禪

حریم خصوصی در محاصره اصوات

برخی برنامههای موبایل از سیگنالهای صوتی جاسوسی میکنند

مجله فورچون میگوید : «ارواح درون گوشی هوشمند، تبلت یا کامپیوتر شما همواره در حال گوش کردن هستند.» فناوری ویژهای که کمیسیون تجارت فدرال (TFC) و ناظران امنیت کامپیوتر درباره آن هشدار دادهاند، ردیاب مافوق صوت چند-دستگاهی (uXDT) نام دارد . این فناوری که در همه دستگاهها وجود دارد به راحتی میتواند حریم خصوصی ما را رصد میکند .

پژوهشگران دانشگاهی کالج لندن مطابق با برنامه زمانبندی شده و همزمان با آغاز به کار کنفرانس بلکهت (یکم تا چهارم نوامبر) به تشریح روشی پرداختند که با استفاده از آن نرمافزارهای بازاریابی قادر هستند اصوات مافوق صوت را رهگیری کرده و به این شکل حریم خصوصی و امنیت کاربران را در معرض خطر قرار دهند . گزارش مفصل این تحقیق در کنفرانس بلکهت که در حال حاضر در لندن برگزار میشود در معرض دید همگان قرار گرفت. این گروه تحقیقاتی نشان دادند چطور یک تلفن همراه میتواند تشخیص دهد شما در حال تماشای چه برنامه تلویزیونی هستید و همچنین چگونه میتوان از تبلت شما به منظور جمعآوری تاریخچهای از بازدیدهای وب استفاده کرد . در هر دو حالت، یک برنامه کاربردی روی دستگاه همراه شما اجرا شده و حتا زمانی که به اجرای برنامه کاربردی خاتمه دهید، این برنامه باز هم قادر است به این اطلاعات گوش کرده و آنها را به اشتراک قرار دهد .

مطلب پیشنهادی

در خدمت سرویس مخفی میکروفون

حملاتِ فیزیکیِ برای اِستخراج کلیدهای رمزنگاری

FTC از مدتها قبل به طراحان در رابطه با خطراتی که به کارگیری کدهای Sliverpush آنها را تهدید میکند، هشدار داده بود . با این وجود، فورچون معتقد است FTC آنگونه که باید و شاید نتوانسته است، به کاربران عادی در ارتباط با پیامدهای این فناوری هشدار داده و رهنمودهای لازم برای حفظ حریم خصوصی را در اختیار آنها قرار دهد . در نتیجه این مدل برنامهها میتوانند آنچه کاربران در تلویزیون خود به تماشای آنها مینشینند را حتا زمانی که کاربران به اجرای این برنامهها خاتمه میدهند تحت نظارت خود قرار دهند . تیم UCL در بخش دیگری از تحقیق خود عنوان کرده است که دامنه این تهدید به مراتب مخربتر از آن چیزی است که توصیف شده است.

به طوری که این برنامهها نه تنها قادر به جمعآوری اطلاعاتی هستند که به طور عادی به دست نمیآیند، بلکه قادر هستند به طور بالقوه و مستمر به سیگنالهای فراصوت گوش کرده، آنها را تحت نظر گرفته و فراتر از آن کلیدهایی که از سوی کاربران فشرده میشوند را رهگیری کنند . به دلیل اینکه این فناوری در همه دستگاهها کار میکند، در نتیجه قادر است بدون آنکه به وایفای، بلوتوث یا دیگر ارتباطات شبکهای نیازی باشد از شکاف هوایی کامپیوترها استفاده کرده و زمانی که سامانهایی برای انجام محاسبات امنیتی مورد استفاده قرار میگیرد از طریق میکروفون یک گوشی هوشمند، تبلت یا کامپیوتر دیگری که در محدوده سیگنالهای فراصوت قرار دارد به شنود اطلاعات بپردازد .

مطلب پیشنهادی

بدافزار جدید پژوهشگران شناسایی نقاط ضعف سیستمها

سرقتِ اطلاعاتِ از ِطریقِ فنِ کامپیوتر

پژوهشگران UCL میگویند، نرمافزارهایی که فاقد گزینههای انتخابی هستند به طور بالقوه یک خطر جدی در زمینه افشای اطلاعات به شمار میروند . واسلیو ماورودیس، از اعضا تیم UCL در این ارتباط به New Scientist گفته است: «رشد فزاینده اینترنت اشیا ریسک دسترسی به امواج مافوق صوت را افزایش داده است. به دلیل اینکه تجهیزات اینترنت اشیا امروزه از هیچ استاندارد جامعی در ارتباط با تامین امنیت سیگنالهای فراصوت استفاده نمیکنند .»

اوایل ماه جاری میلادی بود که حمله منع سرویس انکار شده گستردهای به مدد تجهیزات اینترنت اشیا سامانه نام دامنه را تحت الشعاع خود قرار داد . در همین ارتباط، تیم UCL برای دستگاههای اندرویدی وصلهای را طراحی کرده است که به کاربران کمک میکند در زمان استفاده از برنامههای کاربردی مدیریت بهتری بر سیگنالهای فراصوت داشته باشند . اما این تنها آغاز راه است . این تهدید از سوی نرمافزارهایی که در دستگاههای همراه مورد استفاده قرار گرفته و قادر هستند به طور نامحسوس دادهها را رصد کنند رو به افزایش است . در نتیجه سازمانهای جهانی باید به فکر مکانیزمهای کنترلی قدرتمندی در این زمینه باشند .

نویسنده :

حمیدرضا تائبی

دسته بندی:
امنیت
تاریخ انتشار :
10:37 - 14/08/1395
برچسب:
امنیت - مافوق صوت - تبلت - گوشی هوشمند - استراق سمع - سیگنال - uXDT

□□□□□ منبع: https://www.shabakeh-mag.com/security/5318