Attack tree construction: an application to the connected vehicle

CYBER-PHYSICAL SECURITY EDUCATION WORKSHOP
Paris, France — July 17–19, 2017

Khaled karray, Jean-luc Danger, Sylvain Guilley, Moulay Abdelaziz El Aabid

Presentation Outline

Introduction

- Cyber-physical architecture
- Attacks on cars

Risk assessment and attack tree generation

- Motivation
- Approach to attack modeling

Conclusion

Presentation Outline

Introduction

- Cyber-physical architecture
- Attacks on cars

Risk assessment and attack tree generation

- Motivation
- Approach to attack modeling

Conclusion

Vehicle architectural components (1)

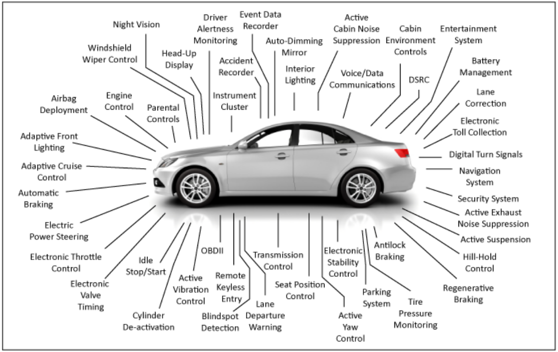


Figure : Automotive services

Cost:

The cost of electronics embedded system in the vehicle is estimated to be between 20% and 25% of total production cost

Vehicle architectural components (2)

Vehicle architectural components (2)

- Sensors: Used to collect information, data measurements of the car environment (speed, radar, temperature . . .)

Vehicle architectural components (2)

- Sensors: Used to collect information, data measurements of the car environment (speed, radar, temperature . . .)

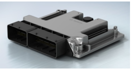
- Actuator: Elements of the vehicle architecture that converts “commands” into “ actions” (exp: engine, wheel orientation . . .)

Vehicle architectural components (2)

- Sensors: Used to collect information, data measurements of the car environment (speed, radar, temperature . . .)

- Actuator: Elements of the vehicle architecture that converts “commands” into “ actions” (exp: engine, wheel orientation . . .)

- ECUs: Electronic Control Units, are embedded interconnected controllers in the vehicle and integrate various data processing functions that guarantee the safety and comfort of the user.



Vehicle architectural components (3)

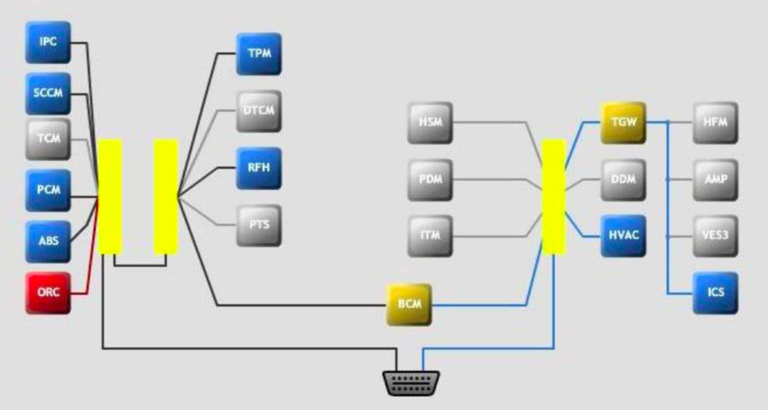
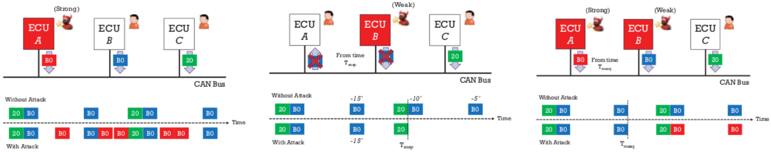


Figure : Vehicle architecture [MV15]

A vehicle architecture consists of these components interconnected by communication buses: CAN, FlexRay, . . .

Attacks on cars (1)

- Attack with physical access to the vehicle:
  - CAN frame injection attack (ECU Impersonation) [MV13, CS16]



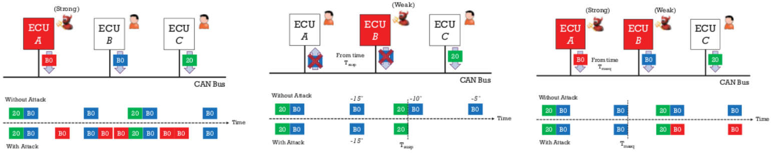
(a) Fabrication attack. (b) Suspension attack. (c) Masquerade attack.

DoS-attack (Denial of Service)

While (True) {Send CAN ID=0, payload = 0 }

Attacks on cars (1)

- Attack with physical access to the vehicle:
  - CAN frame injection attack (ECU Impersonation) [MV13, CS16]



(a) Fabrication attack. (b) Suspension attack. (c) Masquerade attack.

DoS-attack (Denial of Service)

While (True) {Send CAN ID=0, payload = 0 }

  - Attacks exploiting software vulnerabilities to access the internal networks (e.g CAN). [CMK+11, FPKS15]

Attacks on cars (2)

- Attacks with short/long range wireless access:
  - Wifi, Bluetooth, Cellular : [CMK$^+$11, MV15]

Attacks on cars (2)

- Attacks with short/long range wireless access:
  - Wifi, Bluetooth, Cellular : [CMK+11, MV15]

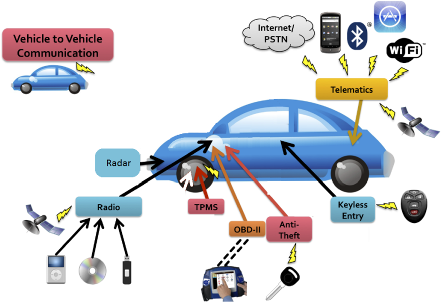


Figure : Vehicle attack vectors [CMK+11]

Presentation Outline

Introduction

- Cyber-physical architecture
- Attacks on cars

Risk assessment and attack tree generation

- Motivation
- Approach to attack modeling

Conclusion

Motivation

- Car manufacturers have to guarantee a level of security: safety, privacy of the user.
- Some security problems have to be addressed at early design phase.
- Write clear and strong security requirements to meet the security needs.

Motivation

1. Asset identification.
2. Threat identification (per asset).
3. Impact estimation (per threat).
4. Threat level estimation [likelihood] (per threat)
    - (1) architectural design
    - (2) Adversary capabilities

How to assess the risk

$$SC = \{SC_i\}$$

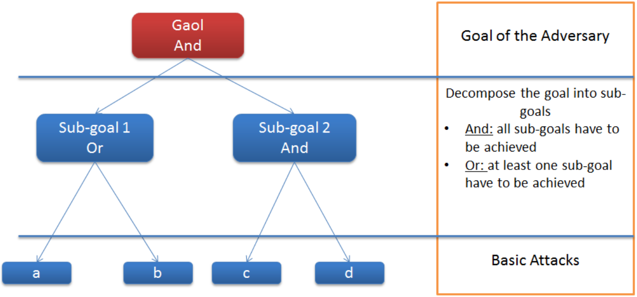
$$Risk = \sum_i Impact(SC_i) \times P_{occ}(SC_i)$$

SC : Set of attack scenarios (threats)

$Impact(x)$: Impact of the attack scenario on safety, availability, confidentiality, . . .

P_{occ} : Likelihood of occurrence of the attack scenario is correlated with the architecture (functional, hardware)

Attack tree [Sch99]


Gaol
And
Sub-goal 1
Or
Sub-goal 2
And
a
b
c
d
Goal of the Adversary
Decompose the goal into sub-goals
• And: all sub-goals have to be achieved
• Or: at least one sub-goal have to be achieved
Basic Attacks

Goal of the attack tree:

- Visualise attack paths (understand *How*)
- Helps to assess the Risk.
- Allows to think about countermeasure in an effective way.

This approach is used to support the risk assessment step.

Using attack trees

Attack trees are used to model attacks:

- Network administration: management of access policy, where to place firewalls, ... [AWK02, JN10]
- SCADA (Supervisory Control And Data Acquisition) [BFM04, TLM08]

In automotive domain:

- EVITA: E-safety vehicle intrusion protected applications (uses attack trees) [HAF+09]
- SAEJ3061: The new automotive cybersecurity standard (2016) [Com16]

Problems:

- Exhaustivity of the attack tree.
- Error prone: Security experts have to imagine all possible ways.
- Complex to draw when the system to analyze is large.

Automatic generation of attack trees

Solution: automatic generation of attack trees

Given a system model and an adversary model we want to see if the adversary can put the system in a vulnerable state, then retrace the actions.

Advantages:

- Addresses all attack vectors in a structured way.
- Automatically analyze the vehicle architecture (however large it may be).
- Lists all possible attack paths (w.r.t) the system and adversary models: exhaustivity.

Graph transformation

Graph transformation:

- The modeling is based on graph transformation system, formal modeling based on graph rewriting, which allows us to express a relational model in the form of a graph (vertex and arcs) and to explore the different possible configurations of this graph by applying transformations rules:
  - Start Graph: architectural system model
  - Transformation rules: inference rules to automate a reasoning method (deduction/derivation)

Tool:

- Groove → a tool for Graph transformation.

System Model

Modeled components: graph

- Communication nodes
- Hardware nodes, communication controllers and data storage.
- Service nodes, and access rights to hardware components.
- Data nodes.

System Model

Modeled components: graph

- Communication nodes
- Hardware nodes, communication controllers and data storage.
- Service nodes, and access rights to hardware components.
- Data nodes.

Behavioral model: transformation rules

- Behavior of hardware nodes.
- Behavior of service nodes.
- Behavior of the attacker.

Illustration: model

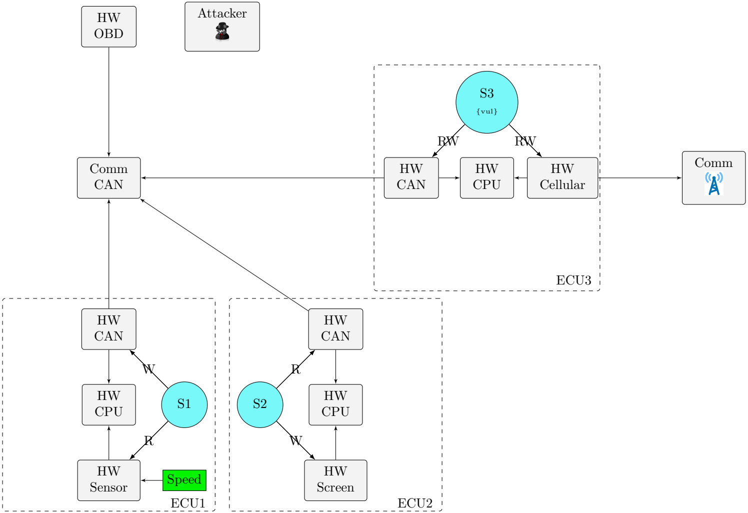


Figure : Speed acquisition and display

Transformation rules

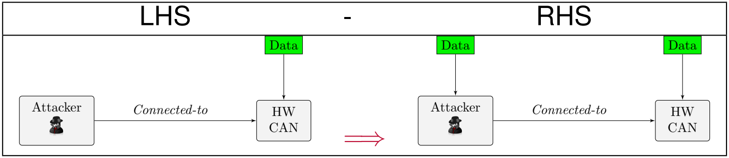


Figure : Transformation rule: attacker eavesdrop on CAN

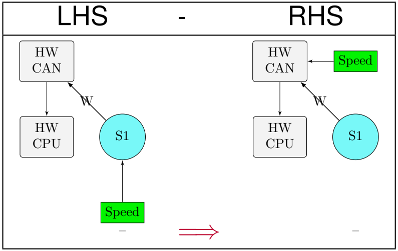


Figure : Transformation rule: Speed send to CAN

State space

state space

State space in the result of the application of transformation rules on the architectural graph.

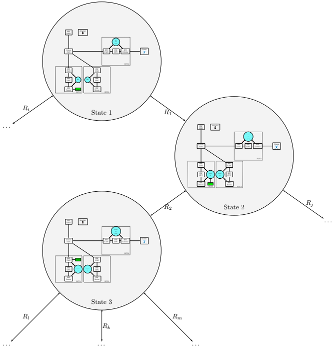


Figure : State space

Query

Query:

To find *all* vulnerable system states we make a query to see if the *threat* occurred.

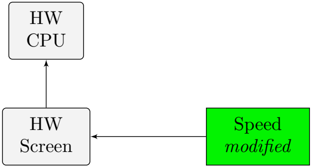
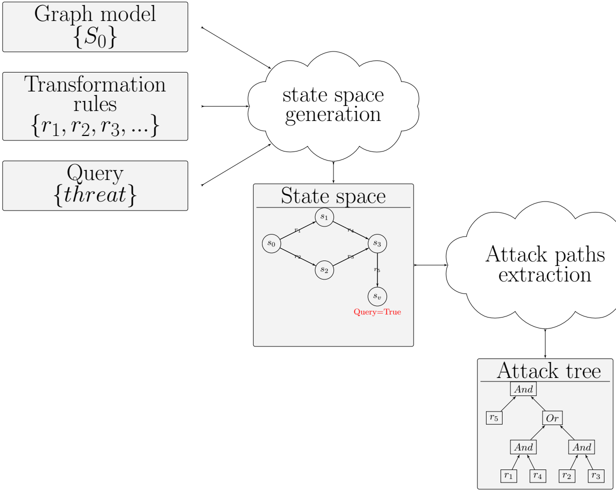


Figure : Speed modification query

Attack tree generation steps



Graph model $\{S_0\}$

Transformation rules $\{r_1, r_2, r_3, ...\}$

Query $\{threat\}$

state space generation

State space

Attack paths extraction

Attack tree

Figure : Automated generation of attack trees

Illustration: Attack tree

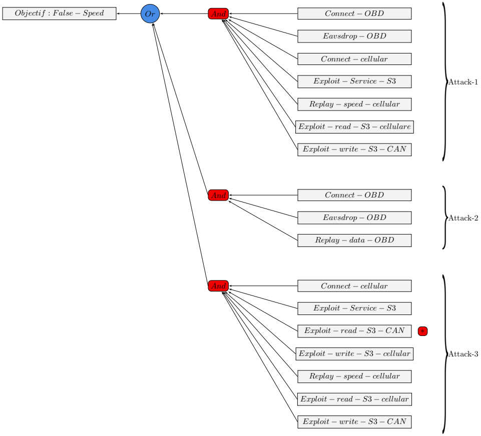

Objectif : False – Speed
Or
And
Connect – OBD
Eavsdrop – OBD
Connect – cellular
Exploit – Service – S3
Replay – speed – cellular
Exploit – read – S3 – cellulare
Exploit – write – S3 – CAN
Attack-1
And
Connect – OBD
Eavsdrop – OBD
Replay – data – OBD
Attack-2
And
Connect – cellular
Exploit – Service – S3
Exploit – read – S3 – CAN
Exploit – write – S3 – cellular
Replay – speed – cellular
Exploit – read – S3 – cellular
Exploit – write – S3 – CAN
Attack-3

Figure : Attack tree: Speed acquisition and display

Illustration: model

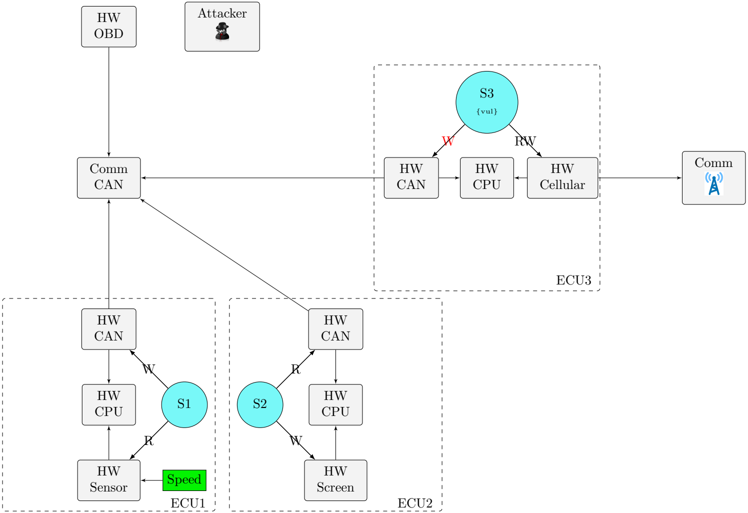


Figure : Speed acquisition and display

Illustration: Attack tree - countermeasure

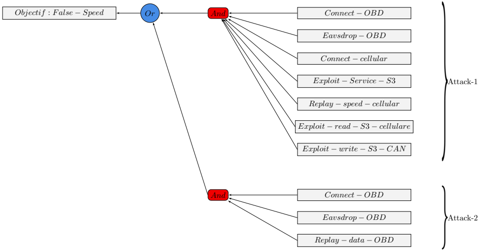


Figure : Attack tree: Speed acquisition and display

Presentation Outline

Introduction

- Cyber-physical architecture
- Attacks on cars

Risk assessment and attack tree generation

- Motivation
- Approach to attack modeling

Conclusion

Conclusion

- We need to consider security from design phase in order to build secure cars.
- We need to properly estimate the risk associated with threats.
- Attack trees are good tool for security risk assessment.
- Automatic generation of attack trees to overcome possible human errors and for exhaustivity.

Conclusion

- We need to consider security from design phase in order to build secure cars.
- We need to properly estimate the risk associated with threats.
- Attack trees are good tool for security risk assessment.
- Automatic generation of attack trees to overcome possible human errors and for exhaustivity.

Thank you for your attention!

References I

- Paul Ammann, Duminda Wijesekera, and Saket Kaushik.
  Scalable, graph-based network vulnerability analysis.
  In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 217–224. ACM, 2002.

- Eric J Byres, Matthew Franz, and Darrin Miller.
  The use of attack trees in assessing vulnerabilities in scada systems.
  In *Proceedings of the international infrastructure survivability workshop*, 2004.

- Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al.
  Comprehensive experimental analyses of automotive attack surfaces.
  In *USENIX Security Symposium*. San Francisco, 2011.

References II

- Vehicle Electrical System Security Committee.
  Sae j3061-cybersecurity guidebook for cyber-physical automotive systems.
  2016.

- Kyong-Tak Cho and Kang G Shin.
  Fingerprinting electronic control units for vehicle intrusion detection.
  In *25th USENIX Security Symposium (USENIX Security 16)*, pages 911–927. USENIX Association, 2016.

- Ian D Foster, Andrew Prudhomme, Karl Koscher, and Stefan Savage.
  Fast and vulnerable: A story of telematic failures.
  In *WOOT*, 2015.

References III

Olaf Henniger, Ludovic Apvrille, Andreas Fuchs, Yves Roudier, Alastair Ruddle, and Benjamin Weyl.
Security requirements for automotive on-board networks.
In *Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on*, pages 641–646. IEEE, 2009.

Sushil Jajodia and Steven Noel.
Topological vulnerability analysis.
In *Cyber situational awareness*, pages 139–154. Springer, 2010.

Charlie Miller and Chris Valasek.
Adventures in automotive networks and control units.
DEF CON, 21:260–264, 2013.

Charlie Miller and Chris Valasek.
Remote exploitation of an unaltered passenger vehicle.
Black Hat USA, 2015, 2015.

References IV

Bruce Schneier.
Attack trees.
Dr. Dobbs journal, 24(12):21–29, 1999.

Chee-Wooi Ten, Chen-Ching Liu, and Govindarasu Manimaran.
Vulnerability assessment of cybersecurity for scada systems.
IEEE Transactions on Power Systems, 23(4):1836–1846, 2008.