WHITEPAPER

Take the Steps to Secure Your Software Supply Chain – What are You Waiting For?

Ken Obuszewski | Director, BlackBerry Jarvis

With the constant news around cyber-attacks, it can be very daunting for CISOs, CSOs, CIOs, and engineering VPs to put in place plans to address cybersecurity threats for all their products across the software supply chain. Automobiles are a very pertinent example of the challenges posed by cybersecurity threats to complex software systems, especially with the onset of ubiquitous connectivity and the move towards autonomous vehicles, intelligent transportation systems, and transportation as a service.

In a recent study on automotive cybersecurity practices performed by the Ponemon Institute[1], 30% of the respondents do not currently have a product security team or program in place, and 63% test less than half of their products and technologies for vulnerabilities. This is aligned with a recent BlackBerry webinar "Why binary scanning is critical for securing your software supply chain"[2] where only 29% of the respondents cited a central security team within their organization and 23% did not currently have a security infrastructure in place.

Vehicles provide a particularly challenging environment for cybersecurity with issues including very complex software, with over 100 million lines of code in a "network on wheels" of distributed computers, a complex supply chain, and very long lifecycles for software in the vehicle. The last point means that the software will inevitably be out of date and must be updated to address the latest vulnerabilities and to stay ahead of bad actors. Even with these known issues, the Ponemon study[1] identified that only 44% of organizations surveyed impose security requirements on their suppliers, despite that 73% expressed a high or very high degree of concern on the quality of software provided by their third parties.

Often with a new challenge, the biggest hurdle is taking the first step, but it is nevertheless imperative that carmakers make the necessary investments to secure their vehicles. The 2015 Fiat Chrysler Jeep hack is still the most visible illustration of the risks associated with inadequate security, as it involved a recall of more than 1.4 million vehicles with significant direct costs to FCA and a public relations firestorm for FCA and its supply chain. One report estimates the total cost to FCA could have approached $1.4B[3]. The same report also revealed that Black Hat attacks in automotive overtook White Hat activity for the first time in 2018, and 28% of these attacks involved the unauthorized control of vehicles. This will become an ever more serious threat to society as autonomy advances and drives home the notion that safety and security must be addressed with a holistic strategy. In fact, in a recent BlackBerry survey, 67% of respondents indicated that they would pay more for a car with the latest safety and security software[4].

BlackBerry, long known as the Gold Standard in Enterprise mobile security, offers practical solutions to address cybersecurity challenges. That expertise, coupled with extensive experience in safety-critical systems such as vehicles, qualifies BlackBerry to provide a unique perspective to meet the challenges of today's connected world. As it pertains specifically to cybersecurity challenges, at BlackBerry we recommend implementing a Secure Software Development Life Cycle Process (S-SDLC), with a 3-phased approach:

1. Assessment
2. Implementation
3. Continuous Improvement

ASSESSMENT

The obvious, yet significant, first step is to take stock of all current software assets, software development and security practices, and to identify the desired state. Here are the major steps that should be taken in the assessment phase:

1. Utilize an industry model to assess your current security practices

BSIMM (Building Security In Maturity Model)[5] or Open SAMM (Software Assurance Maturity Model)[6] are good examples to consider. BSIMM represents a community study involving 120 companies across multiple verticals providing a public cybersecurity framework. Open SAMM is an OWASP (Open Web Application Security Standard) project designed to be flexible based on the individual needs of organizations.

2. Establish a baseline profile of your software assets across your internal and external supply chain, including a vulnerability assessment

To establish the baseline profile, static application security testing (SAST) platforms such as BlackBerry® Jarvis™ are critical since manual analysis is not practical or cost-effective with today's complex software systems. As a binary SAST platform, BlackBerry Jarvis is an ideal solution as it can evaluate the outgoing security and quality of the final deployed solution. The powerful and extensible architecture of BlackBerry Jarvis automatically builds a software inventory and identifies over 100 categories of security vulnerabilities as well as providing a detailed view of software craftsmanship.

3. Define the desired security process based on your risk tolerance

BSIMM and Open SAMM allow an organization to build the framework of their security strategy and benchmark against industry peers. This requires companies to build the infrastructure of a cybersecurity organization. An organization which is implementing a S-SDLC for the first time may initially utilize an external consultancy, but it is critical to establish the proper internal expertise and ownership. This includes an executive with ultimate responsibility for security in the company or organization. A "Center of Competence" concept can be employed, whether the resources report to this leader or not. From a resourcing standpoint, BlackBerry would recommend up to two security researchers and at least one incident response engineer during this phase.

IMPLEMENTATION

As an organization moves from assessment to implementation, it is critical to build cybersecurity into the culture of the organization, and to integrate it into the development and deployment processes. Cybersecurity and software quality standards need to be translated to a set of key performance indicators (KPIs) such that they can be measured and enforced across all development teams, whether internal to the organization or across the software supplier base. BlackBerry Jarvis tracks software quality over time, providing detailed trends into vulnerabilities and software quality. The ability to measure progress is critical for a quantifiable software security strategy. It is important to move away from a "leap of faith" approach, whereby organizations believe they must be getting more secure simply because more is being invested.

A wide set of standards exist that can be deployed as part of your S-SDLC, including community-based databases and common coding standards, such CWE and multiple SEI CERT variants, as well as industry-specific versions such as ISO26262 for automotive and IEC 62304 for medical devices. Also, of critical importance is to measure the adherence to software craftsmanship best practices such as the implementation of compiler defenses and secure APIs to prevent attackers from exploiting memory corruption vulnerabilities.

Deep cybersecurity expertise has allowed BlackBerry to develop specific rules and guidelines for security and software craftsmanship that extend further than published standards, which we have documented in 70+ internal whitepapers. BlackBerry Jarvis exposes this level of expertise for the first time to our customer base. A few practical examples of the how BlackBerry Jarvis can help:

- White hat attackers gained access to Volkswagen and Audi infotainment systems via open debug ports (Telnet). BlackBerry Jarvis detects the presence of insecure protocols and administration tools which can allow unauthorized system access;
- The improper assignment of root privileges is often the exploitation point for attackers, and BlackBerry Jarvis provides a full picture on the access level for all components;
- Attackers look to find vulnerable files that are typically networked and present larger and more complex attack surfaces. BlackBerry Jarvis provides the level of visibility needed to identify the software components that need to be secured.

Additionally, BlackBerry Jarvis is customizable to an organization's internal standards as well as industry standards including use of the Common Vulnerability Scoring System (CVSS) to prioritize the remediation of vulnerabilities.

The final implementation step is to automate within the build and continuous integration processes. It is recommended to integrate directly within the automated build process, which is a quick and easy process for BlackBerry Jarvis based on the use of standard APIs.

The implementation phase requires a business to continue to grow and enhance the capabilities of its cybersecurity team. This includes providing oversight, with decision making authority, for the security team and moving from reactive to proactive security engineering. An example of proactive engineering would be to build a cybersecurity capability maturity model.

CONTINUOUS IMPROVEMENT

Once the implementation infrastructure is in place, the next step is to drive continuous improvement. This requires the ability to track vulnerabilities and software quality over time, both at a product level and at the organizational level. Automated tracking mechanisms will allow a development team lead to ensure that their projects are tracking to success, and to identify potential issues at an early stage. It also provides a mechanism to audit suppliers. Most importantly, it drives a culture and a process to push accountability all the way to the source, the developer, as over time adherence to the defined standards will become second nature. Nevertheless, this never becomes a static process as one must continuously evolve to stay ahead of attackers and to embrace the latest best-in-class practices.

BlackBerry Jarvis is configured to track vulnerabilities at the product level. This allows development teams to track the security posture of their individual development projects from release to release and to ensure that development teams are achieving the desired KPIs. As a SaaS based service, frequent updates provide the latest features and capabilities, allowing companies to stay ahead of malicious hackers. The organization must never rest as the attackers will not do so. Once the continuous improvement phase has been reached, it would be expected that a fully functioning security organization and culture are in place. The size of the team and total investment will vary based on individual organizational needs, but a team of ten or more engineers is not uncommon.

With decades of experience in secure software, BlackBerry has built tremendous knowledge based on internal product development and securing the most critical devices and operations for the likes of G7 governments and top 10 financial institutions. For additional details on BlackBerry's cybersecurity recommendations please read our white paper, "BlackBerry's 7-Pillar Recommendation for Cybersecurity", which provides a framework to secure automobiles and other embedded devices.

References

1 Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices

2 http://blackberry.qnx.com/en/news/webinars#!/webinar/22

3 https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/

4 https://www.blackberry.com/content/dam/blackberry-com/media-gallery/pdf/Consumers-Dont-Trust-Connected-Devices-to-Keep-Data-Safe-and-Secure.pdf

5 https://www.bsimm.com/

6 https://www.opensamm.org/

411.171 – Feb 2019

BlackBerry