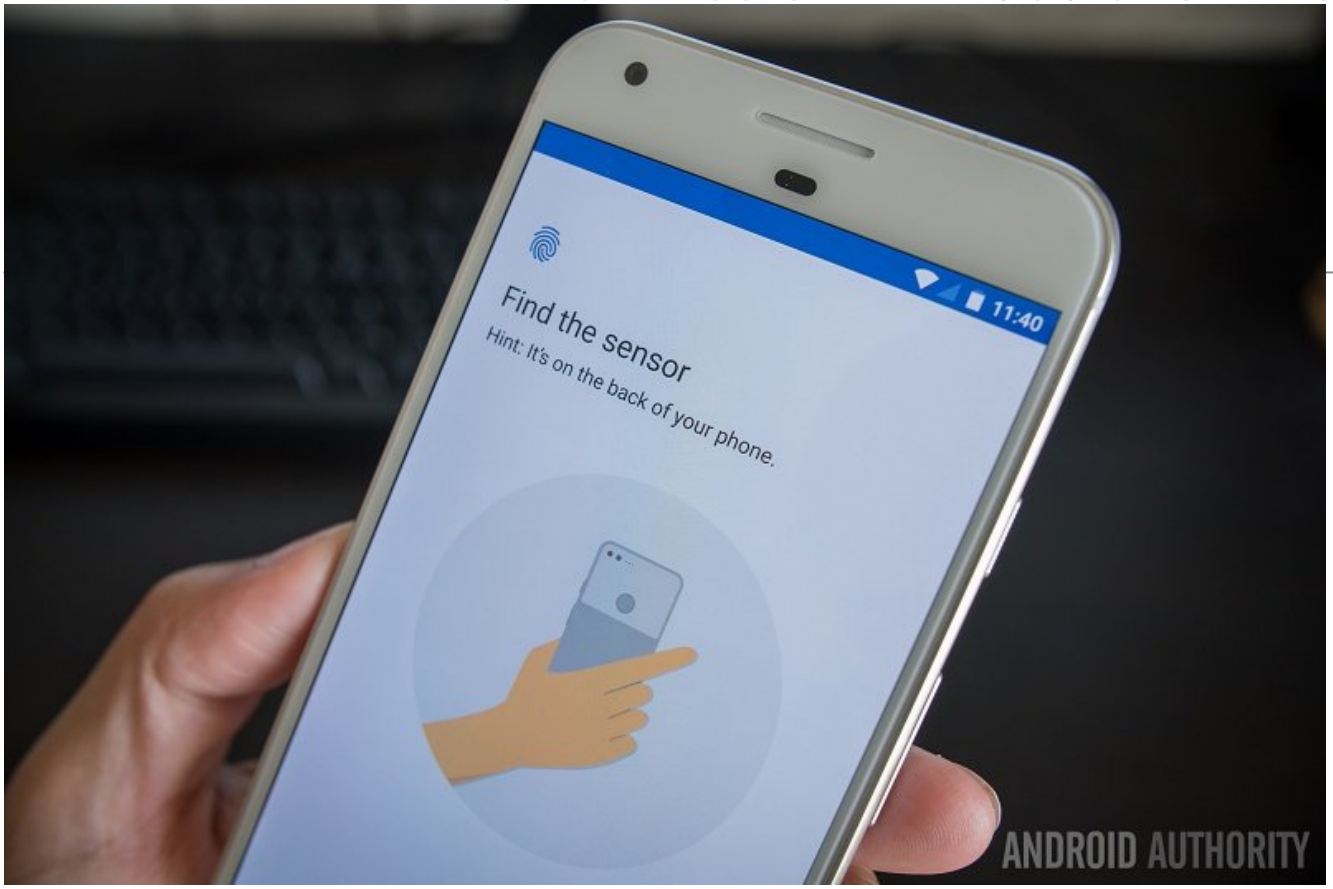
دلایل بهتر، سریع‌تر و مستحکم‌تر بودن پرچم‌دارهای جدید

گوگل فاش کرد چرا پیکسل‌ها امن‌ترین اسمارت‌فون‌های دنیا هستند



گوگل در تازه‌ترین پست خود در بلاگ گوگل Security از برنامه‌ها و قابلیت‌های امنیتی آخرین اسمارت‌فون خود صحبت کرد. عنوانی که گوگل برای این پست انتخاب کرده جالب توجه است: «گوگل پیکسل: بهتر؛ سریع‌تر؛ نیرومندتر».

دو نفر از مهندسان ارشد تیم نرم‌افزاری گوگل درباره نحوه به‌کارگیری و استفاده از سیستم رمزنگاری در اسمارت‌فون‌های پیکسل توضیحاتی را ابراز کردند. آن‌ها توضیح دادند که این سیستم به چه شکلی می‌تواند باعث بهبود "تجربه کاربر؛ کارایی و امنیت" در استفاده از اسمارت‌فون‌ها شود.

مطلب پیشنهادی

مشکلاتی که ما را کلافه می‌کنند
با این 10 راه حل ساده از مشکلات فناوری کلافه‌کننده خلاص شوید

روش‌های معمول رمزنگاری مانند «رمزنگاری فول دیسک» یا FDE که در حال حاضر در بسیاری از اسمارت‌فون‌های موجود در بازار به‌کار گرفته شده با روشی که گوگل برای محصول جدید خود استفاده کرده؛ متفاوت است. گوشی پیکسل برای این منظور از نوعی از رمزنگاری به‌نام «رمزنگاری مبتنی بر فایل» یا FBE استفاده می‌کند. روش کار این سیستم به این شکل است که فایل‌های مختلف با کلیدهای مختلف رمزنگاری می‌شوند، در نتیجه هرکدام از آن‌ها می‌توانند به‌طور جداگانه کدگشایی شوند.

گوگل می‌گوید آن‌ها با استفاده از این روش؛ صفحه‌های آنلاک و decrypt اسمارت‌فون را با هم ترکیب کرده‌اند تا کاربران قادر باشند بلافاصله بعد از بوت شدن دستگاه به اپلیکیشن‌هایی مانند Alarm Clock؛ تنظیمات دسترس‌پذیری و تماس‌های تلفنی دسترسی داشته باشند.

گوگل در پست اخیر خود؛ علاوه بر این مسئله به استفاده از نرم‌افزار TrustZone متعلق به شرکت ARM نیز اشاره کرده و گفته که به‌کارگیری این نرم‌افزار دو مزیت را برای آن‌ها به‌همراه داشته است. اول این‌که؛ TrustZone به اجرای فرآیند Verfified Boot شتاب بیشتری می‌دهد؛ به این معنی‌که اگر این سیستم تشخیص دهد که تغییراتی در سیستم‌عامل به‌وجود آمده؛ آن‌گاه کلیدهای رمزگشایی دیسک را تحت هیچ شرایطی برای رمزگشایی استفاده نمی‌کند. و دوم این‌که TrustZone یک زمان انتظار بین حدس‌هایی که در سمت کاربر زده می‌شود را درنظر می‌گیرد و اگر توالی حدس‌های نادرست ادامه داشته باشد؛ مسلما این فاصله زمانی افزایش پیدا می‌کند.

گوگل ادعا می‌کند اگر این روش مورد استفاده قرار بگیرد؛ تلاش برای یافتن الگوهای لاک اسکرین چهار نقطه‌ای یک اسمارت‌فون می‌تواند چیزی بیشتر از 4 سال زمان ببرد.

در آخر هم؛ گوگل اضافه می‌کند که روش رمزنگاری eCryptFS که بر پایه استاندارد صنعتی استوار است را به‌دلیل برآورده نشدن نیازهای کارایی از سیستم حذف کرده است. این روش رمزنگاری مستقیما داخل سیستم فایل ext4 آندروید نصب می‌شود. گوگل در این خصوص می‌گوید که کارایی روش رمزنگاری ext4 شبیه رمزنگاری فول دیسک است و از نظر کارایی هیچ تفاوتی با راه‌کار تنها-نرم‌افزار ندارد.

منبع:

اندروید آتوریتی
تاریخ انتشار:
29 آبان 1395

نشانی منبع: https://www.shabakeh-mag.com/gadget/5527