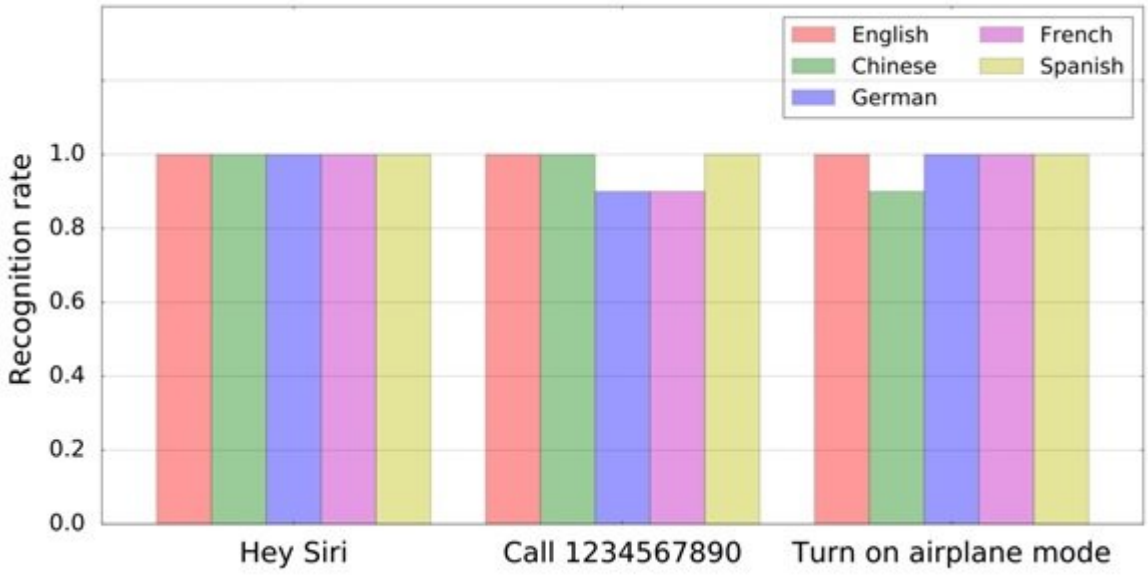
ارسال امواج فراصوت برای هک

هک سیری و الکسا با رخنه‌ای در مکانیزم صوتی آن‌ها

بسیاری از نفوذها بر مبنای اشتباهات کاربران رخ می‌دهد، اما در بعضی موارد می‌توانید شرکت‌های امنیتی را در این ارتباط سرزنش کنید. در همین ارتباط گروهی از پژوهشگران دانشگاه ژجیانگ چین اعلام کرده‌اند آسیب‌پذیری‌هایی را در الکسا و آمازون شناسایی کرده‌اند.

این گروه از پژوهشگران بر مبنای تکنیک ارسال صدا از طریق فرکانس فراصوت موفق شده‌اند الکسا و سیری را فریب دهند تا یک سایت آلوده را باز کند. جالب‌تر آن‌که پژوهشگران اعلام داشته‌اند که از این تکنیک می‌توان برای باز کردن قفل‌های هوشمند درب‌هایی که به این دستیاران مجازی مرتبط شده‌اند استفاده کرد. گوش انسان قادر نیست امواج فراصوت را بشنود، اما در مقابل میکروفون نصب شده روی گوشی‌های هوشمند به خوبی می‌تواند این اصوات را دریافت کند. این روش حمله به نام DolphinAttack شهرت دارد. در این مکانیزم حمله پژوهشگران صدای انسان‌ها را به فرکانس‌های مافوق صوت فراتر از 20000 هرتز تبدیل می‌کنند. زمانی که این تبدیل انجام شد در مرحله بعد می‌توان با استفاده از یک اسمارت‌فون معمولی که سه مولفه آمپلی‌فایر، فرستنده فراصوت و باتری در آن قرار دارد این صوت را ارسال کرد. البته از این تکنیک برای حمله به همه دستیاران صوتی همچون سیری، گوگل اسیستنت، S Voice، آلکسا و دستگاه‌هایی همچون آی‌پادها، مک‌بوک‌ها، اکو آمازون، آئودی Q3 و اسمارت‌فون‌ها استفاده کرد. پژوهشگران گفته‌اند در مجموع 16 فرمان صوتی که گوش انسان نمی‌تواند آن‌ها را بشنود را با سامانه‌های تشخیص صدا تفسیر کرد.



این گروه موفق شدند فرمان‌های Open Dolphinattack.com، Call 123-556-7890 و Open the back door را با موفقیت به مرحله اجرا در آورند. البته این تکنیک حمله دارای محدودیت‌هایی نیز هستند. به‌طور مثال دستگاه هدف باید در فاصله 5 تا 6 فوتی ارسال کننده فراصوت قرار داشته باشد. اما اگر هکرها از یک تقویت‌کننده امواج استفاده کنند قادر هستند حمله خود را از فاصله دورتری اجرا کنند. همچنین این حمله زمانی موفقیت‌آمیز خواهد بود که دستیار شخصی روی اسمارت‌فون قربانی فعال باشد تا بتواند دستورات را دریافت کند. با توجه به این‌که دستیاران صوتی در زمان پاسخ‌گویی به دستورات اعلانی را به کاربران نشان می‌دهند در نتیجه احتمال این‌که حمله فوق در همه موارد جواب دهد خیلی کم خواهد بود. به جزء زمان‌هایی که در مکان‌های شلوغی قرار دارید یا زمانی که قفل اسمارت‌فون شما باز باشد و در نزدیکی هکری قرار داشته باشید. در این حالت احتمال سرقت اطلاعات یا ورود بدافزار به گوشی شما به واسطه بازدید از یک سایت مخرب وجود دارد. این گروه گفته‌اند شرکت‌های سازنده دستیاران صوتی می‌توانند با یک راهکار ساده مانع اجرای این حمله شوند. کافی است آن‌ها مانع شناسایی فرکانس‌های بالای 20 هزار هرتز روی گوشی‌های هوشمند شوند. اما این راهکار یک عیب بزرگ نیز دارد. بعضی از دستگاه‌ها و منجمله گوشی‌های هوشمند در بعضی موارد از طریق این اصوات با یکدیگر ارتباط برقرار کنند!

تاریخ انتشار:
26 شهریور 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/world/9564/%D9%87%DA%A9-%D8%B3%DB%8C%D8%B1%DB%8C-%D9%88-%D8%A7%D9%84%DA%A9%D8%B3%D8%A7-%D8%A8%D8%A7-%D8%B1%D8%AE%D9%86%D9%87%E2%80%8C%D8%A7%DB%8C-%D8%AF%D8%B1-%D9%85%DA%A9%D8%A7%D9%86%DB%8C%D8%B2%D9%85-%D8%B5%D9%88%D8%AA%DB%8C-%D8%A2%D9%86%E2%80%8C%D9%87%D8%A7