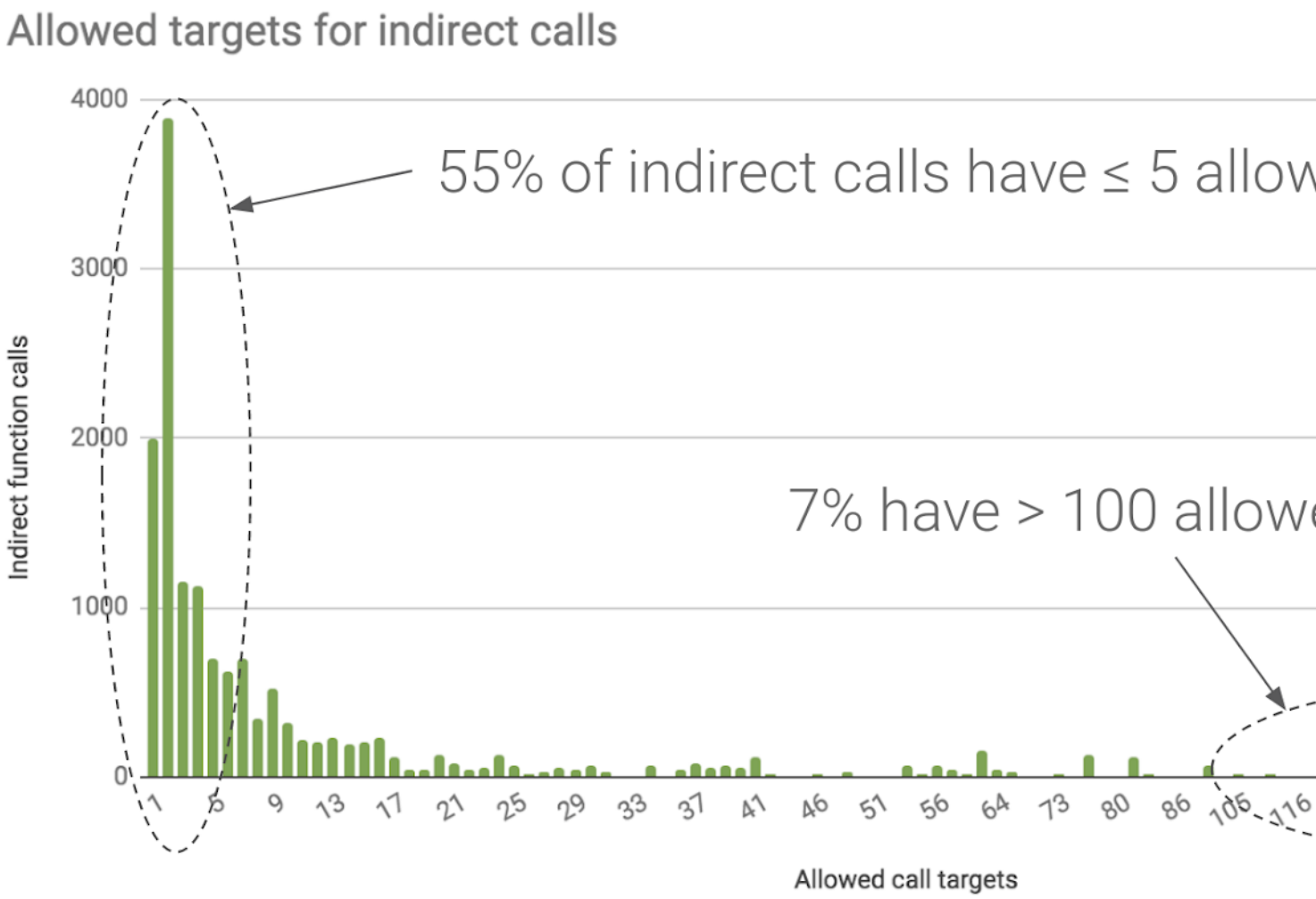
Control Flow Integrity in the Android kernel

By *Rianne Schestowitz*
Created *11/10/2018 - 12:04am*
Submitted by Rianne Schestowitz on Thursday 11th of October 2018 12:04:43 AM Filed under Android [1]



Android's security model is enforced by the Linux kernel, which makes it a tempting target for attackers. We have put a lot of effort into hardening the kernel in previous Android releases and in Android 9, we continued this work by focusing on compiler-based security mitigations against code reuse attacks.

Google's Pixel 3 will be the first Android device to ship with LLVM's forward-edge Control Flow Integrity (CFI)

enforcement in the kernel, and we have made CFI support available in Android kernel versions 4.9 and 4.14. This post describes how kernel CFI works and provides solutions to the most common issues developers might run into when enabling the feature.

[2]

Android

Source URL: http://www.tuxmachines.org/node/116369

Links:
[1] http://www.tuxmachines.org/taxonomy/term/143
[2] https://android-developers.googleblog.com/2018/10/control-flow-integrity-in-android-kernel.html