Network on Wheels (NoW)

Security Architecture

Implementing the Security Architecture - a Network Perspective

---

Matthias Gerlach (FhI FOKUS)
gerlach@fokus.fraunhofer.de

Andreas Festag (NEC)
festag@netlab.nec.de

1st C2C CC Security Workshop, Berlin

Threats Overview

- Major threat classes:
  - Privacy violations
    - Track node
    - Identify user
    - Recognize user
  - Denial of service
    - Disrupt communication
    - Disable sensors
    - Disable processing
    - Disable transceiver
  - Insertion of false data
    - Spoof sensor data
    - Manipulate vehicle bus
    - Fake node (Sybil Attack)
    - Replay node

- Protection:
  - Preventive measures, e.g. PKI, closed system
  - Reactive measures, e.g. plausibility checks, intrusion detection, and revocation
  - Pseudonymity
- Security Toolbox
  - Cryptography
  - Non-cryptographic means, reasoning, ...
  - Tamper resistant hardware, ...
  - etc.

Specifying a Security Architecture

- **Problem**
  - An architecture comprises many different aspects
  - We have different stakeholders
  - Many people look at architecture differently
- **Stakeholders**
  - Application developers
  - Communication system developers
  - Security system developers
  - Researchers

- **Requirements for the NoW security architecture**
  - Integration into existing system architecture
  - Support for basic applications
  - Modularity, upgradeability
  - Ease of use for application developers
  - Algorithm-independent for
    - Expandability
    - Integration of different solution algorithms by different partners

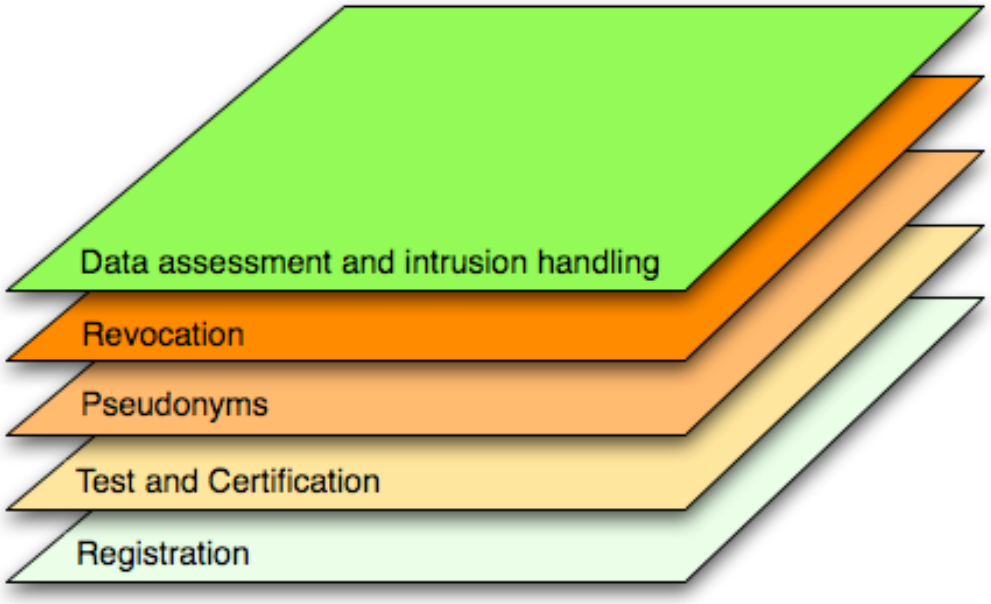
How Do We Specify It?

Solution: We propose different views

- **Functional layers view:** what different functionalities are necessary. Components of the security system
- **Organizational view**: which organizations / entities are necessary, e.g. Certification Authorities
- **Reference model view**: communication centric view, we extend the C2C CC reference architecture
- **Information centric view**: how is security information provided and processed in the local node (e.g. vehicle)

Architecture - Functional Layers

- Every layer relies on the functionality of the underlying one(s)
- Each layer has its own challenges
- Layers may span infrastructure and the local node‘s system



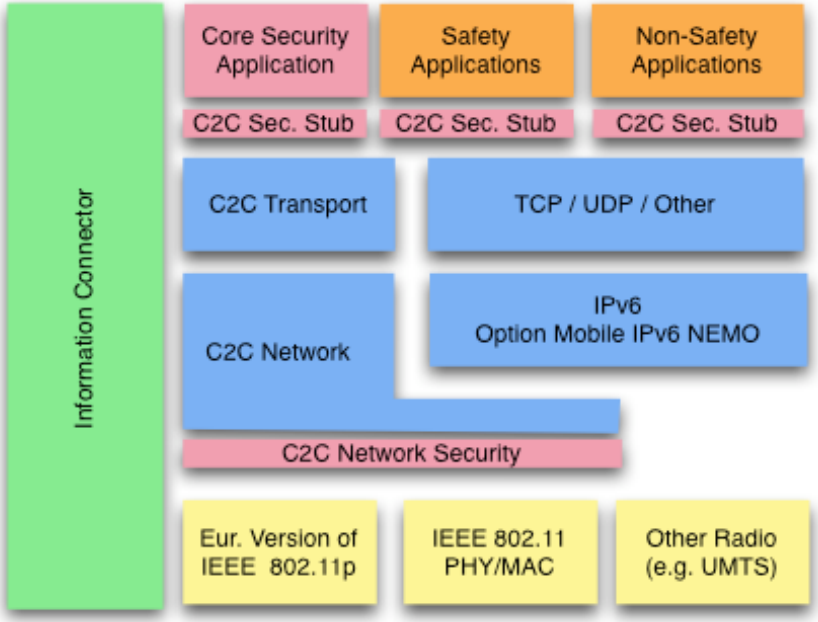
- These layers comprise the functionality of a security system

Architecture - Entities

- **RegistrationEntity**
  - Registers the node with appropriate authorities
  - Yields the acquirer name to node mapping
- **CertificationEntity**
  - Certifies that a node is valid and well-functioning (conform to protocols)
  - Yields network-certified nodes
- **PseudonymEntity**
  - Provides valid pseudonyms
  - Basis for anonymous communication
- **RevocationEntity**
  - Revoke malicious nodes
  - Has the authority to escrow pseudonyms to the identifier of the node (anonymity escrow)
- **Node** - an OBU or RSU
  - Interfaces to registration, pseudonym, revocation
  - Uses valid pseudonyms for communication
  - Local components to assess data

Architecture - Reference Model View

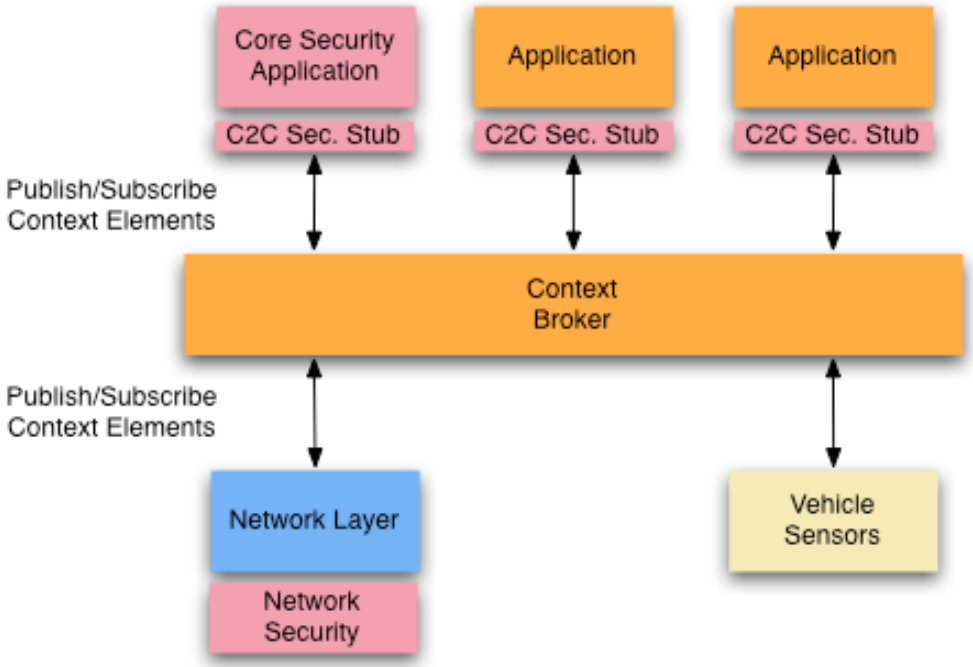
- Based on C2C CC Architecture
- Focus on applications that use vehicular specific data
- There may be also application specific security solutions



- **Core Security Application**:
  - Location privacy protection, confidence tagging, pseudonym assignment
- **C2C Security Stub**:
  - Trust evaluation and filtering based on confidence tags
- **C2C Network Security**:
  - End-to-end and hop-by-hop securing of data, tagging of neighborhood table

Architecture - Information Centric View

- Local information flow
- Open issue: how information is organized / addressed on the local node



- Applications use and provide ContextElements
- Context Broker provides publish/ subscribe access and organizes access to information
- Core security application
  - Amends ContextElements with a confidence value (*"Tag"*)
  - Uses context information to protect the privacy of users (context aware changing of pseudonyms - "Context mix")
- Security stub can be configured by application
  - Allow different security levels

Summary of Main Ideas

- **Context Broker**
  - Applications can access data (e.g. neighborhood table) using a standardized interface
- **Confidence Tags** and **Security Stubs**
  - Confidence: (a value in the range between 0..1 expressing the confidence in a piece of information)
  - Confidence can be built upon **certificates** (propose to use the WAVE / 1609.2 certificate structure) **and plausibility checks**
  - Security stub implements the reasoning / thresholds for filtering information.
- The **Core Security Application** (and possible extensions):
  - Assess confidence in the correctness of the data and „tag“ it. Support different algorithms in parallel
  - Communication system also provides tags (such as the network layer)
  - Pseudonym refresh and change algorithms

Network on Wheels (NoW)

Security Architecture

Implementing the Security Architecture - a Network Perspective

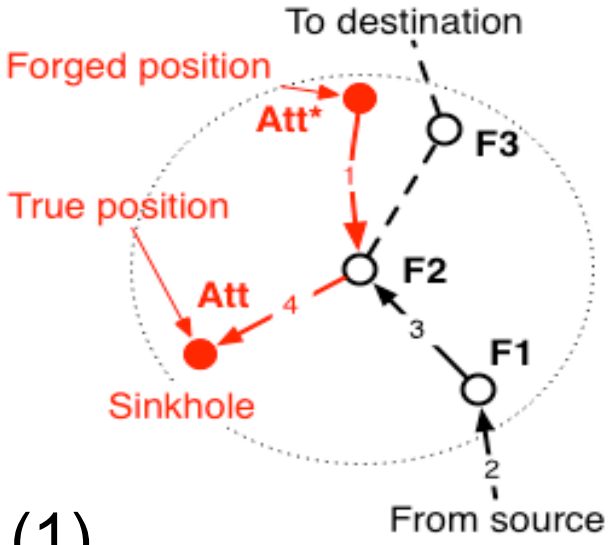
---

Matthias Gerlach (FhI FOKUS)
gerlach@fokus.fraunhofer.de

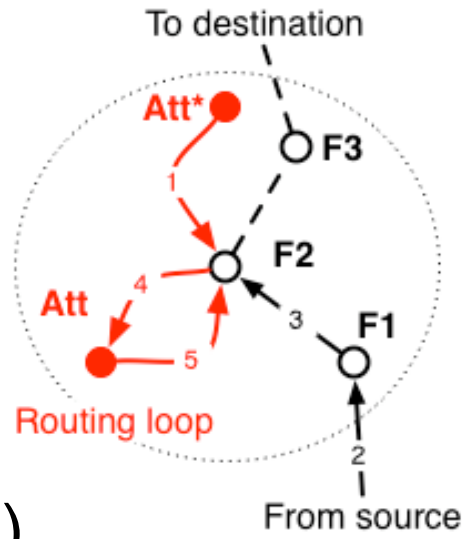
Andreas Festag (NEC)
festag@netlab.nec.de

Specific Attacks on Communication System

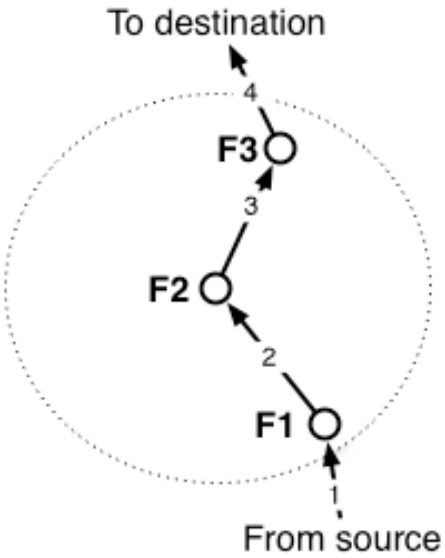
- Use of geographic positions for information dissemination
- Security: two exemplary attacks (see below)
  - (1) Sinkhole, (2) routing loop
  - Without security an attacker can easily disrupt communication
- Privacy: example attacks
  - Use beacon information to trace node
  - Use frequent location queries to track node
- What's the tradeoff between security (identifier stability) and privacy (pseudonymity)?



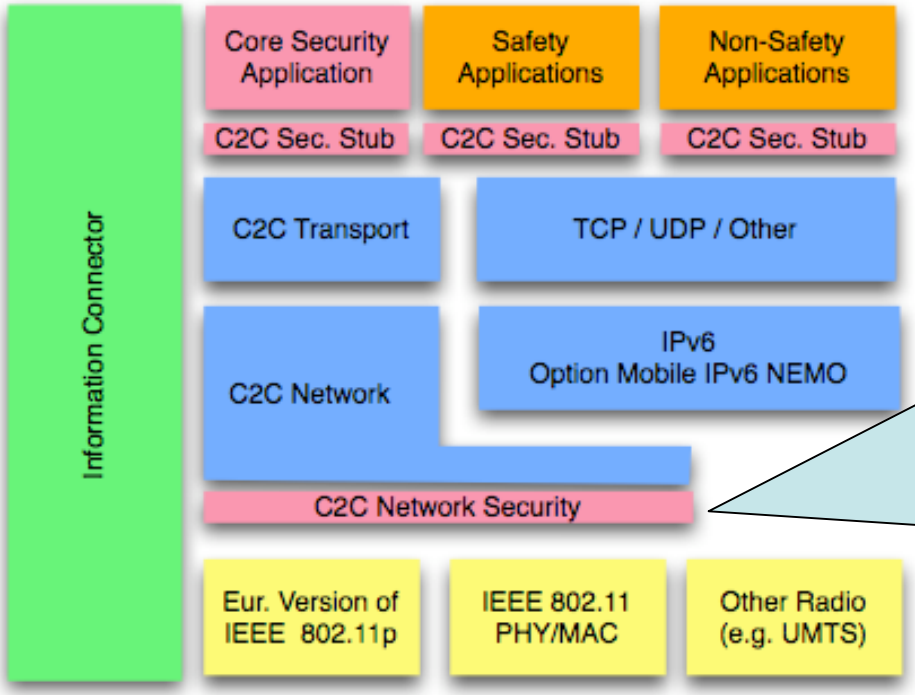
(1)



(2)



Network Security Mechanisms

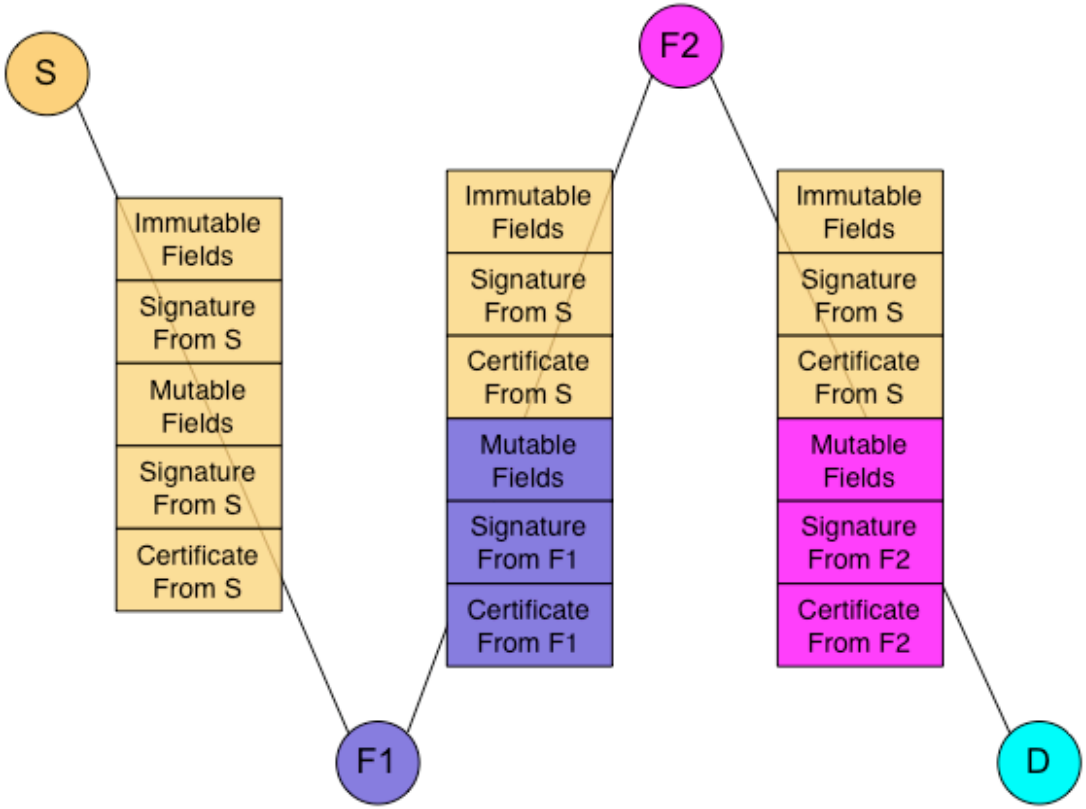


Main mechanisms
C2C network security

- Digital signatures and certificates
- Mutable and immutable fields protection
- Pseudonyms
- Plausibility checks
- Local reputation

Digital Signatures and Certificates

Secure geographical routing



Packets are signed

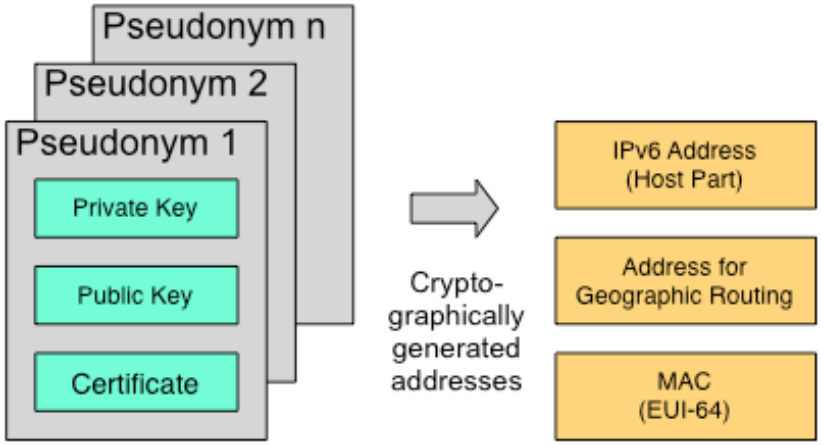
- Immutable fields by sender S
- Mutable fields by current forwarder

Advantages:

- Forwarding only by certified nodes
- Authentication of source and forwarders
- Integrity of data messages
- Non-repudiation

Pseudonyms

- Pseudonymity
  - Randomly chosen and changing identifiers
  - Aggravates tracking of nodes
  - Pseudonyms are certified



Setting of pseudonyms is controlled by *Core Security Application*

- Features
  - Multi-layer addressing
  - Enhanced packet forwarding scheme to minimize affect on routing
  - Pseudonym resolution service
  - Performance issues
- Pseudonym Change
  - Based on simple time interval
  - Alternative: based on context information to increase anonymity (*Context mix*)

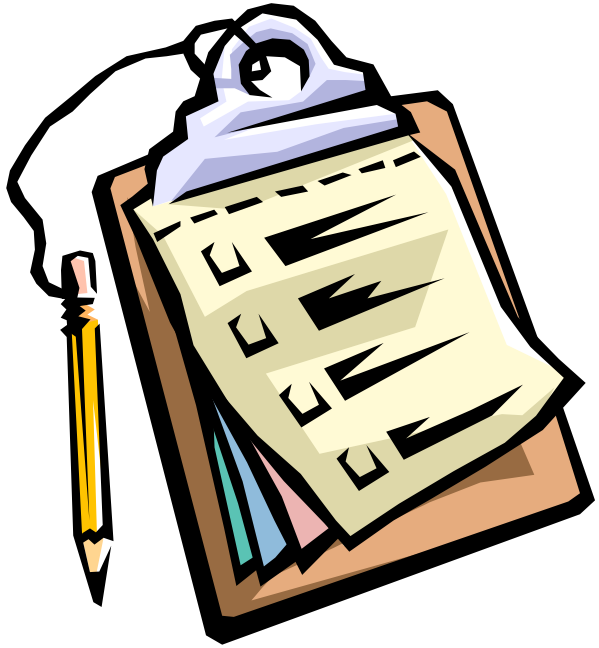
Plausibility Checks and Local Reputation

- Two main methods for plausibility checks
  1. Received information is trustable if more than one node distributes similar information ➔ on application layer
  2. Heuristics to check values (position, speed, heading)

     ➔ Can be applied in communication system (Core security application may implement additional checks)
- Local reputation system
  - Network layer maintains confidence value per nodes in local data structure
  - Can be accessed by applications through information connector
  - For received information confidence is determined based on trust value and plausibility checks
  - Network layer tags message with confidence value and passes it to application domain (security stubs)

Summary

- Proposed approach for network security attempts to combine security and privacy at reasonable costs and security compromises
- Main elements are currently implemented in demonstrator of project *NoW - Network on Wheels* as proof-of-concept and experimental platform



Proposals

- **Architecture description - Views:** Functional layers, organizational, ...
- **Main ideas:** Core security app, confidence tags, security stubs, and context mix
- **Mechanisms for network security:** Digital signatures and certificates, mutable and immutable fields protection, pseudonym support, plausibility checks, local reputation