Fortune 50 Automotive Manufacturer Secures Millions of Next-Gen Vehicles

This global automotive manufacturer was able to store, manage, and process digital certificates on 4M+ vehicles per hour / 96 M vehicles a day.

Company Overview

A global automotive leader, this company manufactures and distributes vehicles across a diverse set of commercial and consumer product lines.

Challenges

IoT devices are increasingly being used to gather data and insights into automotive system operations. With this advancement in connected vehicles comes the greater risk of compromise within these complex systems.

However, updating and patching security software can be expensive. High overhead costs quickly add up when a warranty recall is required. Additionally, there is a potential for physical danger or harm to consumers if a vehicle is hacked due to mistimed security updates.

This global automotive manufacturer recognized that their device and system compromise could be prevented by implementing strong certificate-based authentication and firmware signing within their connected vehicles. However, they had no solution in place to scale with their new fleet of connected cars — until they found Keyfactor.

Industry

Automotive Manufacturer

Employees

100,000+

Keyfactor Products

Keyfactor Command for IoT

Certificates Managing

Millions

"At this processing rate, it was estimated that the replacement for a typical two tier PKI (two chain certificates plus the end entity certificate) would operate at two million vehicles per-hour, excluding the time needed to actually issue the certificates from the certificate authority."

After analyzing the potential of serious financial consequences from warranty returns if they could not remotely update its new fleet, Keyfactor was approached to help develop a secure IoT identity platform for their future.

There are serious financial consequences from a warranty return if the automaker can't remotely update its fleet. A large automotive manufacturer recently requested Keyfactor to engage in a scenario that would push the limits of what security means, helping to determine how managing a security breach successfully from afar could work or not.

Solution

Keyfactor was challenged to secure a large fleet of simulated connected vehicles. The premise was based on a catastrophic re-enrollment scenario where the Root of Trust (RoT) was breached. The goal was to validate the ability to handle revocation & reissuance of 500 million certificates, and understand the time it would take to complete.

All vehicles required an immediate update consisting of new certificates and keys from a new CA. The update of each device's trust store would replace the compromised root and shut off trust of its certificates. Keyfactor Command for IoT served as the orchestration layer between a third-party PKI and Keyfactor Command for IoT agents deployed on each vehicle Engine Control Unit (ecu).

Keyfactor leveraged Microsoft Azure, on a single instance of Keyfactor Command for IoT running one standard-grade quad-core web server and one standard-grade 16-core database server.

The Results

Keyfactor successfully demonstrated the ability to store, manage, and report on over 211 million certificates, and provided instructions to an equivalent load of 68 million vehicle agents checking in once per-day. The aggregate Keyfactor Command for IoT processing rate with the single backend server was 800 operations per-second.

SNAPSHOT:

Why They Chose Keyfactor

1. Proven Scalability:
Ability to update 96 million vehicles per day

2. Crypto-Agility:
Securely update algorithms with certificate and PKI automation

3. Reduced Risk & Warranty Costs:
Over the air updates avoids bringing cars into maintenance shops

4. Strategic Partnership:
Combined cryptography expertize and software versus in house developed solution

At this processing rate, it was estimated that the replacement for a typical two-tier PKI (two chain certificates plus the end entity certificate) would operate at two million vehicles per-hour, excluding the time needed to actually issue the certificates from the certificate authority.

With a single backend Keyfactor Command for IoT server generating the above load, the underlying database was running at about 10% load. Performance scaled up linearly as more server capacity was added. Scaling the numbers by four times would generate a check-in rate of 3,200 per-second and keep the database load reasonably under 50%. Such scaling would process four million vehicles per-hour or 96 million vehicles a day, allowing all 500 million vehicles to have their PKI infrastructure replaced in a week.

Achieving Business Objectives

Now that this company can secure their vehicles at scale, they can start to achieve real business outcomes. Here are just a few:

Secure Updates = Future High Growth Revenue Model

By performing secure updates, the post-vehicle sale of electronic products and features are expected to increase revenue opportunities > 10% of the original vehicle's purchase price. This allows the company to invest further into connected vehicle revenue streams long after the sale of the vehicle is complete.

Improved Functionality, Security Operations

By moving vehicles to a modern security system, the company has streamed the maintenance and quality of data in real-time to manufacturers.

Streamlined Processes for Mergers and Acquisitions

By using Keyfactor as their IoT identity platform, this company can seamlessly transition to an updated Root of Trust during a merger or acquisition.

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human.

Contact Us

- www.keyfactor.com
- +1.216.785.2946