Secure Vehicle Communication

Proposal for a SEVECOM SW Architecture

Frank Kargl
frank.kargl@uni-ulm.de

Institute of Media Informatics
Ulm University

C2C-CC Sec. Workshop – 16.11.2006

Security Mechanisms/Concepts

- Identified ~20 different security mechanisms/concepts needed to conquer the described attacks
- How to implement?

Identification & Authentication Concepts
Identification
Authentication of sender
… and sender is
Authentication of receiver
Property authentication
Authentication of intermediate nodes
Privacy Concepts
Resolvable anonymity
Total anonymity
Location obfuscation
Integrity Concepts
Encryption
Integrity protection
Detection of protocol violation
Jamming protection
Tamper-resistant comm. system
DRM
Replay protection
Consistency/context checking
Attestation of sensor data
Location verification
Access Control/Authorization Concepts
Access control
Firewall/Checkpoint
Closed user groups
Filtering (e.g at intermediate nodes)
Sandbox

Not all modules are active all the time

	SOS services			Stolen vehicle tracking			Map download		Intersection collision avoidance				Vehicle-based road condition warning				El. license plate		Road surface cond. to TOC			Software update/flashing				EV signal preemption		Workzone warning			
	1.1	1.2	1.3	2.1	2.2	2.3	3.1	3.2	4.1	4.2	4.3 (na	4.4	5.1	5.2	5.3	5.4	6.1	6.2	7.1	7.2	7.3	8.1	8.2	8.3	8.4	9.1	9.2	10.1	10.2	10.3	10.4
	Forging of SOS message	Eavesdropping of SOS messages	Blocking SOS messages	Denial of service	Masquerade as other vehicle	Masquerade as authority	Unauthorized access	Manipulation of map content	Attention splitter	Collision warning relay	Confuse navigation data	Forge RSU warning messages	Forging of warning messages	Suppression of warning messages	Eavesdropping and tracking	Impersonation of other cars	Impersonation of infrastructure node	Impersonation of vehicle or forging ELP	Denial of service 1	Denial of service 2	Tracking	Manipulation of data	Injection of malicious software	Eavesdropping	Unauthorized access / impersonation	Impersonate emergency vehicle	Manipulation of EV messages	Forging of messages	Suppression of messages	Manipulation of traffic sign location	Manipulation of message content
Identification & Authentication Concepts																															
Identification	o				o		o						o					o													
Authentication of sender	++		o		+	++	++	++				++	o			++	++	++	++			++	+		o	++	++	+			
… and sender is					stolen vehicle		vehicle	server									infra-structure	vehicle	vehicle			OEM	OEM/ Svc prov			EV	EV	RSU			
Authentication of receiver		+	o																			+	+		+						
Property authentication	+											+	++			+			+	+						++	++	+			
Authentication of intermediate nodes		o																	o												
Privacy Concepts																															
Resolvable anonymity	++												o						+												
Total anonymity	-														++						++										
Location obfuscation																					o										
Integrity Concepts																															
Encryption		++						+							+						+			+		o					
Integrity protection								++														+	+				++				++
Detection of protocol violation			++											++															++		
Jamming protection			++											++															++		
Tamper-resistant comm. system				++	++								+				++	+												+	
DRM								++																++	++						
Replay protection										++		+						+	+	+											
Consistency/context checking	+												++						+	+							o	+		+	+
Attestation of sensor data	+												+						+	o											
Location verification																			o											++	+
Access Control/Authorization Concepts																															
Access control																									++						
Firewall/Checkpoint																							++								
Closed user groups																			++												
Filtering (e.g at intermediate nodes)																				++											
Sandbox																							+								

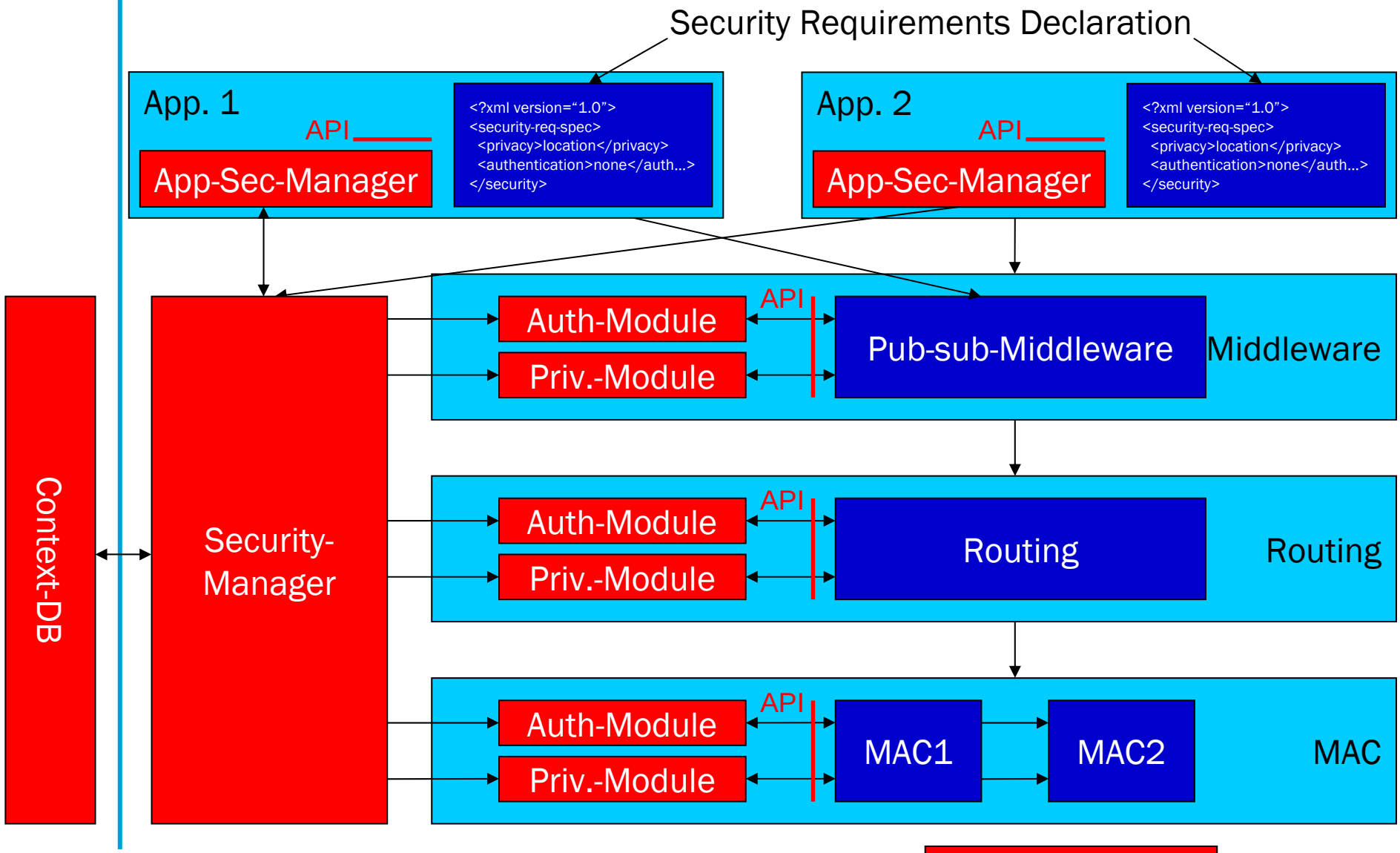
Problems

- Only a subset of modules will be active in parallel
- Some modules influence each other
  - E.g. Authentication vs. Anonymity
- Modules are located on different layers
  - E.g. Anonymity requires changed IDs on MAC-, IP-, application-layer
- Important functions may not be available at all
  - e.g. PKI
- Will the security system need to be changed, when new applications are installed?

➔ Solution: Security architecture which is

- Modular
- Extensible
- Dynamically configurable at runtime
- Security should degrade slowly when components are not present

SW Architecture Proposal



Security Requirements Specification

- Syntax could be
  - XML-based
  - Resource Description Framework / RDF
    - Similar e.g. to CC/PP
- Example

```
<?xml version="1.0"?>
 <rdf:RDF xmlns:rdf="..." xmlns:sv="http://www.sevecom.org/schema#">
  <rdf:Description rdf:about="http://www.c2c-cc.org/vehicle-based_road_cond_warning">
   <rdf:type rdf:resource="esafetyApplication"/>
    <sv:requires>
     <sv:SecurityRequirement module="PropertyAuthentication">
      <sv:nodeType>Vehicle</sv:nodeType>
     </sv:SecurityRequirement>
    </requires>
    <requires>
     <sv:SecurityRequirement module="Privacy">
      <sv:idPrivacy changeInterval="5s"/>
     </sv:SecurityRequirement>
    </sv:requires>
  </rdf:Description>
</rdf:RDF>
```

Priorities

- If two applications have contradicting requirements?
  - Ruleset determines which requirement takes priority

```
<?xml version="1.0"?>
 <rdf:RDF xmlns:rdf="..." xmlns:sv="http://www.sevecom.org/schema#">
  <rdf:Description rdf:about="http://www.c2c-cc.org/defaultPriorities">
   <rdf:type rdf:resource="PriorityRules"/>
    <sv:priority rdf:resource="eSafetyApplication" priority="10" />
    <sv:priority rdf:resource="maintenanceApplication" priority="4" />
    <sv:priority rdf:resource="entertainementApplication" priority="1" />
</rdf:RDF>
```

  - Applications can be informed via callbacks, if their security requirements are not met and then decide to proceed or stop operation

Application Callbacks

- Security modules can inform applications
  - about results of security operations
    - e.g. transmit user ID after authentication
  - about problems with security operations
    - e.g. when privacy requirements can not be met, because of contradicting requirements in other applications

```
<?xml version="1.0"?>
 <rdf:RDF xmlns:rdf="..." xmlns:sv="http://www.sevecom.org/schema#">
  <rdf:Description rdf:about="http://www.c2c-cc.org/vehicle-based_road_cond_warning">
   <rdf:type rdf:resource="esafetyApplication"/>
    <sv:requires>
     <sv:SecurityRequirement module="IdentityAuthentication">
      <sv:InformApplication method="org.sevecom.VehBasRoadCondWarning.authenticated"/>
      …
     </sv:SecurityRequirement>
</sv:requires>
  </rdf:Description>
</rdf:RDF>

package org.sevecom;
public class VehBasRoadCondWarning {
    public void authenticated(Credentials identity) { … }
}
```

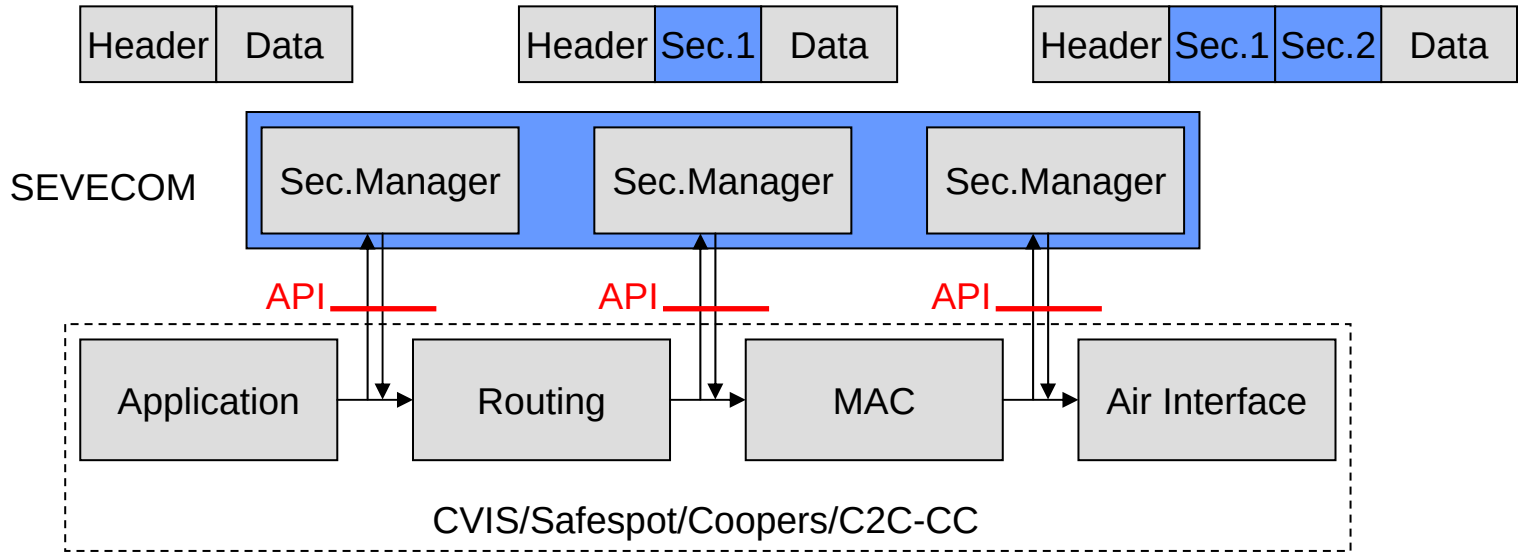
Opportunities

SEVECOM

- Dynamic security and privacy configuration allows
  - Extend security / privacy configuration during operation, e.g. when new applications get installed
  - Personal security and privacy profiles
    - User empowerment
    - How to create / edit? Security User Interface
  - Adapt security / privacy to national regulations
    - Even during use, e.g. when crossing borders
  - …

Integration

- How to combine security modules and other functionality?
  - Communication infrastructure allows registration of callbacks at specified hooks, security modules can analyze, modify, and even drop packets at defined hooks
  - Security headers can be attached
  - Similar to Linux netfilter architecture



Open Questions

- Very communication centric view
  - Captures PDU between layers
  - Interaction between application and security modules only at pre-defined hooks
- Can such a mechanism be integrated into the C2C-CC architecture?
- We (Ulm Univ.) have begun work on a proof-of-concept implementation