GUIDE

Managing and Securing Open Source Software in the Automotive Industry

Table of contents

Executive summary.......... 2

Open source in the auto industry.......... 2

Open source safety and security issues.......... 3

Open source licenses and compliance risk.......... 4

Best practices for managing open source risk across the automotive supply chain.......... 4

Conclusion.......... 5

Executive summary

A revolution is underway in the automotive industry. The car is no longer simply a means of getting from here to there. Today's car now reaches out for music streamed from the cloud, allows hands-free phone calls, and provides real-time traffic information and personalized roadside assistance.

Most every modern car feature—such as speed monitoring, fuel efficiency tracking, and gas level monitoring—is digitized to provide drivers with easier operation and better information. Technological innovation is accelerating with the growth of computing capacity needed to control a self-driving vehicle and the development of low-cost sensors that can make a car react to its surroundings. Recent innovations enable automobiles to monitor and adjust their positions on the highway, alerting drivers if they are drifting out of their lanes, even automatically slowing down when they get too close to another car. And whether we're ready or not, we'll soon be sharing the roads with autonomous vehicles.

Without a doubt, today's cars are defined as much by the power of their integrated technologies as by the power of their engines. Driving the technological revolution in the automotive industry is software, and that software is built on a core of open source. Open source use is pervasive across every industry vertical, including the automotive industry. A recent Forrester Research report acknowledges the widespread prevalence of open source in applications, with custom code now often composing only 10—20% of any given commercial application. Black Duck software audits of commercial applications show similar trends, with open source components composing 23% of automotive applications.

The arguments for open source are straightforward: Open source lowers development costs, speeds time to market, and accelerates innovation. When it comes to software, every auto manufacturer wants to spend less time on what are becoming commodities—such as the core operating system and components connecting the various pieces together—and focus on features that will differentiate the brand. The open source model supports that objective by expediting every aspect of agile product development.

But just as lean manufacturing and ISO 9000 practices brought both greater agility and quality to the automotive industry, visibility and control of open source are essential to maintain the security, license compliance, and code quality of automotive software applications and platforms.

This document reviews challenges and presents recommendations for managing the use of open source software throughout the automotive software supply chain by automakers, suppliers, and technology companies servicing the automotive industry.

Auto connectivity is outpacing security

"When you put new technology into cars, you run into security challenges."

- When security researchers demonstrated that they could hack a Jeep over the internet to hijack its brakes and transmission, it posed a security risk serious enough that Chrysler recalled 1.4 million vehicles to fix the bug that enabled the attack.
- For nearly half a decade, millions of GM cars and trucks were vulnerable to a remote exploit that was capable of everything from tracking vehicles to engaging their brakes at high speed to disabling the brakes altogether.
- The Tesla Model S's infotainment system contained a 4-year-old vulnerability that could potentially let an attacker conduct a fully remote hack to start the car or cut the motor.

Vehicle manufacturers will need to adopt a cyber security approach that addresses not only obvious exposures in their cars' software but also the hidden vulnerabilities that could be introduced by open source components in that software.

Open source in the auto industry

The open source concept was introduced more than 25 years ago, and adoption of open source software has been accelerating ever since. "Open" simply means the source code is freely available to developers under specific license terms. Under many open source licenses, developers have the right to modify and distribute the software to anyone and for any purpose.

The Linux operating system is a prime example of the power of open source, with one of the largest installed bases of any operating system in the world. Many different versions of Linux have been created to meet specific needs, including Automotive Grade Linux (AGL), a collaborative open source project that is bringing together automakers, suppliers, and technology companies to accelerate the development and adoption of a fully open software stack for the connected car. With Linux at its core, AGL is developing an open platform from the ground up that can serve as the de facto industry standard to enable rapid development of new features and technologies.

The Open Automotive Alliance is another group of technology and automotive companies who have come together to bring the best of Android—a Linux-based platform for mobile phones released under the Apache v2 open source license—into the automobile in a seamless and driver-centric way that helps minimize distraction.

Another well-known open source project serving the auto industry is GENIVI. This nonprofit industry alliance is developing an open standard for creating what is known variously as in-car entertainment (ICE) or in-vehicle infotainment (IVI). GENIVI standards help automakers deliver applications that comply with myriad branding, ownership-of-data, and business models. The alliance has more than 140 members, including auto OEMs such as BMW, automotive suppliers such as Bosch, and world-class software and service suppliers such as Synopsys.

Among the more than 2,000 users of Black Duck, our software composition analysis solution, are many companies in the automotive industry, including members of the GENIVI Alliance and GENIVI itself. These companies use Synopsys' industry-leading products to automate the process of securing and managing open source software, eliminating the pain related to security vulnerabilities, compliance, and operational risk.

Open source safety and security issues

When automotive safety is a function of software, the issue of software security becomes paramount—particularly when it comes to new areas such as connected cars, and inevitably, autonomous vehicles. While connected cars offer abundant opportunities for the automobile industry, automakers and their suppliers need to consider what the connected car means for consumer privacy and security.

Most open source components are governed by one of about 2,500 known open source licenses, many with obligations and varying levels of restriction

Open source use is pervasive across every industry, including the automotive industry. Black Duck software audits show that open source components make up an average 23% of automotive commercial applications. Open source dominates application development for good reason, lowering development costs, speeding time to market, and accelerating innovation. However, with those benefits come risks, particularly when organizations do not sufficiently track and manage the open source in use.

Open source is neither more nor less secure than custom code. However, there are certain characteristics of open source that make vulnerabilities in popular components very attractive targets for hackers. Open source is widely used in virtually all forms of commercial and internal applications. For hackers, the return on investment for an open source vulnerability is high. A single exploit can be used to compromise hundreds of thousands of applications and websites. Open source enters in-vehicle applications through a variety of paths. Automobile manufacturers rely on a wide range of component and application suppliers, who build solutions with open source components and extend open source platforms like GENIVI.

Many automakers and their software suppliers deploy testing tools such as static and dynamic application security testing (SAST and DAST) tools to identify coding errors that may result in security issues. While both SAST and DAST are effective in spotting bugs in code written by internal developers, they are not effective in identifying open source vulnerabilities in third-party code, leaving major components of today's applications exposed. Since 2004, more than 74,000 vulnerabilities have been disclosed by the National Vulnerability Database (NVD), but only 13 of those were found by SAST and DAST tools.

According to the National Security Agency (NSA), the average SAST tool can find only 14% of the problems in an application. Similarly, DAST is helpful for verifying compliance and finding misconfiguration issues but is ineffective at finding vulnerabilities that enter code via open source.

When a supplier or auto OEM is not aware of all the open source in use in its product's software, it can't defend against attacks targeting vulnerabilities in those open source components. If your organization plans to leverage connected car technology, you need to examine the software ecosystem you're using to deliver those features, and account for open source identification and management in your security program.

Open source visibility and control are essential to maintain the security, license compliance, and code quality of automotive software applications and platforms

Open source licenses and compliance risk

Open source security risk is top of mind for many organizations because of highly publicized exploits such as Heartbleed and the Apache Struts 2 vulnerability, which brought thousands of attacks against organizations worldwide. However, it is also important to recognize the importance of license compliance in reducing open source risk.

Most open source components are governed by one of about 2,500 known open source licenses, many with obligations and varying levels of restriction. These license requirements can be managed and complied with only if the open source components governed by those licenses are identified. Failure to comply with open source licenses can put businesses at significant risk of litigation and compromise of IP.

The modern automotive software ecosystem is a multitiered digital supply chain. Independent developers may contribute code under a variety of licenses. For example, component manufacturers may develop software to run on top of the GENIVI platform, in addition to modifying and augmenting the GENIVI codebase to suit a particular automobile subsystem. With this complexity comes license and IP management challenges, including the ownership of proprietary code that includes open source components.

Even so-called permissive open source licenses typically require acknowledgment of use and other obligations such as redistribution and documentation requirements. And open source components with no identifiable license terms also can be problematic. When software does not have a license, it generally means no one has permission from the creator of the software to use, modify, or share the software. Creative work (which includes code) is under exclusive copyright by default. Unless a license specifies otherwise, nobody else can use, copy, distribute, or modify that work without being at risk of litigation. The lack of clear statements of rights and obligations leaves organizations using that open source at greater risk of violating "hidden" terms.

Best practices in the use of open source software require developers to understand which components and associated licenses are in their code and what obligations may result from their use of open source. However, managing open source use manually can be a Sisyphean task, as demonstrated by a 2017 Synopsys Center for Open Source Research & Innovation (COSRI) report on over 1,000 Black Duck software audits of commercial codebases.

The audits found that open source license conflicts were pervasive. The audited applications contained 147 open source components on average—a daunting number of license obligations to keep track of—and 85% of audited applications contained components with license conflicts. The most common challenges were GPL license violations; 75% of applications contained components in the GPL family of licenses, but only 45% of those applications were in compliance with GPL obligations.

Best practices for managing open source risk across the automotive supply chain

As auto OEMs work with software providers, a growing set of open source components is making its way into automobile systems. Open source code is being channeled through countless supply chains in almost every part of the automotive ecosystem.

To make progress in defending against open source security threats and compliance risks, both auto OEMs and their suppliers must adopt open source management practices that do the following:

An effective approach to addressing software vulnerabilities

- Examine custom source code for vulnerabilities during development (SAST).
- Test compiled applications for common runtime vulnerabilities (DAST).
- Ensure that open source use is not introducing security vulnerabilities during development, and monitor for newly reported vulnerabilities after the application is deployed (OSVM, or open source vulnerability management).

Fully inventory open source software. Organizations cannot defend against threats that they do not know exist. A full and accurate inventory (bill of materials) of the open source used in their applications is essential.

Map open source to known security vulnerabilities. Public sources, such as the National Vulnerability Database (NVD), provide information on publicly disclosed vulnerabilities in open source software. Organizations need to reference these sources to identify which of the open source components they use are vulnerable.

Identify license and quality risks. Failure to comply with open source licenses can put organizations at significant risk of litigation and compromise of IP. Likewise, use of out-of-date or poor-quality components degrades the quality of applications that use them. These risks also need to be tracked and managed.

Enforce open source risk policies. Many organizations lack even basic documentation and enforcement of open source policies that would help them mitigate risks. Manual policy reviews are a minimum requirement, but as software development becomes more automated, so too must management of open source policies.

Alert on new security threats. With more than 3,500 new open source vulnerabilities discovered every year, the job of tracking and monitoring vulnerabilities does not end when applications leave development. Organizations need to continuously monitor for new threats as long as their applications remain in service.

Conclusion

As open source use continues to increase in the auto industry, effective management of open source security and license compliance risk is becoming increasingly important. By integrating processes and automated solutions such as Black Duck into their software supply chain, automakers, suppliers, and technology companies servicing the automotive industry can maximize the benefits of open source while effectively managing their risks.

Black Duck software composition analysis allows organizations to automate identification of all open source in use, quickly gain visibility into any known open source security vulnerabilities and compliance issues, define and enforce open source use and risk policies, and continuously monitor for new vulnerabilities affecting vehicles currently in service.

Black Duck software audits are recognized as the industry standard for open source due diligence during mergers and acquisitions (M&A) as well as internal audits where there is a need to quickly and completely inventory open source software, identifying license compliance, security, and quality-of-risks.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com