Design and Verification of Secure Autonomous Vehicles

Letitia W. Li, Ludovic Apvrille, Annie Bracquemond
letitia.li@telecom-paristech.fr

ITS
<table>
<thead>
<tr>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tire Pressure Sensor</td>
</tr>
<tr>
<td>Rouf 2010</td>
</tr>
<tr>
<td>OBD-II Diagnostic Port</td>
</tr>
<tr>
<td>Koscher 2010</td>
</tr>
<tr>
<td>Foster 2015</td>
</tr>
<tr>
<td>3G/4G Cellular Network</td>
</tr>
<tr>
<td>Miller 2015</td>
</tr>
<tr>
<td>Malicious Mobile Applications</td>
</tr>
<tr>
<td>Woo 2015</td>
</tr>
<tr>
<td>Exploitation of Web APIs</td>
</tr>
<tr>
<td>Nissan Leaf 2016</td>
</tr>
<tr>
<td>Infotainment Center</td>
</tr>
<tr>
<td>Koscher 2011</td>
</tr>
<tr>
<td>Conclusion</td>
</tr>
</tbody>
</table>

**Attacks on Connected Vehicles**

![Diagram of a car with various attack vectors highlighted]
Attacks on Autonomous Vehicles

Over-the-air Firmware update
GPS Spoofing
Humphreys 2008
Camera Blinding
Petit 2015
LIDAR spoofing
Petit 2015
Computer Virus
EVITA Project

- FP7 project ended in 2012
- E-safety Vehicle Intrusion Protected Applications
- Design of architecture for secure automotive on-board networks
- EVITA does not address side-channel attacks i.e. hardware is assumed to be tamper-resistant
- Several EVITA-compatible ECUs on the market (STM, Bosch, etc.)
Security Requirements

- Authenticity of vehicle software and data
- Authenticity of vehicle communication
- Confidentiality of vehicle communication
- Integrity of vehicle communication
- ...
EVITA Results

- Security Protocols
  - Protocols are CAN compatible
  - Formally verified with SysML-Sec
- APIs
  - Integration in Autosar
- Specification of Hardware Security Modules
Hardware Security Modules

<table>
<thead>
<tr>
<th>EVITA Hardware Security Module</th>
<th>Application core</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC</td>
<td>Flash</td>
</tr>
<tr>
<td>Clock</td>
<td>RAM</td>
</tr>
<tr>
<td>AES-PRNG</td>
<td>CPU</td>
</tr>
<tr>
<td>RAM</td>
<td>EVITA interface</td>
</tr>
<tr>
<td>AES</td>
<td>Flash</td>
</tr>
<tr>
<td>Counter</td>
<td>CPU</td>
</tr>
<tr>
<td>Whirlpool</td>
<td>Interface</td>
</tr>
</tbody>
</table>

In-vehicle system bus

7/25 June, 2017

Institut Mines-Telecom

Security Verification for the Design of Autonomous Vehicles
EVITA Architecture

- Vehicle serial no. provider
- ESP
- ESP
- EVITA full
- GPS
- EVITA light
- EVITA light
- EVITA light
- EVITA light
- EVITA light
- EVITA light
- EVITA medium
- EVITA medium
- EVITA medium
- EVITA medium
- V2X
- Central gateway
- Engine control
- Airbag actuator
- Brake actuator
- RTC clock
- EVITA light

Attacks

Countermeasures

Method

Verification

Conclusion
How to Design a Secure Automotive System?

”Those who fail to plan, plan to fail.”

Benjamin Franklin

- Use of a model-driven approach (SysML-Sec)
- Support of safety, performance and security (formal) verification
Autonomous Vehicle under Design
Institut Mines-Telecom

Security Verification for the Design of Autonomous Vehicles

13/25  June, 2017

Attack Tree

Attacks
Countermeasures
Method
Verification
Conclusion

Attack Tree

AutonomousVehicle

<<block>>

<<root attack>>

attackAutonomousBraking

<<OR>>

<<block>>

AutonomousVehicle

<<block>>

<<attack>>
degradeBrakeFunction

<<attack>>

manipulateEnvironmentalInformation

<<OR>>

<<block>>

<<attack>>

preventBrakingFunction

<<attack>>

preventDataComputation

<<OR>>

<<block>>

<<attack>>

delayBrakingFunction

<<attack>>

delayDataTransmission

<<attack>>

jamInCarCommunications

<<attack>>

ddosController

<<block>>

manipulateEnvironmentalSensor

<<block>>

infectFakeEnvironmentalInformation

<<block>>

disableSensors

<<block>>

corruptControllerData
Hardware Security Modules

- **Attacks**
- **Countermeasures**
- **Method**
- **Verification**
- **Conclusion**

June, 2017

Institut Mines-Telecom

Security Verification for the Design of Autonomous Vehicles
Model Verification

Verification

Safety

Performance

Security

Reachability

Simulation

ProVerif
Security Verification Results
Impact of Security on Performance and Safety

- Encryption/Decryption occupy execution cycles
- Communications increase due to key exchange, increased message size
Model Simulation

14000 cycles
17000 cycles
Secured with HSM

16000 cycles
Test of Security Countermeasures
Conclusion and Future Work

Contributions

▶ New security considerations for autonomous vehicles
▶ Increased connectivity introduces vulnerabilities
▶ Model-Driven approach towards modeling and verification of (automotive) embedded systems

Future Development

▶ Iterations between requirements, attacks and partitioning solutions
▶ Modeling the relationship between safety and security
▶ Better relations between partitioning and subsequent modeling stages
Thank You!

References

TTool: ttool.telecom-paristech.fr
SysML-Sec: http://sysml-sec.telecom-paristech.fr/
Personal website: http://perso.telecom-paristech.fr/~apvrille