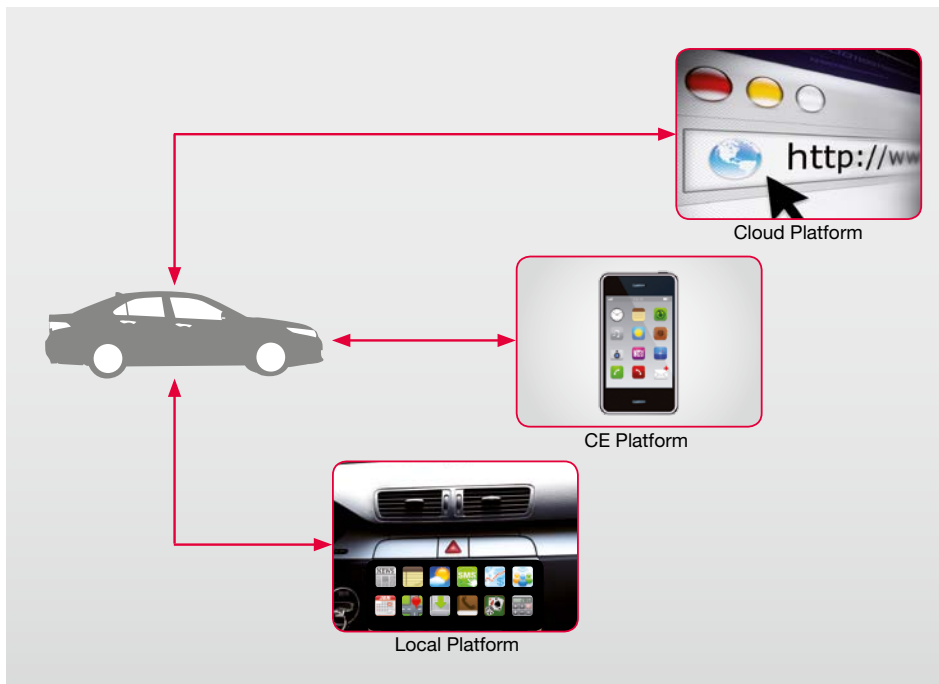


Application Control Unit Implements Security for Connected Cars



Benefits:

- » **Rapid and secure Rollout of new Usecases to fit the drivers needs**
- » **Easy maintenance of the infotainment platform since regular security patching of applications is not mandatory for the safety of the car**
- » **No special hardware required for secure storage of cryptographic keys and routines**

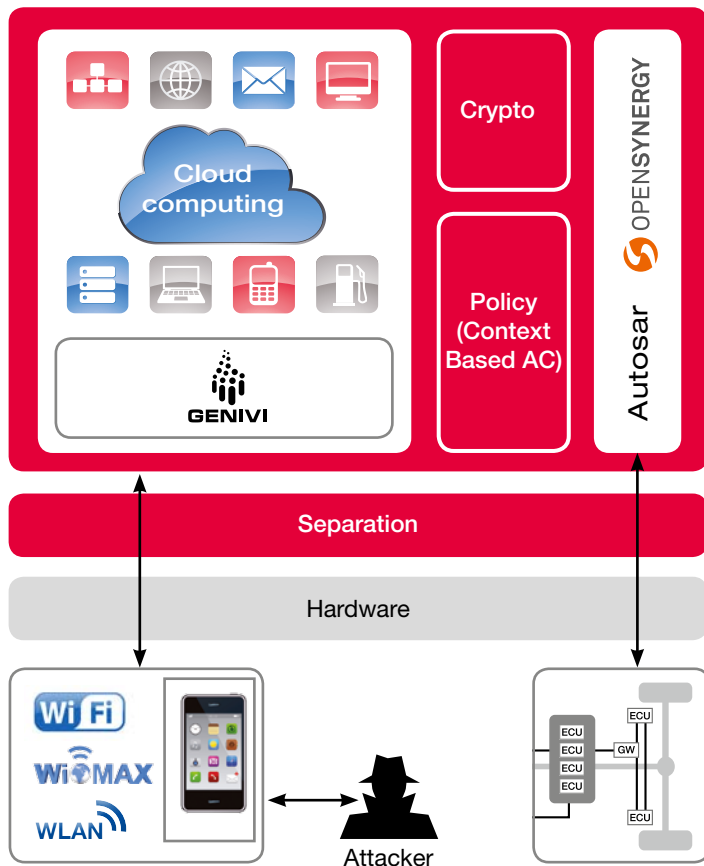
Modern vehicles leverage the power of internet applications inside the car to provide drivers with new options for the flexible selection and use of OEM applications and services tailored to suit driver needs. Such platforms use consumer operating systems like Linux or Android. As a consequence all vulnerabilities of those OS are available in the car and can be exploited by malicious applications and services.

Therefore secunet has developed a security framework, the application control unit (ACU) the security functionality is independent from the applications and guest operating systems and thus it protects the vehicle network even when unknown malware tries to access the car.

Features:

- **Policy check:** A set of rules are derived from the existing specification of the vehicle's internal network controls. The Policy receives commands from applications and checks this command against the rules. The rules can be based on any information that is available on vehicle bus systems like CAN. If the policy is violated, the commands are not transferred to the vehicle network.
- **Active Adjustment:** If a policy violation reveals an attack, policy initiates measures to disable the less trusted code causing the attack; the policy can restart the guest operation system or reboot from a trusted image.
- **Policy update:** If the vehicle network is changed or a new generation of applications is introduced, encrypted and signed new policy files can be rolled out in the field to adjust the security according to new needs.
- **Cryptography:** A set of methods provides standard cryptographic services like signature verification and secure key storage or support for virtual private networks. It includes interfaces for Signature Verification Message Digest computation and Encryption/Decryption.
- **Separation:** A software-based isolation technology with high assurance regards its capability of partitioning computing and hardware resources. Infotainment operating systems have only access to peripherals that are assigned to them at compile time of the platform software.

Resulting Architecture



Benefits of secunet ACU

- supports well modular platform architectures
- supports browser based Head Units, the tethering of consumer electronics (CE) devices like smartphones and embedded platforms
- malware and errors in the consumer operating system or applications cannot propagate into the vehicle networks
- policy, cryptographic keys and routines are independent from applications; thus, malware cannot affect the protection mechanisms of the secunet ACU
- allows updateability of its policies thereby covering newer attack vectors or when platform is updated or features are added
- secure cryptographic routines can be implemented only once and can provide cryptographic services to applications while secrets are not accessible for the applications
- by providing the same high level of security with any set of applications running in the infotainment head unit, the opening up towards more IVI applications (testing issue) and less trustworthy apps (as in appstores) is enabled by ACU
- supports also two controller approach to realise separation

Communication Model:

- » ACU uses sockets to communicate between the infotainment and the vehicle network

Micro Operating System Platform:

- » COQOS from OpenSynergy, that is certifiable according to safety standards like DO178b and security standards like common criteria up to EAL7
- » further POSIX compatible Micro OS and separation kernels available on demand

Supported Hardware:

- » ARM Cortex A8
- » other hardware on demand

Supported Boards:

- » Freescale i.MX51
- » Fresscale i.MX53

Guest Operating Systems:

- » Android 2.1
- » higher Android versions on demand
- » other Operating Systems like Genivi compliant Linux on demand

Supported Cryptography:

- » based on Openssl; other crypto libraries on demand
- » RSA with key length up to 4096
- » SHA1 (Android compatible); longer hash values on demand
- » AES 128-bit-CBC, longer key length values on demand

Technology Provider:



More Information:
www.secunet.com

secunet

secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen, Germany

Phone: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-mail: info@secunet.com
www.secunet.com