Lessons From a Mobile App Security Testing Pilot

Over the past few years, APCO has engaged in a number of efforts to ensure public safety apps are as safe and effective as possible: creating a trusted resource for learning about public safety apps (www.AppComm.org); publishing a list of key attributes of effective apps for public safety and emergency response to provide basic criteria for developers; and issuing guidance on "9-1-1" apps, just to name a few. Recently, APCO partnered with the Department of Homeland Security Science and Technology Directorate (DHS S&T) to focus on cybersecurity for mobile apps. The goal was to refine an evaluation program designed to ensure interoperability, reliability and security for public safety apps. Over the summer, we conducted a pilot to explore the viability of an app evaluation program.

To start, APCO selected twenty apps based on data from AppComm and estimates of the apps' popularity among public safety professionals. Counting iOS and Android versions of an app separately, the pilot involved 33 apps.

Kryptowire, a company that provides mobile app software assurance tools, provided access to its testing platform, which was integrated with AppComm to streamline the testing process. App security experts at DHS and the National Institute of Standards and Technology (NIST) identified a set of testable app software characteristics most relevant to public safety users. The criteria were divided into two categories: (1) critical flaws requiring correction and (2) potential vulnerabilities requiring correction or explanation as necessary for operation. For example, the presence of known malware (software intended to damage or disable devices) in an app's software was a critical flaw. In contrast, an app accessing the contact information on the device was a potential vulnerability. If the app's features did not require accessing the contacts, this was considered an excessive permission that could be exploited to send spam and/or malicious content.

Of the 33 apps tested, 18 had critical flaws. Only one app passed the initial test without any issues. The testing platform generated suggestions for how the apps should be updated, and Kryptowire's experts assisted developers as needed. Based on feedback from the developers who completed the pilot, participation was not burdensome, with most reporting that the suggested changes could be made in approximately one hour. Unfortunately, half of the developers failed to complete the remediation process. In some cases, this was due to shifting priorities and limitations on developer staff.

> **Cybersecurity challenges aren't simple, but mobile apps must be secured for public safety professionals. APCO appreciates the collaboration with DHS, NIST, Kryptowire and app developers, and we look forward to ongoing work to improve security for public safety apps.**

The high drop-out rate and the finding that the overwhelming majority of apps tested had critical or potential vulnerabilities highlight the need for a formal app vetting process to serve the public safety community. While many developers will gladly participate in testing, others will need to be incentivized.

From APCO's perspective, consultation with public safety professionals is a top priority. Their input will dictate the ultimate form and success of a sustainable app evaluation process. Even if evaluations are limited to a baseline set of security criteria, the preferences, policies and laws for individuals or sponsoring public safety agencies will influence outcomes. Combining these factors with the nature of app testing, whereby certain vulnerabilities are acceptable if they are necessary for the function of an app, makes a fully automated app evaluation impractical. In other words, while an automated process can detect critical flaws that must be corrected, evaluating other potential vulnerabilities is not as straightforward. In such cases, an app security evaluator with knowledge of public safety users' needs will likely be required for effective remediation and confidence in the evaluations.

Until a formal evaluation program is in place, public safety officials considering the use of mobile apps should ask their vendors about the measures they have taken to ensure the app is secure. The developer or vendor should step you through how the app performs and the security controls that are in place.

Cybersecurity challenges aren't simple, but mobile apps must be secured for public safety professionals. APCO appreciates the collaboration with DHS, NIST, Kryptowire and app developers, and we look forward to ongoing work to improve security for public safety apps. ●

Jeff Cohen *(cohenj@apcointl.org) is Chief Counsel and Director of Government Relations for APCO International.*

Mark Reddish *(reddishm@apcointl.org), Senior Counsel and Manager of Government Relations and* ***Nicole Zimbelman*** *(zimbelmann@apcointl.org), Government Relations Counsel, also contribute to this column.*