EXHIBIT E

Android Security 2015 Year In Review

April 2016

android

EXHIBIT 4

Contents

Overview

Google is committed to ensuring that Android is a safe ecosystem for users and developers. We do that by investing in multiple layers of protection across a large and growing ecosystem. We provide security applications and services for Android, constantly strengthen the core Android platform, and foster an ecosystem rich with security innovation. We also regularly measure the effectiveness of these efforts by collecting, analyzing, and sharing data about the security of the Android ecosystem. We consider transparency to be critical, so our second annual Android Security Year in Review is intended to share the progress we've made with regards to security in the last year, as well as provide our view of the state of security in the Android ecosystem.

Google security services for Android

To protect the Android ecosystem and its users, Google provides a complete set of endpoint security services that is included automatically as part of Google Mobile Services (GMS). These include both cloud-based services and on-device services delivered as Android applications, so users don't have to install additional security services to keep their devices safe. In 2015, these services protected over 1 billion devices, making Google one of the world's largest providers of on-device security services.

In 2015, we increased our understanding of the ecosystem using automated systems that incorporate large-scale event correlation and machine learning to run more than 400 million automatic security scans per day on devices with Google Mobile Services. Thanks in part to these scans, successful exploitation of vulnerabilities on Android devices continued to be extremely rare during 2015. The largest threat was installation of Potentially Harmful Applications (PHAs), or applications that may harm a device, harm the device's user, or do something unintended with user data. On average, less than 0.5% of devices had a PHA installed during 2015 and devices that only installed applications

from Google Play averaged less than 0.15%. Ongoing protection by Verify Apps, which scans for PHAs, and SafetyNet, which protects from network threats—as well as actions taken by the Android Security Team—helped stop the spread of PHAs like Ghost Push and reduced Russian fraudware by over 80%. We also released the SafetyNet Attest API to help developers check device compatibility and integrity.

Android platform security

All Android devices share a common security model that provides every application with a secure, isolated environment known as an application sandbox. The Android security model has grown stronger over time, with further application isolation enabled by SELinux, enhanced exploit mitigations, and cryptographic features, such as full disk encryption and verified boot.

In 2015, Android continued to iterate and expand platform security technology with the launch of Android 6.0. Most new devices with Android 6.0 have a hardware root of trust and provide a verifiable good boot state. We introduced support for device fingerprint sensors, improving user security through ease of use. We changed the permission model so that users can see, grant, and revoke permissions for applications at a granular level, allowing for better control of the data and capabilities that each application can access. Encryption is now mandatory for all devices capable of supporting it, and has been extended to allow for encrypting data on SD cards. We continue to guide the Android ecosystem to widely adopt the strongest available security technologies.

Ecosystem security programs

Android also has a number of efforts under way to promote security best practices in the ecosystem. The Android Compatibility Definition Document and Compatibility Test Suite provide a detailed series of security requirements and tests to prove compatibility with these requirements. Google works with device manufacturers to ensure that current devices are secure, and to define a roadmap of constantly increasing security for devices (such as the requirement introduced in 2015 for most new Android devices to use encryption and verified boot). Google Play encourages application developers to adopt security best practices; we introduced policy changes that enhanced user data protection in 2015, and also notified developers about potential security issues, resulting in improvement of security for over 100,000 applications.

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.