EXHIBIT F

Android Security 2016 Year In Review

March 2017

android

EXHIBIT 5

Contents

Overview

Google is committed to protecting the security and privacy of all Android users. Keeping more than 1.4 billion devices safe starts with a strong foundation—the core Android platform—which is strengthened by regular security updates for the platform, applications, and devices and constantly evolving security services that monitor and protect the ecosystem.

In 2016, Google worked closely with device manufacturers, system on a chip (SoC) providers, and telecom carriers to release security patches to more devices than ever before. We made key security features like data encryption and verified boot the standard for over one hundred million users. In addition to making devices more secure, we actively protected users from application threats by reducing the impact of Potentially Harmful Applications (PHAs) inside and outside of Google Play and improving the quality of security in hundreds of thousands of applications. Overall, devices, apps, and users are safer than ever.

Looking forward to 2017, we're working to increase the number of patched Android devices and accelerate adoption of key platform security features. We believe that advances in machine learning and automation can help reduce PHA rates significantly in 2017, both inside and outside of Google Play.

This is Google's third annual report on Android's security protections. The report covers new and updated features, provides metrics that informed our view of Android security, and discusses trends around security for Android devices in 2016.

Google security services for Android

Devices with Google Mobile Services (GMS) are protected straight out of the box by a complete set of endpoint security and antivirus services. This set includes both cloud-based and pre-installed on-device services that use

real-time data from the Android ecosystem to understand the security environment. Because Google's security services generally don't require firmware or platform-level patches to update, they provide a first line of defense against evolving security threats.

> By Q4 2016, fewer than 0.71% of devices had Potentially Harmful Applications (PHAs) installed and for devices that exclusively download apps from Google Play, that number was even smaller at 0.05%.

These small numbers are thanks in part to Google's responsive security services.

Google regularly enhances its security services for Android. In 2016, we used machine learning and statistical analysis to further automate and speed up detection of PHAs and other threats. Enhancements to the Safe Browsing service, which protects users from phishing sites and websites hosting malware, improved PHA device-scanning capabilities and enabled third-party developers to leverage the power of Safe Browsing in their own applications. Third-party developers took advantage of the security services offered through SafetyNet APIs, such as SafetyNet Attest, which serves nearly 200 million requests per day.

Android platform security

All Android devices share a common, platform-level security model. This model has been enhanced over multiple years with SELinux protections, application isolation using sandboxing, exploit mitigations, and cryptographic features, like file-based encryption and Verified Boot.

In 2016, Android expanded platform-level security with the launch of Android 7.0. We streamlined our boot-up process to make it easier to install over-the-air (OTA) security updates. To support this faster boot up, we implemented file-based encryption, which also better isolates and protects individual users and profiles on a device. We re-architected the mediaserver stack to address Stagefright-type vulnerabilities by adding integer overflow protections and compartmentalizing mediaserver's components into individual sandboxes with minimal privileges. We also increased the degree of randomness in address space layout randomization (ASLR), making some attacks more difficult.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.