

PRE-EMPTIVE VEHICLE PROTECTION/ ELEKTROBIT EB SOLYS

Securing the cybersecurity health of production vehicles

As vehicles support an increasing number of connections, more avenues open up to hackers. With the cost of malicious hacks ranging from vehicle-line recalls to consumer injuries, the end result can be irreparable brand damage. Most auto cybersecurity companies merely provide perimeter detection, which unfortunately does little to protect vehicles from a dedicated hacker's onslaught.

That's why Irdeto has teamed up with the trusted, automotive supplier Elektrobit to create a new cybersecurity solution specifically designed to address automotive's unique challenges. This product secures the cybersecurity health of vehicles, before hackers learn about its systems. It limits any damage caused by hackers that break past a vehicle's defenses. And it lets OEMs fight back.

- Detects hackers "sniffing" at modules, probing for possible entry points.
- Finds illegal and unanticipated D-Bus calls as well as fuzzing attempts.
- Hardens modules to prevent reverse-engineering.
- Prevents execution of unauthorized software and scripts.
- Secures module software from modification, even when hackers have gained root access.
- Frustrates hacker attempts to understand systems with renewable security.
- Collects post-mortem data on hacker activity.
- Shuts down hacker progress (on OEM authority) and logs activity for legal action.

This new cybersecurity solution combines the unparalleled security of Irdeto's Secure Environment with the deep inspection capabilities of Elektrobit's EB solys to fully lock down automotive systems. It helps automakers avoid bad publicity, recalls and lawsuits.



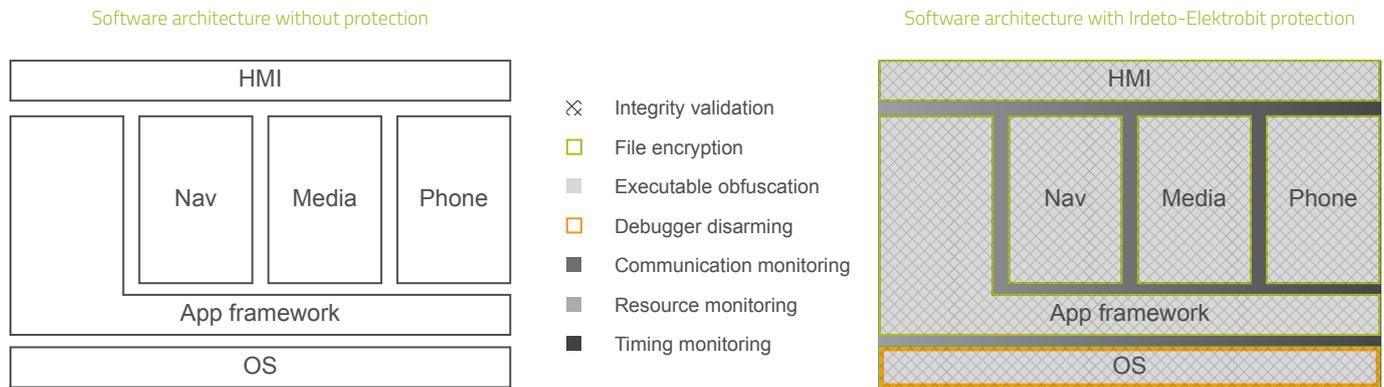


Figure 1. The Irdeto-Elektrobit security solution completely protects all components in the software architecture.

VEHICLE STATE MONITORING

The Irdeto-Elektrobit solution monitors several systems to detect when hackers are “sniffing” around or checking systems for vulnerabilities. It examines D-Bus messages, memory usage, CPU load, IPC traffic, and other system metrics to detect illegal calls, erroneous data and fuzzing attempts. It supports a range of responses from activating honeypot features to system lockdown. Better still, it keeps system load to a minimum, until an intrusion attempt is detected. At this point monitoring increases to capture detailed cyber forensics.

SECURE ENVIRONMENT

Irdeto Secure Environment prevents hackers who have cracked perimeter security from causing damage – stealing user data, overriding engine parameters, installing malicious software, etc. – in a number of ways. It safeguards critical files, protects application data, and prevents hackers from adding malicious code, modifying executables and scripts, and reverse engineering. It also boasts renewable security, which continually starts hackers back at ground zero.

AUTOMOTIVE FOCUSED

The Irdeto-Elektrobit solution is designed specifically for the security challenges found in the automotive industry. By actively shutting down hackers before they learn too much and mitigating damage once they do, it prevents hacks from moving beyond a single vehicle. It also supports security policies on a per-vehicle basis as well as OEM-specific responses. With the Irdeto-Elektrobit solution, all of the automotive hacks published to date would have been stopped dead in their tracks.

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