

IT-Security and Privacy for Telematics-Services

Contribution to PAMPAS '02 - Workshop on Requirements for Mobile Privacy & Security

Albert Held, Rainer Kroh

DaimlerChrysler AG, Telematics Research
D-89013 Ulm, Germany
{*albert.held,rainer.kroh*}@daimlerchrysler.com

July 30, 2002

1 Telematics

For an automotive company, mobile systems are primarily cars. Nowadays cars are equipped with a multitude of electronic devices which - besides operating the car - allow for communication with other cars, the roadside, dedicated service centers and the internet. The percentage of cars with so called *Telematic Platforms* will increase in the future. Besides these onboard systems, the users may bring other devices such as mobile phones, PDAs, etc. into the car. These devices can be plugged into the in-car communication bus and use the car's computing and communication facilities as well as data/information stored in the car's system.

New types of applications will emerge in various areas such as Traffic Management, Emergency Call, Route Guidance, Online Diagnosis, Remote Update, Fleet Management, Mobile Office, etc..

Obviously, for a global company all of the four main areas of the workshop are important, but we will focus on application and technology requirements.

2 Application Requirements

As mentioned before, there are various types of applications. As a first step, we distinguish between user-centric, vehicle-centric, trip-centric, traffic-related and other applications. All of these have specific requirements concerning security and privacy. So the most important issue is the development of a **Security Model** and a **Security Framework** to identify the various components of the entire service-chain, their relationships between each other and to create a common platform for flexible security services. Open standards and scalability are crucial points of this platform.

Other issues are

- **Identity-Services / Authentication of Users and Vehicles:** There are many applications, where cars act as clients or servers. Authentication includes single-sign-on technologies

as well as PKI (Public Key Infrastructure) approaches.

- **Authentication of Software:** Lots of software is transmitted - from email attachments, applets to automatic software updates. To detect malicious code (e.g., computer viruses) the integrity and origin of the software has to be checked.
- **Privacy:** Mobile applications, such as location based services rely more and more on personal information about the user. The protection of a user's privacy will become a key factor for the success of telematics applications. It is necessary to allow users to control what private/personal information is collected, stored, processed and provided to others.
- **End-to-End Security;** Applications are always end-to-end. It is still an open issue how to integrate or to combine the security services of the different system layers. This is especially true if various parties, such as vehicle, mobile communications system, internet, etc. are involved.

3 Technology Requirements

Besides the above mentioned application-oriented view, there is a more system oriented view which deals with problems for all applications.

Issues here are:

- **Vehicle Security:** This looks at the car and its components. Vehicle security includes the protection of hardware and software integrity - for the vehicle networks and devices -, the secure storage and transmission of private or sensitive information administered by the vehicle, the logical separation of different in-car networks and the protection against unauthorized access to the vehicle and its components via radio interfaces or plugged portable devices.
- **Intrusion Detection:** With all the threats, it is important to automatically detect that something unauthorised is going on: within the vehicle, in the communication network's infrastructure or at the service provider.
- **Incident Handling and Recovery:** If a security relevant incident is detected, processes and mechanisms to automatically react are needed. Usually one can not shut down any vehicle components while driving, so some kind of fault tolerance is needed to keep the system running until it can be reset to a secure state.
- **Management:** Cars are not computers. People do not want to become system administrator in order to drive a car. Therefore the security management must take this into account. This includes the key management for all the crypto mechanisms as well as the administration of security components such as vehicle-firewalls