Consiglio Nazionale delle Ricerche

Security-by-Design in Vehicular SoS

Ilaria Matteucci

Istituto di Informatica e Telematica
CNR – Pisa, Italy

Case Study - CS1
Mobility Ecosystem

"*IT is pervasive in automotive systems: cars can request assistance, consult Internet and interact with other vehicles via mobile communication or Wi-Fi connection or other protocols. From the convergence of Vehicular Networks composed by vehicles, infrastructure, and other urban or transportation systems we envision the emergence of a Vehicular System of Systems (VeSoS), which may bring several advantages in terms of ecological and economical benefits, as well as safety. VeSoS can be even part of larger ecosystems, like Smart Mobility Ecosystems (SMEs), which include several heterogeneous systems, such as road users' apps, other VeSoS and infrastructures, which have to be dynamically integrated so to achieve interoperability and information sharing, while suitably reacting to unplanned events (e.g., need of re-planning). GAUSS will study an automatic way to support integration in VeSoS and SMEs by guaranteeing both functional and nonfunctional requirements, also taking into account security and safety issues related to possible cyber-attacks.*"

Case Study - CS1
Mobility Ecosystem

"*IT is pervasive in **automotive systems**: cars can request assistance, consult Internet and interact with other vehicles via mobile communication or Wi-Fi connection or other protocols. From the convergence of Vehicular Networks composed by vehicles, infrastructure, and other urban or transportation systems we envision the emergence of a **Vehicular System of Systems (VeSoS)**, which may bring several advantages in terms of ecological and economical benefits, as well as safety. VeSoS can be even part of larger ecosystems, like Smart Mobility Ecosystems (SMEs), which include several heterogeneous systems, such as road users' apps, other VeSoS and infrastructures, which have to be dynamically integrated so to achieve interoperability and information sharing, while suitably reacting to unplanned events (e.g., need of re-planning). **GAUSS will study an automatic way to support integration in VeSoS and SMEs by guaranteeing both functional and nonfunctional requirements, also taking into account security and safety issues related to possible cyber-attacks.***"

Outline

- Vehicles communication systems
  - four domains: V2V, V2X, Intra-V, and U2V
  - Cyber security attacks surface

- Research challenges
  - Security and safety balance
  - Security-by-Design for automotive

Facing on a growing cyber-security issue

ELECTRONICS > HACKERS CAN UNLOCK CARS VIA SMS

Hackers can unlock cars via SMS

By Sebastian Anthony on July 28, 2011 at 7:10 am | 6 Comments

Share This Article

336 511 9

engineering, the hackers were able to pose as these s
a car's on-board computer via "war texting" — a rift on
wireless networks.

Don Bailey and Mathew Solnik, both employees of iSE
at next week's Black Hat USA conference in Las Vegas
Identifying and Interacting with Devices on the Teleph

In news that will probably leave

RISK ASSESSMENT / SECURITY & HACKTIVISM

Senator: Car hacks that control steering or steal driver data way too easy

Most known hacks could be prevented with simple measures, researcher says.

by Dan Goodin - Feb 3, 2015 10:07pm EST

Share Tweet 122

Wikipedia

Recently manufactured cars expose drivers to hacking attacks that could cause collisions and steal

LATEST F

12.05.15 11:11 AM

PORT SLAMS RS FOR LEAVING ERABLE TO HACKERS

BAD BAR
Head c
tradin
fad"

NEED MO
July 15
deals t
subscr

H,O H,O
BMW
cell ca
GT

LATEST F

FEATURE ST
Our f

Ed Markey
@SenMarkey

Follow

A car's computer shldn't get hacked by an iPad. I spoke w @CarlQuintanilla @KaylaTausche @JonFortt abt my new report bit.ly/1E3DQiu

6:24 PM - 10 Feb 2015

YouTube @YouTube

Facing on a growing cyber-security issue (1)

2010

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

21st, July 2015

30th, July 2015

The 29-year-old hacker who was able to take control over GM cars tells us how easy it was to pull off

CADIE THOMPSON, TECH INSIDER
Jul. 30, 2015, 10:19 PM | 6

Hacking a car is way too easy?

CONNECTED CARS →

- SAFETY
- INNOVATION
- REVENUES

CONNECTIVITY →

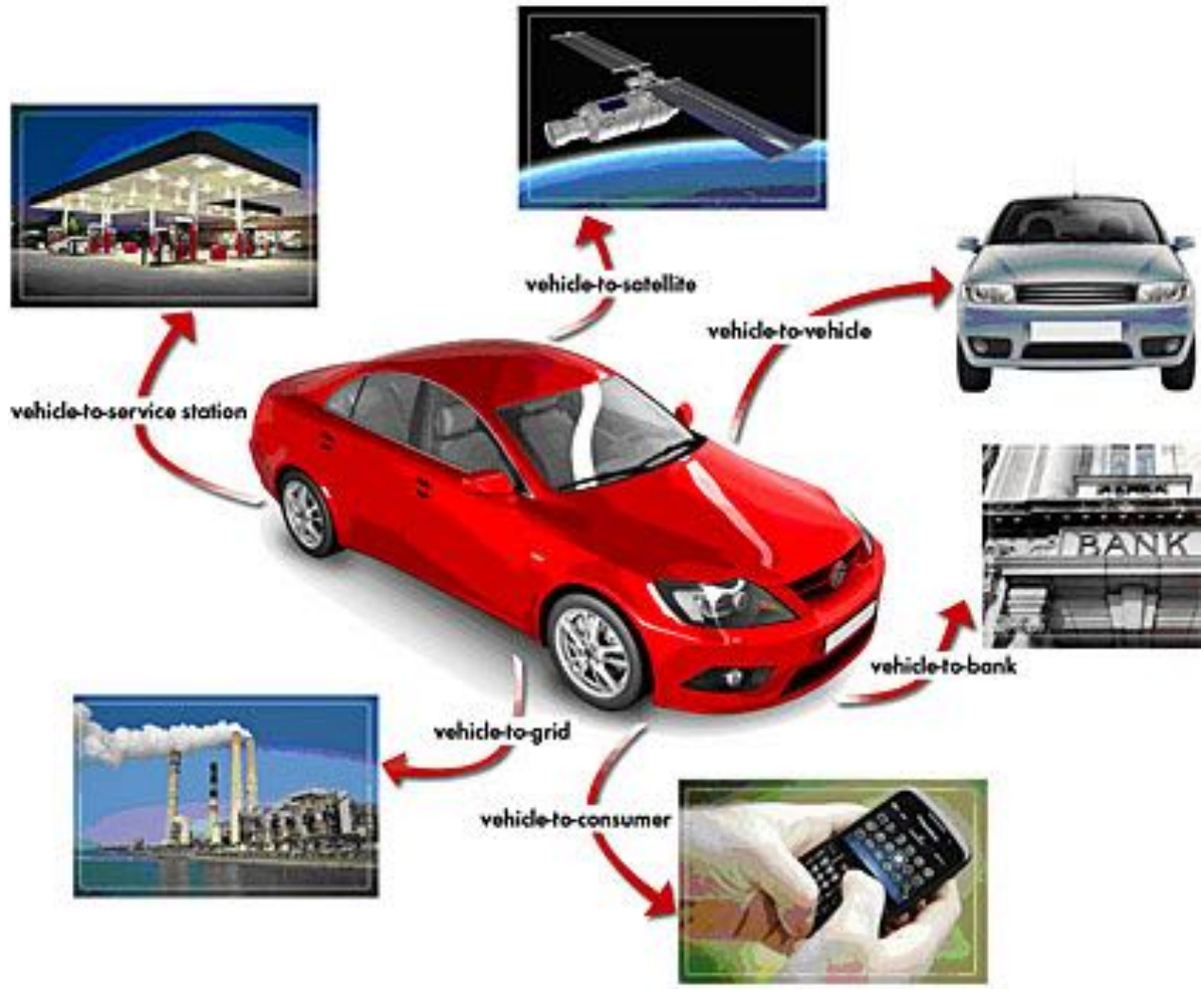
- MULTIPLE PENETRATION
- ATTACK VECTORS

Richard Clarke – Counterterrorism expert:

“There is reason to believe that intelligence agencies for major powers’know how to remotely seize control of a car.”

Vehicle communication

- Vehicle to External Infrastructure (V2X)
  - Vehicle2Roadside
  - Vehicle 2Service
  - Vehicle2Home
  - etc.
- Vehicle to Vehicle (V2V)
- User to Vehicle (U2V)
  - multimedia
  - infoteinment
  - etc.
- Intra Vehicle (Intra-V)



Security impacting on Safety

Authenticity: Unauthorized access through infotainment or another vehicular network may grant access to the overall Intra-Car network.

Data integrity: A hacker can use failures to try to get internal data of the vehicle or try to acquire control of parts of the car.

In the future, with autonomous driving systems,
vehicular assault as a terrorist tactic can be done remotely

Possible remote attack scenarios

Authenticity: Remote control by using personal mobile device (U2V)

Availability: The connectivity system will have to be always available (V2X)

Confidentiality: data is encrypted and can only be read by authorized nodes.

Our Proposal

"Fine tune and apply an integrated and standardized process for enabling security by design in automotive industry coupled with safety aspects."

Security-by-Design in Automotive

A Secure-by-Design Tool-chain is able to

- develop automotive specific and customized solutions
- cope with cyber-security attacks
- detect anomalies in the automotive system
- recover from attacks and anomalies.

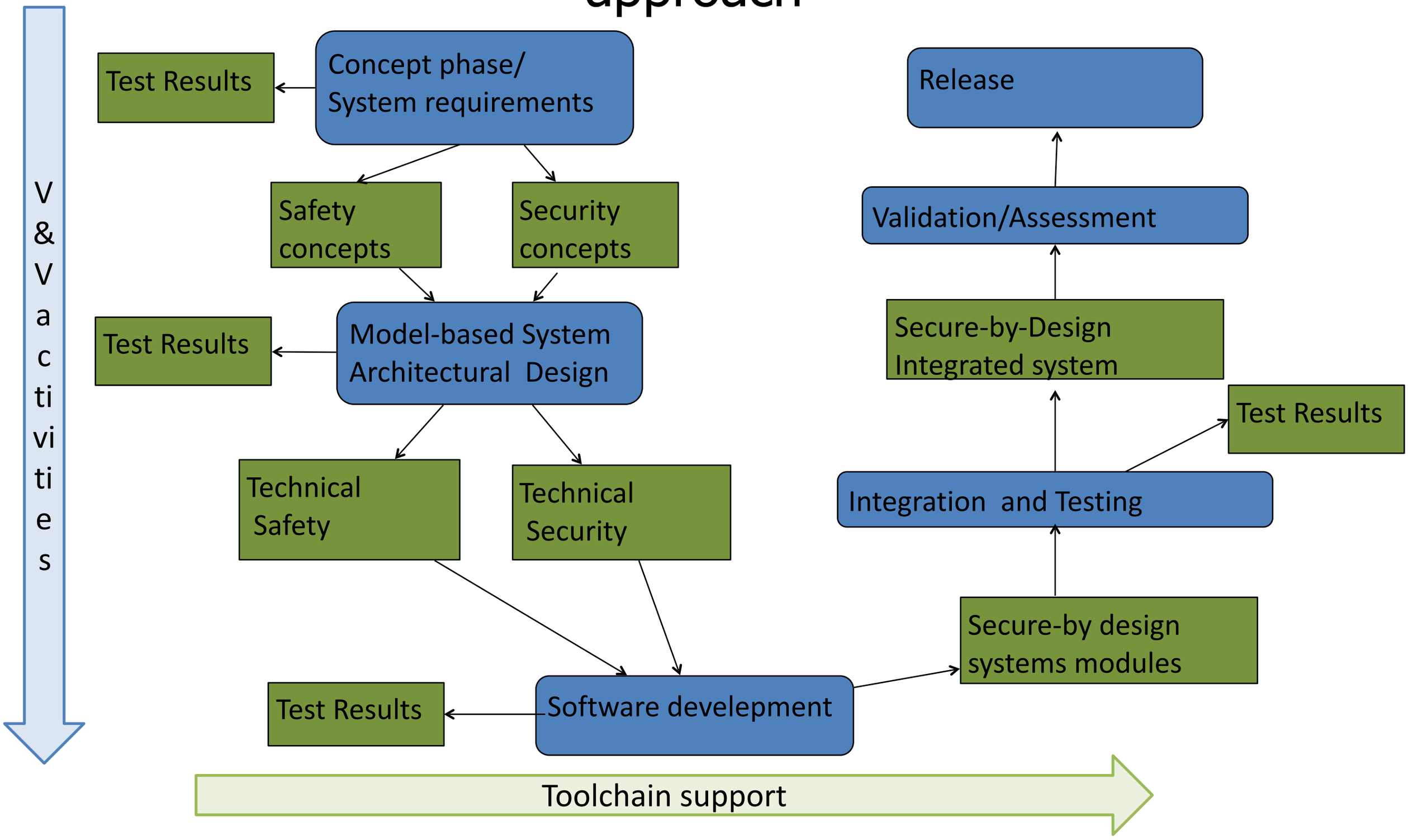
How?

- powerful protection mechanisms to enforce integrated safety and security requirements at design time
- continuous authentication and authorization mechanisms (Usage Control)

Challenges of the security-by-design

- Adoption of security standards (e.g. AUTOSAR,…)
- Definition of new security concepts (reqs, risks, …)
- Integration of security into the “Safety-V-model”
- Adoption of a security-by-design approach:
  - Improving interoperability
  - Improving adoption of V&V best practices
- Toolchain supporting security-by-design approach

Improving V&V adoption into a security-by design approach



Thank you!

Questions?