MOCANA

MOCANA SECURITY OF THINGS

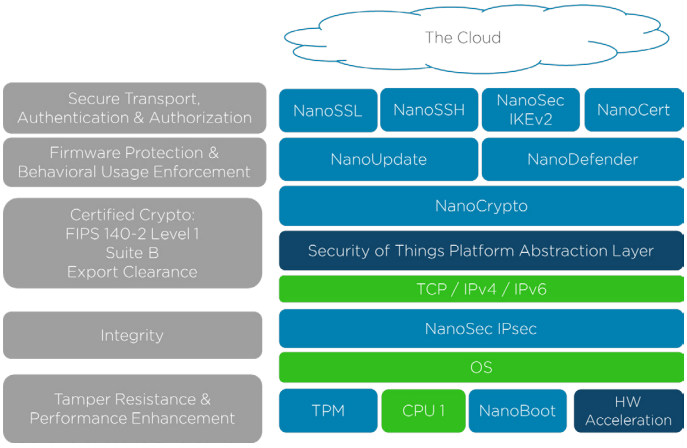
Security Solutions that Prioritize the Safety of Connected Cars

Features and Benefits:

- TPM compatible
- Secure-boot verification
- Byte-efficient code for resource-constrained environments
- Automatic certificate provisioning
- Data integrity during updates

The automobile has become so much more than just a means to get from one location to another; the infotainment system gives forecast updates and real-time traffic conditions. Car doors no longer need keys and keys no longer need to be physically inserted into an ignition. Everything is IP connected, which means that securing all the devices that run on IP is critical.

Mocana's comprehensive Security of Things Platform will cover the major areas of vulnerability in your new connected car.



Mocana's Security of Things Platform Guards Against Vulnerabilities

Secure the crypto foundation—All cryptography relies on a strong random number generator (RNG) seed. If you have a weak seed, it's an easy matter to defeat any and all measures you might otherwise take to ensure security. In addition to using a strong RNG, you should protect the device's private keys by using hardware, such as a TPM (Trusted Platform Module). Mocana crypto products provide a secure RNG seed. You can replace or strengthen Mocana's software RNG with a hardware seed. All the Mocana Security of Things Platform products that use public key encryption are TPM friendly.

Secure the boot process—To prevent tampering, you must strongly protect devices' boot processes. For all of a car's devices that have flash or reprogrammable storage, be sure to use a strong digital signature algorithm, such as ECDSA P-521. Mocana NanoBoot™ provides all the tools and firmware source code you need to perform secure pre-boot verification on your connected devices.

Deliver updates securely—USB thumb drives are convenient, inexpensive update delivery systems. But to ensure security, the data on the drive must be digitally signed in a secure, future-proof manner, the same way you've (presumably) secured the boot process. Mocana NanoUpdate™ enables automatic, secure delivery of messages and firmware images to field devices.

Contact Us

For more information on Mocana and our solutions, visit:

www.mocana.com

or please contact us at:

sales@mocana.com

About Mocana

Mocana provides high-performance, ultra-optimized, OS-independent, high-assurance security solutions for any device class. Mocana's award-winning cryptographic solutions are used in the most stringently constrained and life-critical systems by Fortune 500 companies, world-leading smart device manufacturers, and government agencies.

Secure all network services—Secure every communications system between the vehicle and the outside world. To avoid falling prey to devastating mobile system attacks, assume that links are unsecure, that data can be stolen, and that the communication scheme can be altered; and build in appropriate countermeasures. Mocana NanoSSL™ helps defeat eavesdropping on wired or wireless connections and can be used to deliver secured software packages from and to authenticated endpoints. You can further enhance security by incorporating Mocana NanoSec™, which is an IPsec/IKE solution for resource-constrained environments, and for when you need a FIPS-certified cryptographic engine.

Employ mutual authentication—In addition to securing the actual data that is transmitted to and from a smart car through the authorized cloud services, it's important that the smart car and cloud services use strong, certificate-based, mutual authentication. When both the server and client authenticate themselves to the other party, both parties can be sure that they know with whom they are communicating. With this added layer of security, infrastructure-to-vehicle (I2V) authentication prevents attackers from successfully impersonating a wireless carrier; and vehicle-to-infrastructure (V2I) authentication prevents attackers from impersonating a smart car in order to reverse engineer the cloud service with the intention of gaining a foothold that could be used to attack an entire fleet of cars. Mocana NanoCert™ Client lets you automate the certificate provisioning during manufacturing, periodically update the smart car in the field, and revoke certificates anytime.

Ensure data integrity—It is not enough to simply secure network services. You must also make sure that the data that's received has not been tampered with. For example, if a car receives mapping data from Google, you must ensure that the data is actually coming from Google. Data certification and verification is key, and multiple layers of defense, such as signing the map data to ensure that it is really safe and true map data, provide added security that is especially important in the case of self-driving cars. If there is a failure in one layer, the next layer can recover and prevent a system compromise. Mocana NanoCrypto™ provides a rich selection of cryptographic technologies, and FIPS 140-2 level 1 government-certified binaries for many popular platforms. Pair it with Mocana NanoUpdate™ to ensure data integrity during updates.

Prevent replay attacks—Although a replay attack might be amusing and harmless, such as changing the radio station, replay attacks could seriously compromise safety, such as issuing commands to open the doors while a car is moving. Other potential replay attacks are downgrading a system's firmware or transmitting outdated map data. Simply signing and securing messages isn't enough. You must employ countermeasures such as using session tokens or timestamps, limiting session times, and denying concurrent logins to a car's system. The combination of Mocana NanoBoot™, Mocana NanoUpdate™, and Mocana NanoCrypto™ provides extensive protection against replay attacks.

Prevent runtime tampering—With car systems receiving data while in operation, it's imperative that the operating systems are appropriately hardened to prevent runtime tampering. For example, Mocana offers a stronger version of Android, KeyROM™. KeyROM has strong compartmentalization, and further extends the security of Android SE. Additionally, Mocana offers fine grain control flow integrity (CFI) to prevent arbitrary code execution. Building in such security ensures that smart cars cannot be hacked and that they are safe and secure. Mocana NanoDefender™ protects against zero-day attacks by learning an application's call flow, monitoring that call flow during runtime, and stopping application execution if an unexpected system call or function call occurs.