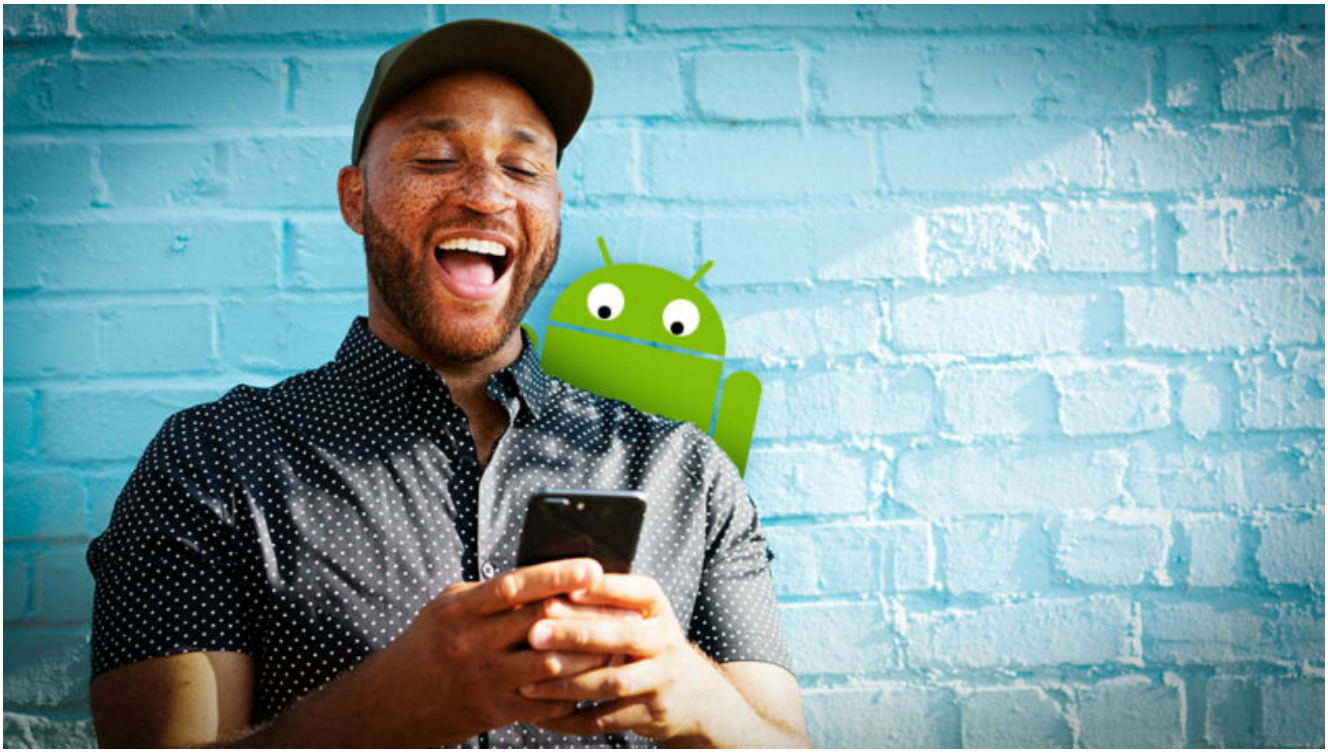
Google’s “Web Integrity” Android API could kill “alternative” media clients



Enlarge / The little Android robot is watching everything you do.

reader comments

18 with

Google is killing off its proposal for “Web Environment Integrity API” as a new web standard, though Android phones may still have to deal with it. According to Google’s proposal document, the primary goal of the project was to “allow web servers to evaluate the authenticity of the device and honest representation of the software stack”—basically Google wanted a DRM gatekeeper for the web. The project got widespread coverage in July and was widely panned.

The ominously vague plan was to allow web browsers to detect

if your computer was “modified” in a way that the webpage didn’t like. Presumably, this could be anything from a rooted/jailbroken phone to having an undesirable plug-in (read: ad blockers) installed. When you tried to access some protected content, a browser supporting the Web Integrity API would first contact a third-party “environment attestation” server, and your computer would have to pass some kind of test. After having your local environment uh… scanned? passing environments receive a signed “IntegrityToken” that points to the content you wanted unlocked. You would bring this back to the web server and would finally get the content unlocked.

Google’s proposal did not go over well. The explainer was full of conflicting information about just how invasive it wanted to be and what its goals were. Google pinky-promised it wasn’t meant to “enforce or interfere with browser functionality, including plugins and extensions”—this is a vague reference to ad blockers—but also the proposal’s very first example had to do with more accurately measuring ad impressions. Even more alarming was that this wasn’t a discussion—Google never publicized the feature for any kind of feedback, and the company was already actively prototyping the feature in Chrome before the Internet really found out about it.

On the Android Developer Blog, oddly, Google has formally announced the death of the proposed web standard. The company says: “We’ve heard your feedback, and the Web Environment Integrity proposal is no longer being considered by the Chrome team.” I believe this is the first time Web Integrity has ever been mentioned in a Google blog post, but hooray! It’s dead. On to the next problem:

Advertisement

Pivot to Android, ensuring YouTube

Vanced doesn’t rise from the grave?

The project isn’t totally dead, though. Google has now pivoted to “an experimental *Android* WebView Media Integrity API [emphasis ours].” Unlike the web version, which would have been a big step “forward” for invasive DRM solutions, Android already has environment attestation, so it doesn’t sound like this is doing that much. Google said the inspiration for the original Web Integrity project was Android’s Play Integrity API, which already scans your phone for root privileges and denies access to things like games, media, and banking apps. Google now wants to be able to do that through embedded Android WebViews (web content displayed in apps), claiming that “media content providers” would be interested in such a thing.

If you are Spotify or YouTube, you could already block modified devices at the app level before the embedded WebView even boots up, via the Play Integrity API. Google also has a preinstalled unremovable Android DRM called “Widevine” made specifically for media playback. Netflix famously demands preinstallation of Widevine on devices in order to show HD content, and problems with the DRM are a common support issue.

Google obviously sees that this proposal is disliked, so its pivot to an Android WebView component suggests it has some specific internal need for locking down WebViews with DRM. Google is so suspiciously vague about these projects, though, that it’s hard to know what exactly the company’s intent is. The blog post notes that while Android’s WebView system brings “a lot of flexibility… it can be used as a means for fraud and abuse, because it allows app developers to access web content, and intercept or modify user interactions with it. While this has its benefits when apps embed their own web content, it does not prohibit bad actors from modifying content and, by proxy, misrepresenting its source.”

Other than the usual malware boogeymen, that sounds a lot like the use case of YouTube Vanced, a (now dead) modified YouTube Android app. Vanced used a WebView and tricked YouTube into playing ad-free videos and unlocked YouTube Premium features like background playback. Because Vanced was just an app, it didn’t require root and wasn’t stopped by the Play Integrity API. Allowing YouTube to reach into your phone via the WebView sounds like something that could shut down these “alternative” clients, though. Google has become increasingly hostile toward ad blockers in recent years, and while the Google legal department already killed YouTube Vanced with a cease-and-desist letter in 2022, having the technical department put a stake through the heart of modified clients sounds like the next plausible step.

https://arstechnica.com/?p=1981663