

Informationstag "Das Automobil als IT-Sicherheitsfall"

Berlin, 11.05.2012

Apps im Auto :

**Auf dem Weg zu einer sicheren, offenen
Softwareplattform im Fahrzeug**

Hakan Cankaya, ESCRYPT GmbH, Berlin



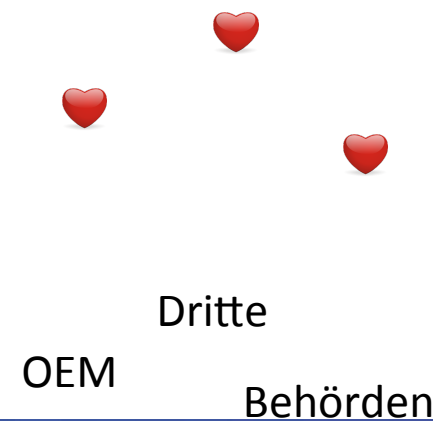
Apps im Auto

Auf dem Weg zu einer sicheren, offenen
Softwareplattform im Fahrzeug

Hakan Cankaya

escrypt GmbH – Embedded Security, München

11.05.2012



IT im Fahrzeug – Gestern vs Heute



Von KITT...

Zur Mittelklasse.



EE Architektur - Heutige Lage

- Komplexe Vernetzung der Funktionen im Auto
- Überschaubare Schnittstellen nach Außen
- Weitgehend statische Architektur
- Individuelle Infotainment Lösungen von Autoherstellern
- Weitgehend statische Infotainment Systeme
- Langsame Integration von Trends
- Beschränkte Anbindung von externen Geräten

Trotzdem viele Sicherheitslücken

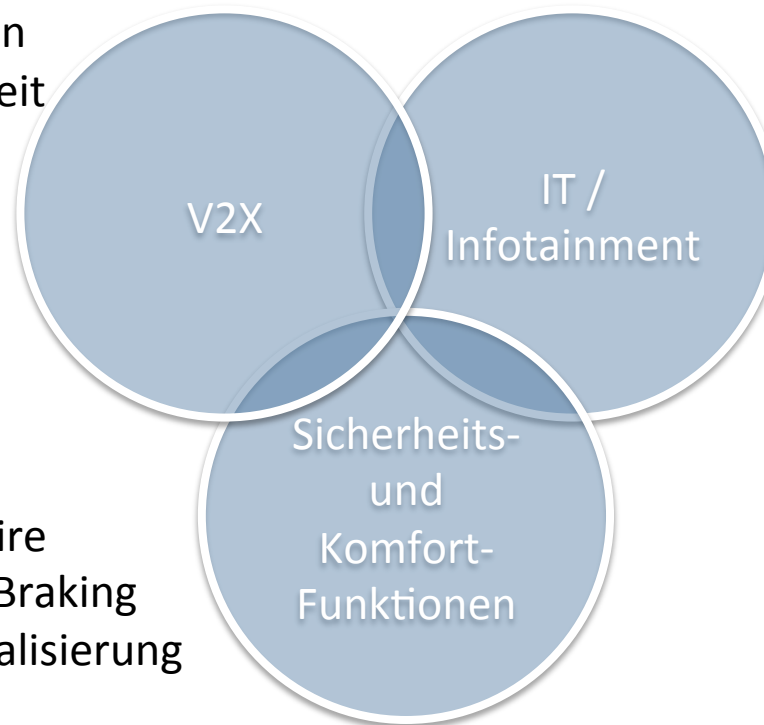
Externer Angriff auf Bordnetz [Checkoway,2011]

- Interne Angriffe (z.B. CAN-Injektion) von 2010 auf externe Schnittstellen erweitert
- Erfolgreiches Abhören (Freisprechmikro) und Eingreifen ins CAN Bus über Fake-CD, GSM und Sprachkanal!



Ein Schritt in die Nahe Zukunft

- Vernetzte Fahrzeuge
- Vernetzte Funktionen
- Kooperative Sicherheit



- App-Store im Auto
- Fahrer-Auto Interaktion
- Offene Architektur/
Schnittstellen
- Gesetzliche Vorschriften
(z.B. Maut)

- X-by-wire
- Active Braking
- Personalisierung

Vision zukünftige IT Plattformen für Automobile

- Fahrzeughalter/OEM kann dynamisch Applikationen / Funktionen installieren.
 - Unterhaltung, ITS, Komfort, Verkehrssicherheit etc.
- Mehrere Parteien können SW für das Fahrzeug entwickeln.
- Sicherer Kommunikations-Gateway
 - Unter anderem auch zu sicherheitskritischen Medien
- Stabilität und Zuverlässigkeit bei verschiedene Arten von Applikationen.
- Nicht Security HW oder SW sondern Secure Computing Plattform.

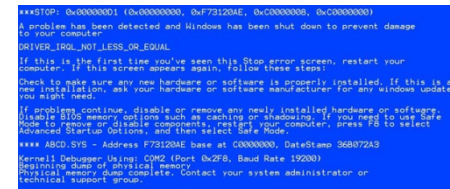
Was kann alles Schief gehen ?!

Einige Beispiele...



Bösartige Apps finden Weg ins Auto

Mehrere Apps mit verschiedenen Anforderungen schwer vereinbar im selben Betriebssystem



Offene Kommunikationsschnittstellen verursachen Sicherheitslücken

Viren oder Fahrzeughalter manipulieren das Betriebssystem



Was machen wir dagegen?

OVERSEE ist ein Ansatz die Vision einer offenen und sicheren IT Plattform für Autos zu realisieren...

OVERSEE



oversee

Open Vehicular Secure Platform



- Projekt im Rahmen von FP7

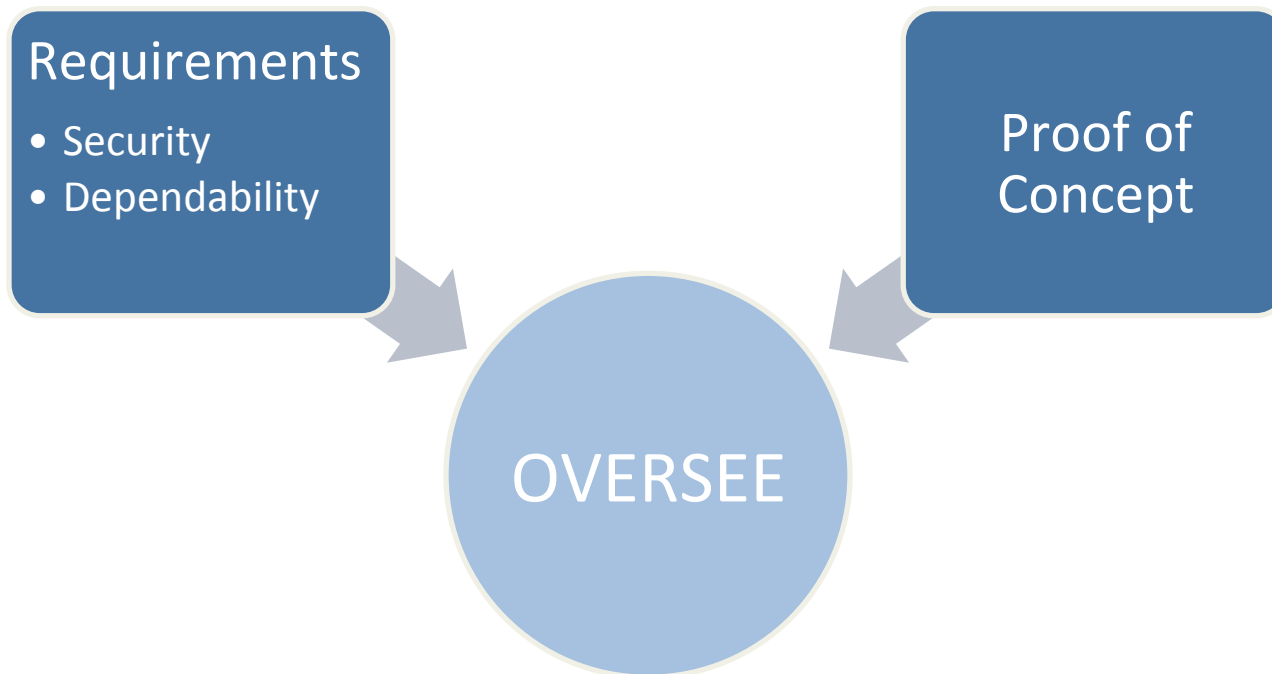
- Teilfinanziert von der EU
- 8 Organisationen involviert.

- Ziele

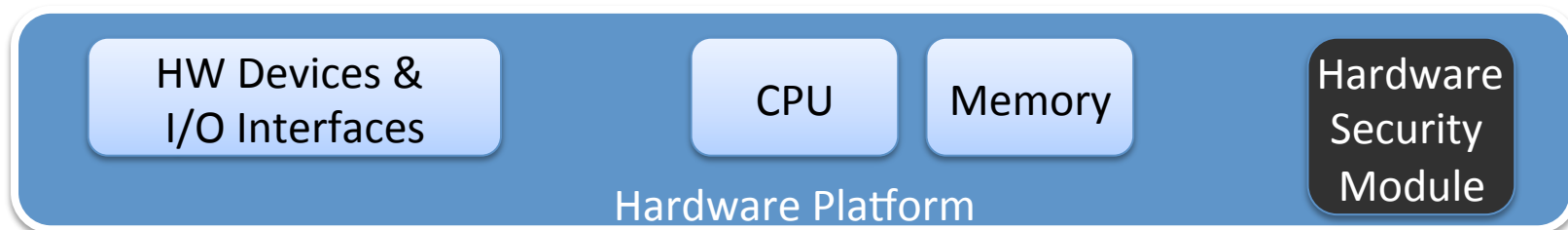
- Offene
- Flexible
- Aber trotzdem sichere

Kommunikations- und Applikations-
Plattform für das Auto.

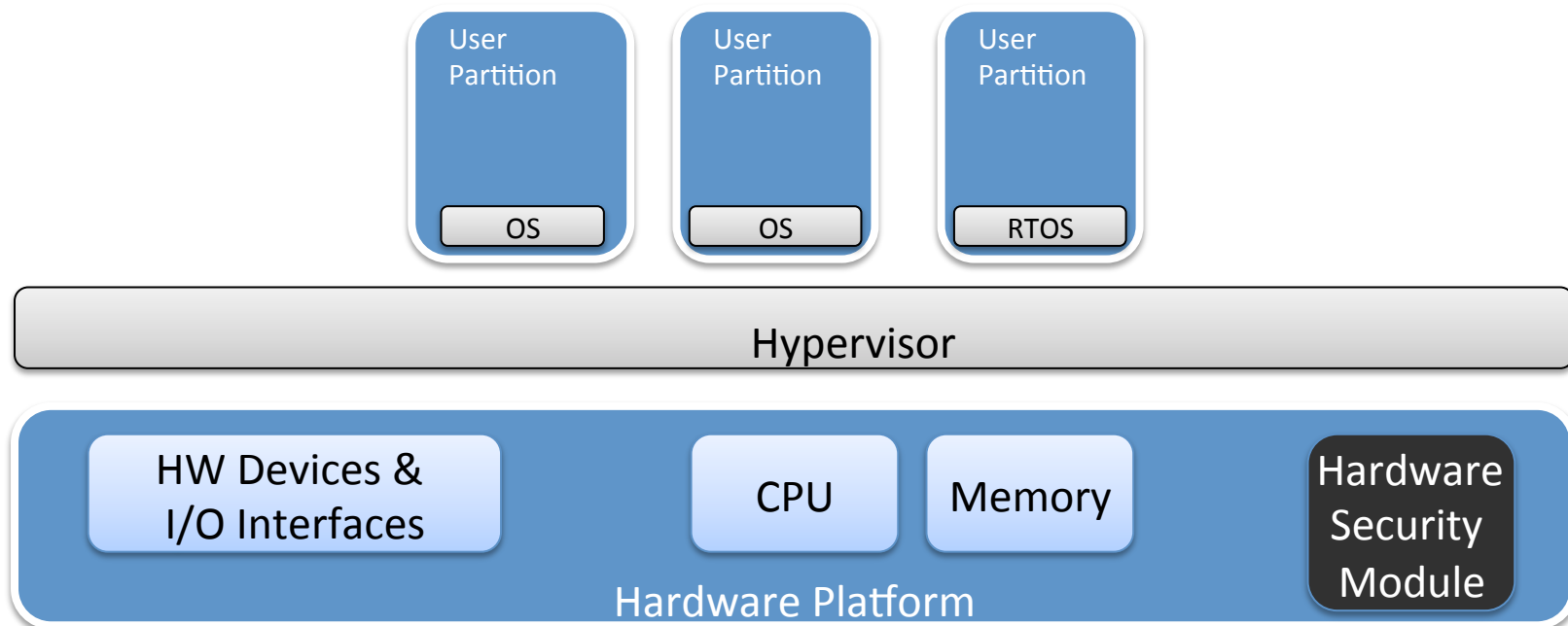




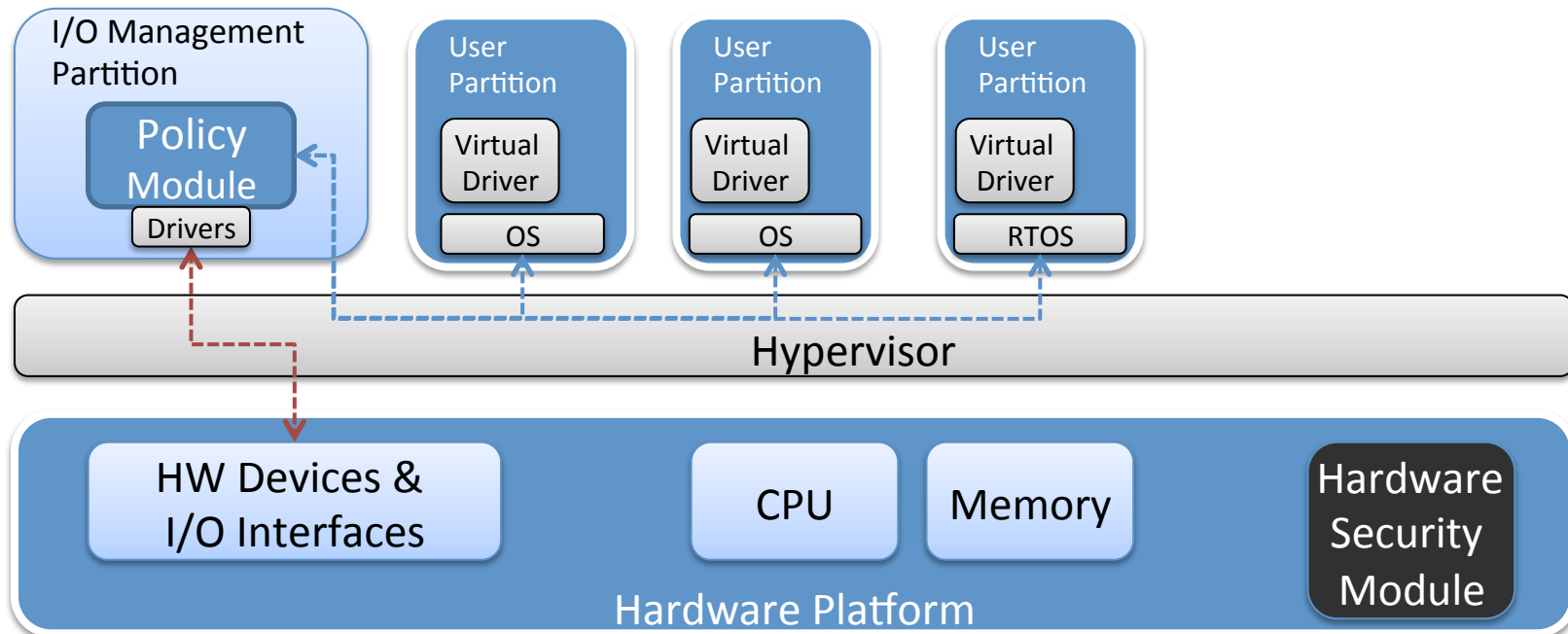
OVERSEE HW



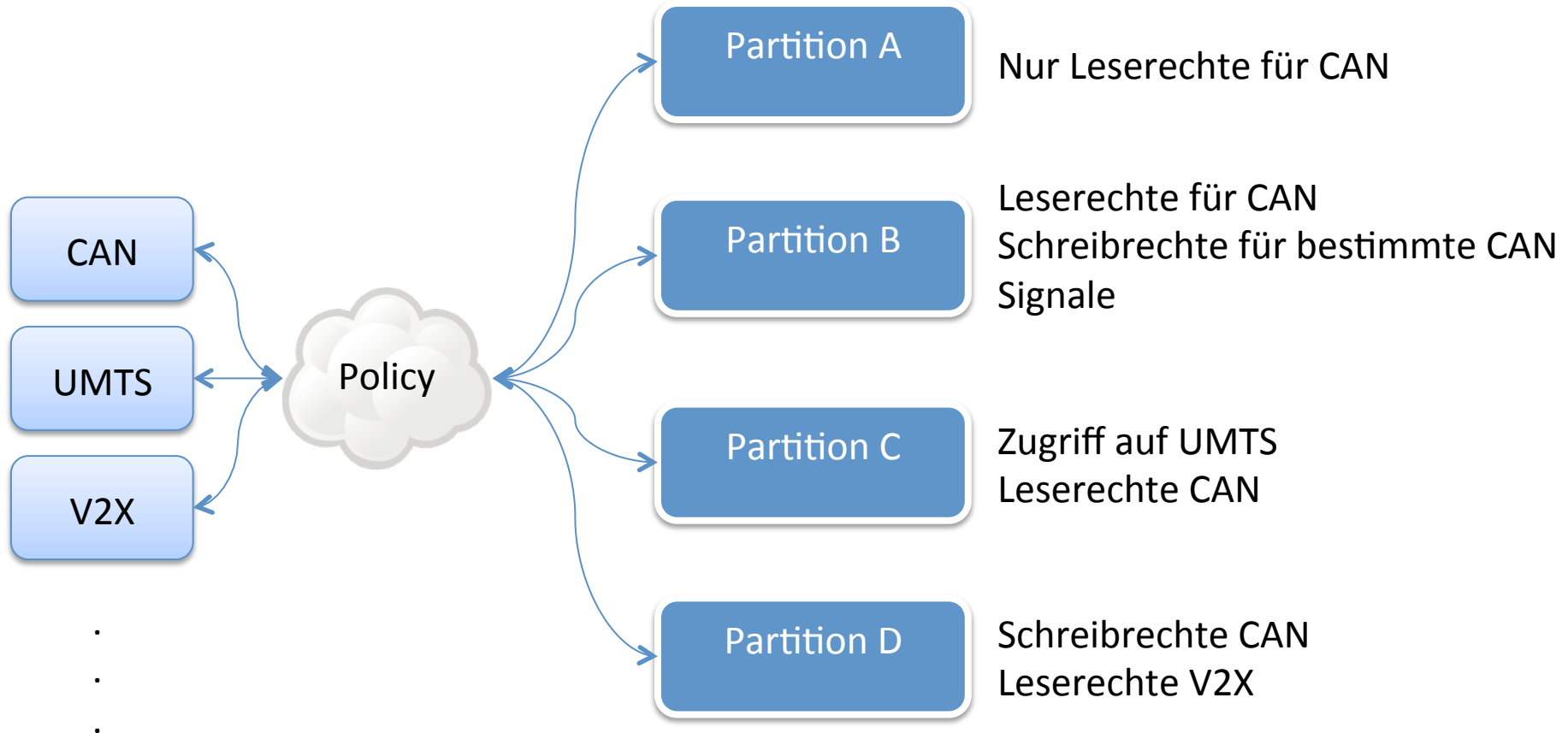
OVERSEE - Virtualisierung



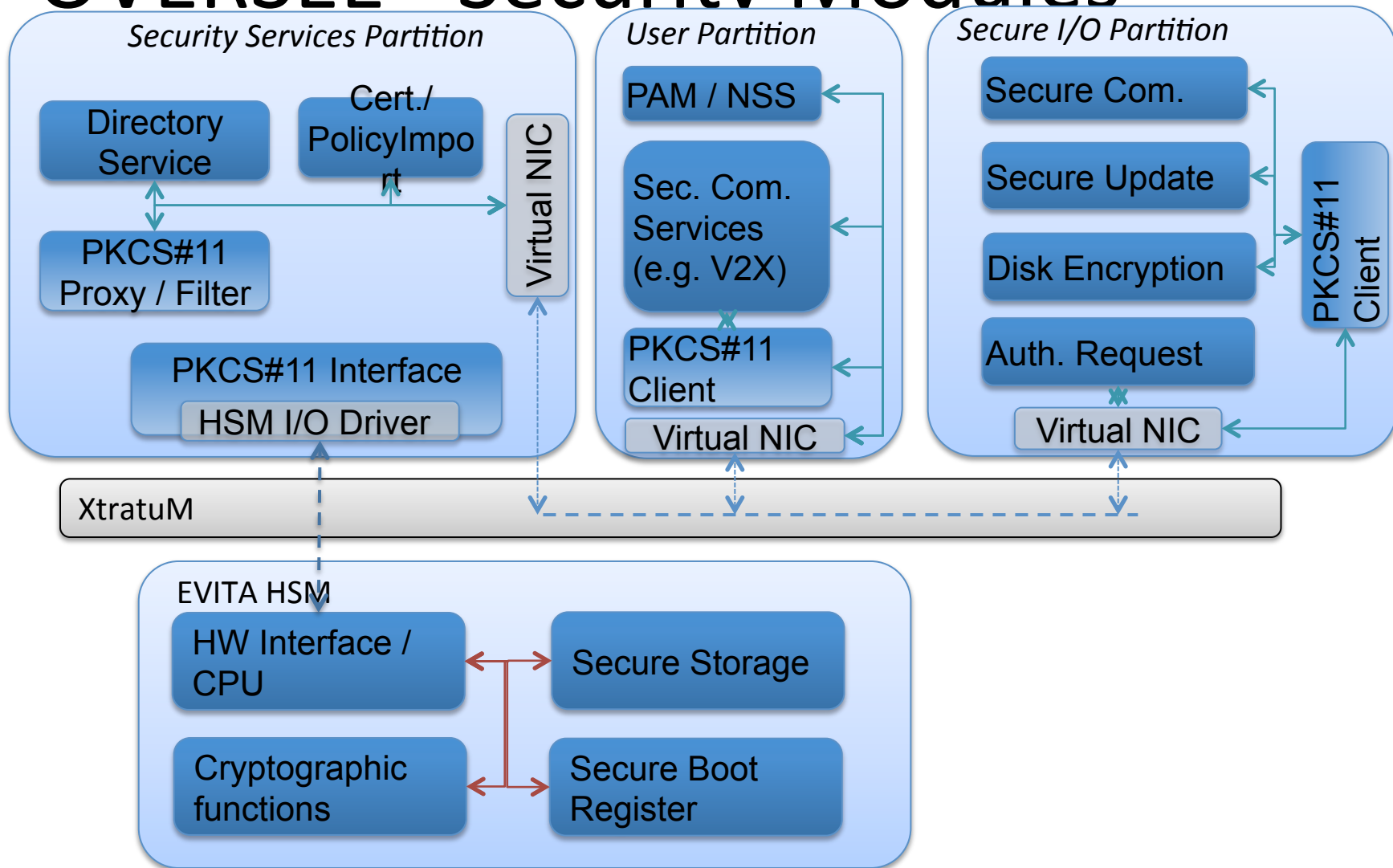
OVERSEE – Ressourcen-Verwaltung



OVERSEE – Ressourcen-Verwaltung



OVERSEE - Security Modules



Weitere Security Services

- Secure Boot
- Secure SW Install/Update
 - SW Pakete werden erst zentral verifiziert danach installiert
 - App Installations-Policies können hier durchgeführt werden
- ITS / V2X Kommunikationsstack
- Zentraler Authentisierungs-/Autorisierungs-Verzeichnis

Warum der Aufwand

- Hardware Security Module
 - Hardware Trust Anchor : Starker Manipulationsschutz
 - Ermöglicht effektiven Secure Boot
 - Sichere Aufbewahrung von Schlüsseln
 - Schnelle Kryptographische Berechnung
- Hypervisor
 - Isolierte Laufzeitumgebungen somit getrennte Risiken und besserer Schutz
 - Ermöglicht Zentrale Verwaltung von I/O Zugriffen
 - Ermöglicht flexible Architekturen mit parallelen Betriebssystemen (RT OS, OseK, Android etc...)
- Security Services
 - Ausführung von sicherheitsrelevanten Services in sicherer Umgebung

Beispielhafter Einsatz

*OVERSEE
System
Partitions*

eCall



ITS / V2X



OEM
Services

Spielplatz



Virtualisierungsschicht

Fazit

OVERSEE ermöglicht

- Security & Dependability
- Einfachen Übergang in die offene IT-Welt
 - Offene Betriebssysteme können wiederverwendet werden
- Sichere Schnittstellen für verschiedene IT Anwendungen mit verschiedenen Anforderungen
- Verschiedene Business-Models für OEM's
- Erfüllung zeitlicher Anforderungen

**Danke.
Fragen?**

M.Sc. Hakan Cankaya
Security Engineer
hakan.cankaya@escrypt.com

Dr.-Ing. Jan Pelzl
Geschäftsführer
jpelzl@escrypt.com

Dr.-Ing. Thomas Wollinger
Geschäftsführer
twollinger@escrypt.com

Dr.-Ing. André Weimerskirch
CEO USA
aweimerskirch@escrypt.com