CERTICOM WHITEPAPER SERIES

Automotive security and trust management: The case for PKI

Jim Alfred, Vice President, BlackBerry Technology Solutions, Certicom

BlackBerry | certicom

Executive Summary

Connected vehicles are using an increasing amount of electronics and these electronic systems are becoming more and more complex. Securing these vehicles is a safety-critical concern, and a federated PKI (public key infrastructure) model for trusted key management is a sound choice for ensuring robust vehicle security. This paper presents the security requirements for vehicle on-board electronics networks and how to meet them with Certicom's security technology, managed PKI offering, and expertise in strong, efficient key management.

Security of Connected Vehicles

The security of connected vehicles is a growing industry concern. The complexity of modern on-board electronics coupled with the integration of wireless interfaces, downloadable applications and connected consumer devices has expanded attack surfaces. The increasingly electronic nature of a vehicle's control systems — brakes, steering, engine controls, even door locks — has vast safety implications. Nearly every week brings a new scenario that demonstrates how cyber security threats are putting safety critical and non-safety critical systems at risk.

Much literature and a few standards initiatives have been devoted to addressing this concern, though few are as ecosystem oriented as those developed for V2X/DSRC security by the Collision Avoidance Metrics Program (CAMP), a security architecture based on public key infrastructure (PKI) that is designed to address the security, interoperability, and privacy issues of ad hoc vehicle to vehicle and vehicle to infrastructure networks.

Federated PKI Model

Certicom, an applied cryptography specialist, proposes a similar PKI-based architecture to help secure on-board electronic networks. Unlike CAMP, which leverages a centralized trust model, we suggest a federated PKI model to facilitate easy adoption and implementation by OEMs and their supply chain partners.

The crux of this new architecture is the concept of trusted key managers, which reside within vehicle electronics subsystems. It leverages the security technology that many automotive silicon vendors have already introduced to the market, tying them together to solve the classic key management problem in network security with adaptations to support the unique requirements of automotive systems. Key managers use PKI technology to manage electronics module interactions, using identity to key bindings for intra-vehicle network key agreement protocols and key life cycle management. Certificates bind keys to module identities. Trust is based on module manufacturers and OEMs provisioning their systems with secure digital identities and protecting sensitive keying material.

The goal of this architecture and trust model is to provide a security framework that the entire industry can leverage. It will afford comprehensive protection of automotive electronic assets while allowing for the practical realities of the industry — complex ecosystems with multi-tiered supply chains, relentless cost pressure, and end products that require flexible long-term service options.

Other Security Tools

Cryptography is not the only tool, though it serves many useful purposes, including the protection of sensitive messages and keys and the ability to detect tampered software or messages. Likewise, the security scheme needs to include isolation mechanisms to protect the integrity of the key manager and to firewall access to safety-critical network interfaces.

A fundamental requirement is resilience — enhanced security must not disrupt the functionality or limit the serviceability of systems it is meant to protect. Thus the trusted key manager must be able to coordinate key distribution for a closed network in a normal operating mode while supporting join and re-bind operations to allow the installation of new components in an authorized service mode.

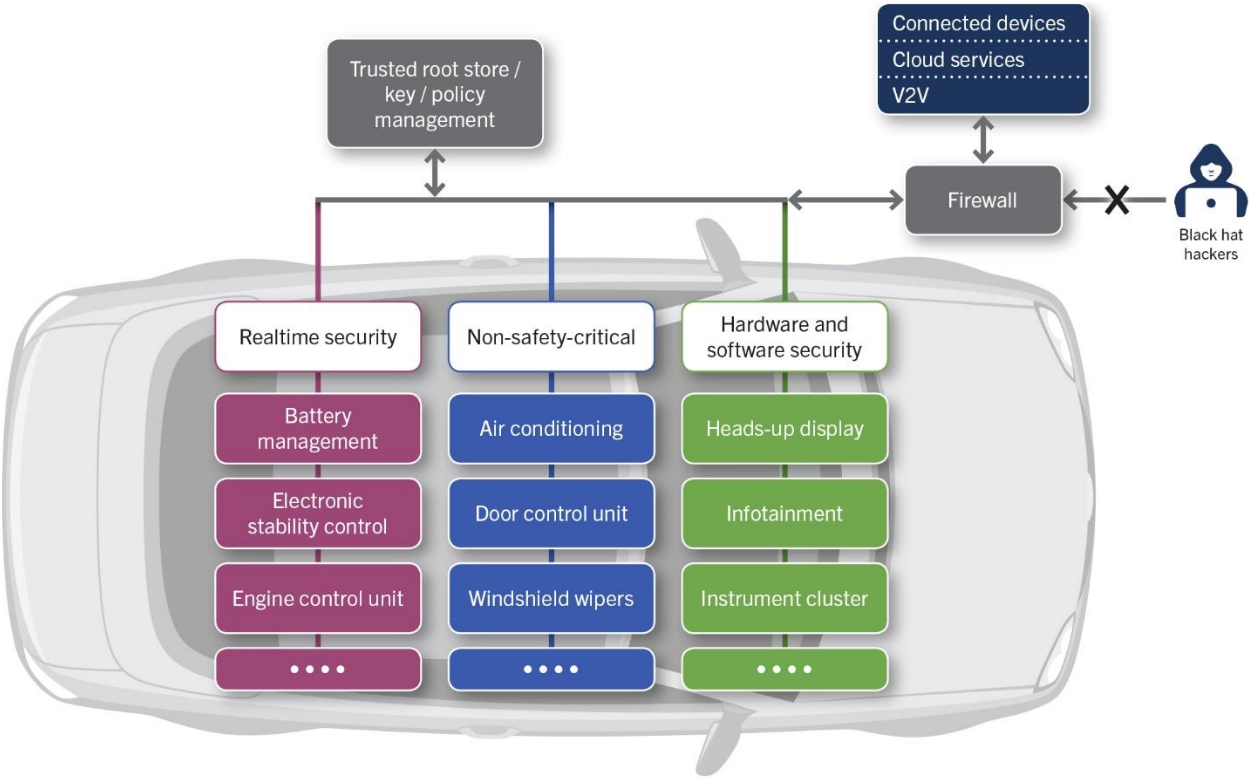

Figure 1: Protecting a vehicle's on-board electronic networks with PKI

Proven Use of the Federated PKI Model

The concept of a federated PKI model is not new. It has been proven in other industries and the suggestion is that it now be applied on a micro network scale to on-board electronics, with the vehicle communications subsystems as individual security domains. The trusted key manager operates locally, managing trust anchors and key distribution between nodes on automotive subsystems based on well-established cryptographic protocols, using certificates where available to map module identities to system security policies.

At its core, the architecture is little different from the well-understood key management and security protocols used to authenticate and protect message integrity and to encrypt sensitive data such as key update messages. Where module certificates are not available the key manager will support shared secret symmetric key-based system provisioning and life cycle management, affording all systems some level of protection, even for lower risk assets protected simply via software security constructs.

It is assumed that OEMs will encourage their module suppliers to participate, particularly to support the identity binding and key management protocols required to bootstrap and secure on-board electronics networks. There is also an opportunity for chip vendors to add value, particularly through hardware security enhancements such as MCUs with Secure Hardware Extension (SHE) or embedded Hardware Security Modules (HSM) capability that protect sensitive keying material.

Conclusion

In summary, while groundwork has been laid by earlier initiatives, none have yet coalesced into an actionable blueprint to secure vehicle on-board electronics networks. A federated PKI-based standard for trusted key management is the logical pathway to robust vehicle security. We believe it can serve as a blueprint for the industry, and with Certicom's security technology, managed PKI offering, and expertise in strong, efficient key management, we are keen to help the automotive industry address its security challenges.

About Certicom

Founded in 1985 with a long-term focus on Elliptic Curve Cryptography, Certicom has been awarded over 500 patents. As a leader in applied cryptography and key management, Certicom provides managed PKI, key management and provisioning technology that helps to protect customers' device firmware, applications, and long-lived assets. Certicom is a critical element of the Blackberry cybersecurity portfolio deploying the first and best in class end-to-end security solutions used in preventing product counterfeiting, re-manufacturing, and rogue network access. Blackberry Certicom's secure key provisioning, code signing and identity management solutions are field- proven to protect next-generation connected cars, critical infrastructure and IoT deployments.

www.certicom.com