Building Comprehensive Security Into Cars

WHITE PAPER

Symantec™

Recently, threats to cars have escalated from the realm of possibility to harrowing reality.

Symantec is working with automakers, chipmakers, and other forward-thinking companies to block hackers' many inroads into vehicles and keep cars—and people—safe.

Executive Summary

Over the past few years, automotive security threats have gone from theory to reality. Tech-savvy thieves have stolen cars throughout Europe and North America. Online videos show hackers remotely hitting the brakes on cars in ways that can endanger drivers and passengers. Hackers can exploit some of these vulnerabilities from an adjacent lane without forewarning to the driver. Other vulnerabilities are open to attack over the cellular network—from halfway around the world—and for large numbers of cars simultaneously.

Even though technology exists to solve many of these security problems, the challenges of deploying such technology in cars loom far larger than similar challenges do in traditional information technology (IT) systems. In traditional IT systems, most problems can be solved with a quick install, update, or configuration change—or at worst, restoring from a backup, executing a failover to a disaster recovery site, or calling in a breach response team to tackle the most sophisticated threats.

However, cars don't work like that. Multi-year safety certification processes to meet Federal Motor Vehicle Safety Standards (FMVSS) requirements don't engender the weekly, daily, and real-time security updates that IT teams enjoy. Nobody can call in a breach response team to investigate the millions of cars you've built, now happily garaged in millions of homes. A car can't safely fail over to another car. Companies often use redundancies at critical IT layers to keep high-volume web services running reliably, but few, if any, carmakers can afford the NASA-like investment of doing this for every vehicle.

Protecting cars against such threats has to be done in a context that works both within the car, and at scale for carmakers. The responsibility doesn't stop at the assembly line: It extends all the way from the carmakers to the full breadth, depth, and complexity of auto supplier relationships. Security is a concern at each tier of the value chain, and attackers seek the weakest links.

Scalable approaches to building-in security require discipline and collaboration in applying the following basic security principles:

1. Protecting all communications
2. Protecting each sensor, actuator, microcontroller (MCU), and microprocessor
3. Safely and effectively managing the entire vehicle over the air (OTA)
4. Mitigating advanced threats

This white paper from Symantec sheds light on a potential path forward, with milestones toward comprehensive automotive security. Starting with components and interfaces that can be locked down individually, it addresses longer-term concerns with fundamental challenges of technologies such as controller area network bus (CAN bus) and FlexRay, which have been the backbone of integration across complex supply chains for many years.

Perhaps most important, this paper sketches a "straw dog" proposal for discussion toward a balanced timeline for phasing in such change, balancing the contexts that:

1. Driver and occupant safety is paramount,
2. The automotive industry needs long certification lead times for safely introducing any new technology.
3. The situation is urgent; neglecting the issue could cause fatalities, as could phasing in technology too quickly.
4. Fiscal reality can be harsh: New technology must bring more customers or increase margins, and defunct companies can't make cars safer.

This large and complex problem requires the insights and efforts of companies in both the automotive industry and IT and OT (operations technology) security. Designing cars that are secure from end to end will take time, and both industries must begin addressing these security issues at every tier of the automotive value chain. The stakes are too high to allow for delay.

Automotive Threats

Rashes of car thefts are striking throughout Europe and North America. Online videos show hackers remotely hitting the brakes on cars, potentially endangering drivers and other occupants. Hackers can exploit some of these vulnerabilities from an adjacent lane without any forewarning to the driver. Other vulnerabilities leave large numbers of cars open to simultaneous attack over the cellular network, from halfway around the world. First we focus on the threats that exist today, then we discuss forward-looking technologies that protect cars from these threats.

Early videos that demonstrated triggering of car behavior, such as brakes and engine shutdown, showed the hacker in the vehicle, plugged into the on-board diagnostics (OBD-II) port of the car.

Recent evidence shows that these attacks can work remotely, spurring costly recalls. Additional information is available to top automakers under special NDA.

Of course, these aren't the only attacks against cars, and some attacks are already hurting customers at scale. Throughout Europe and North America, thieves have been exploiting vulnerabilities in keyless entry systems. Keyless entry systems provide the customer the convenience of entering, leaving, and locking their cars—as well as stopping and even starting their car engines—without taking their keys out of the pocket, purse, or briefcase.

Many of the vulnerable keyless entry systems do this by trying to detect the proximity of the key to car. Few systems take the precaution of capturing position and proximity through relatively strong means, such as via healthier combinations of Global Positioning System (GPS), cellular, Wi-Fi, and accelerometer telemetry, all properly digitally signed by both the car and the car keys for them to agree that they are near each other. Instead, many systems attempt to capture proximity data with simpler signal strength triangulation among sensors on the car. Of course, that is susceptible to relay attacks in which a thief with the right electronics—often carried in a purse—can relay the car signal to the keys, and then relay the keys' signal to the car, as if the keys were in the thief's purse. To date, impacted brands include Audi and BMW, but those two are just the beginning of a long alphabetic list of impacted brands.

Automakers could avoid such costly and brand-damaging mistakes through combinations of digital capture of location, signing data on capture, and using secure boot and code signing to ensure that firmware isn't tampered. Similarly, embedding a richer set of over-the-air (OTA) update mechanisms into most cars could give many automakers more choices in quickly resolving this issue, even if the original set of keys weren't shipped with the more expensive sensors. These options could include using the customer's smartphone; for example, Android devices leveraging technology such as TrustZone™ Integrity Monitoring Architecture (TIMA) as alternate keys. After all, such mobile devices already have all of the sensors mentioned above.

Unfortunately, most carmakers are still building basic OTA update and configuration management into the cars they make and sell. Perhaps most important, such OTA capabilities still don't directly fix the risky vulnerabilities, which let hackers remotely trigger the car. That has to be done by applying the basic security principles to cars, and applying those principles at each tier of the supply chain.

Still, these aren't the only attack paths into the car. Other potential attack paths include Bluetooth connections to the user's mobile device, Bluetooth connections to other devices, attacks directly against Bluetooth implementations, and vulnerabilities of the IVI systems— particularly as those systems stream both entertainment and navigation data, including details on millions of businesses. Fortunately, it's not easy for aggressors to print millions of DVDs or CDs with malicious files to compromise vulnerabilities in DVD and CD players. However, as cars begin to stream entertainment over wireless interfaces, they increase their exposure to countless threats. Also, those threats to the IVI are in addition to the previously discussed OBD-II threats .

Sadly, with today's protocols for CAN bus and FlexRay bus, components do not have many means for adequately authenticating each other, particularly at drivetrain speeds. Even the most important changes touching so many parts of the ecosystem take a long time, and many practical steps need to be taken sooner.

Solution Overview

Protecting cars against such threats requires discipline and collaboration in applying basic security principles at each level of the system.

Four Cornerstones

Long-term, comprehensive security will require building security into the car at each layer. Today's cars have a great number of layers, from the cloud-based and data center systems to which the car connects, to the connection, down the modules themselves—including single- board computer (SBC), body control module (BCM), smaller sensor modules, the chips driving the modules, and the bus protocols connecting them. Protecting the whole "stack" from top to bottom with comprehensive security will take many years, given the complexity of spanning supplier relationships. All sensitive chips will need hardware support for secure boot and credential storage to prevent spoofing and tampering via OTA attack paths.

Sensitive chips include BCM and all MCU that impact drivetrain, hydraulics, and any other part of the car that affects safety in any way. Eventually, all sensitive modules will need cryptographic and key management capabilities for authenticating data to and from the other sensitive modules so that aggressors can't spoof a fake control signal. Some of this change will take much longer, as today's protocols for CAN bus and FlexRay do not have many means for adequate authentication. This makes it all the more urgent for the vehicle bus and all wireless modules, cellular, Wi-Fi, Bluetooth, or other, to quickly get monitoring capabilities to detect and address potentially dangerous anomalies. Finally, the system as a whole will need OTA update capabilities, and all data-center and cloud-based systems will need protection at the high standards appropriate for the lives depending on the security of these systems.

Nearer-term, the automotive industry has many opportunities for deploying high-impact security which, though not comprehensive, can go a long way toward mitigating a vast number of threats. This starts with establishing a beachhead for security in the car. Most commonly, this should start with locking down the "head unit" of a car, typically an SBC, sometimes tasked with also supporting the IVI functionality. Next, automakers can leverage a beachhead as a cornerstone for managing and updating the rest of the car. At the same time, you can deploy other security technologies to address the highest risk areas, such as monitoring the CAN bus, and mediating network facing connections.

To help address these needs, Symantec currently commercially offers:

1. Symantec Critical System Protection for protecting the head unit and IVI systems of most cars. Symantec™ Critical System Protection now supports QNX ™ Neutrino RTOS and, on request, can easily support specific embedded variations of Linux ® including Linux under Android.™
2. Symantec Critical System Protection for protecting OBD-II interface equipment, including dealer diagnostic equipment and UBI dongles.
3. Embeddable Security Certificates for Device Authentication can be used to authenticate data—even in extremely limited devices, such as decades-old 8-bit devices—and includes both message and frame authentication as well as authentication of connections.
4. Symantec Code Signing Certificates currently support the full range of code signing, including signing code for Secure Boot. Additionally, the Symantec Secure Application Service currently supports signing of code in Java and standard Executable and Linkable File (ELF) formats common on real-time operating systems (RTOS).

Additionally, Symantec is currently working with top automakers and tier one suppliers to iteratively refine the following technologies prior to general availability:

5. Embedded Automotive Security Analytics for monitoring any CAN bus or FlexRay bus. This software deploys easily onto most single-board computers, including SBC used for IVI and head units of most cars, and onto many 32-bit MCU used for OBD-II dongles, including UBI dongles.
6. Code Signing for Automotive Secure Boot is backed by Symantec's world-leading Certificate Authority (CA) and Code Signing infrastructures. We are working with interested chipmaker and semiconductor partners to make code signing and secure boot easier for carmakers.
7. Embedded Software Protection similarly builds on our Code Signing and CA services, but extends them to do more than sign the code, embedding obfuscation and other forms of protection directly into the code before signing so that automaker code can defend itself even on limited MCU, including decades-old 8-bit and 16-bit devices.
8. Global IoT Security Analytics to help detect advanced threats by correlating data from millions of cars. In short, no matter how well you protect each module, no matter how well you protect all communications, and no matter how well you manage the car as a whole, you'll always need a monitoring and analytics framework to detect the most advanced threats.

These are first steps toward the long-term vision of cars that are secure by design from end to end.

Uniquely Automotive Security Challenges

As mentioned, the challenges in crafting security for automotive systems differ dramatically from building security for traditional IT. Ad-driven websites can update themselves every hour, or even faster when needed. In cars, where lives are on the line, introducing new technology can take years. Every change to automotive systems must be made with care, and changes often impact many other suppliers in one of the most mature tiered supply-chains to ever evolve in business. Enterprise IT security might be nearly 20 years old, but most of the technologies don't work in cars.

Cars have been changing our lives for more than a hundred years. Of course, the shift to "connected" cars is much more recent. Such connectivity brings exciting new features that better customers' lives. However, at the same time, aggressors can use the connectivity as an attack path. Adding security into such firmly established automotive architectures presents more than a few challenges. To address these challenges, Symantec is not only investing in long-term success for protecting cars comprehensively, but also investing in nearer-term efforts that can produce results for automakers, dealers, and customers much sooner.

Fortunately, and surprisingly, Symantec has already embedded security into more than a billion Internet of Things (IoT) devices spanning several verticals, including key injection with partners on the production line for several device types. We are not new to deeply embedded systems.

We've embedded security into smart meters, cable modems, cellular base stations, and into 8-bit, 16-bit, and 32-bit devices.

However, Symantec is relatively new to the automotive industry. We are investing to build long- term relationships while aiming to deliver nearer-term measurable progress for all partners. We have a strong appreciation for the deep and complex "system of systems" integration among automotive suppliers, as well as the merits of the well-established tiered supply chains for each automaker. With security as a concern at each level, we are actively seeking partners who want a security advantage to create a premium version of their core technology in the supply chain, but with enhanced security for a higher average sales price (ASP).

Protecting Critical Modules

The head unit, IVI, OBD-II port, GSM module, and BCM all play critical roles in the safety and security of the car and its occupants. These modules are powerful assets for improving experiences and managing the car—but without proper security, these assets can be used against you and the driver. Fortunately, most of these modules typically perform predictable functions, meaning that they should always be in a known state, with known "good" code exhibiting known behavior. This makes it possible to lock down many of these systems with powerful security so that hackers can't use them against you and your customers.

Symantec™ Critical System Protection can be configured to enforce whitelisting of good code on many of these modules, ensuring that they can execute only previously approved code and controlling how that code is permitted to behave. Symantec™ Critical System Protection is built on proven technology that protects countless financial transactions daily. It resides in core back-end systems of the world's largest providers of financial services, and is also "embedded" in the countless ATMs that serve as their interface with their customers, much like the IVI presents such a crucial interface to the driver. We've taken this fundamental protection of the financial industry and adapted it for automotive systems.

Of course, Symantec Critical System Protection can do much more than whitelist good code. It can enclose code execution within a sandbox, allowing strict control over the code's behavior. This can provide stronger, more granular, more flexible, and more agile security than the real-time operating system (RTOS) with which it is tightly integrated, all the way down to kernel-level integration. Symantec Critical System Protection uses whitelisting and sandboxing as part of a least-privilege protection strategy that permits only known code to perform known functions. Symantec Critical System Protection not only monitors application behavior directly, but also monitors files, settings, events, and logs to report anomalous behavior. Features include sophisticated policy-based auditing and monitoring; log consolidation for easy search, archival, and retrieval; advanced event analysis; and response capabilities. This is serious security for critical modules in the cars you make.

Symantec Critical System Protection can defend most head units, IVI, OBD-II dongles, OBD-II dealer diagnostic equipment, and 32-bit BCM. Symantec Critical System Protection has been adapted to improve protection even on QNX ™ Neutrino RTOS —and, on request, can be tailored to run on specific variants of Linux,

including embedded variants of Linux, as well as other embedded operating systems. In connected cars, Symantec Critical System Protection can help to report suspicious anomalies and detected threats to the manufacturer in real time. In non-connected cars, such security telemetry can be stored for dealer retrieval during regularly scheduled maintenance.

Of course, protecting critical modules eventually requires code-signing and secure boot atop the runtime protection of Symantec Critical System Protection. Currently, Symantec Code Signing Certificates support a wide range of formats, but the Symantec Secure Application Service for code signing supports signing only a few formats, including Java and standard ELF formats common on RTOS, as well as formats specific to embedded versions of Windows. Of course, this leverages our world-leading CA infrastructure, and includes on- premises code-signing certificates, as well as our cloud-based services for helping you manage the ability of your suppliers to perform code-signing for your chips. Longer term, we are already working with interested chipmaker and semiconductor partners to support a much broader range of formats toward making code signing and secure boot easier for carmakers on all of their MCU.

Perhaps most important, to protect more limited devices—including 8-bit and 16-bit devices, which often lack an operating system (OS)—we at Symantec are developing a form of Embedded Software Protection that does more than sign code. This new offering will embed obfuscation and other forms of protection directly into the code before signing so that any code in the car can defend itself from both runtime attacks and reverse engineering—even on limited MCU, including decades-old 8-bit and 16-bit devices.

Mitigating the Most Advanced Threats

Of course, no matter how well a defender locks down its most sensitive modules, it will still have gaps in its defenses for years to come. Patient and well-resourced adversaries will find ways to exploit these gaps, and automakers need the capability to mitigate such risk.

Security analytics can unobtrusively watch everything happening on a FlexRay or CAN bus within the car, and "learn" models of normal behavior for all modules on the bus, then flag suspicious and potentially dangerous anomalies where components deviate from normal behavior. These analytics technologies can run on a number of SBC already found in most vehicles, such as the IVI or some of the more robust BCM, or on smaller after-market OBD-II dongles. In connected cars, the context for such anomalies can be immediately sent to the manufacturer for correlation with data from other cars, leveraging additional big data analytics. In non-connected cars, the context can be offloaded from the car and sent to the manufacturer during regular maintenance. In either case, the core technical challenge is learning compact models of normal behavior from a security perspective, able to fit within the constraints of existing SBC and smaller dongles, yet able to detect activity that might be an attack. Of course, configuration of fail-safe behavior is up to the manufacturer, but detection of potentially dangerous anomalies in the car is the problem that Symantec is currently solving in collaboration with partners. We invite additional partners to work toward solutions with us.

Symantec Embedded Automotive Security Analytics leverages a proven core technology that has already detected some of the most sophisticated advanced persistent threats (APT) in other Internet of Things (IoT) systems. Symantec is adapting this technology to CAN bus protocols and then to FlexRay protocols so it can run on SBC typically found in vehicles today, as well as on OBD-II dongles already sold by partners.

Global IoT Security Analytics, in contrast, can help detect advanced threats by correlating data from millions of cars. As with most data-driven problems, big data analytics technologies can leverage such breadth of data to vastly improve performance—in this case, performance in detecting advanced threats. Symantec's first big data technologies for security analytics began serving customers behind the scenes roughly seven years ago. For detection of such potentially dangerous anomalies in cars, we are adapting those proven technologies that have already detected the most advanced APT threats for other industries.

Summary

Connected cars bring tremendous promise for automakers and customers alike. At the same time, the connectivity brings new risks. Stolen cars and embarrassing online videos are only the tip of the iceberg compared to what could come. Still, building security into cars end to end will take many years. Symantec is committed to helping on that journey. Neither automakers nor customers can wait for "eventual" success.

As a first step to addressing some of the biggest threats, we've introduced a new product— leveraging proven technology and adapted for cars—to protect many of the most sensitive modules in cars today. Symantec Critical System Protection is easy to build into head unit, IVI, and 32-bit BCM of most cars

coming to market. Dealer OBD-II equipment can also use this technology to be sure that dealer diagnostic equipment doesn't become an infection vector for attacking and infecting cars that the dealer touches for maintenance.

As a second major step to address some of the biggest threats, Symantec is also developing a technology, Embedded Automotive Security Analytics, to protect the whole vehicle bus, either from an SBC such as an IVI or head unit of any car still in design, or from the OBD-II port of cars already on the road. Of course, many of our other security technologies for IoT, including Device Certificates, Code Signing, OTA Management, and Roots of Trust, can all help automotive security as well. In fact, together, it's the most comprehensive portfolio of IoT security relevant to connected cars. Together they can help form the foundation of the longer-term change so strongly needed. Symantec Critical System Protection and Embedded Automotive Security Analytics represent the biggest leaps in security for the automotive industry, for the current year, and the year ahead.

In addition, Symantec is adapting the world's most comprehensive portfolio of security technologies, including our world-leading CA infrastructure, which has already embedded security certificates into more than a billion IoT devices, and our Code Signing products and services, which already support complex supply chain relationships, as an initial few file formats relevant for automotive. Symantec is adapting these technologies to deliver Embedded Software Protection that can deliver runtime security, even in the most constrained automotive MCU, along with supporting the broader array of formats needed for secure boot across the range of automotive MCU. Symantec is delivering these new technologies in parallel to working with partners on longer-term standards.

In short, having begun protecting more than a billion IoT devices, and having detected the most sophisticated threats in other IoT systems for other verticals, Symantec is investing aggressively to adapt its world-leading portfolio of security technologies to fit the needs of the car.

If you'd like to help build security into cars, please contact us at **iot_security@symantec.com**.

Abbreviations and Acronyms

BCM: Body Control Module

CAN bus: Controller Area Network Bus

FMVSS: Federal Motor Vehicle Safety Standards

GPS: Global Positioning System

IVI: In-vehicle Infotainment

MCU: Microcontroller Unit

OBD-II: On-board Diagnostics

OTA: Over-the-air

SBC: Single-board Computer

TIMA: TrustZone™ Integrity Monitoring Architecture

UBI: Usage-based Insurance

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on **Facebook**, **Twitter**, and **LinkedIn**.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

symc_wp_Building_Security_Into_Cars_en-v2a