Secure Vehicle Communication

Security Requirements Engineering using Cluster Analysis

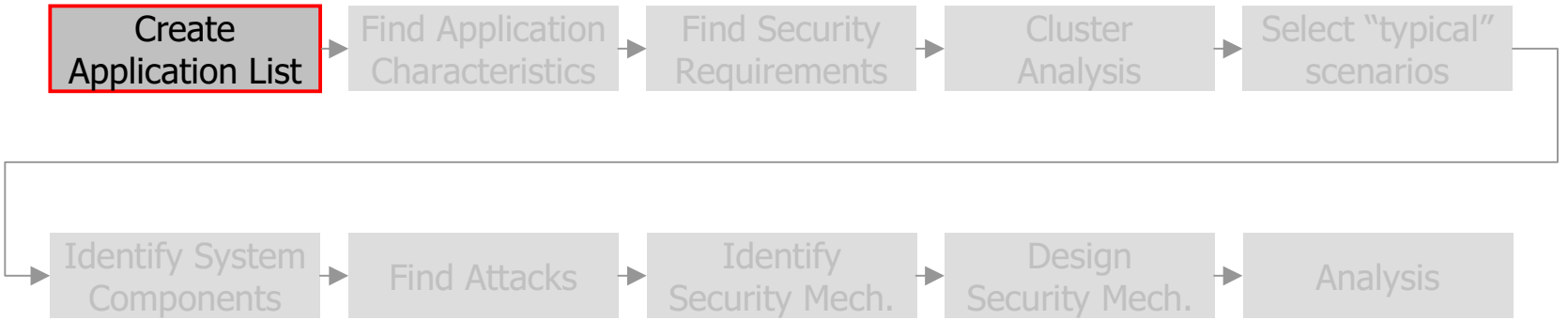
Frank Kargl
Ulm University
frank.kargl@uni-ulm.de

Our Problems with Use Cases

SEVECOM

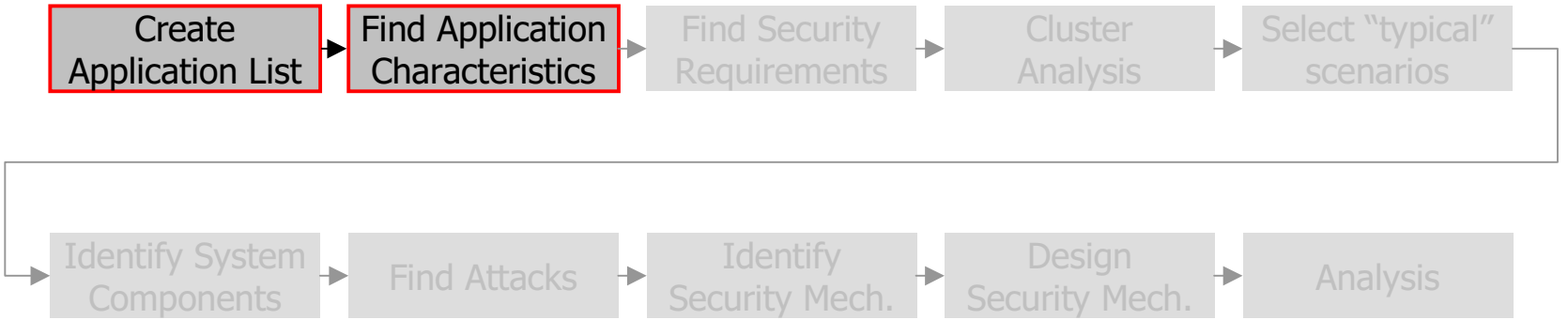
- Selection based only on intuition/experience
  - Might miss important scenarios/aspects
  - Might have multiple use cases that are too similar to be relevant
- Open questions
  - On what detail level should a use case describe a scenario?
    - Application
    - Protocol
    - Attacks
    - Countermeasures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

SEVECOM Approach



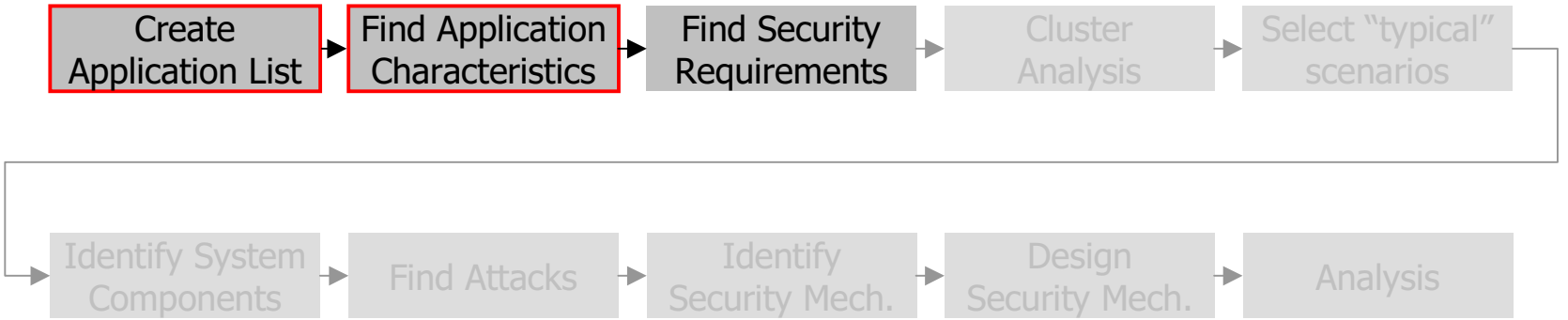
- Based on list from IEEE DSRC Tutorial
- Safety-/Non-Safety Applications
- Input/Validation from other projects

SEVECOM Approach



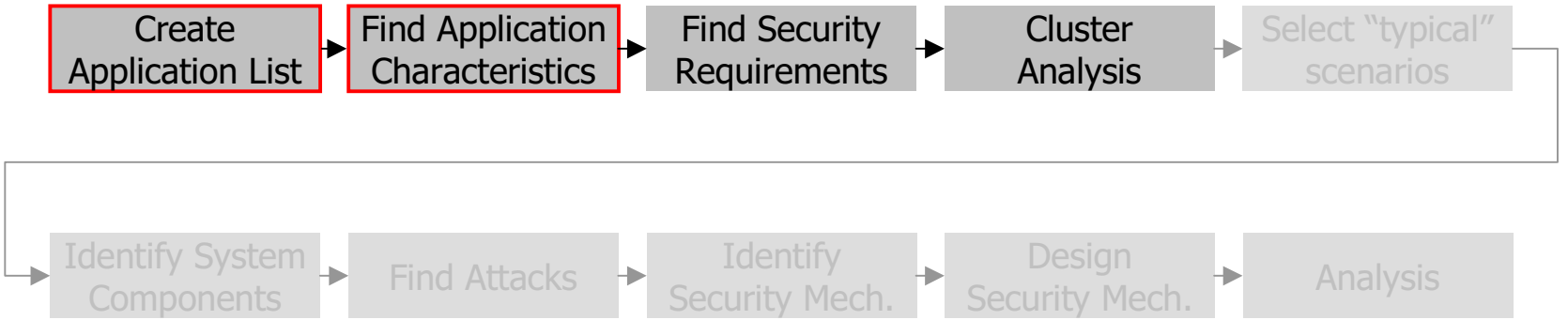
- Different Criterias
  - General Application Requirements
  - Network Requirements
  - More?
- Better understanding of the applications
- Input/Validation from other projects

SEVECOM Approach



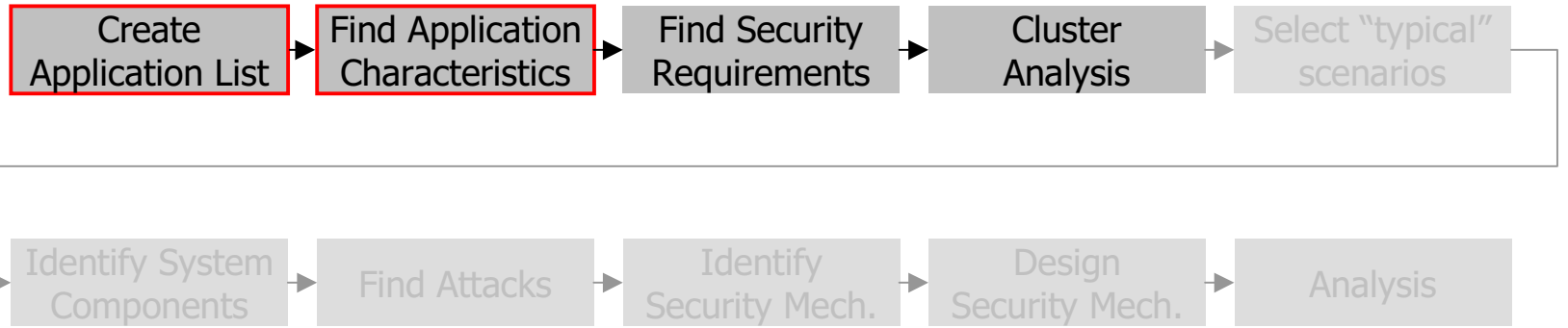
- Authentication
  - Identity authentication
  - Geoauthentication (authenticate location of node)
  - Property Authentication (e.g. IS_CAR property)
- Access-Control
- Integrity
- Confidentiality
- Privacy
  - ID privacy
  - Location privacy
  - … with governmental access
- Non-repudiation / Liability issues
- Availability

SEVECOM Approach



- Rating of characteristics/requirements according to importance for application
- Requirements taken as axis in n-dimensional coordinate space
- Importance values define coordinates of each application in coordinate space
- Goal: find clusters of applications which are located closely together in this coordinate space
- Use SPSS statistics software

SEVECOM Approach



K-means cluster analysis:

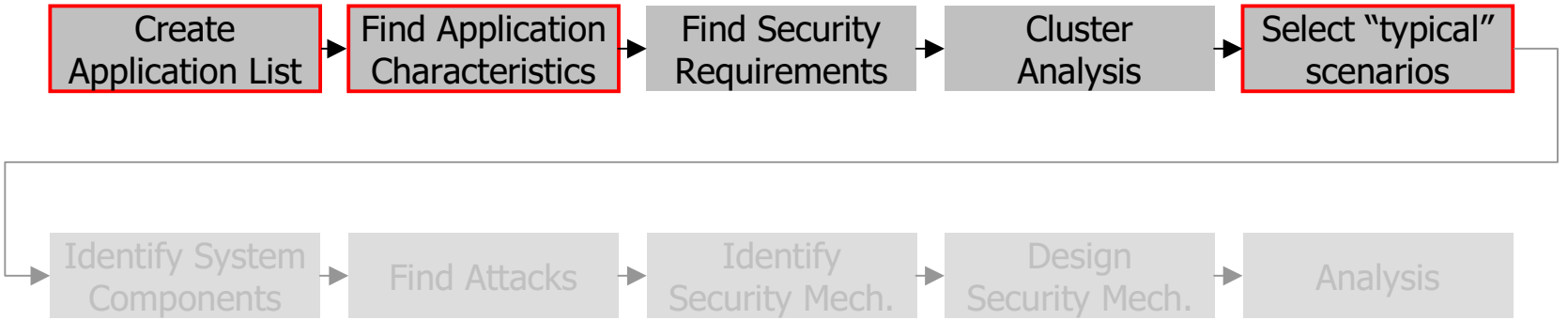
- This procedure attempts to **identify relatively homogeneous groups of cases** based on selected characteristics, using an algorithm that can handle large numbers of cases. However, the algorithm requires you to **specify the number of clusters**. […] You can select one of two methods for classifying cases, either **updating cluster centers iteratively** or classifying only. You can save **cluster membership**, **distance information**, and **final cluster centers**. […]

Cluster Analysis Results

SEVECOM

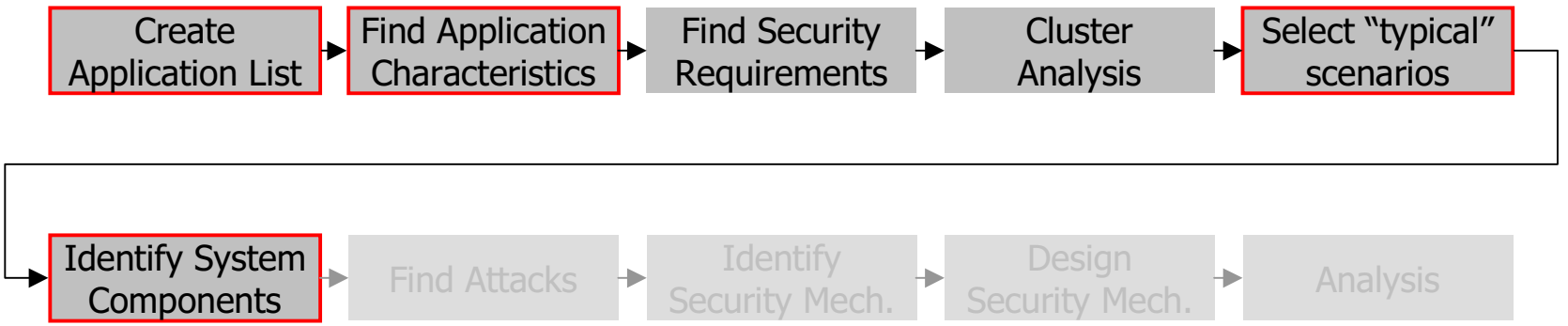
	authentication			privacy			QoS		Cluster 1:	Cluster 2:	Cluster 3:	Cluster 4:	Cluster 5:
	identity authentication	geoauthentication	property authentication	ID privacy	location privacy	with governmental access	delay critical	availability	2	0	0	2	0
									0,8	0	2	0	2
									0	2	2	0	2
									0	2	2	0	2
									0	1,25	0	0	0
									0	0,25	0	0	1,5
									1,27	1,25	1,82	0	2
									1,07	1,25	2	0	2
traffic signal violation warning	2	1	0	0	0	0	2	1	1,00	9,50	8,17	4,00	9,50
stop sign violation warning	2	1	0	0	0	0	2	1	1,00	9,50	8,17	4,00	9,50
left turn assistant	2	1	0	0	0	0	1	1	0,53	9,00	8,83	3,00	10,50
intersection collision warning	2	1	0	0	0	0	1	1	0,53	9,00	8,83	3,00	10,50
blind merge warning	2	1	0	0	0	0	1	2	1,40	9,50	7,83	4,00	9,50
pedestrian crossing information at designated intersecti	2	1	0	0	0	0	1	1	0,53	9,00	8,83	3,00	10,50
approaching emergency vehicle warning	2	0	0	0	0	0	1	2	2,00	8,50	8,83	3,00	10,50
emergency vehicle signal preemption	2	0	0	0	0	0	2	2	2,47	9,00	8,17	4,00	9,50
post-crash warning	2	0	0	0	0	0	1	2	2,00	8,50	8,83	3,00	10,50
road condition warning	2	0	0	0	0	0	0	0	3,13	10,00	11,83	0,00	13,50
SOS services	0	2	2	2	0	1	2	2	9,87	5,50	1,17	13,00	0,50
in-vehicle signage	2	1	0	0	0	0	1	1	0,53	9,00	8,83	3,00	10,50
curve speed warning	2	1	0	0	0	0	1	0	1,53	10,00	9,83	2,00	11,50
low parking structure/bridge warning	2	1	0	0	0	0	1	0	1,53	10,00	9,83	2,00	11,50
wrong way driver warning	0	2	2	2	0	2	2	2	10,87	6,50	2,17	14,00	0,50
work zone warning	2	1	0	0	0	0	1	1	0,53	9,00	8,83	3,00	10,50
in-vehicle amber alert	2	1	0	0	0	0	2	0	2,00	10,50	9,17	3,00	10,50
safety recall notice	2	0	0	0	0	0	0	0	3,13	10,00	11,83	0,00	13,50
just-in-time repair notification	2	0	0	0	0	0	0	0	3,13	10,00	11,83	0,00	13,50
cooperate forward collision warning	0	2	2	2	0	0	2	2	8,87	5,00	0,17	12,00	1,50
vehicle-based road condition warning	0	2	2	2	0	0	1	2	8,40	4,50	0,83	11,00	2,50
emergency eletronic brake lights	0	2	2	2	0	0	2	2	8,87	5,00	0,17	12,00	1,50
blind spot warning	0	2	2	2	0	0	2	2	8,87	5,00	0,17	12,00	1,50
highway merge assistant	0	2	2	2	0	0	2	2	8,87	5,00	0,17	12,00	1,50
visibility enhancer	0	0	2	2	2	0	1	1	9,13	1,50	5,83	10,00	7,50
cooperative collision warning	0	2	2	2	0	0	2	2	8,87	5,00	0,17	12,00	1,50
cooperative vehicle-highway automation system (platoo	0	0	2	2	1	0	1	1	8,13	1,00	4,83	9,00	6,50
cooperative adaptive cruise control	0	0	2	2	1	1	1	1	9,13	1,50	5,83	10,00	5,50
pre-crash sensing	0	0	2	2	1	0	2	2	9,47	2,00	3,17	11,00	4,50
highway/rail collision warning	2	1	0	0	0	0	1	1	0,53	9,00	8,83	3,00	10,50

SEVECOM Approach



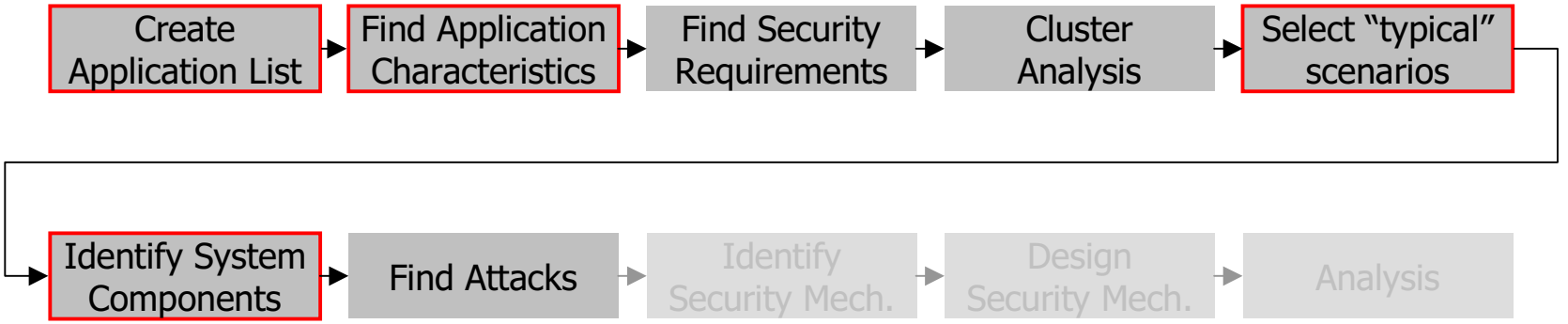
- Cluster 1
  - Inf2Car, Identity Authentication, partial Geoauthentication, no privacy, critical QoS
  - Example: Traffic Signal Violation Warning
- Cluster 2
  - Car2Car, property Authentication, ID & location privacy, critical QoS
  - Example: Cooperative vehicle-highway automation system (platoon)
- Cluster 3
  - Car2Car, property & GeoAuthentication, ID privacy, critical QoS
  - Example: Cooperative forward collision warning
- Cluster 4
  - Inf2Car, Identity Authentication, no privacy, uncritical QoS
  - Example: Safety recall notice
- Cluster 5
  - Car2Car, property & GeoAuthentication, ID privacy (with governm. access), critical QoS
  - Example: Wrong way driver warning

SEVECOM Approach



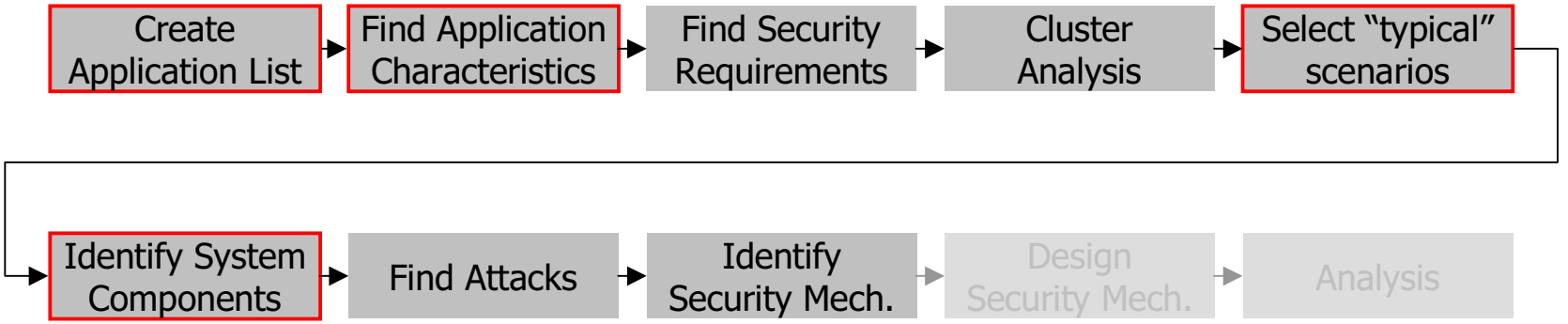
- Example: Traffic Signal Violation Warning
  - Senders with omni-directional antennas at intersections
  - Periodically send Geocast messages to road segments with yellow/red lights
- "Application-based Use Cases"
- Input/Prioritization/Validation from other projects

SEVECOM Approach



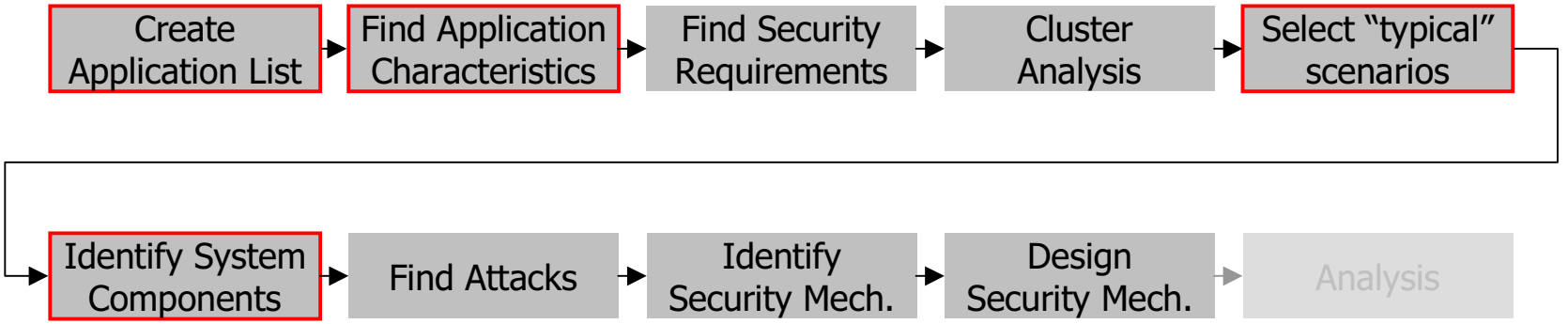
- Example: Traffic Signal Violation Warning
  - Use laptop with wireless device near intersections
  - Send bogus warning messages
  - Brings traffic to a halt
  - Replay of old messages or messages from other traffic lights
  - "Attack Use Case"

SEVECOM Approach



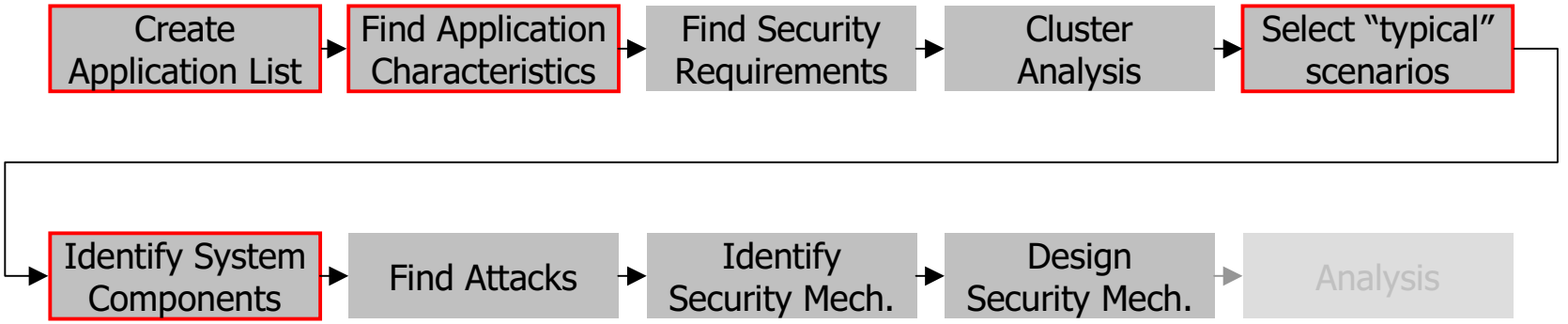
- Example: Traffic Signal Violation Warning
  - Need to validate that messages …
    - are actually from the traffic light at the given location (geoauthentication)
    - are actually from a traffic light (property authentication)
    - are fresh

SEVECOM Approach



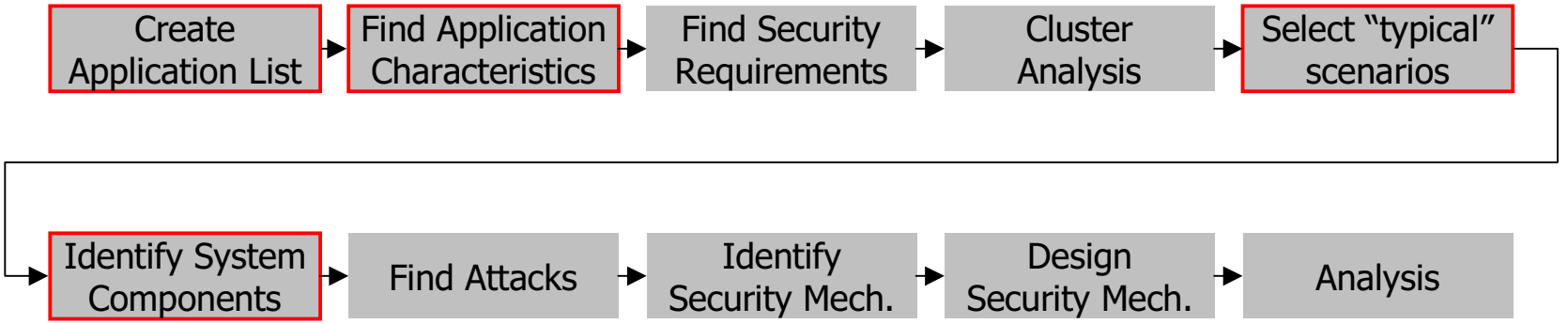
- Example: Traffic Signal Violation Warning
  - Need to authenticate that messages …
    - are actually from the traffic light at the given location
      ➔ geoauthentication protocol ?
    - are actually from a traffic light (property authentication)
      ➔ use some TTP
    - are fresh
      ➔ use signed timestamps

SEVECOM Approach



- Do not engineer one solution per scenario
- Find a modular/flexible architecture

SEVECOM Approach



- Try to find other attacks
- Use other evaluation mechanisms

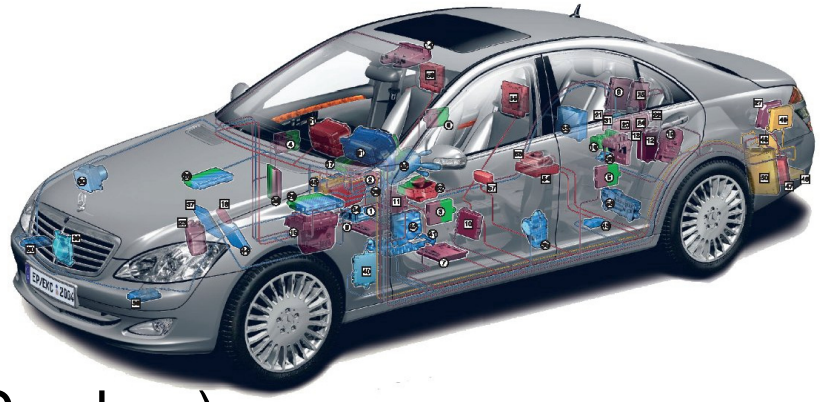
Remarks

SEVECOM

- Current analysis is
  - Focused on network/communication/in-vehicle protection
  - considers only similarity in security requirements
- Consider also application/network characteristics for cluster analysis
  - Work in progress
- Caution
  - One cluster per application?

Incar scenario

- Future car
  - Open system (GSM, UMTS, Bluetooth, ...)
  - Internal harddisk
  - additional interfaces (CD, DVD, USB, PC-Card, SD-Card, ...)
  - New software based and remote functions
  - Integration of consumer devices, DRM
- Increased risks by hackers, malware, ...
- Constraints
  - The car is no PC - the driver is not a sysadmin
  - Difficult to keep software and configuration up to date



Applications

SEVECOM

- Integration of mobile devices
  - Secure access on vehicle sensor data (Navi, Audio, Video, ...)
- Autonomous security management
  - In-vehicle account management
  - Well defined in-vehicle security status
  - Recovery of security status
- Safeguarding of in-vehicle processes
  - Secure download of user/entertainment data (virus protection)
  - Upgrade/flashing of in-vehicle entities
  - Security configuration management

Requirements

Non-Safety Applications	authentication					privacy				QoS			
	identity authentication	geoauthentication	property authentication	integrity	confidence	ID privacy	location privacy	with governmental access	non repudiation / liability	delay critical	availability	authorization	audit/log
in-vehicle protection													
Integration of mobile devices													
Secure access on vehicle sensor data (e.g., Navi, Audio, Video, …)	2		1	2					2			2	
Autonomous Security Management													
In-vehicle account management	2		1	2	1	2					1	2	
Defined in-vehicle security status				2						2	1		2
Recovery of security status				2									2
Safeguarding of in-vehicle processes													
Secure download of "user/entertainment" data (protection against v	2		1	2		2						1	
Upgrade/Flashing of in-vehicles entities	2	1	1	2	1				2			2	2
Security configuration management	2	1	1	2									2

Certification / Quality Assurance

SEVECOM

- Not addressed right now
- If needed: Guidelines provided externally

Input from other Projects

SEVECOM

- Agree on common application taxonomy
- Provide/check characteristics
- Agree on security requirements
- Prioritize the applications
- Provide/check system components

- Role of COMeSafety & C2C CC?