Sectigo IoT Use Case: Firewall for Automotive Gateway ECUs

Modern automobiles are run by dozens or even hundreds of electronic control units (ECUs), and their electronic subsystems and associated network interfaces are rapidly increasing in complexity and connectivity. At the same time, cyber-attacks on connected cars are on the rise via a variety of different routes. That means today's vehicles are increasingly vulnerable and require state-of-the-art embedded device security to help ensure the highest standards of safety, security, and compliance.

Connected cars utilize an Automotive Gateway ECU to manage communication between in-car networks and external systems. Similar to a home gateway, an Automotive Gateway ECU isolates internal ECUs from attack, but in doing so has become a focal point for hackers. As a result, automobile manufacturers and OEMs need to:

- Protect Automotive Gateway ECUs from attack
- Enforce firewall filtering rules to control what network traffic is forwarded to internal networks

Sectigo can help. Our Icon Labs Embedded Firewall SDK is designed specifically to meet the requirements of embedded and IoT systems. Like any firewall, it enforces defined security policies, limiting communication with vehicle control systems to a small set of trusted hosts and blocking attacks from any other source; however, the Icon Labs Embedded Firewall SDK also allows you to layer multiple types of filtering. That improves protection for embedded devices, maximizing driver safety, and helps prevent the loss of intellectual property, disruption of services, or proliferation of an attack to other systems.

Leveraging Icon Labs Embedded Firewall SDK for Automotive Gateway ECUs will enable your security team to benefit from:

- **Configurable filtering policies.** With Icon Labs Embedded Firewall SDK, each packet received by the gateway is inspected before being passed up the TCP/IP stack. As a result, many attacks are blocked before a connection is even established.

  You can combine multiple filter types, including: static/rules-based filtering to block packets based on configurable rules; dynamic filtering/stateful packet inspection (SPI) to block packets based on connection state; and deep packet inspection, allowing control and validation of each individual field within the message.

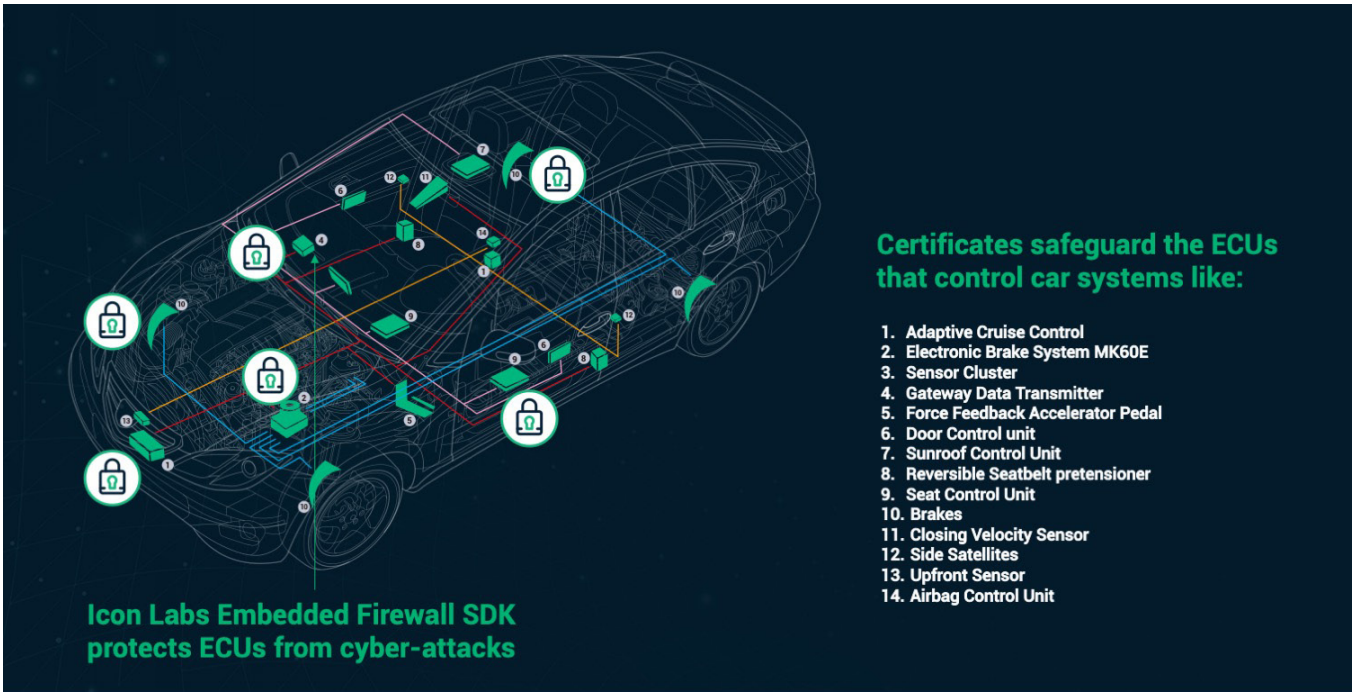
  Deep packet inspection filters messages based on their type, contents, and source, and threshold-based filtering blocks packets based on threshold crossings to protect against denial of service (DDoS) attacks, broadcast storms, and other packet flood conditions.

- **Logging and alerting.** Icon Labs Embedded Firewall SDK automatically maintains a log of security events, policy violations, and changes to firewall policies, enabling support for command audit requirements. These event logs can be used for forensic investigation to determine the source of an attack.

- **Management system integration.** Icon Labs Embedded Firewall SDK integrates with the Embedded Agent, enabling remote management from Security Information and Event Management (SIEM) systems. This integration provides centralized management of security policies, situational awareness and device status monitoring, and event management and log file analysis.

- **Intrusion detection and prevention.** With Icon Labs Embedded Firewall SDK, all unused ports and protocols are blocked, limiting the attack surface potential hackers can exploit. Logging packets that violate configured filtering rules enables detection of unusual traffic patterns, traffic from unknown IP addresses, or other suspicious behavior.

With Icon Labs Embedded Firewall SDK, you can rest assured that all embedded automotive systems have the highest levels of security, not only today, but for the lifetime of the vehicle. It is offered as a stand-alone product or as part of the Sectigo IoT Identity Platform, which includes a broad set of embedded device-hardening technologies along with third-party certificate issuance and management purpose-built for connected devices. Choosing a partner with Sectigo's experience, scale, and commitment to embedded device security gives you peace of mind, so you can stop worrying about cyber-attacks and instead concentrate on what you do best—running your business.



About Sectigo

Sectigo provides purpose-built, automated PKI solutions that secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit **www.sectigo.com.**

