DHS Automated Vetting Process for Mobile Apps Could Cut Costs

The Science & Technology Directorate sees improvements for quickly approving mobile apps for government use.

Kate Macri
Thu, 07/23/2020 - 12:53

Federal agencies faced a new security challenge when their employees transitioned to remote work in March: quickly and efficiently vetting mobile apps for use on government smartphones. The Department of Homeland Security developed an automated security vetting process for mobile apps, cutting out hours of work and thousands of dollars to help streamline remote work.
Vetting just one mobile app according to the National Security Agency's NIAP standards previously consumed as many as 60 hours of work and could cost a federal agency anywhere from $40,000 to $80,000. The entire timeline could take anywhere from three to six months, DHS Mobile Security R&D Program Manager Vincent Sritapan told GovernmentCIO Media & Research.

Sritapan wanted his automated test to reduce the amount of time it takes to vet a mobile app. His team was able to get the automated portion of the test down to just two hours over the course of the study. According to the June 29 report, if the right changes are made, it may be possible to automate as much as 90% of testing.

“Our hope is it can drive down costs and at the end of the day reduce costs and not just the time,” he said.

Sritapan’s automated test is also superior to the former vetting process because it ensures standardization, greater accuracy and “more robust results.”

“If you check between different labs or analysts, you're going to find the technical expertise and methodology is going to vary quite a bit,” Sritapan said of the former vetting process for mobile apps. “Why is it costing me $20,000 at one place and $40,000 at another place? It really depends. So being able to do it with an automated tool, consistency is the key thing. It is more accurate.”

Automating the vetting process not only saves time, but also allows for more layers of vetting to ensure the greatest degree of accuracy possible. It also highlights potential security issues in an app and explains how to fix them.

“By hand you can test for criteria one way, but the tool will test it two or three different ways,” Sritapan said. “If I have analyst A do it one way and analyst B do it a different way, you may find the labs come out with different results for the same app, so this does bring consistency and reduces human error. You still need a human in the loop, but overall I think it's a step in the right direction.”

The automated test will also allow federal agencies to test more mobile apps, potentially allowing federal employees to use more apps on their government phones than before.
“Time [and money] has been a barrier to entry for folks, they say we'd love to do this and follow the rules, but in truth we can only afford so much,” Sritapan said. “Can you test, and can you test in a way that's scaleable and automated?”

Sritapan’s long-term goal is for other organizations outside the federal government to use the test as well.

“If I were an enterprise, a bank or health organization, for my users, I would want their apps to be checked,” he said. “Yes the official stores like Google Play and the Apple App Store do their own types of security and privacy checks, but what we allow as an enterprise might be different than what we allow as an individual.”

A GPS tracking app, for example, might be fine when you’re hiking, but not when you’re at work if you work in an industry or for an organization with security sensitivities.

"It just happens to be that NIAP is the highest bar you can get,” Sritapan said.

Note: A previous version of this article misrepresented how much of the test was automated. It has been revised to clarify that part of the test has been automated and there are still some manual processes present.