EARPA Position Paper

Cross-cutting activity Task Forces

The Role of Cyber security R&D in European Road Transport and ICT

October 2016

About EARPA

Founded in 2002, EARPA is the association of automotive R&D organisations. It brings together the most prominent independent R&D providers in the automotive sector throughout Europe. At present its membership numbers 51, ranging from large and small commercial organisations to national institutes and universities.

The EARPA Cyber security position is a Cross-cutting activity among 10 Task Forces launched in 2016. This cross-cutting activity discusses the R&D needs for design, integration, testing and validation in automotive applications. It will deliver benefits to safety, production, maintenance and mobility.

This position paper presents a synthesis of the Task Forces members' view on the relevance of R&D on automotive cyber security, a description of the role of this cross-cutting activity, suggestions for future research priorities and supported roadmaps and how these automotive solutions will impact our society.

1. Introduction to Cyber security in European Road Transport and ICT

1.1. Overall context for connected and autonomous vehicles and link to cybersecurity.

Vehicles are becoming increasingly automated, personalized. They are a new element of the Internet of Things (IoT). Also, reliance on and complexity of electrical and/or electronic systems are growing in the automotive industry. These trends provide numerous societal and customer benefits but introduce new challenges related to safety, security and privacy. We will focus on the following mostly on the two first aspects.

It has been foreseen that cybercrimes will be a real threat to the industry and ignoring the security aspects by automotive industry (OEMs, TierX, stakeholders…) could result in compromising their users in terms of safety and personal information, risking brand value, and incurring financial and moral liabilities[1]. Cybersecurity, as a cross-cutting issue for the automotive sector, is also about securing the supply chain, involved in our highly globalized logistics industry[2], or securing new transport concepts as advanced urban mobility technologies and its associated business models.

Cybersecurity is not crisis management. **Automotive security must be proactive**: it hinders crimes before they happen and avoids catastrophes before they occur. As a result, research needs to be performed to systematically address security and privacy risks to preserve the comfort and safety of our vehicles and our mobility based economy. To do so, this Cross-cutting activity has been proposed.

[1] N. Tare. NE3001: Cybersecurity in the automotive industry. Frost & Sullivan, October 2014.
[2] PWC, Transportation & Logistics 2030 Volume 4: Securing the supply chain

1.2. Vision and Scope

The vision of the proposed cross-cutting area is to support ongoing activities to establish that security and privacy are assumed to be **necessary brand and quality features of vehicles**. The mission is to contribute to sustainable transport systems and society by adopting "security-by-design" and "privacy-by-design" approaches.

The scope spans from traditionally "isolated" vehicles to connected (to the infrastructure and/or other vehicles), automated (where some or all driving functions are relying on infrastructure and/or other vehicles) and also autonomous vehicles (that can evolve without specific interaction with other vehicles). In the following, "autonomous" covers both automated and autonomous.

The activities and potential projects proposals are expected to cover both fundamental and applied research, ranging from Technology Readiness Level (TRL) 1 (Basic Technology Research) to TRL 7 (System prototype demonstration in an operational environment). EARPA strongly encourages collaboration across multiple stakeholders.

1.3. Main drivers, trends, evolution

Nearly 100 percent of vehicles on the market[3] include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions and most automobile manufacturers are unaware of or unable to report on past hacking incidents. This clearly indicates that research activities need to be performed in order to systematically and effectively deal with security and privacy risks to preserve the overall quality and safety of vehicles.

In addition, the integration of upcoming technologies for connectivity (e.g. satellite, cellular, Wi-Fi, Radio DSRC, Bluetooth, Wireless Sensors) together with the merger of information system and advanced functionality for the vehicle (assisted and autonomous driving, vehicle components management…) call for the co-design of solutions for security, safety and reliability from individual components up to the complete vehicle system. Not only the single electronics components have to be secured but also the Interfaces, Firmware, communication, application software. Generally the security value chain has to be considered from the each level of the value chain – from vehicle part up to the transport infrastructure including the related services (e.g. maintenance, mobility…) and not forgetting the users' privacy and integrity.

1.4. Objectives

The main objective of the cross-cutting activity on Cyber security is to address these challenges by defining relevant research priorities and implementing successful research activities. The EARPA goals of the activities are multiple:

- Understand security challenges and associated safety, privacy, financial, and operational risks
- Develop common best practices, guidelines and policies for the automotive industry in accordance with regulatory perspectives such as the GDPR (General Data Protection Regulation) to enter into force in 2018
- Investigate existing security relevant technologies from other industrial domains (e.g. banking sector experience; energy sector with their recently developed Smart Meter Gateway security architecture[4] or public transport security architecture, both developed for

[3] Staff of Senator Edward J. Markey. Tracking & hacking: Security & privacy gaps put American drivers at risk. Last accessed on 20161012 from https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf February 2015.

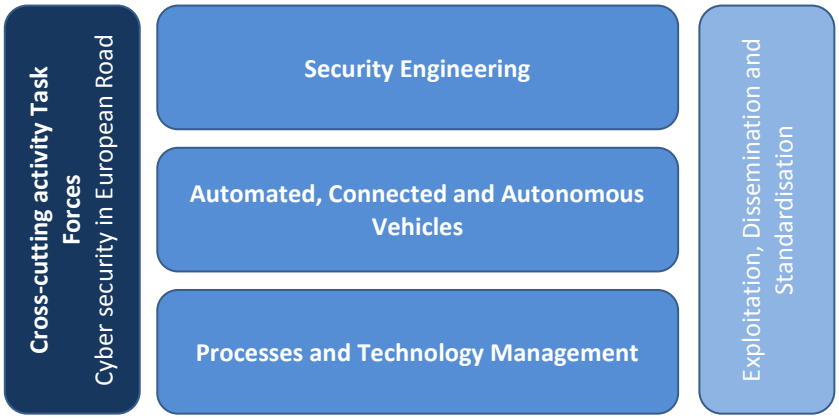
[4] E.g. German BSI TR03109-2, Last access on 20160930, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-2-Sicherheitsmodul_Use_Cases.pdf?__blob=publicationFile&v=1

mass market applications, and if possible adapt them in the context of the automotive industry. If required, investigate and develop new automotive specific security technologies
- Investigate, develop, and integrate processes to ensure "end-to-end security".

The EARPA cross-cutting activity on Cybersecurity ambition is to catalyse that Europe will be the frontrunner in the technical and organizational innovation towards secured value chain for connected, automated and autonomous vehicles and Intelligent Transport Systems (ITS), by optimal co-operation in the triple helix of academia, industry and government. More generally, the cross-cutting activity promotes faster integration of innovative solution (technological and organisational) and take-up by OEMs and suppliers, technology and service providers and authorities.

2. Areas of expertise and role needed in the development of cyber security

The cross-cutting activity is structured in accordance with FFI - Fordonsstrategisk Forskning och Innovation "Program Automotive Security and Privacy"[5]



Security engineering	**Automation, Connected and Autonomous Vehicles**
• Estimating impact of security and privacy breaches • Security requirements and mechanisms • Key management • Development of novel technologies • Adapting existing technologies from other industrial domains • Methods and tools • Security testing, verification and validation (V&V) • E/E system architecture and ECU platform • Software platform and software security • Intrusion detection and tolerance	• Needs from higher automation (cyber physical capabilities) • Needs from exposure from communication technologies • Security for wireless vehicle interface and wireless communication technologies • Security for physical vehicle interface and wired communication technologies • Security for vehicle-to-X (V2X) communication • Impact of security on function performance • IT architecture supporting ITS and connected vehicles • Privacy and data protection • Laws and regulations

[5] http://www.vinnova.se/EffektaXML/ImporteradeUtlysningar/2015-06058/FFI_Strategic_Automotive_Security_Programbeskrivning%202015-10-05%20(003).pdf(685735).pdf

Processes and Technology Management	**Exploitation, Dissemination and Standardisation**
• Societal aspects, human and organisation factors • Incident management • Processes to support end-to-end vehicle security • Development and organisation processes • Interplay among security, privacy and safety	• Exploitation of and alignment with on-going national and international research initiatives • Activities to increase awareness and information exchange • Training seminars, conferences and events • Exploitation of and alignment with on-going European and international standardisation initiatives and activities

The structure above should be considered as an idea-list of research areas and should be used as a support for how we can sort and address different needs. Within this structure, has the following fields of activity been defined as enablers for the continuing work:

2.1. Security engineering

There is a need to detect and deal with security problems in real-time. Not only secure remote software updates are needed, but technologies to detect malicious or unintended communication and application behaviour must be developed. Mechanisms able to reconfigure and possibly disable functions and applications are required to guarantee that basic and important vehicle functions continue to work when malicious activities are detected. Application developers must have a clear understanding of security requirements and problems relating to communications and data sharing. It is essential to have clear regulations and requirements for development and security testing, validation and verification (V&V), and possibly also standardization must be developed dealing with both internal devices and third-party products, including BYOD (bring your own device).

Secure Software (SW) and Hardware (HW) development activities may include: Vulnerability assessment and attack surface analysis; Countermeasures at platform level and application level; Security aspects of embedded SW and HW architecture, its design and implementation; Testing, verification and validation to build security assurance and anomaly detection and prevention; Processes starting from concept and design phases to operational, maintenance and decommissioning phases.

2.2. Automation, Connected and Autonomous vehicles

This covers: Secure communication technologies for traditional, as well as increasingly connected and automated vehicles, considering both wireless as well as physical interfaces, and how security problems may affect its features (safety and comfort) and other components in the system, user acceptance and finally, successful deployment of these technologies in our roads. Performance can also be affected by security requirements, consequently, a balanced trade-off between functionality and cybersecurity shall be addressed.

ITS infrastructure, data and mobility providers, sharing interfaces with vehicles through V2X communications, also face security challenges that may affect the overall performance of the transport network and, thus, shall provide minimum levels of cybersecurity, data privacy and data protection by design and according to national and European level legislation (e.g. GDPR).

2.3. Processes

Integration and synthesis of existing and established results from other industries (IT, avionics, energy, software engineering and industrial control systems) are strongly encouraged where such possibilities exist. For example, automotive security is rapidly converging with traditional information technology (IT) security because of a digital revolution that has made it possible to manufacture vehicles with hi-tech electronic architectures and communication systems, for

example, Ethernet and wireless technologies. Alongside new challenges, this phenomenon opens up new opportunities for the automotive industry to tackle security concerns by taking advantage of well-established IT security methodologies and processes (e.g. integrating the whole automotive software life cycle as an important part of security, since security is not finished when the vehicle is delivered to the customer). In that context, privacy has to be ensured (e.g. via anonymization methods) to avoid misused of information that could for example lead to user activity identification and traceability.

2.4. Dissemination

Manage spreading of the activities within the cyber security area, by conducting a proactive communication plan including: national and international, presentations of progress at relevant forums, dissemination initiatives and activities should be coordinated across the projects within this cross-cutting activity. After the work starts functioning, a committee may be created on request by EARPA's Board. The committee would consist of representatives from involved EARPA Task Forces to secure momentum, broaden perspective and that all aspect has been looked at. This committee would support exploitation and dissemination objectives and EARPA recommendations for updated or new standards.

3. EARPA research priorities in the field of Cyber Security

According to their capabilities, the members of the Task Forces have identified the following priorities:

Key research needs
Concerning the topic of cyber security, EARPA stresses the importance of further research and development on the following elements:

1. ***Vehicle as a cyber-physical entity***
2. ***Secure vehicle in unsecure environment***
3. ***Secured operations in an unsecure environment***
4. ***Secured ownership in an unsecure environment***

The type of attacks will require potentially the same security techniques but their implementation may drastically vary when considering the different types of attacks.

3.1. Vehicle as a cyber-physical entity

The embedded sensing and actuating elements that constitutes the vehicle need to resist several problems such as theft attempt, validation of integrity of several parameters such as the engine (chip tuning) and ensure the safety of driving commands. This means that not only the individual component has to reach a higher level of security but also the vehicle system as a whole need to be considered and evaluated which is not done currently. Indeed, as an object included within the Internet of Things, the vehicle is both a target and a potential door for attacker. The vehicle itself needs to integrate solutions for preventing and countering both attacks.

Key research activities are:

- Developing the understanding and implication of the security of implementation
    - Management scheme for virtual keys (car sharing…) and certificates (car integrity, firmware signature…)
    - ECU own resistance capabilities to attacks
    - Components resistance and protection (such as actuators and sensors)
- Addressing the vehicle electronics architecture design based on industrial specifications and requirements
    - Vehicle internal network resistance to eavesdropping & injection attacks

  - Identification of relevant elements in the security chain and implementation of these new secured solutions
  - Isolation of the vehicle network from external to prevent car to be remotely controlled and to prevent spreading of "malware" i.e. vehicle or ECU level firewalls
- Specifying and implementing the framework for evaluation and testing of components and system (vehicle): preparation for future security certification in accordance to national and European regulation bodies (this will also apply to the three other areas described below)

It is expected that the cost of such protection solution will impact directly the vehicle cost, therefore simplicity and cost-effective secure solutions and protocols are required.

3.2. Secure vehicle within an insecure environment

Future vehicles will heavily rely on communication technologies for the provision of services such as advanced navigation capabilities, infotainment services and dynamic map updates with traffic congestion information (e.g. for truck platooning management). The use of Internet based services is one of the key elements for advancing the services and adoption by a much wider audience. There are multiple heterogeneous technologies that provide communication among vehicles and between vehicles and the outside infrastructure environment. Such technologies include, but are not limited to, satellite, cellular, Wifi (e.g. 802.11p), dedicated short-range communications (e.g. wireless, NFC, BLE) and on-board modules.

Internet connectivity of vehicle is a major concern for potential vulnerability posing a potential target for unauthorized entry into the vehicle's infrastructure. This could happen, for example, by leveraging access from higher layers of the architecture and advance through interconnected systems to the lower critical layers of the vehicle, in order to gain full control.

Key research activities are:

- Monitoring, detection and mitigation of security issues on communication protocols that occur due to external, malicious activities
  - Detection of misbehaviour on communication channel
  - Mitigation of vehicle's external communication network injection attacks
- Segregation and isolation of functional layers of vehicle's internal communication architecture
  - contextually adjust or restrict control policies and permissions among interconnected vehicle components
- Link with higher network level, ITS: How to design solution that isolate internal network (vehicle) to outside network (infrastructure)?
- Safe integration of security solutions - Security and privacy control methods when introducing new solutions, for all stakeholders in the logistics value chain: secure interfaces between vehicles and infrastructure, certificates between vehicles and data/service providers, data/service providers data handling of user data
- Security certification scheme for third party evaluation of various security solutions and implementations
- Certificate management and distribution including certificate revocation lists

3.3. Secured operations in an unsecure environment

Transportation and logistics companies shouldn't expect government to take a leading role in executing supply chain security, although they will continue to regulate security measures. Transportation and logistics companies will need to work together with governmental institutions to develop new security standards that are not only effective, but also efficient.[6]

Key research activities are:

[6] PWC, Transportation & Logistics 2030 Volume 4: Securing the supply chain

- Trusted vehicle data for the operation: Vehicle information on speed, distance and engine operation could be exchanged between firms or towards public authorities for billing, regulatory inspection or fiscal accounting purposes. The integrity and privacy of this data needs to be safeguarded.
- Safe and trustful data sharing for carriers: Carriers may want to share data about loads for collaboration purposes, but would be afraid to do so because of privacy or liability concerns.
- Define level of measures: Identify and define the right level of security preparation in processes and operations, such as intelligence, education, methods, counter measures.
- Define type of actions: Safe managing of action for improved security within the process and operation, such as counter measures, inventories, access control, and transport equipment.

3.4. Secured ownership in an unsecure environment

Transportation and logistics companies will need to work together with governmental institutions to develop new effective security standards.

Key research activities are:

- Improving the ownership security: Develop and support proactive method's and actions and to improve ownership security by partnership with suppliers, partnerships with standard setters and authorities and SCM (Security Compliance Manager) security standard development and implementation.
- Definition of models for data governance: define how to structurally govern the treatment of data related to automotive platforms for a trusted data management

Expected impact and EARPA contribution

Impact of cyber security research and development

The impact is the improvement of industry and product resistance and resilience to threats and attacks through technological and human prevention techniques. Ultimately it protects businesses against significant productivity losses. Indeed consequences of unsafe product in the automotive industry (but not only) are in millions of devices to be recalled. At value chain level, it will reduce the risk of potential market fragmentation and allows to fully benefit from the booming of the cyber security market.

EARPA's intended contribution in automotive cyber security

The deep knowledge of the automotive industrial context in terms of economic, technological and innovation culture together with on one side cutting edge academic background and on the other the application research and development in the field of electronics, logistics, security, communication… places EARPA as a cornerstone in the EU context to address together with industries, end-users and policy makers the challenges of cybersecurity.

A strong impact will be reached with EARPA by gathering the stakeholders along the value chain of cybersecurity in the automotive sector. Through EARPA, we target the reduction of market fragmentation by supporting the establishment of standards encouraging permeability with other sectors (e.g. banking, electronics manufacturers…). Such approach is done for example in the field of electro-mobility by integrating the expertise on environmental assessment to meet societal and political requirement of solutions.

The resilience and resistance to threats and attacks is higher with safer technological solutions but requires ultimately to involve all the users (including manufacturer employees) to ensure the acceptability of solutions and the protection efficiency at each step of the process. Indeed, security in general, even when we are relying on technologies, is ultimately ensured by our own behaviour

as private persons … a very similar approach as in safety in mobility - a sector within which EARPA does not need to demonstrate its added value!

For further information, please contact our contact persons of the Cross cutting activity on Cyber Security:

Contacts

Bernard Strée
E: bernard.stree@cea.fr
T: + 33 4 38 78 09 35

Anders Johnson
E: Anders.Johnson@sp.se
T: + 46 10 516 59 72

More information at our website: www.earpa.eu