دنیای موبایل شماره 183

ساعتهای نهچندان هوشمند !

ابزارهای همراه پوشیدنی نظیر ساعتهای هوشمند طرفداران زیادی دارند و پیشبینی میشود فروش جهانی آنها در چهار سال آینده به حدود سی میلیارد دلار برسد . بحث امنیت این ابزارها همیشه مطرح بوده است و این موضوع از جنبههای مختلفی بررسی و درباره آن اظهار نظر شده است .

محققان انستیتوی فناوری Stevens در مطالعهای جدید، به یکی از چالشهای امنیتی ابزارهای پوشیدنی پی بردهاند . ابزارهایی نظیر ساعتهای هوشمند میتوانند حرکات دست را تشخیص دهند و آنها را به طور پیوسته و خودکار ثبت کنند . در نتیجه اگر هنگام کار با یک دستگاه خودپرداز، ساعت هوشمند به دست داشته باشید، این احتمال وجود دارد که هکرها با به دست آوردن اطلاعات ثبتشده توسط ساعت و با تلاش اندکی، رمز عبور کارت بانکیتان را با دقتی بیش از 90 درصد حدس بزنند.

Yingying Chen، استاد برق و کامپیوتر Stevens که سرپرستی این تحقیق را بر عهده داشته است، میگوید : «نتایج این تحقیق حتی برای کسانی که با این حوزه آشنا هستند هم باعث شگفتی بود . آنطور که پیداست، برای مجرمان به دست آوردن اطلاعات محرمانه کاربران ابزارهای پوشیدنی، سادهتر از آن چیزی است که به نظر میرسد ». گروه Stevens، از بیست داوطلب که انواعی از مچبندهای سلامتی و ساعتهای هوشمند به دست داشتند، درخواست کردند پنج هزار کد رمز (PIN) را از طریق کیپد یا صفحهکلید لپتاپ وارد کنند و اطلاعاتی را که از این ابزارهای پوشیدنی برای تلفن هوشمند داوطلبان ارسال میشد، شنود میکردند . ناگفته نماند این دادهها از حسگرهای دستگاه پوشیدنی با BLE یا بلوتوث کمتوان برای تلفن هوشمند ارسال میشود.

مطلب پیشنهادی

دنیای موبایل شماره 182

بازیافت زبالههای الکترونیکی

به گفته این محققان چنین حملهای به دو صورت قابل اجرا است: روش نخست «شنود دادهها » (Sniffing attacks) است و روش دیگر «حملات داخلی از طریق بدافزارها ». در حمله نوع اول، مجرم میتواند با قرار دادن دستگاه ویژهای در نزدیکی فرد، دادههای ارسالی از ساعت به گوشی را به طور بیسیم شنود کند . در حمله نوع دوم، مهاجم برای به دست آوردن اطلاعات، از یک نرمافزار جاسوسی نصبشده روی ابزار پوشیدنی استفاده کرده و دادههای حسگرها را جمعآوری میکند . گروه Chen بعد از جمعآوری دادههای شتابسنج، ژیروسکوپ و مغناطیسسنج، حرکات تقریبی دست کاربر - فاصله دکمههای فشردهشده و ترتیب فشردن دکمهها- را به دست آوردند و موفق شدند با استفاده از الگوریتمی که طراحی کردند، رمزهای چهار رقمی را حدس بزنند .

برای این کار، به طرح استاندارد کیپدهای ورود رمز و صفحهکلیدها دقت شد . یکی از نکاتی که استفاده شد، توجه به این واقعیت بود که تقریباً همه کاربران بعد از وارد کردن رمز، دکمه ورود (enter) را میزنند . اگر چه از میان ابزارهای استفادهشده در این آزمون، برخی امنیت بیشتری داشتند، به طور متوسط 80 درصد حدسها صحیح بود و با پنج بار تکرار، میزان دقت در برخی ابزارها تا 99 درصد افزایش مییافت. Chen معتقد است در این زمینه باید تحقیقات بیشتری انجام شود، اما اضافه میکند که با اینکه ابزارهای پوشیدنی بهسادگی هک نمیشوند، اما باید توجه کرد که این کار غیرممکن نیست .

نویسنده :

مهدی صنعتجو

دسته بندی:

شاهراه اطلاعات

تاریخ انتشار :

04:39 - 09/06/1395

برچسب:

دنیای موبایل - امنیت ساعت هوشمند - ساعت هوشمند

□□□□□ منبع: https://www.shabakeh-mag.com/information-feature/4340