cloakware® *for automotive* | by irdeto

Component Datasheet

SECURE ENVIRONMENT

Safeguarding all assets from perimeter security breaches

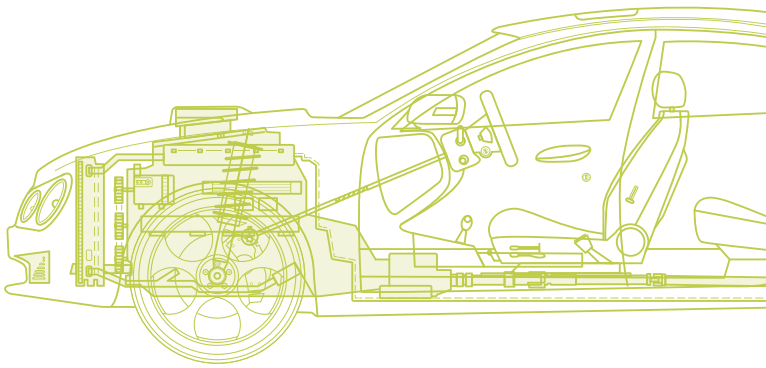
It's challenging enough to secure cloud software from attacks over the internet. But securing a car is orders of magnitude harder with a car sitting in a hacker's driveway. A determined hacker with physical access to a vehicle can do many things to gain root access and compromise system security: extract firmware images, reverse-engineer software, reactivate debug software and so on. History is littered with examples of successfully hacked devices – from network routers through medical devices to credit card systems.

That's why we've created Irdeto Secure Environment with the assumption that a hacker *already* has root access — the highest of all system privileges. Unique to the automotive industry, Secure Environment forces hackers to expend an improbable amount of effort to break into vehicles, making them move on to softer targets that aren't as well protected. Its mutually reinforcing technologies offer unparalleled protection:

- Disables execution of anything except OEM-authorized software.
- Removes debugging capability and memory examination.
- Encrypts binaries and file content.
- Hides decryption keys.
- Makes reverse engineering virtually impossible.
- Monitors hacking attempts and supports a range of OEM responses.
- Collects security incident data for post-mortem analysis.

FROM THE INSIDE OUT

Secure Environment uniquely assumes perimeter security has been compromised and focuses instead on protecting everything else. It safeguards critical files, protects application data, and prevents hackers from adding malicious code, modifying executables and scripts, and reverse engineering. What's more, it uses renewable security to frustrate hacking attempts by continually resetting hacker knowledge to ground zero. And, while a full cybersecurity audit is recommended, Secure Environment can be dropped into a system still under development.



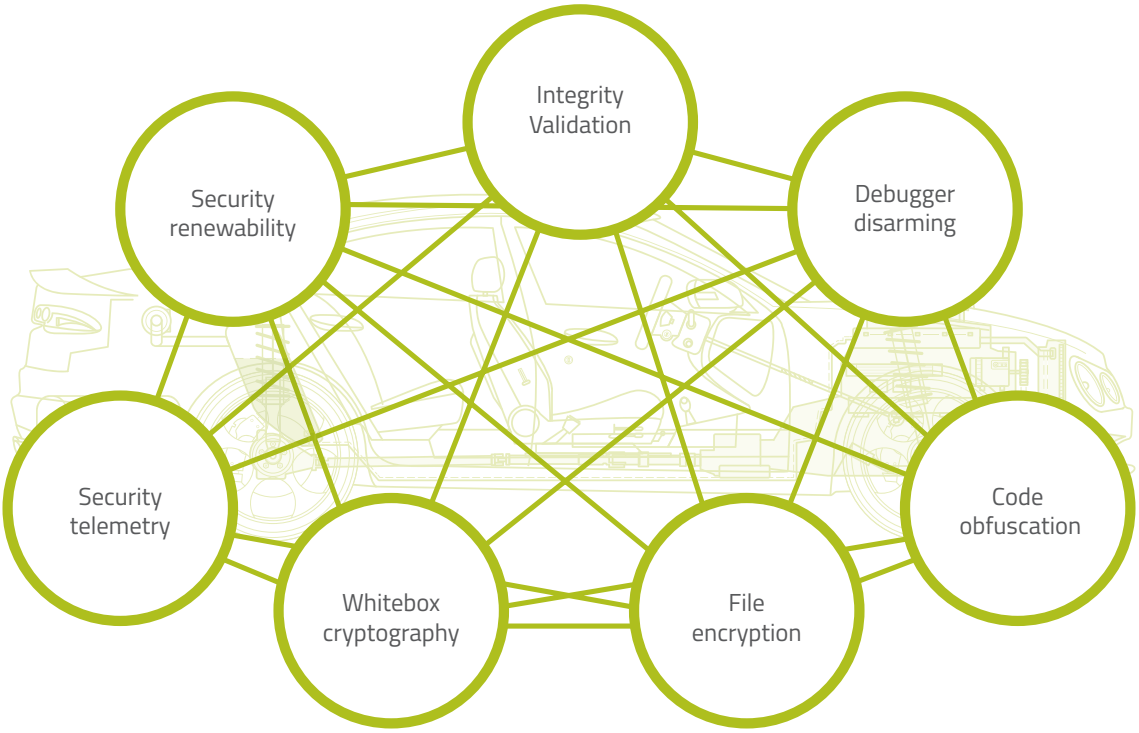


Figure 1: Secure Environment technologies reinforce each other against attack, making it exponentially more difficult for hackers to cause damage.

MUTUALLY REINFORCED

The anti-hacking technologies of Secure Environment mutually reinforce each other to make it exceedingly difficult for hackers to leverage any vulnerabilities. Instead of jumping one barrier, hackers need to jump numerous barriers, simultaneously. Integrity validation, code obfuscation, file encryption, whitebox cryptography, renewable security, and several other technologies work together to encourage hackers to seek softer targets — even when hackers have unlimited physical access. What's more, Secure Environment makes reverse engineering extremely difficult whether the module under attack is running or not.

CONNECTED AMPLIFICATION

When vehicles are connected, Secure Environment provides even more options to prevent damage from security breaches. A connection to our operations center provides security telemetry — reports of hack attempts — allowing automakers to eavesdrop on hacker probing. Secure Environment lets automakers swap out software from underneath hacks in progress, indefinitely extending the time required to break into a system. It also supports a range of OEM-defined responses and contains the damage scope of hacks to the fewest number of vehicles.

Irdeto Cloakware for Automotive is a comprehensive solution that combines innovative, patented technologies and cybercrime services to address a variety of security challenges in a car. It provides automakers and tier-one suppliers with a secure, tamper-proof environment for vehicle software that is virtually impossible to reverse engineer. For more information, please refer to the datasheets for the solution components at irdeto.com