Vorschlag für eine Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks

Dipl.-Wirtsch.-Inf. Klaus Plößl
Universität Regensburg
Lehrstuhl Management der Informationssicherheit

Automotive – Safety & Security 2006
12.10.2006

Gliederung

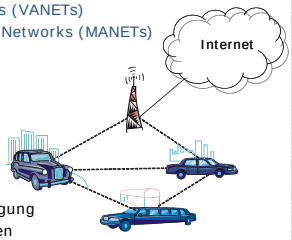
- Begriffe und Annahmen
- Anforderungen an eine Sicherheitsinfrastruktur
- Grundsätzliche Überlegungen
- Vorschlag für eine Sicherheitsinfrastruktur
- Fazit

Automobiles Ad-hoc-Netz

- Engl. Vehicular Ad Hoc Networks (VANETs)
- Untergruppe der Mobile Ad Hoc Networks (MANETs)

- Hauptunterschied
  - Router = Automobil

- Besonderheiten
  - Hohe Geschwindigkeiten
  - Hohe Skalierbarkeit nötig
  - Relativ vorhersehbare Bewegung
  - U. U. hohes Datenaufkommen



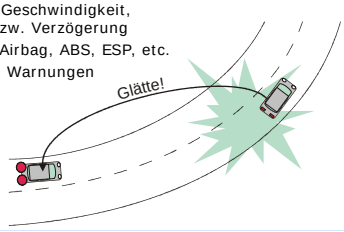
- Betrachtung von
  - Vehicle-to-vehicle communications (V2V)
  - Vehicle-to-roadside communications (V2R)

Automobiles Ad-hoc-Netz

- Hauptziel
  - Erhöhung der Verkehrssicherheit

- Zielerreichung
  - Fahrzeuge agieren als Sensoren
  - Austausch von Telematikdaten, wie
    - Position, aktuelle Geschwindigkeit, Beschleunigung bzw. Verzögerung
    - Sensordaten von Airbag, ABS, ESP, etc.
  - Ggf. Aussendung von Warnungen

- Bsp. für Warnungen
  - Unfallwarnung
  - Stauwarnung
  - Wetterwarnung
  - ...



Anwendungskategorien

- Telematiknachrichten und Warnungen (A1)
  - Geocast
  - Bsp. Warnung bei Vollbremsung, Auslösen eines Airbags, erkanntem Stau, ...

- Alarmsignale und Anordnungen (A2)
  - Geocast und Unicast
  - Bsp. Feuerwehr, Polizei, Geschwindigkeitsbegrenzung, Kreuzungsassistent, ...

- Komfort-Dienste (A3)
  - Meist nicht kritisch für Verkehrssicherheit
  - Meist Unicast
  - Bsp. Breitbandiger Internet-Zugang, Location Based Services, Fernwartung des Fahrzeugs, ...

Begriff „Sicherheitsinfrastruktur“ und Annahmen

- Sicherheitsinfrastruktur
  - Schafft Vertrauensbasis
  - Ermöglicht den Einsatz von Kryptographie
  - Umfasst alle technischen und organisatorischen Maßnahmen und Einrichtungen zum Erreichen der Schutzziele

- Annahmen
  - Daten innerhalb des Fahrzeugs sind korrekt
  - Einbindung korrekter Zeit- und Ortsangaben in die Nachrichten wird durch andere Infrastruktur ermöglicht

Anforderungen

- Integrität
  - Veränderung von Nachrichten bei der Übertragung im VANET verhindern bzw. erkennbar machen (I1)
  - Eindeutige Senderauthentifizierung für A2 (I2a)
  - Nachträgliche Zurechenbarkeit für A1 und A3 (I2b)
- Vertraulichkeit
  - Verschiedene Vertraulichkeitsstufen (V1)
  - Vertraulichkeit administrativer Nachrichten (V2)
  - Schutz der Sicherheitsinfrastruktur (V3)
- Performance und Verfügbarkeit
  - Effizienz bei Rechenkapazität und Bandbreite (P1)

Anforderungen

- Mehrseitige Sicherheit
  - Erstellung von Bewegungs- und Dienstnutzungsprofilen erschweren (D1)
  - Automatisierte Überwachung und Strafverfolgung verhindern (D2)
  - Sender- und Empfängeridentität schützen (D3)
- Wirtschaftlichkeit und Akzeptanz
  - Niedrige Kosten für Fahrzeughard- und Software (W1)
  - Wenig Aufwand bei der Registrierung (W2)
  - Betrieb möglichst kostengünstig (W3)
  - Akzeptanz der Teilnehmer (W4)

Grundsätzliche Überlegungen: Identität

- Fahrzeugbezogene Identität
  - Motivation
    - Viele fahrzeugbezogene, oft automatisch versendete Daten
    - Fahrer unter Umständen nicht für eventuelle Falschmeldungen verantwortlich
  - VANET-Identität aus Identitätsmerkmalen des Fahrzeugs
  - Entspricht in digitaler Form der gegenwärtigen Situation
  - Speicherung
    - In manipulationssicherer Hardware im Fahrzeug

Grundsätzliche Überlegungen: Identität

- Personenbezogene Identität
  - Motivation
    - Alle Nachrichten hängen von der Fahrweise und dem Zustand des Fahrzeugs ab
  - Erleichtert die Rekonstruktion von Unfall- und Fahrerflucht-Situationen
  - Aktuelle Gesetzgebung macht allerdings grundsätzlich den Fahrzeughalter verantwortlich
  - Sinnvoll für Personen mit erhöhten Privilegien
  - Speicherung
    - Fahrzeug und Fahrzeugschlüssel nicht geeignet
    - Elektronischer Führerschein

Grundsätzliche Überlegungen: Identität

- Gemischte Identität
  - Motivation
    - Nachrichten sind sowohl dem Fahrzeug als auch dem Fahrer zurechenbar
  - Einsatz erhöhter Privilegien besser kontrollierbar
  - Unter Umständen genauere Bewegungsprofile möglich
  - Mehrkosten für zwei Identitäten
  - Speicherung
    - Fahrzeug und elektronischer Führerschein

Grundsätzliche Überlegungen: Identität

- Fazit
  - Fahrzeugbezogene Identität angemessen
  - Zusätzliche personenbezogene Identität
    - Für Personengruppen mit erhöhten Privilegien
    - In bestimmten Situationen auch für „normalen“ Fahrer sinnvoll
      - Nachträgliche Identifizierung ausreichend
      - Sollte nicht zwangsweise zur VANET-Identität gehören

Grundsätzliche Überlegungen: Authentifizierung

- Symmetrische oder asymmetrische Kryptographie
- Vorverteilung des benötigten kryptographischen Materials relativ problemlos

- Symmetrische Kryptographie
  - Beide Kommunikationspartner kennen den Schlüssel
  - Verlust der Nichtabstreitbarkeit
  - Nur mit Hilfe einer Trusted Third Party (TTP) realisierbar

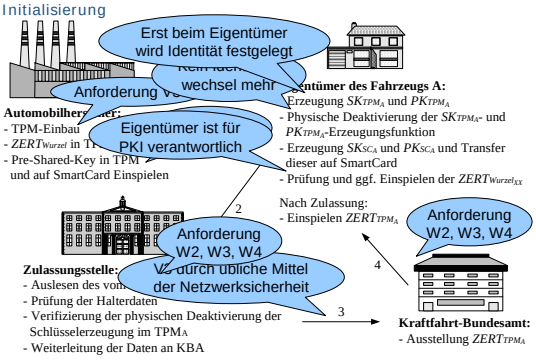
- Asymmetrische Kryptographie
  - Public Key Infrastruktur (PKI) nötig
  - Digitale Signatur und Zertifikate vergrößern die Nachricht
  - Nicht so performant wie symmetrische Kryptographie
  - Zertifikatsrückrufe müssen behandelt werden

Vorschlag für eine Sicherheitsinfrastruktur

- Überblick
  - Asymmetrischer Teil mit PKI
    - Fahrzeugbezogene Identität
    - Erhöhte Privilegien durch Attribut-Zertifikate
    - Integritätssicherung verkehrssicherheitskritischer Nachrichten (A2 und teilweise A1)
    - Basis-Authentifizierung
    - Sicherung der Schlüsselverteilung des symmetrischen Teils
  - Symmetrischer Teil
    - Wechselnde Pseudonyme
    - Integritätssicherung nicht verkehrssicherheitskritischer Nachrichten (A3 und teilweise A1)
    - Verschlüsselung
    - Benötigt manipulationssichere Hardware
    - Einteilung in geographische Cluster mit zuständiger TTP

Vorschlag für eine Sicherheitsinfrastruktur

- Initialisierung



Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Asymmetrischer Teil
    - Asymmetrisch gesicherte Nachricht

Anforderung I1 und I2a bzw. I2b

Daten mit Adressinformationen	Digitale Signatur	$ZERT_{Sender}$

  - Gesicherte Nachrichten
    - Verkehrssicherheitskritische Meldungen
    - Alarmsignale
    - Anweisungen
  - Nach dem Initialisierungsprozess einsetzbar
  - Rückrufisten
    - Für Warnungen nicht kritisch
    - Für Alarmsignale und Anweisungen
      - » Kurzzeit-Attributzertifikate

Bessere Prüfung der Privilegien

Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Symmetrischer Teil
    - Gesicherte Nachrichten
      - Nicht verkehrssicherheitskritische Meldungen
      - Nachrichten der Komfort-Dienste
    - Setzt Kontakt mit zuständiger TTP
      - Verteilung von Pseudonymen
        - » Nur TTP speichert Zuordnung der Ps (fahrzeugbezogenen) Identitäten
        - » Unabhängige Datenschutzorganisationen als TTPs
      - Verteilung symmetrischer Schlüssel für
        - » Nachrichtenverschlüsselung
        - » Nachrichtenauthentifizierung
    - Performanter als asymmetrischer Teil
    - Ausschluss von Störern leicht möglich

Anforderung D1, D2, D3
Anforderung D2, W4
Anforderung P1

Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Symmetrischer Teil
    - Symmetrisch gesicherte Nachricht

Anforderung I2b
Anforderung I1

Daten mit Adressinformationen	PA	HMAC mit $k_{MAC_{PA}}$	HMAC mit $k_{MAC_{ALL}}$

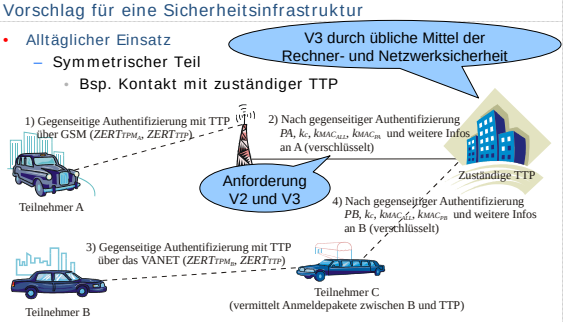
verschlüsselt mit k_c

    - k_c und $k_{MAC_{ALL}}$
      - Für alle Teil… …em bestimmten geographischen Gebiet gleich
      - Periodischer Wechsel
    - PA und $k_{MAC_{PA}}$
      - Mindestens ein Paar pr… …
      - Periodischer Wechsel
    - Nachrichtenbearbeitung… …elspeicherung komplett in manipulationssich…
    - Für Komfort-Dienste anwendungsspezifische Verschlüsselung möglich

Anforderung V1, ggf. D3
Anforderung D1, D3
Anforderung V3
Anforderung V1

Vorschlag für eine Sicherheitsinfrastruktur

- Alltäglicher Einsatz
  - Symmetrischer Teil
    - Bsp. Kontakt mit zuständiger TTP



Fazit und Ausblick

- Fazit
  - Integrität und Authentizität aller Nachrichten wird gewährleistet
  - Keine gravierenden Performance-Einbußen oder Verletzungen der Privatsphäre
  - Gezielte Vergabe erhöhter Privilegien
  - ⇒ Kombination asymmetrischer und symmetrischer Kryptographie erfüllt Anforderungen besser als bisherige getrennte Ansätze
- Ausblick
  - Untersuchungen in Bezug auf den Zeitraum der Schlüsselgültigkeit und der geographischen Verteilung der TTPs
  - Spezifizierung der Bedingungen zur Herausgabe der Zuordnung Identität ↔ Pseudonym
- Kontakt:
  - Klaus.Ploessl@wiwi.uni-regensburg.de