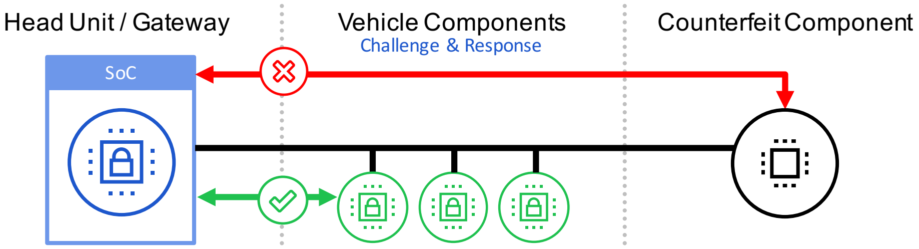
Rambus

SECURITY • CRYPTOGRAPHY
CryptoFirewall
Use Case

Vehicle Equipment Secure Authentication with Rambus CryptoFirewall

The use of stolen and counterfeit automotive components has increased significantly in recent years. A wide range of grey market devices can be found powering high-value modules such as in-vehicle infotainment systems and headlights, as well as in critical safety systems including airbag modules, braking modules, and powertrain controls. The deployment of stolen or sub-par counterfeit components is likely to negatively impact driver and passenger safety, quickly erode OEM and supplier brand equity, and decrease sales of authentic aftermarket modules.

Addressing the proliferation of stolen and counterfeit automotive systems is critical. The Rambus CryptoFirewall platform is a commercially-available, proven solution that can determine component authenticity and identify stolen or improperly removed devices installed on another vehicle.



The CryptoFirewall products have a simple but very secure design consisting of both firmware and a discrete security chip. The firmware is integrated into an ECU with access to the in-vehicle network (such as an in-vehicle infotainment unit or gateway) which then challenges the security chip embedded in a vehicle component. The security chip response to the firmware determines authenticity and device lineage. This authentication process can be performed across any interface protocol, such as CAN or Ethernet, allowing for simple integration into any vehicle architecture. Our unique CryptoFirewall component authentication products create value throughout the vehicle lifecycle, maintaining aftermarket revenue for Tier One suppliers and OEMs, reducing liability and the potential for brand erosion, and supporting a safe environment for drivers.

Benefits

- Commercially-proven technology in high volume markets
- Drives revenue of aftermarket components, reduces safety risks, and addresses threats to brand equity
- Simple integration through vehicle architecture and network agnostic design

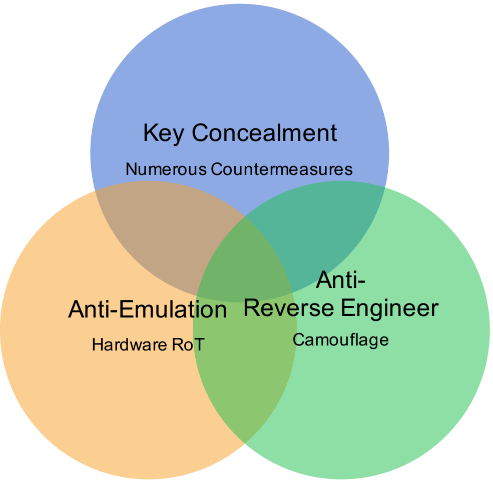
Verifier Firmware

- Ideally run the firmware in one central place and use it to verify all security chips in system
- Protocol between verifier and security chips contains no secrets
  - Does not need to be encrypted
  - Immune from both replay and man-in-the-middle attacks
  - The protocol can be packetized, routed, and relayed
- CPU requirements for firmware:
  - Uses ECDSA P-192 for certificate check
  - Uses AES and SHA256 for authentication
  - 32-bit class CPU (e.g., ARM946ES @192MHz)
  - Minimum 256kB for nonvolatile and RAM

Security Chip

Key tenets of our chip design philosophy:

Difficult to obtain secret-key data and/or analyze the chip's internal operations



Impossible to mimic chip performance with a low cost MCU + software

Difficult to reverse engineer the chip with existing tools and equipment

Threat Vectors Addressed Include:

- Basic Theft
- Decompile MCU firmware
- Decompile verifier firmware
- Protocol attack
- Cryptanalysis
- Power analysis side-channel
- Environmental attack

rambus.com/automotive

© Rambus Inc. 1050 Enterprise Way, Suite 700
Sunnyvale, CA 94089 • rambus.com