VicOne | TRUSTONIC

Why Are an IDPS and a TEE Necessary for Software-Defined Vehicles?

The modern software-defined vehicle (SDV) offers a safer, connected, and autonomous driving experience for the automotive industry. But with millions of lines of code and various connectivity interfaces, an SDV is exposed to more risks.

A Trusted Execution Environment (TEE) provides a secure enclave to isolate and protect customer code and data. Its ability to run trusted applications (TAs) can enhance the security and integrity of services such as an intrusion detection and prevention system (IDPS) by providing secure storage and enabling secure communication.

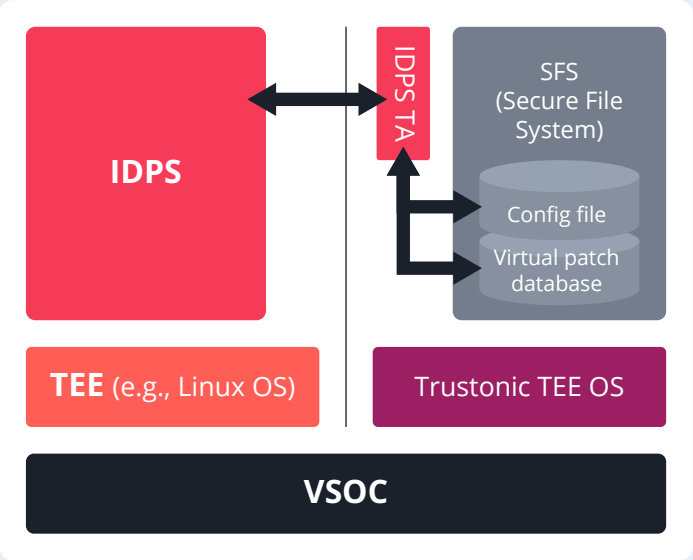
An IDPS helps vehicle manufacturers fulfill UN R155 requirements by detecting and monitoring suspicious activities in electronic control units (ECUs). It also performs real-time protection once a cyberattack is identified and plays a sensor and data aggregator role to communicate with the vehicle security operations center (VSOC) for further data forensics and advanced analysis of threats.

The Power of VicOne + Trustonic: Complete Coverage Using Secure by Design and Cybersecurity

A robust security foundation is a core part of any new vehicle, enabling OEMs to deliver their next-generation experiences with the confidence that their customers will be fully protected. VicOne xCarbon, with virtual patches and selected expert rules, helps protect vehicles against threats that use trusted credentials or exploits. For example, if an authorized component conducts suspicious activities, xCarbon detects and blocks it. Thanks to VicOne's threat intelligence, the virtual patches and expert rules are always updated. Trustonic's TEE provides tamper-protected storage for xCarbon rules, ensuring that only rules signed by a trusted VSOC are accepted by the vehicle. Similarly, traces generated by xCarbon are stored and processed within the TEE, ensuring any confidential data is properly managed and giving high assurance to the VSOC of data received.

Example Architecture

- The IDPS config file and virtual patch (or rule set) database can be encrypted and securely stored by Trustonic's TEE.
- The IDPS sends a command to the IDPS TA to get the config file and then feed to the IDPS engine.
- When deploying a new virtual patch, the IDPS sends a command to the IDPS TA to securely store into database within SFS.



Use Cases for IDPS and TEE

VicOne and Trustonic allow you to create an IDPS TA and add features over time:

- Store the policy in SFS.
  - The IDPS fetches it periodically (avoiding file system attacks in a normal OS).
  - Updates are provided as signed files by the IDPS.
    - The TA validates the signature and version before applying an update.
- Store the logs/database in Secure Database (itself in SFS).
  - The IDPS sends messages to add.
  - The TA enforces an append-only policy.
  - The TA provides local query/analysis capability.
- Sign and/or upload logs.
  - The TA has a signature key to sign logs.
  - The TA can link to device attestation to prove a device is legitimate.
  - The TA can sign individual messages or provide a secure TLS tunnel to the back-end server.
- Monitor the IDPS app.
  - Require the IDPS app to send a periodic heartbeat, with any miss being flagged in the TA.
  - Avoid disablement attacks.
- Utilize deep IDPS integration.
  - The TA/driver monitors the IDPS app directly.