groß sein für Signaturen etc. \rightarrow enorm großer Datenfluss nur für Sicherheit

\rightarrow Jedes CAM muss vor-entsch. werden enorm häufig