whiteCryption®

Securing the Connected Car

> *"eCommerce Times says the Internet of Things is expected to be a US$7 trillion market in six years (2020). IDC estimates there will be approximately 212 billion things globally by the end of 2020."*

whiteCryption Benefits:

- Software-based Solution
- Lower Bill of Materials Cost
- Lower Power Requirements

Stop Tampering and Reengineering

whiteCryption's, Cryptanium™, protects code, stops theft of IP and reverse engineering and keeps cryptographic keys and data private. It adds a layer of protection to help avoid the limitations and risks involved with conventional application security. Integrating with existing applications, our high security software-solutions deliver the next level of obfuscation, self-defense and tamper resistance technology against tampering and piracy. Securing your apps has never been easier.

Why the Next Level of Protection?

Cars are becoming more connected with each new model, driven by infotainment, navigation, safety, diagnostics, and fleet management. The devices and applications that help cars stay connected can introduce vulnerabilities and consumers are concerned about data privacy. The sheer diversity of connecting devices puts tremendous pressure on automobile manufacturers and users. The potential for data leaks will only intensify the need for next-generation tools that can handle today's demanding security landscape.

Examples of vulnerabilities and security risks:

- Lack of sufficient bus protection. The signaling and communications bus, CAN bus, lacks the necessary protection to ensure confidentiality, integrity, availability, authentication, and non-repudiation.
- Weak authentication. It's very possible to re-program the ECUs illicitly.
- Misuse of the protocols. Denial of Service (DoS) attacks via CAN; malicious error messages can be used to trigger the fault-detection-mechanism in CAN.
- Poor protocol implementation. For example… reprogramming the ECU while the vehicle is moving is not allowed, however it is possible to launch commands that disable the CAN communication and set the ECU into programming mode while the vehicle is moving.
- Information leakage and corruption. Hackers can manipulate the diagnostic protocol by sniffing ordinary diagnostic sessions and injecting modified messages.

whiteCryption®

> *"Consulting firm McKinsey & Company released findings that showed consumers are concerned about data privacy when it comes to the connected car and the information it gathers. Forty-five percent of new car buyers in the US are reluctant to use connected car services because of data privacy fears, and 43 percent are afraid that hackers will be able to actually manipulate safety features such as braking."*

Improve Security, Reliability and Manageability

whiteCryption's enterprise-level application security provides the next layer of protection to help avoid the limitations and risks involved with conventional application security. whiteCryption delivers a unique, comprehensive approach that enables enterprises to capitalize on the Internet of Things while making sure their applications are secure. whiteCryption provides protection for the entire application and shields the entire software, including the data it processes.

Integrating with your existing applications, our high security solutions deliver the next level of obfuscation, self-defense and tamper resistance technology against piracy.

Let whiteCryption Help You Protect Your Connected World

whiteCryption's Cryptanium is the best solution for Integrating with your existing applications delivering the next level of obfuscation, self-defense and tamper resistance technology against piracy. Further, our solution will increase your efficiency — saving money and reducing limitations and risks. Connecting your car has never been easier.

For more information about whiteCryption software and data protection solutions, visit www.whitecryption.com.

whiteCryption secures your connected car both at the manufacture level using Cryptanium Code Protection and the user level using Cryptanium Secure Key Box.

Mobile Apps to Access

- Mobile App Unlocks Vehicle (Code Protection and SKB)
- Remote Start
- Status of Vehicle
- Authentication

(Smartphone – Apple iOS, Android)

Operation of Car

- Over the air updates (OTA) & status
- Hacking into systems – threat to car manufacturer (Code Protection)
- Vehicle data – threat to user (Data Protection – SKB)
- GPS
- Speed
- Driving habits

Infotainment

- Apps Integrity (Code Protection)
- Media (Data Protection – SKB)