OPPO Strengthens Its Software Engineering System

Ensuring security robustness with BSIMM

Company overview

Since its inception, OPPO has expanded its business to more than 40 countries and regions in the world. Its smart devices have been used by more than 300 million people. As of 2019, OPPO has invested some RMB10 billion in R&D to strengthen both the technologies and design of its products. At present, several OPPO smartphone models are equipped with advanced technologies such as cybersecurity situational awareness and a network attack identification algorithm, as well as a variety of security features including website inspection, asset risk reminder, permission records, and privacy protection.

The challenge

In the digital era, network and data security are of utmost importance. It they are compromised, assets and personal privacy are at risk. For consumers, the top concern is the safety of the apps in their smartphones.

"OPPO has always treated the protection of users' information and privacy as a priority," said Anyu Wang, terminal security director at OPPO. "In light of this, OPPO strives to strengthen our technological capabilities in security and privacy protection, thus enhancing user experience. Through leveraging intelligence and interconnected scenarios, we are able to strengthen our competitiveness in security and gain users' trust. This will also ensure that OPPO has sustainable developments. [That's why] we implemented the [Building Security in Maturity Model] (BSIMM) security assessment offered by Black Duck."

At OPPO, security and privacy protection are factored into every step of product development. Its Software Engineering System Security Department has a mandate to strengthen the company's abilities to uphold the security of engineering projects and software. As OPPO expands its product portfolio and global business presence, the company has acknowledged the growing importance of security and privacy protection in the software development process. Therefore, it adopted BSIMM and Microsoft SDL to keep abreast of industry best practices and optimize the security compliance of its software development process.

"OPPO wants to support its key business development directions with a robust security compliance mechanism. It should be able to ensure our operation compliance and IT-enabled secured software development process. Through protecting security and privacy of users and products during the R&D stage, we can reduce risks and costs, as well as win trust towards our engineering efforts. To achieve these goals, we need a yardstick to measure the progress of our security program and our software security performance against the industry," Wang said.

The solution

BSIMM is a benchmarking tool for software security assessment for enterprises. A BSIMM assessment can help OPPO compare its security practices against the industry best practices, helping it identify areas where there might be room for improvement. Starting 2020, OPPO has been carrying out BSIMM assessments for its software engineering system operations in Shenzhen, Dongguan, Chengdu, Shanghai, and Nanjing.

After performing BSIMM assessments for two years, OPPO reports that many facets of its software development security system have been significantly improved.

The BSIMM report, released annually since 2008, collects data about the software security practices of participating companies, and then analyzes and compiles it. This report helps companies plan, implement, evaluate, and improve their software security initiatives (SSIs). By comparing its software security performance with the industry best practices, OPPO could drive its software security to new heights.

When carrying out its BSIMM assessment for OPPO, Black Duck focused on the business structure of OPPO's software engineering system. Black Duck performed a thorough interview prebriefing, and experts conducted on-site and online in-depth interviews with OPPO executives. The assessment report summarized OPPO's software security and provided recommendations for improvement.

Through these interviews, OPPO was able to gain a thorough understanding of how its existing SSIs operate, and could set goals for future development. BSIMM is a benchmarking tool for software security, but it can also be used as an SSI roadmap tool. "OPPO can take reference from the recommendations of the BSIMM assessment to fine-tune its SSI," said Kelfen Yang, senior security architect, Black Duck.

The results

After performing BSIMM assessments for two years, OPPO reports that many facets of its software development security system have been significantly improved. It has also developed a clear and effective SSI upgrade plan.

"Throughout the two-year assessment process, the expert team from Black Duck has been extremely professional and competent. Their assessments of our software security are pragmatic. They also provided us with effective recommendations for improving our software security capabilities. OPPO looks forward to having further cooperation with Black Duck in software security enhancement," Wang said.

"The software security performance of OPPO is relatively high in the industry, taking into consideration that its software engineer system department has not been established for a long time. In view of the tremendous security challenges in the digital era, smartphone manufacturers and carriers need to keep on improving the reliability, security, and innovation of their product offerings. Putting security first at the very beginning of new product development is the most cost-effective way of ensuring security. Black Duck is committed to working with OPPO to help build its software security," said Yonglei Wang, Black Duck senior open source expert.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.