HAZOP-based Security Analysis for Embedded Systems

Graduation School of Information Science,
Nagoya University

Jingxuan Wei

Yutaka Matsubara, Hiroaki Takada

Copyright © 2016 著作権保有者名 All Rights Reserved.

Outline

- Research background & purpose
- Related works
- Proposal of a HAZOP-based security analysis method
- Demonstration and evaluation of the proposed method via a case study
- Discussion & Conclusion

Copyright © 2016 著作権保有者名 All Rights Reserved.

Research Background & Purpose

- Computerized automobile vehicle embedded with ECUs and general application of embedded system software
  - Bringing us all kinds of convenience
  - Generating new security concerns
- In order to prevent the theft and misuse of embedded systems
  - Comprehensively discover security threats and vulnerabilities as much as possible
  - Efficiently implement the countermeasures to eliminate vulnerabilities
  - Reduce risks in the design phase of embedded systems
- Develop a system that will assist/aid human to conduct a security analysis.

Related Works: Safety Analysis Techniques

- FMEA(Failure Mode and Effects Analysis)
- FTA(Fault Tree Analysis)
- HAZOP(Hazard and Operability Study)
  - Used in building chemical plants
  - Use guidewords to examine every variables of the plant, such as flow in a pipeline, temperature of a reactor, or time of a reaction
  - Deviations are to be found, if there are any safety flaws

Related Works: Security Analysis Techniques

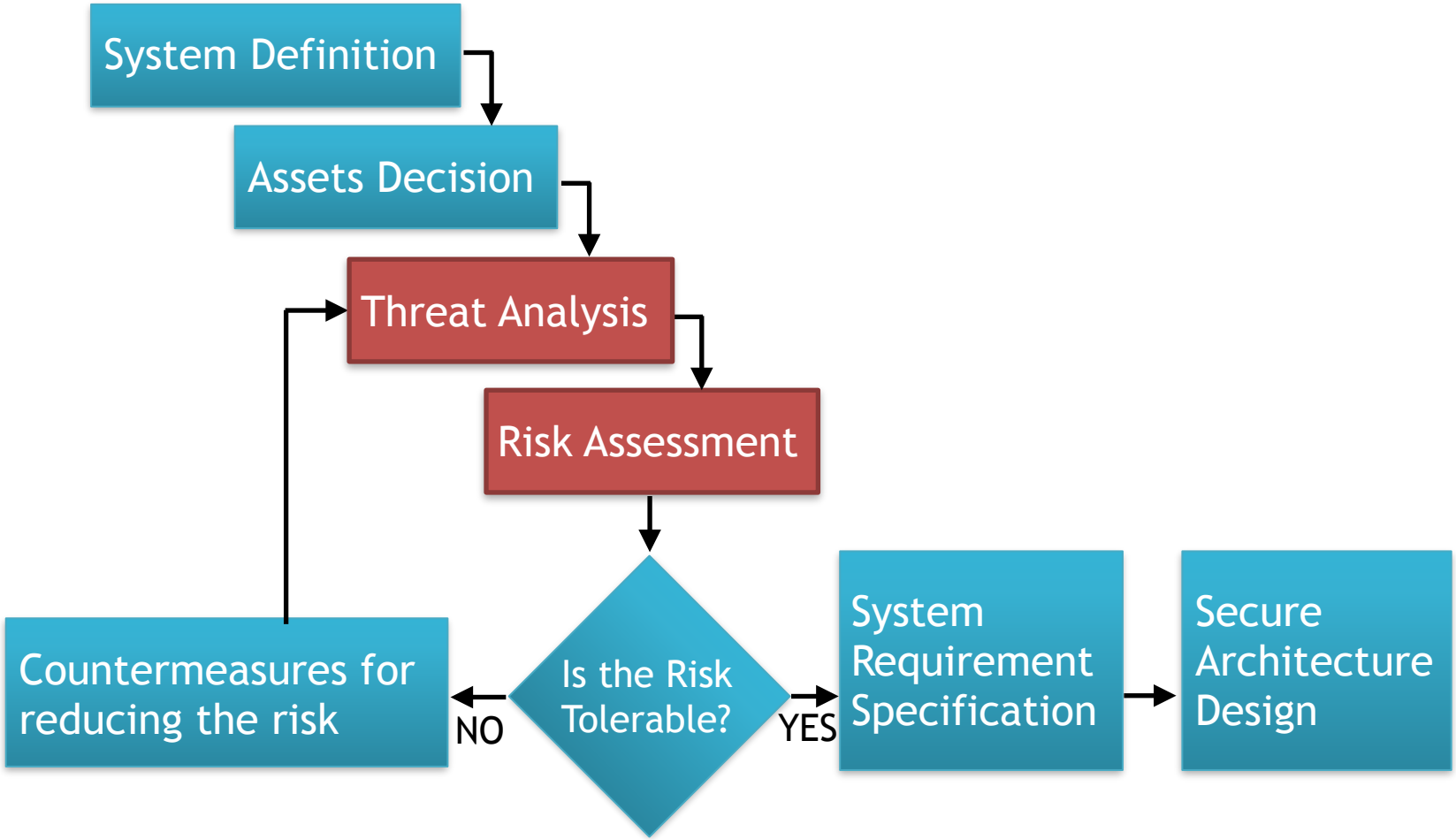
- Attack Tree
- STPA-Sec(System Theoretic Process Analysis for Security)
- SafSec(Safety & Security)

- *Techniques focused on the application of automobile embedded system software still remains unclear.*

Security Analysis

- Security Analysis Flow
- Threat Analysis
  - Objectives: locating potential security concerns in the system. environmental threats, artificial threats(non-intentional, as well as intentional).
  - Target Diagram: input of the proposed method
  - Guidewords: apply each guideword to the system design and conduct security analysis
  - Analysis Sheet: output of the proposed method
- Risk Assessment

Security Analysis: Flow Diagram



Threat Analysis: Target Diagram

- Unified Modelling Language(UML)
  - Class Diagram
  - Object Diagram
  - Use Case Diagram
  - Sequence Diagram
  - State Chart Diagram
  - Activity Diagram
  - Collaboration Diagram
  - Component Diagram
  - Deployment Diagram

Threat Analysis: Guidewords

- PROBE *access a target in order to determine its characteristics
- SCAN *access a set of targets sequentially in order to identify which targets have a specific characteristic
- READ *obtain the content of data in a storage device, or other data medium
- FLOOD *access a target repeatedly in order to overload the target's capacity
- AUTHENTICATE *present an identity of someone to a process and, if required, verify that identity, in order to access a target.
- SPOOF *masquerade by assuming the appearance of a different entity in network communications
- MODIFY *change the content or characteristics of a target
- BYPASS *avoid a process by using an alternative method to access a target

*Reference: J.D. Howard an T. A. Longstaff, "A Common Language for Computer Security Incidents", Sandian Nat. Lab., Sandia Rep. SAND98-8867, 1998.

Threat Analysis: Guidewords

- PROBE
- SCAN
- READ

Primary Guidewords

- FLOOD
- AUTHENTICATE
- SPOOF
- MODIFY
- BYPASS

Secondary Guidewords

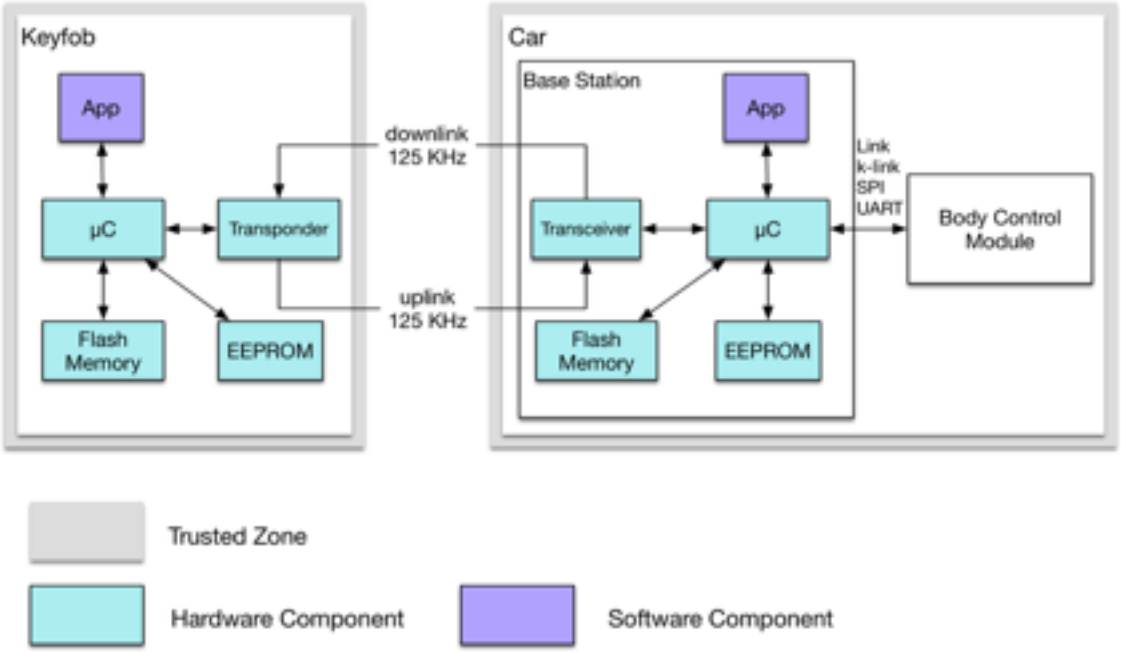
Threat Analysis: Analysis Sheet Sample

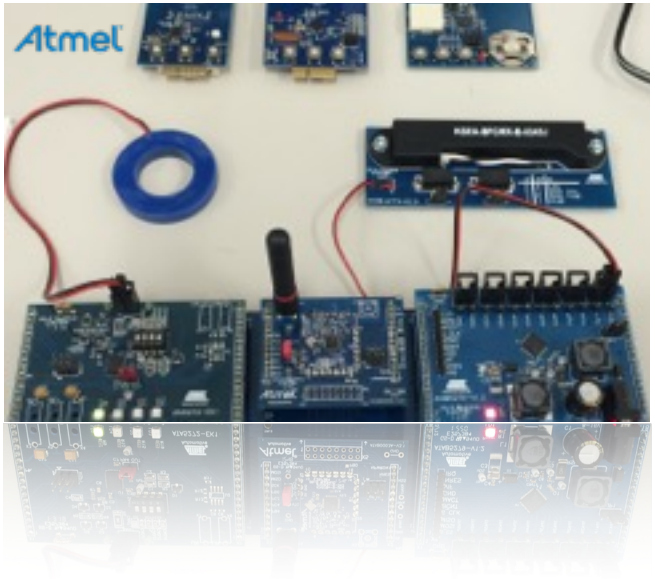
Primary Guideword			Secondary Guideword					Deviation	Local Effect	Global Effect	Possible Attack
Probe	Scan	Read	Flood	Authenticate	Spoof	Modify	Bypass				
-	-	•	•	-	-	-	-				

Security Analysis: Risk Assessment

- Severity
- Threat Occurrence Probability
- Threat Success Probability

$$risk = Severity \times ThreatOccurrenceProbability \times ThreatSuccessProbability$$

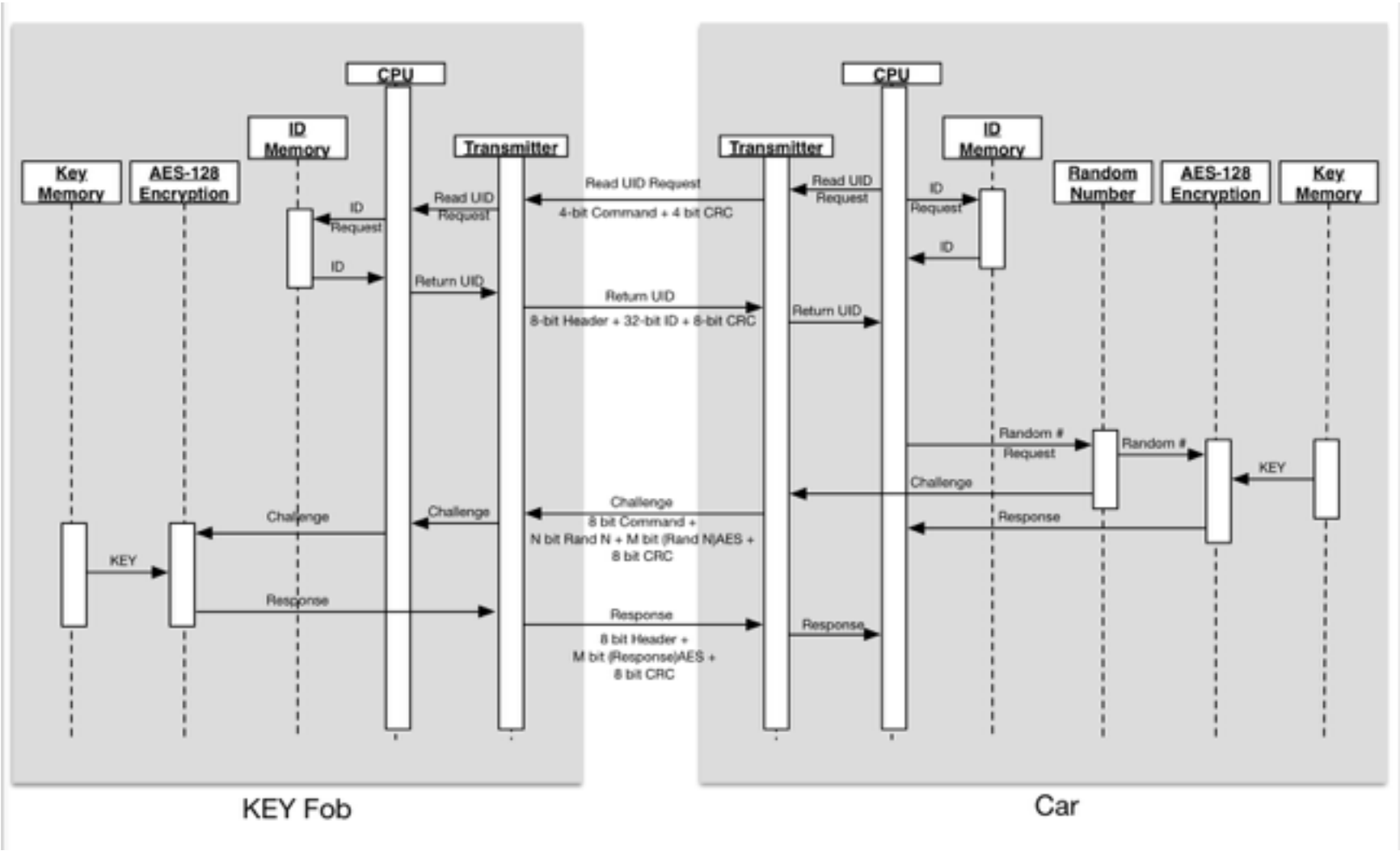




A Case Study

Open Source Immobilizer Protocol Stack
-by Atmel®

Sequence Diagram: Unilateral Authentication



(Partial) Analysis Sheet: READ UID

P*	Secondary			Deviation	Local effect	Global effect	Possible Attacks
R*	F*	S*	M*				
●	●	-	-	Flooding the KEY Fob with Read-UID-like request, which makes the KEY Fob unable to receive and deal with connections any more	The KEY Fob will not be able to send the UID information to the car.	Failure of the exchange of UID information between a registered KEY Fob and the car. The authentication will not be triggered regardless of the user's request.	Denial-Of-Service Attacks
●	-	●	-	Transponders can be used to relay the communications between the car and the key fob.	Without the genuine key fob being in the communication range, the car will be tricked to send a Read UID request to a transponder near the car.	Without user's intention, the key fob will receive a Read UID request through a transponder near the key fob. Person with the KEY Fob that is associated with a specific UID could be tracked down for their whereabouts.	Tracking
●	-	-	●	Falsification of data during the transportation.	A non-Read UID request will be sent to the key fob.	Unauthorized falsification will be ignored by the verification of CRC checksum.	Unauthorized falsification

P*: Primary Guidewords; R*: Read, F*: Flood; A*: Authenticate; S*: Spoof; M*: Modify; B*: Bypass.

Severity Value Table For Risk Evaluation: Read UID

ID	Global Effect	User Awareness	Evaluation			Severity
			Automobile	User's Wellbeing	Privacy	
1	Failure of the exchange of UID information between a registered KEY Fob and the car. The authentication will not be triggered regardless of the user's request.	Users will not notice any unusual change until they try to operate the car.	8	0	0	8
2	Without user's intention, the key fob will receive a Read UID request through a transponder near the key fob. Person with the KEY Fob that is associated with a specific UID could be	No. All communications are implemented wirelessly.	6	0	10	8
3	Unauthorized falsification will be ignored by the verification of CRC checksum.	No. All communications are implemented wirelessly.	0	0	0	0

Discussion

- Evaluate the proposed security analysis technique by conducting a case study.*
  - **Relay attack with genuine key fob**
  - **Tracking**
  - **Denial-of-service attacks**
  - **Replay attack on authentication**
  - Spoofing attack on memory access protection
  - Hijacking communication sessions
- Discovered certain vulnerabilities that may be utilized by attackers to launch attacks. However the analysis results are not to be comprehensive, thus further improvements for an exhaustive analysis are still under discussion.
  - Is it appropriate to combine the guidewords in such way?
  - Is it appropriate to deliberately separate a paired communication as two completely different objects to conduct the analysis?

*Reference: Stefan Tillich and Marcin Wójcik. Security Analysis of an Open Car Immobilizer Protocol Stack. 2012

Summary & Future works

- Present a security analysis technique based on HAZOP, and demonstrate the applicability of the proposed method by conducting a case study.
- In order to further expand the exhaustivity, improvements of this security analysis method are still considered necessary.
  - Arguments of the threshold of guidewords combination.
  - Diagrams on a even higher abstraction level,such as usecase diagram, may be essential to conduct the security analysis.