Talk abstracts of the

2024 Workshop on Security Frameworks

"Privacy Enrooted Car Systems"

*The **Privacy Enrooted Car Systems (PECS)** project addresses the pressing issue of weak privacy control for drivers in modern vehicles. Evidence suggests that car brands harvest diverse personal data from drivers, often raising concerns about full compliance with the General Data Protection Regulation (GDPR). PECS revolutionizes the automotive ecosystem by taking a user-centric approach to tailoring **soft and hard privacy measures** and empowering drivers over their personal data. Soft privacy is enhanced through an innovative PECS interface that allows static and dynamic control of personal data. Drivers can decide what to share, with whom, and when, while monitoring data flows during runtime using multisensory media techniques. Hard privacy is bolstered by obfuscation methods such as **Federated Learning (FL)**, which prevents outbound data flows during model training, and **Secure Multi-Party Computation (SMPC)**, which ensures data remains undisclosed during interactions with external parties. Groundbreaking in its approach, PECS introduces **steering wheel haptic feedback** to inform drivers about unwanted data flows that contradict their set policies—an unprecedented solution in automotive privacy. Developed by academic institutions UNICT and UNIMORE, and tested in MASA-UNIMORE's operational environment, PECS reaches TRL7 and offers open-source, high-impact solutions. It positions Europe as a leader in automotive data protection and paves the way for new business opportunities and privacy-enrooted services, such as apps for dating, praying, or political debate.*

Giampaolo Bella, University of Catania, Italy: *"Why PECS, what is PECS"*

I will be presenting the motivations for the project along with a justification for the individual packages in its work plan.

Mirko Mangano, University of Catania, Italy: *"PECSi Policy Engine: PECSi Policy Engine: Enhancing privacy through effective privacy policy formulation"*

Effective privacy policy management is vital in safeguarding user privacy, especially in complex systems like modern vehicles. Within the PECS Project, the PECSi Policy Engine leverages the OASIS XACML 3.0 Standard to perform core Privacy Policy Operations like administration, enforcement, decision and retrieval. While it is specifically designed and developed for the automotive scenario, it is easily adaptable to many others, including for example smartphones. PECSi ensures robust privacy controls by continuously monitoring third party software and detecting potential violations. In this presentation we delve deeper into the Policy Engine architecture, its key components, data flow and how the potential violations are communicated to the end user in the specific context of User-Centered design in the automotive domain.

Gabriele Veneziano Broccia, University of Catania, Italy: *"*PECSo-SMPC: A Secure Multi-Party Computation Approach*"*

Sharing data anonymously is a crucial aspect of today's privacy scenario. The PECSo-SMPC application, developed within the PECS Project, utilizes Secure Multi-Party Computation (SMPC) to protect sensitive information during the calculation of aggregated values, such as the average speed of the vehicles, without revealing individual data, ensuring compliance with Tier-1 standards of Privacy-Enhancing Technologies (PETs). Using arithmetic secret sharing, PECSo-SMPC maintains privacy in an efficient manner by allowing secure computations. The original solution was based on the EasySMPC project, but was then adapted to work on an Android platform, therefore some porting effort was made for the solution to work with platform-specific libraries and tools. Additionally, EasyBackend is used to provide communication among participants via HTTP services to facilitate data exchange.

Sergio Esposito, University of Catania, Italy: *"PECS Objectives and Architecture"*

This talk explores the key privacy challenges in the automotive ecosystem and presents the PECS framework as a robust and comprehensive solution. We begin by examining the growing need for a sleek, intuitive user interface that enhances transparency by displaying the permissions applied to all vehicle applications. Next, we explore the architecture of PECS, outlining its core components, their functionalities, and their interactions. Finally, we highlight how PECS empowers users to control their data-sharing preferences and ensure data protection through its innovative 3-tier compliance system. This system offers a standardised framework that simplifies the development of PECS-compliant applications, enhancing data protection while enabling users to select their preferred methods for safeguarding their data.