کد خبر: ۴۰۴۱۶۳
دوشنبه ۱۳ تیر ۱۴۰۱ ۱۶:۵۲

هک گوشی آیفون خاموش ممکن است؟

از نظر تئوری، سرقت کلید مجازی از آیفون امکان‌پذیر است، حتی اگر دستگاه خاموش باشد.

به گزارش سایت خبری پرسون، محققان آزمایشگاه شبکه‌های موبایل امن در دانشگاه Darmstadt آلمان مقاله‌ای را منتشر کرده‌اند که در آن روشی نظری برای هک کردن آیفون، حتی اگر دستگاه خاموش باشد، توضیح داده شده است. در این مقاله که در وب‌سایت کسپراسکای منتشر شده، عملکرد ماژول‌های بی‌سیم بررسی شده و راه‌هایی برای تجزیه و تحلیل سیستم عامل بلوتوث و در نتیجه معرفی بدافزارهایی که قادر به اجرای کاملا مستقل از iOS، سیستم عامل دستگاه آیفون هستند را کشف کردند.

با کمی تخیل، تصور سناریویی که در آن مهاجم یک گوشی آلوده را نزدیک دستگاه قربانی نگه می‌دارد و بدافزاری را به آن منتقل می‌کند و سپس اطلاعات کارت پرداخت یا حتی کلید ماشین مجازی را به سرقت می‌برد، دور از ذهن نیست. محققان کارهای زیادی را برای تجزیه و تحلیل عملکرد غیرمستند تلفن، مهندسی معکوس سیستم عامل بلوتوث آن و مدل‌سازی سناریوهای مختلف برای استفاده از ماژول‌های بی‌سیم انجام دادند.

طبق این تحقیقات، اگر دستگاهی خاموش است، اما تعامل با آن (مثلاً هک) هنوز ممکن است، پس به نظر می رسد که دستگاه کاملاً خاموش نیست. اما سوال پیش می‌آید که چگونه به این نتیجه رسیدیم که خاموش کردن چیزی لزوماً به معنای خاموش بودن آن نیست؟

حالت کم‌مصرف اپل

اپل در سال ۲۰۲۱، اعلام کرد که سرویس Find My که برای مکان‌یابی دستگاه گم‌شده استفاده می‌شود، حتی اگر دستگاه خاموش باشد، همچنان کار خواهد کرد. این ویژگی در تمام گوشی‌های هوشمند اپل از زمان آیفون ۱۱ در دسترس است. به عنوان مثال، اگر گوشی خود را در جایی گم کنید و باتری آن پس از مدتی تمام شود، به‌طور کامل خاموش نمی‌شود، بلکه به حالت Low Power Mode می‌رود که در آن تنها مجموعه بسیار محدودی از ماژول‌ها همچنان فعال خواهند ماند. اینها در درجه اول ماژول‌های بی‌سیم بلوتوث و Ultra WideBand (UWB) و همچنین NFC هستند.

بلوتوث در حالت کم‌مصرف برای انتقال داده استفاده می‌شود، در حالی که از UWB برای تعیین مکان گوشی هوشمند استفاده می‌شود. در حالت کم‌مصرف، گوشی هوشمند اطلاعاتی را درباره خود ارسال می‌کند که آیفون‌های عابران می‌توانند آن‌ها را دریافت کنند. اگر صاحب یک تلفن گمشده به‌صورت آنلاین وارد حساب اپل خود شود و قسمت گوشی گمشده را علامت‌گذاری کند، از اطلاعات گوشی‌های هوشمند اطراف برای تعیین محل نگهداری دستگاه و پیدا شدن آن استفاده می‌شود.

این مقاله به‌سرعت بحثی را در میان کارشناسان امنیت اطلاعات در مورد خطرات امنیتی بالقوه آیفون برانگیخت. یک تیم تحقیقاتی از آلمان تصمیم گرفت تا سناریوهای حمله احتمالی را در عمل آزمایش کند. اول از همه، محققان تجزیه و تحلیل دقیقی از سرویس Find My را در حالت کم‌مصرف انجام دادند و برخی از ویژگی‌های ناشناخته قبلی را کشف کردند. پس از خاموش شدن، بیشتر کار توسط ماژول بلوتوث انجام می‌شود که توسط مجموعه‌ای از دستورات iOS بارگیری و پیکربندی می‌شود. سپس به‌صورت دوره‌ای بسته‌های داده را از طریق هوا ارسال می‌کند و به دستگاه‌های دیگر اجازه می‌دهد که آیفون واقعاً خاموش را تشخیص دهند.

مشخص شد که مدت زمان این حالت محدود است: در نسخه iOS ۱۵.۳ تنها ۹۶ جلسه پخش با فاصله ۱۵ دقیقه تنظیم شده است. یعنی یک آیفون گم‌شده و خاموش فقط برای ۲۴ ساعت قابل یافتن خواهد بود. اگر تلفن به دلیل باتری کم خاموش شود، این زمان کوتاه‌تر می‌شود. در این تحقیقات اما یک اشکال واقعی نیز پیدا شد: گاهی اوقات هنگامی که تلفن خاموش است، حالت "beacon" به هیچ وجه فعال نمی شود، در حالی که باید فعال شود.

حمله به تلفن خاموش

در واقع، کشف اصلی تیم این بود که سیستم عامل ماژول بلوتوث رمزگذاری نشده است و توسط فناوری Secure Boot محافظت نمی‌شود. فناوری Secure Boot شامل تأیید چندمرحله‌ای کد برنامه در هنگام راه‌اندازی است، به‌طوری که فقط سیستم عامل مجاز سازنده دستگاه می‌تواند اجرا شود.

فقدان رمزگذاری امکان تجزیه و تحلیل سخت‌افزار و جست‌وجوی آسیب‌پذیری‌ها را فراهم می‌کند که بعداً می‌تواند در حملات مورد استفاده قرار گیرد. اما عدم وجود Secure Boot به مهاجم اجازه می‌دهد تا فراتر رفته و به‌طور کامل کد سازنده را با کد خود جایگزین کند، که سپس ماژول بلوتوث آن را اجرا می‌کند. برای مقایسه، تجزیه و تحلیل سخت‌افزار ماژول UWB آیفون نشان داد که توسط Secure Boot محافظت می‌شود، هر چند که سیستم عامل آن رمزگذاری نشده است.

البته این برای یک حمله جدی و عملی کافی نیست. برای این کار، مهاجم باید سخت‌افزار را تجزیه و تحلیل کند، سعی کند آن را با چیزی که خودش ساخته است جایگزین کند و به دنبال راه‌هایی برای نفوذ باشد. نویسندگان مقاله مدل تئوریک حمله را با جزئیات توضیح می‌دهند، اما عملا نشان

نمی‌دهند آیفون از طریق بلوتوث، NFC یا UWB قابل هک است. آنچه از یافته‌های آنها مشخص است، این است که اگر این ماژول‌ها همیشه روشن باشند، آسیب‌پذیری‌ها نیز همیشه کار خواهند کرد.

اپل تحت تاثیر این مقالات و تحقیقات قرار نگرفت و از پاسخ دادن خودداری کرد، اپل تمام تلاش خود را می‌کند تا اسرار خود را مخفی نگه دارد، محققان باید با کدهای نرم‌افزاری که اغلب رمزگذاری شده‌اند، روی سخت‌افزار خود اپل، با ماژول‌های شخص ثالث سروکار داشته باشند تا تست‌های لازم را انجام دهند. تلفن هوشمند یک سیستم بزرگ و پیچیده است که تشخیص آن سخت است، به‌خصوص اگر سازنده به جای کمک، مانع شود.

دستگاه نیمه‌خاموش

مقاله نتیجه می‌گیرد که سیستم عامل بلوتوث به اندازه کافی محافظت نمی‌شود. از نظر تئوری می‌توان آن را در iOS تغییر داد یا همان حالت کم‌مصرف را با گسترش یا تغییر عملکرد آن دوباره برنامه‌ریزی کرد. سخت‌افزار UWB را نیز می‌توان از نظر آسیب‌پذیری بررسی کرد. اما مشکل اصلی این است که این ماژول‌های بی‌سیم و همچنین (NFC) به‌طور مستقیم با محصور محافظت‌شده Secure Element ارتباط برقرار می‌کنند. که ما را به برخی از هیجان‌انگیزترین نتایج این مقاله می‌رساند: از نظر تئوری، سرقت کلید مجازی از آیفون امکان‌پذیر است، حتی اگر دستگاه خاموش باشد.

اگر آیفون کلید ماشین باشد، از دست دادن دستگاه می‌تواند به معنای از دست دادن ماشین باشد. با این حال، تلفن واقعی در زمانی که کلید به سرقت رفته است، در اختیار شما باقی می‌ماند. اینطور تصور کنید: یک مزاحم در مرکز خرید به شما نزدیک می‌شود، گوشی خود را به کیف شما می‌کشد و کلید مجازی شما را می‌دزدد، در حالی که تلفن همراه همچنان در اختیار شما است.

از نظر تئوری می‌توان داده‌های ارسال‌شده توسط ماژول بلوتوث را تغییر داد و به‌منظور استفاده از گوشی هوشمند برای جاسوسی از قربانی از آن استفاده کرد، حتی اگر تلفن خاموش باشد. دزدیده شدن اطلاعات کارت پرداخت از گوشی شما یک احتمال تئوری دیگر است. همه اینها البته هنوز اثبات نشده است. کار تیم آلمانی بار دیگر نشان می‌دهد که افزودن قابلیت‌های جدید خطرات امنیتی خاصی را به همراه دارد که باید در نظر گرفته شود. به‌خصوص وقتی واقعیت بسیار متفاوت از تصور است: فکر می‌کنید تلفن شما کاملاً خاموش است، در حالی که در واقع اینطور نیست.

البته این یک مشکل جدید نیست، وقتی مادربرد لپ‌تاپ یا رایانه رومیزی به منبع برق متصل می‌شود، موتور مدیریت اینتل و فناوری AMD Secure، که حفاظت از سیستم و مدیریت از راه دور ایمن را نیز انجام می‌دهند همچنان فعال هستند. همانند باندل بلوتوث/UWB/NFC/Secure Element در آیفون‌ها، این سیستم‌ها دارای حقوق گسترده‌ای در داخل کامپیوتر هستند و آسیب‌پذیری‌های موجود در آنها می‌تواند بسیار خطرناک باشد. این مقاله هیچ تاثیر فوری بر کاربران عادی ندارد و داده‌های به‌دست‌آمده در این مطالعه برای یک حمله عملی کافی نیست، اما به‌عنوان یک راه‌حل مطمئن، نویسندگان پیشنهاد می‌کنند که اپل باید یک سوئیچ سخت‌افزاری را اجرا کند که برق گوشی را به‌طور کامل قطع کند.

منبع: عصر ایران