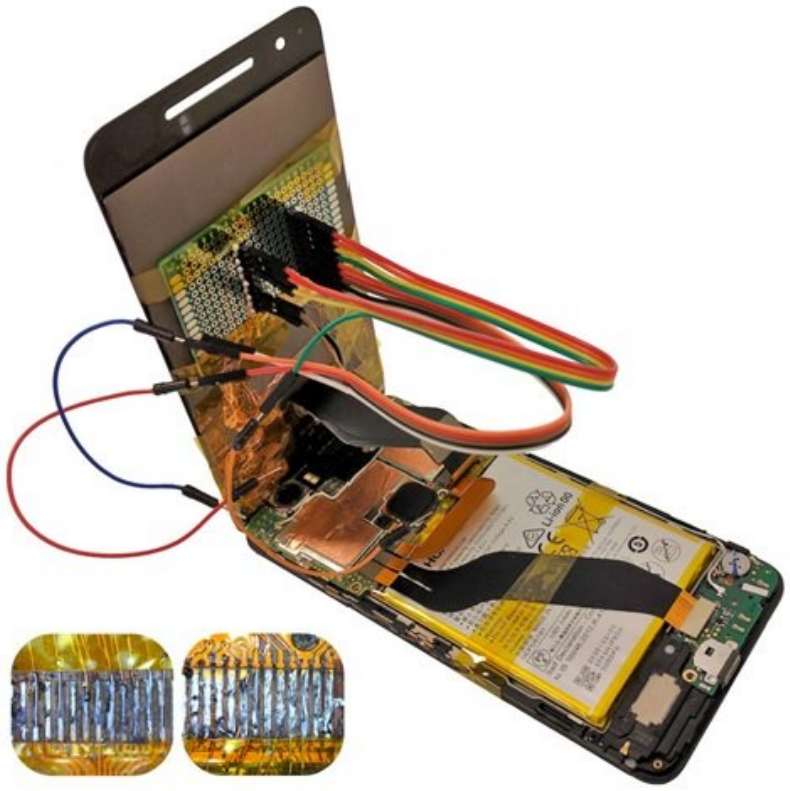
هشدار: صفحه‌نمایش‌های تقلبی باعث هک شدن گوشی‌های هوشمند می‌شوند



پژوهشی که نتایج آن به تازگی منتشر شده نشان می‌دهد کاربرانی که گوشی هوشمند آن‌ها به صفحه‌نمایش‌های تقلبی تجهیز شده است، ممکن است در معرض تهدید هکرها قرار داشته باشند. به واسطه آن‌که ماژول مایکروکنترلر ممکن است راه را برای نفوذ هکرها هموار سازد.

در گزارشی که نتایج آن به تازگی منتشر شده آماده است فرآیندی همچون تعویض صفحه‌نمایش که در ظاهر کاری بی خطر و ساده به نظر می‌سد ممکن است راه را برای نفوذ هکرها مهیا سازد. در این پژوهش آماده است که تبلت‌ها نیز ممکن است در معرض چنین خطری قرار داشته باشند. مشکل فوق در ارتباط با تراشه‌ای است که فرآیند ضبط داده‌های ورودی را مدیریت می‌کند. این تیم تحقیقاتی پس از تعویض صفحه‌نمایش مربوط به گوشی‌های نکسوس 6 پی و ال‌جی جی پد 7 (LG pad 7.0) این شانس را به دست آوردند تا همه ورودهای صفحه‌کلید کاربر را ضبط کرد، در ادامه دوربین گوشی را هک کرده و در نهایت به برنامه‌های کاربردی دست پیدا کنند. به‌طوری که در نهایت هکرها امکان کنترل سیستم‌عامل گوشی هوشمند کاربر را به دست می‌آورند. پژوهشگران می‌گویند نمایشگرهای تقلبی به نمایشگرهای اصلی شباهت زیادی دارند، به‌طوری که در بعضی موارد حتا تکنسین‌های حرفه‌ای نیز قادر به تشخیص این موضوع نیستند. جالب‌تر آن‌که پژوهشگران گفته‌اند که در مدت زمان هک نیازی نیست تغییری در سیستم مدیریت فایلی دستگاه قربانی به وجود آید. همین موضوع باعث می‌شود تا ضدویروس‌ها نیز قادر به تشخیص این مسئله نباشند. پژوهشگران نام حمله فوق را تراشه در میان (chip-in-the-middle) گذاشته‌اند. در این پژوهش کارشناسان امنیتی از یک ماژول میکرو کنترلر نوع ATmega328 که به بورد آردینو مجهز بود استفاده کردند. آن‌ها همچنین از ماژول میکروکنترلر STM32L432 نیز استفاده کردند. البته پژوهشگران فوق گفته‌اند که در این زمینه می‌توان از مایکروکنترلرهای دیگر نیز استفاده کرد. در ادامه با دمیدن جریان هوای گرم، این امکان به وجود می‌آید تا بخش کنترل لمسی را از برد اصلی جدا کرده و تراشه مدنظر را از طریق یک سیم مسی که به برد لحیم‌کاری شده است در میان این صفحه قرار داد. پژوهشگران گفته‌اند که مشکل نمایشگرهای تقلبی تنها مختصر دستگاه‌های اندرویدی نبوده و حتا گوشی‌های آی‌فون نیز ممکن است به همین شکل در معرض تهدید هکری قرار گیرند.

تاریخ انتشار:

31 مرداد 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/9291/%D9%87%D8%B4%D8%AF%D8%A7%D8%B1-%D8%B5%D9%81%D8%AD%D9%87%E2%80%8C%D9%86%D9%85%D8%A7%DB%8C%D8%B4%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AA%D9%82%D9%84%D8%A8%DB%8C-%D8%A8%D8%A7%D8%B9%D8%AB-%D9%87%DA%A9-%D8%B4%D8%AF%D9%86-%DA%AF%D9%88%D8%B4%DB%8C%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%87%D9%88%D8%B4%D9%85%D9%86%D8%AF-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF