1st C2C CC Security Workshop Summary

(Prepared by Matthias Gerlach, <matthias.gerlach@fokus.fraunhofer.de>)

The first open C2C CC Security Workshop took place on the 16.11.2006 in Berlin. 50 participants enjoyed interesting presentations and vivid discussions both in the plenary and in private conversations. The workshop was jointly organized by the C2C CC Security Working Group, and the SEVECOM Project.

The workshop laid the foundation for follow-up workshops both open to the public and private C2C CC meetings.

The Presentations

In his talk on **"Security requirements of C2C Applications"**, **Amer Aijaz (VW)** briefly reviewed the major threats to C2C applications and derived a set of security requirements. Those requirements comprised identity authentication, integrity verification, freshness checks, anonymity, privacy revocation and legal proof of misuse.

Christian Wewetzer (VW) reported on the "**Current Status of the C2C Applications Working Group"**. Currently, 6 types of V2X communication (called *applications*) are defined, as is a list of possible use-cases for these applications. The use-case currently contains 47 entries. For each use-case, an intuitive estimate of the security-criticality is provided. The presentation also raised the issue of cooperation between the security working group and the applications working group.
Discussions: were addressing the applicability of anonymous payment in C2C applications and the identification of nodes. What would be the impact of applications on privacy by changing pseudonyms and vice versa? Are there any constraints applications impose upon pseudonym change algorithms?

The presentation on the **"Current Status of the C2C NET/MAC/PHY Working Group"** by **Massimiliano Lenardi (Hitachi)** summarized the status of these working groups that currently have joint meetings. The talk mentioned the current application for an exclusive frequency-band for safety applications. Further, important characteristics and requirements of the three layers (and cross layer issues) such as QoS support, congestion control, power control, support for multiple addresses are described in the presentation.
Discussions: Concerned the main differences between 802.11p/WAVE and the European approach. Using the channels allocated for safety will be illegal in the EU (by non-safety units). What is the impact of changing pseudonyms on the protocol stack (MAC/NET)? How can cross layer QoS issues be combined with security requirements (may this be a dependability requirement?)? Is the use of authenticated/protected position information e.g. by the GALILEO system considered?

Ken Laberteaux (Toyota) reported on **"CAMP and the Vehicle Safety Communication 2 Consortium"** and his personal perspective on **"DSRC Research topics '07-'09"**. The first presentation provided an overview of the status of the VSC-A

(Successor of the VSC project. A stands for Application). With regard to security, privacy versus authentication, security overhead and coordination with best practices from VIIC, IEEE 1609.2 etc. in the fields of certificate authorities and revocation are mentioned to be an issue. The second presentation sketched research issues from high-power transmission to a hash-chain based authentication scheme. Ken mentioned the possibility for collaboration between US and European work.
Discussions: were mainly about tests for high power level sending and the applicability of a hash-chain based authentication scheme (TESLA) for vehicular ad hoc networks.

Frank Kargl (Uni Ulm) gave a presentation about **"Threats and Security Requirements for VANETs"** presenting work that has been carried out in the SEVECOM project. In includes an extensive and structured risk analysis of vehicular applications and the identification of a list of security mechanisms for those applications. 10 applications out of a list of 55 have been looked at in more detail using semi-formal use case and attack use case descriptions. The information can be accessed via the SEVECOM website (www.sevecom.org) in Deliverable 1.1 of the project.

Matthias Gerlach (Fhl FOKUS) and Andreas Festag (NEC) reported on the **"NoW (Network on Wheels) Security Architecture"**. They propose to look at the security architecture using different views (functional layers, organizational, reference model, information centric) and describe the security architecture accordingly. The main ideas in the first (general) part of the presentation are: the context broker for local access to data (and security data), the use of confidence tags and security stubs and the core security application. The second part of the presentation covered the implementation of the security architecture in the network layer and included the use of digital signatures for mutable and immutable fields, local reputation, plausibility checks and pseudonyms.

Discussions: were concerned about the middleware approach, and if standards for middleware technology are used (they are not yet). Is access to the middleware protected somehow? Another remark was that cross layer aspects are hidden (not reflected) by the simplification of the core security application.

Hans-Peter Schwefel (Aalborg University) presented the "**HIDENETS dependability architecture"** arguing that dependability, QoS provisions and security overlap at least partially. The presentation includes a description of the network scenario and node architecture. One of the main ideas within HIDENETs is the concept of "wormhole communication" where a physically or logically separated channel is used as a backup for the communication system. More information can also be found in the public deliverable D1.1 on the HIDENETS web-server (www.hidenets.aau.dk). It was agreed that more liaison with eSafety projects possibly would be useful. Antonio Kung will contact COMeSafety on this.

Panos Papadimitratos (EPFL) gave a presentation on **"Privacy and Identity Management"**. The talk discussed the transition of identity management from current

transportation systems to vehicular communication (VC) systems. Then, it was concerned with a number of approaches that can independently and more so if combined enhance privacy. Finally, the presentation outlined a number of points of caution for the introduction of privacy enhancing technologies, first in the form of requirements to be satisfied by the pseudonymous/anonymous secure communication system and then by pointing out relevant distinctive VC aspects.
Discussions: touched the subject of federation and the involvement of several different operators. Further, is the approach interoperable with UMTS/GSM approach?

Frank Kargl (Uni Ulm) presented the **"Proposal for a SEVECOM Software Architecture"** i.e. a modular way to integrate different security solutions into a software platform. The main ideas in the architecture are pluggable security modules, e.g. for authentication, integrity protection, privacy, etc., for MAC, NET and PUB/SUB (publish/subscribe) middleware layer integrated using a Linux netfilter-like approach; further a security manager mediating the different security requirements for each application and an xml-based configuration language for each application to specify the security requirements.

Thomas Eymann (Bosch) presented the **"EASIS Security Architecture Approach"**. The core of the approach is a security management architecture based on the AUTOSAR approach. The architecture includes rules for protecting car-internal communication entities, further management databases for own certificates and security session status and common APIs for cryptographic functions and external functions. In the EASIS validator, the basic concepts of the architecture have been presented, for example rule-based access for internal and external communication, standard mechanisms for the cryptographic protection of communication. Further information can be accessed via www.easis.org.

Security Whitepaper

The security whitepaper shall mainly describe legal aspects, business requirements, design guidelines and the environment for a security solution in vehicular communications. A group of contributors to a security whitepaper has been established.

Next Workshop

The next open workshop for C2C CC security shall take place some time in February / March, possibly co-located with a workshop on privacy in Brussels.

Workshop Material

Workshop material will be made available publicly through the C2C CC website www.car-2-car.org.