Secure Vehicle Communication

Threats and Security Requirements for VANETs

Frank Kargl
frank.kargl@uni-ulm.de

Institute of Media Informatics
Ulm University

C2C-CC Sec. Workshop – 16.11.2006

Problem

- SEVECOM WP1:
  - Identification of threats against the communication system, transferred data, and the vehicle itself
  - Identification of necessary security requirements
- But
  - How to analyze security of a not well standardized and not perfectly well understood application domain?
    - How to analyze threats and attacks if protocols are not specified yet?
    - How to find out, what security mechanisms are necessary?

Simple Use Cases Approach

SEVECOM

- Selection based only on intuition/experience
  - Might miss important scenarios/aspects
  - Might have multiple use cases that are too similar to be relevant
- Open questions
  - On what detail level should a use case describe a scenario?
    - Application
    - Protocol
    - Attacks
    - Countermeasures
- Idea: choose an approach where the creation and selection of use cases is embedded into a structured process

Problems with existing approaches

SEVECOM

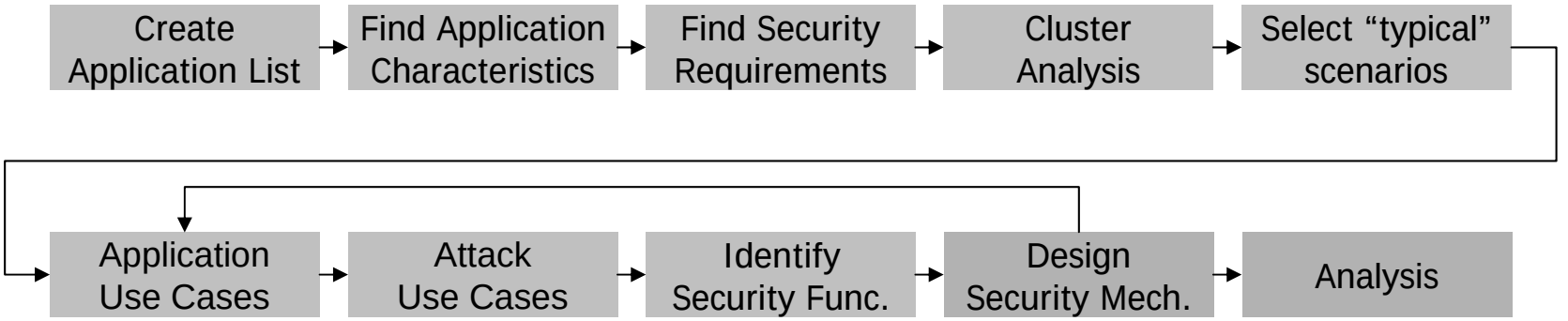
- Typical approaches (CC, CMU Octave, …) need a solid understanding of the system to be analyzed

  ➔ First need to analyze the properties of the applications in question, before we are able to address security requirements and threats

- Too many potential applications (> 50) to analyze them all in details

  ➔ Need to select representative applications for detailed analysis

SEVECOM Req. Eng. Process



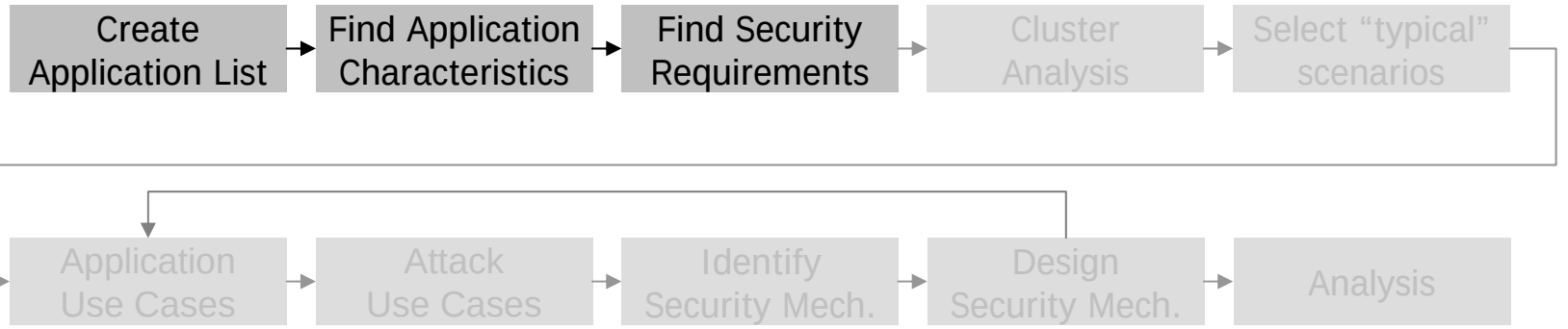
1. Create Application List
2. App. Characteristics
- Security Requirements
- Cluster Analysis
- Select Scenarios
6. Application Use Cases
7. Attack Use Cases
8. Identify Sec. Functions
9. Design Sec. Mech.
10. Analysis

Applications

SEVECOM

- Collected a list of >50 different VC applications
  - Safety-/Non-Safety Applications
  - Different categories like
    - Authority assistance
    - Traffic assistance
    - Accident assistance
    - …
- General Application Characteristics, e.g.
  - Safety Application
  - C2C vs. C2I
  - Addressing (Unicast, Broadcast, Geocast)
  - Single-Hop vs. Multi-Hop
- Made an “educated guess” on what the applications will look like

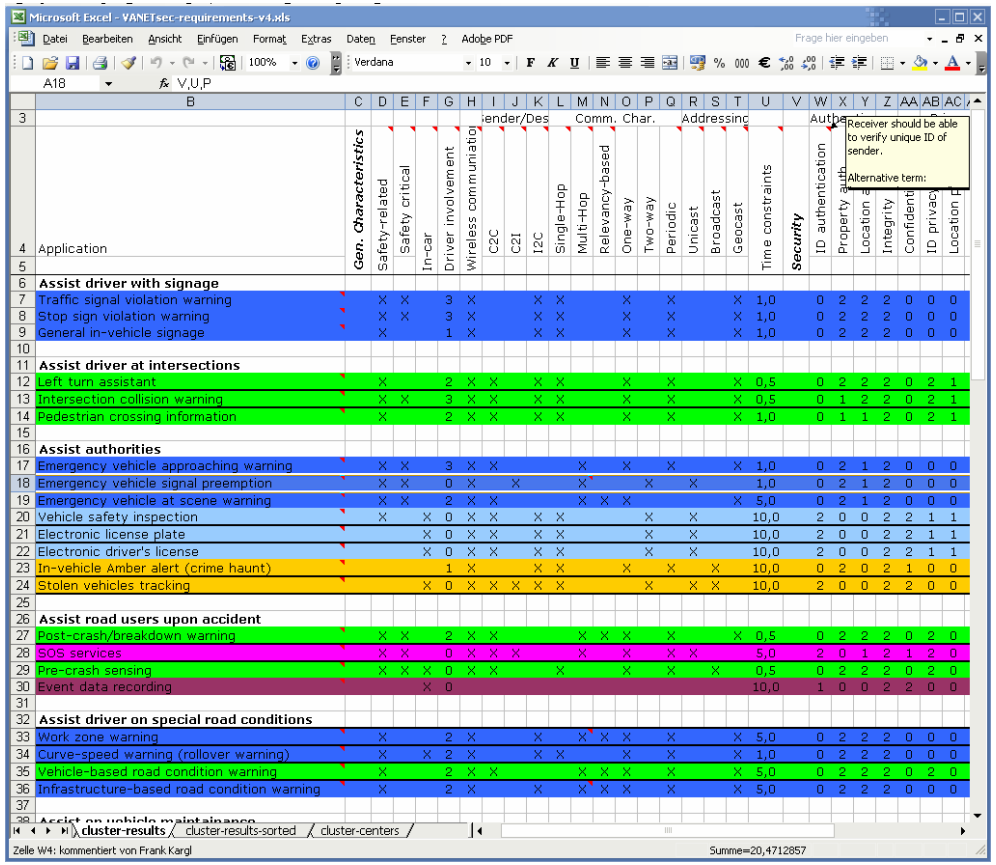
Step 3: Security Requirements



- Authentication
  - Entity authentication
  - Geoauthentication (authenticate location of node)
  - Attribute Authentication (e.g. IS_CAR property)
- No Authorization
  - Implicit step after Authentication
- Integrity
- Confidentiality
- Privacy
  - ID privacy
  - Location privacy
  - … with governmental access
- Non-repudiation / Liability issues
- Availability
- Access-Control
- Auditability

Selection of Application

- Identified 8 different clusters with relatively homogenous characteristics using statistical cluster-analysis



Selection of Application

- Identified 8 different clusters with relatively homogenous characteristics using statistical cluster-analysis
- Selected 10 different applications as representatives for clusters
  - SOS Services
  - Stolen Vehicles Tracking
  - Map Download/update
  - Intersection Collision Warning
  - Vehicle-based Road Condition Warning
  - Electronic License Plate
  - Road Surface Conditions to Traffic Operation Centre
  - Software Update/Flashing
  - Emergency Vehicle Signal Preemption
  - Work Zone Warning
- Analysis showed that these match the C2C-CC application list very well

Application Use Cases

Application use case

Use Case	Vehicle-based road condition warning
Creator	Frank Kargl, UULM
Goal in Context	Vehicles that detect hazardous road conditions send warnings to other approaching vehicles, so that their drivers can adapt their behaviour accordingly.
Scope & Level	Application use case
Preconditions	None
Success End Condition	Drivers receive warnings before reaching hazardous road segments
Failed End Condition	System fails to warn drivers
Involved components (Any logical components, both hardware and software that are involved in application implementation)	Sensors for detection of hazardous road conditions, e.g. - ABS, ASR, or ESP/VSC sensors can detect slippery or icy roads - rain sensors that are used for starting the wipers can detect wet roads On-board processing and wireless communication units
Trigger	Sensors detecting potential hazardous road conditions
Operation description (Complete textual description of application operation)	Sensors constantly monitor road conditions and create a risk-estimation for multiple classes of hazards (e.g. slippery road, wet road, strong wind, …). When at least one of these parameters exceeds a given threshold, the car starts emitting geocast messages that are sent to all nearby road segments which lead to this position. The messages contain the risk-estimations for all hazard-classes. Vehicles receiving such a message will forward the message according to the general geocast-/relevancy-based-forwarding strategy. Vehicles receiving such a message will additionally issue a optical/acoustical warning to the driver. Options: - The warning might be modulated according to the estimated strength of the hazard contained in the message. - Vehicles may apply consistency checks with own sensors or messages received from other cards to detect false-alarms.

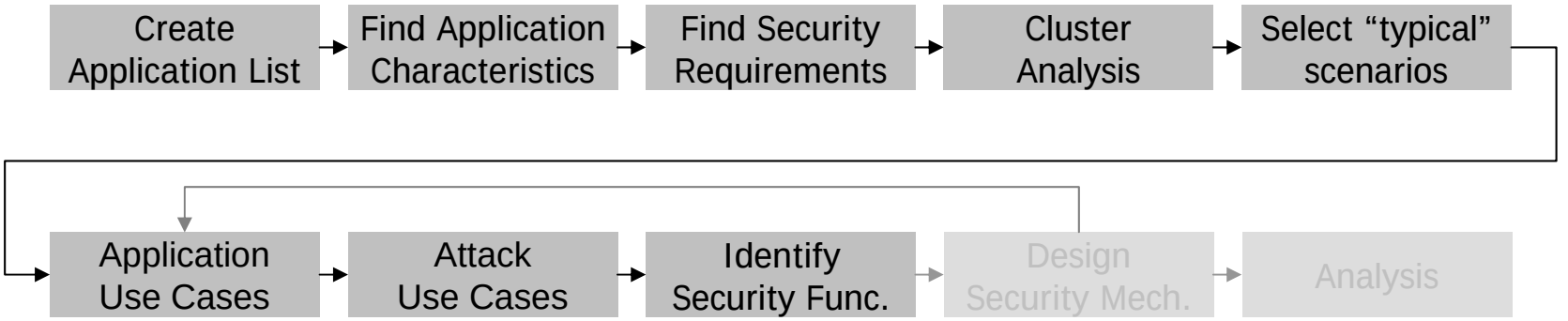
		No relation		Safety relevant	X	Safety critical			
		C2C	X	C2I		I2C			
ne-way	X	Two-way		Single-Hop		Multi-Hop	X		
Unicast		Broadcast		Geocast	X	Relevancy	X		
		Timing constraints	5s	Periodic messages			X		

ID privacy	2
Location privacy	0
Jurisdict. Access	1
Availability	1
Access control	0
Auditability	0

Attack Use Cases

Use Case	Forging of Warning Messages											
Related appl. use case	Vehicle-based road condition warning											
Creator	Frank Kargl, UULM											
Primary Attack Goal	DoS	X	Inform. Theft		Intrusion		Tampering	
Used Techniques	Masquer.		Eavesdrop.		Auth. Violation		Loss/Modific.	
	Repudiat.		Forgery	X	Sabotage			
Goal in Context (Textual description of attackers goal/motivation)	Issue false warnings so that drivers get irritated and may go slower than necessary. Due to hard breaking, rear-end collisions may occur.							
Attacked components (Any logical components, either hardware, software, or user, that are targeted by this attack)	Wireless communication							
Pre-requirements for attack	Wireless communication equipment, capable of creating and sending forged messages							
Attack description (Complete textual description of attack operation)	Attacker places itself near the target area and emits forged messages warning e.g. because of slippery or icy road conditions. The destination area for the geocast may be selected based on topographic features or simply set to a maximum area so that as many cars as possible will be affected. Messages will be automatically distributed in the destination region and drivers will receive warning messages, to whom they are supposed to react accordingly.							
Attack success factors (Reasons why attack may succeed)	Drivers will recognize the warning and slow down.							
Attack failure factors (Reasons why attack may fail)	If there are no cars in the one-hop neighbourhood to distribute the messages, the attack fails. Drivers might simply ignore the warnings.							
Effects of attack (regarding driver and road traffic)	The attack will cause the drivers to slow down, causing traffic jams or in worst case rear-end collisions.							
Severity	low	X	medium		high		fatal	

Security Functions



- Find a list of 23 (abstract) security functions that are suited to address the found attacks

Security Functions

SEVECOM

- Identification & Authentication Concepts
  - ***Identification***
  - ***Authentication of sender***
  - ***Authentication of receiver***
  - Attribute authentication
  - Authentication of intermediate nodes
- Privacy Concepts
  - ***Resolvable anonymity***
  - ***Total anonymity***
  - Location obfuscation

Security Functions

SEVECOM

- Integrity Concepts
  - ***Integrity protection***
  - ***Encryption***
  - Detection of protocol violation
  - Consistency/context checking
  - Attestation of sensor data
  - Location verification
  - Tamper-resistant communication system
  - DRM
  - Replay protection
  - Jamming protection

Security Functions

SEVECOM

- Access Control/Authorization Concepts
  - Access control
  - Closed user groups
  - Firewall/Checkpoint
  - Sandbox
  - Filtering (e.g. at intermediate nodes)

Ongoing and Future Work

SEVECOM

- Ongoing work
  - Select/design suitable mechamisms like
    - Authentication protocols
    - CAs/TTPs for VANETs
    - Revocation mechanisms
    - Privacy mechanisms
    - …
  - Do not engineer one solution per scenario
  - Modular architecture (see second talk)

Security Baseline

SEVECOM

- Problems
  - Will fancy academic mechanisms be accepted by industry?
  - Will every of our assumptions be fulfilled by real-world system?
- Probably NOT!
- SEVECOM answer
  - Identify a baseline system based on established security concepts as a “recommended minimum”
  - Additionally, advanced mechanisms will augment the baseline system
  - Design a modular system where components can deliver (reduced) security also when some assumptions are not fulfilled (e.g. no PKI)

Conclusion

- Structured process that allows to
  - analyze characteristics of applications in a not completely specified domain
  - select representative applications to focus on details
  - find attacks and countermeasures
- By that process, SEVECOM has analyzed 55 different applications, selected 10 representative applications, modeled 22 different attacks and identified 23 required security mechanisms for Secure Vehicle Communication
- Find full details in SEVECOM Deliverable 1.1
- Baseline system and modular approach copes with real-world problems